Citrix Virtual Apps and Desktops 7 2308

Contents

Citrix Virtual Apps and Desktops 7 2308

January 7, 2024

Citrix Virtual Apps and Desktops 7 2308

April 3, 2024

Informazioni sulla versione

Questa versione di Citrix Virtual Apps and Desktops include nuove versioni di Windows Virtual Delivery Agent (VDA) e nuove versioni di diversi componenti principali. È possibile effettuare le seguenti operazioni:

- **Installare o aggiornare un sito**: utilizzare l'ISO di questa versione per installare o aggiornare i componenti principali e i VDA. L'installazione o l'aggiornamento alla versione più recente consente di utilizzare le funzionalità più recenti.
- **Installare o aggiornare i VDA in un sito esistente**: se si dispone già di una distribuzione e non si è pronti per l'aggiornamento dei componenti principali, è comunque possibile utilizzare alcune delle più recenti funzionalità HDX installando (o eseguendo l'aggiornamento a) un nuovo VDA. L'aggiornamento dei soli VDA può essere utile quando si desidera testare i miglioramenti in un ambiente non di produzione.

  Dopo aver aggiornato i VDA a questa versione (dalla versione 7.9 o successiva), non è necessario aggiornare il livello funzionale del catalogo macchine. Il valore 7.9 (or later) [7.9 (o successivo)] rimane il livello funzionale predefinito ed è valido per questa versione. Per ulteriori informazioni, vedere Versioni VDA e livelli funzionali.

Per istruzioni di installazione e aggiornamento:

- Se si sta creando un nuovo sito, seguire la sequenza in Installazione e configurazione.
- Se si sta aggiornando un sito, vedere Aggiornare una distribuzione.

Citrix Virtual Apps and Desktops 7 2308

Supporto di Windows Server Core 2022

È ora possibile utilizzare Windows Server Core 2022 per Delivery Controller, Studio e Director. Per ulteriori informazioni, vedere Requisiti di sistema.

Comandi PowerShell per gestire la cache host locale (LHC)

È ora possibile utilizzare i comandi PowerShell per gestire LHC sui Delivery Controller. Per ulteriori informazioni, vedere Comandi PowerShell della cache host locale.

Supporto di SQL Server 2022

È ora possibile anche usare SQL Server 2022 per salvare le configurazioni del proprio sito. Per ulteriori informazioni, vedere Requisiti di sistema.

Bilanciamento verticale del carico a livello di sito per le implementazioni locali

È ora possibile utilizzare Vertical Load Balancing (VLB) a livello di sito per le implementazioni locali per risparmiare sui costi implementando più sessioni possibile in una macchina prima di passare alla macchina successiva e accenderla.

Supporto del provisioning cloud tramite una licenza di prova di 30 giorni

È ora possibile avere tutte le funzionalità relative al cloud che fanno parte della licenza di abbonamento Citrix Universal utilizzando una versione di prova di 30 giorni senza licenza. Tuttavia, se non si acquista una licenza di abbonamento Citrix Universal dopo la prova, le funzionalità cloud già distribuite non saranno disponibili.

Supporto del lancio locale dei pacchetti MSIX e MSIX App Attach

Con questa funzionalità, è ora possibile eseguire il lancio locale dei pacchetti MSIX e MSIX App Attach sul desktop VDA se è configurato vPrefer. Per ulteriori informazioni sul controllo degli avvii locali con vPrefer, vedere Controllare l'avvio locale delle applicazioni sui desktop pubblicati.

Virtual Delivery Agent (VDA) 2308

Sincronizzazione del volume audio

Il volume dell'audio è ora sincronizzato tra l'audio VDA e i dispositivi audio reindirizzati. È ora possibile regolare il volume usando il cursore del volume audio VDA e avere lo stesso volume sul proprio dispositivo.

Modalità tollerante alle perdite per l'audio (anteprima)

L'audio è ora supportato tramite il protocollo EDT (Enlightened Data Transport) Lossy. Questa funzionalità potenzia l'esperienza utente per lo streaming in tempo reale quando gli utenti si connettono tramite reti con elevata latenza e perdita di pacchetti. Quando questa funzione è abilitata, Adaptive Transport di Citrix Virtual Apps and Desktops utilizza il protocollo di trasporto EDT Lossy per una migliore esperienza audio. Questa funzionalità è disabilitata per impostazione predefinita nel 2308 e può essere abilitata tramite la configurazione del registro di sistema. Per ulteriori informazioni, vedere Supporto dell'audio tramite protocollo EDT Lossy.

EDT ha migliorato il controllo della congestione

L'algoritmo di controllo della congestione EDT è stato aggiornato per ottimizzare la risposta e le prestazioni in reti impegnative.

Web Studio

Citrix Secure Private Access integrato

Il servizio Citrix Secure Private Access può ora essere integrato nella console Web Studio e consente di accedere senza interruzioni al servizio tramite Web Studio. Per accedere al servizio, selezionare **Secure Private Access** nel riquadro sinistro della console Web Studio. L'interfaccia utente del servizio si apre in una nuova scheda del browser Web. Per ulteriori informazioni su Citrix Secure Private Access, vedere il documento relativo.

Per abilitare l'integrazione, effettuare le seguenti operazioni:

1. Aprire **C:\Programmi\Citrix\Web Studio\Site\studio\assets\json\spa-config.json** sul server Web Studio.
2. Individuare la stringa seguente.

```
"Name": "Spa"
"https://[spaserver]:4443/accessSecurity/ui"
<!--NeedCopy-->
```

3. Sostituire [spaserver] con l'indirizzo IP o il nome di dominio completo del server Secure Private Access.

Timeout di inattività configurabile di Studio

In qualità di amministratore con accesso completo, ora è possibile configurare il timeout di inattività per la console Studio. Questa impostazione determina per quanto tempo gli amministratori possono

rimanere inattivi prima di essere automaticamente scollegati dalla console di Studio. La durata dell'inattività deve essere impostata tra 10 minuti e 24 ore. Per ulteriori informazioni, vedere Impostare il timeout di inattività.

Autenticazione Windows integrata

È ora possibile abilitare l'autenticazione integrata di Windows per un accesso rapido e senza interruzioni a Web Studio. Questa funzionalità consente agli utenti di accedere a Web Studio con le proprie credenziali di Windows, utilizzando Kerberos o NTLM. Per ulteriori informazioni, vedere Gestire l'autenticazione.

Opzione di aggiornamento dell'immagine

Quando si selezionano le immagini master per i cataloghi di macchine, è ora possibile ottenere rapidamente l'elenco di immagini master più aggiornato utilizzando l'opzione **Refresh** (Aggiorna) in alto a destra. Tenere presente che l'opzione Refresh non è disponibile per i cataloghi AWS. È inoltre disponibile un'opzione Refresh per i profili di computer e i gruppi di host nei cataloghi di Azure.

Rimosso il supporto della modifica del tipo di sistema operativo per i cataloghi di Azure

Quando si modificano le immagini del catalogo, vengono visualizzate solo le immagini con lo stesso tipo di sistema operativo dell'immagine in uso. Con questo miglioramento, Citrix Virtual Apps and Desktops non supporta più la modifica del tipo di sistema operativo per i cataloghi di Azure dopo la creazione del catalogo.

Tenant condivisi per le connessioni

Ora è possibile aggiungere tenant e sottoscrizioni che condividono la Raccolta di calcolo di Azure con la sottoscrizione della connessione. Di conseguenza, quando si creano o si aggiornano i cataloghi, è possibile selezionare immagini condivise da questi tenant e sottoscrizioni. Per ulteriori informazioni, vedere Gestire le entità servizio e le connessioni.

Supporto dell'organizzazione di cataloghi di macchine, gruppi di consegna e gruppi di applicazioni utilizzando le cartelle

Ora è possibile creare cartelle per organizzare i catalohi di macchine, i gruppi di consegna e gruppi di applicazioni per facilità di accesso.

Citrix Director

Riepilogo dei probe e drill-down

Il probe delle applicazioni e dei desktop automatizza il processo di verifica dello stato delle app e dei desktop pubblicati in un sito mediante un test di avvio seriale che utilizza StoreFront. I risultati del probe sono disponibili in Director.

Ora, tutti i risultati relativi dei probe engono consolidati nella scheda **Trends > Probes** con le seguenti informazioni:

La scheda **Overview** (Panoramica) fornisce un riepilogo di tutte i probe configurati in un'unica visualizzazione. È possibile filtrare i probe in base al periodo di tempo, al tipo di probe, al nome dell'endpoint, al nome dell'applicazione, al nome del desktop e al tipo di risultato del probe. I probe che corrispondono ai criteri di filtro vengono visualizzati con i seguenti dettagli per probe, applicazione/desktop ed endpoint.

- **Completed Runs** (Esecuzioni completate): il numero di probe eseguiti e completati.
- **Failed Runs** (Esecuzioni non riuscite): il numero di probe eseguiti ma non riusciti.

La scheda **Probe Runs** (Probe eseguiti) fornisce i risultati dettagliati dei probe completati. È possibile filtrare i probe eseguiti in base al periodo di tempo, al tipo di probe, al nome dell'endpoint, al nome dell'applicazione, al nome del desktop e allo stadio di errore del probe. Facendo clic sui collegamenti **Probe Name** (Nome probe), **Failed Runs** (Esecuzioni con errori), **Application/Desktop name** (Nome applicazione/desktop) si accede anche alla pagina **Probe Runs** (Probe eseguiti) con l'elenco delle esecuzioni di probe che soddisfano i criteri di filtro.

Per ulteriori informazioni, vedere l'articolo Probe delle applicazioni e dei desktop.

Supporto Citrix Probe Agent per l'autenticazione a più fattori Citrix Gateway

Citrix Probe Agent per l'analisi di applicazioni e desktop ora supporta l'autenticazione a più fattori Citrix Gateway. Questa funzionalità è disponibile solo per Citrix Gateway configurato con LDAP e OTP nativo utilizzando lo schema di accesso singolo. I risultati completi del probe disponibili in Director aiutano a risolvere i problemi relativi alle applicazioni, alla macchina di hosting o alle connessioni prima che gli utenti li riscontrino. Per ulteriori informazioni, vedere l'articolo Probe delle applicazioni e dei desktop.

Disattivare gli avvisi dell'Hypervisor

È ora possibile disabilitare gli avvisi dell'Hypervisor da **Citrix Alerts Policy > Site Policy > Hypervisor Health** (Criterio per gli avvisi Citrix > Criteri del sito > stato dell'Hypervisor). Questo aiuta a ottimizzare

gli avvisi se il proprio ruolo non prevede il monitoraggio dell'infrastruttura. Per ulteriori informazioni, vedere Monitoraggio degli avvisi di Hypervisor.

Tendenze per le metriche relative all'esperienza di sessione

Director introduce una nuova scheda **User Details > Session Experience** (Dettagli utente > Esperienza di sessione) con flussi di lavoro di risoluzione dei problemi migliorati, a partire dalla capacità di mettere in correlazione le metriche in tempo reale per l'identificazione dei problemi all'interno delle sessioni utente. Session Experience ora contiene tendenze di metriche di sessione come ICARTT, Latenza ICA, fotogrammi al secondo, larghezza di banda in uscita disponibile e larghezza di banda in entrata consumata. Questa funzionalità aiuta a ridurre il tempo medio di risoluzione consentendo di mettere in correlazione più metriche delle prestazioni in un'unica visualizzazione. Per ulteriori informazioni, vedere l'articolo Problemi degli utenti.

Machine Creation Services (MCS)

Ambiente sicuro per il traffico gestito di GCP

Con questa funzione, ora è possibile consentire l'accesso privato di Google ai propri progetti Google Cloud. Questa implementazione migliora la sicurezza per la gestione dei dati sensibili. A tale scopo, è possibile effettuare una delle seguenti operazioni:

- Consentire la regola di ingresso per l'account del servizio Cloud Build nel perimetro del servizio VPC
- Se si utilizza un pool di lavoratori privato, aggiungere UsePrivateWorkerPool in CustomProperties.

Per ulteriori informazioni, vedere Creare un ambiente sicuro per il traffico gestito di GCP.

Supporto del profilo macchina in Citrix Hypervisor

In Citrix Hypervisor, è ora possibile creare un catalogo di macchine MCS utilizzando un profilo macchina. L'origine dell'input del profilo macchina è una macchina virtuale. Il profilo della macchina acquisisce le proprietà hardware da un modello di VM e le applica alle macchine virtuali di cui è appena stato effettuato il provisioning nel catalogo. Per ulteriori informazioni, vedere Creare un catalogo di macchine utilizzando un profilo macchina.

Possibilità di reimpostare il disco del sistema operativo di una macchina virtuale persistente in un catalogo di computer creato da MCS in SCVMM

È ora possibile utilizzare il comando `Reset-ProvVMDisk` di **PowerShell** per reimpostare il disco del sistema operativo di una macchina virtuale persistente in un catalogo di macchine creato da MCS. La funzione automatizza il processo di ripristino del disco del sistema operativo. Ad esempio, aiuta a ripristinare la VM allo stato iniziale di un catalogo desktop di sviluppo persistente creato con MCS. Attualmente, questa funzionalità è applicabile agli ambienti di virtualizzazione Azure, Citrix Hypervisor, SCVMM e VMware. Per ulteriori informazioni sull'utilizzo del comando **PowerShell** per reimpostare il disco del sistema operativo, vedere Reimpostare il disco del sistema operativo.

Limitare il caricamento e il download dei dischi gestiti

Negli ambienti Azure, è possibile usare gli endpoint privati per limitare l'accesso ai contenuti del disco. Questa implementazione consente di accedere in modo sicuro ai dati tramite un collegamento privato. Tuttavia, come da criteri di Azure, non è possibile caricare o scaricare più di cinque dischi o snapshot allo stesso tempo con lo stesso oggetto di accesso al disco. Per altre informazioni sull'uso di endpoint privati per limitare l'esportazione e l'importazione di dischi gestiti, vedere Limitare l'accesso di importazione/esportazione per i dischi gestiti usando collegamento privato di Azure.

Questa funzionalità consente di usare l'accesso al disco e gli endpoint privati per bloccare l'ambiente Azure, senza il rischio che si verifichino errori dovuti al superamento del limite. MCS esegue solo cinque operazioni simultanee al massimo. Tutte le operazioni in eccesso vengono messe in coda per essere eseguite quando è disponibile più larghezza di banda.

Supporto dell'assegnazione di una lettera di unità specifica al disco di cache write-back MCS I/O

In precedenza, il sistema operativo Windows assegnava automaticamente una lettera di unità al disco cache di write-back MCS I/O. Con questa funzionalità, ora è possibile assegnare una lettera di unità specifica al disco cache di write-back MCS I/O. Questa implementazione consente di evitare conflitti tra la lettera di unità di qualsiasi applicazione utilizzata e la lettera di unità del disco di cache write-back I/O MCS. Questa funzionalità è applicabile solo al sistema operativo Windows. Per ulteriori informazioni, vedere Assegnare una lettera di unità specifica al disco di cache write-back MCS I/O.

Conservare le impostazioni delle NIC sulle macchine virtuali di cui è stato effettuato il provisioning

In precedenza, le impostazioni NIC dell'immagine master non venivano mantenute nelle macchine virtuali di cui è stato effettuato il provisioning. Ad esempio, se sono state configurate le impostazioni

DNS sull'immagine master, le macchine virtuali predisposte non hanno mantenuto le impostazioni DNS configurate dell'immagine master. Grazie a questa funzionalità, le macchine virtuali predisposte possono ora mantenere le impostazioni delle NIC dell'immagine master. Le impostazioni vengono mantenute anche dopo un aggiornamento di Windows. Il driver del filtro viene installato automaticamente se si esegue una nuova installazione del VDA versione 2308 o successiva su una macchina distribuita con Hyper-V tramite le installazioni di immagini master MCS. Tuttavia, attualmente, se si esegue l'aggiornamento da una versione precedente del VDA (versione precedente alla 2308) e si desidera installare il driver del filtro, è necessario selezionare la casella di controllo `Citrix HyperV Filter Driver` nella pagina `Additional Components` durante l'aggiornamento del VDA. Per ulteriori informazioni, vedere Installare i componenti aggiuntivi. Questa funzionalità è applicabile a:

- VM Hyper-V (inclusi Azure e SCVMM)
- Cataloghi di macchine MCS persistenti e non persistenti
- Cataloghi di macchine MCS non persistenti con MCSIO
- Immagine master con più NIC

Supporto della condivisione di immagini tra diversi tenant di Azure

In precedenza, negli ambienti Azure, era possibile condividere immagini solo con sottoscrizioni condivise mediante Azure Compute Gallery. Con questa funzionalità, ora è possibile selezionare un'immagine in Raccolta di calcolo di Azure che appartiene a una sottoscrizione condivisa diversa in un tenant diverso per creare e aggiornare un catalogo MCS. Per ulteriori informazioni, vedere Condividere immagini tra tenant.

Aggiornare le proprietà delle singole macchine virtuali

È ora possibile aggiornare le proprietà delle singole macchine virtuali incluse in un catalogo di macchine MCS persistente utilizzando un comando PowerShell. Questa implementazione consente di gestire le singole macchine virtuali in modo efficiente senza aggiornare l'intero catalogo di macchine. Attualmente, questa funzionalità è applicabile solo all'ambiente Azure. Per ulteriori informazioni, vedere Aggiornare le proprietà delle singole macchine virtuali.

Supporto di vSAN 8.0

È ora possibile utilizzare MCS per effettuare il provisioning delle macchine virtuali nell'ambiente vSAN 8.0.

Profile Management

Per informazioni sulle nuove funzionalità, vedere l'articolo Novità nel relativo documento.

VDA Linux

Per informazioni sulle nuove funzionalità, vedere l'articolo Novità nel relativo documento.

Registrazione della sessione

Per informazioni sulle nuove funzionalità, vedere l'articolo Novità nel relativo documento.

Workspace Environment Management

Per informazioni sulle nuove funzionalità, vedere l'articolo Novità nel relativo documento.

Citrix Provisioning

Per informazioni sulle nuove funzionalità, vedere l'articolo Novità nel relativo documento.

Federated Authentication Service

Per informazioni sulle nuove funzionalità, vedere l'articolo Novità nel relativo documento.

Problemi risolti

January 7, 2024

Citrix Virtual Apps and Desktops 2308 include i seguenti problemi risolti:

Aspetti generali

- Dopo l'aggiornamento a Citrix Studio versione 2303 da una versione precedente, la disinstallazione potrebbe non funzionare come previsto. I componenti di Citrix Studio, come registri e file, rimangono nel sistema e potrebbero essere visibili nell'elenco Add Programs (Aggiungi programmi) o Remove Programs (Rimuovi programmi). [XAXDINST-1054]

- Se l'agente di registrazione della sessione non è installato sul VDA e si eseguono i comandi PowerShell `Get-BrokerSessionRecordingStatus`, `Start-BrokerSessionRecording` e `Stop-BrokerSessionRecording`, il VDA annulla la registrazione e si registra nuovamente con il Delivery Controller entro pochi secondi. Questa azione non ha alcun impatto sulle sessioni esistenti. Se l'agente di registrazione della sessione è installato sul VDA, i comandi PowerShell funzionano senza problemi. [BRK-14727]

Citrix Director

- In Citrix Director, alla voce relativa all'utilizzo della macchina nella **Director console > Trends > Machine Usage > Multi-session OS Machines** (console Director > Tendenze > Utilizzo della macchina > Macchine con sistema operativo multisessione) viene visualizzato 0 (Zero) nella colonna **In use** per tutti i gruppi di consegna. [CVADHELP-22498]
- Il collegamento Console in **Citrix Director > Machine Details** (Citrix Director > Dettagli macchina) non avvia la console della macchina nei browser Microsoft Edge 44 e Firefox 68 ESR. [DIR-8160]

Criteri Citrix

- I tentativi di applicare i criteri utente Citrix su domini diversi potrebbero non riuscire quando si aggiorna un VDA alla versione LTSR CU7. [CVADHELP-22992]

Delivery Controller

- Quando la memoria riservata è inferiore alla memoria configurata, i tentativi di accensione di una macchina virtuale potrebbero non riuscire riportando questo messaggio di errore:

  Invalid memory setting: Memory reservation (sched.mem.min) should be equal to memsize (94208). The virtual machine failed to start. Failed to turn on the MemSched module. Error parsing scheduler-specific configuration parameters. (Impostazione di memoria non valida: la prenotazione della memoria (sched.mem.min) deve essere uguale a memsize. Impossibile avviare la macchina virtuale. Impossibile attivare il modulo MemSched. Errore durante l'analisi dei parametri di configurazione specifici dello scheduler.)

  [CVADHELP-21052]

- Il supporto di vSAN 8 viene aggiunto ai Machine Creation Services. [CVADHELP-23415]

Grafica

- Nella sessione WebEx Citrix, quando si seleziona Microsoft **Media Foundation > Acquisizione video**, HDX Webcam genera un'immagine verde anziché il video reale proveniente dalla Web-Cam reindirizzata. [CVADHELP-22494]

Ottimizzazione di Microsoft Teams

- Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) potrebbe chiudersi in modo imprevisto durante l'utilizzo di Microsoft Teams. [CVADHELP-22561]

VDA per sistema operativo a sessione singola

Installazione, disinstallazione, aggiornamento

- Quando si aggiorna Citrix Virtual Apps and Desktops 2203 LTSR dal CU1 al CU2, potrebbero scomparire i valori di **EnableVistaMousePointers**, **EnforceUserPolicyEvaluationSuccess**, **Flag** e **CitrixDoD** che sono stati creati manualmente con le seguenti chiavi di registro:
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

    Nome: `EnableVistaMousePointers`

    Tipo: DWORD

    Valore: 1
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\GroupPolicy`

    Nome: `EnforceUserPolicyEvaluationSuccess`

    Tipo: DWORD

    Dati: 0
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\Smart Card Hook`

    Nome: `Flag`

    Tipo: DWORD

    Valore: 0
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits

    Nome: `CitrixDoD`

    Tipo: DWORD

Valore: 0

[CVADHELP-22569]

- Dopo aver aggiornato un VDA alla versione 1912 LTSR CUx o 2203 LTSR CUx, il valore `ApplicationLaunchWaitTimeoutMS` nella chiave di registro `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI` potrebbe non essere ripristinato. [CVADHELP-22758]

Tastiera

- EDT MTU Discovery potrebbe calcolare un MTU errato quando i percorsi tra il VDA e il client sono asimmetrici. Di conseguenza, l'avvio della sessione ha esito positivo. Tuttavia, la tastiera e il mouse non rispondono. [CVADHELP-16654]
- Quando si utilizza un layout di tastiera russo su un dispositivo macOS collegato a un VDA che esegue Windows, i tasti di scelta rapida potrebbero non funzionare. [CVADHELP-17788]
- Quando si passa da un layout di tastiera all'altro, ad esempio fra Regno Unito e Stati Uniti, la tastiera potrebbe presentare problemi di lingua intermittenti durante la sessione. [CVADHELP-23134]
- Con il protocollo Enlightened Data Transport (EDT) abilitato, le sessioni Citrix potrebbero bloccarsi quando si aggiorna il VDA dalla versione 1912 LTSR CU6 alla versione 1912 LTSR CU7. [CVADHELP-23370]

Stampa

- Quando si tenta di stampare un file PDF da una sessione avviata tramite l'app Citrix Workspace per HTML5, il file potrebbe non essere stampato correttamente. [CVADHELP-16809]
- Quando si riavvia un VDA con i criteri Universal Print Server abilitati, il bilanciamento del carico per Universal Print Server potrebbe non avviarsi. [CVADHELP-21498]

Sessione/connessione

- Le sessioni potrebbero rimanere bloccate in stato **Logging Off** (Scollegamento in corso) su Cloud Studio o Monitor fino all'avvio del sistema. Il problema si verifica quando i VDA Remote PC vengono chiusi dall'interno del Remote PC. [CVADHELP-20988]
- I siti Web interni di alcune applicazioni di terze parti con VDA installato potrebbero non consentire l'accesso senza una richiesta. [CVADHELP-22081]

- Con Shellbridge abilitato, tutti i programmi di avvio vengono avviati in una sessione applicativa pubblicata da HDX. La disconnessione da un'applicazione potrebbe impedire una disconnessione regolare. Se il problema persiste, imposta il valore su 0 nel seguente registro:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent`

  Nome: `Shellbridge`

  Tipo: REG_DWORD

  Valore: 0

  [CVADHELP-22199]

- Con il criterio **BrowserCodeIntegritySettingpolicy** abilitato nel browser Microsoft Edge, i tentativi di scaricare file in una directory CDM potrebbero non riuscire. [CVADHELP-22210]
- Le macchine in pool che sono accese potrebbero spegnersi automaticamente e non essere registrate. [CVADHELP-22374]
- In una riunione WebEx in esecuzione in una sessione Citrix con **Microsoft Media Foundation > Acquisizione video** selezionato, la webcam HDX potrebbe produrre un'immagine verde anziché il video reale della webcam reindirizzata. [CVADHELP-22494]
- Quando si copia un contenuto dalla sessione 1 utilizzando la mappatura degli appunti e si tenta di incollarlo nella sessione 2, il contenuto potrebbe non apparire negli appunti della sessione 2. Il problema si verifica quando la sessione 2 viene avviata dopo che il contenuto è stato copiato dalla sessione 1. [CVADHELP-22746]
- La mappatura dell'unità client (CDM) potrebbe non funzionare sulla versione 2203 LTSR CU2 del VDA appena installata che esegue Microsoft Windows Server quando Citrix Print Manager Service è disabilitato. [CVADHELP-22946]
- Quando i VDA Remote PC vengono spenti con la funzionalità Wake-On LAN abilitata anziché essere scollegati, le sessioni rimangono bloccate nello stato Logging Off e il VDA rimane registrato su Cloud Studio/Monitor. [CVADHELP-20988]
- Citrix Audio Redirection potrebbe non funzionare con la versione VDA 2203 LTSR CU3 quando più di otto dispositivi audio sono collegati a un dispositivo utente. [CVADHELP-23238]
- Se l'agente di registrazione della sessione non è installato sul VDA e si eseguono i comandi PowerShell `Get-BrokerSessionRecordingStatus`, `Start-BrokerSessionRecording` e `Stop-BrokerSessionRecording`, il VDA annulla la registrazione e si registra nuovamente con il Delivery Controller entro pochi secondi. Questa azione non ha alcun impatto sulle sessioni esistenti. Se l'agente di registrazione della sessione è installato sul VDA, i comandi PowerShell funzionano senza problemi. [CVADHELP-23491]

Smart card

- L'accesso alle smart card utilizzando il browser Microsoft Edge con SFRhook abilitato potrebbe causare la chiusura imprevista del processo msedge.exe. [CVADHELP-17956]

Eccezioni di sistema

- Il processo dell'indicatore di stato grafico `GfxStatusIndicator.exe` potrebbe arrestarsi ripetutamente. [CVADHELP-23141]
- Il servizio di reindirizzamento video HTML5 (CtxHdxWebSocketService) potrebbe interrompersi in modo imprevisto. [CVADHELP-22012]
- Il driver Citrix PDF Universal Printer potrebbe chiudersi in modo imprevisto a causa di errori nel modulo acfpdfuamd64.dll. [CVADHELP-22085]
- Il processo wfica32.exe potrebbe arrestarsi in modo imprevisto. [CVADHELP-22234]
- Il processo dell'indicatore di stato grafico, GfxStatusIndicator.exe, potrebbe arrestarsi ripetutamente. [CVADHELP-23142]

Esperienza utente

- Più tentativi di copiare il contenuto dall'applicazione Microsoft Access potrebbero non riuscire poiché il pulsante Incolla dell'applicazione viene disabilitato. [CVADHELP-21609]
- La copia del contenuto utilizzando l'opzione Copia su testo e immagine e la copia formattata potrebbero non riuscire. [CVADHELP-21905]
- Il processo wfshell.exe potrebbe non rispondere mentre si copiano e incollano dati di grandi dimensioni in Microsoft Excel. [CVADHELP-22425]

VDA per sistema operativo multisessione

Tastiera

- EDT MTU Discovery potrebbe calcolare un MTU errato quando i percorsi tra il VDA e il client sono asimmetrici. Di conseguenza, l'avvio della sessione ha esito positivo. Tuttavia, la tastiera e il mouse non rispondono. [CVADHELP-16654]
- Quando l'IME (Input Method Editor) del giapponese è impostato sulla modalità **Best Experience**, le stringhe di input potrebbero essere duplicate. [CVADHELP-18259]

Stampa

- Quando si tenta di stampare un file PDF da una sessione avviata tramite l'app Citrix Workspace per HTML5, il file potrebbe non essere stampato correttamente. [CVADHELP-16809]
- Quando si riavvia un VDA con i criteri Universal Print Server abilitati, il bilanciamento del carico per Universal Print Server potrebbe non avviarsi. [CVADHELP-21498]

Sessione/connessione

- Le sessioni potrebbero rimanere bloccate in stato **Logging Off** (Scollegamento in corso) su Cloud Studio o Monitor fino all'avvio del sistema. Il problema si verifica quando i VDA Remote PC vengono chiusi dall'interno del Remote PC. [CVADHELP-20988]
- I tentativi di aprire file PDF utilizzando Adobe Acrobat Reader DC in Citrix Servers potrebbero non riuscire con questo messaggio di errore:

```
exe - Application Error
The application was unable to start correctly (0xc0000142). Click
    Ok to close the application.
<!--NeedCopy-->
```

  [CVADHELP-21779]
- Session Recording potrebbe continuare a registrare anche dopo lo scollegamento della sessione o se la sessione viene disconnessa. [CVADHELP-22097]
- Con l'opzione `BrowserCodeIntegritySettingpolicy` abilitata nel browser Microsoft Edge, i tentativi di scaricare file in una directory CDM potrebbero non riuscire. [CVADHELP-22210]
- Le macchine in pool che sono accese potrebbero spegnersi automaticamente e non essere registrate. [[CVADHELP-22374]
- Quando si copia un contenuto dalla sessione 1 utilizzando la mappatura degli appunti e si tenta di incollarlo nella sessione 2, il contenuto potrebbe non apparire negli appunti della sessione 2. Il problema si verifica quando la sessione 2 viene avviata dopo che il contenuto è stato copiato dalla sessione 1. [CVADHELP-22746]
- Quando si passa da un endpoint all'altro senza disconnettere la sessione, potrebbero apparire più notifiche di riavvio se le notifiche di riavvio pianificato sono abilitate. [CVADHELP-22226]
- In una riunione WebEx in esecuzione in una sessione Citrix con **Microsoft Media Foundation > Acquisizione video** selezionato, la webcam HDX potrebbe produrre un'immagine verde anziché il video reale della webcam reindirizzata. [CVADHELP-22494]

- Dopo aver aggiornato un VDA dalla versione 1912 LTSR CU5 alla CU6 o alla CU7, i valori `LogoffCheckerStartupDelayInSeconds` e `SeamlessFlags`della chiave di registro `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI` potrebbero non essere ripristinati. [CVADHELP-22783]
- Quando ci si riconnette a una sessione dopo aver modificato il valore DPI del client, il nuovo valore potrebbe non essere applicato alla sessione. [CVADHELP-23007]
- I tentativi di riconnessione a una sessione utilizzando l'autenticazione con smart card potrebbero non riuscire e la sessione potrebbe rimanere bloccata sulla pagina **Welcome** (Benvenuti). Il problema si verifica con i VDA in esecuzione su Windows 10 o 11 versione 21H2, configurati con Remote Desktop Session Host (RDSH). [CVADHELP-23139]
- Quando la funzionalità Shellbridge è abilitata sul VDA, le sessioni di applicazioni senza interruzioni provenienti da HTML5 e Android potrebbero visualizzare finestre di interfaccia utente impreviste che possono bloccare l'input dell'utente. [CVADHELP-22984]
- Con il protocollo Enlightened Data Transport (EDT) abilitato, le sessioni Citrix potrebbero bloccarsi quando si aggiorna il VDA dalla versione 1912 LTSR CU6 alla versione 1912 LTSR CU7. [CVADHELP-23370]

Smart card

- L'accesso alle smart card utilizzando il browser Microsoft Edge con **SFRhook** abilitato potrebbe causare la chiusura imprevista del processo msedge.exe. [CVADHELP-17956]

Eccezioni di sistema

- Microsoft potrebbe inviare erroneamente il messaggio **WTS_REMOTE_CONNECT** prima di inviare la notifica di connessione **ConnectNotify**. Di conseguenza, potrebbero verificarsi uno o più dei seguenti problemi funzionali:

  - Le sessioni potrebbero terminare in modo imprevisto.
  - Le riconnessioni della sessione potrebbero non riuscire.
  - RPM Package Manager potrebbe bloccarsi.

  [CVADHELP-18980]
- Quando è selezionata l'opzione di riconnessione automatica del client, la sessione potrebbe chiudersi in modo imprevisto. [CVADHELP-19268]
- Il servizio di terminale potrebbe uscire in modo intermittente sul VDA per il sistema operativo multisessione. Viene registrato l'ID evento 7011 nel registro eventi di sistema con il seguente messaggio:

A timeout (30000 milliseconds) was reached while waiting for a transaction response from the TermService service. (È stato raggiunto un timeout (30000 millisecondi) in attesa di una risposta di transazione dal servizio TermService)

[CVADHELP-20259]

- Il processo Servizi terminal potrebbe terminare in modo imprevisto a causa del modulo RPM.dll guasto. [CVADHELP-21108]
- Il servizio di reindirizzamento video HTML5 (CtxHdxWebSocketService) potrebbe interrompersi in modo imprevisto. [CVADHELP-22012]
- Il driver Citrix PDF Universal Printer potrebbe chiudersi in modo imprevisto a causa di errori nel modulo acfpdfuamd64.dll. [CVADHELP-22085]
- Il processo wfica32.exe potrebbe arrestarsi in modo imprevisto. [CVADHELP-22234]
- Quando si aggiorna un VDA dalla versione 1912 LTSR CU5 alla CU6, si verifica un'eccezione irreversibile su Wdica.sys e viene visualizzata una schermata blu con il codice di controllo degli errori 0x000000CE. [CVADHELP-22365]

Esperienza utente

- Più tentativi di copiare il contenuto dall'applicazione Microsoft Access potrebbero non riuscire poiché il pulsante Incolla dell'applicazione viene disabilitato. [CVADHELP-21609]
- La copia del contenuto utilizzando l'opzione Copia su testo e immagine e la copia formattata potrebbero non riuscire. [CVADHELP-21905]
- Il processo wfshell.exe potrebbe non rispondere mentre si copiano e incollano dati di grandi dimensioni in Microsoft Excel. [CVADHELP-22425]

Interfaccia utente

- In una sessione utente avviata tramite l'app Citrix Workspace, potrebbe non essere possibile nascondere la barra della lingua anche dopo aver impostato l'opzione No, nascondi la barra della lingua. [CVADHELP-18239]
- Potrebbero non apparire messaggi di stato all'avvio delle risorse pubblicate. [CVADHELP-19070]

Componenti dei desktop virtuali

- I tentativi di aggiornamento dello schema del database potrebbero non riuscire durante l'aggiornamento di un Delivery Controller dalla versione LTSR 2203 CU1 alla versione 2206 o suc-

cessiva. [CVADHELP-22235]

Profile Management

- La documentazione di Profile Management 2308 fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

VDA Linux

- La documentazione di Linux VDA 2308 fornisce informazioni specifiche sugli aggiornamenti in questa versione.

Registrazione della sessione

- La documentazione di Session Recording 2308 fornisce informazioni specifiche sugli aggiornamenti in questa versione.

Workspace Environment Management

- La documentazionedi Workspace Environment Management 2308 fornisce informazioni specifiche sugli aggiornamenti di questa versione.

Citrix Provisioning

- La documentazione di Citrix Provisioning 2308 fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

Federated Authentication Service

- La documentazione del Federated Authentication Service 2308 fornisce informazioni specifiche sugli aggiornamenti di questa versione.

Problemi noti

April 3, 2024

Note

- Se un problema noto ha una soluzione alternativa, questa viene fornita dopo la descrizione del problema.
- Il seguente avviso si applica a qualsiasi soluzione alternativa che suggerisce di modificare una voce del Registro di sistema:

  > **Avviso:**
  >
  > La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Aspetti generali

- Se si effettua la migrazione da ambienti locali ad ambienti cloud utilizzando lo strumento di configurazione automatizzata (ACT), i dati elencati in **User Logoff Notifications** (Notifiche di disconnessione utente) nell'interfaccia **Manage Autoscale** (Gestione di Autoscale) diventano **Send logoff reminders without forcing user logoff** (Invia promemoria di scollegamento senza forzare lo scollegamento dell'utente) dopo il completamento della migrazione. Per risolvere il problema, scaricare la versione più recente di ACT da Configurazione automatizzata per Virtual Apps and Desktops.
- Negli ambienti Azure, quando si accede al VDA utilizzando la sessione ICA, potrebbe essere visualizzata una schermata nera per circa cinque minuti se si avvia un'app seamless per lo stesso desktop. [HDX-46159]
- Dopo le modifiche all'architettura di Citrix Virtual Apps and Desktops nella versione 2209, le icone predefinite per i desktop Windows e per le applicazioni distribuite prima di questa versione sono state sostituite da icone desktop PC generiche. Questa modifica è applicabile solo ai desktop e alle applicazioni che puntano all'icona predefinita. Se si desidera riportare le icone all'icona predefinita dell'applicazione Windows, eseguire il seguente script utilizzando l'SDK Remote PowerShell: `Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0`.
- Se si avvia la barra dell'app e si apre il menu Connection Center nell'app Citrix Workspace per Windows, la barra dell'app non viene visualizzata sotto il server che ospita l'app. [HDX-27504]
- Se si utilizza l'app Citrix Workspace per Windows e si avvia la barra dell'app in posizione verticale, la barra copre il menu Start o l'area in cui viene visualizzato l'orologio di sistema. [HDX-27505]

- La casella combinata potrebbe non essere visualizzata correttamente quando un utente seleziona una casella combinata che è già in stato attivo sull'host. Come soluzione alternativa, selezionare un altro elemento dell'interfaccia utente e quindi selezionare la casella combinata. [HDX-21671]
- Per Windows 11 versione 22H2, quando si sposta una finestra di Windows Media Player all' interno di una sessione, viene visualizzata solo la metà inferiore del video. Per ovviare al problema, selezionare: **Impostazioni > Sistema > Multitasking > Snap windows (Accosta finestre) > Show snap layouts when I drag a window to the top of my screen (Mostra layout istantanei quando trascino una finestra nella parte superiore dello schermo)**. [HDX-42092]
- Le impostazioni di **Session limits** (Limiti di sessione) per i VDA multisessione vengono rifiutate negli host di sessione che eseguono Windows Server 2022, Windows 10 Enterprise multisessione e Windows 11 Enterprise multisessione.
  Come soluzione alternativa, è possibile configurare **RDS Session Time Limits** (Limiti di tempo delle sessioni RDS) tramite GPO. [HDX-47001]
- Il criterio **Allow applications to use the physical location of the client device** (Consenti alle applicazioni di utilizzare la posizione fisica del dispositivo client) utilizzato per abilitare l'accesso alla posizione al client è interrotto. [HDX-47197]
- In alcuni scenari, quando si utilizza il filtro dei criteri IP del client, l'indirizzo IP utilizzato per valutare il criterio non è corretto. [HDX-62375]

Grafica

- Quando si condivide un'app ridotta a icona, è possibile che venga condivisa anche la barra del titolo dell'app. [HDX-33898]
- L'impostazione del criterio **View window contents while dragging** (Visualizza il contenuto della finestra durante il trascinamento) su **Prohibited** (Non consentito) non funziona su ESXi e Hyper-V. [HDX-22002]
- Se si avvia un'anteprima video utilizzando un'app webcam a 64 bit con compressione Theora, la sessione potrebbe bloccarsi. [HDX-21443]
- Per Windows 11 versione 22H2, quando si sposta una finestra di Windows Media Player all' interno di una sessione, viene visualizzata solo la metà inferiore del video. Per ovviare al problema, selezionare: **Impostazioni > Sistema > Multitasking > Snap windows (Accosta finestre) > Show snap layouts when I drag a window to the top of my screen (Mostra layout istantanei quando trascino una finestra nella parte superiore dello schermo)** [HDX-42092]

Stampa

- Le stampanti Universal Print Server selezionate sul desktop virtuale non vengono visualizzate nella finestra **Dispositivi e stampanti** del pannello di controllo. Tuttavia, quando gli utenti lavorano nelle applicazioni, possono utilizzare queste stampanti. Questo problema si verifica solo su Windows Server 2012, Windows 10 e Windows 8. Per ulteriori informazioni, vedere CTX213540. [HDX-5043, 335153]
- La stampante predefinita potrebbe non essere contrassegnata correttamente nella finestra di dialogo di stampa. Questo problema non influisce sui processi di stampa inviati alla stampante predefinita. [HDX-12755]

Machine Creation Services

- Il comando PowerShell `Remove-ProvVM` con il parametro `ForgetVM` potrebbe non funzionare correttamente se le versioni del Delivery Controller e di PowerShell remoto non sono compatibili. Ciò implica che le versioni del Delivery Controller e di PowerShell remoto devono essere entrambe precedenti alla 2212 o alla 2212 o successive. Ad esempio, se la versione del Delivery Controller è successiva alla 2212 e la versione di PowerShell remoto è precedente alla 2212, il comando `Remove-ProvVM` con il parametro `ForgetVM` non funziona come previsto. Come soluzione alternativa, scaricare la versione più recente di PowerShell per lavorare con la versione più recente del Delivery Controller. [PMCS-40278]
- In un ambiente VMware ospitato su AWS, la creazione del catalogo macchine MCS non riesce se l'immagine master è abilitata per vTPM. Questo problema riguarda tutte le versioni di Citrix Virtual Apps and Desktops. Per il supporto di VMware, vedere Ricevere assistenza. [PMCS-37603]

Problemi di terze parti

- Chrome supporta l'automazione dell'interfaccia utente solo per barre degli strumenti, schede, menu e pulsanti in una pagina Web. A causa di questo problema di Chrome, la funzionalità di visualizzazione automatica della tastiera potrebbe non funzionare in un browser Chrome sui dispositivi touch. Come soluzione alternativa, eseguire `chrome --force-renderer-accessibility` o aprire una nuova scheda del browser, digitare `chrome://accessibility` e abilitare il supporto dell'**API di accessibilità nativa** per pagine specifiche o per tutte. Inoltre, quando si pubblica un'app seamless, è possibile pubblicare Chrome come app seamless con lo switch `--force-renderer-accessibility`. [HDX-20858]
- Nel reindirizzamento del contenuto del browser, dopo aver avviato un video YouTube utilizzando il lettore video HTML5 di YouTube, la modalità a schermo intero potrebbe non funzionare. Se si fa clic sull'icona nell'angolo in basso a destra del video, il video non viene ridimensionato

e rimane lo sfondo nero nell'intera area della pagina. Come soluzione alternativa, fare clic sul pulsante della modalità a schermo intero, quindi selezionare la modalità teatro. [HDX-11294]

Profile Management

- La documentazione di Profile Management 2308 fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

VDA Linux

- La documentazione di Linux VDA 2308 fornisce informazioni specifiche sugli aggiornamenti in questa versione.

Registrazione della sessione

- La documentazione di Session Recording 2308 fornisce informazioni specifiche sugli aggiornamenti in questa versione.

Workspace Environment Management

- La documentazionedi Workspace Environment Management 2308 fornisce informazioni specifiche sugli aggiornamenti di questa versione.

Citrix Provisioning

- La documentazione di Citrix Provisioning 2308 fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

Federated Authentication Service

- La documentazione del Federated Authentication Service 2308 fornisce informazioni specifiche sugli aggiornamenti di questa versione.

Deprecazione

January 7, 2024

Gli annunci contenuti in questo articolo hanno lo scopo di fornire avvisi preventivi riguardo alle piattaforme, ai prodotti Citrix e alle funzionalità attualmente in corso di eliminazione, in modo da poter prendere decisioni aziendali tempestive. Citrix monitora l'utilizzo da parte dei clienti e il loro feedback per determinare quando procedere al ritiro. Gli annunci possono cambiare nelle versioni successive e potrebbero non includere tutte le funzionalità deprecate. Per informazioni dettagliate sul supporto del ciclo di vita del prodotto, vedere l'articolo Criteri di supporto del ciclo di vita del prodotto. Per informazioni sull'opzione di manutenzione LTSR (Long Term Service Release), vedere https://support.citrix.com/article/CTX205549.

Deprecazioni e rimozioni

La tabella seguente mostra le piattaforme, i prodotti Citrix e le funzionalità che sono deprecati o rimossi. Le date in **grassetto** indicano le modifiche a questa versione.

Deprecazioni

Gli elementi deprecati non vengono rimossi immediatamente. Citrix continua a supportarli, ma verranno rimossi in una versione futura.

Elemento	Deprecazione annunciata nella versione	Alternativa
Supporto di SQL Server 2016 in Broker	2308	Utilizzare le versioni più recenti. Per ulteriori informazioni, vedere Requisiti di sistema.
Supporto di XenApp 5.x in Director	2308	—
Supporto di XenApp 6.x in Director	2308	—
Pacchetto SCOM per avvisi in Director	2308	—
Supporto del plug-in in Director	2308	—
Supporto del formato WebRTC SDP (Piano B)	2308	Aggiornare l'app Citrix Workspace a una versione supportata.

Elemento	Deprecazione annunciata nella versione	Alternativa
Supporto della modalità finestra singola in Microsoft Teams Optimization	2308	Aggiornare l'app Citrix Workspace a una versione che supporti la modalità multifinestra. Per ulteriori informazioni, vedere Supporto delle funzionalità e versioni supportate.
Supporto di NVIDIA Frame Buffer Capture (NVFBC) con HDX 3D Pro	2308	—
Supporto dell'uso di `AwsCaptureInstanceProperties` in ambienti AWS	2308	—
Comando PowerShell `Schedule-ProvVMUpdate`	2305	Utilizzare `Set-ProvVMUpdateTimeWindow`.
Comando PowerShell `Request-ProvVMUpdate`	2305	Utilizzare `Set-ProvVMUpdateTimeWindow` con i parametri `-StartsNow` e `-DurationInMinutes -1`.
Comando PowerShell `Cancel-ProvVMUpdate`	2305	Utilizzare `Clear-ProvVMUpdateTimeWindow`.
Parametro `DedicatedTenancy` usato nel comando `New-ProvScheme`	2303	Utilizzare il parametro `TenancyType`.
License Server VPX	2206	—
Disco non gestito per il provisioning di macchine virtuali in ambienti Azure.	2206	Utilizzare dischi gestiti.
Reindirizzamento da host a client (URL)	2203	Reindirizzamento del contenuto bidirezionale.

Elemento	Deprecazione annunciata nella versione	Alternativa
Supporto di quattro comandi specifici di AWS: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress` e `Grant-HypSecurityGroupIngress` utilizzati in ambienti cloud e locali.	2203	—
Citrix Files per Windows e Citrix Files per Outlook dal metainstaller VDA.	2203	Usare i programmi di installazione autonomi.
Componente WEM Agent dal metainstaller VDA.	2203	—
Opzione Wake on LAN integrata in SCCM per l'accesso remoto a PC.	2012	Utilizzare la funzionalità Wake on LAN standalone.
Citrix SCOM Management Pack per XenApp e XenDesktop, Provisioning Services e StoreFront. Per le versioni del prodotto che è possibile monitorare, vedere la documentazione di Citrix SCOM Management Packs.	1912	Utilizzare Director per monitorare e gestire la distribuzione. Per ulteriori informazioni su SCOM EOL e sulle alternative, vedere https://support.citrix.com/article/CTX266943.
Supporto VDA per l'impostazione dei criteri "Automatic installation of in-box printer drivers" (Installazione automatica dei driver di stampa inclusi).	7.16	None (Nessuno). Impostazione dei criteri supportata solo con VDA su sistemi operativi precedenti (Windows 7, Windows Server 2012 R2 e versioni precedenti).

Elemento	Deprecazione annunciata nella versione	Alternativa
SDK per la mobilità/SDK per dispositivi mobili (degli ex Citrix Labs)	7.16	Sostituiti dalle impostazioni dei criteri di esperienza mobile e dalle esperienze native per desktop/app ospitati.

Rimozioni

Gli elementi rimossi vengono rimossi o non sono più supportati in Citrix Virtual Apps and Desktops.

Elemento	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Codifica hardware GPU NVIDIA (NVENC) con: vGPU 11 e versioni precedenti e versione del driver 466.77 e precedenti.	2305	2305	Utilizza i driver NVIDIA attualmente supportati: vGPU 13 o versione successiva, versione 471.41 o successiva.
Citrix Supportability Tools (Supportability-Tool_x64 .msi) del metainstaller VDA.	—	2212	—
Citrix License Administration Console (inclusa per l'ultima volta in Windows License Server 11.16.3 build 30000 e rimossa in Windows License Server v11.16.6 build 31000).	2003	2006	Utilizzare Citrix Licensing Manager.

Elemento	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Supporto della scheda grafica Citrix Indirect Display Driver (IDD) su Windows 10 versione 1709 e precedenti.	2003	2003	Utilizzare VDA Citrix Virtual Apps and Desktops 7 1912 LTSR.
Codifica hardware con GPU NVIDIA (NVENC) utilizzando driver video GRID 9 o precedenti.	2003	2003	Utilizzare i driver video GRID 10 con VDA Citrix Virtual Apps and Desktops 7 2003 o VDA successivi, oppure utilizzare VDA Citrix Virtual Apps and Desktops 7 1912 LTSR.
Funzionalità di reimpostazione della password self-service (SSPR, Self-Service Password Reset).	2003	2006	—
Supporto delle versioni di Microsoft .NET Framework precedenti alla versione 4.8 per VDA e dei componenti principali del server. Sono compresi Delivery Controller, Studio, Director e StoreFront.	1912	2003	Aggiornamento a .NET Framework versione 4.8.
VDA su Windows Server 2012 R2.	1912	2003	Installare i VDA su un sistema operativo supportato.

Elemento	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Componente di migrazione delle applicazioni AppDNA di Citrix Virtual Apps and Desktops Premium Edition.	1909	2003	—
Installazione di Studio su macchine a 32 bit (x86).	1909	2003	Eseguire l'installazione su un sistema operativo x64 supportato.
Supporto dell'hook Excel in applicazioni senza soluzione di continuità. Questo è stato utilizzato per creare icone separate della barra delle applicazioni per ogni cartella di lavoro di Microsoft Excel 2010.	1909	1909	—
Componenti principali del server in Windows Server 2012 R2 (inclusi i Service Pack). Sono compresi: Delivery Controller, Studio e Director.	1906	2003	Eseguire l'installazione su un sistema operativo supportato più recente.

Elemento	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Supporto dei database di configurazione del sito, di registrazione della configurazione e di monitoraggio su Microsoft SQL Server versioni 2008 R2, 2012 e 2014 (inclusi tutti i Service Pack e le versioni).	1906	2003	Installare i database su una versione supportata di Microsoft SQL Server.
Supporto dei VDA su Windows 10 in piattaforme x86.	1906	1909*	Installare i VDA su un sistema operativo x64 supportato. *Questa funzionalità è ancora supportata in Citrix Virtual Apps and Desktops 7 1912 LTSR.
Rimozione di Citrix Smart Tools Agent dai supporti di installazione di Citrix Virtual Apps and Desktops.	1903	1906	—
Rimozione delle opzioni di Delivery Controller per i seguenti prodotti all'interno di StoreFront che hanno raggiunto la fine del ciclo di vita: VDI-in-a-Box e XenMobile (versione 9.0 e precedenti).	1903	1903	—

Elemento	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Supporto di Linux VDA su Red Hat Enterprise Linux/CentOS 7.5.	1903	1903	Installare Linux VDA su una versione successiva di Red Hat Enterprise Linux.
Supporto StoreFront per TLS 1.0 e protocolli TLS 1.1 tra Citrix Virtual Apps and Desktops (precedentemente XenApp e XenDesktop) e Citrix Receiver e Workspace Hub.	7.17	2203	Aggiornare i Citrix Receiver a un'app Citrix Workspace che supporta il protocollo TLS 1.2. Per ulteriori informazioni sull'app Citrix Workspace, vedere https://docs.citrix.com/en-us/citrix-workspace-app.
Supporto StoreFront per gli utenti per accedere ai desktop nei siti Desktop Appliance	1811	1912	Utilizzare Desktop Lock (Blocco desktop) per casi d'uso non collegati al dominio.
Supporto della tecnologia di gestione remota dei display Framehawk	1811	1903	Utilizzare Thinwire con il trasporto adattivo abilitato.
Supporto di Citrix Smart Scale in tutte le versioni di Citrix Virtual Apps and Desktops (e XenApp e XenDesktop). Questa funzionalità raggiungerà il termine del ciclo di vita il 31 maggio 2019.	1808	1906	Prendere in considerazione l'utilizzo del servizio Virtual Apps and Desktops su Citrix Cloud per migliorare la funzionalità di gestione dell'alimentazione.

Elemento	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Supporto di Microsoft .NET Framework versioni 4.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 e 4.7 da parte di Citrix StoreFront, VDA Citrix, Citrix Studio, Citrix Director e Citrix Delivery Controller.	7.18	1808	Eseguire l'aggiornamento a .NET Framework versione 4.7.1 o successiva (il programma di installazione installa automaticamente .NET Framework 4.7.1 se non è già installato).
Supporto di Linux VDA su Red Hat Enterprise Linux 7.3.	7.18	1808	Installare Linux VDA su una versione successiva di Red Hat Enterprise Linux.
Supporto di Linux VDA su SUSE Linux Enterprise Server 11 Service Pack 4.	7.16	7.16	Installare Linux VDA sulla versione SUSE supportata.
Supporto del driver Citrix WDDM su VDA	7.16	7.16	Il driver Citrix WDDM non viene più installato con i VDA.
VDA su Windows 10 versione 1511 (Threshold 2) e versioni precedenti del sistema operativo Windows a sessione singola, inclusi Windows 8.x e Windows 7 (vedere https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/).	7.15 LTSR (e 7.12)	7.16	Installare VDA del sistema operativo a sessione singola su Windows 10 versione minima 1607 (Redstone 1) o sui canali semi-annuali più recenti. Se si utilizza 1607 LTSB, si consiglia un VDA 7.15. Vedere CTX224843.

Elemento	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
VDA su Windows Server 2008 R2 e Windows Server 2012 (inclusi i Service Pack)	7.15 LTSR (e 7.12)	7.16	Installare i VDA su un sistema operativo supportato.
Reindirizzamento della composizione desktop (precedentemente noto come DCR, DirectX Command Remoting)	7.15 LTSR	7.16	Utilizzare Thinwire.
Esperienza classica di Citrix Receiver per Web (interfaccia utente "con bolle verdi")	7.15 LTSR (e StoreFront 3.12)	1903	Esperienza unificata di Citrix Receiver per Web.
Componenti principali su Windows Server 2012 e Windows Server 2008 R2 (inclusi i Service Pack). Sono compresi: Delivery Controller, Studio, Director, StoreFront, License Server e Universal Print Server.	7.15 LTSR	7.18	Installare i componenti su un sistema operativo supportato.
Funzionalità di reimpostazione della password self-service (SSPR, Self-Service Password Reset) su Windows Server 2012 e Windows Server 2008 R2 (inclusi i Service Pack)	7.15 LTSR	7.18	Eseguire l'installazione su un sistema operativo supportato più recente.

Elemento	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Studio su Windows 7, Windows 8 e Windows 8.1 (inclusi i Service Pack)	7.15 LTSR	7.18	Installare Studio su un sistema operativo supportato.
Reindirizzamento flash	7.15 LTSR	1912	Creare contenuti video come video HTML5. Utilizzare il reindirizzamento video HTML5 per i contenuti gestiti e il reindirizzamento del contenuto del browser per i siti Web pubblici. Per ulteriori informazioni, vedere la nota Termine del ciclo di vita del reindirizzamento flash.
Integrazione Citrix Online (prodotto Goto) con StoreFront	7.14 (e StoreFront 3.11)	StoreFront 3.12	—
L'account utente CtxAppVCOMAdmin, creato durante l'installazione del VDA e aggiunto al gruppo di amministratori locali sulla macchina VDA, non viene più creato. Viene rimosso anche il meccanismo "COM" sottostante.	7.14	7.14	Il servizio Windows CtxAppVService svolge la stessa funzione. Viene installato e configurato automaticamente e non richiede alcuna interazione con l'utente.

Elemento	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Supporto del componente UpsServer di Universal Print Server su Windows Server 2008 a 32 bit	7.14	7.14	Eseguire l'installazione su un sistema operativo supportato più recente.
StoreFront e Receiver per Web su Internet Explorer 8	7.13	7.13	—
Opzione di installazione dalla riga di comando VDA /no_appv per impedire l'installazione dei componenti Citrix App-V	7.13	7.13	Utilizzare l'opzione di installazione dalla riga di comando /exclude "Citrix Personalization for App-V –VDA".
Il programma di installazione del prodotto completo non installa più lo snap-in Citrix.Common.Commands nelle nuove installazioni e lo rimuove automaticamente durante l'aggiornamento delle installazioni esistenti.	7.13	7.13	Alcuni comandi PowerShell forniti dallo snap-in Citrix.Common.Commands sono ancora disponibili nell'SDK XenApp 6.5.
Funzionalità parziale per manipolare i dati delle icone forniti dai cmdlet *-CtxIcon.	7.13	7.13	Ora fornita dai cmdlet *-BrokerIcon nel servizio Broker.

Elemento	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Modalità Thinwire legacy	7.12	7.16	Utilizzare Thinwire. Se si utilizza la modalità Thinwire legacy in Windows Server 2008 R2, eseguire la migrazione a Windows Server 2012 R2 o Windows Server 2016 e utilizzare Thinwire.
Aggiornamenti sul posto da StoreFront 2.0, 2.1, 2.5 e 2.5.2	7.13	7.16	Effettuare l'aggiornamento da una di queste versioni a una versione successiva supportata e quindi a XenApp e XenDesktop 7.16.
Aggiornamenti sul posto da XenDesktop 5.6 o 5.6 FP1	7.12	7.16	Eseguire la migrazione della distribuzione XenDesktop 5.6 o 5.6 FP1 alla versione corrente di XenDesktop. A questo scopo, eseguire prima l'aggiornamento a XenDesktop 7.6 LTSR (con l'ultimo aggiornamento cumulativo), quindi eseguire l'aggiornamento alla versione più recente di Citrix Virtual Desktops (precedentemente XenDesktop) o alla versione LTSR.

Elemento	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Installazione di Delivery Controller, Director, StoreFront o License Server su macchine a 32 bit (x86).	7.12	7.16	Eseguire l'installazione su un sistema operativo x64 supportato.
Leasing di connessione	7.12	7.16	Utilizzare la cache host locale.
XenDesktop 5.6 utilizzato su Windows XP. Le installazioni VDA su Windows XP non sono supportate.	7.12	7.16	Installare i VDA su un sistema operativo supportato.
Supporto delle connessioni CloudPlatform	7.12	2003	Utilizzare un hypervisor o un servizio cloud supportato diverso.
Supporto delle connessioni Azure Classic (noto anche come Gestione servizi di Azure)	7.12	2003	Prendere in considerazione l'utilizzo del servizio Virtual Apps and Desktops su Citrix Cloud.
Funzionalità AppDisks (e integrazione di AppDNA in Studio, che la supporta)	7.13	2003	Utilizzare Citrix App Layering.
Funzionalità Personal vDisk	7.15	2006†	Utilizzare la tecnologia livello utente Citrix App Layering o livello di personalizzazione utente.

† In Citrix Virtual Apps and Desktops 7 2003, il driver Personal vDisk è stato rimosso dal programma di installazione del VDA. In Citrix Virtual Apps and Desktops 7 2006, il flusso di lavoro del driver Personal vDisk è stato rimosso da Studio.

Requisiti di sistema

January 7, 2024

Introduzione

I requisiti di sistema contenuti in questo documento erano validi al momento del rilascio della versione del prodotto. Periodicamente vengono effettuati aggiornamenti. I requisiti di sistema per i componenti non descritti in questa sezione (ad esempio sistemi host, app Citrix Workspace e Citrix Provisioning) sono descritti nella rispettiva documentazione.

Vedere Prepararsi all'installazione prima di iniziare un'installazione.

A eccezione dei casi in cui è specificato, il programma di installazione dei componenti distribuisce automaticamente i prerequisiti software (ad esempio i pacchetti .NET e C++) se le versioni richieste non vengono rilevate sul computer. Il supporto di installazione Citrix contiene anche alcuni di questi prerequisiti software.

Il supporto di installazione contiene svariati componenti di terze parti. Prima di utilizzare il software Citrix, verificare la disponibilità di aggiornamenti di sicurezza forniti dalle corrispondenti terze parti e installarli.

Per informazioni sulla globalizzazione, vedere l'articolo CTX119253 del Knowledge Center.

Per i componenti e le funzionalità che possono essere installati sui server Windows, le installazioni di Nano Server non sono supportate, a meno che non sia specificato. Server Core è supportato solo per i Delivery Controller e Director.

Requisiti hardware

I valori di RAM e spazio su disco si aggiungono ai requisiti per l'immagine del prodotto, il sistema operativo e altri software presenti sul computer. Le prestazioni varieranno a seconda della configurazione. La configurazione include le funzionalità che sono in uso, più il numero di utenti e altri fattori. L'utilizzo solo del minimo può comportare prestazioni lente.

Nella tabella seguente sono elencati i requisiti minimi per i componenti principali.

Componente	Minimo
Tutti i componenti principali e StoreFront su un unico server, solo per una valutazione, non una distribuzione di produzione	5 GB RAM

Componente	Minimo
Tutti i componenti principali e StoreFront su un unico server, per una distribuzione di prova o un piccolo ambiente di produzione	12 GB di RAM
Delivery Controller (maggiore spazio su disco necessario per la cache host locale)	5 GB di RAM, disco rigido da 800 MB, database: vedere Guida al dimensionamento
Studio	1 GB di RAM, disco rigido da 100 MB
Director	2 GB di RAM, disco rigido da 200 MB
StoreFront	2 GB di RAM, vedere la documentazione di StoreFront per consigli sui dischi
License Server	2 GB di RAM, vedere la documentazione sulle licenze per consigli sui dischi

Dimensionamento delle macchine virtuali che forniscono desktop e applicazioni

Non è possibile fornire raccomandazioni specifiche a causa della natura complessa e dinamica delle offerte hardware e ogni implementazione presenta esigenze specifiche. In genere, il dimensionamento di una macchina virtuale Citrix Virtual Apps si basa sull'hardware e non sui carichi di lavoro degli utenti. L'eccezione è la RAM. È necessaria una quantità maggiore di RAM per le applicazioni che ne fanno maggior uso.

Per ulteriori informazioni:

- Citrix Tech Zone contiene linee guida sul dimensionamento.
- L'articolo Scalabilità di un singolo server di Citrix Virtual Apps and Desktops illustra quanti utenti o VM possono essere supportati su un singolo host fisico.

Microsoft Visual C++

Quando si installa un Delivery Controller, un Virtual Delivery Agent (VDA) o un Universal Print Server, il programma di installazione di Citrix installa automaticamente Microsoft Visual C++ 2015–2022 Redistributable.

- Se la macchina contiene una versione precedente di quel runtime (ad esempio 2015-2019), il programma di installazione di Citrix la aggiorna.
- Se la macchina contiene una versione precedente al 2015, Citrix installa la versione più recente in parallelo.

Delivery Controller

Sistemi operativi supportati:

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, edizioni Standard e Datacenter e con l'opzione Server Core
- Windows Server 2016, edizioni Standard e Datacenter e con l'opzione Server Core

Requisiti:

- Microsoft .NET Framework 4.8 viene installato automaticamente se non è già installato (o se ne è installata una versione successiva).
- Windows PowerShell 3.0, 4.0 o 5.0.
- Microsoft Visual C++ 2015–2019 Redistributable.

Database

Versioni di Microsoft SQL Server supportate per la configurazione del sito, la registrazione della configurazione e il monitoraggio dei database:

- SQL Server 2022 edizioni Express, Standard ed Enterprise.
- SQL Server 2019 edizioni Express, Standard ed Enterprise.
- SQL Server 2017 edizioni Express, Standard ed Enterprise.
  - Per le nuove installazioni: per impostazione predefinita, SQL Server Express 2017 con aggiornamento cumulativo 16 viene installato durante l'installazione del controller, se non viene rilevata un'esistente installazione di SQL Server supportata.
  - Per gli aggiornamenti, qualsiasi versione esistente di SQL Server Express non viene aggiornata.
- SQL Server 2016 SP2 edizioni Express, Standard ed Enterprise.

Sono supportate le seguenti soluzioni di database ad alta disponibilità (ad eccezione di SQL Server Express, che supporta solo la modalità standalone):

- Istanze del cluster di failover AlwaysOn di SQL Server
- Gruppi di disponibilità AlwaysOn di SQL Server (inclusi i gruppi di disponibilità di base)
- Mirroring del database di SQL Server

L'autenticazione di Windows è necessaria per le connessioni tra il Controller e il database del sito di SQL Server.

Considerazioni sulla cache host locale: Microsoft SQL Server Express LocalDB è una funzionalità di SQL Server Express utilizzata dalla cache host locale in modo autonomo. La cache host locale non richiede componenti di SQL Server Express diversi da SQL Server Express LocalDB.

- Quando si installa un Controller, viene installato Microsoft SQL Server Express LocalDB 2019 con aggiornamento cumulativo 15 per l'utilizzo con la funzionalità Cache host locale. Questa installazione è separata dall'installazione predefinita di SQL Server Express per il database del sito.
- Quando si aggiorna un Controller, la versione esistente di Microsoft SQL Server Express LocalDB non viene aggiornata automaticamente. Per i requisiti e le procedure di sostituzione, vedere Sostituire SQL Server Express LocalDB.

Ulteriori informazioni sui database:

- Database
- CTX114501 elenca i database supportati più recenti
- Guida al dimensionamento del database
- Cache host locale

Web Studio

> **Nota:**
>
> - È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.
> - Web Studio è una console di gestione basata sul Web che consente di configurare e gestire l'implementazione locale di Citrix Virtual Apps and Desktops. È progettata per una migliore esperienza utente e generalmente risponde più velocemente di Citrix Studio, la console di gestione basata su Windows. Vedere Installare Web Studio.

Sistemi operativi supportati:

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, edizioni Standard e Datacenter e con l'opzione Server Core
- Windows Server 2016, edizioni Standard e Datacenter e con l'opzione Server Core

Citrix Director

Sistemi operativi supportati:

- Windows Server Core 2022

- Windows Server 2022
- Windows Server 2019, edizioni Standard e Datacenter e con l'opzione Server Core
- Windows Server 2016, edizioni Standard e Datacenter e con l'opzione Server Core

Requisiti:

- Microsoft .NET Framework 4.8 viene installato automaticamente se non è già installato (o se ne è installata una versione successiva).
- Microsoft Internet Information Services (IIS) 7.0 e ASP.NET 2.0. Verificare che nel ruolo del server IIS sia installato il servizio ruolo Contenuto statico. Se il software non è già installato, viene richiesto il supporto di installazione di Windows Server. Quindi, quel software viene installato.
- Per visualizzare i registri eventi sui computer in cui è installato Citrix Director, è necessario installare Microsoft.NET Framework 2.0.

Citrix Profile Management:

- Verificare che i plug-in WMI Citrix Profile Management e Citrix Profile Management siano installati nel VDA (pagina **Componenti aggiuntivi** della procedura guidata di installazione) e che Citrix Profile Management Service sia in esecuzione per visualizzare i dettagli del profilo utente in Director.

Requisiti di integrazione di System Center Operations Manager (SCOM):

- System Center 2012 R2 Operations Manager

Browser supportati per visualizzare Director:

- Internet Explorer 11. La modalità di compatibilità non è supportata per Internet Explorer. Utilizzare le impostazioni del browser consigliate per accedere a Director. Quando si installa Internet Explorer, accettare l'impostazione predefinita per utilizzare le impostazioni di protezione e compatibilità consigliate. Se si è già installato il browser e si è scelto di non utilizzare le impostazioni consigliate, andare a **Strumenti > Opzioni Internet > Avanzate > Reimposta** e seguire le istruzioni.
- Microsoft Edge.
- Firefox ESR (Extended Support Release).
- Chrome.

La risoluzione ottimale dello schermo consigliata per la visualizzazione Director è 1366 x 1024.

Virtual Delivery Agent (VDA) per sistema operativo a sessione singola

Sistemi operativi supportati:

- Windows 11
- Windows 10 (solo x64), qualsiasi versione attualmente supportata dal supporto Mainstream.
  - Per informazioni sul supporto delle versioni, vedere l'articolo CTX224843 del Knowledge Center.
  - Per i problemi noti a Citrix della versione 1709, vedere l'articolo CTX229052 del Knowledge Center.

Requisiti:

- Microsoft .NET Framework 4.8 viene installato automaticamente se non è già installato (o se ne è installata una versione successiva).
- Microsoft Visual C++ 2015–2019 Redistributable.

Accesso remoto PC utilizza questo VDA, che viene installato sui PC fisici dell'ufficio. Questo VDA supporta Secure Boot per Accesso remoto PC di Citrix Virtual Desktops su Windows 11 e Windows 10.

Diverse funzionalità di accelerazione multimediale (ad esempio HDX MediaStream Windows Media Redirection) richiedono l'installazione di Microsoft Media Foundation nel computer in cui si installa il VDA. Se nel computer non è installato Media Foundation, le funzionalità di accelerazione multimediale non vengono installate e non funzionano. Non rimuovere Media Foundation dal computer dopo l'installazione del software Citrix. In caso contrario, gli utenti non possono accedere al computer. Nella maggior parte delle edizioni del sistema operativo Windows a sessione singola supportate, il supporto di Media Foundation è già installato e non può essere rimosso. Tuttavia, le edizioni N non includono determinate tecnologie relative ai supporti multimediali; è possibile ottenere tale software da Microsoft o da terze parti. Per ulteriori informazioni, vedere Prepararsi all'installazione.

Per informazioni sui VDA Linux, vedere gli articoli su Linux Virtual Delivery Agent.

Per utilizzare la funzionalità Server VDI, è possibile utilizzare l'interfaccia della riga di comando per installare un VDA per sistema operativo Windows a sessione singola in un computer Windows Server supportato. Per ulteriori informazioni, vedere VDI del server.

Per informazioni sull'installazione di un VDA su una macchina Windows 7, vedere Sistemi operativi precedenti.

Virtual Delivery Agent (VDA) per sistema operativo multisessione

Sistemi operativi supportati:

- Windows 11 (supportato solo con Citrix DaaS)
- Windows 10 (solo x64; supportato solo con Citrix DaaS), qualsiasi versione attualmente supportata dal supporto Mainstream.
- Windows Server 2022

- Windows Server 2019 edizioni Standard e Datacenter
- Windows Server 2016 edizioni Standard e Datacenter

Il programma di installazione implementa automaticamente i seguenti requisiti, che sono disponibili anche sul supporto di installazione Citrix nelle cartelle **Support** :

- Microsoft .NET Framework 4.8 viene installato automaticamente se non è già installato (o se ne è installata una versione successiva).
- Microsoft Visual C++ 2015–2019 Redistributable.

Il programma di installazione installa automaticamente e abilita i servizi ruolo Servizi Desktop remoto, se non sono già installati e abilitati.

Diverse funzionalità di accelerazione multimediale (ad esempio HDX MediaStream Windows Media Redirection) richiedono l'installazione di Microsoft Media Foundation nel computer in cui si installa il VDA. Se nel computer non è installato Media Foundation, le funzionalità di accelerazione multimediale non vengono installate e non funzionano. Non rimuovere Media Foundation dal computer dopo aver installato il software Citrix, altrimenti gli utenti non saranno in grado di accedere al computer. Nella maggior parte delle versioni di Windows Server, la funzionalità Media Foundation viene installata tramite Server Manager. Per ulteriori informazioni, vedere Prepararsi all'installazione.

Se Media Foundation non è presente sul VDA, queste funzionalità multimediali non funzionano:

- Reindirizzamento di Windows Media
- Reindirizzamento video HTML5
- Reindirizzamento webcam HDX RealTime

Per informazioni sui VDA Linux, vedere gli articoli su Linux Virtual Delivery Agent.

Per informazioni sull'installazione di un VDA su una macchina Windows Server 2008 R2, vedere Sistemi operativi precedenti.

Host/risorse di virtualizzazione

Sono supportati gli host/le risorse di virtualizzazione seguenti (in ordine alfabetico). Ove applicabile, sono supportate le versioni *major.minor*, inclusi gli aggiornamenti di tali versioni. L'articolo CTX131239 del Knowledge Center contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

Alcune funzionalità potrebbero non essere supportate su tutte le piattaforme host o su tutte le versioni della piattaforma. Per ulteriori informazioni, vedere la documentazione della relativa funzionalità.

La funzionalità Riattivazione accesso remoto PC su LAN richiede Microsoft System Center Configuration Manager almeno 2012.

Hypervisor supportati:

- **Citrix Hypervisor (in precedenza XenServer)**

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Citrix Hypervisor.

- **Microsoft System Center Virtual Machine Manager**

  Include qualsiasi versione di Hyper-V registrabile con le versioni supportate di System Center Virtual Machine Manager.

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager.

- **Nutanix Acropolis**

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Ambienti di virtualizzazione Nutanix.

- **VMware vSphere (vCenter + ESXi)**

  Non viene fornito alcun supporto del funzionamento della modalità collegata vSphere vCenter.

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Ambienti di virtualizzazione VMware.

Host cloud pubblici supportati:

- **Amazon Web Services (AWS)**

  Per informazioni sull'utilizzo di AWS per il provisioning di macchine virtuali, vedere la sezione Ambienti di virtualizzazione Amazon Web Services.

- **Google Cloud Platform**
  Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Google Cloud Platform e Getting Started with Citrix DaaS on Google Cloud.

- **Microsoft Azure Resource Manager**

  Per informazioni sull'utilizzo di Microsoft Azure Resource Manager per il provisioning di macchine virtuali, vedere Ambienti di virtualizzazione Microsoft Azure Resource Manager.

- **Soluzioni Nutanix Cloud e dei partner**

  Per informazioni sull'utilizzo delle soluzioni Nutanix Cloud e dei partner, vedere Soluzioni Nutanix Cloud e dei partner.

- **Soluzioni VMware Cloud e dei partner**

  Per informazioni sull'utilizzo delle soluzioni VMware Cloud e dei partner, vedere Soluzioni VMware Cloud e dei partner.

Quando si aggiungono connessioni a host cloud pubblici alla propria distribuzione, tenere presente quanto segue:

- È necessaria la licenza Hybrid Rights. Per informazioni sulla licenza Hybrid Rights, vedere Transition and Trade-Up (TTU) with Hybrid Rights. Per informazioni sull'aggiunta di una licenza, vedere Creare un sito.
- Le fonti di informazioni indirizzano alla documentazione di Citrix DaaS. Se si ha familiarità con gli host cloud pubblici del prodotto Citrix DaaS, la versione locale presenta diverse differenze.
  - In Citrix DaaS, l'interfaccia di gestione è nota come Full Configuration (configurazione completa). Nella versione locale di Citrix Virtual Apps and Desktops, l'interfaccia di gestione è nota come Web Studio.
  - Gli aggiornamenti vengono implementati in Citrix DaaS circa ogni quattro settimane. Pertanto, è possibile che alcune funzionalità disponibili con Citrix DaaS non siano disponibili con la versione locale.

Livelli funzionali di Active Directory

Sono supportati i seguenti livelli di funzionalità per la foresta e il dominio di Active Directory:

- Windows Server 2016
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

HDX

Audio

L'audio UDP per Multi-Stream ICA è supportato dall'app Citrix Workspace per Windows e dall'app Citrix Workspace per Linux 13.

L'annullamento dell'eco è supportato nell'app Citrix Workspace per Windows.

Vedere il supporto e i requisiti specifici delle funzionalità HDX. Per ulteriori informazioni sulle funzionalità HDX e sulle app Citrix Workspace, vedere la Matrice delle funzionalità.

Distribuzione HDX Windows Media

I seguenti client sono supportati per il recupero dei contenuti sul lato client Windows Media, il reindirizzamento di Windows Media e la transcodificazione multimediale Windows Media in tempo reale: app Citrix Workspace per Windows, app Citrix Workspace per iOS e app Citrix Workspace per Linux.

Per utilizzare il recupero del contenuto sul lato client di Windows Media sui dispositivi Windows 8, impostare Citrix Multimedia Redirector come programma predefinito: in **Pannello di controllo > Programmi > Programmi predefiniti > Impostare i programmi predefiniti**, selezionare **Citrix Multimedia Redirector** e fare clic su **Imposta questo programma come predefinito** o **Scegli i valori predefiniti per questo programma**. La transcodificazione della GPU richiede una GPU NVIDIA abilitata CUDA con capacità di calcolo 1.1 o superiore; vedere https://developer.nvidia.com/cuda/cuda-gpus.

HDX 3D Pro

Il VDA per sistema operativo Windows a sessione singola rileva la presenza di hardware GPU in fase di esecuzione.

La macchina fisica o virtuale che ospita l'applicazione può utilizzare GPU Passthrough o Virtual GPU (vGPU):

- GPU Passthrough è disponibile con:
  - Citrix Hypervisor
  - Nutanix AHV
  - VMware vSphere e VMware ESX, in cui è denominato vDGA (Virtual Direct Graphics Acceleration)
  - Microsoft Hyper-V in Windows Server 2016 in cui è denominato DDA (Discrete Device Assignment).
- vGPU è disponibile con:
  - Citrix Hypervisor
  - Nutanix AHV
  - VMware vSphere

Vedere https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.html.

Citrix consiglia che il computer host abbia almeno 4 GB di RAM e quattro CPU virtuali con una velocità di clock di 2,3 GHz o superiore.

Unità di elaborazione grafica (GPU):

- Per la compressione basata su CPU (inclusa la compressione senza perdite), HDX 3D Pro supporta qualsiasi scheda display sul computer host compatibile con l'applicazione fornita.
- Per l'accelerazione grafica virtualizzata utilizzando l'API NVIDIA GRID, è possibile utilizzare HDX 3D Pro con tutte le GPU NVIDIA GRID supportate dal driver GRID 10 (vedere NVIDIA GRID). NVIDIA GRID offre una frequenza di aggiornamento elevata, con conseguente esperienza utente altamente interattiva.

- L'accelerazione grafica virtualizzata è supportata dalla piattaforma grafica per centri dati della famiglia di processori Intel Xeon E3. Per ulteriori informazioni, vedere https://www.citrix.com/intel e https://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- L'accelerazione grafica virtualizzata è supportata con AMD RapidFire sulle schede server AMD FirePro serie S Vedere Soluzione di virtualizzazione AMD.

Dispositivo utente:

- HDX 3D Pro supporta tutte le risoluzioni del monitor supportate dalla GPU sul computer host. Per ottenere prestazioni ottimali con le specifiche minime consigliate per il dispositivo utente e la GPU, Citrix consiglia una risoluzione massima del monitor di 1920 x 1200 pixel per le connessioni LAN e 1280 x 1024 pixel per le connessioni WAN.
- Per i dispositivi utente, Citrix consiglia almeno 1 GB di RAM e una CPU con una velocità di clock di 1,6 GHz o superiore. L'utilizzo del codec di compressione profonda predefinito, richiesto per connessioni a bassa larghezza di banda, richiede una CPU più potente a meno che la decodifica non venga eseguita nell'hardware. Per prestazioni ottimali dei dispositivi utente , Citrix consiglia almeno 2 GB di RAM e una CPU dual-core con una velocità di clock di 3 GHz o superiore.
- Per l'accesso a più monitor, Citrix consiglia dispositivi utente con CPU quad-core.
- I dispositivi utente non necessitano di una GPU per accedere ai desktop o alle applicazioni fornite con HDX 3D Pro.
- L'app Citrix Workspace deve essere installata.

Per ulteriori informazioni, vedere gli articoli su HDX 3D Pro e www.citrix.com/xenapp/3d.

Universal Print Server

Universal Print Server comprende componenti client e server. Il componente UpsClient è incluso nell'installazione VDA. Installare il componente UpsServer su ogni server di stampa in cui risiedono stampanti condivise di cui si desidera eseguire il provisioning con Citrix Universal Print Driver nelle sessioni utente.

Il componente UpsServer è supportato in:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Requisiti:

- Microsoft Visual C++ 2015–2019 Redistributable
- Microsoft .NET Framework 4.8 (minimo)

Per i VDA per sistema operativo multisessione, l'autenticazione utente durante le operazioni di stampa richiede che Universal Print Server venga aggiunto allo stesso dominio del VDA.

I pacchetti di componenti client e server autonomi sono disponibili anche per il download.

Per ulteriori informazioni, vedere Eseguire il provisioning delle stampanti.

Altro

Sono supportati solo Citrix License Server 11.17.2 e versioni successive. Per ulteriori informazioni, vedere Licenze.

Quando si utilizza Citrix Provisioning (già Provisioning Services) con questa release, la versione 7.x è coperta dal ciclo di vita di XenApp e XenDesktop 7.x e dal ciclo di vita di Citrix Virtual Apps and Desktops. Per ulteriori informazioni sulla compatibilità delle versioni, vedere la matrice dei prodotti.

Per le versioni StoreFront supportate, vedere i requisiti di sistema di StoreFront.

La Console Gestione Criteri di gruppo Microsoft (GPMC) è necessaria se si memorizzano le informazioni sui criteri Citrix in Active Directory anziché nel database di configurazione del sito. Se si installa `CitrixGroupPolicyManagement_x64.msi` separatamente (ad esempio, su una macchina in cui non è installato un componente principale di Citrix Virtual Apps and Desktops), tale macchina deve avere installato Visual Studio 2015 runtime. Per ulteriori informazioni, vedere la documentazione Microsoft.

Se si desidera modificare gli oggetti Criteri di gruppo di dominio utilizzando GPMC, attivare la funzionalità Gestione Criteri di gruppo (in Windows Server Manager) in tutti i computer contenenti Delivery Controller.

Sono supportate più NIC.

Per impostazione predefinita, l'app Citrix Workspace per Windows non viene installata quando si installa un VDA corrente. Per ulteriori informazioni, vedere la documentazione dell'app Citrix Workspace per Windows.

Per informazioni sul browser supportato per tale funzionalità, vedere Accesso alle app locali.

Questa versione di Citrix Virtual Apps and Desktops richiede almeno HDX RealTime Connector 2.9 LTSR. Per ulteriori informazioni, vedere la documentazione di HDX RealTime Optimization Pack.

Questo prodotto supporta le versioni di PowerShell dalla 3 alla 5.

Panoramica tecnica

January 7, 2024

Citrix Virtual Apps and Desktops è un insieme di soluzioni di virtualizzazione che offrono all'IT il controllo di macchine virtuali, applicazioni, licenze e sicurezza, fornendo al tempo stesso l'accesso ovunque per qualsiasi dispositivo.

Citrix Virtual Apps and Desktops consente:

- Agli utenti finali di eseguire applicazioni e desktop indipendentemente dal sistema operativo e dall'interfaccia del dispositivo.
- Agli amministratori di gestire la rete e controllare l'accesso da dispositivi selezionati o da tutti i dispositivi.
- Agli amministratori di gestire un'intera rete da un unico centro dati.

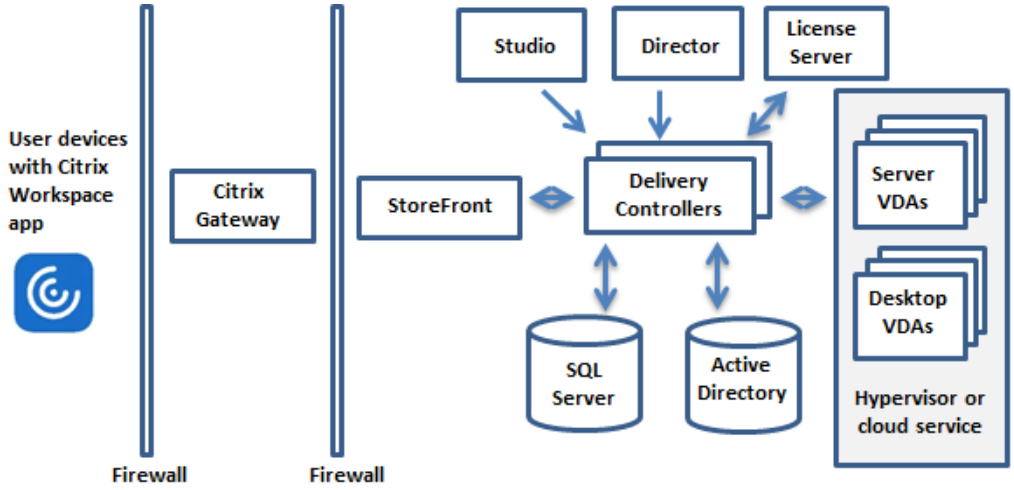
Citrix Virtual Apps and Desktops condivide un'architettura unificata denominata FlexCast Management Architecture (FMA). Le caratteristiche principali di FMA sono la possibilità di eseguire più versioni di Citrix Virtual Apps o Citrix Virtual Desktops da un unico sito e il provisioning integrato.

Ulteriori informazioni sulle modifiche dei nomi dei prodotti.

Componenti chiave

Questo articolo è molto utile se si utilizza Citrix Virtual Apps and Desktops da poco. Se al momento si dispone di una farm XenApp 6.x o precedente o di un sito XenDesktop 5.6 o precedente, vedere anche Modifiche di 7.x.

In questa illustrazione sono visualizzati i componenti chiave di una distribuzione tipica, denominata sito.



Delivery Controller

Il Delivery Controller è la componente centrale di gestione di un sito. Ogni sito ha uno o più Delivery Controller. Viene installato su almeno un server del centro dati. Per garantire l'affidabilità e la

disponibilità del sito, installare i Controller su più server. Se la distribuzione include un hypervisor o un altro servizio, i servizi Controller comunicano con esso per:

- Distribuire applicazioni e desktop
- Autenticare e gestire l'accesso degli utenti
- Gestire le connessioni tra gli utenti e i loro desktop e applicazioni
- Ottimizzare le connessioni utente
- Bilanciare il carico delle connessioni

Il servizio Broker del controller tiene traccia di quali utenti sono connessi e dove, di quali risorse di sessione dispongono gli utenti e se gli utenti hanno bisogno di riconnettersi alle applicazioni esistenti. Il servizio Broker esegue i cmdlet di PowerShell e comunica con un agente broker sui VDA tramite la porta TCP 80. Non ha la possibilità di utilizzare la porta TCP 443.

Il servizio di monitoraggio raccoglie i dati storici e li inserisce nel database di monitoraggio. Questo servizio utilizza la porta TCP 80 o 443.

I dati provenienti dai servizi del Controller sono memorizzati nel database del sito.

Il Controller gestisce lo stato dei desktop, avviandoli e arrestandoli in base alla richiesta e alla configurazione amministrativa.

Database

È necessario almeno un database di Microsoft SQL Server per ogni sito per archiviare le informazioni di configurazione e sessione. Questo database memorizza i dati raccolti e gestiti dai servizi che compongono il Controller. Installare il database all'interno del centro dati e assicurarsi che disponga di una connessione permanente al Controller.

Il sito utilizza anche un database di registrazione della configurazione e un database di monitoraggio. Per impostazione predefinita, tali database vengono installati nella stessa posizione del database del sito, ma questa impostazione può essere modificata.

Virtual Delivery Agent (VDA)

Il VDA viene installato in ogni macchina fisica o virtuale del sito che viene messa a disposizione degli utenti. Queste macchine forniscono applicazioni o desktop. Il VDA consente alla macchina di registrarsi con il Controller, che a sua volta consente di mettere a disposizione degli utenti la macchina e le risorse che ospita. I VDA stabiliscono e gestiscono la connessione tra la macchina e il dispositivo utente. I VDA verificano inoltre che sia disponibile una licenza Citrix per l'utente o la sessione e applicano i criteri configurati per la sessione.

Il VDA comunica le informazioni di sessione al servizio Broker nel Controller tramite l'agente broker nel VDA. L'agente broker ospita più plug-in e raccoglie dati in tempo reale. Esso comunica con il Controller tramite la porta TCP 80.

La parola "VDA"viene spesso utilizzata per fare riferimento all'agente e alla macchina su cui è installato.

I VDA sono disponibili per i sistemi operativi Windows a sessione singola e multisessione. I VDA per sistemi operativi Windows multisessione consentono a più utenti di connettersi al server contemporaneamente. I VDA per i sistemi operativi Windows a sessione singola consentono a un solo utente di connettersi al desktop alla volta. Sono disponibili anche VDA Linux.

Citrix StoreFront

StoreFront autentica gli utenti e gestisce gli archivi dei desktop e delle applicazioni a cui gli utenti accedono. Può ospitare lo store delle applicazioni aziendali, che offre agli utenti l'accesso self-service ai desktop e alle applicazioni che vengono messi a loro disposizione. Inoltre tiene traccia delle sottoscrizioni delle applicazioni, dei nomi di collegamenti e di altri dati degli utenti. Ciò consente di garantire che gli utenti dispongano di un'esperienza coerente su più dispositivi.

App Citrix Workspace

Installata sui dispositivi utente e su altri endpoint (ad esempio desktop virtuali), l'app Citrix Workspace offre agli utenti un accesso rapido, sicuro e self-service a documenti, applicazioni e desktop. L'app Citrix Workspace consente l'accesso on-demand alle applicazioni Windows, Web e SaaS (Software as a Service). Per i dispositivi che non possono installare il software dell'app Citrix Workspace specifico del dispositivo, l'app Citrix Workspace per HTML5 fornisce una connessione tramite un browser Web compatibile con HTML5.

Studio

È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questa documentazione del prodotto riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Web Studio Web Studio è una console di gestione basata sul Web che consente di configurare e gestire l'implementazione locale di Citrix Virtual Apps and Desktops. È progettata per una migliore esperienza utente e generalmente risponde più velocemente di Citrix Studio, la console di gestione basata su Windows. Vedere Installare Web Studio.

Citrix Studio Citrix Studio è la console di gestione in cui è possibile configurare e gestire la distribuzione di Citrix Virtual Apps and Desktops. Citrix Studio elimina la necessità di console di gestione separate per gestire la distribuzione di applicazioni e desktop. Citrix Studio fornisce procedure guidate che guidano l'utente attraverso la configurazione dell'ambiente, la creazione di carichi di lavoro per ospitare applicazioni e desktop e l'assegnazione di applicazioni e desktop agli utenti. È inoltre possibile utilizzare Studio per allocare e tenere traccia delle licenze Citrix per il proprio sito.

Citrix Studio ottiene le informazioni visualizzate dal servizio Broker nel Controller, comunicando tramite la porta TCP 80.

Citrix Director

Director è uno strumento basato sul Web che consente ai team di supporto IT e dell'helpdesk di monitorare un ambiente, risolvere i problemi prima che diventino critici per il sistema ed eseguire attività di supporto per gli utenti finali. È possibile utilizzare una distribuzione Director per connettersi a più siti Citrix Virtual Apps o Citrix Virtual Desktops e monitorarli.

Director visualizza:

- Dati di sessione in tempo reale provenienti dal Servizio Broker all'interno del Controller, inclusi i dati che il Servizio Broker ottiene dall'agente broker nel VDA.
- Dati storici del sito provenienti dal servizio di monitoraggio all'interno del Controller.

Director utilizza i dati relativi alle prestazioni e all'euristica ICA acquisiti dal dispositivo Citrix Gateway per creare analisi a partire dai dati e quindi presentarle agli amministratori.

È inoltre possibile visualizzare e interagire con le sessioni di un utente tramite Director, utilizzando Assistenza remota di Windows.

Citrix License Server

License Server gestisce le licenze dei prodotti Citrix. Comunica con il Controller per gestire le licenze per ogni sessione utente e con Studio per allocare i file di licenza. Un sito deve disporre di almeno un server licenze per archiviare e gestire i file delle licenze.

Hypervisor o altro servizio

L'hypervisor o altro servizio effettua l'hosting delle macchine virtuali nel sito. Queste possono essere le VM utilizzate per ospitare applicazioni e desktop e le VM utilizzate per ospitare i componenti di Citrix Virtual Apps and Desktops. Un hypervisor viene installato su un computer host interamente dedicato all'esecuzione dell'hypervisor e all'hosting di macchine virtuali.

Citrix Virtual Apps and Desktops supporta vari hypervisor e altri servizi.

Sebbene molte distribuzioni richiedano un hypervisor, non è necessario un hypervisor per fornire la funzionalità di accesso remoto a PC. Non è necessario un hypervisor neanche quando si utilizza Provisioning Services (PVS) per eseguire il provisioning delle macchine virtuali.

Componenti aggiuntivi

Anche i seguenti componenti possono essere inclusi nelle distribuzioni di Citrix Virtual Apps and Desktops. Per ulteriori informazioni, vedere la relativa documentazione.

Citrix Provisioning

Citrix Provisioning (in precedenza Provisioning Services) è un componente opzionale disponibile con alcune edizioni. Fornisce un'alternativa a MCS per il provisioning delle macchine virtuali. MCS crea copie di un'immagine master, mentre PVS trasmette l'immagine master ai dispositivi utente. PVS non richiede un hypervisor per farlo, quindi è possibile utilizzarlo per ospitare macchine fisiche. PVS comunica con il Controller per fornire risorse agli utenti.

Citrix Gateway

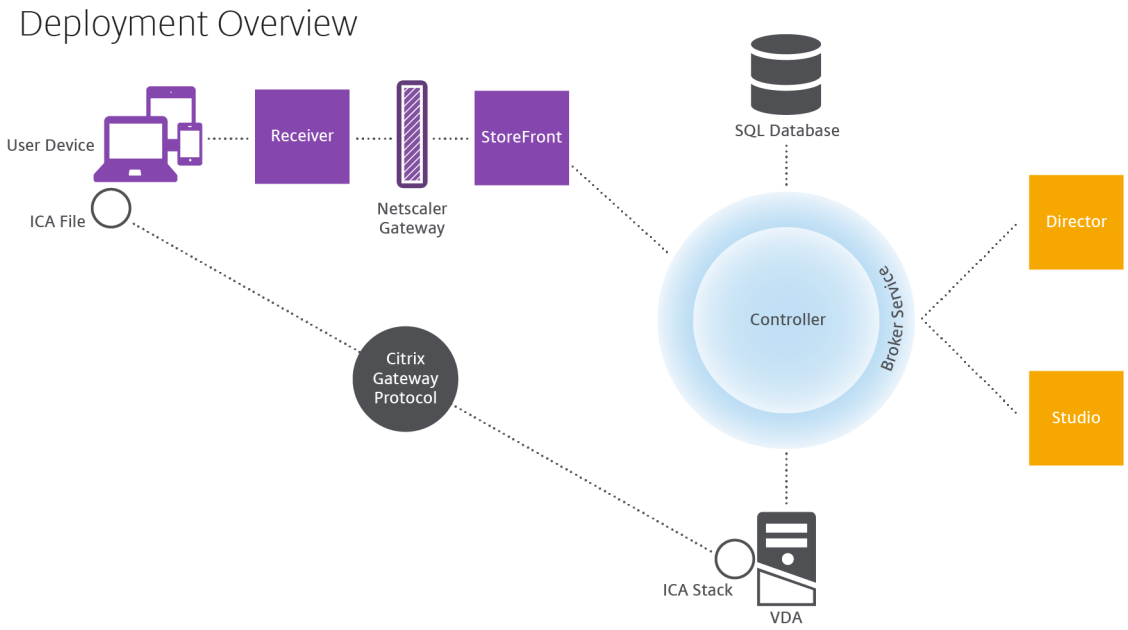
Quando gli utenti si connettono dall'esterno del firewall aziendale, Citrix Virtual Apps and Desktops può utilizzare la tecnologia Citrix Gateway (precedentemente Access Gateway e NetScaler Gateway) per proteggere queste connessioni con TLS. L'appliance virtuale Citrix Gateway o VPX è un'appliance VPN SSL distribuita nella zona demilitarizzata (DMZ). Fornisce un unico punto di accesso sicuro attraverso il firewall aziendale.

Citrix SD-WAN

Nelle distribuzioni in cui i desktop virtuali vengono distribuiti agli utenti in sedi remote quali le filiali, la tecnologia Citrix SD-WAN può essere utilizzata per ottimizzare le prestazioni. I ripetitori accelerano le prestazioni nelle reti WAN. Con i ripetitori nella rete, gli utenti delle filiali sperimentano prestazioni simili alla LAN sulla WAN. Citrix SD-WAN può dare priorità a diverse parti dell'esperienza utente in modo che, ad esempio, l'esperienza utente non peggiori nella posizione della filiale quando un file di grandi dimensioni o un processo di stampa viene inviato attraverso la rete. L'ottimizzazione HDX WAN fornisce compressione in formato token e deduplicazione dei dati, riducendo drasticamente i requisiti di larghezza di banda e migliorando le prestazioni.

Come funzionano le distribuzioni tipiche

Un sito è costituito da macchine con ruoli dedicati che consentono scalabilità, elevata disponibilità e failover e offrono una soluzione progettata per essere sicura. Un sito è costituito da server e computer desktop installati dal VDA e dal Delivery Controller, che gestisce l'accesso.



Il VDA consente agli utenti di connettersi a desktop e applicazioni. Viene installato su macchine virtuali del centro dati per la maggior parte dei metodi di distribuzione, ma può anche essere installato su PC fisici per l'accesso remoto ai PC.

Il Controller è costituito da servizi Windows indipendenti che gestiscono risorse, applicazioni e desktop e ottimizzano e bilanciano le connessioni degli utenti. Ogni sito ha uno o più Controller. Poiché le sessioni sono influenzate da latenza, larghezza di banda e affidabilità di rete, se possibile è bene posizionare tutti i controller sulla stessa LAN.

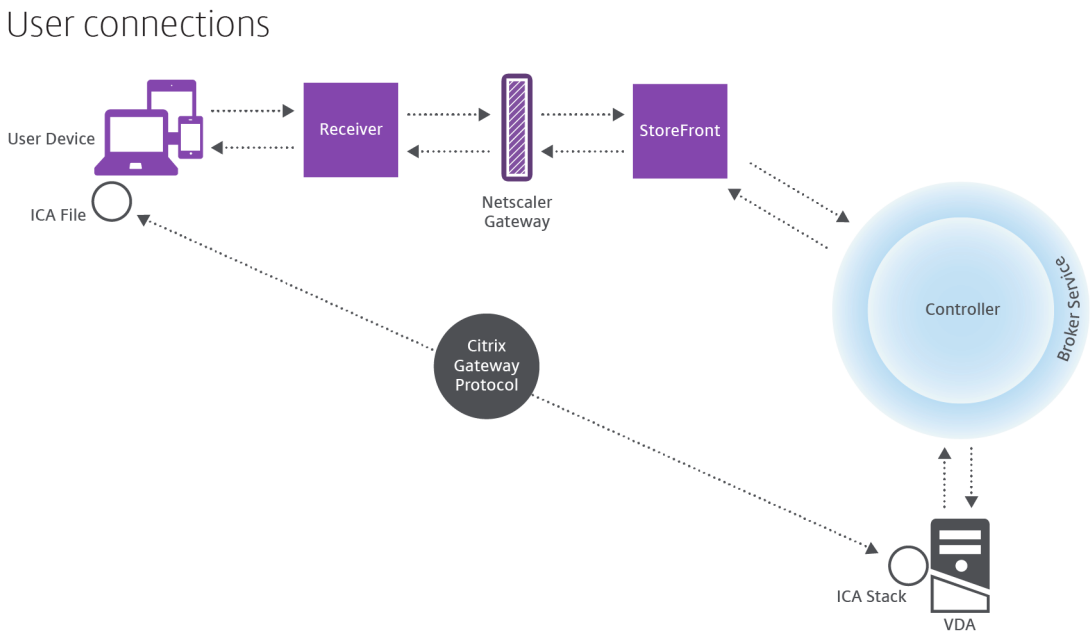
Gli utenti non accedono mai direttamente al Controller. Il VDA funge da intermediario tra gli utenti e il Controller. Quando gli utenti accedono utilizzando StoreFront, le loro credenziali passano attraverso il servizio Broker sul Controller. Il servizio Broker ottiene quindi i profili e le risorse disponibili in base ai criteri impostati per essi.

Come vengono gestite le connessioni utente

Per avviare una sessione, l'utente si connette tramite l'app Citrix Workspace installata sul dispositivo dell'utente o tramite un sito Web StoreFront.

L'utente seleziona il desktop fisico o virtuale o l'applicazione virtuale necessaria.

Le credenziali dell'utente si spostano attraverso questo percorso per accedere al Controller, che determina quali risorse sono necessarie comunicando con un servizio Broker. Citrix consiglia agli amministratori di inserire un certificato SSL su StoreFront per crittografare le credenziali provenienti dall'app Citrix Workspace.



Il servizio Broker determina a quali desktop e applicazioni l'utente può accedere.

Dopo la verifica delle credenziali, le informazioni sulle applicazioni o sui desktop disponibili vengono inviate all'utente tramite il percorso dell'app StoreFront-Citrix Workspace. Quando l'utente seleziona applicazioni o desktop da questo elenco, tali informazioni seguono di nuovo il percorso verso il controller. Il Controller determina quindi il VDA appropriato per ospitare le applicazioni specifiche o il desktop.

Il Controller invia un messaggio al VDA con le credenziali dell'utente, quindi invia tutti i dati sull'utente e sulla connessione al VDA. Il VDA accetta la connessione e invia le informazioni attraverso gli stessi percorsi all'app Citrix Workspace. Una serie di parametri richiesti viene raccolta su StoreFront. Questi parametri vengono quindi inviati all'app Citrix Workspace o come parte della conversazione del protocollo Citrix-Workspace-App-StoreFront o convertiti in un file ICA (Independent Computing Architecture) e scaricati. Se il sito è stato configurato correttamente, le credenziali rimangono crittografate durante tutto il processo.

Il file ICA viene copiato sul dispositivo dell'utente e stabilisce una connessione diretta tra il dispositivo e lo stack ICA in esecuzione sul VDA. Questa connessione ignora l'infrastruttura di gestione (app Citrix Workspace, StoreFront e Controller).

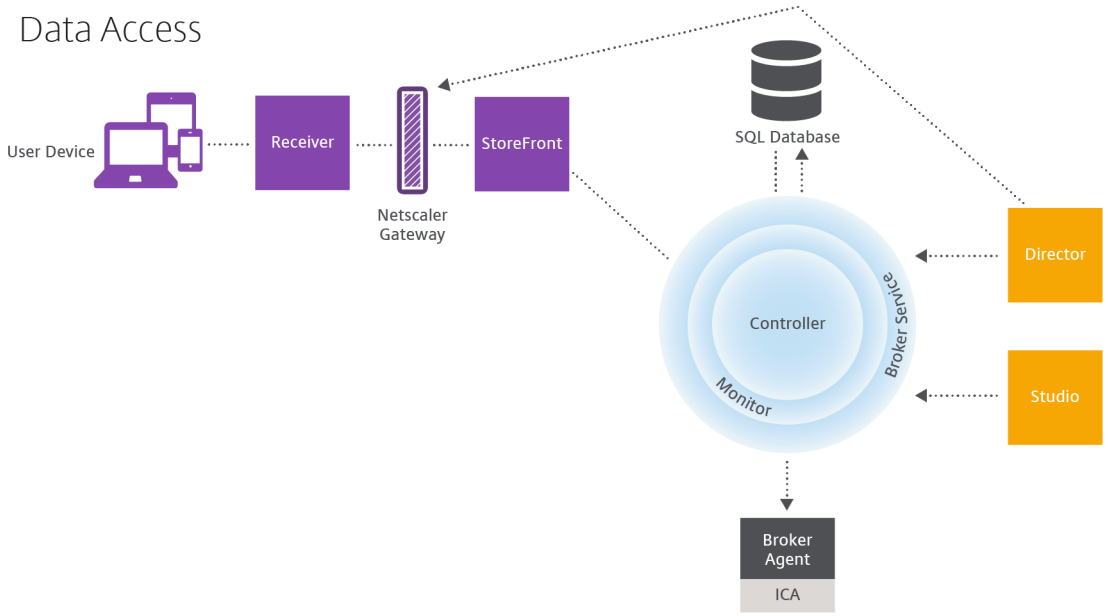
La connessione tra l'app Citrix Workspace e il VDA utilizza il protocollo CGP (Citrix Gateway Protocol). In caso di perdita di una connessione, la funzionalità Affidabilità sessione consente all'utente di ricon-

nettersi al VDA invece di dover riavviare l'infrastruttura di gestione. L'affidabilità delle sessioni può essere attivata o disattivata nei criteri Citrix.

Dopo che il client si connette al VDA, questo notifica al controller che l'utente ha effettuato l'accesso. Il Controller invia quindi queste informazioni al database del sito e inizia a registrare i dati nel database di monitoraggio.

Come funziona l'accesso ai dati

Ogni sessione di Citrix Virtual Apps and Desktops produce dati a cui l'IT può accedere tramite Studio o Director. Utilizzando Studio, gli amministratori possono accedere ai dati in tempo reale provenienti dall'agente Broker per gestire i siti. Director accede agli stessi dati e ai dati storici memorizzati nel database di monitoraggio. Consente inoltre di accedere ai dati HDX provenienti da NetScaler Gateway per il supporto dell'helpdesk e la risoluzione dei problemi.



All'interno del Controller, il Servizio Broker riporta i dati di sessione per ogni sessione sulla macchina fornendo dati in tempo reale. Il servizio di monitoraggio tiene inoltre traccia dei dati in tempo reale e li memorizza come dati storici nel database di monitoraggio.

Studio comunica solo con il servizio Broker. Accede solo ai dati in tempo reale. Director comunica con il servizio Broker (tramite un plug-in dell'agente Broker) per accedere al database del sito.

Director può anche accedere a Citrix Gateway per ottenere informazioni sui dati HDX.

Distribuzione di desktop e applicazioni

È possibile configurare le macchine che forniscono applicazioni e desktop con cataloghi di macchine. Quindi, si creano gruppi di consegna che specificano le applicazioni e i desktop che saranno disponibili (utilizzando i computer presenti nei cataloghi) e quali utenti possono accedervi. Facoltativamente, è possibile creare gruppi di applicazioni per gestire raccolte di applicazioni.

Cataloghi di macchine

I cataloghi di macchine sono raccolte di macchine virtuali o fisiche gestite come singola entità. Queste macchine e l'applicazione o i desktop virtuali che contengono sono le risorse fornite agli utenti. Tutte le macchine di un catalogo hanno lo stesso sistema operativo e lo stesso VDA installato. Hanno anche le stesse applicazioni o gli stessi desktop virtuali.

In genere, si crea un'immagine master e la si utilizza per creare macchine virtuali identiche nel catalogo. Per le macchine virtuali è possibile specificare il metodo di provisioning per le macchine di quel catalogo: strumenti Citrix (Citrix Provisioning o MCS) o altri strumenti. In alternativa, è possibile utilizzare le proprie immagini esistenti. In tal caso, è necessario gestire i dispositivi di destinazione individualmente o collettivamente utilizzando strumenti di distribuzione elettronica di software (ESD) di terze parti.

I tipi di macchine validi sono:

- **Sistema operativo multisessione:** macchine virtuali o fisiche con sistema operativo multisessione. È utilizzato per la distribuzione di app pubblicate Citrix Virtual Apps (note anche come applicazioni ospitate basate su server) e di desktop pubblicati Citrix Virtual Apps (noti anche come desktop ospitati su server). Queste macchine consentono a più utenti di connettersi a loro allo stesso tempo.
- **Sistema operativo a sessione singola:** macchine virtuali o fisiche con un sistema operativo a sessione singola. Utilizzato per la distribuzione di desktop VDI (desktop che eseguono sistemi operativi a sessione singola che possono essere personalizzati), app ospitate nella VM (applicazioni da sistemi operativi a sessione singola) e desktop fisici ospitati. A ciascuno di questi desktop può connettersi solo un utente alla volta.
- **Accesso remoto PC:** consente agli utenti remoti di accedere ai PC dell'ufficio fisico da qualsiasi dispositivo in cui sia in esecuzione l'app Citrix Workspace. I PC dell'ufficio vengono gestiti tramite la distribuzione di Citrix Virtual Desktops e richiedono che i dispositivi utente siano specificati in un elenco di autorizzazioni.

Per ulteriori informazioni, vedere Gestione delle immagini di Citrix Virtual Apps and Desktops e Creare cataloghi di macchine.

Gruppi di consegna

I gruppi di consegna specificano gli utenti che possono accedere alle varie applicazioni, ai desktop o entrambi e su quali computer. I gruppi di consegna contengono le macchine dei cataloghi di macchine e gli utenti di Active Directory che hanno accesso al sito. È possibile assegnare utenti ai gruppi di consegna in base al gruppo Active Directory, poiché i gruppi di consegna e i gruppi di Active Directory sono modi di raggruppare gli utenti con requisiti simili.

Ciascun gruppo di consegna può contenere macchine provenienti da più di un catalogo e ogni catalogo di macchine può contribuire a più di un gruppo di consegna. Tuttavia, ogni singola macchina può appartenere a un solo gruppo di consegna alla volta.

È possibile definire a quali risorse possono accedere gli utenti del gruppo di consegna. Ad esempio, per distribuire applicazioni diverse a utenti diversi, è possibile installare tutte le applicazioni nell'immagine master di un catalogo e creare in tale catalogo un numero sufficiente di macchine da distribuire tra diversi gruppi di consegna. È quindi possibile configurare ogni gruppo di consegna in modo da distribuire un sottoinsieme diverso di applicazioni installate sui computer.

Per ulteriori informazioni, vedere Creare gruppi di consegna.

Gruppi di applicazioni

I gruppi di applicazioni offrono vantaggi in termini di gestione delle applicazioni e di controllo delle risorse rispetto all'uso di più gruppi di consegna. Utilizzando la funzione di restrizione tag, è possibile utilizzare i computer esistenti per più di un'attività di pubblicazione, risparmiando i costi associati alla distribuzione e gestendo più macchine. Una restrizione tag può essere spiegata come una suddivisione (o la creazione di partizioni) delle macchine che fanno parte di un gruppo di consegna. I gruppi di applicazioni possono essere utili anche per isolare e risolvere i problemi di un sottoinsieme di macchine che fanno parte di un gruppo di consegna.

Per ulteriori informazioni, vedere Creare gruppi di applicazioni.

Ulteriori informazioni

- Diagrammi di Citrix Virtual Apps and Desktops
- Porte di rete
- Database
- Hypervisor supportati e altri servizi

Database

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Un sito Citrix Virtual Apps o Citrix Virtual Desktops utilizza tre database SQL Server:

- **Sito:** (noto anche come configurazione del sito) memorizza la configurazione del sito in esecuzione, oltre allo stato della sessione corrente e alle informazioni di connessione.
- **Registrazione:** (nota anche come registrazione configurazione) memorizza le informazioni sulle modifiche alla configurazione del sito e sulle attività amministrative. Questo database viene utilizzato quando è abilitata la funzione di registrazione di configurazione (impostazione predefinita= abilitato).
- **Monitoraggio:** memorizza i dati utilizzati da Director, ad esempio le informazioni sulla sessione e la connessione.

Ogni Delivery Controller comunica con il database del sito. È richiesta l'autenticazione di Windows tra il controller e i database. Un controller può essere scollegato o disattivato senza influire sugli altri controller presenti nel sito. Ciò significa, tuttavia, che il database del sito forma un singolo punto di errore. In caso di errori del server del database, le connessioni esistenti continuano a funzionare fino a quando un utente non si scollega o si disconnette. Per informazioni sul comportamento di connessione quando il database del sito diventa non disponibile, vedere Cache host locale.

Citrix consiglia quanto segue per quanto riguarda i database:

- **Eseguire regolarmente il backup.** Eseguire regolarmente il backup dei database in modo da poter eseguire il ripristino dal backup se vi sono errori nel server dei database. La strategia di backup per ogni database può essere diversa. Per ulteriori informazioni, vedere CTX135207; si noti, tuttavia, che si riferisce a CitrixXenDesktopDB, che non è più supportato e non è disponibile per i clienti.
- **Eseguire regolarmente il backup e il ripristino del sito, del monitoraggio e della registrazione dei database SQL Server.** Per informazioni specifiche sui database SQL Server, vedere Creating Full and Differential Backups of a SQL Server Database (Creare backup completi e differenziali di un database SQL Server).

Se il sito contiene più zone, assicurarsi che la zona primaria contenga sempre il database del sito. I controller di ogni zona comunicano con quel database.

Elevata disponibilità

Esistono diverse soluzioni a disponibilità elevata da considerare per garantire il failover automatico:

- **Gruppi di disponibilità AlwaysOn (inclusi i gruppi di disponibilità di base):** questa soluzione di elevata disponibilità e ripristino di emergenza a livello aziendale introdotta in SQL Server 2012 consente di ottimizzare la disponibilità per uno o più database. La soluzione Gruppi di disponibilità AlwaysOn richiede che le istanze di SQL Server risiedano nei nodi di clustering di failover di Windows Server (WSFC). Per ulteriori informazioni, vedere Clustering di failover di Windows Server con SQL Server.
- **Mirroring del database SQL Server:** il mirroring del database garantisce che, se si perde il server di database attivo, si verifichi un processo di failover automatico in pochi secondi, in modo che gli utenti in genere non ne risentano. Questo metodo è più costoso rispetto ad altre soluzioni perché sono necessarie licenze complete di SQL Server in ogni server di database. Non è possibile utilizzare SQL Server Express Edition in un ambiente con mirroring.
- **Clustering SQL:** la tecnologia di clustering Microsoft SQL può essere utilizzata per consentire automaticamente a un server di assumere le attività e le responsabilità di un altro server che ha riportato errori. Tuttavia, l'impostazione di questa soluzione è più complicata e il processo di failover automatico è in genere più lento rispetto ad alternative come il mirroring SQL.
- **Utilizzo delle funzionalità di alta disponibilità dell'hypervisor:** con questo metodo, è possibile distribuire il database come macchina virtuale e utilizzare le funzionalità di elevata disponibilità dell'hypervisor. Questa soluzione è meno costosa del mirroring perché utilizza il software dell'hypervisor esistente e consente anche di utilizzare SQL Server Express Edition. Tuttavia, il processo di failover automatico è più lento, in quanto per l'avvio di un nuovo computer per il database potrebbe richiedere tempo, interrompendo quindi il servizio per gli utenti.

La funzionalità Cache host locale integra le procedure consigliate per la disponibilità elevata di SQL Server. La cache host locale consente agli utenti di connettersi e riconnettersi ad applicazioni e desktop anche quando il database del sito non è disponibile. Per ulteriori informazioni, vedere Cache host locale.

Se tutti i controller di un sito presentano errori, è possibile configurare i VDA in modo che funzionino in modalità ad alta disponibilità, consentendo agli utenti di continuare ad accedere ai desktop e alle applicazioni. In modalità ad alta disponibilità, il VDA accetta connessioni ICA dirette dagli utenti, anziché le connessioni negoziate dal controller. Utilizzare questa funzione solo nelle rare occasioni in cui la comunicazione con tutti i controller non riesce. La funzionalità non è un'alternativa ad altre soluzioni ad alta disponibilità. Per ulteriori informazioni, vedere CTX 127564.

L'installazione di un controller in un nodo in un cluster SQL o un'installazione di mirroring SQL non è supportata.

Installare il software del database

Per impostazione predefinita, SQL Server Express Edition viene installato quando si installa il primo Delivery Controller se un'altra istanza di SQL Server non viene rilevata in tale server. Tale azione predefinita è generalmente sufficiente per la prova di concetto o per le implementazioni pilota. Tuttavia, SQL Server Express non supporta le funzionalità di disponibilità elevata Microsoft.

L'installazione predefinita utilizza gli account e le autorizzazioni predefiniti del servizio Windows. Per informazioni dettagliate su queste impostazioni predefinite, inclusa l'aggiunta di account del servizio Windows al ruolo sysadmin, vedere la documentazione di Microsoft. Il controller utilizza l'account Servizio di rete in questa configurazione. Il controller non richiede ulteriori ruoli o autorizzazioni di SQL Server.

Se necessario, è possibile selezionare **Nascondi istanza** per l'istanza di database. Quando si configura l'indirizzo del database in Web Studio, immettere il numero di porta statica dell'istanza anziché il nome. Per informazioni dettagliate su come nascondere un'istanza del Motore di database di SQL Server, vedere la documentazione Microsoft.

Per la maggior parte delle distribuzioni di produzione e per qualsiasi distribuzione che utilizza le funzionalità di disponibilità elevata di Microsoft, è consigliabile utilizzare solo le edizioni non Express supportate di SQL Server. Installare SQL Server su macchine diverse dal server in cui è installato il primo controller. I requisiti di sistema elencano le versioni supportate di SQL Server. I database possono risiedere su una o più macchine.

Assicurarsi che il software SQL Server sia installato prima di creare un sito. Non è necessario creare il database, ma se lo si crea, deve essere vuoto. Si consiglia inoltre di configurare le tecnologie Microsoft ad alta disponibilità.

Utilizzare Windows Update per mantenere SQL Server aggiornato.

Impostare i database nella creazione guidata sito

Specificare i nomi e gli indirizzi (posizione) dei database nella pagina **Database** della creazione guidata sito (vedere Formati degli indirizzi del database). Per evitare potenziali errori quando Director esegue una query sul servizio di monitoraggio, non utilizzare spazi nel nome del database di monitoraggio.

La pagina **Database** offre due opzioni per l'impostazione dei database: automatico e mediante script. In genere, è possibile utilizzare l'opzione automatica se l'utente di Web Studio e l'amministratore Citrix dispongono dei privilegi di database richiesti (vedere Autorizzazioni necessarie per impostare i database).

È possibile modificare il percorso del database di registrazione e monitoraggio della configurazione in un secondo momento, dopo aver creato il sito. Vedere Modificare le posizioni dei database.

Per configurare un sito per l'utilizzo di un database mirror, eseguire le operazioni riportate di seguito e procedere con la procedura di installazione automatica o con script.

1. Installare il software SQL Server su due server, A e B.
2. Nel server A creare il database destinato a essere utilizzato come principale. Eseguire il backup del database sul server A e copiarlo nel server B.
3. Nel server B ripristinare il file di backup.
4. Avviare il mirroring sul server A.

Per verificare il mirroring dopo aver creato il sito, eseguire il cmdlet PowerShell `get-configdbconnection` per assicurarsi che il partner di failover sia stato impostato nella stringa di connessione al mirror.

Se in un secondo momento si aggiunge, si sposta o si rimuove un Delivery Controller in un ambiente di database con mirroring, vedere Delivery Controller.

Impostazione automatica

Se si dispone dei privilegi di database richiesti, selezionare **Crea e impostare database da Studio** nella pagina **Database** della creazione guidata sito. Quindi fornire i nomi e gli indirizzi dei database principali.

Se esiste un database in un indirizzo specificato, il database deve essere vuoto. Se non esistono database in un indirizzo specificato, si viene informati che non è possibile trovare un database e quindi viene chiesto se si desidera che il database venga creato automaticamente. Quando si conferma tale azione, Web Studio crea automaticamente i database e quindi applica gli script di inizializzazione per i database principale e duplicato.

Configurazione con script

Se non si dispone dei diritti richiesti per database, chiedere assistenza a qualcuno che ne dispone, ad esempio un amministratore del database. Ecco la sequenza:

1. Nella pagina **Database** della creazione guidata sito selezionare **Generate scripts to manually set up** (Genera script per configurare manualmente). Questa azione genera i seguenti tre tipi di script per ciascuno dei seguenti database principali e per i database replica: database del sito, di monitoraggio e di registrazione.

    - *Script contenente "SysAdmin" nel nome*. Uno script che crea i database e l'accesso del Delivery Controller. Queste attività richiedono diritti securityadmin.
    - *Script contenente "DbOwner" nel nome*. Script che crea i ruoli utente nel database, aggiunge gli account di accesso e quindi crea gli schemi del database. Queste attività richiedono diritti `db_owner`.

- *Script contenente "Mixed" nel nome*. Tutte le attività in un solo script, indipendentemente dai diritti richiesti.

È possibile indicare dove memorizzare gli script.

> **Nota:**
>
> Negli ambienti aziendali, la configurazione del database include script che potrebbero essere gestiti da team diversi con ruoli (diritti) diversi: `securityadmin` o `db_owner`. Se applicabile, si dispone innanzitutto di script "SysAdmin" eseguiti dagli amministratori con il ruolo `securityadmin` e quindi di script "DbOwner" eseguiti dagli amministratori con diritti `db_owner`. Per generare questi script, è anche possibile utilizzare PowerShell. Per i dettagli, vedere Script dei diritti di database preferiti.

2. Dare questi script all'amministratore dei database. A questo punto, la creazione guidata sito si interrompe automaticamente. Quando si torna in un secondo momento, viene richiesto di continuare la creazione del sito.

L'amministratore dei database crea quindi i database. Ogni database deve avere le seguenti caratteristiche:

- Utilizzare regole di raccolta che terminano con `_CI_AS_KS`. Si consiglia di utilizzare una raccolta che termina con `_100_CI_AS_KS`.
- Per ottenere prestazioni ottimali, attivare la copia istantanea in lettura di SQL Server. Per ulteriori informazioni, vedere CTX 137161.
- Funzionalità di alta disponibilità configurate, se applicabile.
- Per configurare il mirroring, impostare innanzitutto il database in modo che utilizzi il modello di ripristino completo (il modello semplice è l'impostazione predefinita). Eseguire il backup del database principale in un file e copiarlo nel server mirror. Quindi, ripristinare il file di backup sul server mirror. Infine, avviare il mirroring sul server principale.

L'amministratore del database utilizza l'utilità della riga di comando SQLCMD o SQL Server Management Studio in modalità SQLCMD per:

- Eseguire ciascuno degli script `xxx_Replica.sql` nelle istanze di database SQL Server ad alta disponibilità (se è configurata la disponibilità elevata).
- Eseguire ciascuno degli script `xxx\\_Principal.sql` nelle istanze principali del database di SQL Server.

Per dettagli di SQLCMD vedere la documentazione Microsoft.

Quando tutti gli script sono stati completati correttamente, l'amministratore del database fornisce all'amministratore Citrix i tre indirizzi principali del database.

Web Studio richiede di continuare la creazione del sito. Si torna alla pagina **Databases** . Immettere gli indirizzi. Se non è possibile contattare nessuno dei server che ospitano un database, viene visualizzato un messaggio di errore.

Autorizzazioni necessarie per impostare i database

Per creare e inizializzare i database o modificarne la posizione, è necessario essere un amministratore locale e un utente di dominio. È inoltre necessario disporre di determinate autorizzazioni di SQL Server. Le seguenti autorizzazioni possono essere configurate o acquisite in modo esplicito dall'appartenenza al gruppo Active Directory. Se le credenziali utente di Web Studio non includono queste autorizzazioni, vengono richieste le credenziali utente di SQL Server.

Operazione	Scopo	Ruolo del server	Ruolo del database
Creare un database	Creare un database vuoto adatto	`dbcreator`	
Creare uno schema	Creare tutti gli schemi specifici del servizio e aggiungere il primo controller al sito	`securityadmin`*	`db_owner`
Aggiungere un controller	Aggiungere un controller (diverso dal primo) al sito	`securityadmin`*	`db_owner`
Aggiungi un controller (server mirror)	Aggiungere un account di accesso controller al server di database attualmente nel ruolo mirror di un database con mirroring	`securityadmin`*	
Rimuovi il controller	Rimuovere il controller dal sito	**	`db_owner`
Aggiorna uno schema	Applicare gli aggiornamenti o gli aggiornamenti rapidi dello schema		`db_owner`

* Mentre tecnicamente più restrittivo, in pratica, è possibile considerare il ruolo del server `securityadmin` come equivalente al ruolo del server `sysadmin`.

** Quando un controller viene rimosso da un sito, l'accesso del controller al server dei database non

viene rimosso. Questo per evitare di rimuovere potenzialmente un accesso utilizzato da servizi diversi da questo prodotto Citrix sullo stesso computer. Se non è più necessario, l'accesso deve essere rimosso manualmente. Questa azione richiede l'appartenenza al ruolo `securityadmin` del server.

Quando si utilizza Web Studio per eseguire queste operazioni, l'utente di Web Studio deve disporre di un account del server di database che appartenga esplicitamente ai ruoli server appropriati oppure essere in grado di fornire le credenziali di un account che vi appartiene.

Script dei diritti di database preferiti

Negli ambienti aziendali, la configurazione del database include script che devono essere gestiti da team diversi con ruoli (diritti) diversi: `securityadmin` o `db_owner`.

Utilizzando PowerShell, è ora possibile specificare i diritti preferiti per i database. La specifica di un valore non predefinito comporta la creazione di script separati. Uno script contiene attività che richiedono il ruolo `securityadmin`. L'altro script richiede solo diritti `db_owner` e può essere eseguito da un amministratore Citrix, senza dover contattare un amministratore del database.

Nei cmdlet `get-*DBSchema`, l'opzione `-DatabaseRights` hai i seguenti valori validi:

- `SA`: genera uno script che crea i database e l'accesso del Delivery Controller. Queste attività richiedono diritti `securityadmin`.
- `DBO`: genera uno script che crea i ruoli utente nel database, aggiunge gli account di accesso e quindi crea gli schemi del database. Queste attività richiedono diritti `db_owner`.
- `Mixed`: (impostazione predefinita) tutte le attività presenti in uno script, indipendentemente dai diritti richiesti.

Per ulteriori informazioni, vedere la Guida del cmdlet.

Formati degli indirizzi di database

È possibile specificare un indirizzo di database in uno dei seguenti formati:

- `ServerName`
- `ServerName\InstanceName`
- `ServerName,PortNumber`

Per un gruppo di disponibilità AlwaysOn, specificare il listener del gruppo nel campo della posizione.

Modifica delle posizioni dei database

Dopo aver creato un sito, è possibile modificare il percorso dei database di registrazione e monitoraggio della configurazione. Non è possibile modificare la posizione del database del sito. Quando si modifica la posizione di un database:

- I dati del database precedente non vengono importati nel nuovo database.
- I log non possono essere aggregati da entrambi i database durante il recupero dei log.
- La prima voce di registro nel nuovo database indica che si è verificata una modifica nel database, ma non identifica il database precedente.

Non è possibile modificare la posizione del database di registrazione della configurazione quando è abilitata la registrazione obbligatoria.

Per modificare la posizione di un database:

1. Verificare che nel server in cui si desidera che risieda il database sia installata una versione supportata di Microsoft SQL Server. Impostare le funzionalità di alta disponibilità in base alle esigenze.
2. Accedere a Web Studio e quindi selezionare **Settings** nel riquadro a sinistra.
3. Individuare il riquadro **Database** e selezionare **Edit**.
4. Nella pagina **Manage Database** (Gestione database), selezionare il database per il quale si desidera specificare una nuova posizione, quindi selezionare **Change Database** (Modifica database) nella barra delle azioni.
5. Specificare la nuova posizione e il nome del database.
6. Se si desidera che Web Studio crei il database e si dispone delle autorizzazioni appropriate, fare clic su **Done**. Quando richiesto, fare clic su **Done**e quindi Web Studio creerà automaticamente il database. Web Studio tenta di accedere al database utilizzando le credenziali dell'utente. Se l'operazione non riesce, viene richiesto di specificare le credenziali dell'utente del database. Web Studio carica quindi lo schema del database nel database Le credenziali vengono conservate solo per il periodo di tempo di creazione del database.
7. Se non si desidera che Web Studio crei il database o non si dispone di autorizzazioni sufficienti, fare clic su **Generate database script**. Gli script generati includono istruzioni per la creazione manuale del database e un database mirror, se necessario. Prima di caricare lo schema, assicurarsi che il database sia vuoto e che almeno un utente disponga dell'autorizzazione di accesso e modifica del database.

Ulteriori informazioni

- Strumento di dimensionamento database.
- Dimensionamento del database del sito e configurazione delle stringhe di connessione quando si utilizzano soluzioni SQL Server ad alta disponibilità.

Metodi di consegna

January 7, 2024

Citrix Virtual Apps and Desktops offre vari metodi di consegna. Un singolo metodo di consegna probabilmente non soddisferà tutte le tue esigenze.

Introduzione

La scelta del metodo di distribuzione delle applicazioni appropriato consente di migliorare la scalabilità, la gestione e l'esperienza utente.

- **App installata:** l'applicazione fa parte dell'immagine desktop di base. Il processo di installazione comporta la copia di file dll, exe e di altro tipo nell'unità immagine, oltre a modifiche del Registro di sistema. Per ulteriori informazioni, vedere Creare cataloghi di macchine.
- **App in streaming (Microsoft App-V):** l'applicazione viene profilata e consegnata ai desktop mediante la rete su richiesta. I file dell'applicazione e le impostazioni del Registro di sistema vengono collocati in un contenitore sul desktop virtuale e isolati dal sistema operativo di base e tra loro. Questo isolamento aiuta a risolvere i problemi di compatibilità. Per i dettagli, vedere Distribuire e rendere disponibili applicazioni App-V.
- **App a più livelli (Citrix App Layering):** ogni livello contiene una singola applicazione, un singolo agente o un singolo sistema operativo. Integrando un livello del sistema operativo, un unico livello di piattaforma (VDA, agente Citrix Provisioning) e molti livelli applicativi, un amministratore può facilmente creare nuove immagini distribuibili. La stratificazione semplifica la manutenzione continua, poiché un sistema operativo, un agente e un'applicazione esistono in un unico livello. Quando si aggiorna il livello, tutte le immagini distribuite che contengono tale livello vengono aggiornate. Per ulteriori informazioni, vedere Citrix App Layering.
- **App Windows ospitata:** applicazione installata su un host Citrix Virtual Apps multi-utente e distribuita come applicazione e non come desktop. Un utente accede all'app Windows ospitata senza soluzione di continuità dal desktop o dal dispositivo endpoint VDI, nascondendo il fatto che l'app è in esecuzione in modalità remota. Per ulteriori informazioni, vedere Creare gruppi di consegna.
- **App locale:** applicazione distribuita sul dispositivo endpoint. L'interfaccia dell'applicazione viene visualizzata all'interno della sessione VDI ospitata dell'utente, anche se viene eseguita sull'endpoint. Per ulteriori informazioni, vedere Accesso alle app locali e reindirizzamento URL.

Per i desktop, prendere in considerazione i desktop pubblicati o i desktop VDI.

App e desktop pubblicati da Citrix Virtual Apps

Utilizzare computer con sistema operativo multisessione per distribuire Citrix Virtual Apps and Desktops e desktop pubblicati.

Caso d'uso:

- Desiderate una distribuzione economica basata su server per ridurre al minimo i costi di distribuzione delle applicazioni a molti utenti, offrendo al contempo un'esperienza utente sicura e ad alta definizione.
- Gli utenti eseguono attività ben definite e non richiedono personalizzazione né accesso offline alle applicazioni. Gli utenti possono includere task worker, ad esempio operatori del call center e addetti al dettaglio, oppure utenti che condividono le workstation.
- Tipi di applicazione: qualsiasi applicazione.

Vantaggi e considerazioni:

- Soluzione gestibile e scalabile all'interno del data center.
- La soluzione più conveniente per la distribuzione delle applicazioni.
- Le applicazioni ospitate vengono gestite centralmente e gli utenti non possono modificare l'applicazione. Ciò fornisce un'esperienza utente coerente, sicura e affidabile.
- Gli utenti devono essere online per accedere alle loro applicazioni.

Esperienza utente:

- L'utente richiede una o più applicazioni da StoreFront, dal menu **Start** o dall'URL fornito dall'utente.
- Le applicazioni vengono distribuite virtualmente e vengono visualizzate perfettamente in alta definizione sui dispositivi utente.
- A seconda delle impostazioni del profilo, le modifiche dell'utente vengono salvate al termine della sessione dell'applicazione dell'utente. Altrimenti, le modifiche vengono eliminate.

Elaborare, ospitare e distribuire le applicazioni:

- L'elaborazione delle applicazioni avviene su macchine di hosting, piuttosto che sui dispositivi dell'utente. La macchina di hosting può essere una macchina fisica o virtuale.
- Applicazioni e desktop risiedono su una macchina con sistema operativo multisessione.
- Le macchine si rendono disponibili attraverso i cataloghi di macchine.
- Le macchine dei cataloghi macchine sono organizzate in gruppi di consegna che forniscono lo stesso set di applicazioni a gruppi di utenti.
- Le macchine del sistema operativo multisessione supportano gruppi di consegna che ospitano desktop o applicazioni o entrambi.

Gestione e assegnazione delle sessioni:

- I sistemi operativi multisessione eseguono più sessioni su un'unica macchina per distribuire più applicazioni e desktop a più utenti connessi contemporaneamente. Ogni utente richiede una singola sessione da cui eseguire tutte le sue applicazioni ospitate.

  Ad esempio, un utente accede e richiede un'applicazione. Una sessione di quella macchina diventa non disponibile per gli altri utenti. Un secondo utente accede e richiede un'applicazione ospitata su quella macchina. Una seconda sessione attiva sulla stessa macchina ora non è disponibile. Se entrambi gli utenti richiedono più applicazioni, non sono necessarie sessioni aggiuntive perché un utente può eseguire più applicazioni utilizzando la stessa sessione. Se altri due utenti eseguono l'accesso richiedendo desktop e sono disponibili due sessioni su quella stessa macchina, quella singola macchina ora utilizza quattro sessioni per ospitare quattro utenti diversi.

- All'interno del gruppo di consegna a cui è assegnato un utente, viene selezionata una macchina sul server meno caricato. Una macchina con disponibilità di sessione viene assegnata in modo casuale alla consegna di applicazioni a un utente quando questi esegue l'accesso.

App ospitate nella VM

Utilizzare macchine del sistema operativo a sessione singola per distribuire applicazioni ospitate nella VM

Caso d'uso:

- Si desidera una soluzione di distribuzione delle applicazioni basata su client che sia sicura, che fornisca una gestione centralizzata e che supporti molti utenti per server host. Si desidera fornire a quegli utenti applicazioni che vengono visualizzate senza soluzione di continuità in alta definizione.
- Gli utenti sono collaboratori interni, esterni su contratto, di terze parti e altri membri del team provvisorio. Gli utenti non necessitano di accesso offline alle applicazioni ospitate.
- Tipi di applicazione: applicazioni che potrebbero non funzionare correttamente con altre applicazioni o potrebbero interagire con il sistema operativo, ad esempio Microsoft .NET Framework. Questi tipi di applicazioni sono ideali per l'hosting su macchine virtuali.

Vantaggi e considerazioni:

- Le applicazioni e i desktop dell'immagine master sono gestiti, ospitati ed eseguiti in modo sicuro su macchine all'interno del data center, offrendo una soluzione di distribuzione delle applicazioni più conveniente.
- All'accesso, gli utenti possono essere assegnati casualmente a un computer all'interno di un gruppo di consegna configurato per ospitare la stessa applicazione. È inoltre possibile assegnare staticamente una singola macchina alla distribuzione di un'applicazione a un

singolo utente ogni volta che l'utente esegue l'accesso. Le macchine assegnate staticamente consentono agli utenti di installare e gestire le proprie applicazioni nella macchina virtuale.
- L'esecuzione di più sessioni non è supportata sui computer con sistema operativo a sessione singola. Pertanto, ogni utente utilizza una singola macchina all'interno di un gruppo di consegna al momento dell'accesso e gli utenti devono essere online per accedere alle proprie applicazioni.
- Questo metodo può aumentare la quantità di risorse server per l'elaborazione delle applicazioni e aumentare la quantità di spazio di archiviazione per i dati degli utenti.

Esperienza utente:

- La stessa esperienza applicativa senza soluzione di continuità dell'hosting di applicazioni condivise su sistemi operativi multisessione.

Elaborare, ospitare e distribuire le applicazioni:

- Come nelle macchine con sistema operativo multi-sessione, tranne per il fatto che sono macchine con sistema operativo virtuale a sessione singola.

Gestione e assegnazione delle sessioni:

- Le macchine del sistema operativo a sessione singola eseguono una singola sessione desktop da una singola macchina. Quando si accede solo alle applicazioni, un singolo utente può utilizzare più applicazioni (e non deve limitarsi a una singola applicazione), perché il sistema operativo vede ogni applicazione come una nuova sessione.
- All'interno di un gruppo di consegna, quando gli utenti accedono possono accedere a una macchina assegnata staticamente (ogni volta che l'utente accede allo stesso computer) o a una macchina assegnata in modo casuale selezionata in base alla disponibilità di sessioni.

Desktop VDI

Utilizzaa le macchine del sistema operativo a sessione singola per distribuire i desktop VDI di Citrix Virtual Apps and Desktops.

I desktop VDI sono ospitati su macchine virtuali e forniscono a ciascun utente un sistema operativo desktop.

I desktop VDI richiedono più risorse rispetto ai desktop pubblicati, ma non richiedono che le applicazioni installate supportino sistemi operativi basati su server. Inoltre, a seconda del tipo di desktop VDI scelto, questi desktop possono essere assegnati a singoli utenti. Ciò consente agli utenti un alto livello di personalizzazione.

Quando si crea un catalogo di macchine per desktop VDI, si crea uno dei seguenti tipi di desktop:

- **Desktop casuale non persistente, noto anche come desktop VDI in pool:** ogni volta che un utente accede a uno di questi desktop, tale utente si connette a un desktop selezionato in un pool di desktop. Quel pool è basato su una singola immagine master. Tutte le modifiche apportate al desktop vengono perse al riavvio del computer.
- **Desktop statico non persistente:** durante il primo accesso, a un utente viene assegnato un desktop tratto da un pool di desktop. Ogni macchina del pool è basata su una singola immagine master. Dopo il primo utilizzo, ogni volta che un utente accede per utilizzare un desktop, tale utente si connette allo stesso desktop assegnato al primo utilizzo. Tutte le modifiche apportate al desktop vengono perse al riavvio del computer.
- **Desktop statico persistente:** a differenza di altri tipi di desktop VDI, questi desktop possono essere personalizzati completamente dagli utenti. Durante il primo accesso, a un utente viene assegnato un desktop tratto da un pool di desktop. Gli accessi successivi di tale utente si connettono allo stesso desktop assegnato al primo utilizzo. Le modifiche apportate al desktop vengono mantenute al riavvio del computer.

Accesso remoto al PC

Accesso remoto PC è una funzionalità di Citrix Virtual Apps and Desktops che consente alle organizzazioni di consentire ai dipendenti di accedere facilmente alle risorse aziendali in remoto in modo sicuro. La piattaforma Citrix rende possibile questo accesso sicuro offrendo agli utenti l'accesso ai PC fisici dell'ufficio. If users can access their office PCs, they can access all the applications, data, and resources they need to do their work. Accesso remoto PC elimina la necessità di introdurre e fornire altri strumenti per il telelavoro. Ad esempio, desktop o applicazioni virtuali e la relativa infrastruttura associata.

Accesso remoto PC utilizza gli stessi componenti Citrix Virtual Apps and Desktops che forniscono desktop e applicazioni virtuali. Di conseguenza, i requisiti e il processo di distribuzione e configurazione di Accesso remoto PC sono gli stessi richiesti per la distribuzione di Citrix Virtual Apps and Desktops per la distribuzione di risorse virtuali. Questa uniformità offre un'esperienza amministrativa coerente e unificata. Gli utenti ricevono la migliore esperienza utente utilizzando Citrix HDX per offrire la propria sessione PC da ufficio.

Per ulteriori informazioni, vedere Accesso remoto al PC.

Porte di rete

January 7, 2024

Le informazioni complete sulle porte di rete sono fornite nelle porte di comunicazione utilizzate da Citrix Technologies.

Quando vengono installati i componenti Citrix, anche il firewall host del sistema operativo viene aggiornato per impostazione predefinita, in modo da corrispondere alle porte di rete predefinite.

Potrebbe essere necessario avere informazioni sulla porta:

- Per la conformità alle normative.
- Se è presente un firewall di rete tra i componenti Citrix Virtual Apps and Desktops e altri prodotti o componenti Citrix, per consentire di configurare il firewall in modo appropriato.
- Se si utilizza un firewall host di terze parti, ad esempio uno fornito con un pacchetto antimalware, anziché il firewall host del sistema operativo.
- Se si modifica la configurazione del firewall host su questi componenti (in genere il servizio Windows Firewall).
- Se si riconfigurano delle funzionalità dei componenti per utilizzare una porta o un intervallo di porte diverso e quindi si desidera disabilitare o bloccare le porte non utilizzate nella configurazione.

Alcune delle porte sono registrate presso l'IANA (Internet Assigned Numbers Authority). I dettagli di queste assegnazioni sono disponibili all'indirizzo http://www.iana.org/assignments/port-numbers. Tuttavia, le informazioni descrittive in possesso di IANA non sempre riflettono l'utilizzo odierno.

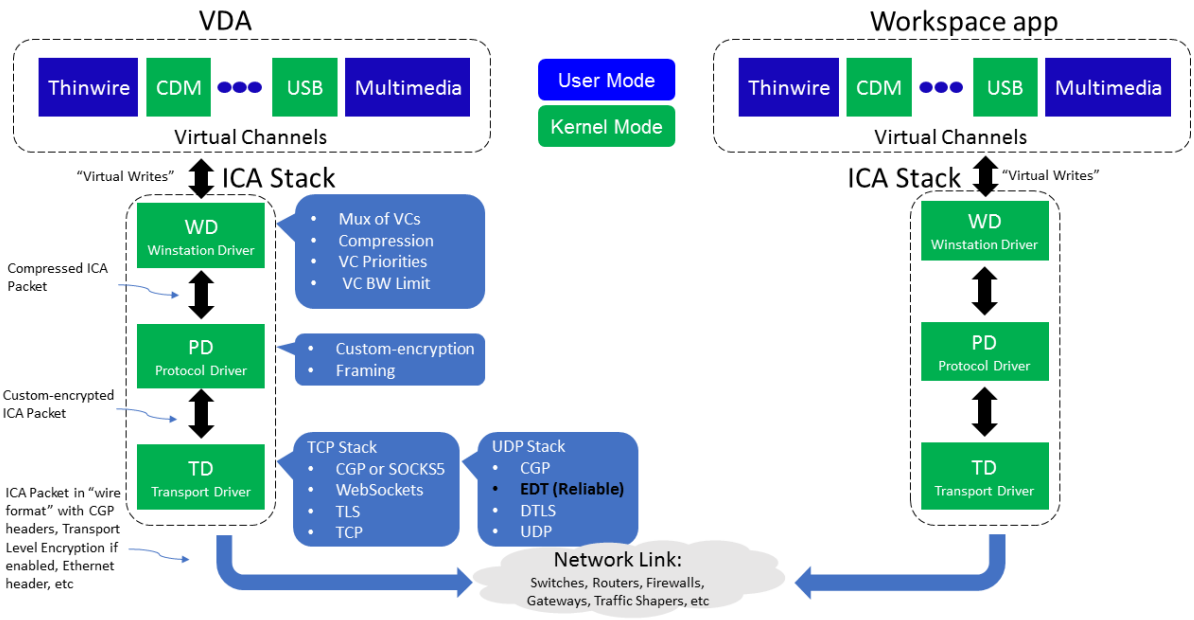
Inoltre, i sistemi operativi sul VDA e sul Delivery Controller richiedono porte in ingresso da utilizzare. Per ulteriori informazioni, vedere la documentazione di Microsoft Windows.

HDX

January 7, 2024

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Citrix HDX rappresenta un ampio set di tecnologie che offrono un'esperienza ad alta definizione agli utenti di applicazioni e desktop centralizzati, su qualsiasi dispositivo e su qualsiasi rete.

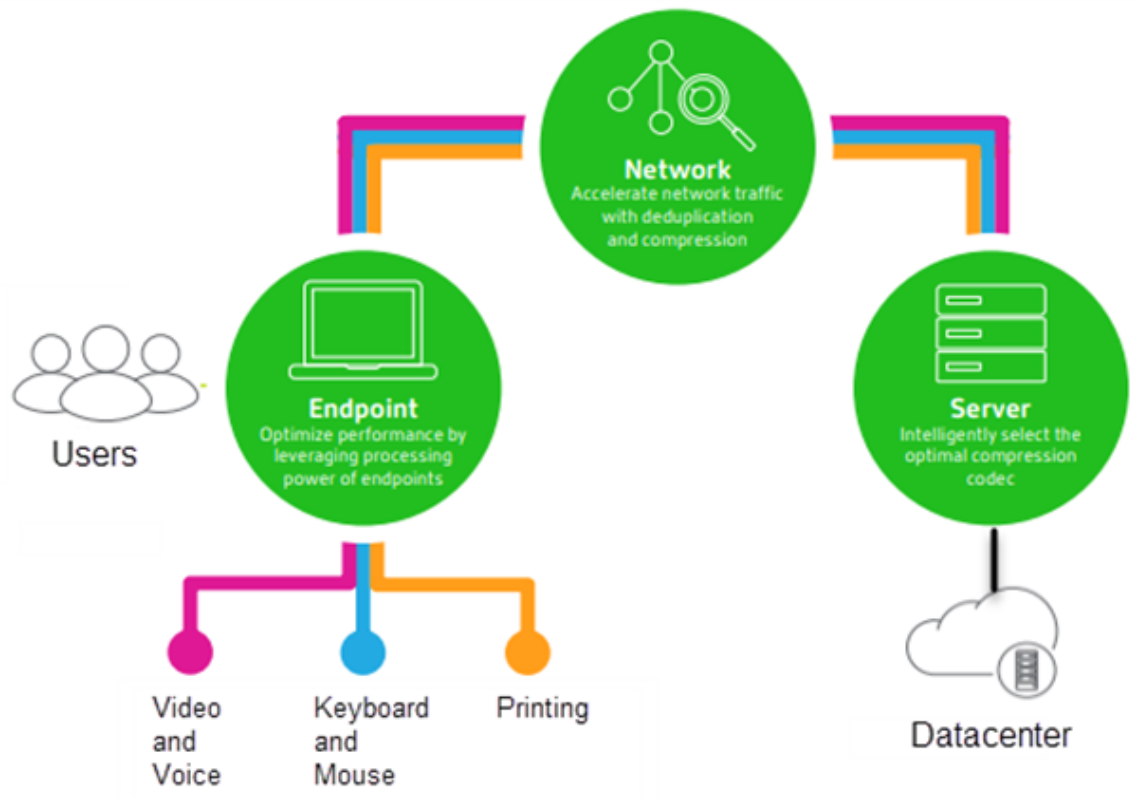


HDX è progettato in base a tre principi tecnici:

- Reindirizzamento intelligente
- Compressione adattiva
- Deduplicazione dei dati

Applicati in diverse combinazioni, questi ottimizzano l'IT e l'esperienza utente, riducono il consumo di larghezza di banda e aumentano la densità degli utenti per server di hosting.

- **Reindirizzamento intelligente**: il reindirizzamento intelligente esamina l'attività sullo schermo, i comandi delle applicazioni, il dispositivo endpoint e le funzionalità di rete e del server per determinare immediatamente come e dove eseguire il rendering di un'applicazione o un'attività desktop. Il rendering può avvenire sul dispositivo endpoint o sul server di hosting.
- **Compressione adattiva**: la compressione adattiva consente di fornire display multimediali avanzati su connessioni di rete thin. HDX valuta innanzitutto diverse variabili, ad esempio il tipo di input, dispositivo e visualizzazione (testo, video, voce e multimediale). Sceglie il codec di compressione ottimale e la migliore percentuale di utilizzo della CPU e della GPU. Si adatta quindi in modo intelligente in base a ogni singolo utente e base. Questo adattamento intelligente è utente per utente o anche sessione per sessione.



- **Deduplicazione dei dati**: la deduplicazione del traffico di rete riduce i dati aggregati inviati tra client e server. Lo fa sfruttando i modelli ripetuti in dati comunemente accessibili come immagini bitmap, documenti, processi di stampa e dati multimediali in streaming. La memorizzazione nella cache di questi modelli consente di trasmettere solo le modifiche attraverso la rete, eliminando il traffico duplicato. HDX supporta anche il multicasting di flussi multimediali, in cui una singola trasmissione dalla sorgente viene visualizzata da più abbonati in un'unica posizione, piuttosto che utilizzare una connessione individuale per ogni utente.

Per ulteriori informazioni, vedere Aumentare la produttività con un'area di lavoro utente ad alta definizione.

Nel dispositivo

HDX utilizza la capacità di elaborazione dei dispositivi utente per migliorare e ottimizzare l'esperienza utente. La tecnologia HDX garantisce agli utenti un'esperienza fluida e senza interruzioni con contenuti multimediali nei loro desktop o applicazioni virtuali. Il controllo dell'area di lavoro consente agli utenti di mettere in pausa i desktop e le applicazioni virtuali e di riprendere a lavorare da un dispositivo diverso nel punto in cui si erano interrotti.

Sulla rete

HDX incorpora funzionalità avanzate di ottimizzazione e accelerazione per offrire le migliori prestazioni su qualsiasi rete, incluse le connessioni WAN a bassa larghezza di banda e ad alta latenza.

Le funzioni HDX si adattano ai cambiamenti dell'ambiente. Le caratteristiche mantengono un equilibrio fra prestazioni e larghezza di banda. Applicano le migliori tecnologie per ogni scenario utente, indipendentemente dal fatto che l'accesso al desktop o l'applicazione venga effettuato localmente sulla rete aziendale o in remoto dall'esterno del firewall aziendale.

Nel centro dati

HDX utilizza la potenza di elaborazione e la scalabilità dei server per offrire prestazioni grafiche avanzate, indipendentemente dalle funzionalità dei dispositivi client.

Il monitoraggio dei canali HDX fornito da Citrix Director visualizza lo stato dei canali HDX collegati sui dispositivi utente.

HDX Insight

HDX Insight è l'integrazione di NetScaler Network Inspector e Performance Manager con Director. Acquisisce i dati sul traffico ICA e fornisce una panoramica dei dettagli storici e in tempo reale. Questi dati includono la latenza della sessione ICA lato client e lato server, l'uso della larghezza di banda dei canali ICA e il valore temporale di andata e ritorno ICA di ogni sessione.

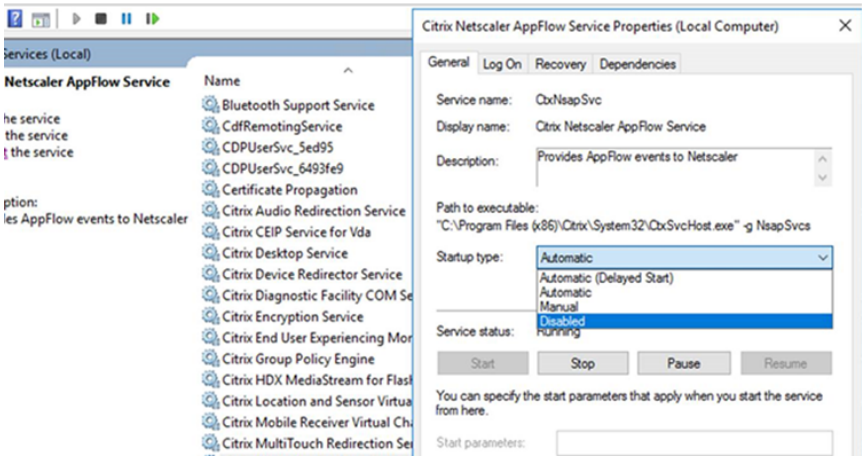
È possibile consentire a NetScaler di utilizzare il canale virtuale HDX Insight per spostare tutti i punti dati richiesti in un formato non compresso. Se si disattiva questa funzione, il dispositivo NetScaler decrittografa e decomprime il traffico ICA diffuso su vari canali virtuali. L'utilizzo del singolo canale virtuale riduce la complessità, migliora la scalabilità ed è più conveniente.

Requisiti minimi:

- Citrix Virtual Apps and Desktops 7 v1808
- XenApp e XenDesktop 7.17
- NetScaler versione 12.0 Build 57.x
- App Citrix Workspace per Windows 1808
- Citrix Receiver per Windows 4.10
- App Citrix Workspace per Mac 1808
- Citrix Receiver per Mac 12.8

Attivare o disattivare il canale virtuale HDX Insight

Per disattivare questa funzione, impostare le proprietà del servizio Citrix NetScaler Application Flow su Disabilitato. Per attivarla, impostare il servizio su Automatico. In entrambi i casi, si consiglia di riavviare il server dopo aver modificato queste proprietà. Per impostazione predefinita, questo servizio è abilitato (Automatico).



Sperimentare le funzionalità HDX dal proprio desktop virtuale

- Per vedere come il reindirizzamento dei contenuti del browser, una delle quattro tecnologie di reindirizzamento multimediale HDX, accelera la distribuzione di contenuti multimediali HTML5 e WebRTC:

  1. Scaricare l'estensione del browser Chrome e installarla sul desktop virtuale.
  2. Per scoprire come il reindirizzamento dei contenuti del browser accelera la distribuzione di contenuti multimediali ai desktop virtuali, è possibile visualizzare un video sul desktop da un sito Web contenente video HTML5, come YouTube. Gli utenti non sanno quando è in esecuzione il reindirizzamento dei contenuti del browser. Per verificare se è in uso il reindirizzamento del contenuto del browser, trascinare rapidamente la finestra del browser. Verrà visualizzato un ritardo o un fuori quadro tra il riquadro di visualizzazione e l'interfaccia utente. È inoltre possibile fare clic con il pulsante destro del mouse sulla pagina Web e cercare **Informazioni su HDX Browser Redirection** nel menu.

- Per vedere come HDX fornisce l'audio ad alta definizione:

  1. Configurare il client Citrix per la massima qualità audio; vedere la documentazione dell'app Citrix Workspace per i dettagli.
  2. Riprodurre file musicali utilizzando un lettore audio digitale (ad esempio iTunes) sul desktop.

HDX offre un'esperienza grafica e video superiore per la maggior parte degli utenti per impostazione predefinita e la configurazione non è necessaria. Le impostazioni dei criteri Citrix che offrono la migliore esperienza per la maggior parte dei casi d'uso sono abilitate per impostazione predefinita.

- HDX seleziona automaticamente il metodo di consegna migliore in base al client, alla piattaforma, all'applicazione e alla larghezza di banda della rete, per poi eseguire l'ottimizzazione automatica in base alle condizioni che cambiano.
- HDX ottimizza le prestazioni di grafica e video 2D e 3D.
- HDX consente ai dispositivi utente di trasmettere file multimediali direttamente dal provider di origine su Internet o Intranet, anziché tramite il server host. Se i requisiti per il recupero dei contenuti sul lato client non vengono soddisfatti, la distribuzione dei contenuti multimediali effettua il fallback sul recupero dei contenuti sul lato server e sul reindirizzamento multimediale. In genere, non è necessario modificare i criteri delle funzionalità di reindirizzamento multimediale.
- HDX offre contenuti video avanzati con rendering via server ai desktop virtuali quando non è disponibile il reindirizzamento multimediale: visualizzare un video su un sito Web contenente video ad alta definizione, quale http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.

Buono a sapersi:

- Per informazioni sul supporto e sui requisiti per le funzionalità HDX, vedere l'articolo Requisiti di sistema. Salvo diversamente indicato, le funzionalità HDX sono disponibili per i computer con il sistema operativo Windows multi-sessione e a sessione singola supportati, oltre ai desktop Accesso remoto PC.
- Questo contenuto descrive come ottimizzare l'esperienza utente, migliorare la scalabilità del server o ridurre i requisiti di larghezza di banda. Per informazioni sull'utilizzo dei criteri e delle impostazioni dei criteri Citrix, vedere la documentazione dei criteri Citrix relativa a questa versione.
- Per istruzioni che includono la modifica del Registro di sistema, procedere con cautela: la modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Riconnessione automatica del client e affidabilità della sessione

Quando si accede ad applicazioni o desktop ospitati, potrebbe verificarsi un'interruzione della rete. Per godere di una riconnessione più fluida, offriamo la riconnessione automatica del client e l'affid-

abilità della sessione. In una configurazione predefinita, viene prima avviata l'affidabilità della sessione e quindi segue la riconnessione automatica del client.

Riconnessione automatica del client:

La riconnessione automatica del client riavvia il motore client per riconnettersi a una sessione disconnessa. La riconnessione automatica del client chiude (o disconnette) la sessione utente dopo il tempo specificato nella relativa impostazione. Se è in corso la riconnessione automatica del client, il sistema invia all'utente una notifica di interruzione della rete per le applicazioni e i desktop nel modo seguente:

- **Desktop.** La finestra della sessione è disattivata e un conto alla rovescia mostra il tempo che manca alla riconnessione.
- **Applicazioni.** La finestra della sessione si chiude e viene visualizzata una finestra di dialogo contenente un conto alla rovescia che mostra il tempo che manca al tentativo di riconnessione.

Durante la riconnessione automatica del client, le sessioni si riavviano in attesa della connettività di rete. L'utente non può interagire con le sessioni mentre è in corso la riconnessione automatica del client.

Durante la riconnessione, le sessioni disconnesse si riconnettono utilizzando le informazioni di connessione salvate. L'utente può interagire normalmente con le applicazioni e i desktop.

Impostazioni predefinite di riconnessione automatica del client:

- Timeout di riconnessione automatica del client: 120 secondi
- Riconnessione automatica del client: abilitata
- Autenticazione di riconnessione automatica del client: disattivata
- Registrazione della riconnessione automatica del client: disabilitata

Per ulteriori informazioni, vedere Impostazioni dei criteri di riconnessione automatica del client.

Affidabilità della sessione:

L'affidabilità della sessione riconnette le sessioni ICA senza problemi durante le interruzioni di rete. L'affidabilità della sessione chiude (o disconnette) la sessione utente dopo il tempo specificato nell'impostazione. Dopo il timeout dell'affidabilità della sessione, avranno effetto le impostazioni di riconnessione automatica del client, tentando di riconnettere l'utente alla sessione disconnessa. Quando l'affidabilità della sessione è in corso, la notifica di interruzione della rete delle applicazioni e dei desktop viene inviata all'utente come segue:

- **Desktop.** La finestra della sessione diventa trasparente e un conto alla rovescia visualizza il tempo che manca alle riconnessioni.
- **Applicazioni.** La finestra diventa trasparente, così come le finestre a comparsa interrotte dalla connessione dall'area di notifica.

Mentre l'affidabilità della sessione è attiva, l'utente non può interagire con le sessioni ICA. Tuttavia, le azioni dell'utente quali le sequenze di tasti vengono memorizzate nel buffer per pochi secondi immediatamente dopo l'interruzione della rete e vengono ritrasmesse quando la rete è disponibile.

Al momento della riconnessione, il client e il server riprendono dallo stesso punto in cui si trovavano nel loro scambio di protocollo. Le finestre di sessione perdono la trasparenza e vengono visualizzate le finestre a comparsa appropriate dell'area di notifica per le applicazioni.

Impostazioni predefinite dell'affidabilità della sessione

- Timeout dell'affidabilità della sessione: 180 secondi
- Livello di opacità dell'interfaccia utente di riconnessione: 80%
- Connessione all'affidabilità della sessione: abilitata
- Numero di porta dell'affidabilità della sessione: 2598

Per ulteriori informazioni, vedere Impostazioni dei criteri di affidabilità delle sessioni.

NetScaler con riconnessione automatica del client e affidabilità della sessione:

Se i criteri Multistream e Multiport sono attivati sul server e una o tutte queste condizioni sono vere, la riconnessione automatica del client non funziona:

- L'affidabilità della sessione è disabilitata su NetScaler Gateway.
- Si verifica un failover sull'appliance NetScaler.
- NetScaler SD-WAN viene utilizzato con NetScaler Gateway.

Velocità effettiva adattiva di HDX

La velocità effettiva adattiva di HDX consente di ottimizzare in modo intelligente la velocità di picco della sessione ICA regolando i buffer di output. Il numero di buffer di output viene inizialmente impostato su un valore elevato. Questo valore elevato consente di trasmettere i dati al client in modo più rapido ed efficiente, soprattutto nelle reti ad alta latenza. Fornire una migliore interattività, trasferimenti di file più rapidi, riproduzione video più fluida, frequenza di aggiornamento e risoluzione più elevate si traduce in un'esperienza utente migliorata.

L'interattività della sessione viene costantemente misurata per determinare se qualsiasi flusso di dati all'interno della sessione ICA influisce negativamente sull'interattività. In tal caso, la velocità effettiva viene ridotta per ridurre l'impatto sulla sessione del flusso di dati di grandi dimensioni e consentire il ripristino dell'interattività.

> **Importante:**
>
> La velocità effettiva adattiva di HDX modifica il modo in cui vengono impostati i buffer di out-

> put spostando questo meccanismo dal client alla VDA e non è necessaria alcuna configurazione manuale.

Questa funzione ha i seguenti requisiti:

- VDA versione 1811 o successiva
- App Workspace per Windows 1811 o versione successiva

Migliorare la qualità dell'immagine inviata ai dispositivi utente

Le seguenti impostazioni dei criteri di visualizzazione visiva controllano la qualità delle immagini inviate dai desktop virtuali ai dispositivi utente.

- Qualità visiva. Controlla la qualità visiva delle immagini visualizzate sul dispositivo utente: media, alta, sempre senza perdite, compila per senza perdite (impostazione predefinita= media). La qualità video effettiva mediante l'impostazione predefinita del supporto dipende dalla larghezza di banda disponibile.
- Frequenza di aggiornamento target. Specifica il numero massimo di fotogrammi al secondo inviati dal desktop virtuale al dispositivo utente (impostazione predefinita= 30). Per i dispositivi con CPU più lente, specificando un valore inferiore, si può migliorare l'esperienza utente. La massima frequenza di fotogrammi supportata al secondo è 60.
- Limite di memoria di visualizzazione. Specifica la dimensione massima del buffer video per la sessione in kilobyte (impostazione predefinita= 65536 KB). Per le connessioni che richiedono una maggiore profondità di colore e una risoluzione più elevata, aumentare il limite. È possibile calcolare la memoria massima richiesta.

Migliorare le prestazioni delle videoconferenze

Moltre delle applicazioni per videoconferenze più diffuse sono ottimizzate per la distribuzione da Citrix Virtual Apps and Desktops attraverso il reindirizzamento multimediale (vedere, ad esempio, HDX RealTime Optimization Pack). Per le applicazioni non ottimizzate, la compressione video HDX della webcam migliora l'efficienza della larghezza di banda e la tolleranza alla latenza per le webcam durante le videoconferenze in una sessione. Questa tecnologia trasmette il traffico delle webcam su un canale virtuale multimediale dedicato. Questa tecnologia utilizza meno larghezza di banda rispetto al supporto isocrono HDX Plug-n-Play USB per il reindirizzamento e funziona bene sulle connessioni WAN.

Gli utenti dell'app Citrix Workspace possono ignorare il comportamento predefinito scegliendo l'impostazione Mic & Webcam (Microfono e webcam) di Desktop Viewer **Don't use my microphone or webcam** (Non utilizzare il microfono e la webcam). Per impedire agli utenti di modificare la compressione video HDX della webcam, disabilitare il reindirizzamento dei dispositivi USB utilizzando le

impostazioni dei criteri in ICA policy settings (Impostazioni criteri ICA) > USB Devices policy (Criteri dispositivi USB).

La compressione video HDX della webcam richiede che siano abilitate le seguenti impostazioni dei criteri (sono tutte abilitate per impostazione predefinita).

- Client audio redirection (Reindirizzamento audio client)
- Client microphone redirection (Reindirizzamento microfono client)
- Multimedia conferencing (Conferenze multimediali)

Se una webcam supporta la codifica hardware, la compressione video HDX utilizza la codifica hardware per impostazione predefinita. La codifica hardware potrebbe consumare più larghezza di banda rispetto alla codifica software. Per forzare la compressione del software, aggiungere il seguente valore di chiave DWORD alla chiave del Registro di sistema: HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1.

Priorità relative al traffico di rete

Vengono assegnate priorità al traffico di rete tra più connessioni per una sessione utilizzando router supportati da Quality of Service. Quattro flussi TCP e due flussi UDP (User Datagram Protocol) sono disponibili per trasportare il traffico ICA tra il dispositivo utente e il server:

- Flussi TCP: in tempo reale, interattivi, in background e in blocco
- Flussi UDP: comunicazione remota display Framehawk e voce

Ogni canale virtuale è associato a una priorità specifica e trasportato nella connessione corrispondente. È possibile impostare i canali in modo indipendente, in base al numero della porta TCP utilizzata per la connessione.

Le connessioni in streaming a più canali sono supportate per gli agenti di distribuzione virtuali (VDA) installati su computer Windows 10, Windows 8 e Windows 7. Collaborare con l'amministratore di rete per assicurarsi che le porte CGP (Common Gateway Protocol) configurate nell'impostazione Criterio multi-porta siano assegnate correttamente ai router di rete.

La qualità del servizio è supportata solo quando sono configurate più porte di affidabilità della sessione o le porte CGP.

> **Avviso:**
>
> Utilizzare la sicurezza di trasporto quando si utilizza questa funzione. Citrix consiglia di utilizzare IPsec (Internet Protocol Security) o TLS (Transport Layer Security). Le connessioni TLS sono supportate solo quando le connessioni attraversano un NetScaler Gateway che supporta ICA multi-flusso. In una rete aziendale interna, le connessioni multi-flusso con TLS non sono supportate.

Per impostare la qualità del servizio per più connessioni in streaming, aggiungere le seguenti impostazioni dei criteri Citrix a un criterio (vedere Impostazioni dei criteri delle connessioni multi-flusso per i dettagli):

- Criterio multi-porta: questa impostazione specifica le porte per il traffico ICA tra più connessioni e stabilisce le priorità della rete.
  - Selezionare una priorità dall'elenco delle priorità per la porta predefinita CGP. Per impostazione predefinita, la porta primaria (2598) ha una priorità alta.
  - Digitare più porte CGP in CGP port1, CGP port2, and CGP port3 in base alle esigenze e identificare le priorità per ciascuna. Ogni porta deve avere una priorità univoca.

  Configurare in modo esplicito i firewall sui VDA per consentire il traffico TCP aggiuntivo.
- Impostazione computer multi-flusso: questa impostazione è disabilitata per impostazione predefinita. Se si utilizza Citrix NetScaler SD-WAN con supporto multi-flusso nell'ambiente, non è necessario configurare questa impostazione. Configurare questa impostazione dei criteri quando si utilizzano router di terze parti o SD-WAN NetScaler legacy per ottenere la qualità del servizio desiderata.
- Impostazione utente multi-flusso: questa impostazione è disabilitata per impostazione predefinita.

Perché i criteri contenenti queste impostazioni abbiano effetto, gli utenti devono scollegarsi e quindi accedere alla rete.

Visualizzare o nascondere la barra della lingua remota

La barra della lingua visualizza la lingua di input preferita in una sessione dell'applicazione. Se questa funzione è abilitata (impostazione predefinita), è possibile mostrare o nascondere la barra della lingua dall'interfaccia utente **Preferenze avanzate > Barra della lingua** nell'app Citrix Workspace per Windows. Utilizzando un'impostazione del Registro di sistema sul lato VDA, è possibile disattivare il controllo client della funzionalità barra della lingua. Se questa funzionalità è disabilitata, l'impostazione dell'interfaccia utente client non ha effetto e l'impostazione corrente per utente determina lo stato della barra della lingua. Per ulteriori informazioni, vedere Migliorare l'esperienza utente.

Per disabilitare il controllo client della funzionalità barra della lingua dal VDA:

1. Nell'editor del Registro di sistema passare a HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cit
2. Creare una chiave valore DWORD, SeamlessFlags, e impostarla su 0x40000.

Mappatura tastiera Unicode

Le versioni non Windows di Citrix Receiver utilizzano il layout di tastiera locale (Unicode). Se un utente modifica il layout della tastiera locale e il layout della tastiera del server (codice di scansione), questi potrebbero non essere sincronizzati e l'output potrebbe non essere corretto. Ad esempio, Utente1 modifica il layout di tastiera locale da inglese a tedesco. Utente1 cambia quindi la tastiera lato server scegliendo il layout tedesco. Anche se entrambi i layout di tastiera sono tedeschi, potrebbero non essere sincronizzati causando un output di caratteri errati.

Abilitare o disabilitare il mapping del layout di tastiera Unicode

Per impostazione predefinita, la funzionalità è disabilitata sul lato VDA. Per abilitare la funzionalità, attivarla utilizzando l'editor del Registro di sistema regedit sul VDA. Aggiungere la seguente chiave del Registro di sistema:

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: EnableKlMap

Tipo: DWORD

Valore: 1

Per disattivare questa funzione, impostare **EnableKlMap** su 0 o eliminare la chiave **CtxKlMap**.

Abilitare la modalità compatibile con la mappatura del layout della tastiera Unicode

Per impostazione predefinita, la mappatura del layout di tastiera Unicode effettua automaticamente l'hook di alcune API di Windows per ricaricare la nuova mappa del layout di tastiera Unicode quando si modifica il layout di tastiera sul lato server. Alcune applicazioni non consentono di effettuare l'hook. Per mantenere la compatibilità, è possibile modificare la funzionalità in modalità compatibile per supportare queste applicazioni non collegate con l'hook. Aggiungere la seguente chiave del Registro di sistema:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: DisableWindowHook

Tipo: DWORD

Valore: 1

Per utilizzare la normale mappatura del layout di tastiera Unicode, impostare **DisableWindowHook** su 0.

Canali virtuali Citrix ICA

January 7, 2024

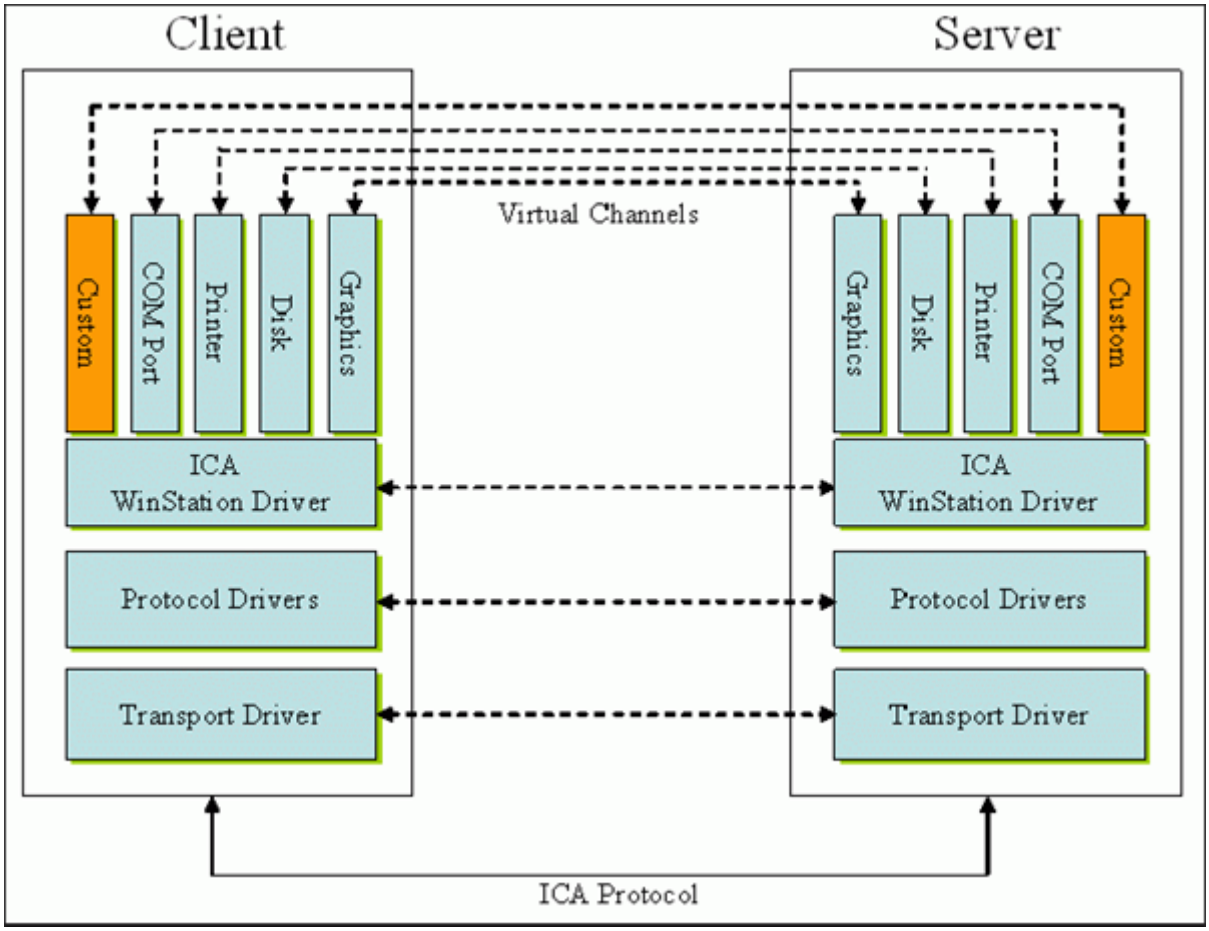
> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Cosa sono i canali virtuali ICA?

Gran parte delle funzionalità e della comunicazione tra l'app Citrix Workspace e i server Citrix Virtual Apps and Desktops avviene su canali virtuali. I canali virtuali sono una parte necessaria dell'esperienza di elaborazione remota con i server Citrix Virtual Apps and Desktops. I canali virtuali sono utilizzati per:

- Audio
- Porte COM
- Dischi
- Grafica
- Porte LPT
- Stampanti
- Smart card
- Canali virtuali personalizzati di terze parti
- Video

A volte vengono rilasciati nuovi canali virtuali con le nuove versioni dei server Citrix Virtual Apps and Desktops e dei prodotti app Citrix Workspace per fornire maggiori funzionalità.



Un canale virtuale è costituito da un driver virtuale lato client che comunica con un'applicazione lato server. Citrix Virtual Apps and Desktops viene fornito con vari canali virtuali inclusi. Sono progettati per consentire a clienti e fornitori terzi di creare i propri canali virtuali utilizzando uno dei kit di sviluppo software (SDK) in dotazione.

I canali virtuali offrono un modo sicuro per svolgere varie attività. Ad esempio, un'applicazione in esecuzione su un server Citrix Virtual Apps che comunica con un dispositivo lato client o un'applicazione che comunica con l'ambiente lato client.

Sul lato client, i canali virtuali corrispondono a driver virtuali. Ogni driver virtuale fornisce una funzione specifica. Alcuni sono necessari per il normale funzionamento, mentre altri sono facoltativi. I driver virtuali operano a livello di protocollo sul livello di presentazione. Ci possono essere diversi protocolli attivi in qualsiasi momento tramite canali multiplexing forniti dal livello di protocollo Windows Station (WinStation).

Le seguenti funzioni sono contenute nel valore del Registro di sistema VirtualDriver in questo percorso del Registro di sistema:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\
Advanced\Modules\ICA 3.0
```


oppure

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0` (per 64 bit)

- Thinwire3.0 (obbligatorio)
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- Appunti
- ClientComm
- ClientAudio
- LicenseHandler (obbligatorio)
- TWI (obbligatorio)
- SmartCard
- ICACTL (obbligatorio)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> **Nota:**
>
> È possibile disattivare funzionalità client specifiche rimuovendo uno o più di questi valori dalla chiave del Registro di sistema. Ad esempio, se si desidera rimuovere gli Appunti client, rimuovere la parola **Appunti**.

Questo elenco contiene i file dei driver virtuali client e le rispettive funzioni. Citrix Virtual Apps e l'app Citrix Workspace per Windows utilizzano questi file. Sono sotto forma di librerie di collegamento dinamico (modalità utente) e non di driver Windows (modalità kernel) ad eccezione di USB generico come descritto nel canale virtuale USB generico.

- vd3dn.dll: canale virtuale Direct3D utilizzato per il reindirizzamento della composizione desktop
- vdcamN.dll: audio bidirezionale
- vdcdm30n.dll: mappatura unità client
- vdcom30N.dll: mappatura porta COM client
- vdcpm30N.dll: mappatura stampante client
- vdctln.dll: canale dei controlli ICA
- vddvc0n.dll: canale virtuale dinamico
- vdeuemn.dll: monitoraggio dell'esperienza utente finale
- vdgusbn.dll: canale virtuale USB generico
- vdkbhook.dll: pass-through della chiave trasparente

- vdlfpn.dll: canale di visualizzazione Framehawk su trasporto simil-UDP
- vdmmn.dll: supporto multimediale
- vdmrvc.dll: canale virtuale di Receiver mobile
- vdmtchn.dll: supporto multi-touch
- vdscardn.dll: supporto delle smartcard
- vdsens.dll: canale virtuale dei sensori
- vdspl30n.dll: UPD client
- vdsspin.dll: Kerberos
- vdtuin.dll: interfaccia utente trasparente
- vdtw30n.dll: client Thinwire
- vdtwin.dll: Seamless
- vdtwn.dll: Twain

Alcuni canali virtuali sono compilati in altri file. Ad esempio, la mappatura degli Appunti è disponibile in wfica32.exe

Compatibilità con 64 bit

L'app Citrix Workspace per Windows è compatibile con 64 bit. Come avviene per la maggior parte dei file binari compilati per 32 bit, questi file client hanno equivalenti compilati a 64 bit:

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

Canale virtuale USB generico

L'implementazione del canale virtuale USB generico utilizza due driver in modalità kernel insieme al driver del canale virtuale vdgusbn.dll:

- ctxusbm.sys
- ctxusbr.sys

Come funzionano i canali virtuali ICA

I canali virtuali vengono caricati in più modi. La Shell (WfShell per il server e PicaShell per la workstation) carica alcuni canali virtuali. Alcuni canali virtuali sono ospitati come servizi Windows.

Moduli di canale virtuale caricati dalla Shell, ad esempio:

- EUEM
- Twain
- Appunti
- Contenuti multimediali
- Condivisione delle sessioni Seamless
- Fuso orario

Alcuni sono caricati come modalità kernel, ad esempio:

- CtxDvcs.sys: canale virtuale dinamico
- Icausbb.sys: reindirizzamento USB generico
- Picadm.sys: mappatura dell'unità client
- Picaser.sys: reindirizzamento porta COM
- Picapar.sys: reindirizzamento porta LPT

Canale virtuale grafico sul lato server

A partire da XenApp 7.0 e XenDesktop7.0, `ctxgfx.exe` ospita il canale virtuale grafico per le sessioni basate su workstation e server terminal. `Ctxgfx` ospita moduli specifici della piattaforma che interagiscono con il driver corrispondente (`Icardd.dll` per RDSH e `vdod.dll` e `vidd.dll` per workstation).

Per le distribuzioni di XenDesktop 3D Pro è installato un driver di grafica OEM per la GPU corrispondente sul VDA. `Ctxgfx` carica moduli adattatori specializzati per interagire con il driver grafico OEM.

Hosting di canali specializzati nei servizi di Windows

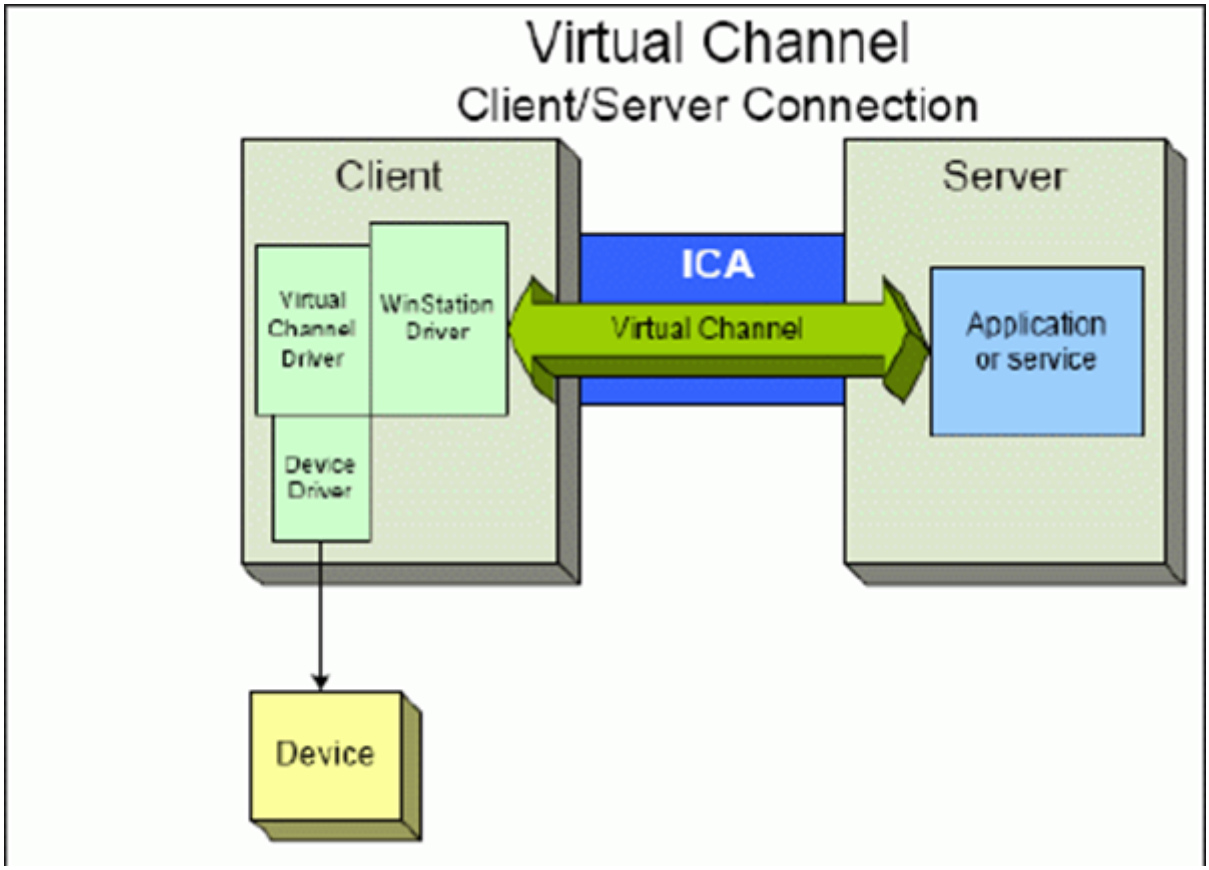
Sui server di Citrix Virtual Apps and Desktops, vari canali sono ospitati come servizi Windows. Tale hosting fornisce semantica da uno a molti per più applicazioni in una sessione e più sessioni sul server. Esempi di tali servizi sono:

- Servizio di redirector periferiche Citrix
- Servizio di canale virtuale dinamico Citrix
- Servizio di monitoraggio dell'esperienza utente finale Citrix

- Servizio canale virtuale di posizione e sensore Citrix
- Servizio di reindirizzamento Citrix MultiTouch
- Servizio Citrix Print Manager
- Servizio smartcard Citrix
- Servizio di reindirizzamento audio Citrix (solo Citrix Virtual Desktops)

Il canale audio virtuale su Citrix Virtual Apps è ospitato utilizzando il servizio Windows Audio.

Sul lato server, tutti i canali virtuali client vengono instradati tramite il driver WinStation, Wdica.sys. Sul lato client, il driver WinStation corrispondente, incorporato in wfica32.exe, esegue il polling dei canali virtuali del client. Questa immagine illustra la connessione client-server del canale virtuale.



Questa panoramica contiene uno scambio di dati client-server che utilizza un canale virtuale.

1. Il client si connette al server di Citrix Virtual Apps and Desktops. Il client passa informazioni sui canali virtuali che supporta al server.
2. L'applicazione lato server viene avviata, ottiene un handle per il canale virtuale e, facoltativamente, interroga per ottenere ulteriori informazioni sul canale.
3. Il driver virtuale client e l'applicazione lato server passano i dati utilizzando i due metodi seguenti:

- Se l'applicazione server dispone di dati da inviare al client, i dati vengono inviati immediatamente al client. Quando il client riceve i dati, il driver WinStation effettua il de-multiplex dei dati del canale virtuale provenienti dal flusso ICA e li passa immediatamente al driver virtuale client.
- Se il driver virtuale client dispone di dati da inviare al server, i dati vengono inviati alla successiva esecuzione del polling del driver WinStation. Quando il server riceve i dati, questi vengono messi in coda fino a quando l'applicazione del canale virtuale non li legge. Non c'è modo di avvisare l'applicazione del canale virtuale del server che i dati sono stati ricevuti.

4. Una volta completata l'applicazione del canale virtuale del server, chiude il canale virtuale e libera tutte le risorse eventualmente allocate.

Creazione di un canale virtuale personalizzato utilizzando Virtual Channel SDK

> **Nota:**
>
> Gli SDK Citrix sono disponibili nel portale per sviluppatori Citrix all'indirizzo https://developer.cloud.com.

La creazione di un canale virtuale mediante Virtual Channel SDK richiede conoscenze di programmazione di livello intermedio. Utilizzare questo metodo per fornire un percorso di comunicazione principale tra il client e il server. Ad esempio, se si sta implementando l'utilizzo di un dispositivo sul lato client, ad esempio uno scanner, da utilizzare con un processo nella sessione.

> **Nota:**
>
> - L'SDK Virtual Channel richiede l'SDK WFAPI per scrivere il lato server del canale virtuale.
> - Per via della sicurezza avanzata per Citrix Virtual Apps and Desktops, è necessario specificare quali canali virtuali possono essere aperti in una sessione ICA. Per ulteriori informazioni, vedere Impostazione dei criteri Virtual channel allow list (Elenco di elementi consentiti del canale virtuale).

Creazione di un proprio canale virtuale utilizzando l'SDK ICA Client Object

Creare un canale virtuale utilizzando l'ICO (ICA Client Object) è più semplice rispetto all'utilizzo di Virtual Channel SDK. Utilizzare l'ICO creando un oggetto con nome nel programma utilizzando il metodo **CreateChannels**.

> **Importante:**
>
> A causa della sicurezza avanzata a partire dalla versione 10.00 di Citrix Receiver per Windows e

> versioni successive (e le app Citrix Workspace per Windows), è necessario eseguire un ulteriore passo durante la creazione di un canale virtuale ICO.

Funzionalità pass-through dei canali virtuali

La maggior parte dei canali virtuali forniti da Citrix funziona senza modifiche quando si utilizza l'app Citrix Workspace per Windows all'interno di una sessione ICA (nota anche come sessione pass-through). Ci sono aspetti da considerare quando si utilizza il client in hop extra.

Le seguenti funzioni funzionano allo stesso modo in hop singolo o multiplo:

- Mappatura porta COM client
- Mappatura unità client
- Mappatura stampante client
- UPD client
- Monitoraggio dell'esperienza utente finale
- USB generico
- Kerberos
- Supporto multimediale
- Supporto smartcard
- Pass-through della chiave trasparente
- Twain

Poiché la natura intrinseca della latenza e di fattori quali compressione, decompressione e rendering eseguiti a ogni hop, le prestazioni potrebbero essere influenzate da ogni hop aggiuntivo sottoposto al client. Le aree di influenza sono:

- Audio bidirezionale
- Trasferimenti di file
- Reindirizzamento USB generico
- Seamless
- Thinwire

> **Importante:**
>
> Per impostazione predefinita, le unità client mappate da un'istanza del client in esecuzione in una sessione pass-through sono limitate alle unità client del client di connessione.

Funzionalità pass-through dei canali virtuali tra una sessione di Citrix Virtual Desktop e una sessione di Citrix Virtual App

La maggior parte dei canali virtuali forniti da Citrix funziona senza modifiche quando si utilizza l'app Citrix Workspace per Windows all'interno di una sessione ICA su un server Citrix Virtual Desktops (noto

anche come sessione pass-through).

In particolare, sul server Citrix Virtual Desktops, è presente un hook VDA che esegue **picaPassthruHook**. Questo hook fa credere al client di essere in esecuzione su un server CPS e posiziona il client nella sua tradizionale modalità pass-through.

Supportiamo i seguenti canali virtuali tradizionali e le loro funzionalità:

- Client
- Mappatura porta COM client
- Mappatura unità client
- Mappatura stampante client
- USB generico (limitato a causa delle prestazioni)
- Supporto multimediale
- Supporto smartcard
- SSON
- Pass-through della chiave trasparente

Sicurezza e canali virtuali ICA

La protezione dell'utilizzo è una parte importante della pianificazione, dello sviluppo e dell'implementazione di canali virtuali. Questo documento fa riferimento a specifiche aree di sicurezza in molte sue parti.

Procedure consigliate

Aprire i canali virtuali quando ci si **connette** e ci si **riconnette**. Chiudere i canali virtuali quando ci si scollega e ci si **disconnette**.

Tenere presenti le seguenti linee guida quando si creano script che utilizzano le funzioni del canale virtuale.

Denominazione dei canali virtuali:

È possibile creare un massimo di 32 canali virtuali. Diciassette canali su 32 sono riservati per scopi speciali.

- I nomi dei canali virtuali non devono contenere più di sette caratteri.
- I primi tre caratteri sono riservati al nome del fornitore e i quattro successivi al tipo di canale. Ad esempio, **CTXAUD** rappresenta il canale audio virtuale Citrix.

I canali virtuali sono indicati da un nome ASCII di sette caratteri (o più breve). In alcune versioni precedenti del protocollo ICA, i canali virtuali erano numerati. I numeri vengono ora assegnati dinamicamente in base al nome ASCII, rendendo più facile l'implementazione. Gli utenti che stanno

sviluppando codice per canali virtuali solo per uso interno possono utilizzare qualsiasi nome di sette caratteri che non sia in conflitto con i canali virtuali esistenti. Utilizzare solo numeri e caratteri ASCII maiuscoli e minuscoli. Seguire la convenzione di denominazione esistente quando si aggiungono i propri canali virtuali. Ci sono diversi canali predefiniti. I canali predefiniti iniziano con l'identificatore OEM CTX e sono riservati all'uso da parte di Citrix.

Supporto a doppio hop:

Canale virtuale	Il doppio hop è supportato?
Audio	No
Browser Content Redirection	No
CDM	Sì
CEIP	No
Appunti	Sì
Continuum (MRVC)	No
VC di controllo	Sì
Reindirizzamento video HTML5 (v1)	Sì
Tastiera, mouse	Sì
MultiTouch	No
NSAPVC	No
Stampa	Sì
SensVC	No
Smartcard	Sì
Twain	Sì
VC USB	Sì
Dispositivi WAYCOM -K2M mediante VC USB	Sì
Compressione video della webcam	Sì
Reindirizzamento di Windows Media	Sì

Vedere anche

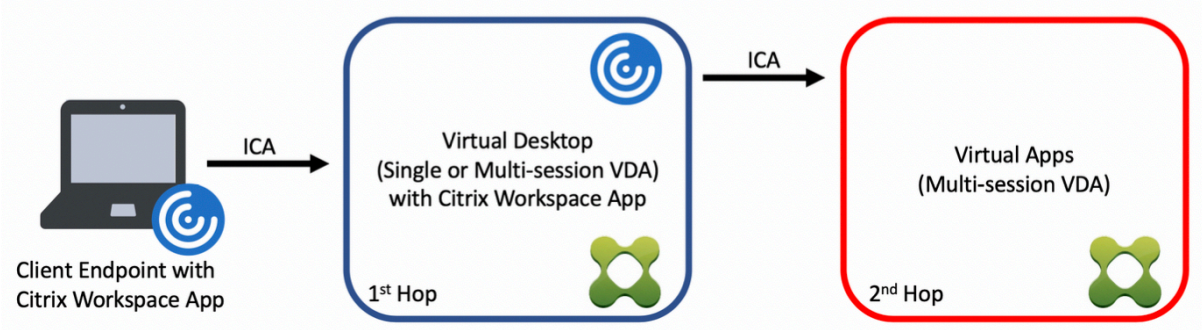
- SDK per il canale virtuale ICA
- Citrix Developer Network è la sede di tutte le risorse tecniche e le discussioni che riguardano l'utilizzo di SDK Citrix. In questa rete, è possibile trovare l'accesso a SDK, codice di esempio e

script, estensioni e plug-in e documentazione SDK. Sono inclusi anche i forum Citrix Developer Network, dove si svolgono discussioni tecniche su ciascuno degli SDK Citrix.

Doppio hop in Citrix Virtual Apps and Desktops

January 7, 2024

Nel contesto di una sessione client Citrix, il termine "doppio hop"si riferisce a una sessione di Citrix Virtual App in esecuzione all'interno di una sessione di Citrix Virtual Desktop. Il diagramma seguente illustra un doppio hop.



In uno scenario a doppio hop, si tratta di quando l'utente si connette a un Citrix Virtual Desktop in esecuzione su un sistema operativo VDA a sessione singola (noto come VDI) o un sistema operativo VDA multisessione (noto come desktop pubblicato), che è considerato il primo hop. Dopo che si connette al desktop virtuale, l'utente può avviare una sessione di Citrix Virtual Apps. Questo è considerato il secondo hop.

È possibile utilizzare un modello di distribuzione a doppio hop per supportare vari casi d'uso. Un esempio comune è il caso in cui gli ambienti Citrix Virtual Desktop e Citrix Virtual Apps sono gestiti da entità diverse. Questo metodo può anche essere efficace nella risoluzione dei problemi di compatibilità delle applicazioni.

Requisiti di sistema

Tutte le versioni di Citrix Virtual Apps and Desktops incluso il servizio Citrix Cloud supportano il doppio hop.

Il primo hop deve utilizzare una versione supportata del sistema operativo VDA a sessione singola o multisessione e dell'app Citrix Workspace. Il secondo hop deve utilizzare una versione supportata del sistema operativo multisessione VDA. Vedere la pagina Matrice dei prodotti per le versioni supportate.

Per ottenere prestazioni ottimali e compatibilità, Citrix consiglia di utilizzare un client Citrix della stessa versione o più recente rispetto alle versioni VDA in uso.

Negli ambienti in cui il primo hop comporta una soluzione desktop virtuale di terze parti (non Citrix) in combinazione con una sessione di Citrix Virtual Apps, il supporto è limitato all'ambiente Citrix Virtual Apps. In caso di problemi relativi al desktop virtuale di terze parti, tra cui, a titolo esemplificativo e non esaustivo, la compatibilità delle app Citrix Workspace, il reindirizzamento dei dispositivi hardware e le prestazioni delle sessioni, Citrix è in grado di fornire supporto tecnico a livello limitato. Per la risoluzione dei problemi potrebbe essere necessario un Citrix Virtual Desktop al primo hop.

Considerazioni sulla distribuzione per HDX in doppio hop

In generale, ogni sessione di un doppio hop è univoca e le funzioni client-server sono isolate in un dato hop. Questa sezione include aspetti che richiedono una particolare considerazione da parte degli amministratori di Citrix. Citrix consiglia ai clienti di eseguire test approfonditi delle funzionalità HDX necessarie per garantire che l'esperienza utente e le prestazioni siano adeguate per una determinata configurazione dell'ambiente.

Grafica

Utilizzare le impostazioni grafiche predefinite (codifica selettiva) per il primo e il secondo hop. Nel caso di HDX 3D Pro, Citrix consiglia vivamente che tutte le applicazioni che richiedono accelerazione grafica vengano eseguite localmente nel primo hop con le risorse GPU appropriate disponibili per il VDA.

Latenza

La latenza end-to-end può influire sull'esperienza utente complessiva. Considerare la latenza aggiunta tra il primo e il secondo hop. Ciò è particolarmente importante con il reindirizzamento dei dispositivi hardware.

Contenuti multimediali

Il rendering lato server (in sessione) dei contenuti audio e video funziona meglio nel primo hop. La riproduzione video nel secondo hop richiede la decodifica e la ricodifica al primo hop, aumentando così la larghezza di banda e l'utilizzo delle risorse hardware. I contenuti audio e video devono limitarsi al primo hop quando possibile.

Reindirizzamento dei dispositivi USB

HDX include modalità di reindirizzamento generiche e ottimizzate per supportare una vasta gamma di tipi di dispositivi USB. Prestare particolare attenzione alla modalità in uso ad ogni hop e utilizzare la seguente tabella come riferimento per ottenere i migliori risultati. Per ulteriori informazioni sulle modalità di reindirizzamento generiche e ottimizzate, vedere Dispositivi USB generici.

Primo hop (VDI o desktop pubblicato)	Secondo hop (app virtuali)	Note di supporto
Ottimizzato	Ottimizzato	Consigliato (in base al supporto del dispositivo). Ad esempio, memoria di massa USB, scanner TWAIN, Webcam, Audio.
Generico	Generico	Per i dispositivi in cui l'opzione ottimizzata non è disponibile.
Generico	Ottimizzato	Sebbene tecnicamente possibile, si consiglia di utilizzare la modalità ottimizzata su entrambi gli hop quando è disponibile il supporto del dispositivo.
Ottimizzato	Generico	Non supportato

> **Nota:**
>
> A causa della verbosità intrinseca dei protocolli USB, le prestazioni possono diminuire fra un hop e l'altro. Funzionalità e risultati variano a seconda dei requisiti specifici del dispositivo e dell'applicazione. I test di convalida sono altamente raccomandati in tutti i casi di reindirizzamento del dispositivo e risultano particolarmente importanti in scenari a doppio hop.

Eccezioni al supporto

Le sessioni a doppio hop supportano la maggior parte delle funzioni e funzionalità HDX, ad eccezione delle seguenti:

- Browser content redirection (Reindirizzamento del contenuto del browser)
- Accesso alle app locali
- RealTime Optimization Pack for Skype for Business
- Ottimizzazione di Microsoft Teams

Installazione e configurazione

April 3, 2024

Leggere gli articoli a cui si fa riferimento prima di avviare ciascuna fase di distribuzione per informazioni su ciò che viene visualizzato e specificato durante la distribuzione.

Utilizzare la sequenza seguente per distribuire Citrix Virtual Apps and Desktops.

Preparazione

Vedere Preparazione per l'installazione e completare tutte le attività necessarie.

- Dove trovare informazioni su concetti, caratteristiche, differenze rispetto alle versioni precedenti, requisiti di sistema e database.
- Aspetti da considerare quando si decide dove installare i componenti principali.
- Requisiti delle autorizzazioni e di Active Directory.
- Informazioni sui programmi di installazione, gli strumenti e le interfacce disponibili.

Installare i componenti principali

Installare Delivery Controller, Web Studio, Citrix Director e Citrix License Server. È inoltre possibile installare Citrix StoreFront. Per i dettagli, vedere Installare i componenti principali o Installare utilizzando la riga di comando.

Creare un sito

Dopo aver installato i componenti principali e aver avviato Studio, viene chiesto di creare un sito.

Installazione di uno o più Virtual Delivery Agent (VDA)

Installare un VDA su un computer che esegue un sistema operativo Windows, su un'immagine master o direttamente su ciascun computer. Vedere Installare i VDA o Installare utilizzando la riga di comando. Vengono forniti script di esempio se si desidera installare i VDA tramite Active Directory.

Per le macchine con sistema operativo Linux, segui le indicazioni fornite in Linux Virtual Delivery Agent.

Per una distribuzione di Accesso remoto PC, installare un VDA per il sistema operativo a sessione singola in ciascun PC dell'ufficio. Se si necessita solo dei servizi VDA principali, usare il programma di

installazione `VDAWorkstationCoreSetup.exe` autonomo e i metodi ESD (Electronic Software Distribution) esistenti (Preparazione per l'installazione descrive i programmi di installazione di VDA disponibili).

Installazione dei componenti opzionali

Se si prevede di utilizzare Citrix Universal Print Server, installare il componente server sui server di stampa. Vedere Installare i componenti principali o Installare utilizzando la riga di comando.

Per consentire a StoreFront di utilizzare opzioni di autenticazione come le asserzioni SAML, installare Citrix Federated Authentication Service.

Per consentire agli utenti finali di avere un maggiore controllo sui propri account utente, installare Reimpostazione password self-service.

Facoltativamente, è possibile integrare più componenti Citrix nella distribuzione di Citrix Virtual Apps and Desktops.

- Citrix Provisioning è un componente opzionale che esegue il provisioning delle macchine trasmettendo un'immagine master ai dispositivi di destinazione.
- Citrix Gateway è una soluzione sicura per l'accesso alle applicazioni che fornisce agli amministratori criteri e controlli di azione granulari a livello di applicazione per proteggere l'accesso alle applicazioni e ai dati.
- Citrix SD-WAN è un insieme di appliance che ottimizzano le prestazioni WAN.

Creare un catalogo di macchine

Dopo aver creato un sito in Studio, si viene guidati a creare un catalogo di macchine.

Un catalogo può contenere macchine fisiche o virtuali (VM). Le macchine virtuali possono essere create a partire da un'immagine master. Quando si utilizza un hypervisor o un altro servizio per fornire macchine virtuali, è innanzitutto necessario creare un'immagine master su tale host. Quindi, quando si crea il catalogo, si specifica tale immagine, che viene utilizzata durante la creazione di macchine virtuali.

Creare un gruppo di consegna

Dopo aver creato il primo catalogo di macchine in Web Studio, si viene guidati a creare un gruppo di consegna.

Un gruppo di consegna specifica quali utenti possono accedere ai computer in un catalogo selezionato e quali applicazioni sono disponibili per tali utenti.

Creare un gruppo di applicazioni (facoltativo)

Dopo aver creato un gruppo di consegna, si ha la possibilità di creare un gruppo di applicazioni. È possibile creare gruppi di applicazioni per applicazioni condivise tra gruppi di consegna diversi o utilizzate da un sottoinsieme di utenti all'interno di gruppi di consegna.

Identità macchina

January 7, 2024

Ciascuna macchina deve avere un'identità macchina univoca, nota anche come account computer. Le identità delle macchine possono essere create e gestite nelle macchine localmente o in una directory, ad esempio Active Directory (AD) on-premise o Azure AD. Citrix supporta l'hosting di applicazioni e desktop virtuali su macchine aggiunte ad Active Directory, ad Azure Active Directory, ad Azure Active Directory ibrido o non aggiunte a un dominio.

Tipi di identità delle macchine

Sono supportati i seguenti tipi di identità delle macchine.

Tipo di identità della macchina	Descrizione
Aggiunte ad AD	Le identità vengono create e gestite in Active Directory on-premise. Le macchine sottoposte a provisioning vengono aggiunte ad Active Directory on-premise utilizzando le identità delle macchine assegnate.
Aggiunto ad Azure AD ibrido	Le identità vengono create in Active Directory on-premise e vengono sincronizzate con Azure AD tramite Azure AD Connect. Le macchine sottoposte a provisioning vengono aggiunte ad Active Directory locale. Le macchine vengono quindi aggiunte ad Azure AD ibrido. Per l'importazione di una macchina virtuale aggiunta ad Azure AD ibrido, la macchina virtuale viene trattata da Citrix Virtual Apps and Desktops come se fosse aggiunta ad Active Directory.

Configurazioni supportate

Di seguito sono riportati i dettagli delle configurazioni supportate per ciascuno scenario.

Infrastruttura supportata

Identità della macchina	Citrix Virtual Apps and Desktops	Citrix Workspace	Citrix StoreFront	Citrix Gateway Service	Citrix Gateway
Aggiunte ad AD	Sì	Sì	Sì	Sì	Sì
Aggiunte ad Azure AD	No	Sì	No	Sì	No
Aggiunto ad Azure AD ibrido	Sì	Sì	Sì	Sì	Sì
Non aggiunte al dominio	No	Sì	No	Sì	No

Provider di autenticazione dell'identità per l'area di lavoro supportati

Identità della macchina	Azure Active Directory	Active Directory	Active Directory e token	Okta	SAML	Citrix Gateway	Autenticazione adattiva
Aggiunte ad AD	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Aggiunte ad Azure AD	Sì	No	No	No	No	No	No
Aggiunto ad Azure AD ibrido	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Non aggiunte al dominio	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Aggiunto a Active Directory

January 7, 2024

Active Directory è necessario per l'autenticazione e l'autorizzazione. L'infrastruttura Kerberos presente in Active Directory viene utilizzata per garantire l'autenticità e la riservatezza delle comunicazioni con i Delivery Controller. Per informazioni su Kerberos, vedere la documentazione di Microsoft.

Nell'articolo Requisiti di sistema sono elencati i livelli di funzionalità supportati per la foresta e il dominio. Per utilizzare la modellazione dei criteri, il Controller di dominio deve essere in esecuzione sul server da Windows Server 2003 a Windows Server 2012 R2. Questo non influisce sul livello di funzionalità del dominio.

Questo prodotto supporta:

- **Distribuzioni in cui gli account utente e gli account computer sono presenti nei domini in una singola foresta Active Directory.** Gli account utente e computer possono esistere in domini arbitrari all'interno di una singola foresta. In questo tipo di distribuzione sono supportati tutti i livelli di funzionalità del dominio e i livelli di funzionalità della foresta.
- **Distribuzioni in cui esistono account utente in una foresta di Active Directory diversa dalla foresta di Active Directory contenente gli account computer dei controller e dei desktop virtuali.** In questo tipo di distribuzione, i domini contenenti gli account Controller e computer desktop virtuale devono considerare attendibili i domini contenenti account utente. È possibile utilizzare trust tra foreste o trust esterni. In questo tipo di distribuzione sono supportati tutti i livelli di funzionalità del dominio e i livelli di funzionalità della foresta.
- **Distribuzioni in cui esistono account computer in una foresta di Active Directory diversa dalla foresta o dalle ulteriori foreste di Active Directory contenenti gli account computer dei desktop virtuali.** In questo tipo di distribuzione deve esistere un trust bidirezionale tra i domini contenenti gli account del computer Controller e tutti i domini contenenti gli account del computer desktop virtuale. In questo tipo di distribuzione, tutti i domini contenenti account Controller o computer desktop virtuale devono essere a livello funzionale "Windows 2000 nativo"o superiore. Sono supportati tutti i livelli funzionali della foresta.
- **Controller di dominio scrivibili.** I controller di dominio di sola lettura non sono supportati.

Facoltativamente, i Virtual Delivery Agent (VDA) possono utilizzare le informazioni pubblicate in Active Directory per determinare con quali controller possono registrarsi (individuazione). Questo metodo è supportato principalmente per la compatibilità con le versioni precedenti ed è disponibile solo se i VDA si trovano nella stessa foresta di Active Directory in cui si trovano i controller. Per informazioni su questo metodo di rilevamento, vedere Individuazione basata su unità organizzativa di Active Directory e CTX118976.

> **Nota:**
>
> Non modificare il nome del computer o l'appartenenza al dominio di un Delivery Controller dopo la configurazione del sito.

Distribuire in un ambiente con più foreste Active Directory

Queste informazioni si applicano alle versioni minime di XenDesktop 7.1 e XenApp 7.5. Non si applicano alle versioni precedenti di XenDesktop o XenApp.

In un ambiente Active Directory con più foreste, se esistono trust unidirezionali o bidirezionali, è possibile utilizzare server di inoltro DNS o condizionali per la ricerca e la registrazione dei nomi. Per consentire agli utenti di Active Directory appropriati di creare account computer, utilizzare la Delega guidata del controllo. Per ulteriori informazioni su questa procedura guidata, vedere la documentazione Microsoft.

Non sono necessarie zone DNS inverse nell'infrastruttura DNS se sono presenti server di inoltro DNS appropriati tra le foreste.

La chiave `SupportMultipleForest` è necessaria se i VDA e i Controller si trovano in foreste separate, indipendentemente dal fatto che i nomi di Active Directory e NetBIOS siano diversi. Utilizzare le seguenti informazioni per aggiungere la chiave del Registro di sistema al VDA e ai Delivery Controller:

> **Attenzione:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Eseguire il backup del Registro di sistema prima di modificarlo.

Sul VDA, configurare: `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`.

- Nome: `SupportMultipleForest`
- Tipo: `REG_DWORD`
- Dati: `0x00000001 (1)`

In tutti i Delivery Controller, configurare: `HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest`.

- Nome: `SupportMultipleForest`
- Tipo: `REG_DWORD`

- Dati: 0x00000001 (1)

Potrebbe essere necessaria la configurazione DNS inversa se lo spazio dei nomi DNS è diverso da quello di Active Directory.

È stata aggiunta una voce del Registro di sistema per evitare l'attivazione indesiderata nei VDA dell'autenticazione NTLM, che è meno sicura di Kerberos. Questa voce può essere utilizzata al posto della voce SupportMultipleForest, che può essere comunque utilizzata per la compatibilità con le versioni precedenti.

Sul VDA configurare:HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent
.

- Nome: SupportMultipleForestDdcLookup
- Tipo: REG_DWORD
- Dati: 0x00000001 (1)

Questa chiave del Registro di sistema esegue una ricerca DDC in un ambiente a più foreste di trust bidirezionale che consente di rimuovere l'autenticazione basata su NTLM durante il processo di registrazione iniziale.

Se durante l'installazione sono presenti trust esterni, è necessaria la chiave ListOfSIDs del Registro di sistema. La chiave ListOfSIDs del Registro di sistema è inoltre necessaria se il nome di dominio completo di Active Directory è diverso dal nome FQDN DNS o se il dominio contenente il controller di dominio ha un nome NetBIOS diverso da quello di Active Directory FQDN. Per aggiungere la chiave del Registro di sistema, utilizzare le seguenti informazioni:

Per il VDA, individuare la chiave del Registro di sistema HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs.

- Nome: ListOfSIDs
- Tipo: REG_SZ
- Dati: identificativo di sicurezza (SID) dei controller. I SID sono inclusi nei risultati del cmdlet Get-BrokerController.

Quando sono presenti trust esterni, apportare le seguenti modifiche al VDA:

1. Individuare il file Program Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config.
2. Effettuare una copia di backup del file.
3. Aprire il file in un programma di modifica del testo, ad esempio Blocco note.
4. Individuare il testo allowNtlm="false" e modificare il testo in allowNtlm="true".
5. Salvare il file.

Dopo aver aggiunto la chiave ListOfSIDs del Registro di sistema e aver modificato il file brokeragent.exe.config, riavviare Citrix Desktop Service per applicare le modifiche.

Nella tabella seguente sono elencati i tipi di trust supportati:

Tipo di trust	Transitività	Direzione	Supportato in questa versione
Elemento principale e secondario	Transitivo	Bidirezionale	Sì
Origine struttura	Transitivo	Bidirezionale	Sì
Esterno	Non transitivo	A senso unico o bidirezionale	Sì
Foresta	Transitivo	A senso unico o bidirezionale	Sì
Scelta rapida	Transitivo	A senso unico o bidirezionale	Sì
Area di autenticazione	Transitivo o non transitivo	A senso unico o bidirezionale	No

Per ulteriori informazioni sugli ambienti Active Directory complessi, vedere CTX134971.

Hybrid Azure Active Directory joined (Aggiunta ad Azure Active Directory ibrida)

January 7, 2024

Questo articolo descrive i requisiti per creare cataloghi aggiunti ad Azure Active Directory ibrido (HAAD) utilizzando Citrix DaaS oltre ai requisiti descritti nella sezione dei requisiti di sistema di Citrix DaaS.

Le macchine aggiunte ad Azure AD ibrido utilizzano AD locale come provider di autenticazione. È possibile assegnarle a utenti o gruppi di dominio in AD locale. Per abilitare l'esperienza SSO senza soluzione di continuità di Azure AD, è necessario sincronizzare gli utenti del dominio con Azure AD.

> **Nota:**
>
> Le VM aggiunte ad Azure AD ibrido sono supportate nelle infrastrutture di identità sia federate che gestite.

Requisiti

- Tipo VDA: a sessione singola (solo desktop) o multisessione (app e desktop)

- Versione VDA: 2212 o successiva
- Tipo di provisioning: Machine Creation Services (MCS), persistente e non persistente
- Tipo di assegnazione: dedicato e in pool
- Piattaforma di hosting: qualsiasi hypervisor o servizio cloud

Limiti

- Se si utilizza Citrix Federated Authentication Service (FAS), il Single Sign-On viene indirizzato ad AD in locale anziché ad Azure AD. In questo caso, si consiglia di configurare l'autenticazione basata sul certificato di Azure AD in modo che il token di aggiornamento primario (PRT) venga generato all'accesso dell'utente, in modo da facilitare il single sign-on alle risorse di Azure AD all'interno della sessione. Altrimenti, il PRT non sarà presente e l'accesso SSO alle risorse di Azure AD non funzionerà. Per informazioni su come ottenere l'accesso singolo (SSO) da Azure AD a VDA uniti ibridi utilizzando Citrix Federated Authentication Service (FAS), vedere Hybrid-joined VDAs.
- Non saltare la preparazione delle immagini durante la creazione o l'aggiornamento dei cataloghi di macchine. Se si desidera saltare la preparazione delle immagini, assicurarsi che le macchine virtuali master non siano aggiunte ad Azure AD o a Azure AD ibrido.

Considerazioni

- La creazione di macchine aggiunte ad Azure Active Directory ibrido richiede l'autorizzazione `Write userCertificate` nel dominio di destinazione. Assicurarsi di immettere le credenziali di un amministratore con tale autorizzazione durante la creazione del catalogo.
- Il processo di join di Azure AD ibrido è gestito da Citrix. È necessario disabilitare `autoWorkplaceJoin` controllato da Windows nelle macchine virtuali master come segue: L'operazione di disattivazione manuale `autoWorkplaceJoin` è richiesta solo per la versione VDA 2212 o precedente.

  1. Eseguire `gpedit.msc`.
  2. Accedere a **Configurazione computer > Modelli amministrativi > Componenti di Windows > Registrazione dispositivo**.
  3. Impostare **Registra i computer aggiunti a un dominio come dispositivi** su **Disabilitato**.

- Selezionare l'unità organizzativa (OU) configurata per la sincronizzazione con Azure AD quando si creano le identità delle macchine.
- Per la macchina virtuale master basata su Windows 11 22H2, creare un'attività pianificata nella macchina virtuale master che esegua i seguenti comandi all'avvio del sistema utilizzando l'account SYSTEM. Questa attività di pianificazione di un'attività nella macchina virtuale master è richiesta solo per la versione VDA 2212 o precedente.


```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'
$WorkplaceJoinKeyPath = 'HKLM:\SOFTWARE\Policies\Microsoft\
    Windows\WorkplaceJoin'
$MaxCount = 60

for ($count = 1; $count -le $MaxCount; $count++)
{

  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)
  {

    $provider = (Get-Item -Path $VirtualDesktopKeyPath).GetValue(
        "Provider", $null)
    if ($provider -eq 'Citrix')
    {

        break;
     }


    if ($provider -eq 1)
    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "
            Provider" -Value "Citrix" -Force
        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name "
            autoWorkplaceJoin" -Value 1 -Force
        Start-Sleep 5
        dsregcmd /join
        break
     }

   }


  Start-Sleep 1
 }

<!--NeedCopy-->
```

Passaggi successivi

Per ulteriori informazioni sulla creazione di cataloghi aggiunti ad Azure Active Directory ibrido, vedere Creare cataloghi aggiunti ad Azure Active Directory ibrido.

Preparazione per l'installazione

January 7, 2024

La distribuzione di Citrix Virtual Apps and Desktops inizia con l'installazione dei componenti che seguono. Questo processo prepara per la distribuzione di applicazioni e desktop agli utenti all'interno del firewall.

- Uno o più Delivery Controller
- Citrix Director
- Citrix StoreFront
- Citrix License Server
- Uno o più Citrix Virtual Delivery Agent (VDA)
- Componenti e tecnologie opzionali quali Universal Print Server, Federated Authentication Service e Reimpostazione password self-service

Per gli utenti esterni al firewall, installare e configurare un componente aggiuntivo quale Citrix Gateway. Per un'introduzione, vedere Integrare Citrix Virtual Apps and Desktops con Citrix Gateway.

Se la distribuzione include carichi di lavoro di Windows Server, configurare un Server licenze Microsoft RDS.

È possibile utilizzare il programma di installazione del prodotto completo sulla ISO del prodotto per distribuire molti componenti e tecnologie. È possibile utilizzare un programma di installazione VDA autonomo per installare i VDA. I programmi di installazione VDA autonomi sono disponibili sul sito di download Citrix. Tutti i programmi di installazione offrono la possibilità di utilizzare l'interfaccia grafica o la riga di comando. Vedere Programmi di installazione.

L'ISO del prodotto contiene script di esempio che installano, aggiornano o rimuovono i VDA nei computer in Active Directory. È inoltre possibile utilizzare gli script per gestire le immagini utilizzate da Machine Creation Services (MCS) e Citrix Provisioning (in precedenza Provisioning Services). Per ulteriori informazioni, vedere Installare i VDA utilizzando script.

Informazioni da leggere prima dell'installazione

- Panoramica tecnica: se non si ha familiarità con il prodotto e i suoi componenti.
- Sicurezza: quando si pianifica l'ambiente di distribuzione.
- Problemi noti: problemi che si potrebbero riscontrare in questa versione.
- Database: informazioni sui database di sistema e su come configurarli. Durante l'installazione del controller, è possibile installare SQL Server Express per l'utilizzo come database del sito. È possibile configurare la maggior parte delle informazioni del database quando si crea un sito, dopo aver installato i componenti principali.

- Accesso remoto PC: se si sta distribuendo un ambiente che consente agli utenti di accedere in remoto alle proprie macchine fisiche che si trovano nell'ufficio.
- Connessioni e risorse: se si utilizza un hypervisor o un altro servizio per ospitare macchine virtuali per applicazioni e desktop o per eseguirne il provisioning. È possibile configurare la prima connessione quando si crea un sito (dopo aver installato i componenti principali). Configurare l'ambiente di virtualizzazione prima di quel momento.
- Microsoft System Center Configuration Manager: se si utilizza ConfigMgr per gestire l'accesso alle applicazioni e ai desktop o se si utilizza la funzione di riattivazione LAN con Accesso remoto PC.
- **Connessioni host Public Cloud:** se si dispone di una licenza Hybrid Rights, è possibile creare connessioni host al cloud pubblico. Per informazioni relative alla licenza Hybrid Rights, vedere Hybrid Rights Renewals. Per informazioni relative all'adesione al cloud pubblico e al motivo di questa modifica, vedere CTX270373.

Dove installare i componenti

Rivedere i requisiti di sistema per conoscere le piattaforme, i sistemi operativi e le versioni supportate. I prerequisiti dei componenti vengono installati automaticamente, se non diversamente indicato. Per le piattaforme e i prerequisiti supportati, vedere la documentazione di Citrix StoreFront e Citrix License Server.

È possibile installare i componenti principali sullo stesso server o su server diversi.

- L'installazione di tutti i componenti principali su un server può essere adatta per la valutazione, il test o le distribuzioni di produzione di piccole dimensioni.
- Per essere pronti a future espansioni, è consigliabile installare componenti su server diversi. Ad esempio, l'installazione di Studio su un computer diverso dal server in cui è stato installato il Controller consente di gestire il sito in remoto.
- Per la maggior parte delle distribuzioni di produzione, si consiglia di installare i componenti principali su server separati.

  Installare Citrix License Server e le licenze prima di installare altri componenti su altri server.
- Per installare un componente supportato su un server CoreOS (ad esempio un Delivery Controller), è necessario utilizzare la riga di comando. Questo tipo di sistema operativo non offre un'interfaccia grafica, quindi installare Studio e altri strumenti altrove e quindi puntarli al server Controller.

È possibile installare sia un Delivery Controller che un VDA per il sistema operativo multisessione sullo stesso server. Avviare il programma di installazione e selezionare il Delivery Controller (più tutti gli altri componenti principali che si desidera avere su quella macchina). Quindi avviare nuovamente

il programma di installazione e selezionare **Virtual Delivery Agent** per sistema operativo multisessione.

Assicurarsi che ciascun sistema operativo disponga degli aggiornamenti più recenti.

Assicurarsi che tutte le macchine abbiano gli orologi di sistema sincronizzati. L'infrastruttura Kerberos che protegge la comunicazione tra le macchine richiede la sincronizzazione.

Con Citrix Hypervisors, lo stato di alimentazione della macchina virtuale potrebbe apparire come sconosciuto anche se appare registrato. Per risolvere questo problema, modificare il valore `HostTime` della chiave del Registro di sistema per disabilitare la sincronizzazione dell'ora con l'host:

```
HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\HostTime="Local"
```

```
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\XenTools\HostTime="
Local"
```

> **Suggerimento:**
>
> Il valore predefinito è `HostTime="UTC"`. Modificare questo valore in qualcosa di diverso da UTC, ad esempio `Local`. Questa modifica disabilita efficacemente la sincronizzazione dell'ora con l'host.

Le linee guida sull'ottimizzazione per i computer Windows 10 a sessione singola sono disponibili in CTX216252.

Dove NON installare i componenti:

- Non installare alcun componente in un controller di dominio Active Directory.
- Non è supportata l'installazione di un controller in un nodo di un'installazione di cluster di SQL Server, di un'installazione di mirroring di SQL Server o in un server che esegue Hyper-V.

Se si tenta di installare o aggiornare un VDA su un sistema operativo Windows non supportato da questa versione del prodotto, viene visualizzato un messaggio per accedere a un articolo che descrive le opzioni.

Requisiti delle autorizzazioni e di Active Directory

È necessario essere un utente di dominio e un amministratore locale nei computer in cui si installano i componenti.

Per utilizzare un programma di installazione VDA autonomo, è necessario disporre di privilegi amministrativi elevati o utilizzare **Esegui come amministratore**.

Configurare il dominio Active Directory prima di avviare un'installazione.

- I requisiti di sistema elencano i livelli di funzionalità di Active Directory supportati. Aggiunti ad Azure Active Directory contiene ulteriori informazioni.
- È necessario disporre di almeno un controller di dominio che esegua Servizi di dominio Active Directory.
- Non installare alcun componente Citrix Virtual Apps and Desktops su un controller di dominio.
- Non utilizzare una barra (/) quando si specificano i nomi delle unità organizzative in Studio.

L'account utente Windows utilizzato per installare Citrix License Server viene configurato automaticamente come amministratore completo di amministrazione delegata.

Per ulteriori informazioni:

- Procedure consigliate per la sicurezza
- Amministrazione delegata
- Documentazione Microsoft per la configurazione di Active Directory

Guida all'installazione, considerazioni e procedure consigliate

Durante l'installazione di qualsiasi componente

- Quando si installa o si aggiorna un Delivery Controller, Studio, License Server o Director dal supporto del prodotto completo, se il programma di installazione di Citrix rileva che è in sospeso un riavvio da una precedente installazione di Windows sul computer, il programma di installazione si interrompe con il codice di uscita/restituzione 9. Viene richiesto di riavviare il computer.

  Questo non è un riavvio forzato Citrix. È dovuto ad altri componenti installati in precedenza sul computer. In questo caso, riavviare il computer e riavviare il programma di installazione Citrix.

  Quando si utilizza l'interfaccia della riga di comando, è possibile impedire il controllo del riavvio in sospeso includendo nel comando l'opzione `/no_pending_reboot_check`.
- In genere, se un componente ha dei prerequisiti, il programma di installazione li distribuisce se non sono presenti. Alcuni prerequisiti potrebbero richiedere il riavvio del computer.
- Quando si creano oggetti prima, durante e dopo l'installazione, specificare un nome univoco per ciascun oggetto. Ad esempio, fornire nomi univoci per reti, gruppi, cataloghi e risorse.
- Se un componente non viene installato correttamente, l'installazione si interrompe e viene visualizzato un messaggio di errore. I componenti installati correttamente vengono mantenuti. Non è necessario reinstallarli.
- I dati per Citrix Analytics vengono raccolti automaticamente quando si installano (o si aggiornano) componenti. Per impostazione predefinita, tali dati vengono caricati automaticamente su Citrix al termine dell'installazione. Inoltre, quando si installano i componenti, si viene automaticamente registrati nel CEIP (Citrix Customer Experience Improvement Program), che carica dati anonimi.

Durante l'installazione, è inoltre possibile scegliere di partecipare ad altre tecnologie Citrix che raccolgono diagnostica per la manutenzione e la risoluzione dei problemi. Per informazioni su questi programmi, vedere Citrix Insight Services.

- I dati per Google Analytics vengono raccolti (e successivamente caricati) automaticamente quando si installa (o si aggiorna) Studio. Dopo aver installato Studio, è possibile modificare questa impostazione con la chiave del Registro di sistema `HKLM\Software\Citrix\DesktopStudio\GAEnabled`. Il valore **1** abilita la raccolta e il caricamento, il valore **0** disabilita la raccolta e il caricamento.
- Se un'installazione VDA non riesce, un analizzatore MSI analizza il registro MSI in errore, visualizzando il codice di errore esatto. L'analizzatore suggerisce un articolo CTX, se si tratta di un problema noto. L'analizzatore raccoglie anche dati anonimi sul codice di errore. Questi dati sono inclusi con altri dati raccolti dal CEIP. Se si termina la registrazione in CEIP, i dati dell'analizzatore MSI raccolti non vengono più inviati a Citrix.

Durante l'installazione dei VDA

- L'app Citrix Workspace per Windows è disponibile, ma non installata per impostazione predefinita quando si installa un VDA. L'amministratore o gli utenti possono scaricare e installare (e aggiornare) l'app Citrix Workspace per Windows e altre app Citrix Workspace dal sito Web Citrix. In alternativa, è possibile rendere disponibili tali app Citrix Workspace dal server StoreFront. Vedere la Documentazione di StoreFront.
- Il servizio spooler di stampa Microsoft deve essere abilitato. Non è possibile installare correttamente un VDA se tale servizio è disabilitato.
- La maggior parte delle edizioni Windows supportate viene fornita con Microsoft Media Foundation già installato. Se il computer non dispone di Media Foundation (ad esempio le edizioni N), varie funzionalità multimediali non verranno installate e non funzioneranno.

  - Reindirizzamento di Windows Media
  - Reindirizzamento video HTML5
  - Reindirizzamento webcam HDX RealTime

  È possibile riconoscere la limitazione o terminare l'installazione di VDA e riavviarla in un secondo momento, dopo aver installato Media Foundation. Nell'interfaccia grafica, questa scelta è presentata in un messaggio. Nella riga di comando, è possibile utilizzare l'opzione `/no_mediafoundation_ack` per riconoscere la limitazione.
- Quando si installa il VDA, viene creato automaticamente un nuovo gruppo di utenti locale denominato **Direct Access Users** (Utenti con accesso diretto). In un VDA per sistema operativo a sessione singola, questo gruppo si applica solo alle connessioni RDP. Su un VDA per sistema operativo multisessione, questo gruppo si applica alle connessioni ICA e RDP.

- Il VDA deve disporre di indirizzi di controller validi con cui comunicare. In caso contrario, non è possibile stabilire sessioni. È possibile specificare gli indirizzi del controller quando si installa il VDA o in un secondo momento. Ricordare che deve essere fatto. Per ulteriori informazioni, vedere Registrazione dei VDA.

Strumenti di supportabilità dei VDA

Ogni programma di installazione di VDA include un MSI di supportabilità che contiene strumenti Citrix per il controllo di prestazioni del VDA quali l'integrità generale e la qualità delle connessioni. Attivare o disattivare l'installazione di questo MSI nella pagina **Componenti aggiuntivi** dell'interfaccia grafica del programma di installazione del VDA. Dalla riga di comando, è possibile disabilitare l'installazione con l'opzione `/exclude "Citrix Supportability Tools"`.

Per impostazione predefinita, l'MSI di supportabilità è installato in `c:\Program Files (x86)\Citrix\Supportability Tools\`. È possibile modificare questo percorso nella pagina **Componenti** dell'interfaccia grafica del programma di installazione VDA o con l'opzione della `/installdir` riga di comando. Tenere presente che la modifica della posizione interessa tutti i componenti VDA installati, non solo gli strumenti di supportabilità.

Strumenti attualmente presenti nell'MSI di supportabilità:

- Citrix Health Assistant: per i dettagli, vedere CTX207624.
- VDA Cleanup Utility: per i dettagli, vedere CTX209255.

Se non si installano gli strumenti quando si installa il VDA, l'articolo CTX contiene un collegamento al pacchetto di download corrente.

Riavvia dopo e durante l'installazione del VDA

Al termine dell'installazione del VDA è necessario riavviare. Tale riavvio avviene automaticamente per impostazione predefinita.

Quando si esegue l'aggiornamento di un VDA alla versione 7.17 (o a una versione supportata successiva), si verifica un riavvio durante l'aggiornamento. Questo non può essere evitato.

Per ridurre al minimo il numero di riavvii necessari durante l'installazione di VDA:

- Assicurarsi che sia installata una versione di .NET Framework supportata prima di iniziare l'installazione del VDA.
- Per le macchine con sistema operativo multisessione Windows, installare e abilitare i servizi ruolo di Servizi Desktop remoto prima di installare il VDA.

Se non si installano tali prerequisiti prima di installare il VDA:

- Se si utilizza l'interfaccia grafica o l'interfaccia della riga di comando senza l'opzione `/noreboot`, la macchina si riavvia automaticamente dopo aver installato il prerequisito.
- Se si utilizza l'interfaccia della riga di comando con l'opzione `/noreboot`, è necessario effettuare personalmente il riavvio.

Quando si esegue l'aggiornamento di un VDA alla versione 7.17 o a una versione successiva supportata, si verifica un riavvio durante l'aggiornamento. Questo non può essere evitato.

Ripristino in caso di errore di installazione o aggiornamento

> **Nota:**
>
> Questa funzionalità è disponibile per VDA a sessione singola e multisessione.

Se un'installazione o un aggiornamento di un VDA a sessione singola non va a buon fine e la funzionaltà Restore on failure (Ripristina in caso di errore) è abilitata, la macchina viene riportata a un punto di ripristino impostato prima dell'inizio dell'installazione o dell'aggiornamento.

Se un'installazione o un aggiornamento VDA multisessione non riesce e la funzionalità "restore on failure"(ripristino in caso di errore) è abilitata, la macchina viene riportata a un backup che è stato eseguito prima dell'avvio dell'installazione o dell'aggiornamento.

Quando un'installazione o un aggiornamento di un VDA a sessione singola inizia con questa funzionalità abilitata, il programma di installazione crea un punto di ripristino del sistema prima di iniziare l'installazione o l'aggiornamento effettivi. Se l'installazione o l'aggiornamento del VDA non riesce, la macchina viene riportata allo stato del punto di ripristino. La cartella `%temp%/Citrix` contiene log di distribuzione e altre informazioni sul ripristino.

Quando un'installazione o un aggiornamento di un VDA multisessione inizia con questa funzionalità abilitata, il programma di installazione crea un backup del server prima di iniziare l'installazione o l'aggiornamento effettivi. Se l'installazione o l'aggiornamento del VDA non riesce, la macchina viene riportata allo stato di backup. La cartella `%temp%/Citrix` contiene log di distribuzione e altre informazioni sul ripristino. Il tempo necessario per creare il backup del server è basato sulle dimensioni del backup necessario e sulla quantità di risorse disponibili per il server. Il backup è archiviato in *C:\WindowsImageBackup\servername*.

Per impostazione predefinita, questa funzionalità è disabilitata.

Se si prevede di abilitare questa funzionalità, assicurarsi che il ripristino del sistema non sia disabilitato tramite un'impostazione dell'oggetto Criteri di gruppo (`Computer Configuration > Administrative Templates > System > System Restore`).

> **Nota:**
>
> Questa impostazione dell'oggetto Criteri di gruppo non si applica al ripristino di un VDA multi-

> sessione.

Per abilitare questa funzionalità durante l'installazione o l'aggiornamento di un VDA multisessione:

- Quando si utilizza l'interfaccia grafica di un programma di installazione VDA (ad esempio si utilizza **Autostart** o il comando `XenDesktopVDASetup.exe` senza alcuna opzione di ripristino o non interattiva), selezionare la casella di controllo **Enable automatic restore if update fails** (Abilita ripristino automatico in caso di errore dell'aggiornamento) nella pagina **Summary** (Riepilogo).

  Se l'installazione/aggiornamento viene completato correttamente, il punto di ripristino/il backup non viene utilizzato, ma viene mantenuto.

- Eseguire un programma di installazione VDA con l'opzione `/enablerestore` o `/enablerestorecleanup` utilizzando la riga di comando.

  - Se si utilizza l'opzione `/enablerestorecleanup` e l'installazione/aggiornamento viene completato correttamente, il punto di ripristino/il backup del server viene rimosso automaticamente.
  - Se si utilizza l'opzione `/enablerestore` e l'installazione/aggiornamento viene completato correttamente, il punto di ripristino non viene utilizzato, ma viene mantenuto.

Programmi di installazione

Programma di installazione del prodotto completo

Utilizzando il programma di installazione del prodotto completo fornito nell'ISO, è possibile:

- Installare, aggiornare o rimuovere i componenti principali: Delivery Controller, Studio, Director e License Server.
- Installare o aggiornare StoreFront.
- Installare o aggiornare i VDA Windows per sistemi operativi a sessione singola o multisessione.
- Installare il componente `UpsServer` di Universal Print Server sui server di stampa.
- Installare il Federated Authentication Service.
- Installare Session Recording.
- Installare Workspace Environment Management.

> **Nota:**

> Il programma di installazione dell'agente Workspace Environment Management non è localizzato. È disponibile solo in inglese.

Per distribuire un desktop da un sistema operativo multisessione per un utente (ad esempio, per lo sviluppo Web), utilizzare l'interfaccia della riga di comando del programma di installazione del prodotto completo. Per ulteriori informazioni, vedere VDI del server.

Programmi di installazione dei VDA autonomi

Nelle pagine di download di Citrix sono disponibili programmi di installazione dei VDA autonomi (Non sono disponibili nel supporto di installazione del prodotto). Gli installatori VDA standalone sono molto più piccoli rispetto all'ISO del prodotto completo. Si adattano più facilmente alle distribuzioni che:

- Utilizzano pacchetti ESD (Electronic Software Distribution) che vengono installati o copiati localmente
- Hanno macchine fisiche
- Hanno uffici remoti

Per impostazione predefinita, i file dei VDA autonomi autoestraenti vengono estratti nella cartella **Temp**. Durante l'estrazione nella cartella **Temp** è necessario più spazio sul disco del computer rispetto a quando si utilizza il programma di installazione del prodotto completo. Tuttavia, i file estratti nella cartella **Temp** vengono eliminati automaticamente al termine dell'installazione. In alternativa, è possibile utilizzare il comando `/extract` con un percorso assoluto.

Sono disponibili per il download tre programmi di installazione VDA autonomi.

VDAServerSetup.exe:

Installa un VDA per sistema operativo multisessione. Supporta tutte le opzioni VDA per sistema operativo multisessione disponibili con il programma di installazione del prodotto completo.

VDAWorkstationSetup.exe:

Installa un VDA per sistema operativo a sessione singola. Supporta tutte le opzioni VDA per sistema operativo a sessione singola disponibili con il programma di installazione del prodotto completo.

VDAWorkstationCoreSetup.exe:

Installa un VDA per il sistema operativo a sessione singola ottimizzato per le distribuzioni di Accesso remoto PC o le installazioni VDI principali. Accesso remoto PC utilizza macchine fisiche. Le installazioni VDI principali sono macchine virtuali che non vengono utilizzate come immagine. Installa solo i servizi di base necessari per le connessioni VDA in tali distribuzioni. Pertanto supporta solo un sottoinsieme delle opzioni che sono valide con il prodotto completo o i programmi di installazione `VDAWorkstationSetup.exe`.

Questo programma di installazione non installa né contiene i componenti utilizzati per:

- App-V.
- Profile Management. L'esclusione di Citrix Profile Management dall'installazione influisce sui display Citrix Director. Per ulteriori informazioni, vedere Installare i VDA.
- Servizio di identità macchina.
- Strumenti di supportabilità Citrix.
- Citrix Files per Windows.
- Citrix Files per Outlook.

Il programma di installazione `VDAWorkstationCoreSetup.exe` non installa né contiene un'app Citrix Workspace per Windows.

L'utilizzo di `VDAWorkstationCoreSetup.exe` equivale a utilizzare il prodotto completo o il programma di installazione `VDAWorkstationSetup` per installare un VDA con sistema operativo a sessione singola e a una delle seguenti azioni:

- Nell'interfaccia grafica: selezionare l'opzione Remote PC Access (Accesso remoto PC) nella pagina **Environment** (Ambiente).
- Nell'interfaccia della riga di comando: specificare l'opzione `/remotepc`.
- Nell'interfaccia della riga di comando: specificare `/components vda` più l'opzione `/exclude` che elenca tutti i nomi dei componenti aggiuntivi validi.

È possibile installare i componenti e/o le funzionalità omessi in un secondo momento eseguendo il programma di installazione del prodotto completo. Questa azione consente di installare tutti i componenti mancanti.

Il programma di installazione `VDAWorkstationCoreSetup.exe` installa automaticamente l'MSI di reindirizzamento del contenuto del browser. Questa installazione automatica si applica alla versione 2003 e alle versioni successive supportate.

Codici restituiti per l'installazione Citrix

Il registro di installazione contiene il risultato delle installazioni dei componenti come codice restituito Citrix, non come valore Microsoft.

- 0 = Success (riuscita)
- 1 = Failed (non riuscita)
- 2 = PartialSuccess (riuscita parzialmente)
- 3 = PartialSuccessAndRebootNeeded (riuscita parzialmente e riavvio necessario)
- 4 = FailureAndRebootNeeded (non riuscita e riavvio necessario)
- 5 = UserCanceled (cancellata dall'utente)
- 6 = MissingCommandLineArgument (argomento della riga di comando mancante)
- 7 = NewerVersionFound (trovata nuova versione)

Ad esempio, quando si utilizzano strumenti come Microsoft System Center Configuration Manager, l'installazione di un VDA mediante script potrebbe non riuscire quando il registro di installazione contiene il codice restituito 3. Ciò può verificarsi quando il programma di installazione VDA è in attesa di un riavvio che deve essere effettuato dall'utente (ad esempio, dopo l'installazione di un prerequisito del ruolo di Servizi Desktop remoto su un server). L'installazione di un VDA viene considerata riuscita solo dopo che sono stati installati tutti i prerequisiti e i componenti selezionati e che il computer è stato riavviato dopo l'installazione.

In alternativa, è possibile eseguire il wrapping dell'installazione in script CMD (che restituiscono i codici di uscita Microsoft) o modificare i codici di riuscita nel pacchetto di Configuration Manager.

Configurare un server di licenze Servizi Desktop remoto Microsoft per i carichi di lavoro di Windows Server

Questo prodotto consente di accedere alle funzionalità di sessione remota di Windows Server quando viene consegnato un carico di lavoro di Windows Server, ad esempio Windows 2016. Questa operazione richiede in genere una licenza di accesso client (CAL) di Servizi Desktop remoto. Il VDA deve essere in grado di contattare un server licenze di Servizi Desktop remoto per richiedere licenze CAL di Servizi Desktop remoto. Installare e attivare il server licenze. Per ulteriori informazioni, vedere il documento Microsoft Attivare il server licenze di Servizi Desktop remoto. Per gli ambienti Proof of Concept (POC), è possibile utilizzare il periodo di prova fornito da Microsoft.

Con questo metodo, è possibile fare in modo che questo servizio applichi le impostazioni del server licenze. È possibile configurare il server licenze e la modalità per utente nella console di Servizi Desktop remoto sull'immagine. È inoltre possibile configurare il server licenze utilizzando le impostazioni di Criteri di gruppo Microsoft. Per ulteriori informazioni, vedere il documento Microsoft Concedere licenze CAL (Client Access License) per la distribuzione di Servizi Desktop remoto.

Per configurare il server licenze di Servizi Desktop remoto utilizzando le impostazioni di Criteri di gruppo:

1. Installare un server licenze di Servizi Desktop remoto in un computer disponibile. La macchina deve essere sempre disponibile. I carichi di lavoro dei prodotti Citrix devono essere in grado di raggiungere questo server licenze.
2. Specificare l'indirizzo del server licenze e la modalità di licenza per utente utilizzando Criteri di gruppo Microsoft. Per ulteriori informazioni, vedere il documento Microsoft Specify the Remote Desktop Licensing Mode for an RD Session Host Server (Specificare la modalità di gestione licenze Desktop remoto per un server Host sessione Desktop remoto).

I carichi di lavoro di Windows 10 richiedono l'adeguata attivazione della licenza di Windows 10. Si consiglia di seguire la documentazione Microsoft per attivare i carichi di lavoro di Windows 10.

Ulteriori informazioni

Per impostare le posizioni risorsa per tipi di host specifici:

- Ambienti cloud AWS
- Ambienti di virtualizzazione Citrix Hypervisor
- Ambienti Google Cloud
- Ambienti cloud Microsoft Azure Resource Manager
- Ambienti Microsoft System Center Configuration Manager
- Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager
- Ambienti di virtualizzazione Nutanix
- Soluzioni Nutanix Cloud e dei partner
- Ambienti di virtualizzazione VMware
- Soluzioni VMware Cloud e dei partner

Ambienti cloud AWS

April 3, 2024

Questo articolo illustra la configurazione dell'account AWS come posizione risorsa che è possibile utilizzare con Citrix Virtual Apps and Desktops. La posizione risorsa include un set di componenti di base, ideale per una Proof of Concept o un'altra distribuzione che non richiede risorse distribuite in più zone di disponibilità. Dopo aver completato queste attività, è possibile installare VDA, eseguire il provisioning delle macchine, creare cataloghi delle macchine e creare gruppi di consegna.

Una volta completate le attività descritte in questo articolo, la posizione risorsa include i seguenti componenti:

- Un cloud privato virtuale (VPC) con subnet pubbliche e private all'interno di un'unica zona di disponibilità.
- Un'istanza che viene eseguita sia come controller di dominio Active Directory che come server DNS, situata nella subnet privata del VPC.
- Un'istanza che funge da host bastion nella subnet pubblica del VPC. Questa istanza viene utilizzata per avviare connessioni RDP alle istanze nella subnet privata per scopi amministrativi. Dopo aver completato la configurazione della posizione risorsa, è possibile chiudere questa istanza in modo che non sia più facilmente accessibile. Quando è necessario gestire altre istanze nella subnet privata, come le istanze VDA, è possibile riavviare l'istanza host bastion.

Panoramica delle attività

Configurare un cloud privato virtuale (VPC) con subnet pubbliche e private. Una volta completata questa attività, AWS distribuisce un gateway NAT con un indirizzo IP elastico nella subnet pubblica. Questa azione consente alle istanze nella subnet privata di accedere a Internet. Le istanze nella subnet pubblica sono accessibili al traffico pubblico in entrata, mentre le istanze nella subnet privata non lo sono.

Configurare i gruppi di sicurezza. I gruppi di sicurezza agiscono come firewall virtuali che controllano il traffico per le istanze nel VPC. È possibile aggiungere regole ai gruppi di sicurezza che consentono alle istanze nella subnet pubblica di comunicare con le istanze nella subnet privata. Inoltre, questi gruppi di sicurezza saranno associati anche a ogni istanza nel VPC.

Creare un set di opzioni DHCP. Con un VPC Amazon, i servizi DHCP e DNS sono forniti per impostazione predefinita, il che influisce sulla configurazione del DNS sul controller di dominio Active Directory. Il DHCP di Amazon non può essere disabilitato e il DNS di Amazon può essere utilizzato solo per la risoluzione DNS pubblica, non per la risoluzione dei nomi di Active Directory. Per specificare i server di dominio e dei nomi trasferiti alle istanze tramite DHCP, creare un set di opzioni DHCP. Il set assegna il suffisso di dominio Active Directory e specifica il server DNS per tutte le istanze nel VPC. Per garantire che i record Host (A) e Ricerca inversa (PTR) vengano registrati automaticamente quando le istanze entrano a far parte del dominio, è necessario configurare le proprietà dell'adattatore di rete per ogni istanza aggiunta alla subnet privata.

Aggiungere un host bastion e un controller di dominio al VPC. Tramite l'host bastion, è possibile accedere alle istanze nella subnet privata per configurare il dominio e unire le istanze al dominio.

Attività 1: Configurare il VPC

1. Dalla console di gestione AWS, selezionare **VPC**.
2. Dalla dashboard VPC, selezionare **Create VPC**.
3. Selezionare **VPC and more** (VPC e altro).
4. In NAT gateways ($) selezionare **In 1 AZ** o **1 per AZ**.
5. In DNS options (Opzioni DNS), lasciare selezionata l'opzione **Enable DNS hostnames** (Abilita nomi host DNS).
6. Selezionare **Create VPC** (Crea VPC). AWS crea le subnet pubbliche e private, il gateway Internet, le tabelle di instradamento e il gruppo di sicurezza predefinito.

Attività 2: Configurare i gruppi di sicurezza

Questa attività crea e configura i seguenti gruppi di sicurezza per il VPC:

- Un gruppo di sicurezza pubblico da associare alle istanze della subnet pubblica.

- Un gruppo di sicurezza privato da associare alle istanze della tua sottorete privata.

Per creare i gruppi di sicurezza:

1. Nella dashboard del VPC, selezionare **Security Groups** (Gruppi di sicurezza).
2. Creare un gruppo di sicurezza per il gruppo di sicurezza pubblico. Selezionare **Create Security Group** (Crea gruppo di sicurezza) e immettere un nome e una descrizione per il gruppo. Nel VPC, selezionare il VPC creato in precedenza. Selezionare **Yes, Create** (Sì, crea).

Configurare il gruppo di sicurezza pubblico

1. Dall'elenco dei gruppi di sicurezza, selezionare il gruppo di sicurezza pubblico.
2. Selezionare la scheda **Inbound Rules** (Regole in entrata) e selezionare **Edit** (Modifica) per creare le seguenti regole:

Tipo	Origine
TUTTO il traffico	Selezionare il gruppo di sicurezza privato.
TUTTO il traffico	Selezionare il gruppo di sicurezza pubblico.
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (affidabilità della sessione)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. Al termine, selezionare **Save** (Salva).
4. Selezionare la scheda **Outbound Rules** (Regole in uscita) e selezionare **Edit** (Modifica) per creare le seguenti regole:

Tipo	Destinazione
TUTTO il traffico	Selezionare il gruppo di sicurezza privato.
TUTTO il traffico	0.0.0.0/0
ICMP	0.0.0.0/0

5. Al termine, selezionare **Save** (Salva).

Configurare il gruppo di sicurezza privato

1. Dall'elenco dei gruppi di sicurezza, selezionare il gruppo di sicurezza privato.
2. Se non è stato impostato il traffico dal gruppo di sicurezza pubblico, è necessario impostare le porte TCP; selezionare la scheda **Inbound Rules** (Regole in entrata) e selezionare **Edit** (Modifica) per creare le seguenti regole:

Tipo	Origine
TUTTO il traffico	Selezionare il gruppo di sicurezza privato.
TUTTO il traffico	Selezionare il gruppo di sicurezza pubblico.
ICMP	Selezionare il gruppo di sicurezza pubblico.
TCP 53 (DNS)	Selezionare il gruppo di sicurezza pubblico.
UDP 53 (DNS)	Selezionare il gruppo di sicurezza pubblico.
80 (HTTP)	Selezionare il gruppo di sicurezza pubblico.
TCP 135	Selezionare il gruppo di sicurezza pubblico.
TCP 389	Selezionare il gruppo di sicurezza pubblico.
UDP 389	Selezionare il gruppo di sicurezza pubblico.
443 (HTTPS)	Selezionare il gruppo di sicurezza pubblico.
TCP 1494 (ICA/HDX)	Selezionare il gruppo di sicurezza pubblico.
TCP 2598 (affidabilità della sessione)	Selezionare il gruppo di sicurezza pubblico.
3389 (RDP)	Selezionare il gruppo di sicurezza pubblico.
TCP 49152-65535	Selezionare il gruppo di sicurezza pubblico.

3. Al termine, selezionare **Save** (Salva).
4. Selezionare la scheda **Outbound Rules** (Regole in uscita) e selezionare **Edit** (Modifica) per creare le seguenti regole:

Tipo	Destinazione
TUTTO il traffico	Selezionare il gruppo di sicurezza privato.
TUTTO il traffico	0.0.0.0/0

Tipo	Destinazione
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. Al termine, selezionare **Save** (Salva).

Attività 3: Avviare le istanze

Eseguire i seguenti passaggi per creare due istanze EC2 e decrittografano la password dell'amministratore predefinita generata da Amazon:

1. Dalla Console di gestione AWS, selezionare **EC2**.
2. Dalla dashboard di EC2, selezionare **Launch Instance** (Avvia istanza).
3. Selezionare un'immagine e un tipo di istanza della macchina Windows Server.
4. Nella pagina **Configure Instance Details** (Configura dettagli istanza), inserire un nome per l'istanza e selezionare il VPC configurato in precedenza.
5. In **Subnet**, effettuare le seguenti selezioni per ogni istanza:
   - Host bastion: selezionare la subnet pubblica
   - Controller di dominio: selezionare la subnet privata
6. In **Auto-assign Public IP address** (Assegna automaticamente l'indirizzo IP pubblico), effettuare le seguenti selezioni per ogni istanza:
   - Host bastion: selezionare **Enable** (Abilita).
   - Controller di dominio: selezionare **Use default setting** (Usa impostazione predefinita) o **Disable** (Disabilita).
7. In **Network Interfaces** (Interfacce di rete), immettere un indirizzo IP primario all'interno dell'intervallo IP della subnet privata per il controller di dominio.
8. Se necessario, nella pagina **Add Storage** (Aggiungi spazio di archiviazione), modificare le dimensioni del disco.
9. Nella pagina **Tag Instance** (Istanza tag), inserire un nome descrittivo per ogni istanza.
10. Nella pagina **Configure Security Groups** (Configura gruppi di sicurezza), selezionare **Select an existing security group** (Seleziona un gruppo di sicurezza esistente) e quindi effettuare le seguenti selezioni per ogni istanza:
    - Host bastion: selezionare il gruppo di sicurezza pubblico.

- Controller di dominio: selezionare il gruppo di sicurezza privato.

11. Controllare le selezioni e quindi selezionare **Launch** (Avvia).
12. Creare una nuova coppia di chiavi o selezionarne una esistente. Se si crea una nuova coppia di chiavi, scaricare il file della chiave privata (.pem) e conservalo in un luogo sicuro. È necessario fornire la chiave privata quando si acquisisce la password di amministratore predefinita per l'istanza.
13. Selezionare **Launch Instances** (Avvia istanze). Selezionare **View Instances** (Visualizza istanze) per visualizzare un elenco delle istanze. Attendere che l'istanza appena avviata abbia superato tutti i controlli di stato prima di accedervi.
14. Acquisire la password di amministratore predefinita per ogni istanza:
    a) Dall'elenco delle istanze, selezionare l'istanza e quindi selezionare **Connect** (Connetti).
    b) Andare alla scheda **RDP client** (Client RDP), selezionare **Get Password** (Ottieni password) e caricare il file della chiave privata (`.pem`) quando richiesto.
    c) Selezionare **Decrypt Password** (Decrittografa password) per ottenere la password leggibile dall'uomo. AWS visualizza la password predefinita.
15. Ripeti i passaggi dal passaggio 2 fino ad aver creato due istanze:
    - Un'istanza di host bastion nella tua sottorete pubblica
    - Un'istanza nella propria sottorete privata da utilizzare come controller di dominio.

Attività 4: Creare un set di opzioni DHCP

1. Dalla dashboard del VPC, selezionare **DHCP Options Sets** (Set di opzioni DHCP).
2. Inserire le seguenti informazioni:
    - Nome: inserire un nome descrittivo per il set.
    - Nome di dominio: immettere il nome di dominio completo utilizzato quando si configura l'istanza del controller di dominio.
    - Server del nome di dominio: immettere l'indirizzo IP privato assegnato all'istanza del controller di dominio e la stringa **AmazonProvidedDNS**, separati da virgole.
    - Server NTP: lasciare vuoto questo campo.
    - Server dei nomi NetBIOS: immettere l'indirizzo IP privato dell'istanza del controller di dominio.
    - Tipo di nodo NetBIOS: immettere **2**.
3. Selezionare **Yes, Create** (Sì, crea).
4. Associare il nuovo set al VPC:

a) Dalla dashboard del VPC, selezionare **Your VPCs** (VPC disponibili), quindi selezionare il VPC configurato in precedenza.
b) Selezionare **Actions > Edit DHCP Options Set** (Azioni > Modifica set di opzioni DHCP).
c) Quando richiesto, selezionare il nuovo set che hai creato e quindi selezionare **Save** (Salva).

Attività 5: Configurare le istanze

1. Utilizzando un client RDP, connettersi all'indirizzo IP pubblico dell'istanza host bastion. Quando richiesto, inserire le credenziali per l'account amministratore.
2. Dall'istanza host bastion, avviare Connessione Desktop remoto e connettersi all'indirizzo IP privato dell'istanza che si desidera configurare. Quando richiesto, inserire le credenziali dell'amministratore per l'istanza.
3. Per tutte le istanze nella subnet privata, configurare le impostazioni DNS:
   a) Selezionare **Start > Pannello di controllo > Rete e Internet > Centro connessioni di rete e condivisione > Modifica impostazioni scheda**. Fare doppio clic sulla connessione di rete visualizzata.
   b) Selezionare **Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties** (Proprietà > Protocollo Internet versione 4 (TCP/IPv4) > Proprietà).
   c) Selezionare **Advanced > DNS**. Assicurarsi che le seguenti impostazioni siano abilitate e selezionare **OK**:
      - Registrare gli indirizzi di questa connessione nel DNS
      - Utilizzare il suffisso DNS di questa connessione nella registrazione DNS
4. Per configurare il controller di dominio:
   a) Utilizzando Server Manager, aggiungere il ruolo Servizi di dominio Active Directory con tutte le funzionalità predefinite.
   b) Promuovere l'istanza a un controller di dominio. Durante la promozione, abilitare il DNS e utilizzare il nome di dominio specificato al momento della creazione del set di opzioni DHCP. Riavviare l'istanza quando richiesto.

Passaggi successivi

- Installare i componenti principali
- Installare i VDA
- Creare un sito
- Per informazioni su come creare e gestire una connessione in AWS, vedere Connessione ad AWS

Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Creare cataloghi di macchine

Ambienti di virtualizzazione Citrix Hypervisor

January 7, 2024

Citrix Hypervisor semplifica la gestione operativa, garantendo un'esperienza utente ad alta definizione per carichi di lavoro intensivi.

Per configurare l'hypervisor Citrix, vedere Preparazione per l'installazione.

Passaggi successivi

- Installare i componenti principali
- Installare i VDA
- Creare un sito
- Per informazioni su come creare e gestire una connessione, vedere Connessione a Citrix Hypervisor.

Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Creare cataloghi di macchine

Ambienti Google Cloud

January 7, 2024

Citrix Virtual Apps and Desktops consente di effettuare il provisioning delle macchine su Google Cloud e gestirle.

Requisiti

- Account Citrix Cloud. La funzionalità descritta in questo articolo è disponibile solo in Citrix Cloud.
- Un progetto Google Cloud. Il progetto memorizza tutte le risorse di elaborazione associate al catalogo delle macchine. Può essere un progetto esistente o nuovo.
- Abilitare quattro API nel progetto Google Cloud. Per i dettagli, consultare Abilitare le API di Google Cloud.
- Account del servizio Google Cloud. L'account del servizio si autentica su Google Cloud per consentire l'accesso al progetto. Per informazioni dettagliate, vedere Configurare e aggiornare gli account di servizio.
- Abilitare l'accesso privato di Google. Per i dettagli, consultare Abilitare l'accesso privato di Google.

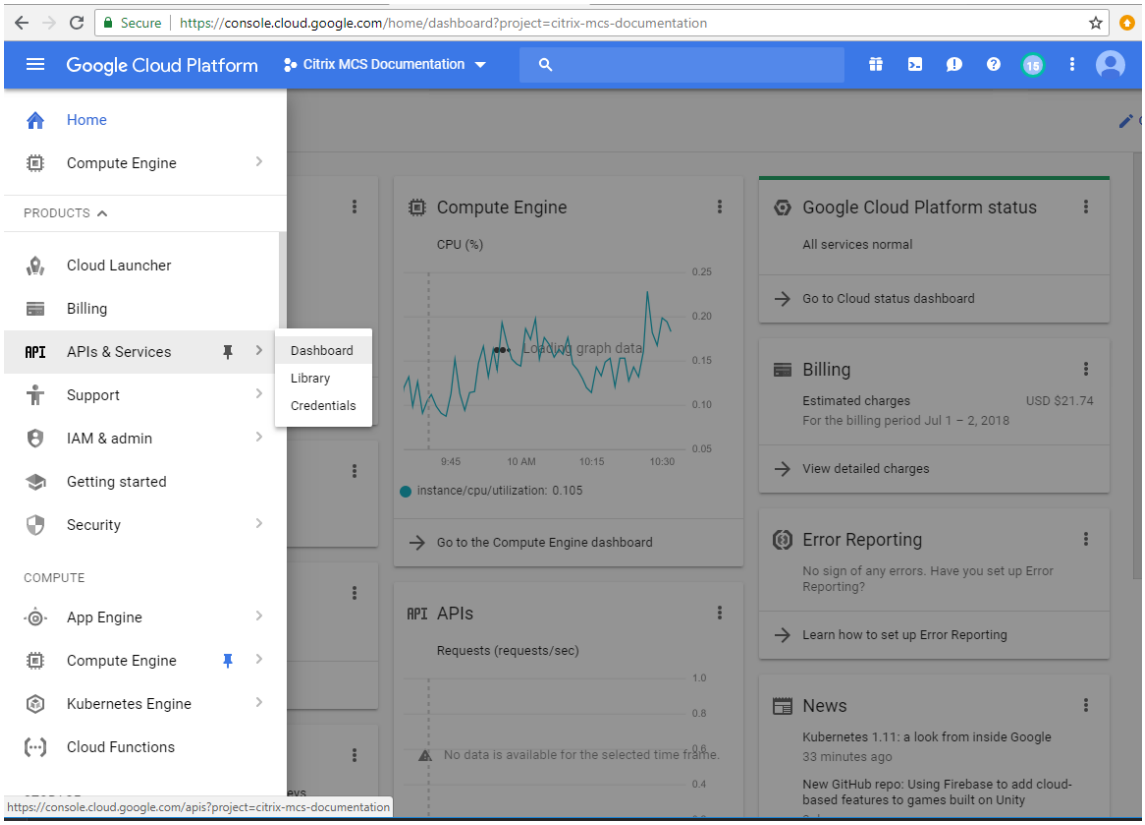
Abilitare le API di Google Cloud

Per utilizzare la funzionalità Google Cloud tramite Web Studio, abilitare queste API nel proprio progetto Google Cloud:

- API di Compute Engine
- API di Cloud Resource Manager
- API di Gestione delle identità e degli accessi (IAM)
- API Cloud Build
- Cloud Key Management Service (KMS)

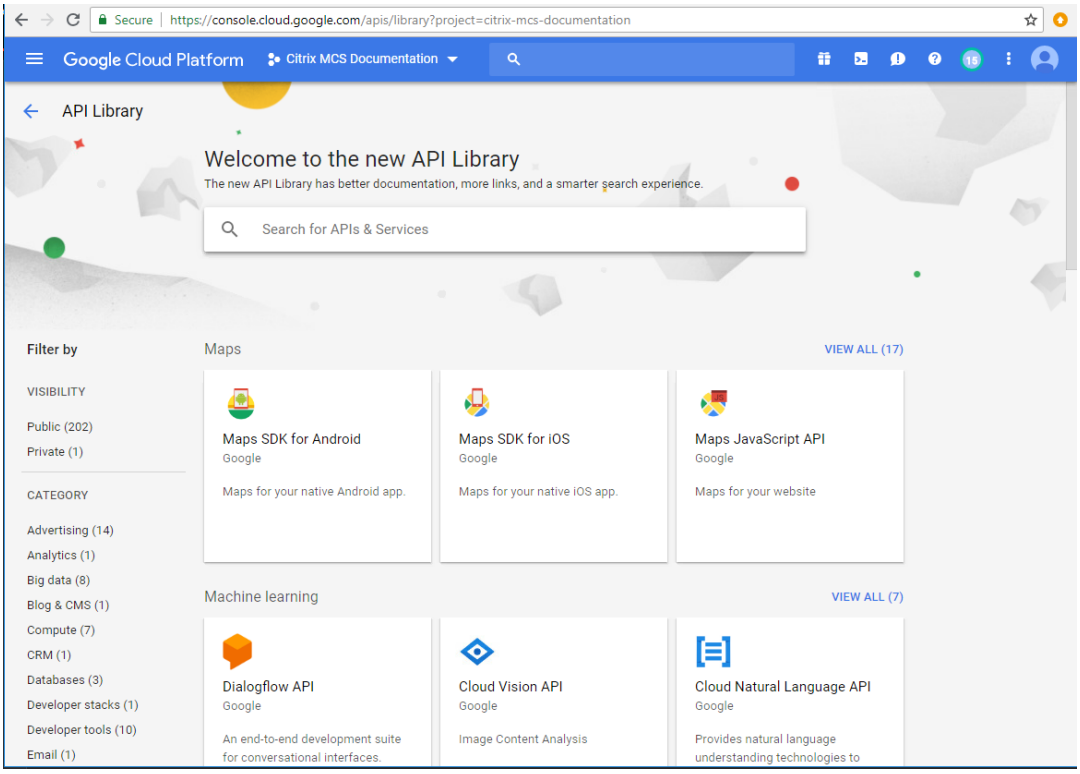
Dalla console di Google Cloud, completare questi passaggi:

1. Nel menu in alto a sinistra, selezionare **API e servizi > Dashboard**.



2. Nella schermata **Dashboard**, assicurarsi che l'API Compute Engine sia abilitata. In caso contrario, attenersi alla seguente procedura:

    a) Andare ad **API e servizi > Libreria**.



b) Nella casella di ricerca, digitare *Compute Engine*.

c) Dai risultati della ricerca, selezionare **Compute Engine API** (API Compute Engine).

d) Nella pagina **Compute Engine API** (API Compute Engine), selezionare **Abilita**.

3. Abilitare l'API Cloud Resource Manager.

   a) Andare ad **API e servizi > Libreria**.

   b) Nella casella di ricerca, digitare *Cloud Resource Manager*.

   c) Dai risultati della ricerca, selezionare **Cloud Resource Manager API** (API Cloud Resource Manager).

   d) Nella pagina **Cloud Resource Manager API** (API Cloud Resource Manager), selezionare **Abilita**. Viene visualizzato lo stato dell'API.

4. Allo stesso modo, abilitare **Identity and Access Management (IAM) API** (API Gestione dell'identità e degli accessi [IAM]) e **Cloud Build API** (API Cloud Build).

È anche possibile utilizzare Google Cloud Shell per abilitare le API. A questo scopo:

1. Aprire la Google Console e caricare Cloud Shell.
2. Eseguire i seguenti quattro comandi in Cloud Shell:

   - gcloud services enable compute.googleapis.com

- gcloud services enable cloudresourcemanager.googleapis.com
- gcloud services enable iam.googleapis.com
- gcloud services enable cloudbuild.googleapis.com

3. Fare clic su **Authorize** se richiesto da Cloud Shell.

Configurare e aggiornare gli account di servizio

Citrix Cloud utilizza tre account di servizio separati all'interno del progetto Google Cloud:

- *Account di servizio Citrix Cloud*: questo account di servizio consente a Citrix Cloud di accedere al progetto Google, di effettuare il provisioning e di gestire le macchine. L'account Google Cloud esegue l'autenticazione su Citrix Cloud utilizzando una chiave generata da Google Cloud.

  È necessario creare questo account di servizio manualmente.

  È possibile identificare questo account di servizio con un indirizzo e-mail. Ad esempio, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

  Ogni account (personale o di servizio) ha diversi ruoli che definiscono la gestione del progetto. Assegnare i seguenti ruoli a questo account di servizio:

  - Amministratore Compute
  - Amministratore archiviazione
  - Editor Cloud Build
  - Utente account di servizio
  - Utente di Cloud Datastore

- *Account del servizio Cloud Build*: questo account di servizio viene fornito automaticamente dopo aver abilitato tutte le API menzionate in Enable Google Cloud APIs (Abilita le API di Google Cloud).

  È possibile identificare questo account di servizio tramite un indirizzo e-mail che inizia con l'**ID del progetto** e la parola **cloudbuild**. Ad esempio, `<project-id>@cloudbuild.gserviceaccount.com`

  Assegnare i seguenti ruoli a questo account di servizio:

  - Account del servizio Cloud Build
  - Amministratore istanze Compute
  - Utente account di servizio

- *Account del servizio Cloud Compute*: questo account di servizio viene aggiunto da Google Cloud alle istanze create in Google Cloud una volta attivata l'API Compute. Questo account ha il ruolo

di editor di base IAM per eseguire le operazioni. Tuttavia, se si elimina l'autorizzazione predefinita per avere un controllo più granulare, è necessario aggiungere il ruolo **Storage Admin** che richiede le seguenti autorizzazioni:

- resourcemanager.projects.get
- storage.objects.create
- storage.objects.get
- storage.objects.list

È possibile identificare questo account di servizio tramite un indirizzo e-mail che inizia con l'ID del progetto e la parola compute. Ad esempio, `<project-id>-compute@developer.gserviceaccount.com`.

Creare un account Citrix Cloud Service

Per creare un account Citrix Cloud Service, effettuare le seguenti operazioni:

1. Nella console di Google Cloud, andare a **IAM e amministrazione > Account di servizio**.
2. Nella pagina **Account di servizio**, selezionare **CREA ACCOUNT DI SERVIZIO**.
3. Nella pagina **Create service account** (Crea account di servizio), immettere le informazioni richieste e quindi selezionare **CREATE AND CONTINUE** (CREA E CONTINUA).
4. Nella pagina **Grant this service account access to project** (Concedi a questo account di servizio l'accesso al progetto), fare clic sul menu a discesa **Select a role** (Seleziona un ruolo) e selezionare i ruoli richiesti. Fare clic su **+ADD ANOTHER ROLE** (+AGGIUNGI UN ALTRO RUOLO) se si desidera aggiungere altri ruoli.

   > **Nota:**
   >
   > Abilitare tutte le API per ottenere l'elenco completo dei ruoli disponibili durante la creazione di un nuovo account di servizio.

5. Fare clic su **CONTINUE** (Continua).
6. Nella pagina **Grant users access to this service account** (Concedi agli utenti l'accesso a questo account di servizio), aggiungere utenti o gruppi per concedere loro l'accesso necessario per eseguire azioni in questo account di servizio.
7. Fare clic su **DONE** (Fine).
8. Accedere alla console principale di IAM.
9. Identificare l'account di servizio creato.
10. Confermare che i ruoli sono stati assegnati correttamente.

Considerazioni:

Quando si crea l'account di servizio, tendere in considerazione quanto segue:

- I passaggi **Grant this service account access to project** (Concedi a questo account di servizio l'accesso al progetto) e **Grant users access to this service account** (Consenti agli utenti l'accesso a questo account di servizio) sono facoltativi. Se si sceglie di saltare questi passaggi di configurazione facoltativi, l'account di servizio appena creato non viene visualizzato nella pagina **IAM e amministrazione > IAM**.
- Per visualizzare i ruoli associati a un account di servizio, aggiungere i ruoli senza saltare i passaggi facoltativi. Questo processo garantisce la visualizzazione dei ruoli per l'account di servizio configurato.

Chiave dell'account Citrix Cloud Service Quando si crea un account di servizio, è disponibile un'opzione per creare una chiave per l'account. Questa chiave è necessaria quando si crea una connessione in Citrix Virtual Apps and Desktops. La chiave è contenuta in un file di credenziali (.json). Il file viene scaricato e salvato automaticamente nella cartella **Download** dopo aver creato la chiave. Quando si crea la chiave, assicurarsi di impostare il tipo di chiave su JSON. Altrimenti, Web Studio non può analizzarlo.

> **Suggerimento:**
>
> Creare chiavi utilizzando la pagina **Account di servizio** nella console di Google Cloud. Si consiglia di cambiare le chiavi regolarmente per motivi di sicurezza. È possibile fornire nuove chiavi all'applicazione Citrix Virtual Apps and Desktops modificando una connessione Google Cloud esistente.

Aggiungere ruoli all'account Citrix Cloud Service

Per aggiungere ruoli all'account Citrix Cloud Service:

1. Nella console di Google Cloud, andare a **IAM e amministrazione > IAM**.
2. Nella pagina **IAM > PERMISSIONS** (AUTORIZZAZIONI), individuare l'account di servizio creato, identificabile con un indirizzo e-mail.

   Ad esempio, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Selezionare l'icona a forma di matita per modificare l'accesso al principale dell'account del servizio.
4. Nella pagina **Edit access to "project-id"** (Modifica accesso a "project-id") per l'opzione principale selezionata, selezionare **ADD ANOTHER ROLE** (AGGIUNGI UN ALTRO RUOLO) per aggiungere i ruoli richiesti al proprio account di servizio uno per uno, quindi selezionare **SAVE** (SALVA).

Aggiungere ruoli all'account di servizio Cloud Build

Per aggiungere ruoli all'account di servizio Cloud Build:

1. Nella console di Google Cloud, andare a **IAM e amministrazione > IAM**.
2. Nella pagina **IAM**, individuare l'account di servizio Cloud Build, identificabile con un indirizzo e-mail che inizia con l'**ID del progetto** e la parola **cloudbuild**.

   Ad esempio, `<project-id>@cloudbuild.gserviceaccount.com`
3. Selezionare l'icona a forma di matita per modificare i ruoli dell'account Cloud Build.
4. Nella pagina **Edit access to "project-id"** (Modifica accesso a "project-id") per l'opzione principale selezionata, selezionare **ADD ANOTHER ROLE** (AGGIUNGI UN ALTRO RUOLO) per aggiungere i ruoli richiesti al proprio account di servizio Cloud Build uno per uno, quindi selezionare **SAVE** (SALVA).

   > **Nota:**
   >
   > Abilitare tutte le API per ottenere l'elenco completo dei ruoli.

Permessi di archiviazione e gestione dei bucket

Citrix Virtual Apps and Desktops migliora il processo di segnalazione degli errori di compilazione cloud per il servizio Google Cloud. Questo servizio esegue le compilazioni su Google Cloud. Citrix Virtual Apps and Desktops crea un bucket di archiviazione denominato `citrix-mcs-cloud-build-logs-{ region } -{ 5 random characters }` in cui i servizi Google Cloud acquisiscono le informazioni del log di compilazione. In questo bucket è impostata un'opzione che elimina i contenuti dopo un periodo di 30 giorni. Questo processo richiede che l'account di servizio utilizzato per la connessione abbia le autorizzazioni di Google Cloud impostate su `storage.buckets.update`. Se l'account di servizio non dispone di questa autorizzazione, Citrix Virtual Apps and Desktops ignora gli errori e procede con il processo di creazione del catalogo. Senza questa autorizzazione, la dimensione dei log di compilazione aumenta e richiede una pulizia manuale.

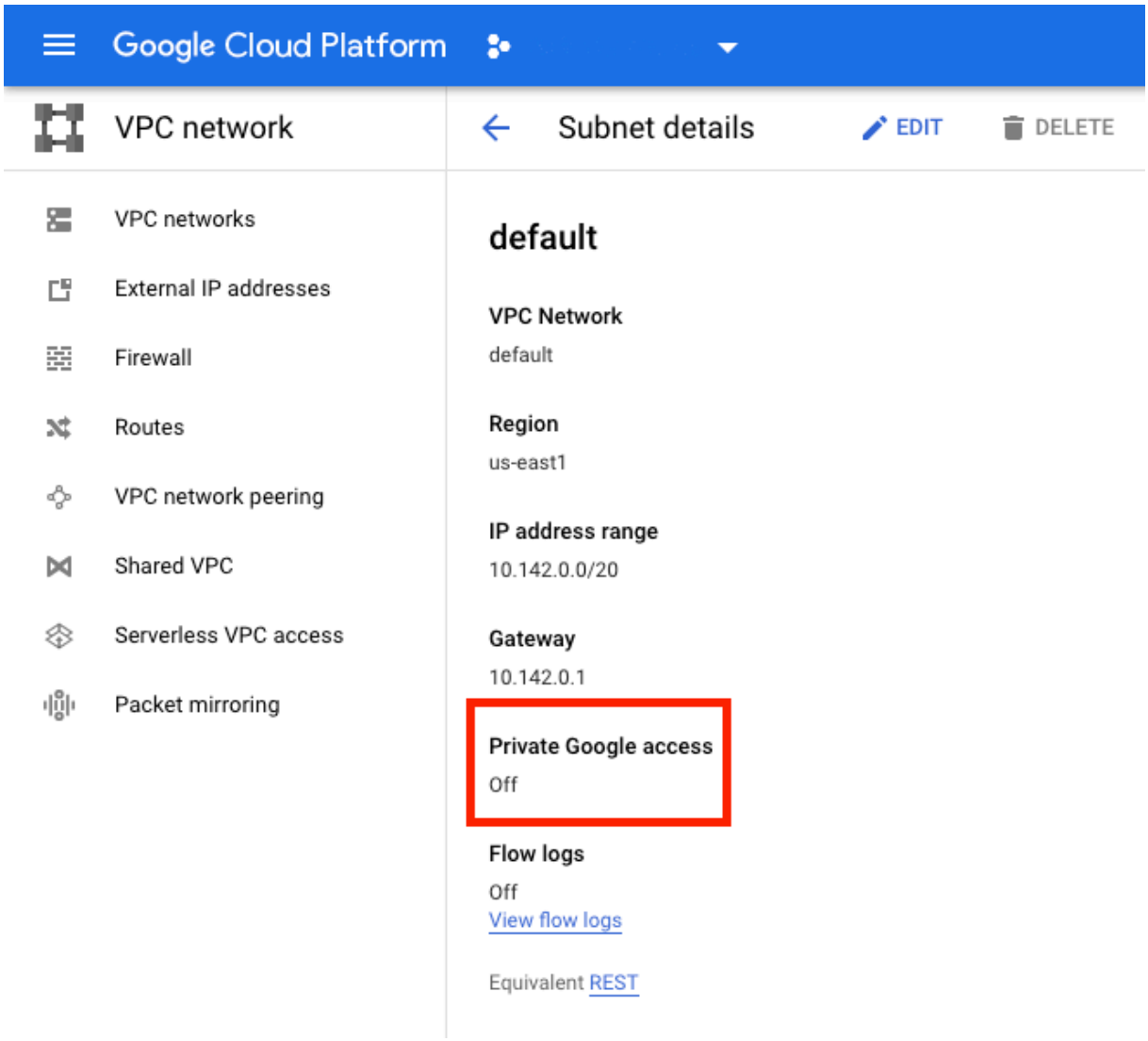
Abilitare l'accesso privato a Google

Quando una macchina virtuale non ha un indirizzo IP esterno assegnato alla relativa interfaccia di rete, i pacchetti vengono inviati solo ad altre destinazioni di indirizzi IP interni. Quando si abilita l'accesso privato, la macchina virtuale si connette all'insieme di indirizzi IP esterni utilizzati dall'API Google e dai servizi associati.

> **Nota:**
>
> Se l'accesso privato a Google è abilitato, tutte le macchine virtuali con e senza indirizzi IP pubblici devono essere in grado di accedere alle API pubbliche di Google, soprattutto se nell'ambiente sono stati installati dispositivi di rete di terze parti.

Per assicurare che una macchina virtuale nella subnet possa accedere alle API Google senza un indirizzo IP pubblico per il provisioning MCS:

1. In Google Cloud, accedere alla **configurazione della rete VPC**.
2. Nella schermata dei dettagli della subnet, attivare **Private Google access** (Accesso privato a Google).



Per ulteriori informazioni, consultare Configurazione dell'accesso privato a Google.

> **Importante:**
>
> Se la rete è configurata per impedire l'accesso delle macchine virtuali a Internet, assicurarsi che l'organizzazione si assuma i rischi associati all'abilitazione dell'accesso privato a Google per la subnet a cui è connessa la macchina virtuale.

Passaggi successivi

- Installare i componenti principali
- Installare i VDA
- Creare un sito
- Per creare e gestire una connessione negli ambienti Google Cloud, vedere Connessione agli ambienti cloud di Google

Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Creare cataloghi di macchine

Ambienti cloud Microsoft Azure Resource Manager

January 7, 2024

Quando si utilizza Microsoft Azure Resource Manager per eseguire il provisioning di macchine virtuali nella distribuzione del servizio Citrix Virtual Apps and Desktops, prendere dimestichezza con quanto segue:

- Azure Active Directory: https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/
- Framework di consenso: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/plan-an-application-integration
- Entità servizio: https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals/

Per configurare Microsoft Azure Resource Manager, vedere Preparazione per l'installazione.

Passaggi successivi

- Installare i componenti principali

- Installare i VDA
- Creare un sito
- Per creare e gestire una connessione in ambienti Azure, vedere Connessione a Microsoft Azure

Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Creare cataloghi di macchine
- CTX219211: Configurare un account Microsoft Azure Active Directory
- CTX219243: Concedere a XenApp e XenDesktop l'accesso alla sottoscrizione di Azure
- CTX219271: Distribuire il cloud ibrido utilizzando una VPN da sito a sito

Ambienti Microsoft System Center Configuration Manager

January 7, 2024

I siti che utilizzano Microsoft System Center Configuration Manager (Configuration Manager) per gestire l'accesso alle applicazioni e ai desktop possono estenderne l'uso a Citrix Virtual Apps and Desktops utilizzando le seguenti opzioni:

- Installare i VDA utilizzando SCCM.
- **Funzione proxy di riattivazione di Configuration Manager:** la funzione Riattivazione accesso remoto PC su LAN è supportata con Configuration Manager. Per i dettagli, vedere Riattivazione su LAN - SCCM integrato.
- **Proprietà di Citrix Virtual Apps and Desktops:** le Proprietà consentono di identificare Citrix Virtual Desktops per la gestione tramite Configuration Manager (in alcune versioni, Configuration Manager utilizza il nome precedente di Citrix Virtual Apps and Desktops: XenApp e XenDesktop).

Proprietà

Le proprietà sono disponibili per Microsoft System Center Configuration Manager per la gestione dei desktop virtuali.

Le proprietà booleane visualizzate in Configuration Manager vengono visualizzate come `1` o `0`, non true o false.

Le proprietà sono disponibili per la classe `Citrix_virtualDesktopInfo` nello spazio dei nomi `Root\Citrix\DesktopInformation`. I nomi delle proprietà provengono dal provider Strumentazione gestione Windows (WMI).

Proprietà	Descrizione
AssignmentType	Imposta il valore di IsAssigned. I valori validi sono: ClientIPClientName, None e User (imposta IsAssigned su True)
BrokerSiteName	Restituisce lo stesso valore di HostIdentifier
DesktopCatalogName	Catalogo macchine associato al desktop.
DesktopGroupName	Gruppo di consegna associato al desktop.
HostIdentifier	Restituisce lo stesso valore di BrokerSiteName.
IsAssigned	True per assegnare il desktop a un utente, impostare su False per un desktop casuale
IsMasterImage	Consente di prendere decisioni sull'ambiente. Ad esempio, installare le applicazioni nell'immagine e non sulle macchine con provisioning. I valori validi sono: True su una macchina virtuale utilizzata come immagine. Questo valore viene impostato durante l'installazione in base a una selezione o cancellato su una macchina virtuale di cui viene eseguito il provisioning da tale immagine.
IsVirtualMachine	True per una macchina virtuale, **false** per una macchina fisica.
OSChangesPersist	False se l'immagine del sistema operativo desktop viene ripristinata allo stato pulito ogni volta che viene riavviata; in caso contrario, **true**.
PersistentDataLocation	Posizione in cui Configuration Manager memorizza i dati persistenti. Questo non è accessibile agli utenti.
BrokerSiteName, DesktopCatalogName, DesktopGroupName, HostIdentifier	Determinato quando il desktop si registra con il controller. Sono nulli per un desktop che non è completamente registrato.

Per raccogliere le proprietà, eseguire un inventario hardware in Configuration Manager. Per visualizzare le proprietà, utilizzare Esplora risorse di Configuration Manager. In questi casi, i nomi includono spazi o variano leggermente dai nomi delle proprietà. Ad esempio, BrokerSiteName appare come

`Broker Site Name`.

- Configurare Configuration Manager per raccogliere le proprietà di Citrix WMI da Citrix VDA
- Creare raccolte di dispositivi basati su query utilizzando le proprietà di Citrix WMI
- Creare condizioni globali basate sulle proprietà di Citrix WMI
- Utilizzare le condizioni globali per definire i requisiti del tipo di distribuzione dell'applicazione

È inoltre possibile utilizzare le proprietà Microsoft nella classe `CCM_DesktopMachine` Microsoft nello spazio dei nomi `Root\ccm_vdi`. Per ulteriori informazioni, vedere la documentazione Microsoft.

Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager

January 7, 2024

Seguire queste indicazioni se si utilizza Hyper-V con Microsoft System Center Virtual Machine Manager (VMM) per fornire macchine virtuali.

Questa versione supporta le versioni di VMM elencate in Requisiti di sistema.

> **Nota:**
>
> I cluster Hyper-V misti (contenenti server che eseguono versioni di Hyper-V diverse) non sono supportati.

È possibile utilizzare Citrix Provisioning (in precedenza Provisioning Services) e Machine Creation Services per eseguire il provisioning di quanto segue:

- Macchine virtuali con sistema operativo desktop o server supportate di generazione 1.
- Macchine virtuali con sistema operativo desktop o server supportate di seconda generazione, incluso il supporto dell'avvio sicuro.

Installare e configurare un hypervisor

> **Importante:**
>
> Tutti i Delivery Controller devono trovarsi nella stessa foresta dei server VMM.

1. Installare il server Microsoft Hyper-V e VMM sui server.
2. Installare la console di System Center Virtual Machine Manager in tutti i controller. La versione della console deve corrispondere alla versione del server di gestione. Sebbene una console

precedente possa connettersi al server di gestione, il provisioning dei VDA non riesce se le versioni sono diverse.

3. Verificare le seguenti informazioni sull'account:

   L'account utilizzato per specificare gli host in Studio è un amministratore VMM o un amministratore delegato VMM per i computer Hyper-V pertinenti. Se questo account ha solo il ruolo di amministratore delegato in VMM, i dati di archiviazione non vengono elencati in Studio durante il processo di creazione dell'host.

   L'account utente utilizzato per l'integrazione in Studio deve anche essere membro del gruppo di protezione locale degli amministratori in ogni server Hyper-V. Questa configurazione supporta la gestione del ciclo di vita delle macchine virtuali, ad esempio la creazione, l'aggiornamento e l'eliminazione di macchine virtuali.

   L'installazione di un controller in un server che esegue Hyper-V non è supportata.

Nelle implementazioni di grandi dimensioni in cui un singolo SCVMM gestisce più cluster in diversi data center, è possibile limitare l'ambito degli amministratori delegati dei gruppi host.

Per limitare l'ambito dei gruppi di host, utilizzare il ruolo di amministratore delegato nella console di Microsoft System Center Virtual Machine Manager (VMM):

1. In **Create User Roles Wizard** (Creazione guidata di creazione ruoli utente), selezionare Fabric Administrator (Delegated Administrator) come ruolo utente.
2. In **Members**, aggiungere l'account utente in Active Directory che si desidera utilizzare come amministratore delegato.
3. In **Scope**, selezionare i gruppi host a cui si desidera che l'amministratore delegato abbia accesso.
4. Creare un nuovo **account Esegui come** utilizzando le credenziali utente dell'amministratore delegato. Utilizzare queste credenziali per creare una connessione hypervisor in un secondo momento. Non utilizzare gli account con ruolo di amministratore principale.

Effettuare il provisioning di Azure Stack HCI tramite SCVMM

Azure Stack HCI è una soluzione cluster di infrastruttura iperconvergente (HCI) che ospita i carichi di lavoro Windows e Linux virtualizzati e la relativa archiviazione in un ambiente ibrido locale.

I servizi ibridi di Azure migliorano il cluster dotandolo di funzionalità come il monitoraggio basato su cloud, il ripristino del sito e i backup delle macchine virtuali. È anche possibile ottenere una visione centrale di tutte le distribuzioni di Azure Stack HCI nel portale di Azure.

Integrazione di Azure Stack HCI con SCVMM

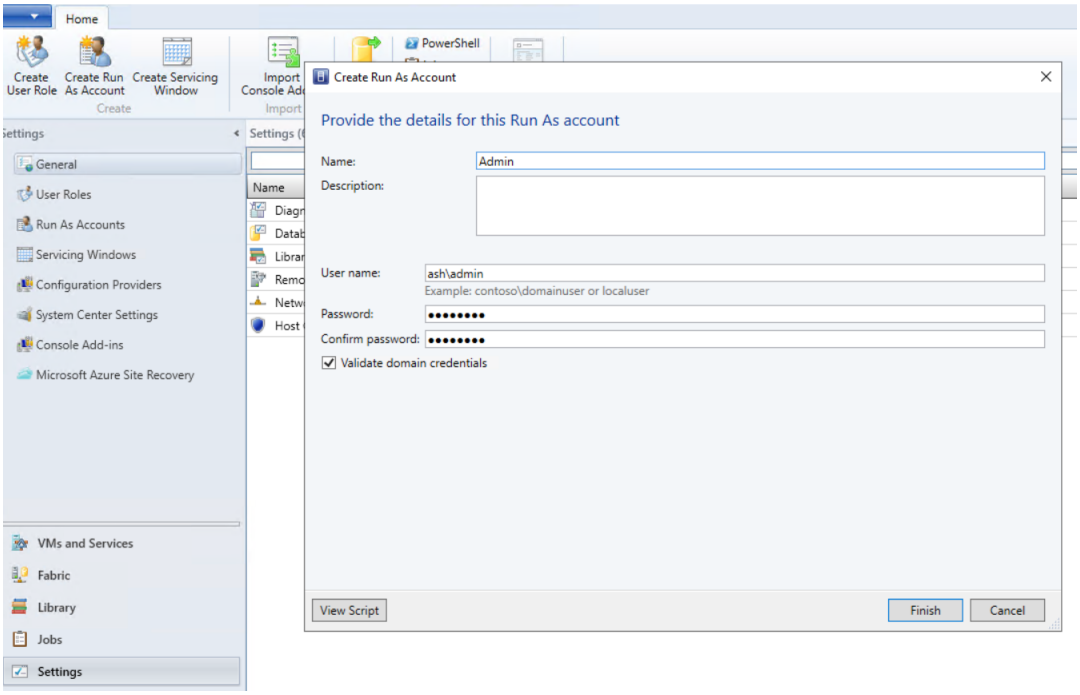
Per integrare Azure Stack HCI con SCVMM, è prima necessario creare un cluster HCI di Azure Stack e quindi integrare quel cluster con SCVMM.

1. Per creare il cluster HCI di Azure Stack, vedere il documento Microsoft Connettersi e gestire la registrazione di Azure Stack HCI.
2. Per integrare il cluster HCI di Azure Stack con SCVMM, effettuare le seguenti operazioni:

   a) Accedere alla macchina preparata per ospitare il server SCVMM e installare SCVMM 2019 UR3 o versione successiva.

   > **Nota:**
   >
   > Installare la Console di amministrazione SCVMM 2019 UR3 o versione successiva su tutti i controller.

   b) Nella pagina **Settings** (Impostazioni) della console VMM, creare un account Esegui come.

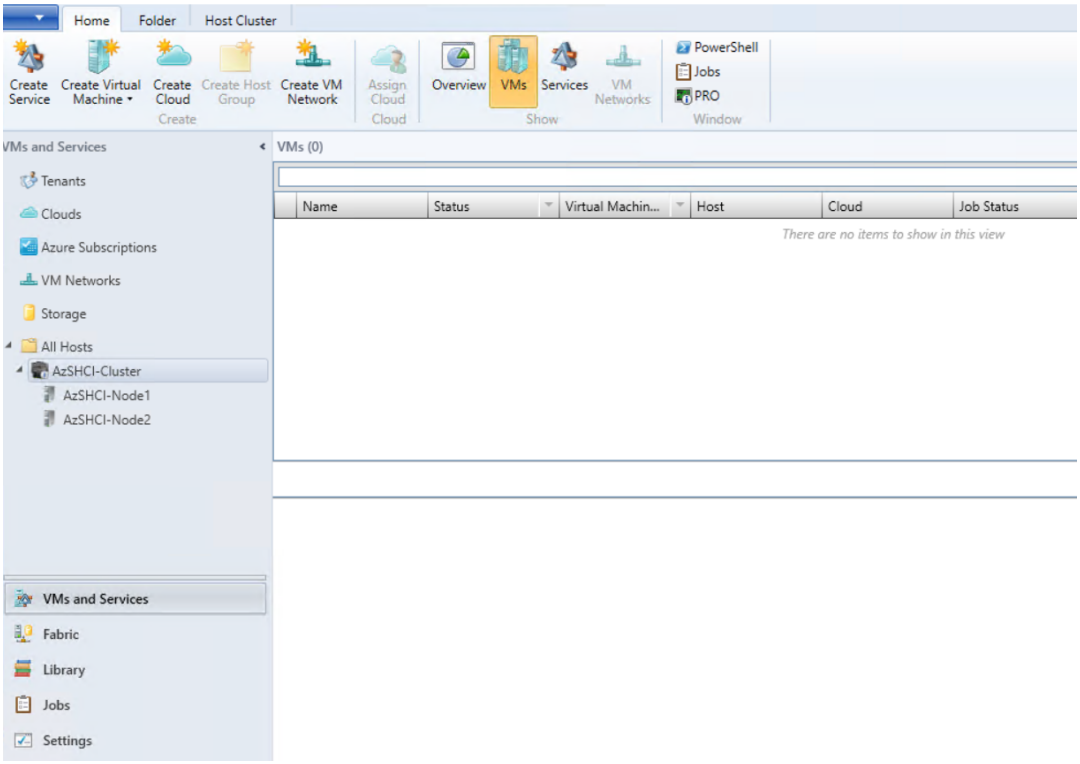
   c) Eseguire i seguenti comandi PowerShell con privilegi amministrativi nel server SCVMM per aggiungere il cluster HCI di Azure Stack come host:

```
$runAsAccountName = 'Admin'
$runAsAccount = Get-SCRunAsAccount -Name $runAsAccountName
$hostGroupName = 'All Hosts'
$hostGroup = Get-SCVMHostGroup -Name $hostGroupName
$hostCluster = 'FQDN of Azure Stack HCI cluster'
Add-SCVMHostCluster -Name $hostCluster -RunAsynchronously -
    VMHostGroup
```



```
$hostGroup -Credential $runAsAccount -RemoteConnectEnabled
    $true
<!--NeedCopy-->
```

d) È ora possibile visualizzare il cluster HCI di Azure Stack insieme ai nodi nella console VMM.



e) Creare la connessione di hosting SCVMM in Web Studio.

Passaggi successivi

- Installare i componenti principali
- Installare i VDA
- Creare un sito
- Per informazioni su come creare e gestire una connessione in SCVMM, vedere Connessione a Microsoft System Center Virtual Machine Manager

Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Creare cataloghi di macchine

Ambienti di virtualizzazione Nutanix

January 7, 2024

Seguire queste indicazioni quando si utilizza Nutanix Acropolis per fornire macchine virtuali nella distribuzione di Citrix Virtual Apps and Desktops. Il processo di installazione include le seguenti attività:

- Installare e registrare il plug-in Nutanix nell'ambiente Citrix Virtual Apps and Desktops.
- Creare una connessione all'hypervisor Nutanix Acropolis.
- Creare un catalogo di macchine che utilizzi un'istantanea di un'immagine master creata sull'hypervisor Nutanix.

Per ulteriori informazioni, vedere la Guida all'installazione del plug-in Nutanix Acropolis MCS, disponibile presso il Portale di supporto Nutanix.

Installare e registrare il plug-in Nutanix

Completare la seguente procedura per installare e registrare il plug-in Nutanix su tutti i controller di consegna. Utilizzare Citrix Studio per creare una connessione con Nutanix. Quindi creare un catalogo di macchine che utilizzi un'istantanea di un'immagine master creata nell'ambiente Nutanix.

> **Suggerimento:**
>
> Consigliamo di arrestare, quindi riavviare Citrix Host Service, Citrix Broker Service e Machine Creation Services quando si installa o si aggiorna il plug-in Nutanix.

Per informazioni sull'installazione del plug-in Nutanix, vedere il sito della documentazione di Nutanix.

Passaggi successivi

- Installare i componenti principali
- Installare i VDA
- Creare un sito
- Per informazioni su come creare e gestire una connessione in ambienti Nutanix, vedere Connessione a Nutanix.

Ulteriori informazioni

- Creare e gestire connessioni e risorse

- Creare cataloghi di macchine

Soluzioni Nutanix Cloud e dei partner

January 7, 2024

Citrix Virtual Apps and Desktops supporta la seguente soluzione Nutanix Cloud e dei partner:

- Nutanix Cloud Clusters su AWS

Nutanix Cloud Clusters su AWS

Citrix Virtual Apps and Desktops supporta i Nutanix Cloud Clusters su AWS. I cluster Nutanix semplificano il modo in cui le applicazioni vengono eseguite su cloud privati o su più cloud pubblici. Per ulteriori informazioni su Nutanix Cloud Clusters su AWS, vedere Nutanix Cloud Clusters on AWS Deployment and User Guide.

> **Suggerimento:**
>
> Questo supporto offre le stesse funzionalità di un cluster locale Nutanix. È supportato solo un singolo cluster, *Prism Element*. Per ulteriori informazioni, vedere questa pagina.

Requisiti

Per utilizzare Nutanix Clusters on AWS sono necessari i seguenti elementi:

- Un account Nutanix.
- Un account AWS con le seguenti autorizzazioni:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Creare un cluster Nutanix

Per creare un cluster Nutanix:

1. Accedere all'account Nutanix.
2. Individuare l'opzione **Nutanix cluster** (Cluster Nutanix) e fare clic su **Launch** (Avvia). Si apre la **console Nutanix**. Per ulteriori informazioni, consultare Introduzione a Nutanix Clusters on AWS.

3. Scegliere di creare un **nuovo VPC**.

Il processo di creazione del cluster potrebbe non riuscire con i seguenti errori:

- Il cluster non è stato creato in un determinato periodo di tempo. Eliminazione del cluster.
- Host Nutanix Cluster - Nodo `XXXXXXXXXX: Instance i-xxxxxxxxxxxx: disable network interface source/dest check error.`
- Host Nutanix Cluster - Nodo `XXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info.`

Se la creazione del cluster non è riuscita:

- Provare a ricrearne uno in un'altra regione.
- Assicurarsi di eliminare Nutanix CloudFormation Stack (CFS) prima di riprovare.

Oltre ad altre risorse, Nutanix CFS crea:

- 1 VPC denominato *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16
- 2 subnet 10.0.128.0/24 e 10.0.129.0/24
- 1 gateway Internet
- 1 gateway NAT

Una volta creato il cluster, recuperare l'indirizzo del **Nutanix Prism**:

1. Andare alla **console Nutanix**.
2. In alto a destra nella console, passare il mouse sul link **Launch Prism Element** (Avvia Prism Element) e copiare l'URL.

Passaggi successivi

- Installare i componenti principali
- Installare i VDA
- Creare un sito
- Per informazioni su come creare e gestire una connessione del cloud Nutanix e delle soluzioni dei partner, vedere Connessione alle soluzioni Nutanix Cloud e dei partner.

Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Creare cataloghi di macchine

Ambienti di virtualizzazione VMware

January 7, 2024

Seguire queste indicazioni se si utilizza VMware per fornire macchine virtuali.

Installare vCenter Server e gli strumenti di gestione appropriati. Non viene fornito alcun supporto per il funzionamento della modalità collegata vSphere vCenter.

Se si prevede di utilizzare MCS, non disattivare la funzionalità Datastore Browser in vCenter Server (descritta in https://kb.vmware.com/s/article/2101567). Quando si disattiva questa funzionalità, MCS non funziona correttamente.

Passaggi successivi

- Installare i componenti principali
- Installare i VDA
- Creare un sito
- Per creare e gestire una connessione in ambienti VMware, vedere Connessione a VMware

Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Creare cataloghi di macchine

Soluzioni cloud VMware e dei partner

April 3, 2024

Citrix Virtual Apps and Desktops supporta le seguenti soluzioni VMware Cloud e dei partner:

- Soluzione Azure VMware (AVS)
- Google Cloud VMware Engine
- VMware Cloud on Amazon Web Services (AWS)

Integrazione con la soluzione Azure VMware (AVS)

Il servizio Citrix Virtual Apps and Desktops supporta AVS. AVS fornisce un'infrastruttura cloud contenente cluster vSphere creati dall'infrastruttura Azure. Sfruttare il servizio Citrix Virtual Apps and

Desktops per utilizzare AVS per il provisioning del carico di lavoro VDA nello stesso modo in cui si utilizzerebbe vSphere negli ambienti on-premise.

Configurare il cluster AVS

Per abilitare il servizio Citrix Virtual Apps and Desktops per l'utilizzo di AVS, eseguire i seguenti passaggi in Azure:

- Richiedere una quota host
- Registrare il provider di risorse Microsoft.AVS
- Elenco di controllo di rete
- Creare un cloud privato della soluzione Azure VMware
- Accedere a un cloud privato della soluzione Azure VMware
- Configurare la rete per il cloud privato VMware in Azure
- Configurare DHCP per la soluzione Azure VMware
- Aggiungere un segmento di rete nella soluzione Azure VMware
- Verificare l'ambiente della soluzione Azure VMware

Richiedere una quota host per i clienti del contratto Azure Enterprise Nella pagina **Guida e supporto** del portale di Azure, selezionare **Nuova richiesta di supporto**e includere le seguenti informazioni:

- Tipo di problema: tecnico
- Sottoscrizione: selezionare la propria sottoscrizione
- Servizio: Tutti i servizi > Soluzione Azure VMware
- Risorsa: domanda generale
- Riepilogo: è necessaria capacità
- Tipo di problema: problemi di gestione della capacità
- Sottotipo di problema: richiesta del cliente per quota/capacità host aggiuntiva

Nel campo **Description** (Descrizione) del ticket di supporto, includere le seguenti informazioni nella scheda **Details** (Dettagli):

- POC o implementazione in produzione
- Nome regione
- Numero di host
- Eventuali altri dettagli

> **Nota:**
>
> AVS richiede un minimo di tre host e consiglia di utilizzare una ridondanza di N+1 host.

Dopo aver specificato i dettagli per il ticket di supporto, selezionare **Controlla e crea** per inviare la richiesta ad Azure.

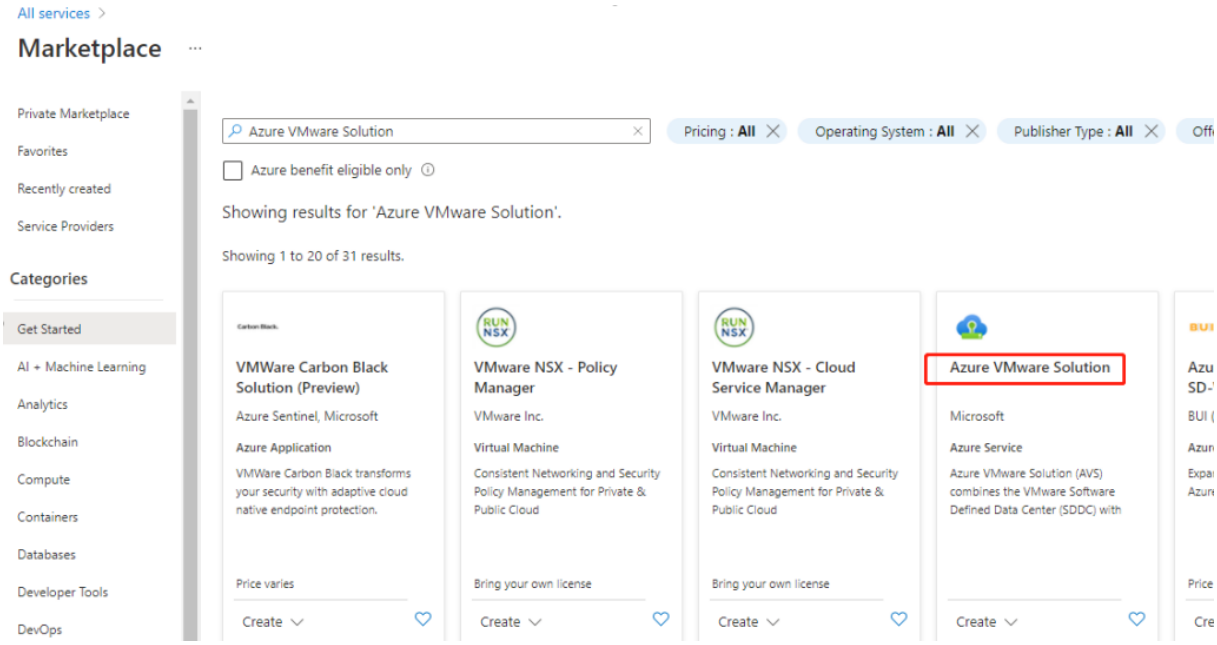
Registrare il provider di risorse Microsoft.AVS Dopo aver richiesto la quota host, registrare il provider di risorse:

1. Accedere al portale di Azure.
2. Nel menu del portale di Azure, selezionare **Tutti i servizi**.
3. Nel menu **Tutti i servizi**, inserire la sottoscrizione e selezionare **Sottoscrizioni**.
4. Selezionare la sottoscrizione dall'elenco delle sottoscrizioni.
5. Selezionare **Provider di risorse** e inserire **Microsoft.AVS** nella barra di ricerca.
6. Se il provider di risorse non è registrato, selezionare **Registra**.

Considerazioni sul networking AVS offre servizi di networking che richiedono specifici intervalli di indirizzi di rete e porte firewall. Vedere Elenco di controllo per la pianificazione della rete per la soluzione Azure VMware per ulteriori informazioni.

Creare un cloud privato della soluzione Azure VMware Dopo aver considerato i requisiti di rete per l'ambiente, creare un cloud privato ASV:

1. Accedere al portale di Azure.
2. Selezionare **Crea una nuova risorsa**.
3. Nella casella di testo **Cerca nel Marketplace**, digitare *Soluzione Azure VMware* e selezionare **Soluzione Azure VMware** dall'elenco.



Immagine

Nella finestra della **soluzione Azure VMware**:

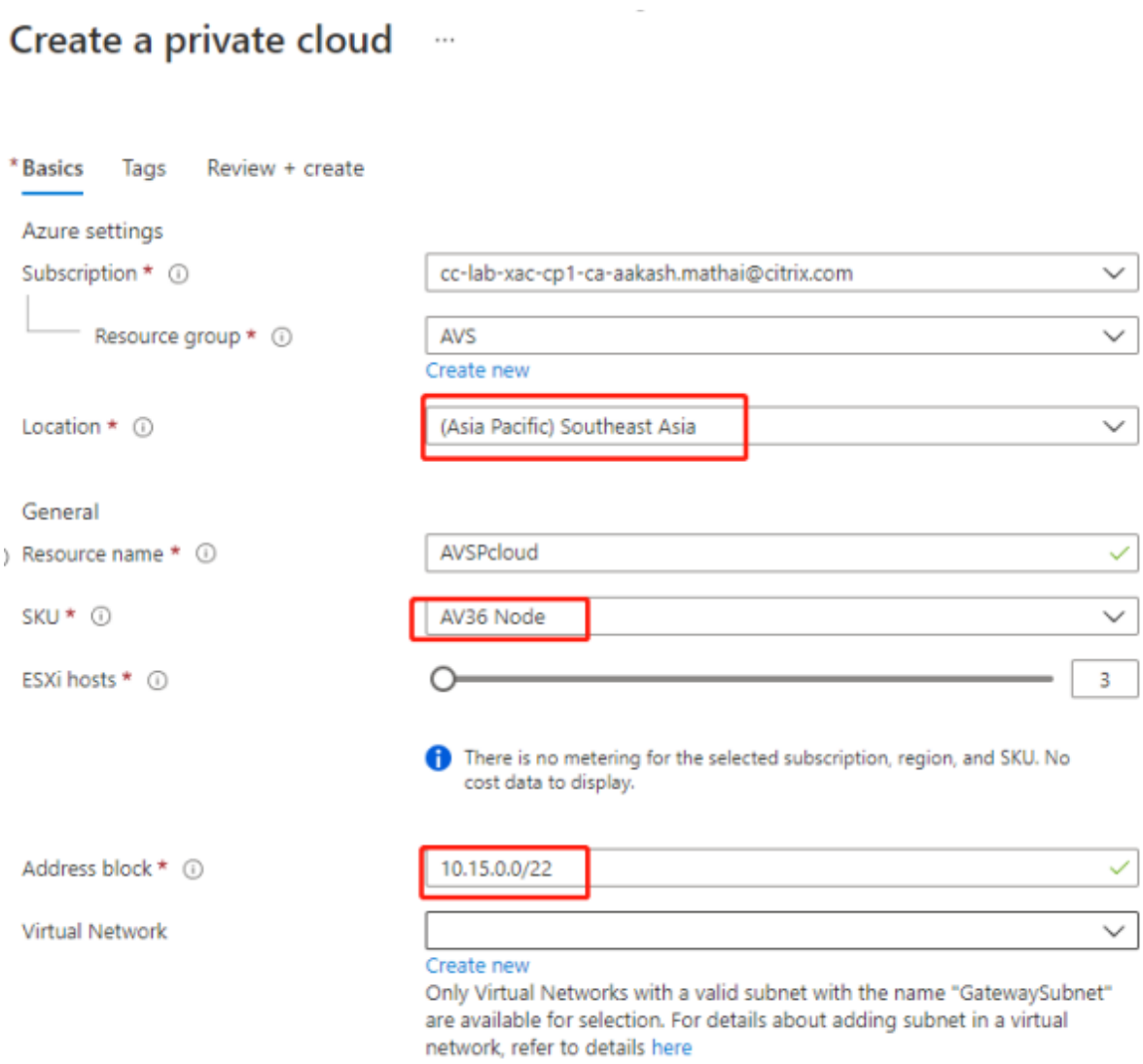
1. Selezionare **Crea**.
2. Fare clic sulla scheda **Informazioni di base**.
3. Immettere i valori per i campi, utilizzando le informazioni nella tabella seguente:

Campo	Valore
Sottoscrizione	Selezionare la sottoscrizione che si prevede di utilizzare per la distribuzione. Tutte le risorse in una sottoscrizione di Azure vengono fatturate insieme.
Gruppo di risorse	Selezionare il gruppo di risorse per il cloud privato. Un gruppo di risorse di Azure è un contenitore logico in cui vengono distribuite e gestite le risorse di Azure. In alternativa, è possibile creare un nuovo gruppo di risorse per il cloud privato.
Posizione	Selezionare una posizione, ad esempio "east us" (Stati Uniti orientali). Questa è la regione definita durante la fase di pianificazione.
Nome della risorsa	Fornire il nome del cloud privato della soluzione Azure VMware.
SKU	Selezionare AV36.
Host	Mostra il numero di host allocati per il cluster del cloud privato. Il valore predefinito è 3, che può essere aumentato o abbassato dopo la distribuzione.
Blocco di indirizzi	Fornire un blocco di indirizzi IP per il cloud privato. La notazione CIDR rappresenta la rete di gestione del cloud privato e verrà utilizzata per i servizi di gestione del cluster, come vCenter Server e NSX-T Manager. Utilizzare lo spazio degli indirizzi /22, ad esempio 10.175.0.0/22. L'indirizzo deve essere univoco e non sovrapporsi ad altre reti virtuali di Azure, oltre che alle reti on-premise.

Campo	Valore
Rete virtuale	Lasciare vuoto questo campo perché il circuito ExpressRoute della soluzione Azure VMware viene definito come passaggio successivo alla distribuzione.

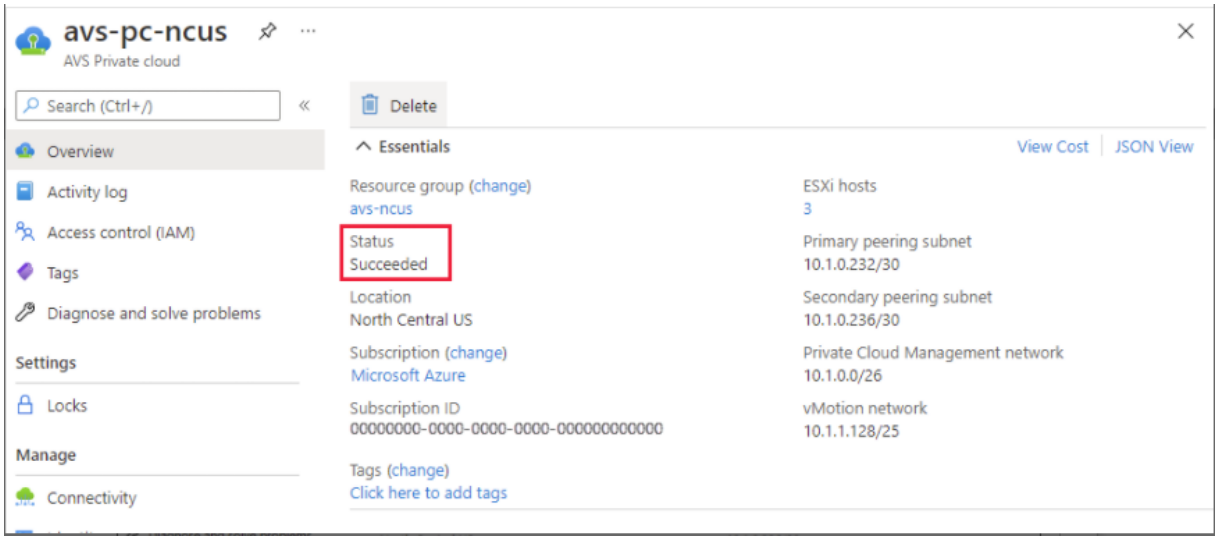
Nella schermata **Crea un cloud privato**:

1. Nel campo **Posizione**, selezionare la regione in cui si trova AVS; la regione del gruppo di risorse è la stessa della regione AVS.
2. Nel campo **SKU**, selezionare **Nodo AV36**.
3. Specificare un indirizzo IP nel campo **Blocco di indirizzi**. Ad esempio, 10.15.0.0/22.
4. Selezionare **Controlla e crea**.
5. Dopo aver esaminato le informazioni, fare clic su **Crea**.



> **Suggerimento:**
>
> La creazione di un cloud privato può richiedere 3-4 ore. L'aggiunta di un singolo host al cluster può richiedere 30-45 minuti.

Verificare che la distribuzione sia andata a buon fine. Andare al gruppo di risorse creato e selezionare il cloud privato. Quando lo **Stato** è **Operazione completata**, la distribuzione è completata.



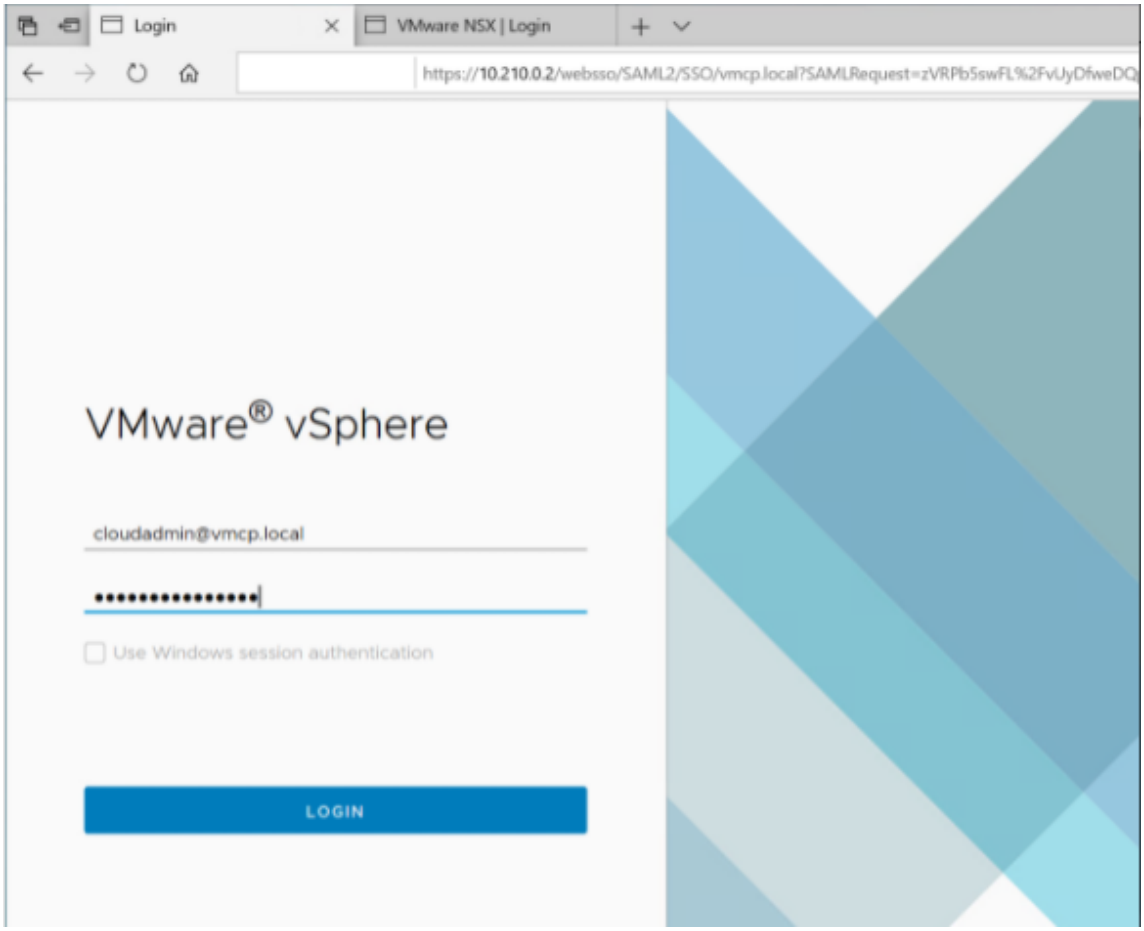
Accedere a un cloud privato della soluzione Azure VMware Dopo aver creato un cloud privato, creare una macchina virtuale Windows e connettersi al vCenter locale del cloud privato.

Creare una nuova macchina virtuale Windows

1. Nel gruppo di risorse, selezionare **+ Aggiungi**, quindi cercare e selezionare **Microsoft Windows 10/2016/2019**.
2. Fare clic su **Create** (Crea).
3. Inserire le informazioni richieste, quindi selezionare **Controlla e crea**.
4. Una volta superata la convalida, selezionare **Crea** per avviare il processo di creazione delle macchine virtuali.

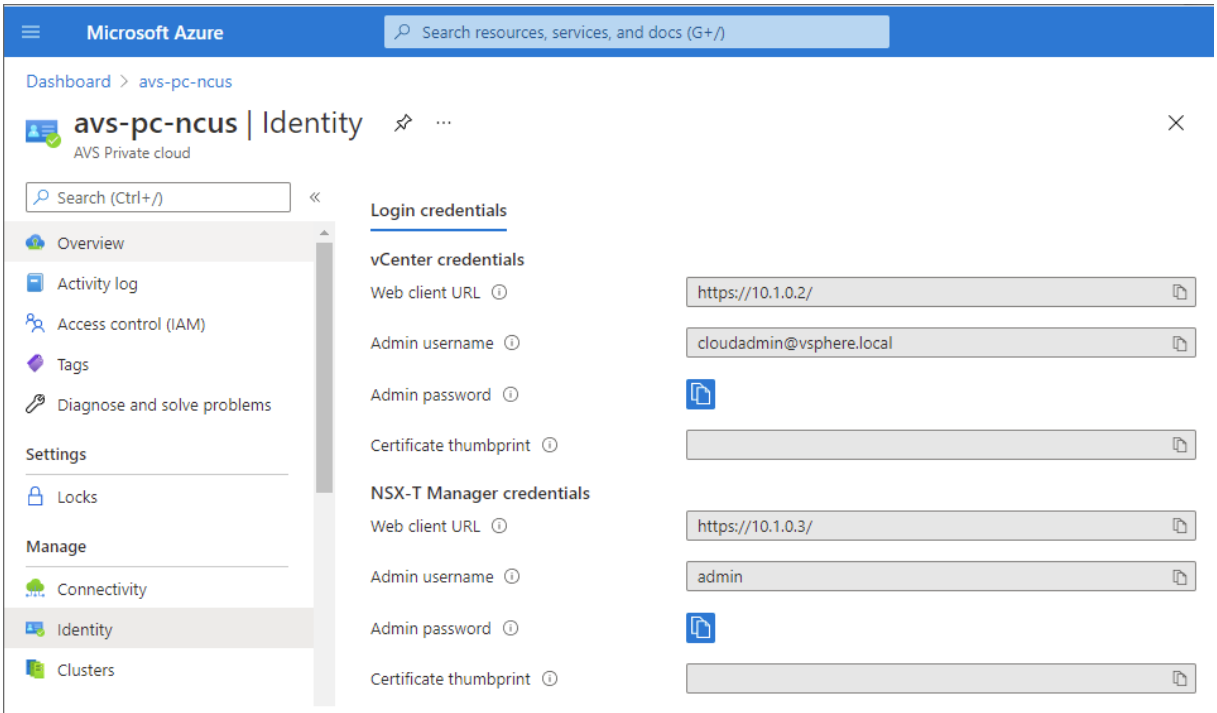
Connettersi al vCenter locale del cloud privato

1. Accedere a **vSphere Client con VMware vCenter SSO** come amministratore cloud.



2. Nel portale di Azure, selezionare il cloud privato, quindi **Gestisci > Identità**.

Vengono visualizzati gli URL e le credenziali utente per il cloud privato vCenter e NSX-T Manager:



Display private cloud vCenter and NSX Manager URLs and credentials.

Dopo aver confermato gli URL e le credenziali utente:

1. Accedere alla macchina virtuale creata nel passaggio precedente e connettersi alla macchina virtuale.
2. Nella macchina virtuale Windows, aprire un browser e accedere agli URL vCenter e NSX-T Manager in due schede del browser. Nella scheda vCenter, inserire le credenziali utente *cloudadmin@vmcp.local* dal passaggio precedente.

Configurare la rete per il cloud privato VMware in Azure Dopo aver effettuato l'accesso a un cloud privato ASV, configurare la rete creando una rete virtuale e un gateway.

Creare una rete virtuale

1. Accedere al portale di Azure.
2. Passare al gruppo di risorse creato in precedenza.
3. Selezionare **+ Aggiungi** per definire una nuova risorsa.
4. Nella casella di testo **Cerca nel Marketplace**, digitare *rete virtuale*. Trovare la risorsa di rete virtuale e selezionarla.
5. Nella pagina **Rete virtuale**, selezionare **Crea** per configurare la rete virtuale per il cloud privato.
6. Nella pagina **Crea rete virtuale**, inserire i dettagli della rete virtuale.
7. Nella scheda **Informazioni di base**, immettere un nome per la rete virtuale, selezionare la regione appropriata e fare clic su **Avanti: Indirizzi IP.**

8. Nella scheda **Indirizzi IP**, in Spazio indirizzi IPv4, immettere l'indirizzo creato in precedenza.

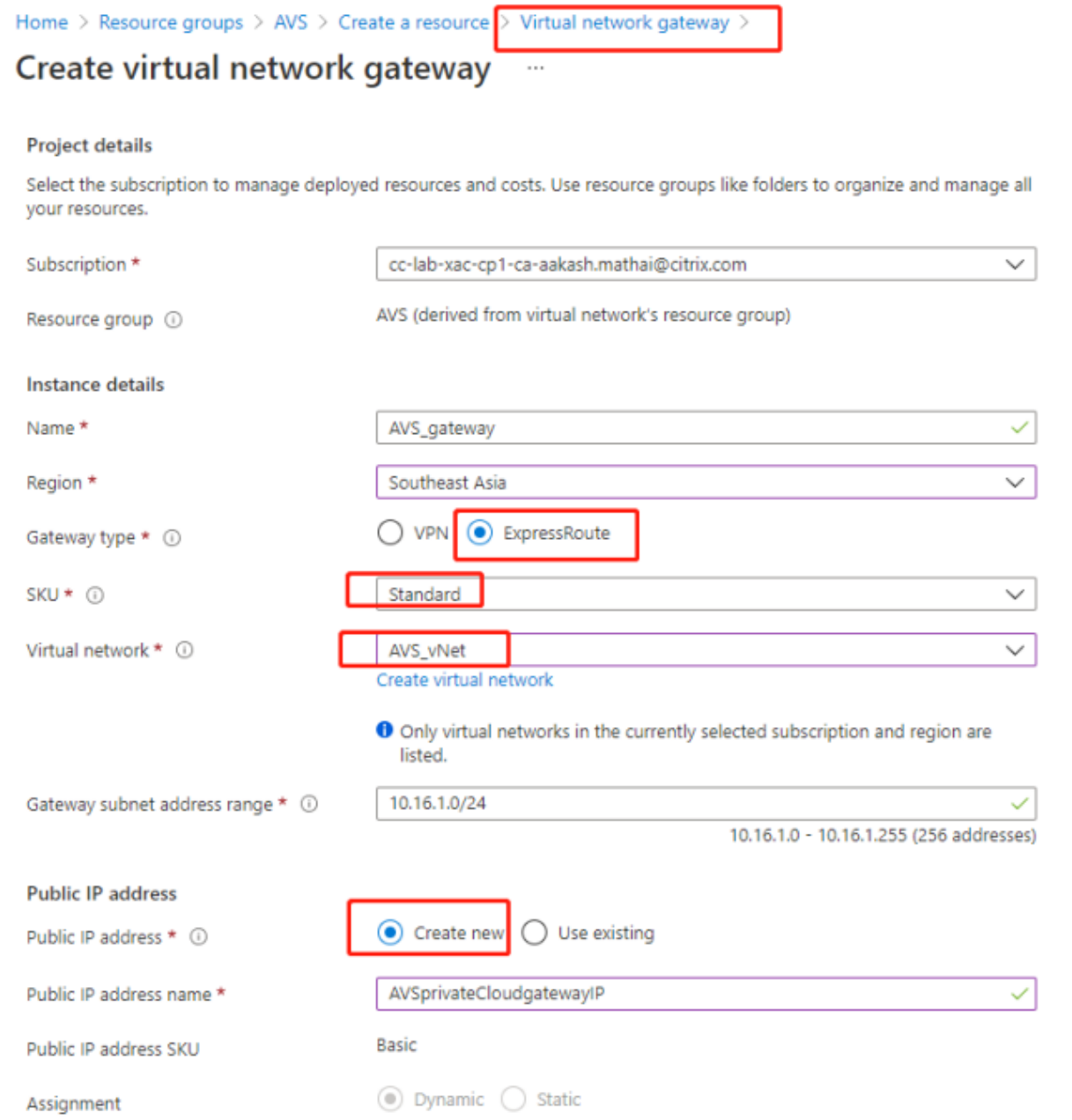
> **Importante:**
>
> Utilizzare un indirizzo che non si sovrapponga allo spazio degli indirizzi usato durante la creazione del cloud privato.

Dopo aver inserito lo spazio degli indirizzi:

1. Selezionare **+ Aggiungi subnet**.
2. Nella pagina **Aggiungi subnet**, assegnare alla subnet un nome e un intervallo di indirizzi appropriato.
3. Fare clic su **Aggiungi**.
4. Selezionare **Controlla e crea**.
5. Verificare le informazioni e fare clic su **Crea**. Una volta completata la distribuzione, la rete virtuale viene visualizzata nel gruppo di risorse.

Creare un gateway di rete virtuale Dopo aver creato una rete virtuale, creare un gateway di rete virtuale.

1. Nel gruppo di risorse, selezionare **+ Aggiungi** per aggiungere una nuova risorsa.
2. Nella casella di testo **Cerca nel Marketplace**, digitare *gateway di rete virtuale*. Trovare la risorsa di rete virtuale e selezionarla.
3. Nella pagina **Gateway di rete virtuale**, fare clic su **Crea**.
4. Nella scheda **Informazioni di base** della pagina **Crea gateway di rete virtuale**, fornire i valori per i campi.
5. Fare clic su **Controlla e crea**.

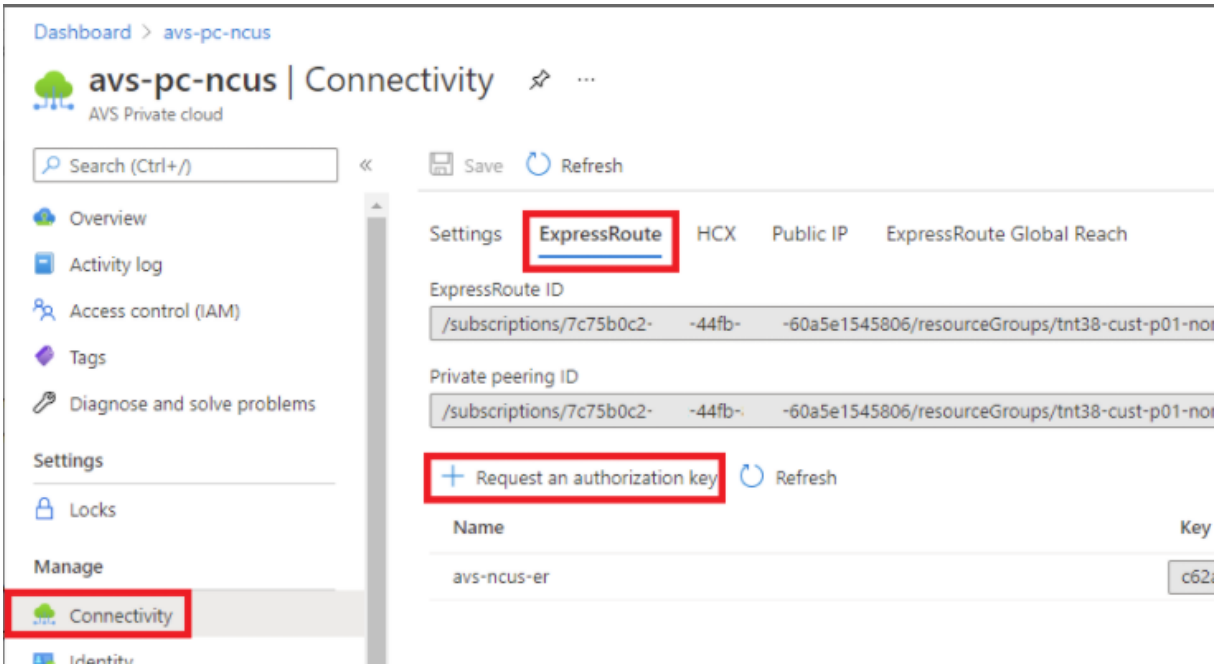


Dopo aver esaminato la configurazione del gateway di rete virtuale, fare clic su **Crea** per distribuire il gateway di rete virtuale.
Una volta completata la distribuzione, connettere la connessione **ExpressRoute** al gateway di rete virtuale contenente il cloud privato di Azure AVS.

Connettere ExpressRoute al gateway di rete virtuale Dopo aver distribuito un gateway di rete virtuale, aggiungere una connessione tra il gateway e il cloud privato di Azure AVS:

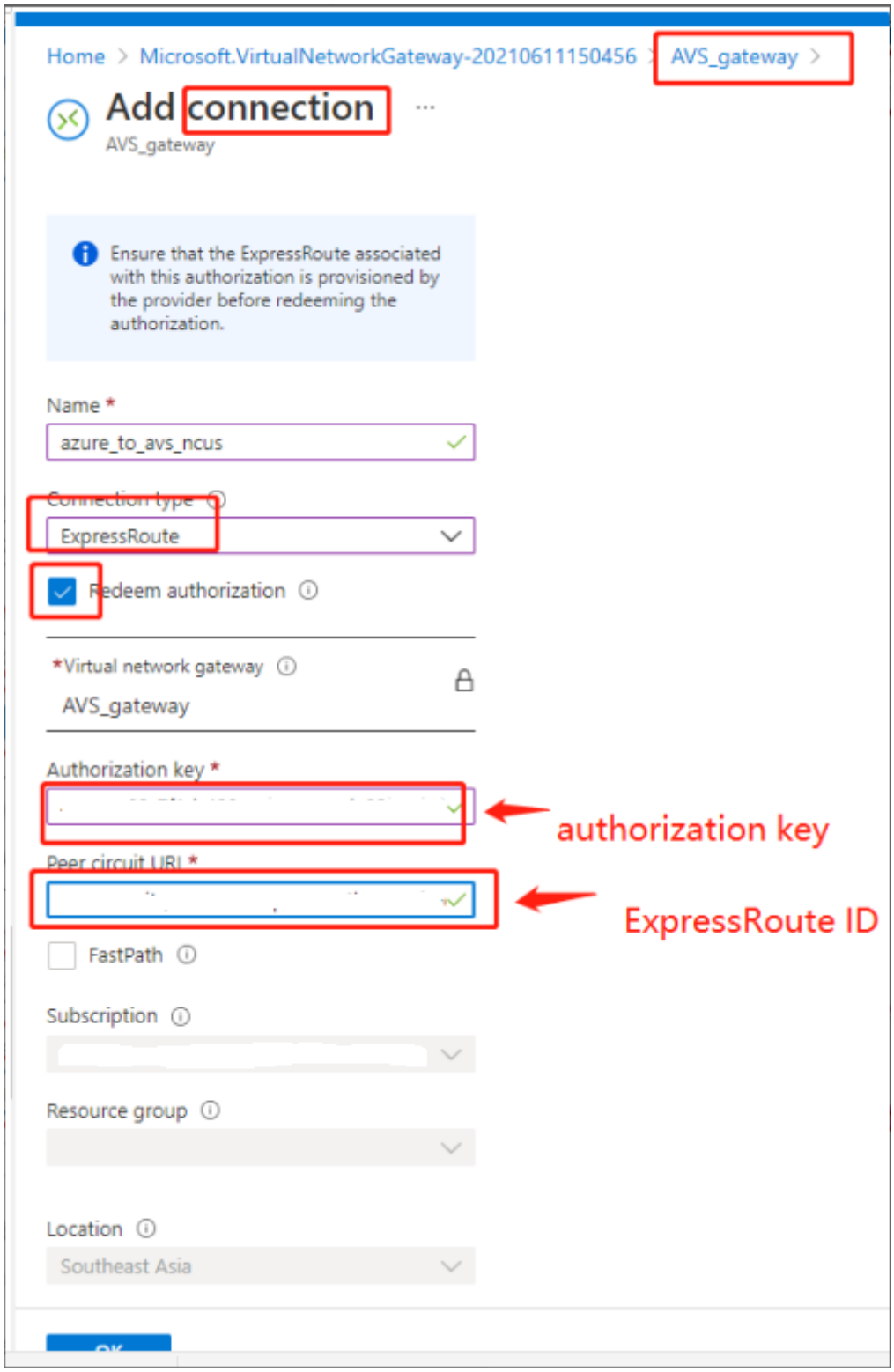
1. Richiedere una chiave di autorizzazione ExpressRoute.

2. Nel portale di Azure, accedere al **cloud privato della soluzione Azure VMware**. Selezionare **Gestisci > Connettività > ExpressRoute** e quindi selezionare **+ Richiedi una chiave di autorizzazione**.

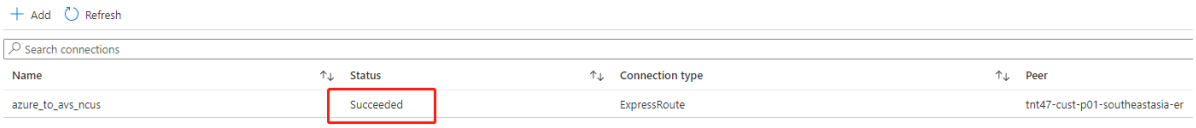


Dopo aver richiesto una chiave di autorizzazione:

1. Inserire un nome per la chiave e fare clic su **Crea**. Potrebbero essere necessari circa 30 secondi per creare la chiave. Una volta creata, la nuova chiave viene visualizzata nell'elenco delle chiavi di autorizzazione per il cloud privato.
2. Copiare la **chiave di autorizzazione** e l'**ID ExpressRoute**. Saranno necessari per completare il processo di peering. La chiave di autorizzazione scompare dopo un po'di tempo, quindi copiarla non appena viene visualizzata.
3. Accedere al **gateway di rete virtuale** che si intende utilizzare e selezionare **Connessioni > + Aggiungi**.
4. Nella pagina **Aggiungi connessione**, fornire i valori per i campi e selezionare **OK**.



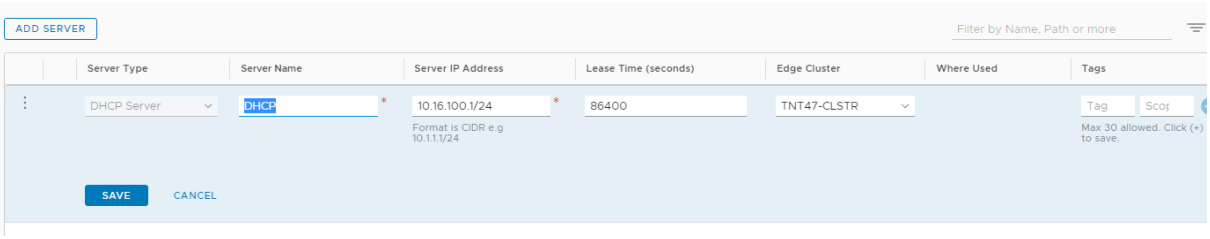
La connessione viene stabilita tra il circuito ExpressRoute e la rete virtuale:



Configurare DHCP per la soluzione Azure VMware Dopo aver connesso ExpressRoute al gateway virtuale, configurare DHCP.

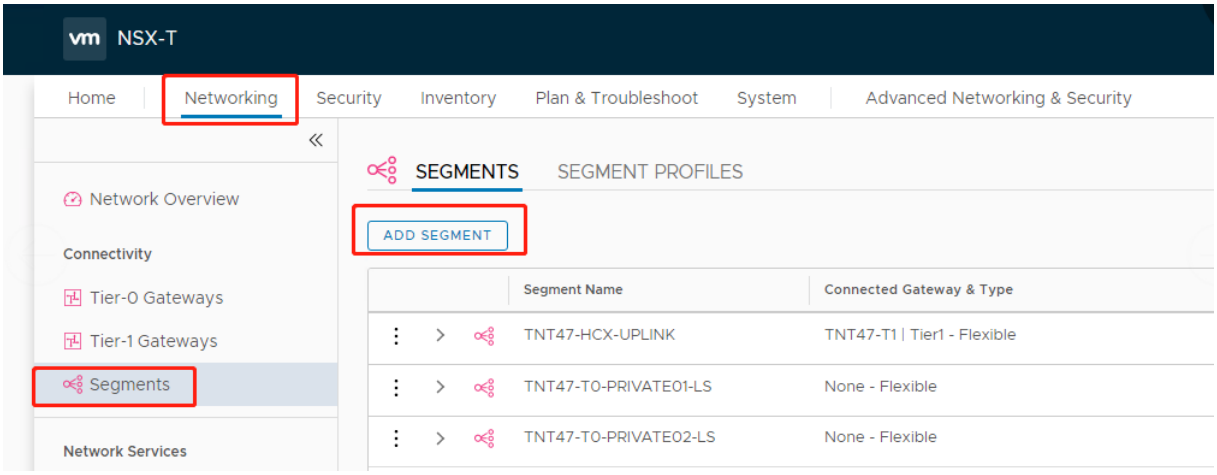
Utilizzare NSX-T per ospitare il server DHCP In NSX-T Manager:

1. Selezionare **Networking > DHCP** (Rete > DHCP), quindi selezionare **Add Server** (Aggiungi server).
2. Selezionare **DHCP** come **Server Type** (Tipo di server), fornire il nome del server e l'indirizzo IP.
3. Fare clic su **Salva**.
4. Selezionare **Tier 1 Gateways** (Gateway di livello 1), selezionare i puntini di sospensione verticali sul gateway di livello 1, quindi selezionare **Edit** (Modifica).
5. Selezionare **No IP Allocation Set** (Nessun set di allocazione IP) per aggiungere una subnet.
6. Selezionare **DHCP Local Server** (Server locale DHCP) per **Type** (Tipo).
7. Per **DHCP Server** (Server DHCP), selezionare **Default DHCP** (DHCP predefinito), quindi fare clic su **Save** (Salva).
8. Fare di nuovo clic su **Save** (Salva) e quindi selezionare **Close Editing** (Chiudi modifica).



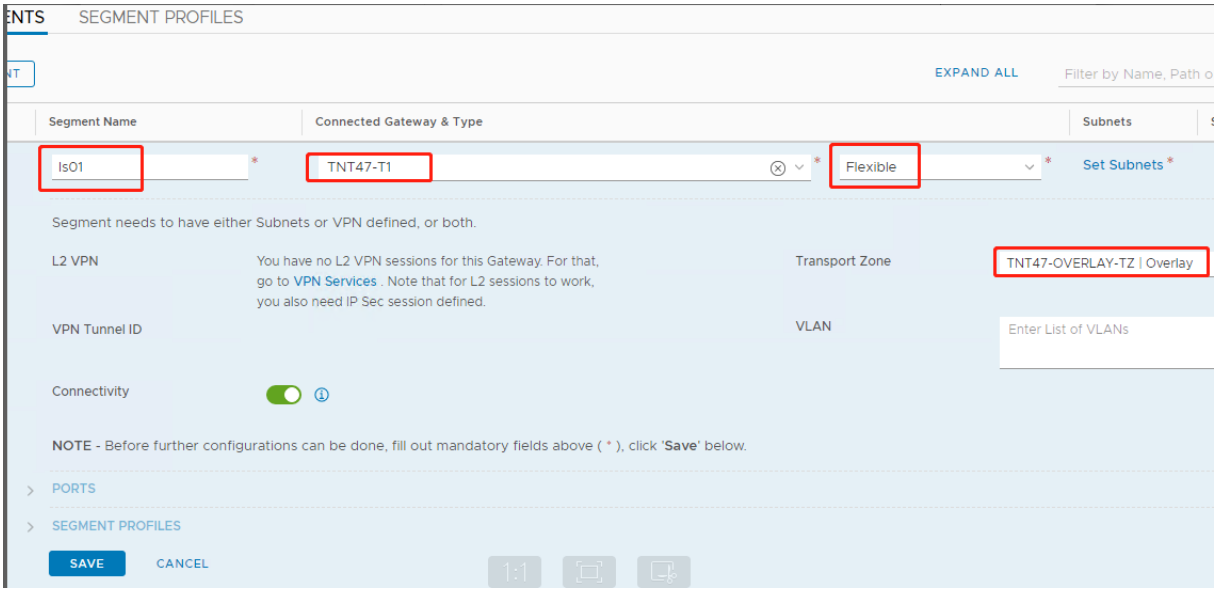
Aggiungere un segmento di rete nella soluzione Azure VMware Dopo aver configurato DHCP, aggiungere un segmento di rete.

Per aggiungere un segmento di rete, in NSX-T Manager selezionare **Networking > Segments** (Rete > Segmenti), quindi fare clic su **Add Segment** (Aggiungi segmento).



Nella schermata **Segments profile** (Profilo segmenti):

1. Immettere un **nome** per il segmento.
2. Selezionare **Tier-1 Gateway (TNTxx-T1)** (Gateway di livello 1 [TNTxx-T1]) come **Connected Gateway (Gateway connesso)** e lasciare **Type** (Tipo) impostato su **Flexible** (Flessibile).
3. Selezionare la sovrapposizione preconfigurata **Transport Zone(TNTxx-OVERLAY-TZ)** (Zona di trasporto [TNTxx-OVERLAY-TZ]).
4. Fare clic su **Set Subnets** (Imposta subnet).

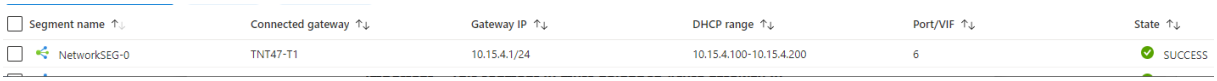


Nella sezione **Subnets** (Subnet):

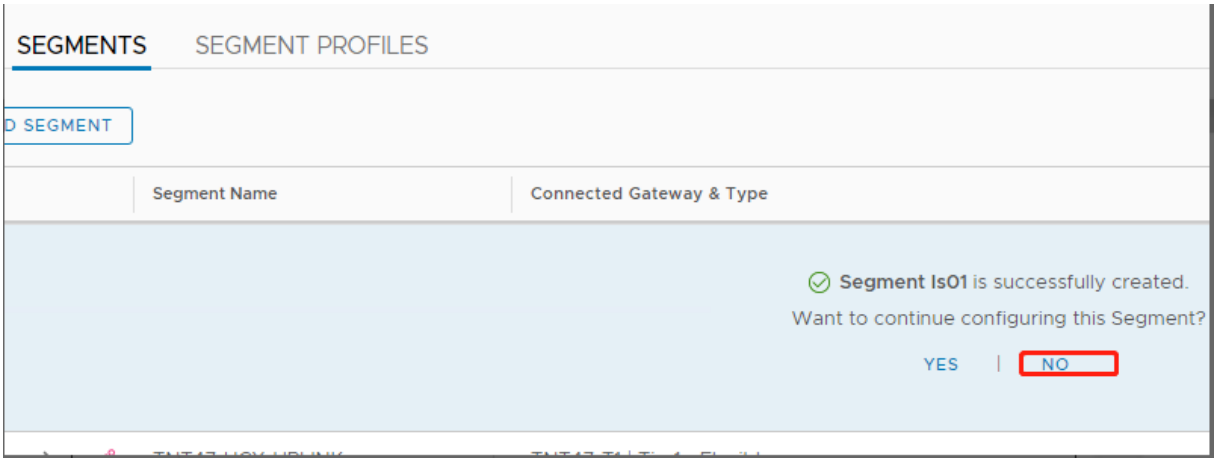
1. Immettere l'indirizzo IP del gateway.
2. Selezionare **Add** (Aggiungi).

> **Importante:**
>
> Questo indirizzo IP del segmento deve appartenere all'indirizzo IP del gateway Azure, 10.15.0.0/22.

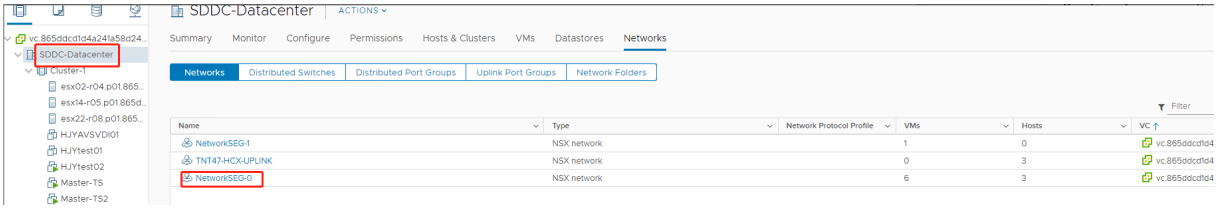
L'intervallo DHCP deve appartenere all'indirizzo IP del segmento:



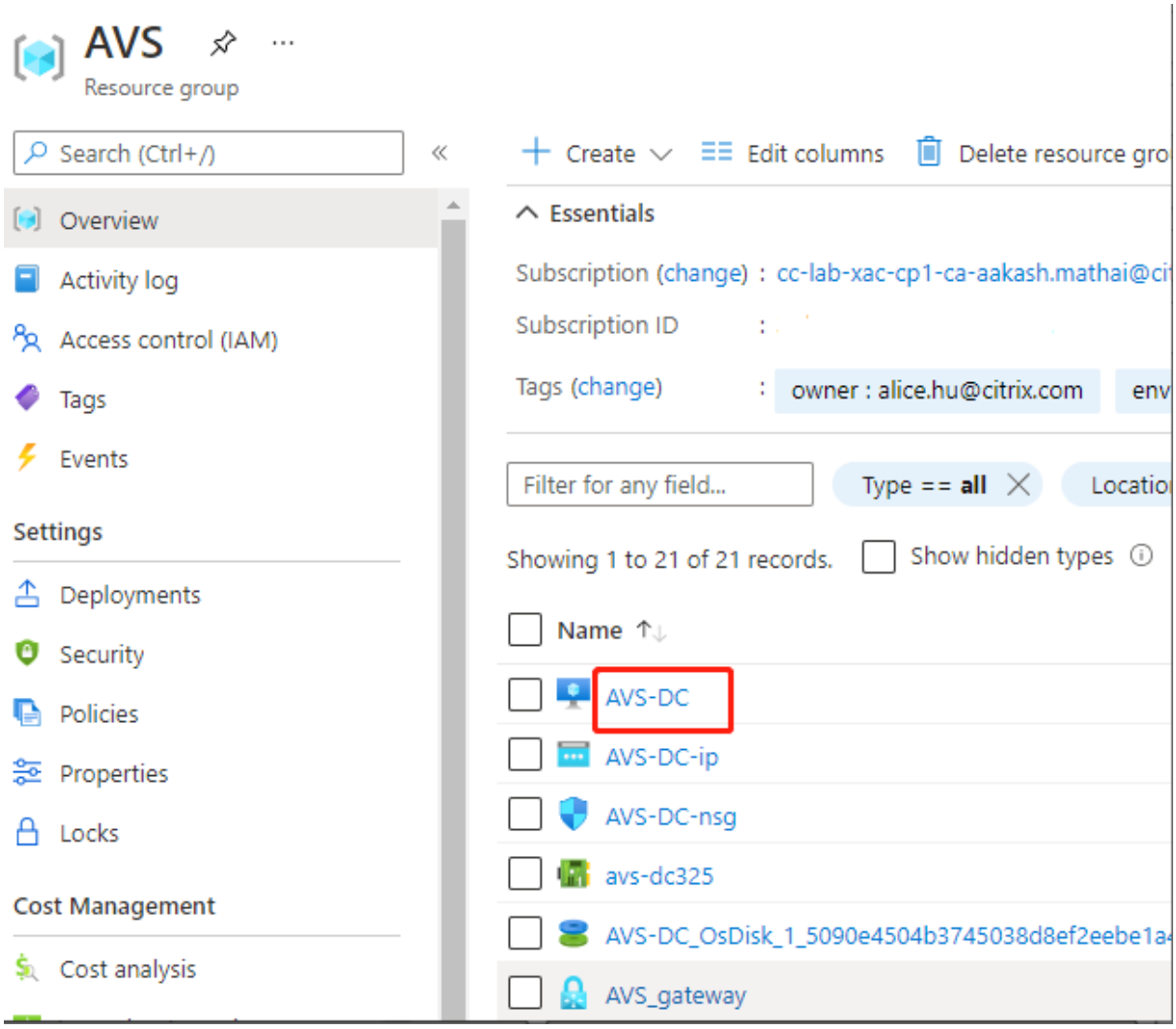
Selezionare **No** per rifiutare l'opzione per continuare a configurare il segmento:



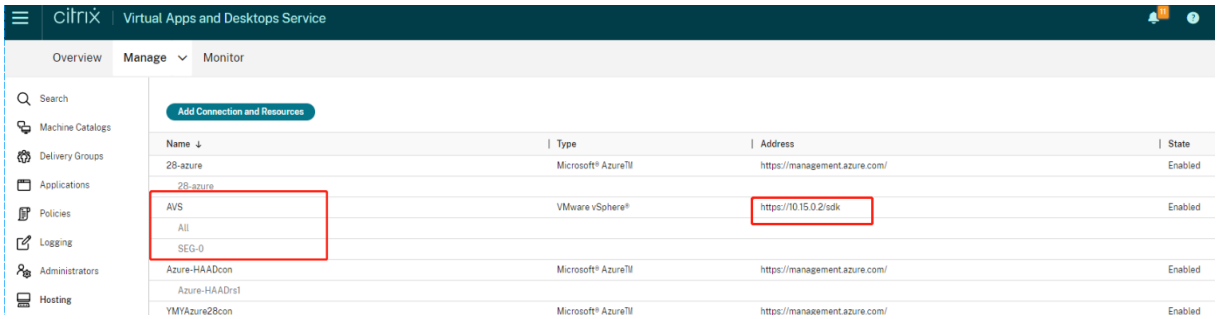
In vCenter, selezionare **Networking > SDDC-Datacenter** (Rete > SDDC-Datacenter):



Verificare l'ambiente Azure AVS Configurare una connessione diretta e un connettore nel gruppo di risorse di Azure:



Verificare la connessione con le credenziali vCenter:



Google Cloud VMware Engine

Citrix Virtual Apps and Desktops consente di migrare i carichi di lavoro Citrix locali basati su VMware a Google Cloud VMware Engine.

Configurare Google Cloud VMware Engine

La seguente procedura descrive come acquisire e configurare un cluster su Google Cloud VMware Engine.

Accedere al portale di VMware Engine

1. In **Google Cloud Console**, fare clic sul menu di navigazione.
2. Nella sezione **Computing**, fare clic su **VMware Engine** per aprire VMware Engine in una nuova scheda del browser.

Requisiti per creare il primo cloud privato È necessario avere accesso a Google Cloud VMware Engine, alla quota di nodi VMware Engine disponibile e a un ruolo IAM appropriato. Preparare i seguenti requisiti prima di continuare a creare il cloud privato:

1. Richiedere l'accesso all'API e la quota dei nodi. Per ulteriori informazioni, consultare Richiedere l'accesso all'API e la quota.
2. Annotare gli intervalli di indirizzi che si desidera utilizzare per le appliance di gestione VMware e la rete di distribuzione HCX. Per ulteriori informazioni, vedere Requisiti di rete.
3. Ottenere il ruolo IAM Amministratore servizio VMware Engine.

Creare il primo cloud privato

1. Accedere al portale di VMware Engine.
2. Nella home page di VMware Engine, fare clic su **Create a private cloud** (Crea un cloud privato). Sono elencati la posizione di hosting e i tipi di nodi hardware.
3. Selezionare il numero di nodi per il cloud privato. Sono necessari almeno tre nodi.
4. Immettere un intervallo CIDR (Classless Inter-Domain Routing) per la rete di gestione VMware.
5. Immettere un intervallo CIDR per la rete di distribuzione HCX.

   > **Importante:**
   >
   > L'intervallo CIDR non deve sovrapporsi a nessuna delle subnet on-premise o cloud. L'intervallo CIDR deve essere pari o superiore a /27.

6. Selezionare **Review and create** (Rivedi e crea).
7. Controllare le impostazioni. Per modificare le impostazioni, fare clic su **Back** (Indietro).
8. Fare clic su **Create** (Crea) per iniziare a creare il cloud privato.

Man mano che VMware Engine crea il nuovo cloud privato, distribuisce diversi componenti VMware e imposta i criteri iniziali di scalabilità automatica per i cluster nel cloud privato. La creazione di un cloud privato può richiedere da 30 minuti a 2 ore. Una volta completato il provisioning, si riceverà un' e-mail.

Configurare il gateway VPN di Google Cloud VMware Engine Per stabilire una connettività iniziale a Google Cloud VMware Engine, è possibile utilizzare un gateway VPN. Si tratta di una VPN client basata su OpenVPN che consente di connettersi al Software Defined Data Center (SDDC) VMware vCenter ed eseguire qualsiasi configurazione iniziale richiesta.

Prima di distribuire il gateway VPN, configurare l'intervallo di **servizi Edge** per l'area geografica in cui viene distribuito l'SDDC. A questo scopo:

1. Accedere al portale **Google Cloud VMware Engine** e andare a **Rete > Impostazioni regionali**. Fare clic su **Aggiungi area geografica**.
2. Scegliere l'area geografica in cui viene distribuito l'SDDC e abilitare l'**accesso a Internet** e il **servizio IP pubblico**.
3. Indicare l'intervallo dei servizi Edge di cui si è preso nota durante la pianificazione e fare clic su **Invia**. L'abilitazione di questi servizi richiede 10-15 minuti.

   Al completamento della procedura, i servizi Edge vengono visualizzati come **Abilitati** nella pagina Impostazioni regionali. L'abilitazione di queste impostazioni consente di allocare gli IP pubblici all'SDDC, che è un requisito per la distribuzione di un gateway VPN.

Per distribuire un gateway VPN:

1. Nel portale **Google Cloud VMware Engine**, andare a **Rete > Gateway VPN**. Fare clic su **Create New VPN Gateway** (Crea nuovo gateway VPN).
2. Fornire il nome per il gateway VPN e la subnet client riservati durante la pianificazione. Fare clic su **Next** (Avanti).
3. Selezionare gli utenti a cui concedere l'accesso alla VPN. Fare clic su **Next** (Avanti).
4. Specificare le reti che devono essere accessibili tramite VPN. Fare clic su **Next** (Avanti).
5. Viene visualizzata una schermata di riepilogo. Verificare le selezioni e fare clic su **Submit** (Invia) per creare il gateway VPN. La pagina VPN Gateways (Gateway VPN) viene visualizzata con lo stato del nuovo gateway VPN **Creating** (Creazione in corso).
6. Dopo che lo stato viene modificato in **Operational** (Operativo), fare clic sul nuovo gateway VPN.
7. Fare clic su **Download my VPN configuration** (Scarica la mia configurazione VPN) per scaricare un file ZIP contenente profili OpenVPN preconfigurati per il gateway VPN. Sono disponibili profili per la connessione tramite UDP/1194 e TCP/443. Scegliere la propria preferenza e importala in Open VPN, quindi connettersi.
8. Andare a **Resources** (Risorse) e seleziona il proprio SDDC.

Connettere la VPN

1. Stabilire una connessione da punto a sito tra la propria rete locale e il cloud privato tramite la configurazione VPN Gateway. Vedere Configurare il gateway VPN di Google Cloud VMware Engine.
2. Caricare la configurazione della VPN scaricata in Configurare il gateway VPN di Google Cloud VMware Engine.
3. Importarla nel proprio client VPN, ad esempio OpenVPN Connect.

Per ulteriori informazioni, vedere Connessione tramite VPN.

Creare la prima subnet

Accedere a NSX-T Manager dal portale VMware Engine Il processo di creazione di una subnet avviene in NSX-T, a cui si accede tramite VMware Engine. Effettuare le seguenti operazioni per accedere a NSX-T Manager.

1. Accedere al portale **Google Cloud VMware Engine**.
2. Dalla navigazione principale, andare a **Resources** (Risorse).
3. Fare clic sul **nome del cloud privato** corrispondente al cloud privato in cui si desidera creare la subnet.
4. Nella pagina dei dettagli del cloud privato, fare clic sulla scheda **vSphere Management Network** (Rete di gestione di vSphere).
5. Fare clic sul **nome di dominio completo** corrispondente a NSX-T Manager.
6. Quando richiesto, inserire le proprie credenziali di accesso. Se si è configurato vIDM e lo si è connesso a un'origine identità, ad esempio Active Directory, utilizzare invece le credenziali dell'origine identità.

   > **Promemoria:**
   >
   > È possibile recuperare le credenziali generate dalla pagina dei dettagli del cloud privato.

Configurare il servizio DHCP per la subnet Prima di poter creare una subnet, configurare un servizio DHCP:

In NSX-T Manager:

1. Andare a **Networking > DHCP**. La dashboard di rete mostra che il servizio DHCP crea un gateway Tier-0 e uno Tier-1.
2. Per iniziare il provisioning di un server DHCP, fare clic su **Add Server** (Aggiungi server).

3. Selezionare **DHCP** come **Server Type** (Tipo di server), fornire il nome del server e l'indirizzo IP.
4. Fare clic su **Save** (Salva) per creare il servizio DHCP.

Effettuare le seguenti operazioni per collegare questo servizio DHCP al gateway Tier-1 pertinente. Un gateway Tier-1 predefinito è già fornito dal servizio DHCP:

1. Selezionare **Tier 1 Gateways** (Gateway di livello 1), selezionare i puntini di sospensione verticali sul gateway di livello 1, quindi selezionare **Edit** (Modifica).
2. Nel campo **IP Address Management** (Gestione indirizzi IP), selezionare **No IP Allocation Set** (Nessuna allocazione IP impostata).
3. Selezionare **DHCP Local Server** (Server locale DHCP) per **Type** (Tipo).
4. Selezionare il server DHCP creato per il **server DHCP**.
5. Fare clic su **Salva**.
6. Fare clic su **Close Editing** (Chiudi modifica).

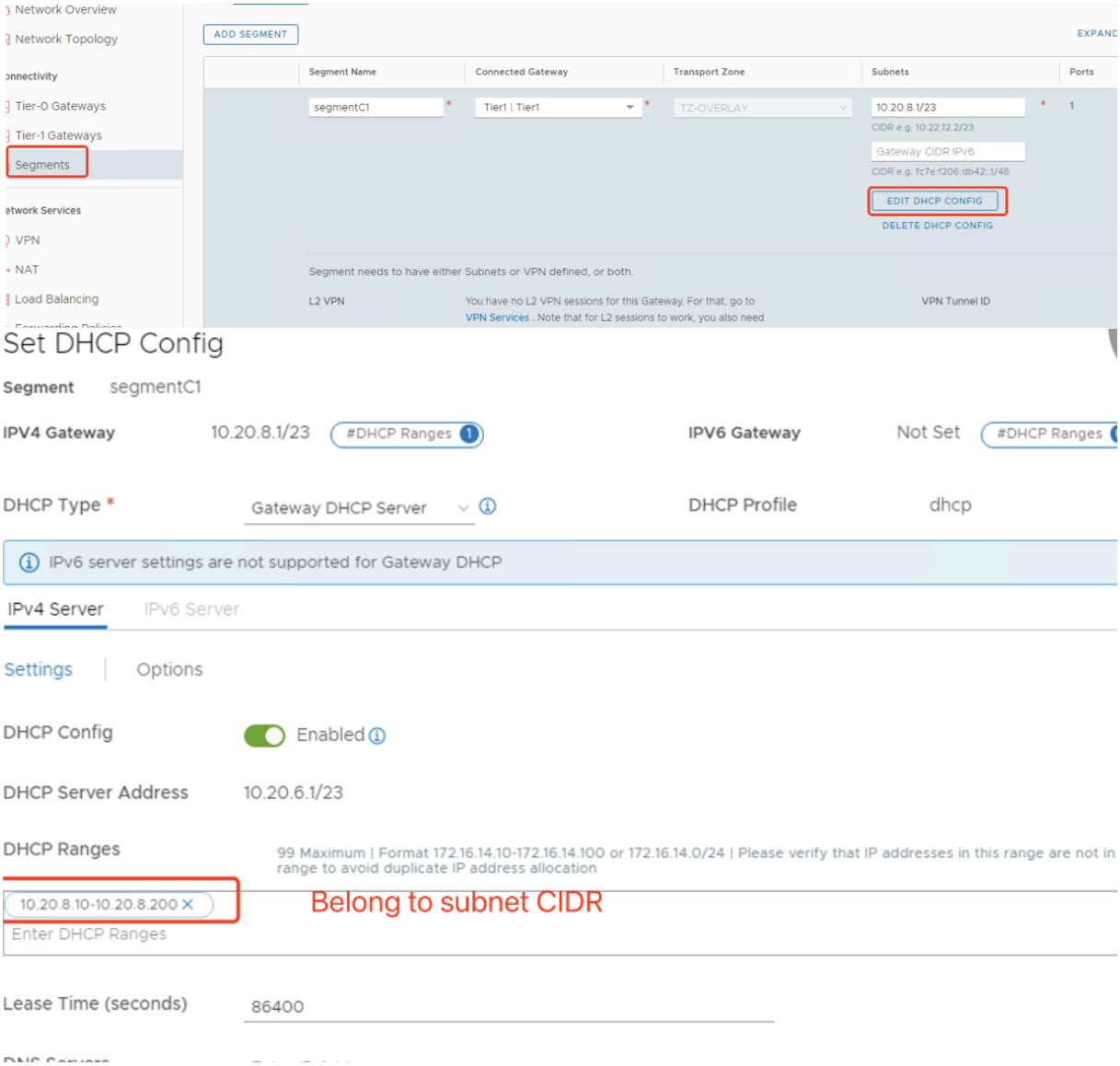
È ora possibile creare un segmento di rete in NSX-T. Per ulteriori informazioni sul DHCP in NSX-T, vedere la documentazione di VMware per DHCP.

Creare un segmento di rete in NSX-T Per le macchine virtuali dei carichi di lavoro si creano subnet come segmenti di rete NSX-T per il cloud privato:

1. In NSX-T Manager, andare a **Networking > Segments** (Networking > Segmenti).
2. Fare clic su **Add Segment** (Aggiungi segmento).
3. Immettere un nome per il segmento.
4. Selezionare **Tier-1** come **Connected Gateway** (Gateway connesso) e lasciare Type (Tipo) impostato su **Flexible** (Flessibile).
5. Fare clic su **Set Subnets** (Imposta subnet).
6. Fare clic su **Add Subnets** (Aggiungi subnet).
7. Immettere l'intervallo di subnet nel campo **Gateway IP/Prefix Length** (Lunghezza del prefisso/IP gateway). Specificare l'intervallo di subnet con **.1** come ultimo ottetto. Ad esempio, **10.12.2.1/24**.
8. Specificare gli intervalli DHCP e fare clic su **ADD** (AGGIUNGI).
9. In **Transport Zone** (Zona di trasporto), selezionare **TZ-OVERLAY** dall'elenco a discesa.
10. Fare clic su **Salva**. Ora è possibile selezionare questo segmento di rete in vCenter quando si crea una macchina virtuale.

In una determinata area geografica, è possibile impostare al massimo 100 route uniche da VMware Engine alla rete VPC utilizzando l'accesso ai servizi privati. Ciò include, ad esempio, gli intervalli di indirizzi IP per la gestione del cloud privato, i segmenti di rete del carico di lavoro NSX-T e gli intervalli di indirizzi IP di rete HCX. Questo limite include tutti i cloud privati nella regione.

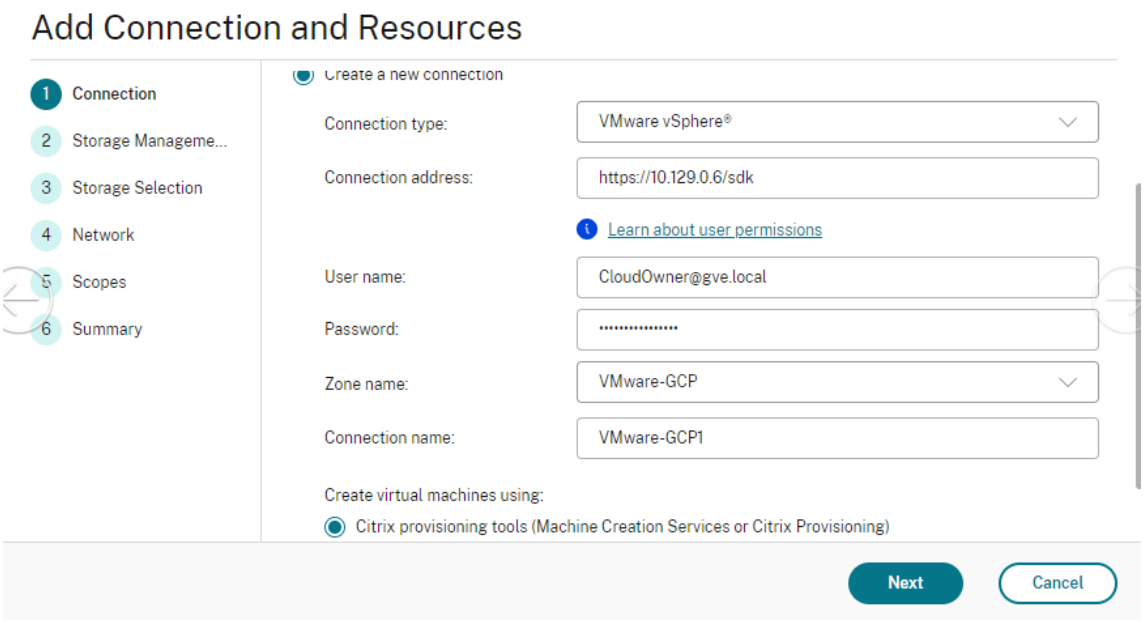
> **Nota:**
>
> A causa di un problema di configurazione di Google Cloud, è necessario configurare più volte l'impostazione dell'intervallo DHCP. Pertanto, assicurarsi di configurare l'impostazione dell'intervallo DHCP dopo la configurazione di Google Cloud. Fare clic su **EDIT DHCP CONFIG** (MODIFICA CONFIGURAZIONE DHCP) per configurare gli intervalli DHCP.



Creare la connessione VMware a Google Cloud in Citrix Studio

1. Creare una macchina in vCenter.
2. Avviare Citrix Studio.

3. Selezionare il nodo di hosting e fare clic su **Add Connection and Resources** (Aggiungi connessione e risorse).
4. Nella schermata **Connessione**, selezionare **Create a new Connection** (Crea una nuova connessione) e i seguenti dettagli:



   a) Selezionare **VMware vSphere** come **Connection type** (Tipo di connessione).
   b) In **Connection address** (Indirizzo di connessione), inserire l'indirizzo IP privato di vCenter.
   c) Inserire le credenziali di vCenter.
   d) Immettere un nome per la connessione.
   e) Scegliere lo strumento per creare macchine virtuali.

5. Nella schermata **Network** (Rete), selezionare la subnet creata nel server NSX-T.
6. Completare la procedura guidata.

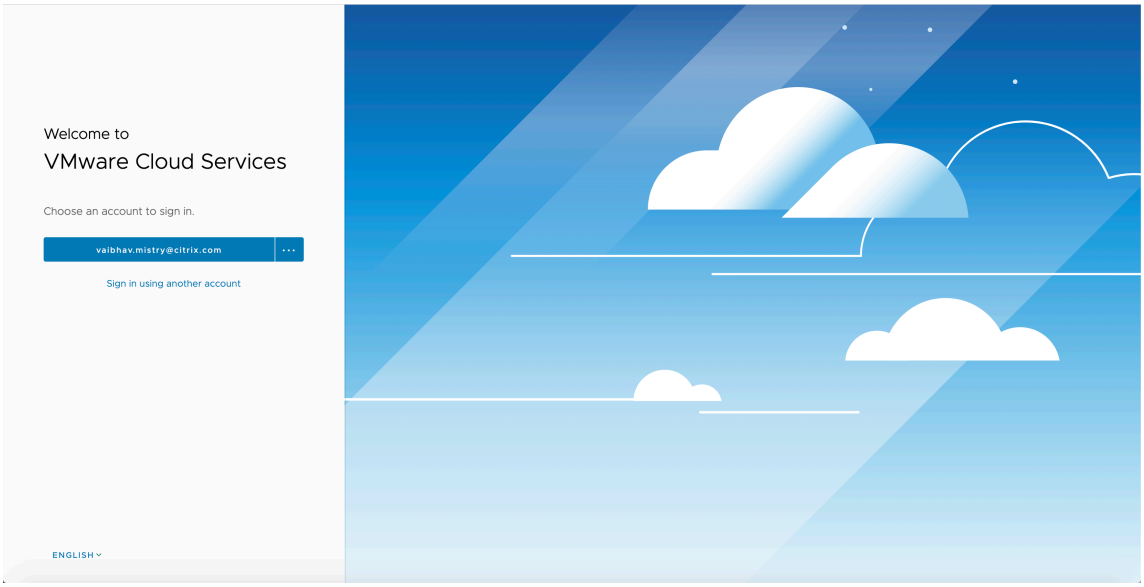
VMware Cloud on Amazon Web Services (AWS)

VMware Cloud on Amazon Web Services (AWS) consente di migrare i carichi di lavoro Citrix on-premise basati su VMware nel cloud AWS.

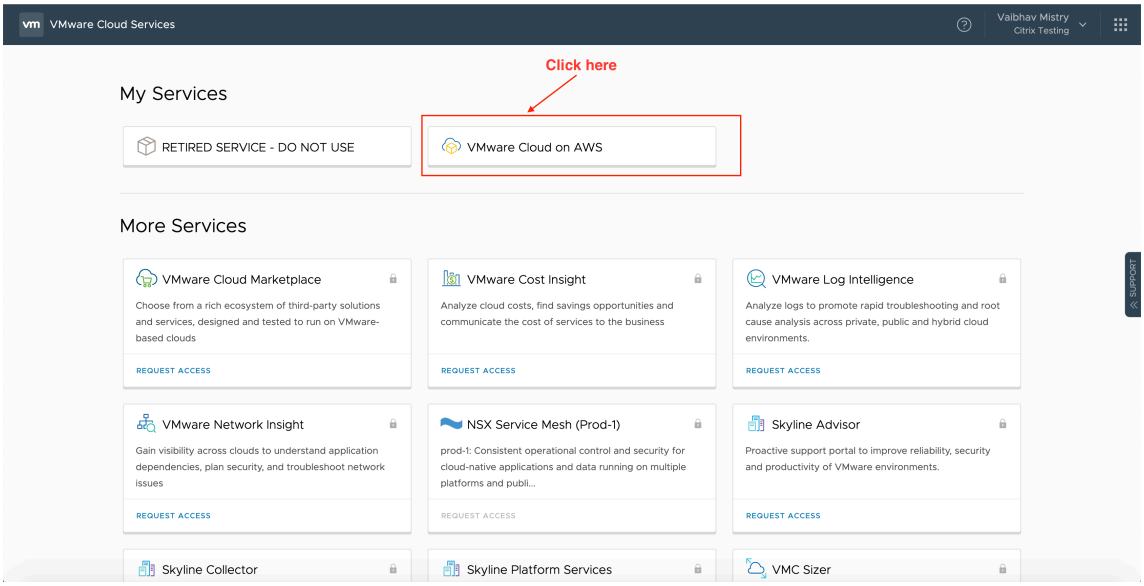
Questo articolo descrive la procedura per configurare VMware Cloud on AWS.

Accedere all'ambiente VMware Cloud

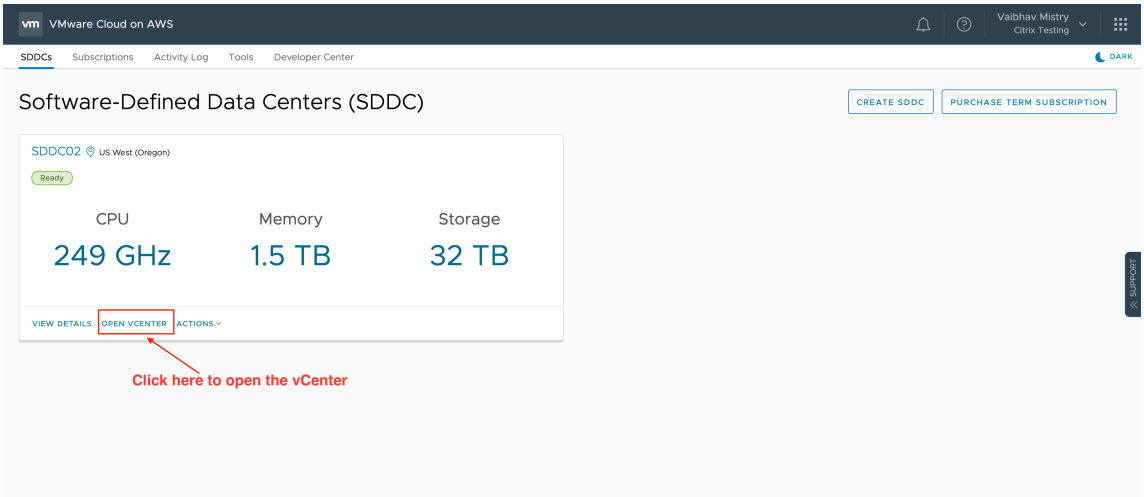
1. Accedere ai servizi VMware Cloud utilizzando l'URL https://console.cloud.vmware.com/.



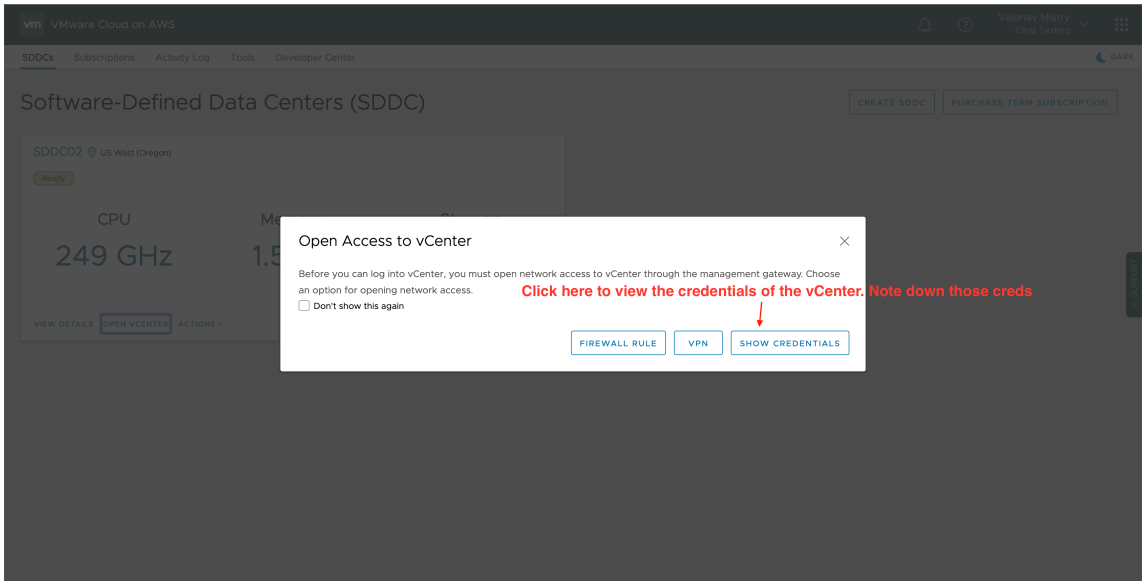
2. Fare clic su **VMware Cloud on AWS**. Viene visualizzata la pagina Software-Defined Data Centers (SDDC) (Software-Defined Data Center [SDDC]).



3. Fare clic su **OPEN VCENTER** (APRI VCENTER) e quindi fare clic su **SHOW CREDENTIALS** (MOSTRA CREDENZIALI). Prendere nota delle credenziali per usarle in seguito.

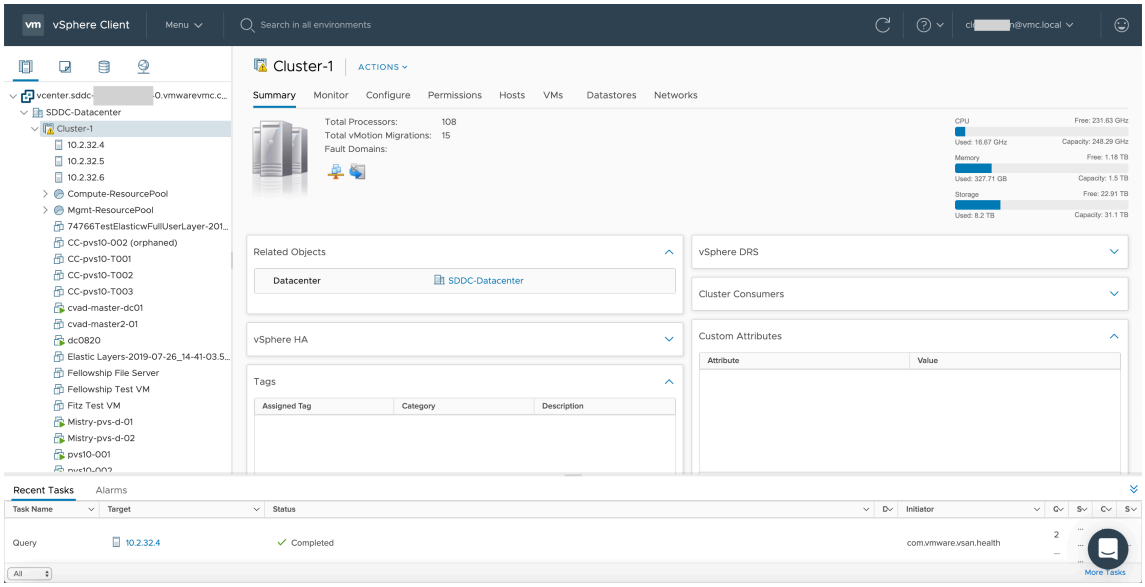


(Apri vCenter)



(Mostra credenziali)

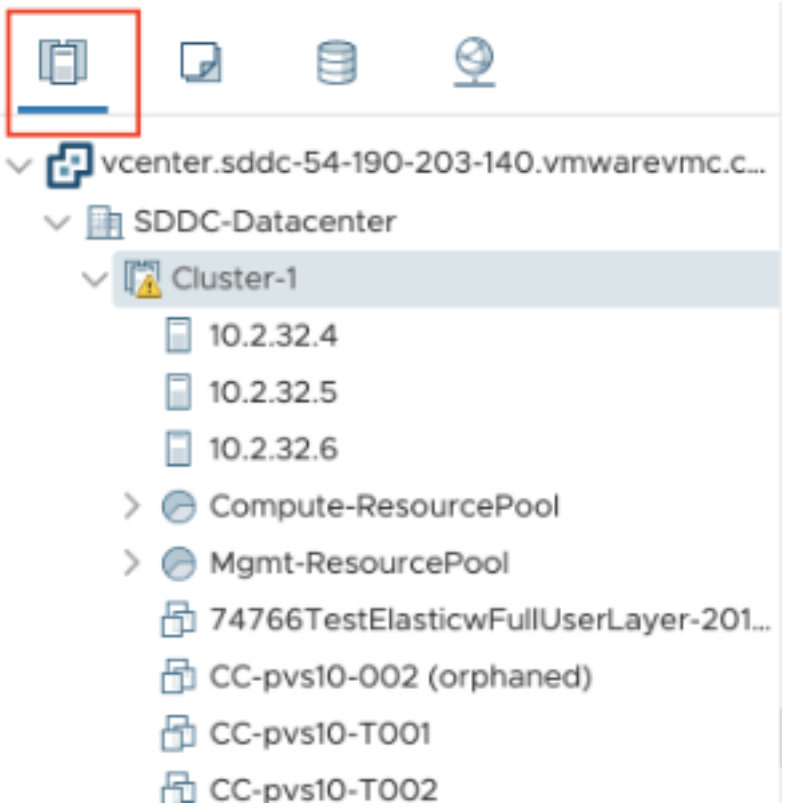
4. Aprire un browser Web e immettere l'URL del Web Client vSphere.
5. Inserire le credenziali come indicato e fare clic su **Login** (Accedi). La pagina Web del client vSphere è simile all'ambiente on-premise.



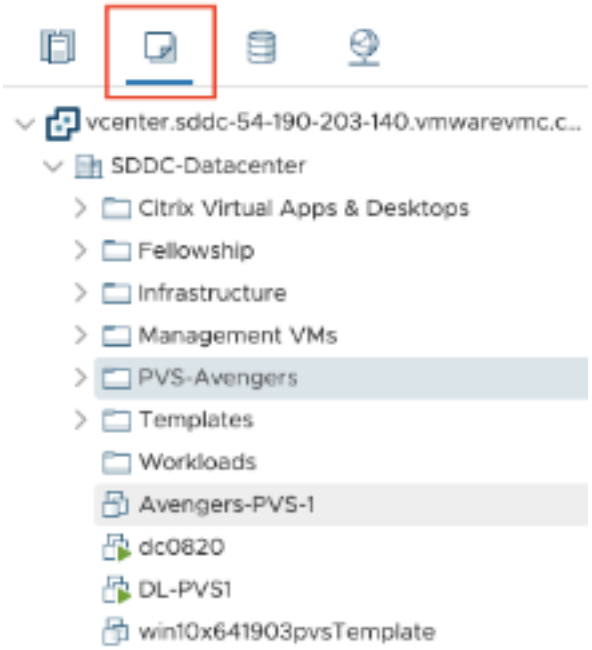
Informazioni sull'ambiente VMware Cloud

Sono disponibili quattro visualizzazioni sulla pagina Web del client vSphere.

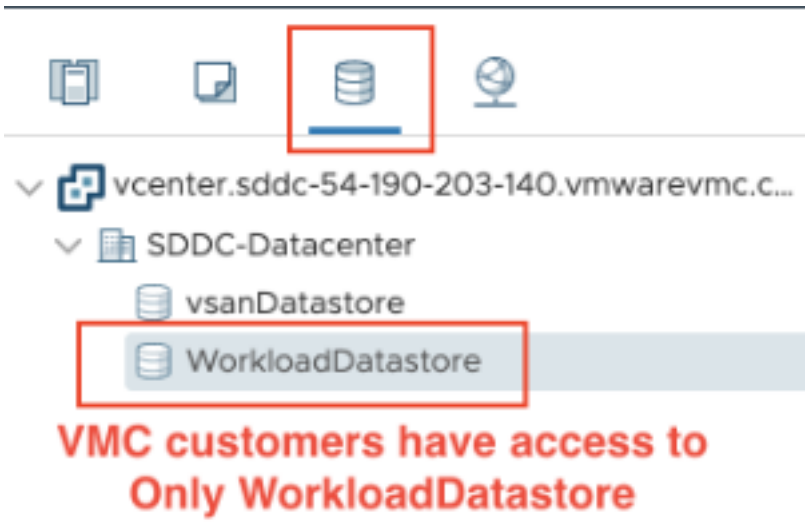
- Visualizzazione host e cluster: non è possibile creare un nuovo cluster, ma l'amministratore del cloud può creare più pool di risorse.



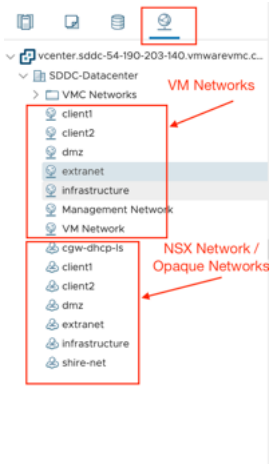
- Visualizzazione macchine virtuali e modelli: l'amministratore del cloud può creare molte cartelle.



- Visualizzazione archiviazione: selezionare l'archiviazione **WorkloadDatastore** quando si aggiunge un'unità di hosting in Citrix Studio, perché si ha accesso solo all'archivio dati dei carichi di lavoro.



- Visualizzazione rete: le icone sono diverse per le reti VMware Cloud e le reti opache.



Dopo aver configurato il cluster, fare riferimento agli ambienti di virtualizzazione VMware per l'aggiunta di connessioni e risorse.

Passaggi successivi

- Installare i componenti principali
- Installare i VDA
- Creare un sito

- Per informazioni su come creare e gestire una connessione, vedi Connessione a soluzioni cloud e partner VMware

Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Creare cataloghi di macchine

Installare i componenti principali

January 7, 2024

> **Importante:**
>
> Citrix raccoglie i dati di licenza di base necessari per i suoi interessi legittimi, inclusa la conformità delle licenze. Per ulteriori informazioni, vedere Citrix Licensing Data.

I componenti principali sono Citrix Delivery Controller, Citrix Studio, Citrix Director e Citrix License Server.

> **Nota:**
>
> Citrix Studio è una console di gestione basata su Windows che consente di configurare e gestire l'implementazione locale di Citrix Virtual Apps and Desktops. Web Studio è la nuova generazione di Citrix Studio, una console di gestione basata sul Web che offre la parità di funzionalità completa con Citrix Studio. Per ulteriori informazioni su Web Studio, vedere Installare Web Studio.

Nelle versioni precedenti al 2003, i componenti principali includevano Citrix StoreFront. È comunque possibile installare StoreFront facendo clic sul riquadro **Citrix StoreFront** o eseguendo il comando disponibile sul supporto di installazione.

Prima di iniziare un'installazione, leggere questo articolo e Prepararsi all'installazione.

In questo articolo viene descritta la sequenza di installazione guidata durante l'installazione dei componenti principali. Vengono forniti equivalenti della riga di comando. Per ulteriori informazioni, vedere Installare utilizzando la riga di comando.

Passaggio 1. Scaricare il software del prodotto e avviare la procedura guidata

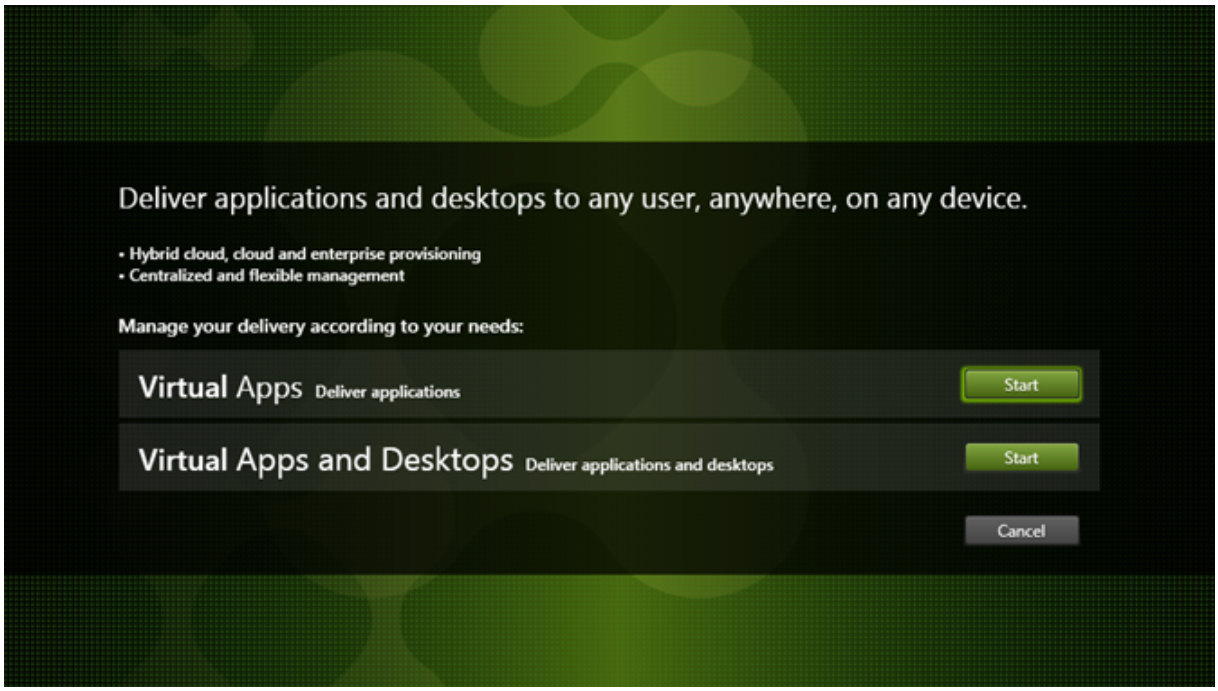
Utilizzare le credenziali dell'account Citrix per accedere alla pagina di download di Citrix Virtual Apps and Desktops. Scaricare il file ISO del prodotto.

Decomprimere il file. Facoltativamente, masterizzare un DVD con il file ISO.

Eseguire l'accesso sul computer in cui si stanno installando i componenti principali, utilizzando un account amministratore locale.

Inserire il DVD nell'unità o montare il file ISO. Se il programma di installazione non si avvia automaticamente, fare doppio clic sull'applicazione **AutoSelect** o sull'unità montata.

Passaggio 2. Scegliere il prodotto da installare

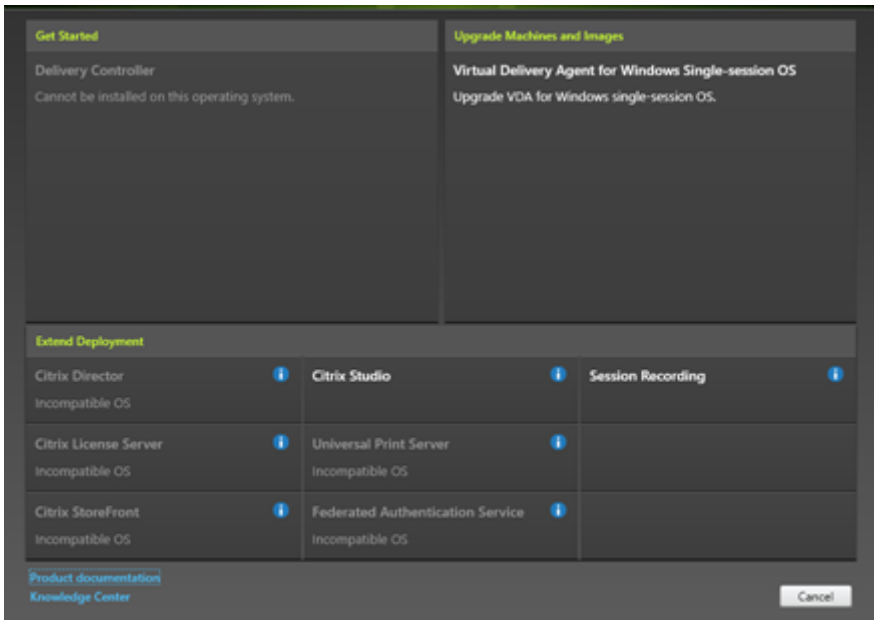


Fare clic su **Start** accanto al prodotto da installare: Virtual Apps o Virtual Apps and Desktops.

Se sul computer sono già installati componenti di Citrix Virtual Apps and Desktops, questa pagina non viene visualizzata.

Opzione della riga di comando: `/xenapp` per installare Citrix Virtual Apps. Se l'opzione viene omessa, viene installato Citrix Virtual Apps and Desktops.

Passaggio 3. Scegliere cosa installare

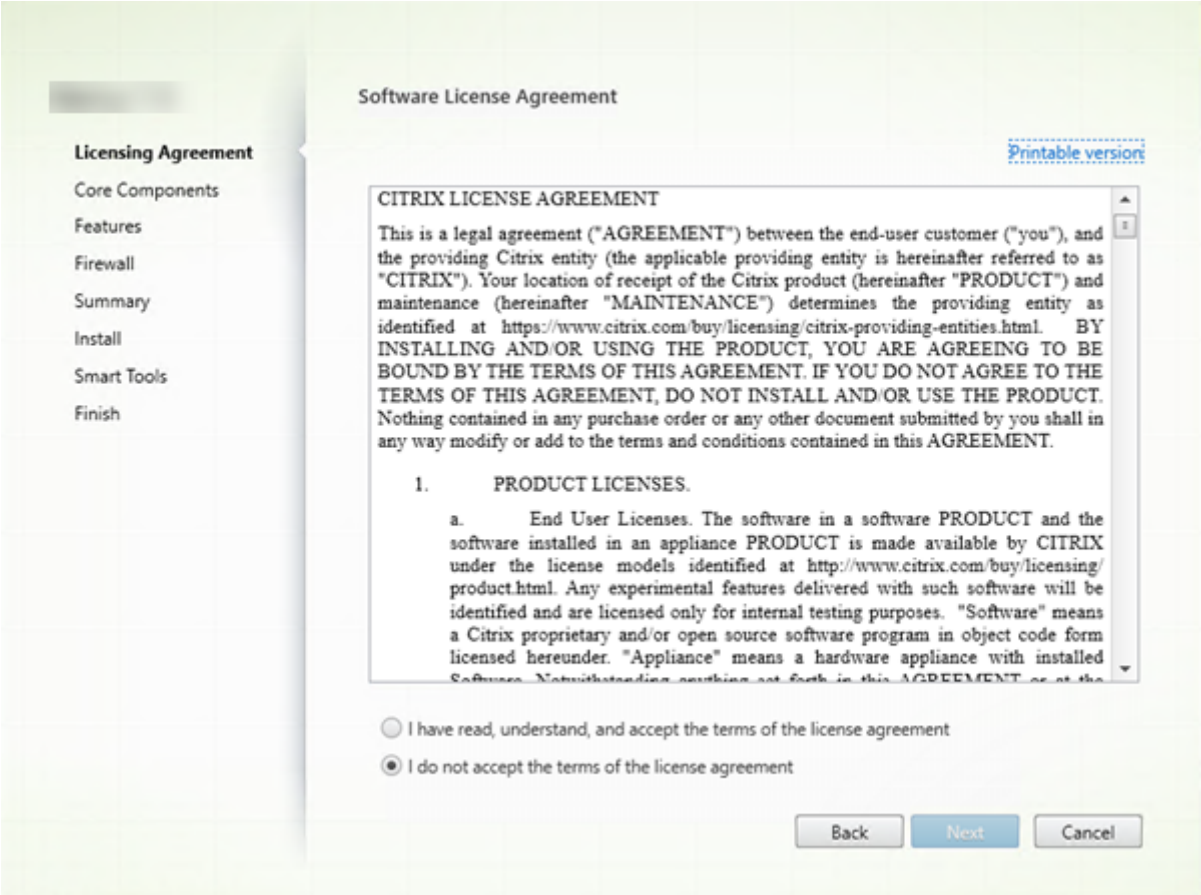


Se si è appena iniziato, selezionare **Delivery Controller**. In una pagina successiva, si selezionano i componenti specifici da installare sul computer.

Se è già stato installato un controller (su questo computer o in un altro computer) e si desidera installare un altro componente, selezionare il componente dalla sezione **Extend Deployment** (Estendi distribuzione).

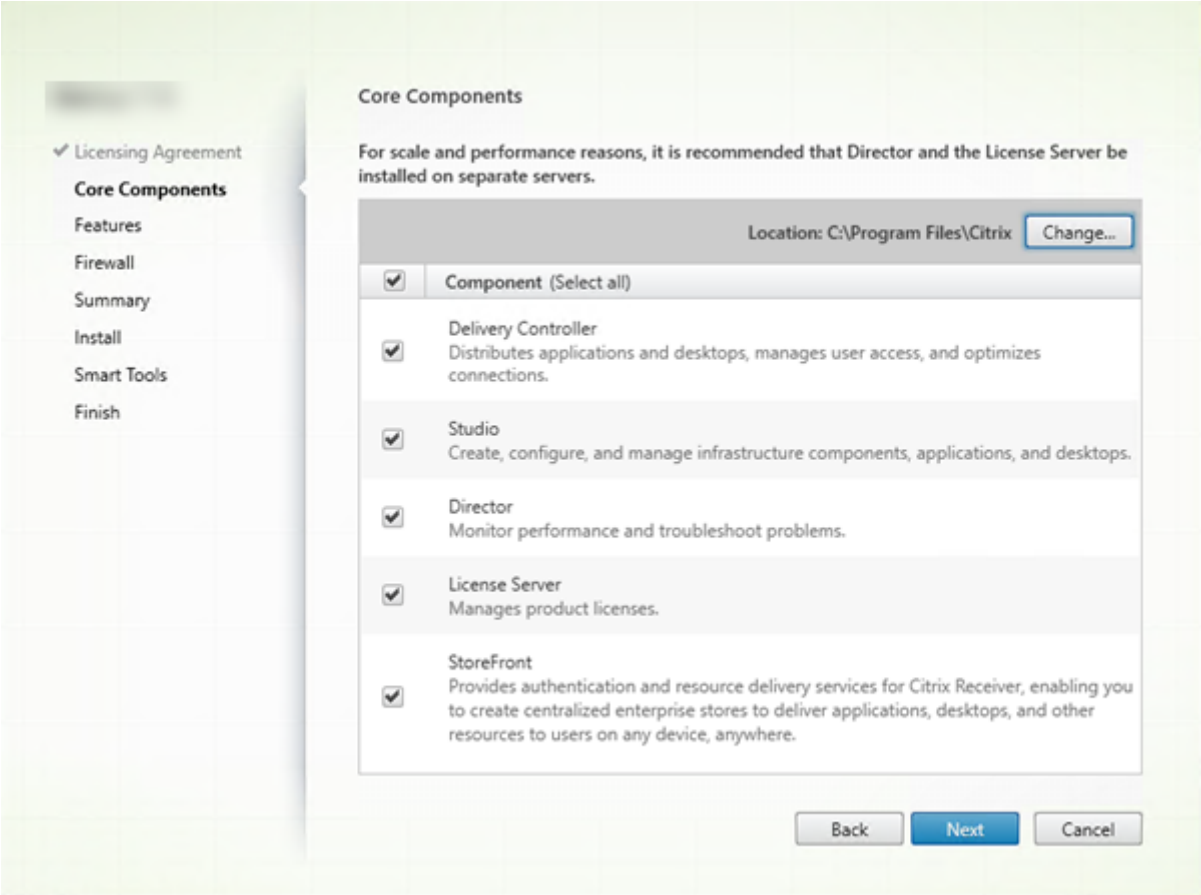
Opzione della riga di comando: `/components`

Passaggio 4. Leggere e accettare il contratto di licenza



Nella pagina **Licensing Agreement**, dopo aver letto il contratto di licenza, indicare di averlo letto e accettato. Quindi, fare clic su **Next** (Avanti).

Passaggio 5. Selezionare i componenti da installare e il percorso di installazione



Nella pagina **Core components**:

- **Location (Percorso):** per impostazione predefinita, i componenti sono installati in `C:\Program Files\Citrix`. Il valore predefinito è adatto per la maggior parte delle distribuzioni. Se si specifica un percorso diverso, è necessario disporre delle autorizzazioni di esecuzione per il servizio di rete.
- **Componenti:** per impostazione predefinita, vengono selezionate le caselle di controllo relative a tutti i componenti principali. L'installazione di tutti i componenti principali su un unico server va bene per installazioni di prova, test o piccole distribuzioni di produzione. Per gli ambienti di produzione più grandi, Citrix consiglia di installare Director, StoreFront e License Server su server separati.

  > **Nota:**
  >
  > Se si installano componenti su più server, installare Citrix License Server e le licenze prima di installare altri componenti su altri server. Per la guida, vedere la sezione Installazione automatica della Guida alle licenze per Citrix Virtual Apps and Desktops.

> Un'icona avvisa quando si sceglie di non installare un componente principale richiesto su questo computer. Questo avviso ricorda di installare quel componente, anche se non necessariamente su questo computer.

Fare clic su **Next** (Avanti).

Opzioni della riga di comando: `/installdir`, `/components`, `/exclude`

Controllo dell'hardware

Quando si installa o si aggiorna un Delivery Controller, l'hardware viene controllato. Il programma di installazione avvisa se il computer dispone di una quantità di RAM inferiore alla quantità consigliata (5 GB), in quanto ciò può influire sulla stabilità del sito. Per ulteriori informazioni, vedere Requisiti hardware.

Interfaccia grafica: viene visualizzata una finestra di dialogo.

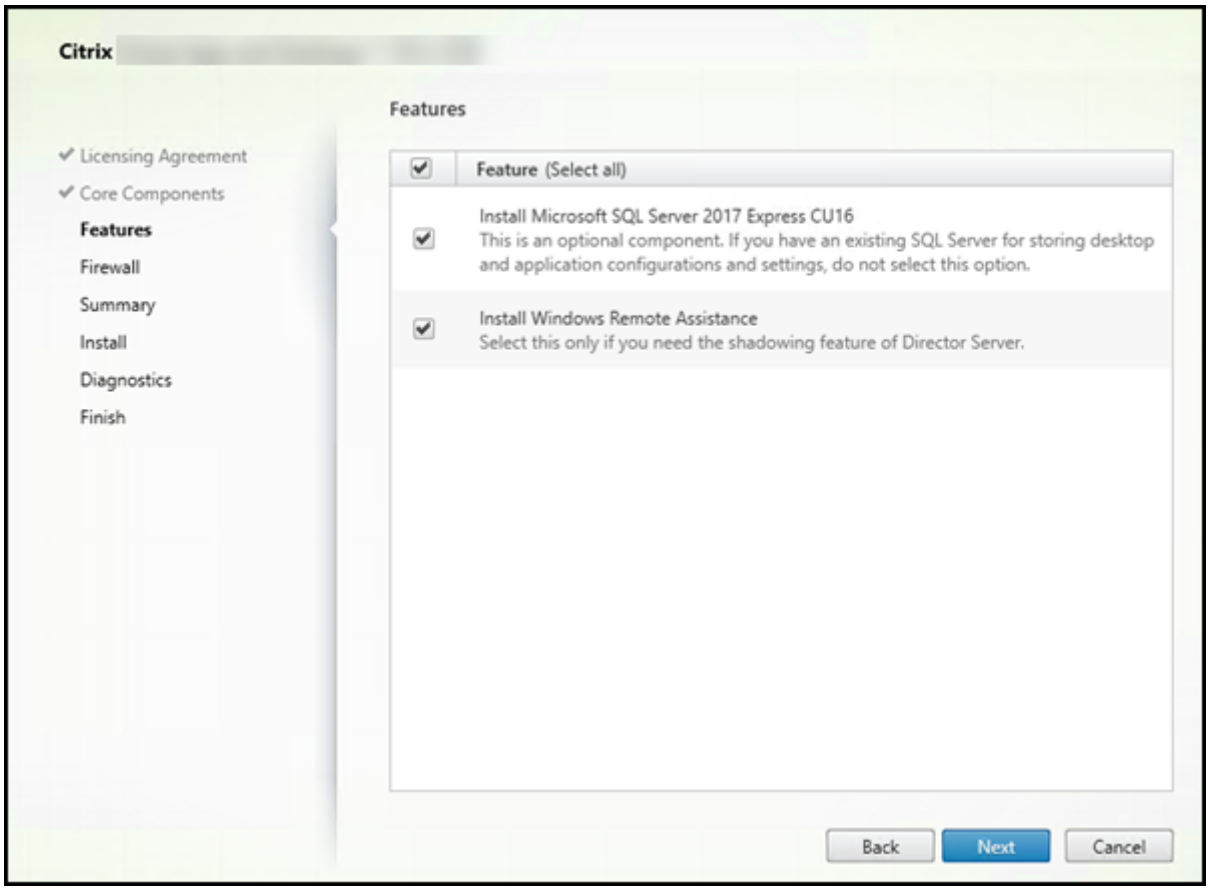
- Consigliato: fare clic su **Cancel** per interrompere l'installazione. Aggiungere più RAM al computer e quindi riavviare l'installazione.
- In alternativa, fare clic su **Next** per continuare con l'installazione. Il sito potrebbe avere problemi di stabilità.

Interfaccia della riga di comando: termina l'installazione/aggiornamento. I registri di installazione contengono un messaggio che descrive cosa è stato trovato e le opzioni disponibili.

- Consigliato: aggiungere più RAM al computer e quindi eseguire nuovamente il comando.
- In alternativa, eseguire nuovamente il comando con l'opzione `/ignore_hw_check_failure` per ignorare l'avviso. Il sito potrebbe avere problemi di stabilità.

Durante l'aggiornamento, viene inoltre visualizzata una notifica se il sistema operativo o la versione di SQL Server non è più supportata. Vedere Aggiornare una distribuzione.

Passaggio 6. Attivare o disattivare funzionalità



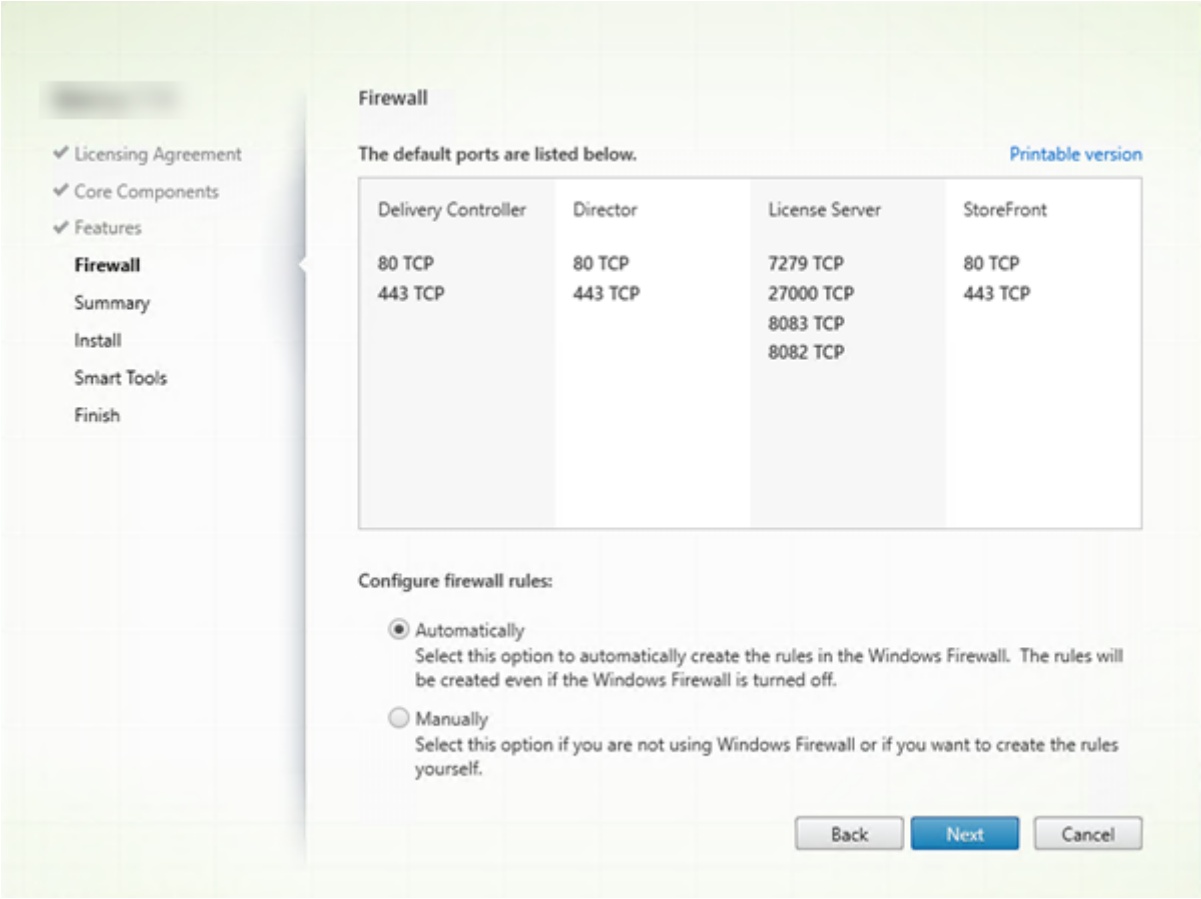
Nella pagina **Features**:

- Scegliere se installare Microsoft SQL Server Express per l'utilizzo come database del sito. Per impostazione predefinita, questa selezione è abilitata. Se non si ha familiarità con i database Citrix Virtual Apps and Desktops, consultare Database.
- Quando si installa Director, Assistenza remota di Windows viene installato automaticamente. È possibile scegliere se attivare lo shadowing in Assistenza remota di Windows per l'utilizzo con lo shadowing utente di Director. Attivando lo shadowing si apre la porta TCP 3389. Per impostazione predefinita, questa funzionalità è abilitata. L'impostazione predefinita è adatta per la maggior parte delle distribuzioni. Questa funzionalità viene visualizzata solo quando si installa Director.

Fare clic su **Next** (Avanti).

Opzioni della riga di comando: `/nosql` (per impedire l'installazione), `/no_remote_assistance` (per impedire l'abilitazione)

Passaggio 7. Aprire le porte del firewall di Windows



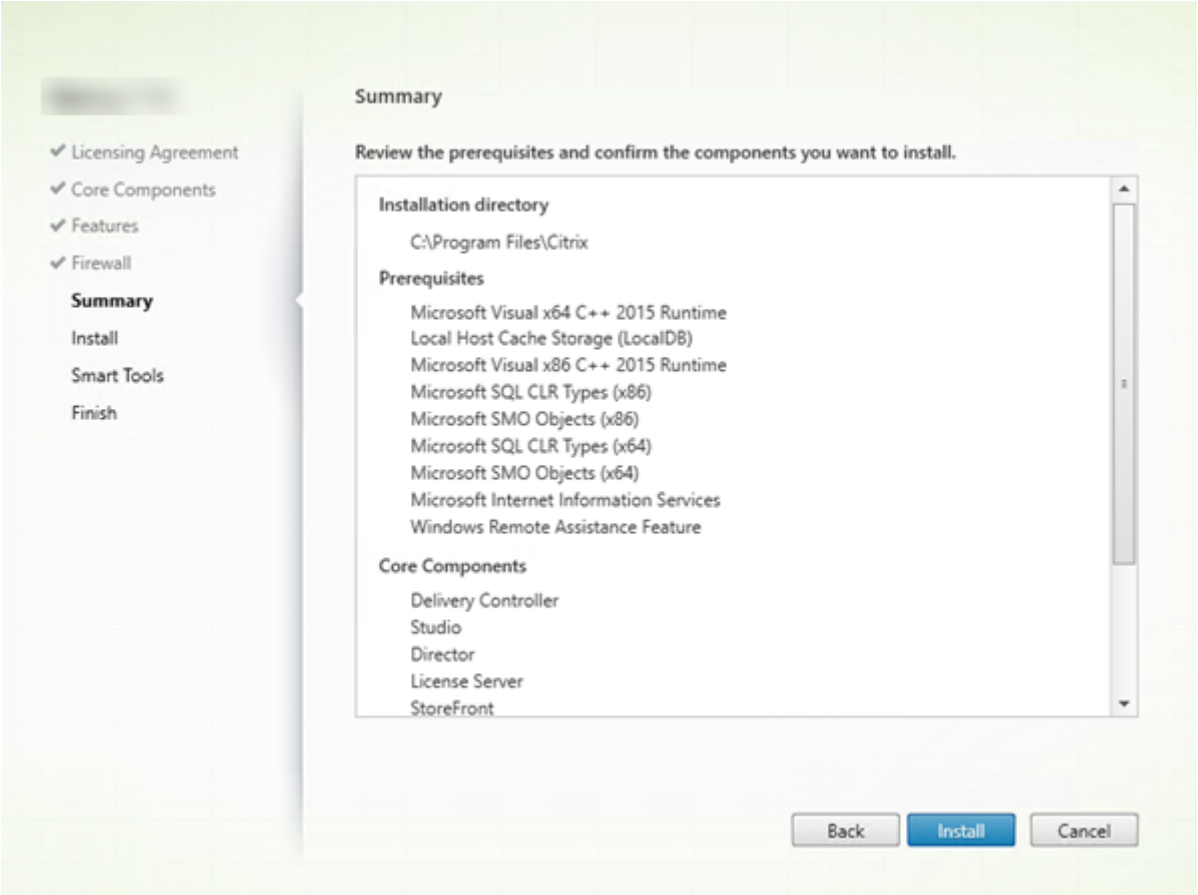
Per impostazione predefinita, le porte nella pagina **Firewall** vengono aperte automaticamente se il servizio Windows Firewall è in esecuzione, anche se il firewall non è abilitato. L'impostazione predefinita è adatta per la maggior parte delle distribuzioni. Per informazioni sulle porte, vedere Porte di rete.

Fare clic su **Next** (Avanti).

L'immagine mostra gli elenchi delle porte quando si installano tutti i componenti principali su questo computer. Questo tipo di installazione è in genere solo per distribuzioni di prova.

Opzione della riga di comando: `/configure_firewall`

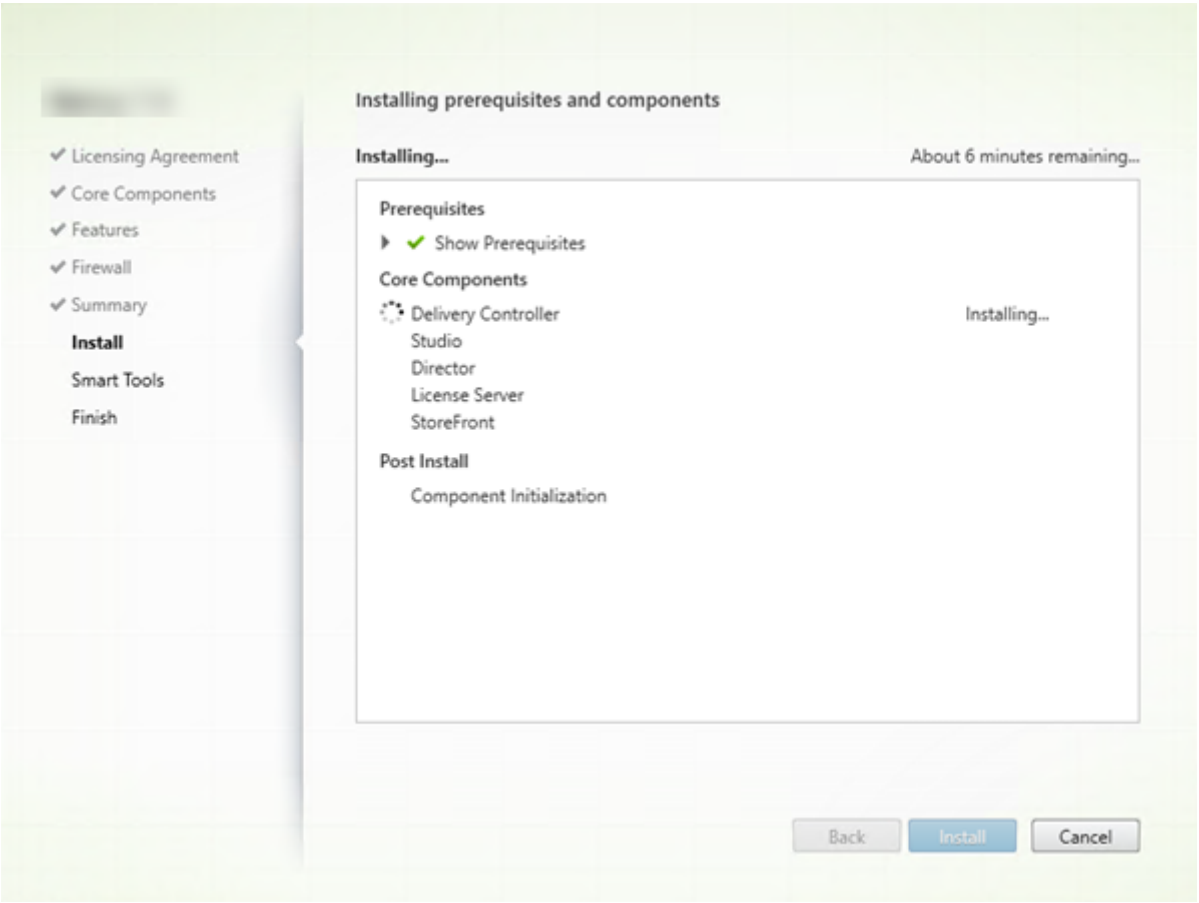
Passaggio 8. Esaminare i prerequisiti e confermare l'installazione



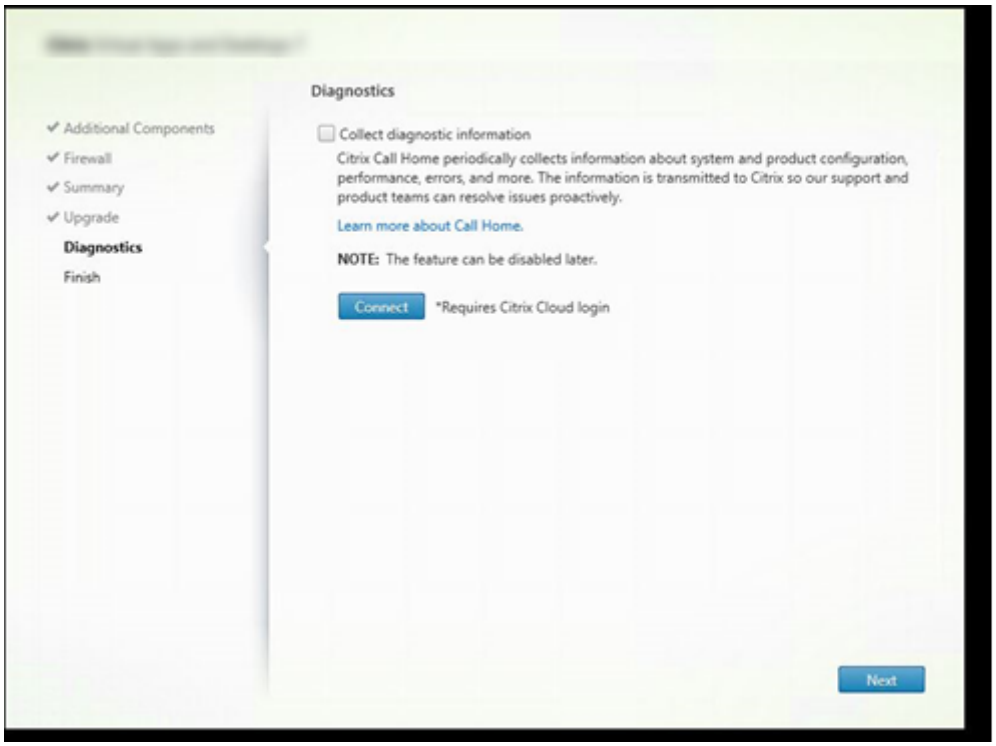
Nella pagina **Summary** sono elencati gli elementi che verranno installati. Utilizzare il pulsante **Back** per tornare alle pagine precedenti della procedura guidata e modificare le selezioni, se necessario.

Quando si è pronti, fare clic su **Install**.

Viene visualizzato lo stato di avanzamento dell'installazione:



Passaggio 9 Condividere informazioni diagnostiche con Cloud Software Group



Nella pagina **Diagnostics** (Diagnostics), scegliere se partecipare a Citrix Call Home.

Questa pagina viene visualizzata quando si installa un Delivery Controller utilizzando l'interfaccia grafica. Quando si installa StoreFront (ma non un controller), la procedura guidata visualizza questa pagina. Quando si installano altri componenti principali (ma non un controller o StoreFront), la procedura guidata non visualizza questa pagina.

Durante un aggiornamento, questa pagina non viene visualizzata se Call Home è già abilitato o se il programma di installazione rileva un errore di Citrix Telemetry Service.

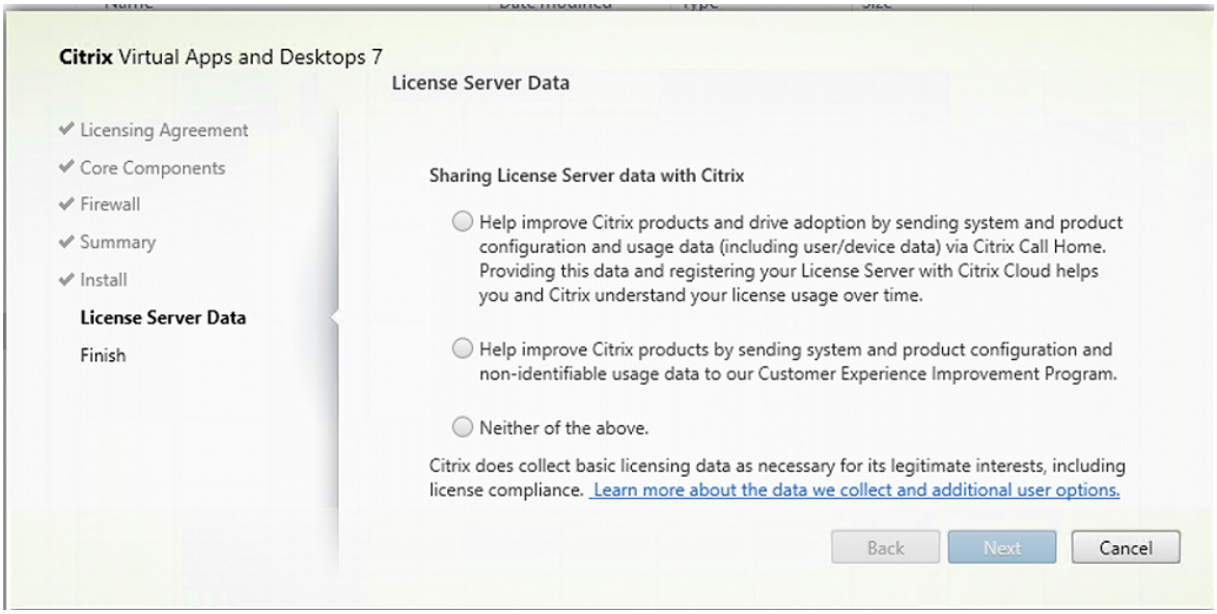
Se si sceglie di partecipare (impostazione predefinita), fare clic su **Connect**. Quando richiesto, immettere le credenziali dell'account Citrix. È possibile modificare la scelta di registrazione in un secondo momento, dopo l'installazione.

Dopo aver convalidato le credenziali (o se si sceglie di non partecipare), fare clic su **Next**.

Se si fa clic su **Connect** (Connetti) nella pagina **Diagnostics** (Diagnostica) senza prima selezionare **Collect diagnostic information** (Raccogli informazioni diagnostiche), dopo aver chiuso la finestra di dialogo **Connect to Citrix Insight Services** (Connetti a Citrix Insight Services) il pulsante **Next** (Avanti) è disabilitato. Non è possibile passare alla pagina successiva. Per riattivare il pulsante **Next** (Avanti), selezionare e deselezionare immediatamente **Collect diagnostic information** (Raccogli informazioni diagnostiche).

Per ulteriori informazioni, vedere Call Home.

Passaggio 10. Condividere i dati del server di licenza con Cloud Software Group



Nella pagina **License Server Data**, chiediamo di condividere i dati di Call Home o i dati del Programma di miglioramento dell'esperienza cliente (CEIP) per aiutarci. Inoltre, Cloud Software Group richiede anche la raccolta di dati di licenza di base, inclusa la conformità delle licenze, nella misura necessaria per i suoi interessi legittimi.

La pagina **License Server Data** viene visualizzata dopo che è stato installato License Server:

- In modalità autonoma.
- Come componente principale, durante l'installazione di un Delivery Controller.

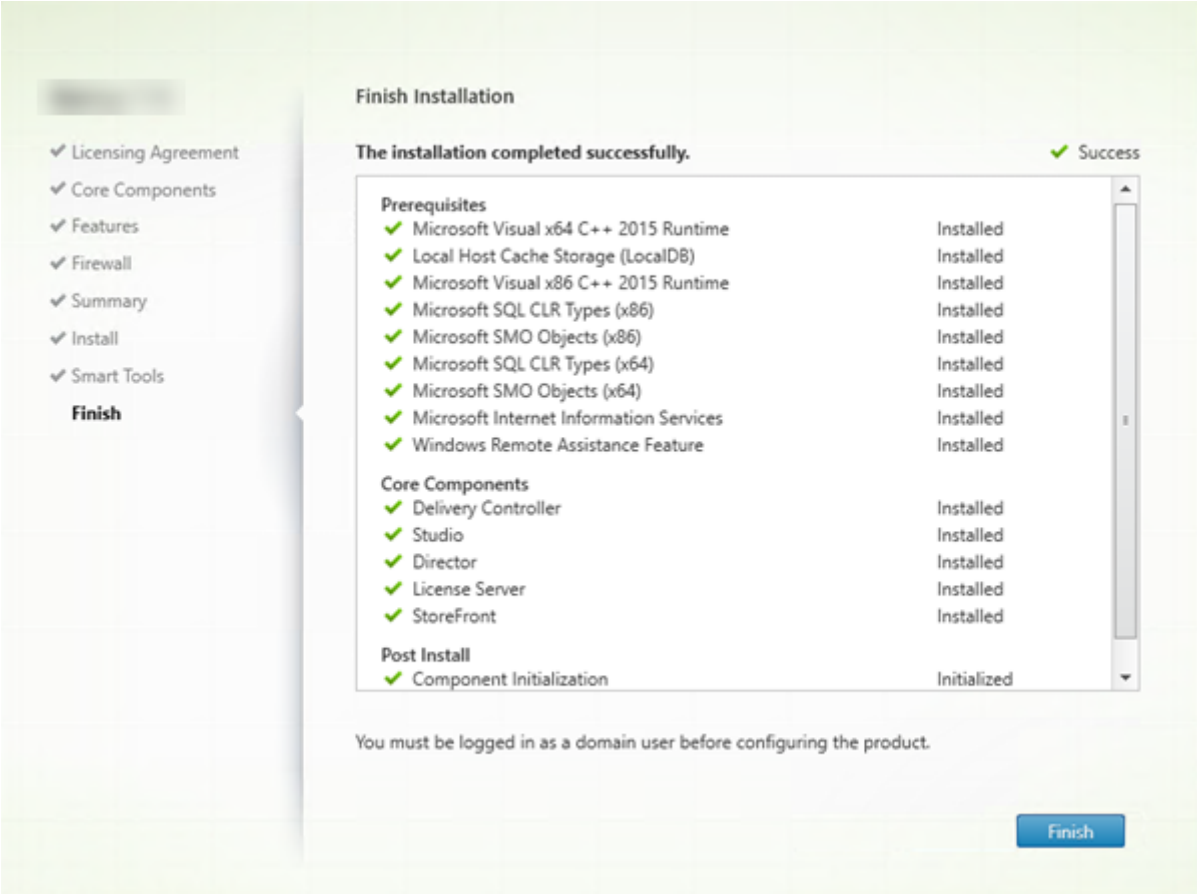
Durante un aggiornamento, questa pagina non viene visualizzata se la configurazione è già impostata nel file `/CITRIX.opt:`.

License Server monitora diversi tipi di dati utente, come dati di licenza, dati Call Home e dati CEIP. Per attivare la raccolta dei dati Call Home e del CEIP, è necessario scegliere di partecipare (opt-in).

Per ulteriori informazioni su come abilitare la raccolta dei dati Call Home e CEIP durante l'installazione mediante la riga di comando, vedere Command line options for installing core components (Opzioni della riga di comando per installare i componenti principali).

Per ulteriori informazioni sulla raccolta dati License Server Data, vedere Citrix Licensing data collection programs (Programmi di raccolta dati Citrix Licensing).

Passaggio 11. Completare l'installazione



La pagina **Finish** contiene segni di spunta verdi per tutti i prerequisiti e i componenti installati e inizializzati correttamente.

Fare clic su **Finish**.

Passaggio 12. Installare i componenti principali rimanenti su altre macchine

Se tutti i componenti principali sono stati installati su una macchina, continuare con Passaggi successivi In caso contrario, eseguire il programma di installazione su altri computer per installare altri componenti. È inoltre possibile installare più controller su altri server.

Passaggi successivi

Dopo aver installato tutti i componenti necessari, utilizzare Studio per creare un sito.

Dopo aver creato il sito, installare i VDA.

In qualsiasi momento, è possibile utilizzare il programma di installazione del prodotto completo per estendere la distribuzione con i seguenti componenti:

- **Componente server di Universal Print Server:** avviare il programma di installazione sul server di stampa.

  1. Selezionare **Universal Print Server** nella sezione **Extend Deployment**.
  2. Accettare il contratto di licenza
  3. Nella pagina **Firewall**, per impostazione predefinita, le porte TCP 7229 e 8080 vengono aperte nel firewall se il servizio Windows Firewall è in esecuzione, anche se il firewall non è abilitato. È possibile disattivare l'azione predefinita se si desidera aprire manualmente le porte.

  Per installare questo componente dalla riga di comando, vedere Opzioni della riga di comando per l'installazione di un Universal Print Server.

- Federated Authentication Service.
- Registrazione della sessione.
- Workspace Environment Management.

Installare utilizzando la riga di comando

April 3, 2024

> **Importante:**
>
> - Se si sta eseguendo l'aggiornamento e sulla versione corrente è installato o viene utilizzato il software Personal vDisk o AppDisks, vedere Rimozione di PvD, AppDisk e host non supportati.
> - Citrix raccoglie i dati di licenza di base necessari per i suoi interessi legittimi, inclusa la conformità delle licenze. Per ulteriori informazioni, vedere Citrix Licensing Data.

Introduzione

Questo articolo si applica all'installazione di componenti su macchine con sistemi operativi Windows. Per informazioni sui VDA per i sistemi operativi Linux, vedere Linux Virtual Delivery Agent.

In questo articolo viene descritto come emettere i comandi di installazione del prodotto. Prima di iniziare qualsiasi installazione, vedere Prepararsi all'installazione. Quell'articolo include le descrizioni dei programmi di installazione disponibili.

Per visualizzare l'avanzamento dell'esecuzione dei comandi e i valori restituiti, è necessario essere l'amministratore originale oppure utilizzare **Esegui come amministratore**. Per ulteriori informazioni, vedere la documentazione dei comandi Microsoft.

Come complemento all'utilizzo diretto dei comandi di installazione, nella ISO del prodotto vengono forniti script di esempio che installano, aggiornano o rimuovono i VDA sui computer in Active Directory. Per ulteriori informazioni, vedere Installare i VDA utilizzando script.

Se si tenta di installare o eseguire l'aggiornamento su una versione del sistema operativo Windows non supportata per questa versione di Citrix Virtual Apps and Desktops, viene visualizzato un messaggio di informazioni sulle opzioni disponibili. Vedere Sistemi operativi precedenti.

Per informazioni su come Citrix riporta il risultato delle installazioni dei componenti, vedere Codici restituiti per l'installazione Citrix.

Utilizzare il programma di installazione del prodotto completo

Per accedere all'interfaccia della riga di comando del programma di installazione del prodotto completo:

1. Scaricare il pacchetto del prodotto da Citrix. Per accedere al sito di download, sono necessarie le credenziali dell'account Citrix.
2. Decomprimere il file. Facoltativamente, masterizzare un DVD con il file ISO.
3. Accedere al server in cui si stanno installando i componenti utilizzando un account amministratore locale.
4. Inserire il DVD nell'unità o montare il file ISO.
5. Dalla directory `\x64\XenDesktop Setup` del supporto, eseguire il comando appropriato.

   Per installare i componenti principali: eseguire `XenDesktopServerSetup.exe` con le opzioni elencate in Opzioni della riga di comando per l'installazione dei componenti principali.

   Per installare un VDA: eseguire `XenDesktopVDASetup.exe` con le opzioni elencate in Opzioni della riga di comando per l'installazione di un VDA.

   Per installare StoreFront: eseguire `CitrixStoreFront-x64.exe` nella cartella `x64 > StoreFront` del supporto di installazione.

   Per installare Universal Print Server: seguire le istruzioni riportate in Opzioni della riga di comando per l'installazione di un Universal Print Server.

   Per installare Federated Authentication Service: Citrix consiglia di utilizzare l'interfaccia grafica.

   Per installare Session Recording: seguire le istruzioni riportate in Session Recording.

Per installare Workspace Environment Management: seguire le indicazioni fornite in Workspace Environment Management.

Opzioni della riga di comando per l'installazione dei componenti principali

Le seguenti opzioni di parametro sono valide quando si installano componenti principali con il comando `XenDesktopServerSetup.exe`. Per maggiori dettagli sulle opzioni, vedere Installare i componenti principali.

- **/ceipoptin** *ceipoptin* [,*ceipoptin*] …

  Consente la raccolta di dati Call Home e dati CEIP (Programma di miglioramento dell'esperienza cliente). I valori validi sono:

  - `DIAGNOSTIC`: Scegliere questo valore per consentire a Citrix Licensing di raccogliere dati Call Home.
  - `ANONYMOUS`: Scegliere questo valore per consentire a Citrix Licensing di raccogliere dati CEIP non identificati (che non identificano gli utenti).
  - `NONE`: Scegliere questo valore per disabilitare la raccolta di dati CEIP da parte di Citrix Licensing.

  Per ulteriori informazioni sulla raccolta di dati Call Home, vedere Citrix Licensing Call Home.

  Per maggiori dettagli sulla raccolta dei dati CEIP, vedere Citrix Licensing Customer Experience Improvement Program.

  Per maggiori dettagli sui dati CEIP, vedere Citrix Licensing CEIP data elements.

  Per maggiori dettagli sui dati di licenza di License Server, vedere Citrix Licensing Data.

- **/componenti** *componente* [,*componente*] …

  Elenco separato da virgole di componenti da installare o rimuovere. I valori validi sono:

  - `CONTROLLER`: Controller
  - `DESKTOPSTUDIO`: Studio
  - `WEBSTUDIO`: Web Studio
  - `DESKTOPDIRECTOR`: Director
  - `LICENSESERVER`: Citrix License Server

  Se questa opzione viene omessa, tutti i componenti vengono installati (o rimossi, se viene specificata anche l'opzione `/remove`).

  (Nelle versioni precedenti alla 2003, i valori validi includevano `STOREFRONT`. Per la versione 2003 e successive, utilizzare il comando di installazione StoreFront dedicato indicato in Utilizzare il programma di installazione completo del prodotto.

- **/configure_firewall**

  Apre tutte le porte del firewall di Windows utilizzate dai componenti installati, se il servizio Windows Firewall è in esecuzione, anche se il firewall non è abilitato. Se si utilizza un firewall di terze parti o non si utilizza un firewall, è necessario aprire manualmente le porte.

- **/disableexperiencemetrics**

  Impedisce l'invio automatico a Citrix delle analisi raccolte durante l'installazione, l'aggiornamento o la rimozione.

- **/exclude** "*funzione*"[,"*funzione*"]

  Impedisce l'installazione di una o più funzionalità, servizi o tecnologie separate da virgole, ciascuna racchiusa tra virgolette diritte. I valori validi sono:

  - `"Local Host Cache Storage (LocalDB)"`: impedisce l'installazione del database utilizzato per la cache host locale. Questa opzione non ha alcun effetto sul fatto che SQL Server Express sia installato o meno per l'utilizzo come database del sito.

- **/help** o **/h**

  Visualizza la Guida dei comandi.

- **/ignore_hw_check_failure**

  Consente di continuare l'installazione o l'aggiornamento del Delivery Controller, anche se i controlli hardware non riescono (ad esempio, a causa di RAM insufficiente). Per ulteriori informazioni, vedere Controllo hardware.

- **/ignore_site_test_failure**

  Valido solo durante l'aggiornamento del controller. In genere, tutti gli errori di test del sito vengono ignorati e l'aggiornamento procede. Se omesso (o impostato su false), qualsiasi errore di test del sito causa il fallimento del programma di installazione, senza eseguire l'aggiornamento. Predefinito = false

  Durante un aggiornamento, questa opzione viene ignorata se viene rilevata una versione di SQL Server non supportata. Per ulteriori informazioni, vedere Controllo della versione di SQL Server.

- **/installdir *directory***

  Directory vuota esistente in cui verranno installati i componenti. Impostazione predefinita= c:\Programmi\Citrix.

- **/logpath *percorso***

  Percorso del file di registro. La cartella specificata deve esistere. Il programma di installazione non la crea. Impostazione predefinita= `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

  Valido solo durante l'installazione di Director. Disattiva la funzionalità di shadowing utente che utilizza Assistenza remota di Windows.

- **/noreboot**

  Impedisce un riavvio dopo l'installazione. Per la maggior parte dei componenti principali, il riavvio non è abilitato per impostazione predefinita.

- **/noresume**

  Per impostazione predefinita, quando è necessario un riavvio della macchina durante un'installazione, il programma di installazione riprende automaticamente al termine del riavvio. Per ignorare il valore predefinito, specificare `/noresume`. Ciò può risultare utile se è necessario rimontare il supporto o acquisire informazioni durante un'installazione automatica.

- **/nosql**

  Impedisce l'installazione di Microsoft SQL Server Express sul server in cui si sta installando il controller. Se questa opzione viene omessa, SQL Server Express viene installato per l'utilizzo come database del sito.

  Questa opzione non ha alcun effetto sull'installazione di SQL Server Express LocalDB utilizzato per la cache host locale.

- **/quiet** o **/passive**

  Durante l'installazione non viene visualizzata alcuna interfaccia utente. L'unica prova del processo di installazione è in Task Manager (Gestione attività) di Windows. Se questa opzione viene omessa, viene avviata l'interfaccia grafica.

- **/remove**

  Rimuove i componenti principali specificati con l'opzione `/components`.

- **/removeall**

  Rimuove tutti i componenti principali installati.

- **/sendexperiencemetrics**

  Invia automaticamente a Citrix le analisi raccolte durante l'installazione, l'aggiornamento o la rimozione. Se questa opzione viene omessa (o viene specificata l'opzione `/disableexperiencemetrics`), le analisi vengono raccolte localmente, ma non inviate automaticamente.

- **/tempdir** *directory*

  Directory che contiene i file temporanei durante l'installazione. Impostazione predefinita= c:\Windows\Temp.

- **/xenapp**

  Installa Citrix Virtual Apps. Se questa opzione viene omessa, viene installato Citrix Virtual Apps and Desktops.

Esempi di installazione di componenti principali

Il comando seguente installa un Delivery Controller, Studio, Licensing Citrix e SQL Server Express su un server. Le porte del firewall necessarie per le comunicazioni dei componenti vengono aperte automaticamente.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller
,desktopstudio,licenseserver /configure_firewall
```

Il comando seguente installa un Citrix Virtual Apps Controller, Studio e SQL Server Express sul server. Le porte del firewall necessarie per la comunicazione dei componenti vengono aperte automaticamente.

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components
controller,desktopstudio /configure_firewall
```

Utilizzare un programma di installazione VDA autonomo

Per accedere al sito di download, sono necessarie le credenziali dell'account Citrix. È necessario disporre di privilegi amministrativi elevati prima di avviare l'installazione oppure utilizzare **Esegui come amministratore**.

1. Scaricare il pacchetto appropriato da Citrix:

   - Virtual Delivery Agent per sistema operativo multisessione: `VDAServerSetup_xxxx.exe`
   - Virtual Delivery Agent per sistema operativo a sessione singola: `VDAWorkstationSetup_xxxx.exe`
   - Core Services Virtual Delivery Agent per sistema operativo a sessione singola: `VDAWorkstationCoreSetup_xxxx.exe`

2. Estrarre prima i file dal pacchetto in una directory esistente e quindi eseguire il comando di installazione o semplicemente eseguire il pacchetto.

   Per estrarre i file prima di installarli, utilizzare `/extract` con il percorso assoluto, ad esempio `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia` La directory deve esistere. In caso contrario, l'estrazione non riesce. Quindi, in un comando separato, eseguire il comando appropriato, utilizzando le opzioni valide elencate in questo articolo.

- Per `VDAServerSetup_XXXX.exe`, eseguire `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
- Per `VDAWorkstationCoreSetup_XXXX.exe`, eseguire `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
- Per `VDAWorkstationSetup_XXXX.exe`, eseguire `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

Per eseguire il pacchetto scaricato, eseguirne il nome: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` o `VDAWorkstationCoreSetup.exe`. Utilizzare le opzioni valide elencate in questo articolo.

Se si ha familiarità con il programma di installazione del prodotto completo:

- Eseguire il programma di installazione autonomo `VDAServerSetup.exe` o `VDAWorkstationSetup.exe` come se fosse il comando `XenDesktopVdaSetup.exe` in tutto tranne il nome
- Il programma di installazione `VDAWorkstationCoreSetup.exe` è diverso, perché supporta un sottoinsieme delle opzioni disponibili per gli altri programmi di installazione.

Opzioni della riga di comando per l'installazione di un VDA

Le opzioni seguenti sono valide con uno o più dei seguenti comandi (programmi di installazione): `VDAServerSetup_xxxx.exe`, `VDAWorkstationSetup_xxxx.exe` e `VDAWorkstationCoreSetup_x.exe`.

Per maggiori dettagli sulle opzioni, vedere Installare i VDA.

- **/componenti** *componente*[,*componente*]

  Elenco separato da virgole di componenti da installare o rimuovere. I valori validi sono:

  - `VDA`: Virtual Delivery Agent
  - `PLUGINS`: app Citrix Workspace per Windows

  Per installare il VDA e l'app Citrix Workspace per Windows, specificare `/components vda,plugins`.

  Se questa opzione viene omessa, viene installato solo il VDA (non l'app Citrix Workspace).

  Questa opzione non è valida quando si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`. Tale programma di installazione non può installare l'app Citrix Workspace.

- **/controllers** "*controller* [*controller*]"

  FQDN separati da spazi dei controller con cui il VDA può comunicare, racchiusi tra virgolette diritte. Non specificare entrambe le opzioni `/site_guid` e `/controllers`.

- **/disableexperiencemetrics**

  Impedisce l'invio automatico a Citrix delle analisi raccolte durante l'installazione, l'aggiornamento o la rimozione.

- **/enable_hdx_ports**

  Apre le porte del firewall di Windows richieste dal VDA e dalle funzionalità abilitate (ad eccezione di Assistenza remota di Windows), se viene rilevato il servizio Windows Firewall, anche se il firewall non è abilitato. Se si utilizza un firewall diverso o nessun firewall, è necessario configurare manualmente il firewall. Per informazioni sulle porte, vedere Porte di rete.

  Per aprire le porte UDP utilizzate dal trasporto adattivo HDX, specificare l'opzione /`enable_hdx_udp_ports`, oltre a questa opzione /`enable_hdx_ports`.

- **/enable_hdx_udp_ports**

  Apre le porte UDP del firewall di Windows utilizzate dal trasporto adattivo HDX, se viene rilevato il servizio Windows Firewall, anche se il firewall non è abilitato. Se si utilizza un firewall diverso o nessun firewall, è necessario configurare manualmente il firewall. Per informazioni sulle porte, vedere Porte di rete.

  Per aprire porte aggiuntive utilizzate dal VDA, specificare l'opzione /`enable_hdx_ports`, oltre all'opzione /`enable_hdx_udp_ports`.

- **/enable_real_time_transport**

  Abilita o disabilita l'uso di UDP per i pacchetti audio (RealTime Audio Transport per audio). L'attivazione di questa funzione può migliorare le prestazioni audio. Includere l'opzione /`enable_hdx_ports` se si desidera che le porte UDP vengano aperte automaticamente quando viene rilevato il servizio Windows Firewall.

- **/enable_remote_assistance**

  Attiva la funzionalità di shadowing in Assistenza remota di Windows per l'utilizzo con Director. Se si specifica questa opzione, Assistenza remota di Windows apre le porte dinamiche del firewall.

- **/enablerestore** o **/enablerestorecleanup**

  (valido solo per VDA a sessione singola) Abilita il ritorno automatico al punto di ripristino, se l'installazione o l'aggiornamento del VDA non vanno a buon fine.

  Se l'installazione/aggiornamento viene completato correttamente:

  - /`enablerestorecleanup` indica al programma di installazione di rimuovere il punto di ripristino.
  - /`enablerestore` indica al programma di installazione di mantenere il punto di ripristino, anche se non è stato utilizzato.

Per ulteriori informazioni, vedere Ripristino in caso di errore di installazione o aggiornamento.

- **/enable_ss_ports**

  Apre le porte del firewall Windows necessarie per la condivisione dello schermo, se viene rilevato il servizio Windows Firewall, anche se il firewall non è abilitato. Se si utilizza un firewall diverso o nessun firewall, è necessario configurare manualmente il firewall.

- **/exclude** "*componente*"[,"*componente*"]

  Impedisce l'installazione di uno o più componenti opzionali separati da virgole, ciascuno racchiuso tra virgolette diritte. Ad esempio, l'installazione o l'aggiornamento di un VDA su un'immagine non gestita da MCS non richiede il componente Machine Identity Service. I valori validi sono i seguenti:

Sistema operativo multisessione	Sistema operativo a sessione singola	Core Services per sistema operativo a sessione singola
Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in
Citrix Backup and Restore	Citrix Backup and Restore	Citrix Browser Content Redirection
Citrix Browser Content Redirection	Citrix Browser Content Redirection	Citrix Personalization **for** App-V - VDA
Citrix MCS IODriver	Citrix MCS IODriver	Citrix Telemetry Service
Citrix Personalization **for** App-V - VDA	Citrix Personalization **for** App-V - VDA	Citrix Universal Print Client
Citrix Profile Management	Citrix Profile Management	Citrix Vda Log Capture Service
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in	CSE Component
Citrix Rendezvous V2	Citrix Rendezvous V2	Director VDA Plug-in
Citrix Telemetry Service	Citrix Telemetry Service	Machine Management Provider

Sistema operativo multisessione	Sistema operativo a sessione singola	Core Services per sistema operativo a sessione singola
`Citrix Universal Print Client`	`Citrix Universal Print Client`	`VDA Monitor Plug-in`
`Citrix Vda Log Capture Service`	`Citrix Vda Log Capture Service`	`VDA WMI Proxy Plug-in`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`	
`CSE Component`	`CSE Component`	
`Director VDA Plug-in`	`Director VDA Plug-in`	
`Machine Identity Service`	`Machine Identity Service`	
`Machine Management Provider`	`Machine Management Provider`	
`VDA Monitor Plug-in`	`User Personalization Layer`	
`VDA WMI Proxy Plug-in`	`VDA Monitor Plug-in`	
	`VDA WMI Proxy Plug-in`	

L'esclusione di Citrix Profile Management dall'installazione (`/exclude "Citrix Profile Management"`) influisce sul monitoraggio e la risoluzione dei problemi dei VDA con Citrix Director. Nelle pagine **User details** (Dettagli utente) ed **EndPoint**, i pannelli Personalization e Logon Duration riportano errori. Nelle pagine **Dashboard** e **Trends**, il pannello Average Logon Duration visualizza i dati solo per i computer in cui è installato Profile Management.

Anche se si utilizza una soluzione di gestione dei profili utente di terze parti, Citrix consiglia di installare ed eseguire Citrix Profile Management Service. L'attivazione del servizio Citrix Profile Management non è necessaria.

Se si specificano entrambi `/exclude` e `/includeadditional` con lo stesso nome di componente, tale componente non viene installato.

Questa opzione non è valida quando si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`. Tale programma di installazione esclude automaticamente molti di questi elementi.

- **/h** o **/help**

  Visualizza la Guida dei comandi.

- **/includeadditional** "*componente*"[,"*componente*"]

  Include l'installazione di uno o più componenti opzionali separati da virgole, ciascuno racchiuso tra virgolette diritte. Questa opzione può risultare utile quando si crea una distribuzione di Accesso remoto PC e si desidera installare altri componenti non inclusi per impostazione predefinita. I valori validi sono i seguenti:

Sistema operativo multisessione	Sistema operativo a sessione singola
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

  Se si specificano entrambi `/exclude` e `/includeadditional` con lo stesso nome di componente, tale componente non viene installato.

- **/installdir** *directory*

  Directory vuota esistente in cui verranno installati i componenti. Impostazione predefinita= c:\Programmi\Citrix.

- **/install_mcsio_driver**

  Non utilizzare. Utilizzare invece `/includeadditional "Citrix MCS IODriver"` o `/exclude "Citrix MCS IODriver"`

- **/logpath** *percorso*

  Percorso del file di registro. La cartella specificata deve esistere. Il programma di installazione non la crea. Impostazione predefinita= "%TEMP%\Citrix\XenDesktop Installer"

  Questa opzione non è disponibile nell'interfaccia grafica.

- **/masterimage**

  Valido solo quando si installa un VDA in una macchina virtuale. Imposta il VDA come immagine da utilizzare per creare altre macchine. Questa opzione è equivalente a `/mastermcsimage`.

  Questa opzione non è valida quando si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`.

- **/mastermcsimage**

  Specifica che questa macchina verrà utilizzata come immagine con Machine Creation Services. Questa opzione è equivalente a `/masterimage`.

- **/masterpvsimage**

  Specifica che il computer verrà utilizzato come immagine con Citrix Provisioning o uno strumento di provisioning di terze parti (ad esempio Microsoft System Center Configuration Manager) per eseguire il provisioning delle macchine virtuali.

- **/no_mediafoundation_ack**

  Riconosce che Microsoft Media Foundation non è installato e diverse funzionalità multimediali HDX non verranno installate e non funzioneranno. Se questa opzione viene omessa e Media Foundation non è installato, l'installazione del VDA viene terminata poiché i prerequisiti non sono soddisfatti. La maggior parte delle edizioni di Windows supportate ha Media Foundation già installato, ad eccezione delle edizioni N. Se si abilita *manualmente* Funzionalità Windows > Funzionalità multimediali, la chiave di registro richiesta da Citrix Meta Installer potrebbe non avere un valore impostato. Controllare la chiave di registro `SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` prima di avviare il processo di installazione per confermare che il valore esista e non sia vuoto.

- **/nodesktopexperience**

  La funzionalità Enhanced desktop experience non è più disponibile. Questa opzione (e l'impostazione dei criteri) viene ignorata, se specificato.

  Valida solo quando si installa un VDA per un sistema operativo multisessione. Impedisce l'attivazione della funzionalità Enhanced desktop experience. Questa funzione è inoltre controllata con l'impostazione dei criteri Enhanced Desktop Experience Citrix.

- **/noreboot**

  Impedisce un riavvio dopo l'installazione. Il VDA non può essere utilizzato fino a dopo un riavvio.

- **/noresume**

  Per impostazione predefinita, quando è necessario un riavvio della macchina durante un'installazione, il programma di installazione riprende automaticamente al termine del riavvio. Per ignorare il valore predefinito, specificare `/noresume`. Ciò può risultare utile se è necessario rimontare il supporto o acquisire informazioni durante un'installazione automatica.

- **/physicalmachine**

  Utilizzare questo argomento insieme a /remotepc per l'installazione di RemotePC. In caso contrario, il VDA potrebbe non comportarsi come previsto in alcuni scenari utente.

- **/portnumber** *porta*

  Valido solo quando viene specificata l'opzione /reconfig. Numero di porta da abilitare per le comunicazioni tra il VDA e il Controller. La porta configurata in precedenza è disabilitata, a meno che non sia la porta 80.

- **/proxyconfig** "*indirizzo o percorso del file PAC*"

  Valido solo se il comando contiene /includeadditional "Citrix Rendezvous V2". L'indirizzo o il percorso del file PAC del proxy da utilizzare con il protocollo Rendezvous. Per dettagli delle funzionalità, vedere Protocollo Rendezvous.

  - Formato dell'indirizzo proxy: http://<url-or-ip>:<port>
  - Formato del file PAC: http://<url-or-ip>:<port>/<path>/<filename>.pac

- **/quiet** o **/passive**

  Durante l'installazione non viene visualizzata alcuna interfaccia utente. L'unica prova del processo di installazione e configurazione è in Task Manager di Windows. Se questa opzione viene omessa, viene avviata l'interfaccia grafica.

- **/reconfigure**

  Consente di personalizzare le impostazioni del VDA configurate in precedenza se utilizzate con le opzioni /portnumber, /controllers o /enable_hdx_ports. Se si specifica questa opzione senza specificare anche l'opzione /quiet, viene avviata l'interfaccia grafica per la personalizzazione del VDA.

- **/remotepc**

  Valido solo per le distribuzioni di Accesso remoto PC (sistema operativo a sessione singola) o per le connessioni mediate (sistema operativo multisessione). Esclude l'installazione di componenti aggiuntivi (vedere elenchi di componenti con le opzioni /exclude e /includeadditional).

  Questa opzione non è valida quando si utilizza il programma di installazione VDAWorkstationCoreSetup.exe. Tale programma di installazione esclude automaticamente l'installazione di questi componenti.

  /remotepc non è compatibile con l'opzione /servervdi.

- **/remove**

  Rimuove i componenti specificati con l'opzione /components.

- **/remove_appdisk_ack**

  Autorizza il programma di installazione del VDA a disinstallare il plug-in VDA AppDisks, se è installato.

- **/remove_pvd_ack**

  Autorizza il programma di installazione VDA a disinstallare Personal vDisk se è installato.

- **/removeall**

  Rimuove il VDA. Non rimuove l'app Citrix Workspace (se installata).

- **/sendexperiencemetrics**

  Invia automaticamente a Citrix le analisi raccolte durante l'installazione, l'aggiornamento o la rimozione. Se questa opzione viene omessa (o viene specificata l'opzione `/disableexperiencemetrics`), le analisi vengono raccolte localmente, ma non inviate automaticamente.

- **/servervdi**

  Installa un VDA per sistema operativo a sessione singola in un computer multisessione Windows supportato. Omettere questa opzione quando si installa un VDA per sistema operativo multisessione su un computer multisessione Windows.

  Prima di utilizzare questa opzione, vedere VDI del server.

  Utilizzare questa opzione solo con il programma di installazione del VDA completo.

- **/site_guid** *guid*

  Identificatore univoco globale (GUID) dell'unità organizzativa (OU) di Active Directory del sito. Questo associa un desktop virtuale a un sito quando si utilizza Active Directory per l'individuazione (l'aggiornamento automatico è il metodo di individuazione consigliato e predefinito). Il GUID del sito è una proprietà del sito visualizzata in Studio. Non specificare entrambe le opzioni `/site_guid` e `/controllers`.

- **/tempdir** *directory*

  Directory in cui contenere i file temporanei durante l'installazione. Impostazione predefinita= c:\Windows\Temp.

  Questa opzione non è disponibile nell'interfaccia grafica.

- **/virtualmachine**

  Valido solo quando si installa un VDA in una macchina virtuale. Sovrascrive l'individuazione da parte del programma di installazione di una macchina fisica, in cui le informazioni del BIOS passate alle macchine virtuali le fanno apparire come macchine fisiche.

  Questa opzione non è disponibile nell'interfaccia grafica.

- **/xendesktopcloud**

  Indica che il VDA è installato in una distribuzione di Citrix DaaS (Citrix Cloud).

Esempi di installazione di un VDA

Installare un VDA con il programma di installazione del prodotto completo:

Il comando seguente installa un VDA per sistema operativo a sessione singola e l'app Citrix Workspace nella posizione predefinita in una macchina virtuale. Questo VDA verrà utilizzato come immagine e utilizzerà MCS per eseguire il provisioning delle macchine virtuali. Il VDA verrà registrato inizialmente con il controller sul server denominato `Contr-Main` nel dominio `mydomain`. Il VDA utilizzerà il livello di personalizzazione utente e Assistenza remota di Windows.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda
,plugins /controllers "Contr-Main.mydomain.local"/enable_hdx_ports
 /includeadditional "user personalization layer"/mastermcsimage /
enable_remote_assistance
```

Installare un VDA con sistema operativo a sessione singola con il programma di installazione autonomo di VDAWorkstationCoreSetup:

Il comando seguente installa un VDA di Core Services in un sistema operativo a sessione singola per l'utilizzo in una distribuzione VDI o Accesso remoto PC. L'app Citrix Workspace e altri servizi non core non vengono installati. Viene specificato l'indirizzo di un controller e le porte del servizio Windows Firewall verranno aperte automaticamente. L'amministratore gestirà i riavvii.

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.
com"/enable_hdx_ports /noreboot
```

Personalizzare un VDA

Dopo aver installato un VDA, è possibile personalizzare diverse impostazioni. Dalla directory `\x64\XenDesktop Setup` sul supporto del prodotto, eseguire `XenDesktopVdaSetup.exe`utilizzando una o più delle seguenti opzioni, descritte in Opzioni della riga di comando per l'installazione di un VDA.

- `/reconfigure` (necessario per la personalizzazione di un VDA)
- `/h` o `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

Risoluzione dei problemi relativi ai VDA

- Nella visualizzazione Studio per un gruppo di consegna, la voce **Installed VDA version** (Versione VDA installata) nel riquadro **Details** potrebbe non essere la versione installata nei computer. La visualizzazione Programmi e funzionalità di Windows della macchina mostra la versione VDA effettiva.
- Dopo l'installazione di un VDA, non è possibile distribuire app o un desktop agli utenti fino a quando non si registra con un Delivery Controller.

  Per informazioni sui metodi di registrazione dei VDA e sulla risoluzione dei problemi di registrazione, vedere Registrazione dei VDA.

Opzioni della riga di comando per l'installazione di un Universal Print Server

L'opzione seguente è valida con il comando `XenDesktopPrintServerSetup.exe`.

- **/enable_upsserver_port**

Software	Cartella	Nome file
Runtime di Microsoft Visual C++ 2017, a 32 bit e 64 bit.	**Support > VcRedist_2017**	`vcredist_x64.exe` e `vcredist_x86.exe`
Citrix Diagnostic Facility	x64 > Virtual Desktop Components	`cdf_x64.msi`
Componente server Universal Print Server	x64 > Universal Print Server	`UpsServer_x64.msi`

Quando questa opzione non è specificata, il programma di installazione visualizza la pagina **Firewall** dell'interfaccia grafica. Selezionare **Automatically** perché il programma di installazione aggiunga automaticamente le regole firewall di Windows o **Manually** per consentire all'amministratore di configurare manualmente il firewall.

Dopo aver installato il software sui server di stampa, configurare Universal Print Server utilizzando le indicazioni fornite in Provisioning delle stampanti.

Ulteriori informazioni

Per informazioni su come Citrix riporta il risultato delle installazioni dei componenti, vedere Codici restituiti per l'installazione Citrix.

Installare Web Studio

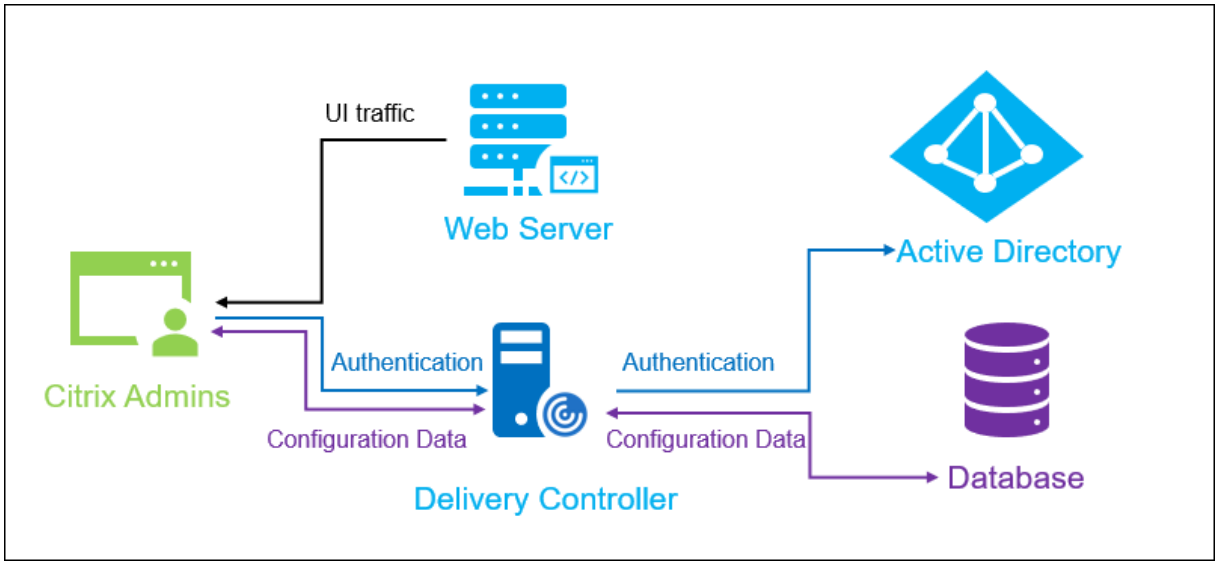
April 4, 2024

> **Requisiti di licenza:**
>
> Per utilizzare Web Studio, è necessario disporre di uno dei seguenti tipi di licenza:
>
> - Licenza di abbonamento universale Citrix.
> - Abbonamento Citrix on-premise per licenze al dettaglio annuali e a termine.
> - Qualsiasi licenza locale per Citrix Service Providers (CSP).

Introduzione

Citrix Studio è una console di gestione basata su Windows che consente di configurare e gestire l'implementazione di Citrix Virtual Apps and Desktops. Web Studio è la nuova generazione di Citrix Studio, una console di gestione basata sul Web che offre la parità di funzionalità completa con Citrix Studio. Web Studio ha lo stesso aspetto dell'interfaccia Full Configuration di Citrix DaaS e modernizza l'esperienza di gestione fornendo un'esperienza Web nativa.

È possibile distribuire Web Studio su qualsiasi server Windows con Internet Information Service (IIS) installato. Per una distribuzione rapida, si consiglia di installare Web Studio insieme a un Delivery Controller. In tal caso, Web Studio viene installato come sito Web sul Delivery Controller. Consigliamo di seguire questa configurazione per semplificare l'architettura e ridurre i costi di gestione. Il diagramma seguente illustra l'architettura di Web Studio:



Un flusso di lavoro generale per rendere Web Studio operativo e funzionante è il seguente:

1. Installare Web Studio.
2. Configurare un sito.
3. Aggiungere i Delivery Controller a Web Studio per la gestione.
4. Accedere a Web Studio.

Nuove funzionalità disponibili in Web Studio rispetto a 2305

Vedere l'articolo Novità.

Requisiti di sistema

Sistemi operativi supportati:

- Windows Server 2022
- Windows Server 2019, edizioni Standard e Datacenter e con l'opzione Server Core
- Windows Server 2016, edizioni Standard e Datacenter e con l'opzione Server Core
- Windows 11
- Windows 10

Prerequisiti

Questa versione di Web Studio è compatibile con le distribuzioni di Citrix Virtual Apps and Desktops 2212 e versioni successive.

Per le distribuzioni precedenti alla 2212, eseguire prima l'aggiornamento a 2212 e quindi installare Web Studio.

Limitazioni note

- Web Studio e StoreFront devono essere installati su macchine separate.

  > **Nota:**
  >
  > Se Web Studio e StoreFront sono installati sulla stessa macchina e si desidera aggiornarli entrambi a questa versione, vedere Aggiornamento di Web Studio per istruzioni dettagliate.

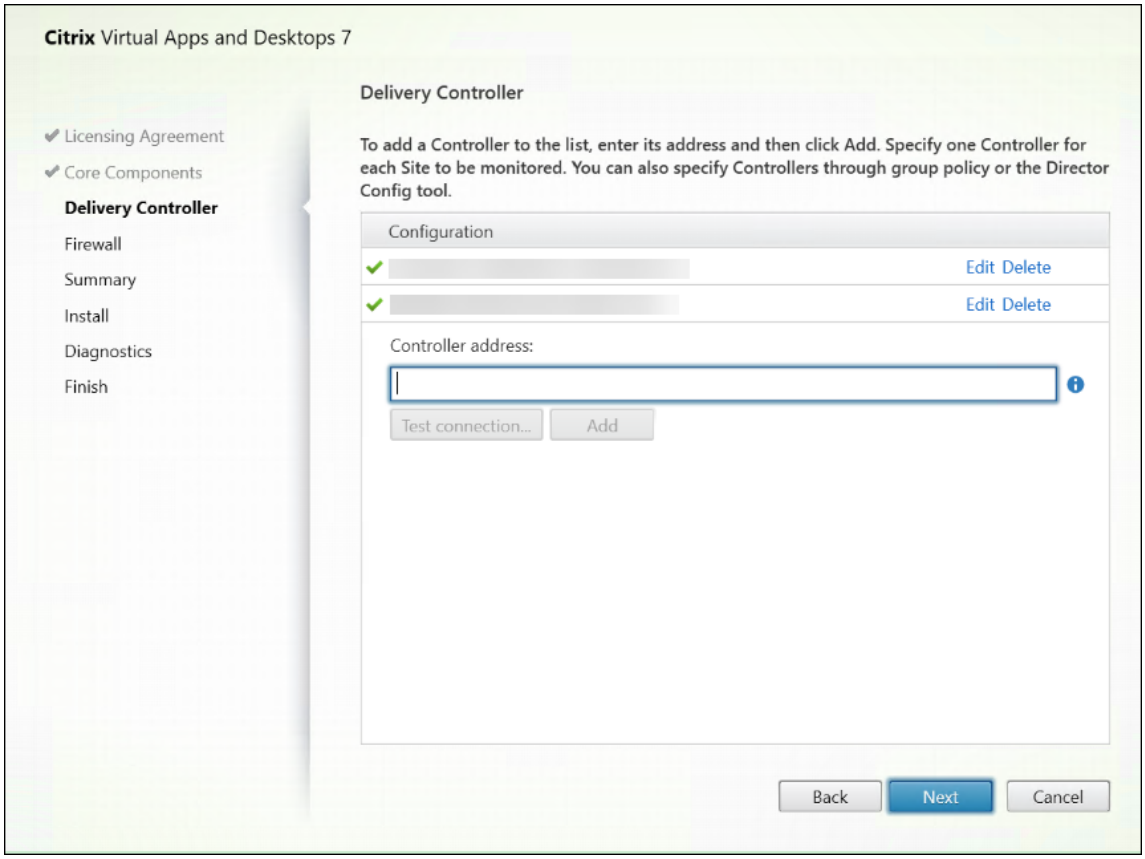
- Se si utilizzano Web Studio e Citrix Studio in modo intercambiabile, tenere presente la seguente limitazione: un modello creato in Web Studio non viene visualizzato in Citrix Studio e viceversa. Questo perché Web Studio utilizza un database diverso da Citrix Studio per archiviare i modelli. Come soluzione alternativa, creare un criterio a partire da un modello in Web Studio e quindi creare un nuovo modello a partire da quel criterio in Citrix Studio e viceversa.
- Per garantire una corretta installazione di Web Studio, non modificare il nome del sito predefinito (**Default Web Site**) in Internet Information Services (IIS) Manager. Qualsiasi modifica al nome del sito predefinito comporta errori di installazione.

Installare Web Studio

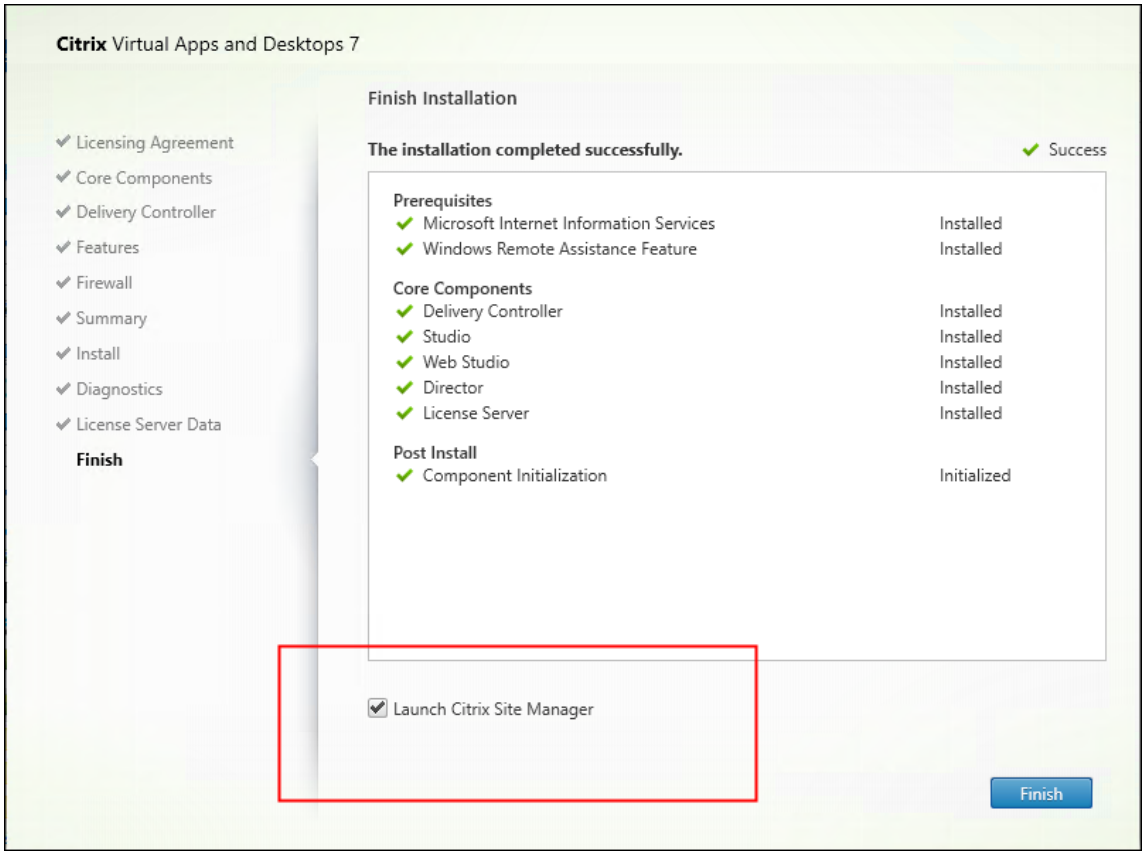
Le seguenti informazioni completano la guida contenuta in Installare i componenti principali. Per installare Web Studio:

- Installare Web Studio utilizzando il programma di installazione ISO completo del prodotto per Citrix Virtual Apps and Desktops. L'installatore ISO verifica i prerequisiti, installa eventuali componenti mancanti, configura il sito Web di Web Studio (sul Delivery Controller se incluso nell'installazione del Delivery Controller) ed esegue la configurazione di base.
- Se Web Studio non è stato incluso durante l'installazione, utilizzare il programma di installazione per aggiungerlo.
- Quando si installa Web Studio, viene richiesto di digitare l'indirizzo di un Delivery Controller.

  > **Nota:**
  >
  > - È possibile aggiungere più di un Delivery Controller. Web Studio tenta di connettersi a essi in ordine casuale. Se il Delivery Controller a cui Web Studio sta tentando di connettersi non è raggiungibile, Web Studio ricorre automaticamente ad altri Delivery Controller.
  > - Se Director è stato selezionato in **Core Components** e installato, i Delivery Controller che si aggiungono qui vengono utilizzati sia per Web Studio che per Director.
  > - Se non è stato configurato il certificato di attendibilità pubblico esterno e non si desidera richiedere il certificato a una CA aziendale, è sufficiente configurare l'FQDN del proprio Delivery Controller.
  > - Se si dispone del certificato di attendibilità pubblico esterno e si è in grado di configurare il DNS pubblico per il proprio Delivery Controller, è possibile digitare il nome DNS come indirizzo del Delivery Controller.
  > - Se si è in grado di richiedere il certificato alla propria CA aziendale e di specificare il proprio DNS personale, è possibile aggiungere il proprio DNS personale come indirizzo del Delivery Controller.



- Per proteggere le comunicazioni tra il browser e il server Web e tra il browser e il Delivery Controller, la crittografia TLS deve essere abilitata sul sito Web IIS che ospita Web Studio e sul Delivery Controller. Se non è configurato alcun certificato TLS per il Delivery Controller, il programma di installazione crea un certificato autofirmato, con il nome di dominio completo del Delivery Controller e localhost come certificato del nome DNS. Se è configurato un certificato TLS, il programma di installazione non apporta alcuna modifica. Per ulteriori informazioni sulla crittografia TLS, vedere Proteggere una distribuzione di Web Studio (facoltativo).
- Nella pagina **Finish**, la casella di controllo **Launch Site Manager** è selezionata per impostazione predefinita in modo che Citrix Site Manager si apra automaticamente. Per avviarlo in un secondo momento, aprire il menu Start del desktop e selezionare **Citrix > Citrix Site Manager**. Prima di avviare Web Studio, è necessario utilizzare Citrix Site Manager per creare un sito o unirsi a un sito esistente. Per ulteriori informazioni, vedere Configurare un sito.



> **Nota:**
>
> È inoltre possibile utilizzare la riga di comando per installare Web Studio. Esempio: `.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local"/configure_firewall /quiet`. Per ulteriori informazioni, vedere Installare utilizzando la riga di comando.

Configurare un sito

Per configurare la distribuzione di Citrix Virtual Apps and Desktops (noto anche come sito), utilizzare lo strumento Citrix Site Manager. Lo strumento viene installato automaticamente con un Delivery Controller.

Per configurare un sito, effettuare le seguenti operazioni:

1. Su un Delivery Controller, aprire il menu Start del desktop, quindi selezionare **Citrix > Citrix Site Manager**.
2. In Citrix Site Manager, selezionare **Create a site** (Crea un sito). Viene visualizzata la procedura guidata di configurazione del sito.
3. Creare un sito e configurarne le impostazioni come segue:

- Nella pagina **Introduction**, digitare un nome da dare al sito.
- La pagina **Databases** contiene le selezioni per l'impostazione dei database di registrazione del sito, del monitoraggio e della configurazione. Per ulteriori informazioni, vedere il Passaggio 3. Database.
- Nella pagina **Licensing** specificare l'indirizzo del server licenze e quindi indicare la licenza da utilizzare (installare). Per ulteriori informazioni, vedere il Passaggio 4. Licenze.

4. Nella pagina **Summary** (Riepilogo), controllare tutte le impostazioni e fare clic su **Submit** (Invia).

   L'indirizzo IP di questo Controller viene aggiunto automaticamente al sito.

   > **Nota:**
   >
   > L'utente che crea un sito ne diventa amministratore completo. Per ulteriori informazioni, vedere Amministrazione delegata.

Se si installa un nuovo controller dopo aver creato un sito, è necessario aggiungere il controller al sito. I passaggi dettagliati sono i seguenti:

1. Eseguire Citrix Site Manager su questo nuovo controller.
2. Selezionare **Join an existing site** (Unirsi a un sito esistente).
3. Digitare l'indirizzo di un controller già aggiunto al sito.
4. Fare clic su **Submit**.

Aggiungere Delivery Controller a Web Studio per la gestione

Utilizzare lo strumento di configurazione di Studio per aggiungere i Delivery Controller a Web Studio per la gestione. Questo strumento è disponibile nella cartella di installazione di Web Studio.

Per impostazione predefinita, lo strumento è installato nella seguente cartella predefinita.

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Si supponga di voler configurare i seguenti due Delivery Controller per il sito che si desidera gestire con Web Studio: `ddc1.studio.local` e `ddc2.studio.local`. Eseguire il seguente comando PowerShell:

- `.\StudioConfig.exe /server "ddc1.studio.local,ddc2.studio.local"`

> **Nota:**
>
> - Lo strumento richiede le autorizzazioni dell'amministratore del computer.
> - Le modifiche apportate alla configurazione del Delivery Controller potrebbero non avere effetto immediato a causa delle impostazioni della cache sul server IIS. Per un effetto imme-

> diato, accedere al server Web Studio, aprire Gestione Internet Information Services (IIS), passare a Pagina iniziale > Siti > Sito Web predefinito e selezionare **Riavvia** nel riquadro Gestione del sito Web.

Configurare Web Studio come proxy per i Delivery Controller (opzionale)

Per impostazione predefinita, quando si gestisce la distribuzione utilizzando la console Web Studio, ci si connette sia al server Web Studio che ai Delivery Controller tramite il browser Web. Offriamo un'opzione per configurare il server Web Studio come proxy per i Delivery Controller. Di conseguenza, quando si gestisce la distribuzione, ci si connette solo al server Web Studio.

Questa sezione guida l'utente alla configurazione del server Web Studio come proxy per i Delivery Controller. Si presume che Web Studio e Delivery Controller siano installati su server diversi.

Prima di iniziare, verificare di avere tutti i componenti principali necessari installati nella distribuzione. Per ulteriori informazioni, vedere Installare i componenti principali.

Per abilitare la modalità proxy per Web Studio, effettuare le seguenti operazioni:

1. Effettuare il backup del file `manifest.json` in `C:\Program Files\Citrix\Web Studio\Site\assets\json\`.
2. Sul server Web Studio, eseguire Windows PowerShell come amministratore.
3. Eseguire il seguente comando sostituendo `fqdn_of_webstudio_machine` con il nome di dominio completo del proprio server Web Studio.

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe"/
   ProxyServer fqdn_of_webstudio_machine
   ```

Per disabilitare la modalità proxy per Web Studio, sovrascrivere `manifest.json` in `C:\Program Files\Citrix\Web Studio\Site\assets\json\` con il file `manifest.json` di cui si è eseguito il backup.

> **Nota:**
>
> La procedura consigliata è proteggere la distribuzione di Web Studio utilizzando un certificato di attendibilità pubblico esterno o un certificato rilasciato da una CA (autorità di certificazione) aziendale. Per ulteriori informazioni, vedere Proteggere una distribuzione di Web Studio.

Accedere a Web Studio

Il sito Web Studio si trova all'indirizzo `https://<address of the server hosting Web Studio>/Citrix/WebStudio`.

Per accedere a Web Studio, aprire il menu Start del desktop e selezionare **Citrix > Citrix Web Studio**. Gli amministratori con autorizzazioni per Web Studio devono essere utenti del dominio Active Directory. Quando si accede a Web Studio, considerare i seguenti scenari:

- Se non si sono ancora specificati i Delivery Controller per il sito. Viene richiesto di specificare un Delivery Controller in modo da avere accesso temporaneo a Web Studio.
- Se i Delivery Controller specificati non sono attualmente raggiungibili, non è possibile accedere a Web Studio. Verificare le proprie connessioni per assicurarsi che i Delivery Controller siano raggiungibili. Oppure specificare un Delivery Controller alternativo in modo da avere accesso temporaneo a Web Studio.

Passaggi successivi

1. Installare i VDA
2. Utilizzare Web Studio per distribuire app e desktop virtuali ai propri utenti come segue:
   a) Creare un catalogo di macchine
   b) Creare un gruppo di consegna
   c) Creare un gruppo di applicazioni (facoltativo)

Installare i VDA

April 3, 2024

> **Importante:**
>
> Se si sta eseguendo l'aggiornamento e nella versione corrente è installato il software Personal vDisk o AppDisks, vedere Rimozione di PvD, AppDisk e host non supportati.

Esistono due tipi di VDA per computer Windows: VDA per sistema operativo multisessione e VDA per sistema operativo a sessione singola (per informazioni sui VDA per macchine Linux, vedere la documentazione relativa a Linux Virtual Delivery Agent).

Prima di iniziare un'installazione, vedere Prepararsi all'installazione e completare tutte le attività di preparazione.

Prima di installare i VDA, installare i componenti principali. È inoltre possibile creare il sito prima di installare i VDA.

In questo articolo viene descritta la sequenza di installazione guidata di un VDA. Vengono forniti equivalenti della riga di comando. Per ulteriori informazioni, vedere Installare utilizzando la riga di comando.

Passaggio 1. Scaricare il software del prodotto e avviare la procedura guidata

Se si utilizza il programma di installazione del prodotto completo:

1. Se non si è ancora scaricato l'ISO del prodotto:
   - Utilizzare le credenziali dell'account Citrix per accedere alla pagina di download di Citrix Virtual Apps and Desktops. Scaricare il file ISO del prodotto.
   - Decomprimere il file. Facoltativamente, masterizzare un DVD con il file ISO.
2. Utilizzare un account amministratore locale sull'immagine o sul computer in cui si sta installando il VDA. Inserire il DVD nell'unità o montare il file ISO. Se il programma di installazione non si avvia automaticamente, fare doppio clic sull'applicazione **AutoSelect** sull'unità montata.

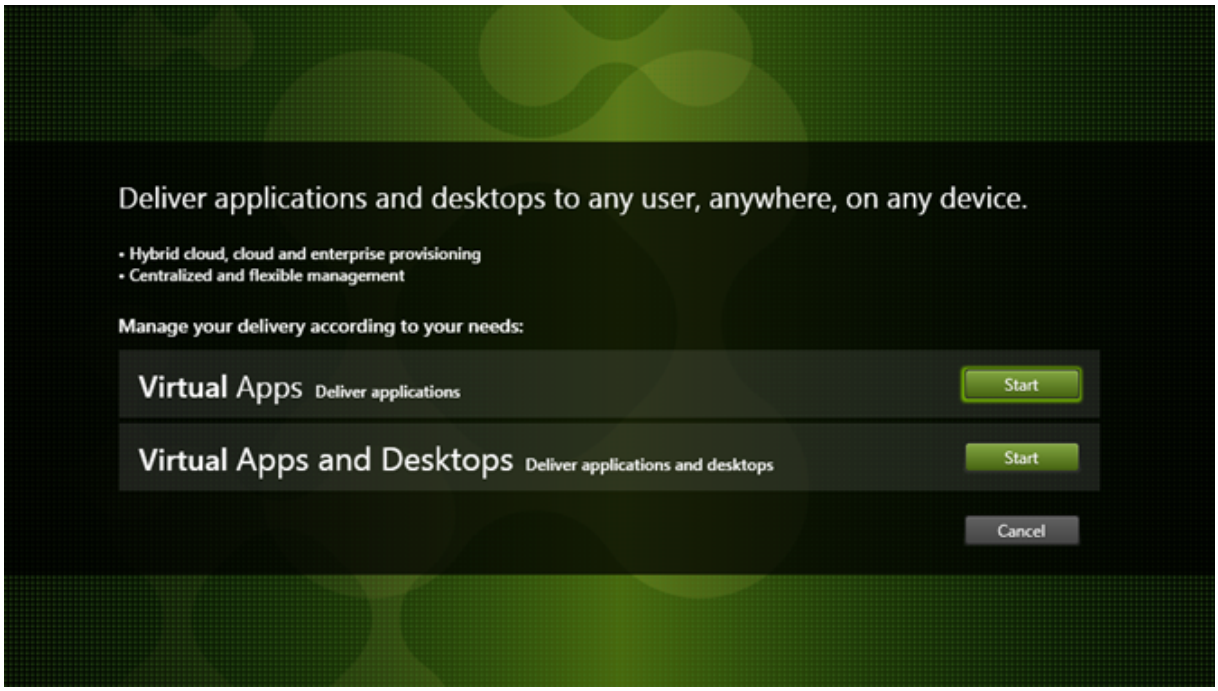
   Viene avviata l'installazione guidata.

Se si utilizza un pacchetto autonomo:

1. Utilizzare le credenziali dell'account Citrix per accedere alla pagina di download di Citrix Virtual Apps and Desktops. Scaricare il pacchetto appropriato:
   - `VDAServerSetup_2308.exe`: *Versione* del VDA per sistema operativo multisessione
   - `VDAWorkstationSetup_2308.exe`: *Versione* del VDA per sistema operativo a sessione singola
   - `VDAWorkstationCoreSetup_2308.exe`: *versione* del Core Services VDA per sistema operativo a sessione singola
2. Fare clic con il pulsante destro del mouse sul pacchetto e scegliere **Esegui come amministratore.**

   Viene avviata l'installazione guidata.

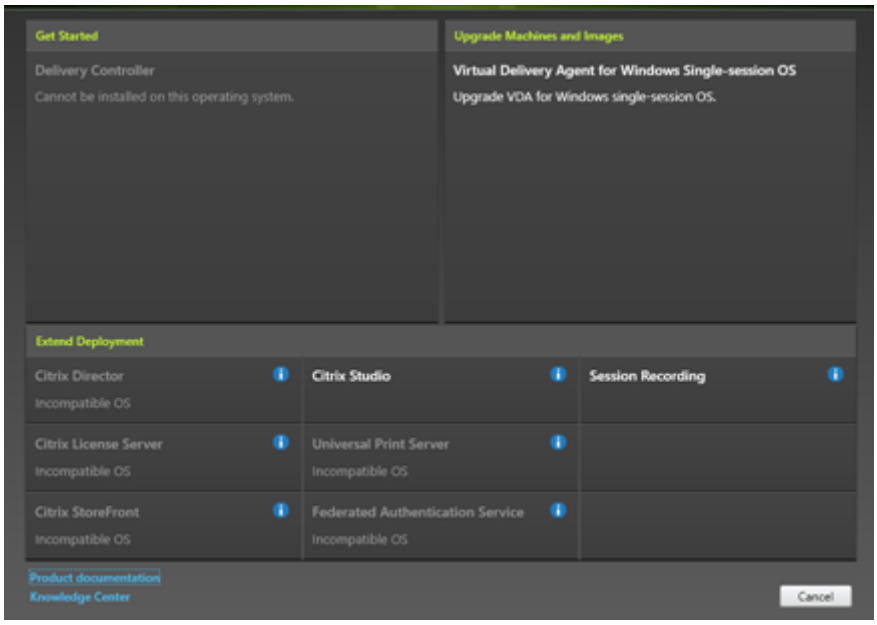
Passaggio 2. Scegliere il prodotto da installare



Fare clic su **Start** accanto al prodotto da installare: Citrix Virtual Apps o Citrix Virtual Desktops. Se nel computer è già installato un componente di Citrix Virtual Apps o Citrix Virtual Desktops, questa pagina non viene visualizzata.

Opzione della riga di comando: `/xenapp` per installare Citrix Virtual Apps. Viene installato Citrix Virtual Desktops se questa opzione viene omessa.

Passaggio 3. Selezionare il VDA

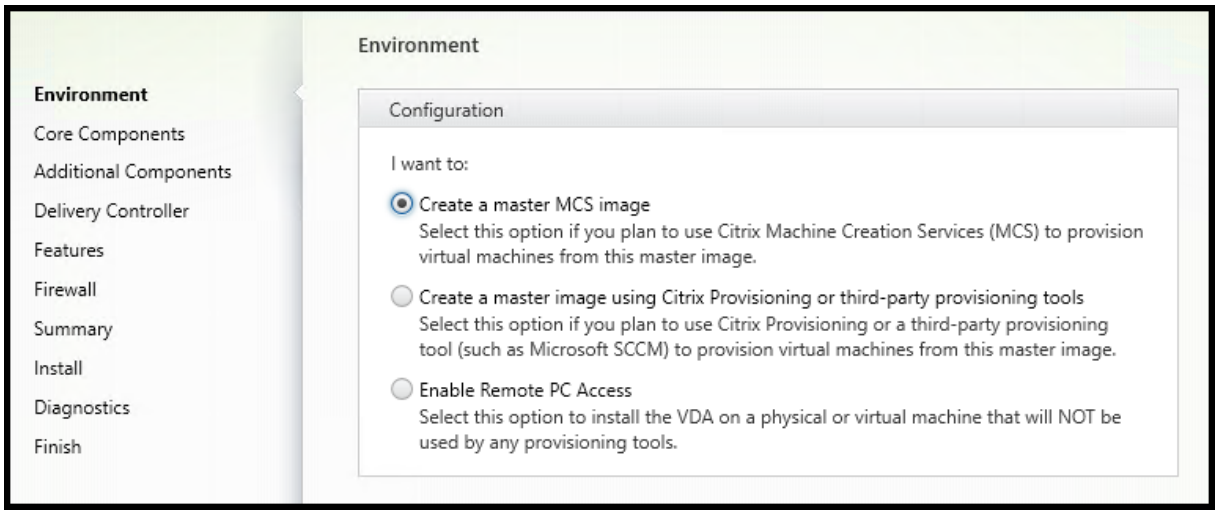


Selezionare la voce **Virtual Delivery Agent**. Il programma di installazione rileva se è in esecuzione su un sistema operativo a sessione singola o multisessione, quindi offre solo il tipo di VDA appropriato.

Ad esempio, quando si esegue il programma di installazione su un computer Windows Server 2019, è disponibile l'opzione di VDA per sistema operativo multisessione. L'opzione VDA per sistema operativo a sessione singola non è disponibile.

Se si tenta di installare (o eseguire l'aggiornamento a) un VDA per Windows su un sistema operativo non supportato per questa versione di Citrix Virtual Apps and Desktops, viene visualizzato un messaggio di informazioni sulle opzioni.

Passaggio 4. Specificare come verrà utilizzato il VDA



Nella pagina **Environment** specificare la modalità di utilizzo del VDA, indicando se si utilizzerà il computer come immagine per eseguire il provisioning di più macchine.

L'opzione scelta influisce sugli strumenti di provisioning Citrix che verranno installati automaticamente (se presenti) e sui valori predefiniti nella pagina Additional Components (Componenti aggiuntivi) del programma di installazione dei VDA.

Diversi MSI (di provisioning e altri) vengono installati automaticamente quando si installa un VDA. L'unico modo di impedirne l'installazione è con l'opzione `/exclude` in un'installazione dalla riga di comando.

Scegliere una delle seguenti opzioni:

- **Create a master MCS image (Crea un'immagine MCS master):** selezionare questa opzione per installare un VDA in un'immagine di macchina virtuale, se si prevede di utilizzare Machine Creation Services per eseguire il provisioning delle macchine virtuali. Questa opzione installa Machine Identity Service. Questa è l'opzione predefinita.

  Opzione della riga di comando: `/mastermcsimage` o `/masterimage`

> **Importante:**
>
> Il supporto di installazione o l'immagine ISO devono essere montati localmente. Il montaggio di un'immagine ISO da un'unità di rete ai fini dell'installazione del software non è supportato.

- **Create a master image using Citrix Provisioning or third-party provisioning tools (Creare un'immagine master utilizzando Citrix Provisioning o strumenti di provisioning di terze parti):** selezionare questa opzione per installare un VDA su un'immagine VM, se si prevede di utilizzare Citrix Provisioning o strumenti di provisioning di terze parti (ad esempio Microsoft System Center Configuration Manager) per eseguire il provisioning delle macchine virtuali.

Opzione della riga di comando: `/masterpvsimage`

- (appare solo su macchine con sistema operativo multisessione) **Enable brokered connections to a server** (Abilita connessioni negoziate a un server): selezionare questa opzione per installare un VDA su una macchina fisica o virtuale che non viene utilizzata come immagine per il provisioning di altre macchine.

  Opzione della riga di comando: `/remotepc`

- (Appare solo su computer con sistema operativo a sessione singola) **Enable Remote PC Access (Abilita accesso remoto PC):** selezionare questa opzione per installare un VDA su un computer fisico da utilizzare con Accesso remoto PC.

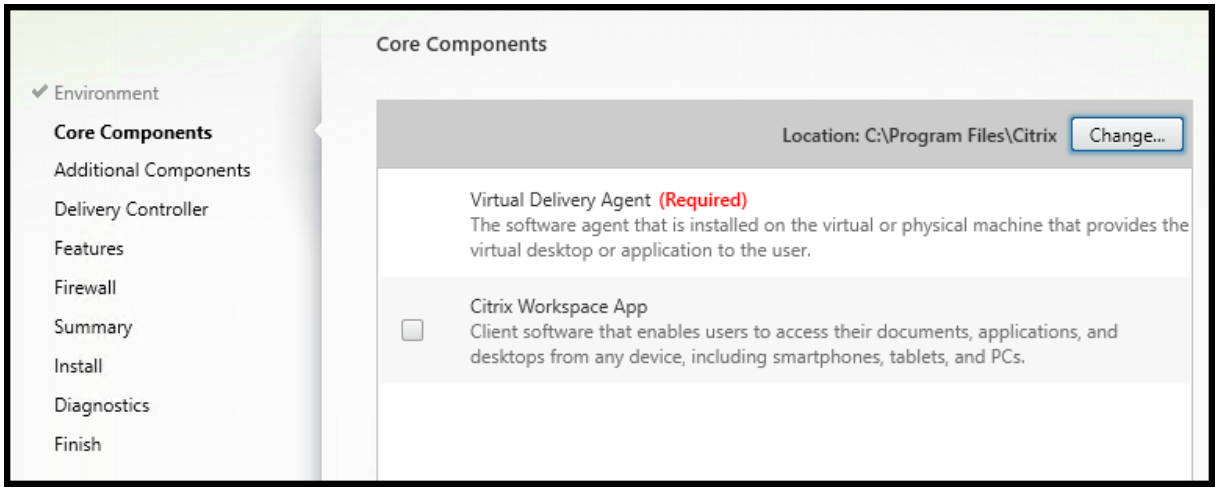
  Opzione della riga di comando: `/remotepc`

Fare clic su **Next** (Avanti).

Questa pagina non viene visualizzata:

- Se si sta aggiornando un VDA
- Se si utilizza il programma di installazione `VDAWorkstationCoreSetup_2308.exe`, `VDAServerSetup_2308.exe` o `VDAWorkstationSetup_2308.exe`

Passaggio 5. Selezionare i componenti da installare e il percorso di installazione



Nella pagina **Core components**:

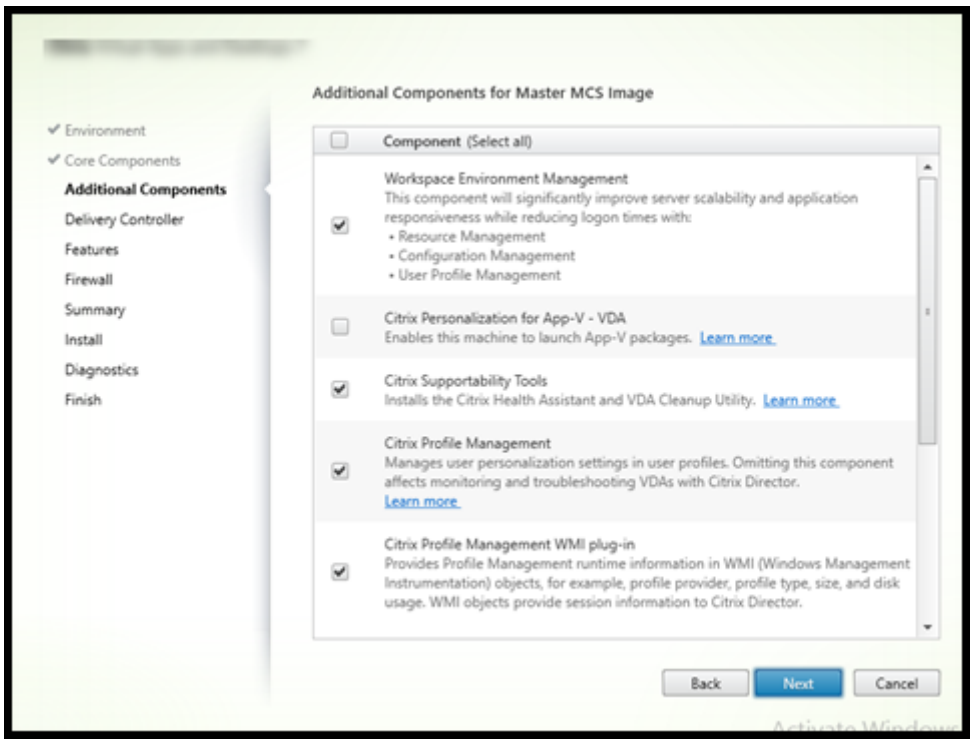
- **Location (Percorso):** per impostazione predefinita, i componenti sono installati in `C:\Program Files\Citrix`. Questa impostazione predefinita va bene per la maggior parte delle distribuzioni. Se si specifica un percorso diverso, tale percorso deve disporre delle autorizzazioni di esecuzione per il servizio di rete.

- **Componenti:** per impostazione predefinita, l'app Citrix Workspace per Windows non è installata con il VDA. Se si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`, l'app Citrix Workspace per Windows non viene mai installata, quindi questa casella di controllo non viene visualizzata.

Fare clic su **Next** (Avanti).

Opzioni della riga di comando: `/installdir`, `/components vda,plugin` per installare il VDA e l'app Citrix Workspace per Windows

Passaggio 6. Installare componenti aggiuntivi



La pagina **Additional Components** (Componenti aggiuntivi) contiene caselle di controllo che consentono di abilitare o disabilitare l'installazione di altre funzionalità e tecnologie con il VDA. In un'installazione mediante riga di comando, è possibile utilizzare l'opzione `/exclude` o `/includeadditional` per omettere o includere espressamente uno o più componenti disponibili.

Nella tabella seguente è indicata l'impostazione predefinita degli elementi presenti in questa pagina. L'impostazione predefinita dipende dall'opzione selezionata nella pagina **Environment**.

Pagina Additional Components	Pagina Environment: opzione “Master image with MCS” (Immagine master con MCS) o “Master image with Citrix Provisioning”(Immagine master con Citrix Provisioning) selezionata	Pagina Environment: opzione “Enable brokered connections to server”(Abilita connessioni negoziate al server) (per sistema operativo multisessione) o “Remote PC Access”(Accesso remoto PC) (per sistema operativo a sessione singola) selezionata
Personalizzazione Citrix per App-V - VDA	Non selezionato	Non selezionato
Livello di personalizzazione utente	Non selezionato	Non visualizzato perché non valido per questo caso d’uso.
Citrix Profile Management	Selezionato	Non selezionato
Plug-in WMI Citrix Profile Management	Selezionato	Non selezionato
Agente di aggiornamento Citrix VDA	Non selezionato	Non selezionato
Citrix Backup and Restore	Non selezionato	Non selezionato
Citrix MCS IODriver	Non selezionato	Non selezionato
Citrix Rendezvous V2	Non selezionato	Non selezionato

Questa pagina non viene visualizzata se:

- Si sta utilizzando il programma di installazione `VDAWorkstationCoreSetup.exe`. Inoltre, le opzioni della riga di comando per i componenti aggiuntivi non sono valide con tale programma di installazione.
- Si sta aggiornando un VDA e tutti i componenti aggiuntivi sono già installati. Se alcuni dei componenti aggiuntivi sono già installati, nella pagina vengono elencati solo i componenti non installati.

Selezionare o deselezionare le seguenti caselle di controllo (i componenti potrebbero apparire in un ordine diverso nel programma di installazione).

- **Citrix Personalization for App-V (Personalizzazione Citrix per App-V):** installare questo componente se si utilizzano applicazioni provenienti da pacchetti Microsoft App-V. Per i dettagli, vedere Distribuire e rendere disponibili applicazioni App-V.

  Opzione della riga di comando: `/includeadditional "Citrix Personalization`

`for App-V – VDA"` per abilitare l'installazione dei componenti, `/exclude "Citrix Personalization for App-V – VDA"` per impedire l'installazione dei componenti.

- **Livello di personalizzazione utente Citrix:** installa MSI per il livello di personalizzazione utente. Per ulteriori informazioni, vedere Livello di personalizzazione utente.

  Questo componente viene visualizzato solo quando si installa un VDA su una macchina Windows 10 a sessione singola.

  Opzione della riga di comando: `/includeadditional "User Personalization Layer"` per abilitare l'installazione dei componenti, `/exclude "User Personalization Layer"` per impedire l'installazione dei componenti.

- **Citrix Profile Management:** questo componente gestisce le impostazioni di personalizzazione degli utenti nei profili utente. Per ulteriori informazioni, vedere Profile Management.

  L'esclusione di Citrix Profile Management dall'installazione influisce sul monitoraggio e la risoluzione dei problemi dei VDA con Citrix Director. Nelle pagine **User details** (Dettagli utente) ed **End Point** (Punto finale), saranno riportati errori del pannello **Personalization** e del pannello **Logon Duration** (Durata accesso). Nelle pagine **Dashboard** e **Trends**, il pannello **Average Logon Duration** (Durata media dell'accesso) visualizza i dati solo per le macchine su cui è installato Profile Management.

  Anche se si utilizza una soluzione di gestione dei profili utente di terze parti, Citrix consiglia di installare ed eseguire Citrix Profile Management Service. L'attivazione del servizio Citrix Profile Management non è necessaria.

  Opzione della riga di comando: `/includeadditional "Citrix Profile Management "` per abilitare l'installazione dei componenti, `/exclude "Citrix Profile Management "` per impedire l'installazione dei componenti.

- **Plug-in WMI Citrix Profile Management:** questo plug-in fornisce informazioni di runtime Profile Management negli oggetti WMI (Windows Management Instrumentation) (ad esempio provider di profili, tipo di profilo, dimensioni e utilizzo del disco). Gli oggetti WMI forniscono informazioni sulla sessione a Director.

  Opzione della riga di comando: `/includeadditional "Citrix Profile Management WMI Plug-in"` per abilitare l'installazione dei componenti, `/exclude "Citrix Profile Management WMI Plug-in"` per impedire l'installazione dei componenti.

- **VDA Upgrade Agent (Agente di aggiornamento VDA):** valido solo per le distribuzioni di Citrix DaaS (precedentemente servizi Citrix Virtual Apps and Desktops). Consente al VDA di partecipare alla funzione di aggiornamento VDA. È possibile utilizzare questa funzione per aggiornare i VDA di un catalogo dalla console di gestione, immediatamente o in un orario pianificato. Se questo agente non è installato, è possibile aggiornare un VDA eseguendo il programma di installazione VDA sulla macchina.

Opzioni della riga di comando: `/includeadditional "Citrix VDA Upgrade Agent"` per abilitare l'installazione dei componenti, `/exclude "Citrix VDA Upgrade Agent"` per impedire l'installazione dei componenti.

- **Cache di scrittura MCSIO per l'ottimizzazione dell'archiviazione:** installa il driver Citrix MCS IO. Per ulteriori informazioni, vedere Archiviazione condivisa dagli hypervisor e Configurare la cache per i dati temporanei.

  Opzioni della riga di comando: `/includeadditional "Citrix MCS IODriver"` per abilitare l'installazione dei componenti, `/exclude "Citrix MCS IODriver"` per impedire l'installazione dei componenti.

- **Configurazione del proxy Rendezvous:** installare questo componente se si intende utilizzare il protocollo Rendezvous con il servizio Citrix Gateway nel proprio ambiente e si dispone di un proxy non trasparente nella rete per le connessioni in uscita. Sono supportati solo i proxy HTTP.

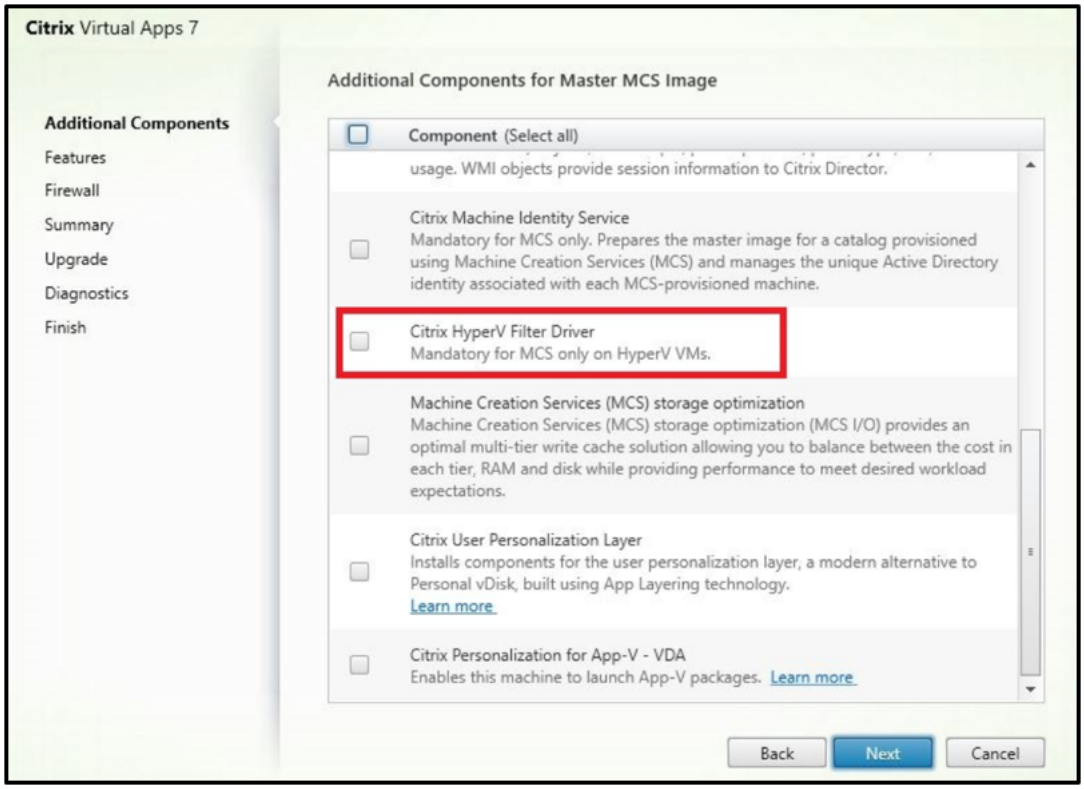
  Se si installa questo componente, specificare l'indirizzo del proxy o il percorso del file PAC nella pagina **Rendezvous Proxy Configuration** (Configurazione del proxy Rendezvous). Per dettagli delle funzionalità, vedere Protocollo Rendezvous.

  Opzione della riga di comando: `/includeadditional "Citrix Rendezvous V2"` per abilitare l'installazione dei componenti, `/exclude "Citrix Rendezvous V2"` per impedire l'installazione dei componenti.

- **Citrix Backup and Restore:** se l'installazione o l'aggiornamento di un VDA falliscono, questo componente può riportare la macchina a un backup eseguito prima dell'installazione o dell'aggiornamento.

  Opzione della riga di comando: `/includeadditional "Citrix Backup and Restore"` per abilitare l'installazione dei componenti, `/exclude "Citrix Backup and Restore"` per impedire l'installazione dei componenti.

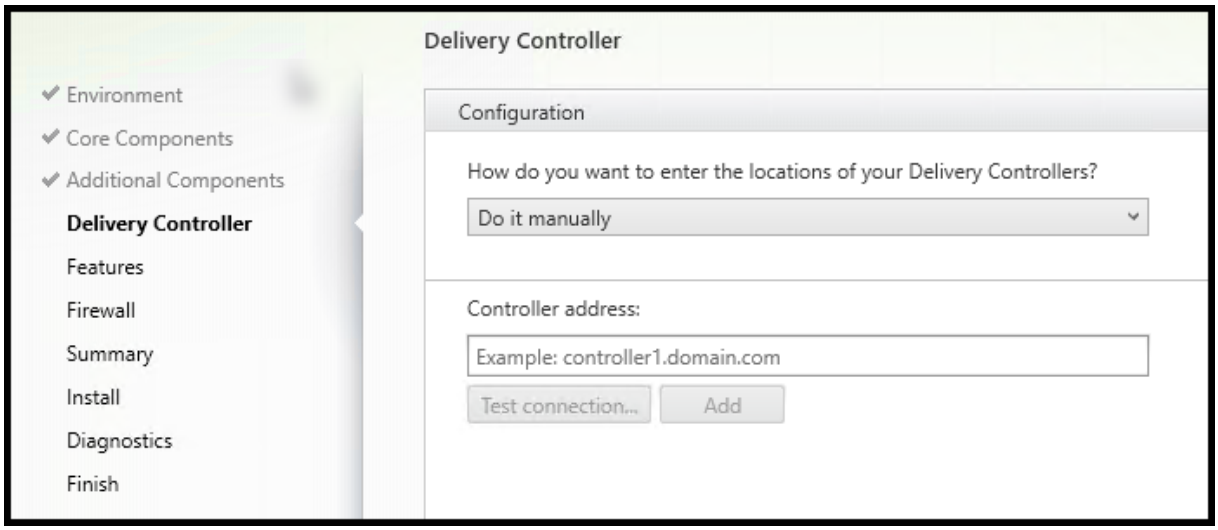
- **Citrix HyperV Filter Driver** (Driver di filtro Citrix HyperV): questo componente deve essere abilitato utilizzando la casella di controllo solo se si esegue l'aggiornamento da una versione precedente del VDA (precedente alla 2308). Il componente mantiene le impostazioni relative alla NIC dell'immagine master nelle macchine virtuali di cui effettua il provisioning. Le impostazioni vengono mantenute anche dopo un aggiornamento di Windows.



Opzione della riga di comando: `/includeadditional "Citrix HyperV Filter Driver"` per abilitare l'installazione dei componenti, `/exclude "Citrix HyperV Filter Driver"` per impedire l'installazione dei componenti.

> **Nota:**
>
> Questo componente viene installato automaticamente se si esegue una nuova installazione del VDA versione 2308 o successiva su una macchina distribuita con Hyper-V (inclusi Azure e SCVMM) tramite le installazioni di immagini master MCS.

Passaggio 7. Indirizzi dei Delivery Controller



Nella pagina **Delivery Controller**, scegliere come inserire gli indirizzi dei controller installati. Citrix consiglia di specificare gli indirizzi durante l'installazione del VDA (**Do it manually** (Eseguire manualmente)). Il VDA non può registrarsi con un controller fino a quando non dispone di queste informazioni. Se un VDA non è in grado di registrarsi, gli utenti non possono accedere alle applicazioni e ai desktop su tale VDA.

- **Do it manually** (Eseguire manualmente): (impostazione predefinita) immettere il nome di dominio completo di un controller installato e quindi fare clic su **Add**. Se sono stati installati più controller, aggiungerne gli indirizzi.
- **Do it later (Advanced)** (Eseguirlo più tardi (avanzato)) se si sceglie questa opzione, la procedura guidata chiede una conferma prima di continuare. Per specificare gli indirizzi in un secondo momento, è possibile eseguire nuovamente il programma di installazione o utilizzare i Criteri di gruppo Citrix. La procedura guidata inserisce anche un promemoria nella pagina **Summary**.
- **Choose locations from Active Directory** (Scegliere i percorsi da Active Directory): valido solo quando il computer viene aggiunto a un dominio e l'utente è un utente di dominio.
- **Let Machine Creation Services do it automatically** (Farlo eseguire automaticamente da Machine Creation Services): valido solo quando si utilizza MCS per eseguire il provisioning delle macchine.

Fare clic su **Next** (Avanti). Se è stata selezionata l'opzione **Do it later (Advanced)**, verrà richiesto di confermare che verranno specificati gli indirizzi del controller in un secondo momento.

Altre considerazioni:

- L'indirizzo non può contenere caratteri non alfanumerici.
- Se si specificano gli indirizzi durante l'installazione del VDA e in Criteri di gruppo, le impostazioni dei criteri sostituiscono le impostazioni fornite durante l'installazione.

- La corretta registrazione del VDA richiede che le porte firewall utilizzate per comunicare con il controller siano aperte. Tale azione è abilitata per impostazione predefinita nella pagina **Firewall** della procedura guidata.
- Dopo aver specificato le posizioni dei controller (durante o dopo l'installazione del VDA), è possibile utilizzare la funzionalità di aggiornamento automatico per aggiornare i VDA quando i controller vengono aggiunti o rimossi. Per informazioni dettagliate su come i VDA individuano e si registrano con i controller, vedere Registrazione dei VDA.

Opzione della riga di comando: `/controllers`

Passaggio 8. Configurazione del proxy Rendezvous

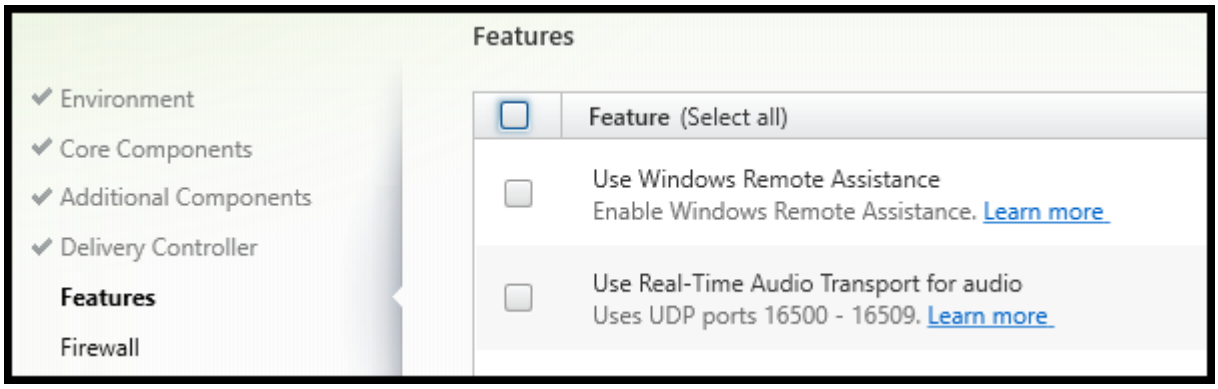
La pagina **Configurazione proxy Rendezvous** viene visualizzata solo se è stata abilitata la casella di controllo **Configurazione proxy Rendezvous** nella pagina **Componenti aggiuntivi** .

1. Selezionare se si dovrà specificare l'origine del proxy mediante l'indirizzo proxy o il percorso del file PAC.
2. Specificare l'indirizzo del proxy o il percorso del file PAC.
   - Formato dell'indirizzo proxy: `http://<url-or-ip>:<port>`
   - Formato del file PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

Il firewall per la porta proxy deve essere aperto affinché il test di connessione abbia esito positivo. Se non è possibile stabilire una connessione al proxy, è possibile scegliere se continuare l'installazione di VDA.

Opzione della riga di comando: `/proxyconfig`

Passaggio 9 Attivare o disattivare funzionalità



Nella pagina **Features** utilizzare le caselle di controllo per attivare o disattivare le funzionalità che si desidera utilizzare.

- **Use Windows Remote Assistance (Utilizzare Assistenza remota di Windows):** quando questa funzionalità è abilitata, Assistenza remota di Windows viene utilizzata con la funzionalità di shadowing utente di Director. Assistenza remota di Windows apre le porte dinamiche nel firewall. (Impostazione predefinita= disabilitato)

  Opzione della riga di comando: `/enable_remote_assistance`

- **Use Real-Time Audio Transport for audio** (Utilizza il trasporto audio in tempo reale per l'audio): abilitare questa funzione se la funzionalità voice-over-IP è ampiamente utilizzata nella rete. La funzione riduce la latenza e migliora la resilienza audio sulle reti con perdita di dati. Consente di trasmettere i dati audio utilizzando RTP su trasporto UDP. (Impostazione predefinita= disabilitato)

  Opzione della riga di comando: `/enable_real_time_transport`

- **Use screen sharing (Usa la condivisione dello schermo):** se abilitata, le porte utilizzate dalla condivisione dello schermo vengono aperte nel firewall di Windows. (Impostazione predefinita= disabilitato)

  Opzione della riga di comando: `/enable_ss_ports`

- **Is this VDA installed on a VM in a cloud (Questo VDA è installato su una macchina virtuale in un cloud?)** Questa impostazione aiuta Citrix a identificare correttamente le posizioni delle risorse per le distribuzioni VDA on-premise e come servizio (Citrix Cloud) a scopi di telemetria. Questa funzionalità non ha alcuna ripercussione sull'utilizzo da parte del cliente. Attivare questa impostazione se la distribuzione utilizza Citrix DaaS (predefinito= disabilitato).

  Opzione della riga di comando: `/xendesktopcloud`

Fare clic su **Next** (Avanti).

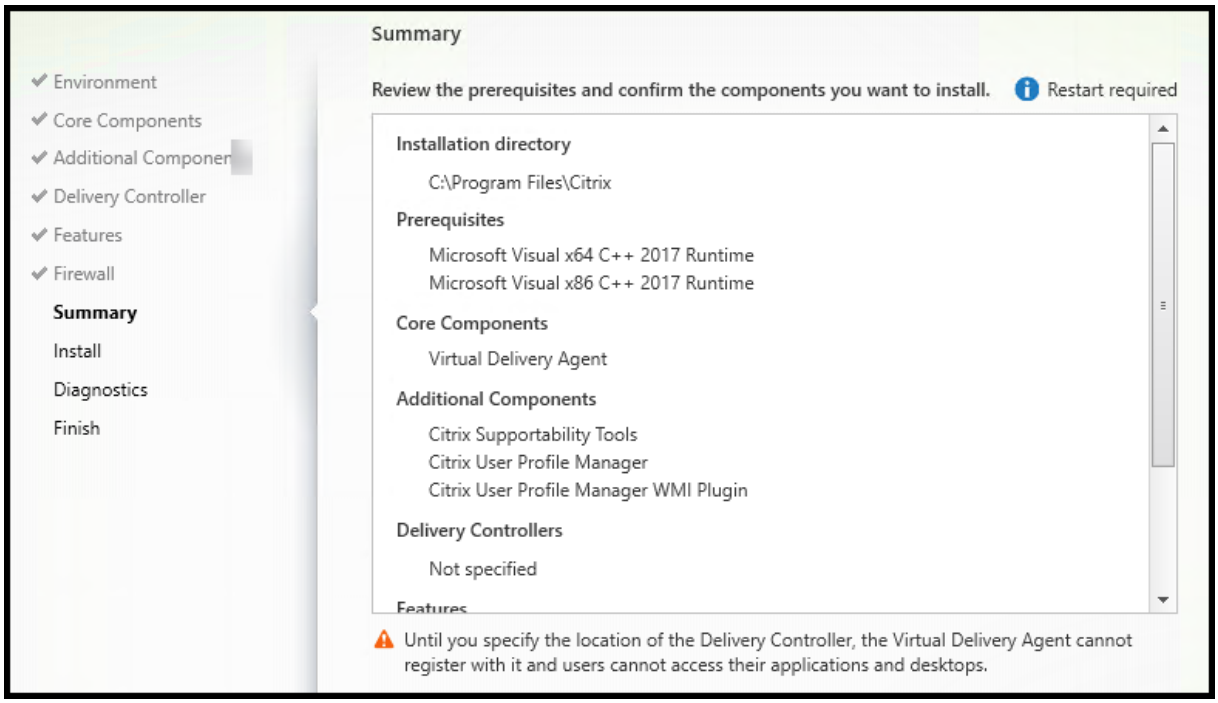
Passaggio 10. Porte del firewall

Nella pagina **Firewall**, per impostazione predefinita, le porte vengono aperte automaticamente se il servizio Windows Firewall è in esecuzione, anche se il firewall non è abilitato. Questa impostazione predefinita è adatta alla maggior parte delle distribuzioni. Per informazioni sulle porte, vedere Porte di rete.

Fare clic su **Next** (Avanti).

Opzione della riga di comando: `/enable_hdx_ports`

Passaggio 11. Esaminare i prerequisiti e confermare l'installazione

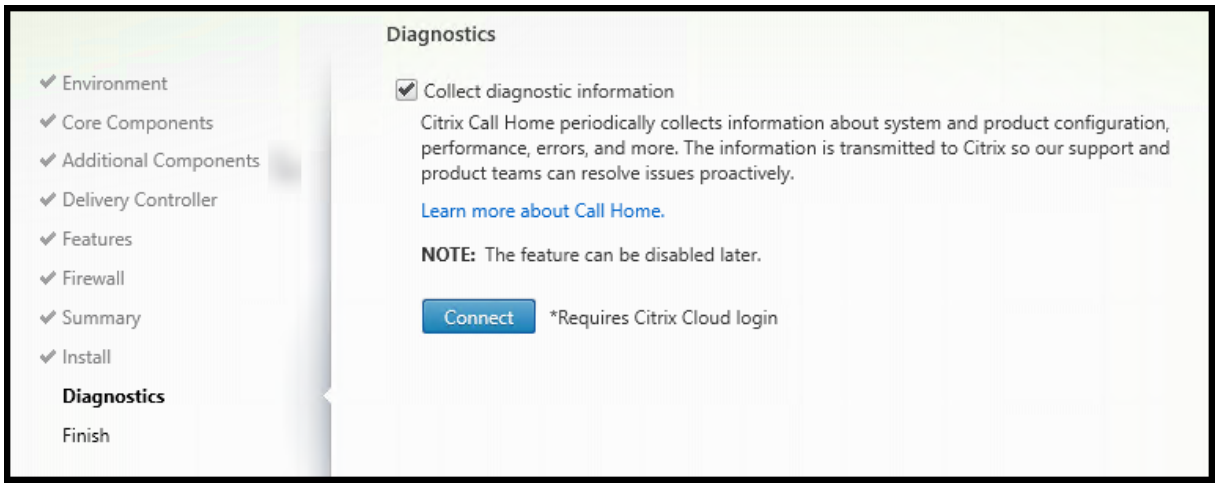


Nella pagina **Summary** sono elencati gli elementi che verranno installati. Utilizzare il pulsante **Back** per tornare alle pagine precedenti della procedura guidata e modificare le selezioni.

Quando si è pronti, fare clic su **Install**.

Se i prerequisiti non sono già installati o abilitati, il computer potrebbe riavviarsi una o più volte. Vedere Prepararsi all'installazione.

Passaggio 12. Diagnostica



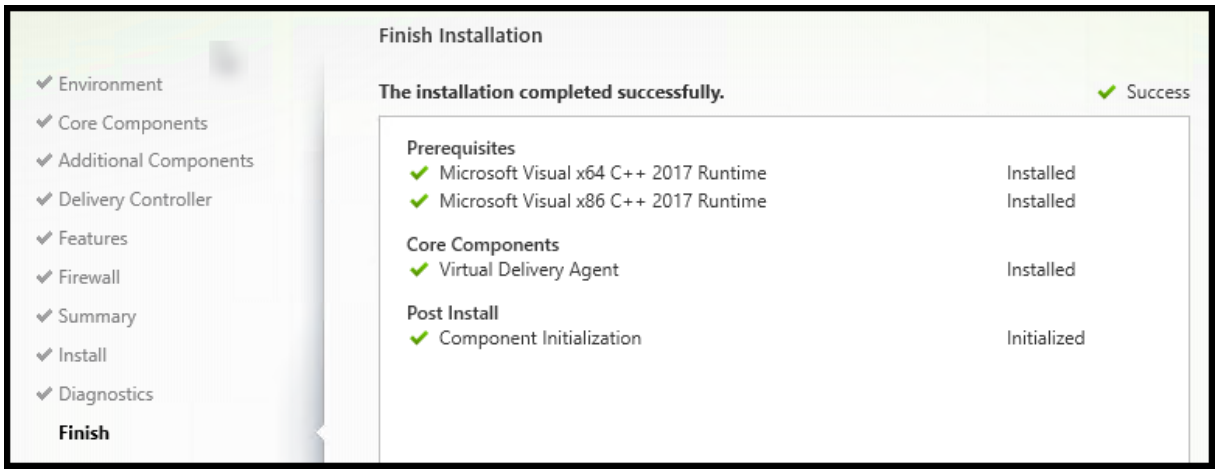
Nella pagina **Diagnostics** (Diagnostics), scegliere se partecipare a Citrix Call Home. Se si sceglie di partecipare (impostazione predefinita), fare clic su **Connect**. Quando richiesto, immettere le credenziali dell'account Citrix.

Dopo aver convalidato le credenziali (o se si sceglie di non partecipare), fare clic su **Next**.

Quando si utilizza il programma di installazione completo del prodotto, se si fa clic su **Connect** (Connetti) nella pagina **Diagnostics** (Diagnostica) senza prima selezionare **Collect diagnostic information** (Raccogli informazioni diagnostiche), dopo aver chiuso la finestra di dialogo **Connect to Citrix Insight Services** (Connetti a Citrix Insight Services) il pulsante **Next** (Avanti) è disabilitato. Non è possibile passare alla pagina successiva. Per riattivare il pulsante **Next** (Avanti), selezionare e deselezionare immediatamente **Collect diagnostic information** (Raccogli informazioni diagnostiche).

Per ulteriori informazioni, vedere Call Home.

Passaggio 13. Completare questa installazione



La pagina **Finish** contiene segni di spunta verdi per tutti i prerequisiti e i componenti installati e inizializzati correttamente.

Fare clic su **Finish**. Per impostazione predefinita, la macchina si riavvia automaticamente. Sebbene sia possibile disattivare questo riavvio automatico, il VDA non può essere utilizzato fino al completamento del riavvio della macchina.

Passaggi successivi

Ripetere la procedura precedente per installare i VDA su altri computer o altre immagini, se necessario.

Dopo aver installato tutti i VDA, avviare Studio. Se non si è ancora creato un sito, Studio guida automaticamente allo svolgimento di tale attività. Al termine di questa operazione, Studio guida alla

creazione di un catalogo macchine e quindi un gruppo di consegna. Vedere:

- Creare un sito
- Creare cataloghi di macchine
- Creare gruppi di consegna

Citrix Optimizer

Citrix Optimizer è uno strumento per il sistema operativo Windows che aiuta gli amministratori Citrix a ottimizzare i VDA rimuovendo e ottimizzando vari componenti.

Dopo aver installato un VDA e completato il riavvio finale, scaricare e installare Citrix Optimizer. Vedere CTX224676. L'articolo CTX contiene il pacchetto di download, oltre a istruzioni sull'installazione e l'utilizzo di Citrix Optimizer.

Personalizzare un VDA

Per personalizzare un VDA installato:

1. Dalla funzione Windows per la rimozione o la modifica dei programmi, selezionare **Citrix Virtual Delivery Agent** o **Citrix Remote PC Access/VDI Core Services VDA**. Quindi fare clic con il pulsante destro del mouse e selezionare **Modifica**.
2. Selezionare **Customize Virtual Delivery Agent Settings** (Personalizza impostazioni del Virtual Delivery Agent). All'avvio del programma di installazione è possibile modificare:
    - Indirizzi dei controller
    - Porta TCP/IP da registrare con il controller (impostazione predefinita= 80)
    - Se aprire automaticamente le porte di Windows Firewall

Risoluzione dei problemi

- Per informazioni su come Citrix riporta i risultati delle installazioni dei componenti, vedere Codici restituiti per l'installazione Citrix.
- Nella visualizzazione Studio per un gruppo di consegna, la voce **Installed VDA version** (Versione VDA installata) nel riquadro **Details** potrebbe non essere la versione installata nei computer. La visualizzazione Programmi e funzionalità di Windows della macchina mostra la versione VDA effettiva.
- Dopo l'installazione di un VDA, non è possibile distribuire app o un desktop agli utenti fino a quando non si registra con un Delivery Controller.

Per informazioni sui metodi di registrazione dei VDA e sulla risoluzione dei problemi di registrazione, vedere Registrazione dei VDA.

Installare i VDA utilizzando script

January 7, 2024

> **Nota:**
>
> Citrix non è responsabile per i problemi causati da script adattati agli ambienti di produzione dei clienti. Per qualsiasi problema relativo all'installazione di Citrix, aprire una richiesta di supporto tecnico specificando i registri di installazione pertinenti mediante il portale di assistenza Citrix.

Questo articolo si applica all'installazione di VDA su macchine con sistemi operativi Windows. Per informazioni sui VDA per i sistemi operativi Linux, vedere la documentazione di Linux Virtual Delivery Agent.

Il supporto di installazione contiene script di esempio che installano, aggiornano o rimuovono i VDA (Virtual Delivery Agent) per le macchine in Active Directory. È inoltre possibile utilizzare gli script per gestire le immagini master utilizzate da Machine Creation Services e Citrix Provisioning (in precedenza Provisioning Services).

Accesso richiesto:

- Gli script richiedono l'accesso in lettura per tutti gli utenti alla condivisione di rete in cui si trova il comando di installazione del VDA. Il comando di installazione è `XenDesktopVdaSetup.exe` nell'ISO del prodotto completo oppure `VDAWorkstationSetup.exe` o `VDAServerSetup.exe` in un programma di installazione autonomo.
- I dettagli di registrazione vengono memorizzati su ogni macchina locale. Per registrare i risultati a livello centrale per la revisione e l'analisi, gli script richiedono l'accesso in lettura e scrittura per tutti gli utenti alla condivisione di rete appropriata.

Per verificare i risultati dell'esecuzione di uno script, esaminare la condivisione di registro centrale. I registri acquisiti includono il registro script, il registro del programma di installazione e i registri di installazione MSI. Ogni tentativo di installazione o rimozione viene registrato in una cartella con indicatore di orario. Il titolo della cartella indica il risultato dell'operazione con il prefisso PASS o FAIL. È possibile utilizzare gli strumenti di ricerca delle directory standard per trovare un'installazione o una rimozione non riuscita nella condivisione di registro centrale. Questi strumenti offrono un'alternativa alla ricerca a livello locale sulle macchine di destinazione.

Prima di iniziare qualsiasi installazione, leggere e completare le attività indicate in Preparazione per l'installazione.

Installare o aggiornare i VDA utilizzando lo script

1. Ottenere lo script di esempio **InstallVDA.bat** da \Support\AdDeploy\ sul supporto di installazione. Citrix consiglia di eseguire un backup dello script originale prima di personalizzarlo.
2. Modificare lo script:
   - Specificare la versione del VDA da installare: `SET DESIREDVERSION`. Ad esempio, la versione 7 può essere specificata come 7.0. Il valore completo è reperibile sul supporto di installazione nel file ProductVersion.txt. Tuttavia, non è richiesta una corrispondenza completa.
   - Specificare la condivisione di rete in cui verrà richiamato il programma di installazione. Puntare alla radice del livello (il punto più alto della struttura). La versione appropriata del programma di installazione (32 bit o 64 bit) viene richiamata automaticamente all'esecuzione dello script. Ad esempio: `SET DEPLOYSHARE=\\fileserver1\share1`.
   - Facoltativamente, specificare un percorso di condivisione di rete per archiviare i registri centralizzati. Ad esempio: `SET LOGSHARE=\\fileserver1\log1`).
   - Specificare le opzioni di configurazione VDA come descritto in Installare utilizzando la riga di comando. Le opzioni `/quiet` e `/noreboot` sono incluse per impostazione predefinita nello script e sono obbligatorie: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT`.
3. Utilizzando gli script di avvio dei criteri di gruppo, assegnare lo script all'unità organizzativa contenente i computer. Questa unità organizzativa deve contenere solo i computer in cui si desidera installare il VDA. Quando le macchine incluse in tale unità organizzativa vengono riavviate, lo script viene eseguito su tutte le unità organizzative. Un VDA viene installato su ogni computer che dispone di un sistema operativo supportato.

Rimuovere i VDA utilizzando lo script

1. Ottenere lo script di esempio UninstallVDA.bat da \Support\AdDeploy\ sul supporto di installazione. Citrix consiglia di eseguire un backup dello script originale prima di personalizzarlo.
2. Modificare lo script.
   - Specificare la versione del VDA da rimuovere: `SET CHECK\_VDA\_VERSION`. Ad esempio, la versione 7 può essere specificata come 7.0. Il valore completo è reperibile sul supporto di installazione nel file ProductVersion.txt (ad esempio 7.0.0.3018). Tuttavia, non è richiesta una corrispondenza completa.
   - Facoltativamente, specificare un percorso di condivisione di rete per archiviare i registri centralizzati.
3. Utilizzando gli script di avvio dei criteri di gruppo, assegnare lo script all'unità organizzativa contenente i computer. Questa unità organizzativa deve contenere solo le macchine da cui

si desidera rimuovere il VDA. Quando le macchine incluse nell'unità organizzativa vengono riavviate, lo script viene eseguito su tutte le unità organizzative. Il VDA viene rimosso da ogni macchina.

Risoluzione dei problemi

- Lo script genera file di registro interni che descrivono l'avanzamento dell'esecuzione dello script. Lo script copia un registro `Kickoff_VDA_Startup_Script` nella condivisione di registro centrale entro pochi secondi dall'avvio della distribuzione. È possibile verificare che il processo complessivo funzioni. Se questo registro non viene copiato nella condivisione di registro centrale come previsto, eseguire una ulteriore risoluzione problemi ispezionando il computer locale. Lo script inserisce due file di registro di debug nella cartella `%temp%` su ogni computer:
  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  Esaminare questi registri per verificare che lo script:
  - Sia in esecuzione come previsto.
  - Stia correttamente rilevando il sistema operativo di destinazione.
  - Sia configurato correttamente per puntare alla `ROOT` della condivisione `DEPLOYSHARE` (contiene il file denominato `AutoSelect.exe`).
  - In grado di autenticare entrambe le condivisioni `DEPLOYSHARE` e `LOG`.
- Per informazioni su come Citrix riporta il risultato delle installazioni dei componenti, vedere Codici restituiti per l'installazione Citrix.
- Nella visualizzazione Studio per un gruppo di consegna, la voce **Installed VDA version** (Versione VDA installata) nel riquadro **Details** potrebbe non essere la versione installata nei computer. La visualizzazione dei programmi e delle funzionalità della macchina indica la versione VDA effettiva.
- Dopo l'installazione di un VDA, non è possibile distribuire app o un desktop agli utenti fino a quando non si registra con un Delivery Controller.

  Per informazioni sui metodi di registrazione dei VDA e sulla risoluzione dei problemi di registrazione, vedere Registrazione dei VDA.

Installare i VDA utilizzando SCCM

January 7, 2024

> **Nota:**
>
> Citrix non è responsabile dei problemi causati dall'implementazione di un Virtual Delivery Agent (VDA) utilizzando strumenti di distribuzione software come Microsoft System Center Configuration Manager (SCCM) adattati agli ambienti di produzione dei clienti. Per qualsiasi problema relativo all'installazione di Citrix, aprire una richiesta di supporto tecnico specificando i registri di installazione pertinenti mediante il portale di assistenza Citrix.

Panoramica

Per distribuire correttamente un Virtual Delivery Agent (VDA) utilizzando Microsoft System Center Configuration Manager (SCCM) o strumenti di distribuzione software simili, Citrix consiglia di utilizzare il programma di installazione VDA in una sequenza di passaggi.

Citrix sconsiglia di utilizzare VDA Cleanup Utility come parte di un'installazione o di un aggiornamento di VDA. Utilizzare VDA Cleanup Utility solo nel caso limitato in cui il programma di installazione del VDA non è riuscito in precedenza.

Riavvii

Il numero richiesto di riavvii durante l'installazione del VDA dipende dall'ambiente. Ad esempio:

- Potrebbe essere necessario un riavvio per gli aggiornamenti in sospeso o più riavvii richiesti da installazioni software precedenti.
- I file precedentemente bloccati da altri processi potrebbero richiedere aggiornamenti, forzando un ulteriore riavvio.
- Alcuni componenti opzionali del programma di installazione VDA (ad esempio Citrix Profile Management e Citrix Files) potrebbero richiedere un riavvio.

SCCM Task Sequencer gestisce tutti i riavvii necessari.

Definire la sequenza di attività

Dopo aver identificato tutti i prerequisiti e i riavvii, utilizzare SCCM Task Sequencer per completare quanto segue:

- Il VDA può essere installato da una copia accessibile del supporto di installazione o da uno dei programmi di installazione VDA autonomi:
  - `VDAWorkstationSetup_XXXX.exe`
  - `VDAServerSetup_XXXX.exe`
  - `VDAWorkstationCoreSetup_XXXX.exe`

Per ulteriori informazioni sui programmi di installazione VDA, vedere Programmi di installazione.

- Quando si aggiorna un VDA, la macchina su cui è installato deve essere in modalità di manutenzione, senza sessioni.
- Quando un'installazione VDA viene eseguita per la prima volta su una macchina, il programma di installazione VDA utilizzato viene copiato su tale macchina.
  - Quando si utilizza un programma di installazione VDA diverso da `VDAWorkstationCoreSetup_XXX.exe`, il programma di installazione VDA viene copiato in `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`.
  - Se si utilizza `VDAWorkstationCoreSetup_XXXX.exe`, il programma di installazione VDA viene copiato in `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe`.
    ‘
- Anche la posizione della directory del programma di installazione VDA è memorizzata nella chiave del Registro di sistema “`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall`” “`MetaInstallerInstallLocation`”.
- Aggiungere le opzioni della riga di comando `/NOREBOOT`, `/NORESUME` e `/QUIET` alle proprie opzioni della riga di comando.
  - `/QUIET`: non mostrare l'interfaccia utente durante l'installazione, in modo che SCCM abbia il controllo del processo di installazione.
  - `/NOREBOOT`: impedire il riavvio automatico del programma di installazione VDA. SCCM attiva i riavvii quando necessario.
  - `/NORESUME`: di solito, quando è necessario un riavvio durante l'installazione, il programma di installazione VDA imposta una `runonce` chiave del Registro di sistema (`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`). Al riavvio del computer, Windows utilizza la chiave per avviare il programma di installazione VDA. Questo è un problema per SCCM, perché SCCM non è in grado di monitorare l'installazione e acquisire il codice di uscita.

Esempio di sequenza di installazione con SCCM

L'esempio seguente mostra la sequenza di installazione.

1. **SCCM TASK1:** preparare la macchina riavviandola.
2. **SCCM TASK2:** avviare l'installazione del VDA.

   a) Aggiungere le opzioni `/quiet`, `/noreboot` e `/noresume` alle proprie opzioni della riga di comando.

b) Eseguire il programma di installazione VDA preferito (immagine locale o uno dei programmi di installazione minimi).
c) SCCM deve acquisire il codice restituito.
   - Se il codice restituito è 0 o 8, l'installazione è completata ed è necessario un riavvio.
   - Se il codice restituito è 3, riavviare la macchina e trasferire il controllo a SCCM TASK3.

3. **SCCM TASK3:** continuare l'installazione del VDA.

a) Se SCCM TASK2 non restituisce 0 o 8, l'installazione deve essere continuata al termine del riavvio.
b) SCCM TASK3 viene ripetuto fino a quando il programma di installazione VDA non restituisce 0 o 8 (che indica un'installazione riuscita) o 3 (che indica che SCCM TASK3 deve essere ripetuto). Considerare qualsiasi altro codice restituito come un errore. SCCM TASK3 dovrebbe segnalare un errore e arrestarsi.
c) Riprendere l'installazione del VDA eseguendo il programma di installazione VDA appropriato (`XenDesktopVdaSetup.exe` nella maggior parte dei casi, o `XenDesktopRemotePCSetup.exe` se è stato utilizzato `VDAWorkstationCoreSetup_XXXX.exe`) dalla posizione in cui è stato copiato (come descritto in Definire la sequenza di attività), senza parametri della riga di comando (il programma di installazione VDA utilizza i parametri salvati durante la prima esecuzione del programma di installazione).
d) Controllare il codice restituito dal programma di installazione VDA.
   - 0 o 8: operazione terminata correttamente, installazione completata, riavvio richiesto.
   - 3: installazione non completata. Riavviare la macchina e ripetere SCCM TASK3 fino a quando non viene restituito un valore 0 o 8. Considerare qualsiasi altro codice restituito come un errore. SCCM TASK3 dovrebbe segnalare un errore e arrestarsi.

Per ulteriori informazioni sui codici restituiti, vedere Codici restituiti dell'installazione Citrix.

Esempi di comandi di installazione di VDA

Le opzioni di installazione disponibili variano a seconda del programma di installazione utilizzato. Vedere i seguenti articoli per i dettagli delle opzioni della riga di comando.

- Installare i VDA
- Installare utilizzando la riga di comando

Comandi di installazione per Accesso remoto PC

- Il comando seguente utilizza il programma di installazione VDA principale a sessione singola (`VDAWorkstationCoreSetup.exe`):


```
VDAWorkstationCoreSetup.exe /quiet /controllers "control.domain.
com" /enable_hdx_ports /noresume /noreboot
```

- Il comando seguente utilizza il programma di installazione VDA completo a sessione singola (`VDAWorkstationSetup.exe`):

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /
  controllers "control.domain.com" /enable_hdx_ports /noresume /
  noreboot
  ```

Comando di installazione per VDI dedicato

- Il comando seguente utilizza il programma di installazione VDA completo a sessione singola (`VDAWorkstationSetup.exe`):

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers "
  control.domain.com" /enable_hdx_ports /enable_remote_assistance /
  noresume /noreboot
  ```

Creare un sito

January 7, 2024

> **Nota:**
>
> Durante la creazione del sito, dopo aver aggiunto una licenza per abilitare la licenza Hybrid Rights, gli host cloud pubblici (come Microsoft Azure, Google Cloud Platform e Amazon Web Services) non compaiono nell'elenco dei tipi di connessione fino al completamento della creazione del sito.

Un sito è il nome assegnato a una distribuzione Citrix Virtual Apps and Desktops. Comprende i Delivery Controller e altri componenti principali, i Virtual Delivery Agent (VDA), le connessioni agli host, i cataloghi di macchine e i gruppi di consegna. È possibile creare il sito dopo aver installato i componenti principali e prima di creare il primo catalogo di macchine e gruppo di consegna.

Se il controller è installato in Server Core, utilizzare i cmdlet PowerShell in Citrix Virtual Apps and Desktops SDK per creare un sito.

Quando si crea un sito, si viene automaticamente iscritti al programma Citrix Customer Experience Improvement Program (CEIP). Il programma CEIP raccoglie statistiche anonime e informazioni sull'utilizzo e le invia a Citrix. Il primo pacchetto dati viene inviato a Citrix circa sette giorni dopo la creazione

del sito. È possibile modificare la registrazione in qualsiasi momento dopo la creazione del sito. Selezionare **Settings** nel riquadro a sinistra di Web Studio quindi localizzare l'impostazione **Citrix Customer Experience Improvement Program**. Per i dettagli, vedere http://more.citrix.com/XD-CEIP.

L'utente che crea un sito diventa amministratore completo. Per ulteriori informazioni, vedere Amministrazione delegata.

Leggere questo articolo prima di creare il sito, in modo da sapere cosa aspettarsi.

Passaggio 1. Aprire la procedura guidata per la creazione del sito - Citrix Site Manager

Utilizzare lo strumento Citrix Site Manager per configurare la distribuzione di Citrix Virtual Apps and Desktops (noto anche come sito). Lo strumento viene installato automaticamente quando si installa un Delivery Controller.

Per eseguire questo strumento, aprire il menu Start del desktop su un Delivery Controller e selezionare **Citrix > Citrix Site Manager**. Vedere Installare Web Studio.

Passaggio 2. Nome sito

Nella pagina **Introduction**, digitare un nome da dare al sito.

Passaggio 3. Database

La pagina **Databases** contiene le selezioni per l'impostazione dei database di registrazione del sito, del monitoraggio e della configurazione. Per informazioni dettagliate sulle scelte e sui requisiti di impostazione del database, vedere Database.

> **Nota:**
>
> Se un listener di SQL Server Always On è configurato per la crittografia TLS, potrebbe essere richiesto di immettere le credenziali con le autorizzazioni di creazione del database. I tentativi di creazione del database hanno esito negativo anche se si immettono credenziali di amministratore valide. Verificare che il certificato di SQL Server includa il nome DNS del listener nei SAN (Subject Alternative Names). Per ulteriori informazioni, vedere https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates.

Se si sceglie di installare SQL Server Express per l'utilizzo come database del sito (impostazione predefinita), dopo l'installazione del software si verifica un riavvio. Tale riavvio non si verifica se si sceglie di non installare il software SQL Server Express per l'utilizzo come database del sito.

Se non si utilizza SQL Server Express predefinito, assicurarsi che il software SQL Server sia installato sui computer prima di creare un sito. I requisiti di sistema elencano le versioni supportate.

Se si desidera aggiungere altri Delivery Controller al sito e si è già installato il software Controller su altri server, è possibile aggiungere tali Controller da questa pagina. Se si prevede anche di generare script che configurano i database, aggiungere i Controller prima di generare gli script.

Passaggio 4. Licenze

Nella pagina **Licensing** specificare l'indirizzo del server licenze e quindi indicare la licenza da utilizzare (installare).

- Specificare l'indirizzo del server licenze nel modulo `name:[port]`. Il *nome* deve essere un nome di dominio completo, un NetBIOS o un indirizzo IP. È consigliato il nome di dominio completo. Se si omette il numero di porta, il valore predefinito è 27000. Fare clic su **Connect**. Non è possibile passare alla pagina successiva fino a quando non viene effettuata una connessione al server licenze.
- Quando viene effettuata una connessione, per impostazione predefinita viene selezionata l'opzione **Use an existing license** (Usa una licenza esistente). Il display elenca i prodotti compatibili in base ai quali è possibile configurare questo prodotto, tenendo conto delle licenze attualmente installate.
  - Se si desidera configurare questo prodotto come uno dei prodotti elencati (ad esempio Citrix Virtual Apps Premium o Citrix Virtual Desktops Premium), utilizzando una di queste licenze, selezionare tale voce.
  - Se è già stata allocata e scaricata una licenza (utilizzando Citrix Manage Licenses Tool) da utilizzare con questo prodotto, ma non si è ancora installata la licenza:
    * Fare clic su **Browse for license file** (Sfoglia per il file di licenza).
    * In Esplora file, individuare e selezionare la licenza scaricata. I prodotti associati vengono ora visualizzati nella pagina **Gestione licenze** della creazione guidata sito. Selezionare la voce che si desidera utilizzare.
  - Se il prodotto desiderato non viene visualizzato o se non si dispone di licenze allocate e scaricate, è possibile allocare, scaricare e installare una licenza. A tale scopo, il server licenze deve disporre di accesso a Internet. È necessario disporre di un codice di accesso alla licenza per il prodotto desiderato. Citrix invia quel codice per e-mail.
    * Fare clic su **Allocate and download** (Allocare e scaricare).
    * Nella finestra di dialogo **Allocate Licenses**, immettere il codice di accesso alla licenza inviato da Citrix. Fare clic su **Allocate licenses**.

* I prodotti associati alla nuova licenza vengono visualizzati nella pagina **Licensing** della creazione guidata sito. Selezionare la voce che si desidera utilizzare.

In alternativa, selezionare **Use the free 30-day trial** (Utilizza la versione di prova gratuita di 30 giorni) e installare le licenze in un secondo momento. Per ulteriori informazioni, vedere la Documentazione delle licenze.

Passaggio 5. Riepilogo

Nella pagina **Summary** sono elencate le informazioni specificate. Utilizzare il pulsante **Back** se si desidera modificare qualcosa. Al termine, fare clic su **Finish** (Fine).

Ulteriori informazioni

Connessione host, rete e archiviazione

Se si utilizzano macchine virtuali su un hypervisor o un altro servizio per distribuire applicazioni e desktop, è possibile creare la prima connessione a tale host. È inoltre possibile specificare risorse di archiviazione e di rete per tale connessione. Dopo aver creato il sito, è possibile modificare questa connessione e le risorse e creare ulteriori connessioni. Per ulteriori informazioni, vedere Connessioni e risorse.

- Per informazioni specifiche sulla pagina **Connection**, vedere Connessioni e risorse.
  - Se non si utilizzano le macchine virtuali in un hypervisor o in un altro servizio (o se si utilizza Web Studio per gestire desktop su PC blade dedicati), selezionare il tipo di connessione **None**.
  - Se si sta configurando un sito con Accesso remoto PC e si prevede di utilizzare la funzionalità di riattivazione su LAN, selezionare il tipo **Microsoft System Center Virtual Machine Manager** o **Remote PC Wake on LAN**. Per ulteriori informazioni, vedere Riattivazione LAN.

  Oltre al tipo di connessione, specificare se si utilizzeranno gli strumenti Citrix (ad esempio Machine Creation Services) o altri strumenti per creare le macchine virtuali.
- Per informazioni specifiche sulle pagine **Storage** e **Network**, vedere Archiviazione host, Gestione dell'archiviazionee Gestione delle risorse di archiviazione.
- Se si dispone di una licenza Hybrid Rights e sono state aggiunte connessioni a host cloud pubblici (ad esempio, AWS), tali connessioni sono elencate qui. Per visualizzare le connessioni host del cloud pubblico, aggiornare Web Studio alcuni minuti dopo averle aggiunte.

Accesso remoto al PC

Per informazioni su Remote PC Access, vedere Accesso remoto al PC.

Se si utilizza la funzionalità di riattivazione su LAN, completare la procedura di configurazione in Microsoft System Center Configuration Manager prima di creare il sito. Per i dettagli, vedere Configuration Manager e Riattivazione accesso remoto PC su LAN.

Creare e gestire connessioni e risorse

April 3, 2024

> **Importante:**
>
> A partire da Citrix Virtual Apps and Desktops 7 2006, se la distribuzione corrente utilizza una delle seguenti tecnologie, è possibile aggiornare la distribuzione alla versione corrente solo dopo aver rimosso gli elementi del ciclo di vita (EOL) che utilizzano tali tecnologie.
>
> - Personal vDisks (PvDs)
> - AppDisks
> - Tipi di host cloud pubblici: Citrix CloudPlatform, Microsoft Azure Classic
>
> Per ulteriori informazioni, vedere Rimuovere PVD, AppDisk e host non supportati.
>
> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Se si desidera utilizzare connessioni a host cloud pubblici per la distribuzione, è necessaria la licenza Hybrid Rights per completare la nuova installazione o l'aggiornamento alla versione corrente.

Quando il programma di installazione rileva una o più tecnologie o connessioni host non supportate senza la licenza Hybrid Rights, l'aggiornamento viene sospeso o interrotto e viene visualizzato un messaggio esplicativo. I registri del programma di installazione ne contengono i dettagli. Per ulteriori informazioni, vedere Aggiornare una distribuzione.

Effetto della licenza Hybrid Rights sulla connessione host

Esistono tre scenari in cui la connessione host agli host cloud pubblici è influenzata in base al diritto della licenza Hybrid Rights:

- Per creare una nuova connessione host agli host cloud pubblici, è necessario disporre di Hybrid Rights License.
- Se si dispone della licenza Hybrid Rights, ma la licenza è scaduta, le connessioni esistenti agli host cloud pubblici vengono contrassegnate come non autorizzate ed entrano in modalità di manutenzione. Quando le connessioni host esistenti sono in modalità di manutenzione, non è possibile effettuare le seguenti operazioni:
  - Aggiungere o modificare connessioni host
  - Creare catalogo e aggiornare l'immagine
  - Eseguire azioni sull'alimentazione
- Quando le connessioni host non autorizzate diventano connessioni aventi diritto, le connessioni host esistenti vengono riabilitate.

Introduzione

Facoltativamente, è possibile creare la prima connessione alle risorse di hosting quando si crea un Sito. Successivamente, è possibile modificare tale connessione e creare altre connessioni. La configurazione di una connessione include la selezione del tipo di connessione tra gli hypervisor supportati e l'archivazione e la rete selezionate dalle risorse per tale connessione.

Gli amministratori di sola lettura possono visualizzare i dettagli della connessione e delle risorse. È necessario essere un amministratore completo per eseguire attività di connessione e gestione delle risorse. Per ulteriori informazioni, vedere Amministrazione delegata.

Dove trovare informazioni sui tipi di connessione

È possibile utilizzare le piattaforme di virtualizzazione supportate per ospitare e gestire macchine nell'ambiente Citrix Virtual Apps o Citrix Virtual Desktops. L'articolo Requisiti di sistema elenca i tipi supportati.

Per ulteriori informazioni, vedere le seguenti fonti di informazione:

- **Citrix Hypervisor (in precedenza XenServer):**
  - Ambienti di virtualizzazione Citrix Hypervisor.
  - Documentazione di Citrix Hypervisor.
- **Nutanix Acropolis:**
  - Ambienti di virtualizzazione Nutanix.
  - Documentazione Nutanix.

- **VMware:**
  - Ambienti di virtualizzazione VMware
  - Documentazione dei prodotti VMware.
- **Microsoft Hyper-V:**
  - Articolo sugli ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager.
  - Documentazione Microsoft.
- **Connessioni a host cloud pubblici (AWS, Google Cloud, Microsoft Azure, cloud Nutanix e soluzioni partner e cloud VMware e soluzioni partner):** per informazioni relative agli host cloud pubblici, vedere Set up resource type.

> **Nota:**
>
> Le fonti di informazioni indirizzano alla documentazione di Citrix DaaS. Se si ha familiarità con gli host cloud pubblici del prodotto Citrix DaaS, la versione locale presenta diverse differenze. Nella versione locale di Virtual Apps and Desktops, l'interfaccia di gestione è nota come Web Studio. Gli aggiornamenti vengono distribuiti al servizio circa ogni quattro settimane. Pertanto, è possibile che alcune funzionalità disponibili con il servizio non siano disponibili con la versione locale.

Archiviazione host

Un prodotto di archiviazione è supportato se gestito da un hypervisor supportato. Citrix Support assiste i fornitori di prodotti di archiviazione nella risoluzione e nella risoluzione dei problemi e documenta tali problemi nel Knowledge Center, secondo necessità.

Quando si esegue il provisioning delle macchine, i dati sono classificati per tipo:

- Dati del sistema operativo (OS), incluse le immagini master.
- Dati temporanei. Questi dati includono tutti i dati non persistenti scritti su macchine con provisioning MCS, file di paging di Windows, dati del profilo utente e tutti i dati sincronizzati con ShareFile. Questi dati vengono eliminati ogni volta che una macchina si riavvia.

Fornire archiviazione separata per ogni tipo di dati può ridurre il carico e migliorare le prestazioni su ciascun dispositivo di archiviazione, sfruttando al meglio le risorse disponibili dell'host. Consente inoltre di utilizzare l'archiviazione appropriata per i diversi tipi di dati: la persistenza e la resilienza sono più importanti per alcuni dati che per altri.

L'archiviazione può essere condivisa (in posizione centrale, separato da qualsiasi host, utilizzato da tutti gli host) o locale per un hypervisor. Ad esempio, l'archiviazione condivisa centrale può essere

costituita da uno o più volumi di archiviazione in cluster di Windows Server 2012 (con o senza archiviazione collegata) o un'appliance di un fornitore di archiviazione. L'archiviazione centrale potrebbe anche fornire ottimizzazioni quali i percorsi di controllo dell'archiviazione dell'hypervisor e l'accesso diretto tramite plug-in di partner.

L'archiviazione locale dei dati temporanei evita di dover attraversare la rete per accedere all'archiviazione condivisa. Riduce inoltre il carico sul dispositivo di archiviazione condiviso. L'archiviazione condivisa può essere più costosa, quindi l'archiviazione locale dei dati può ridurre le spese. I vantaggi devono essere valutati in base alla disponibilità di spazio di archiviazione sufficiente sui server hypervisor.

Quando si crea una connessione, si sceglie uno dei due metodi di gestione dell'archiviazione: archiviazione condivisa da hypervisor o archiviazione locale per l'hypervisor.

Quando si utilizza l'archiviazione locale su uno o più host Citrix Hypervisor per l'archiviazione temporanea dei dati, assicurarsi che ogni posizione di archiviazione nel pool abbia un nome univoco. Per modificare un nome in XenCenter, fare clic con il pulsante destro del mouse sulla posizione di archiviazione e modificare la proprietà del nome.

Archiviazione condivisa dagli hypervisor

Il metodo di archiviazione condiviso dagli hypervisor memorizza centralmente i dati che necessitano di persistenza a lungo termine, fornendo backup e gestione centralizzati. Tale archiviazione contiene i dischi del sistema operativo.

Quando si seleziona questo metodo, è possibile scegliere se utilizzare l'archiviazione locale (su server nello stesso pool di hypervisor) per i dati temporanei della macchina. Questo metodo non richiede persistenza né tanta resilienza quanta ne richiedono i dati contenuti nell'archiviazione condivisa, denominata *cache dei dati temporanei*. Il disco locale aiuta a ridurre il traffico verso l'archiviazione principale del sistema operativo. Il disco viene cancellato dopo ogni riavvio della macchina. Il disco è accessibile tramite una cache di memoria write-through. Se si utilizza l'archiviazione locale per i dati temporanei, il VDA sottoposto a provisioning è collegato a un host hypervisor specifico. Se l'host è in condizione di errore, la macchina virtuale non può essere avviata.

Eccezione: Microsoft System Center Virtual Machine Manager non accetta i dischi di cache dei dati temporanei sull'archiviazione locale quando si utilizza Clustered Storage Volumes (CSV).

Creare una connessione per archiviare i dati temporanei localmente, quindi abilitare e configurare valori non predefiniti per le dimensioni del disco cache e le dimensioni della memoria di ciascuna macchina virtuale. I valori predefiniti sono personalizzati per il tipo di connessione e sono sufficienti per la maggior parte dei casi. Per ulteriori informazioni, vedere Creare cataloghi di macchine.

L'hypervisor è inoltre in grado di fornire tecnologie di ottimizzazione attraverso la memorizzazione nella cache in lettura delle immagini del disco a livello locale. Ad esempio, Citrix Hypervisor offre

IntelliCache, che riduce il traffico di rete verso l'archiviazione centrale.

Archiviazione locale per l'hypervisor

Il metodo di archiviazione locale per l'hypervisor consente di archiviare i dati localmente sull'hypervisor. Con questo metodo, le immagini master e altri dati del sistema operativo vengono trasferiti agli hypervisor del Sito. Questo processo si verifica per la creazione iniziale della macchina e per i futuri aggiornamenti delle immagini. Questo processo si traduce in un traffico significativo sulla rete di gestione. Inoltre il trasferimento delle immagini richiede molto tempo e le immagini diventano disponibili per ciascun host in un momento diverso.

Creare una connessione e risorse

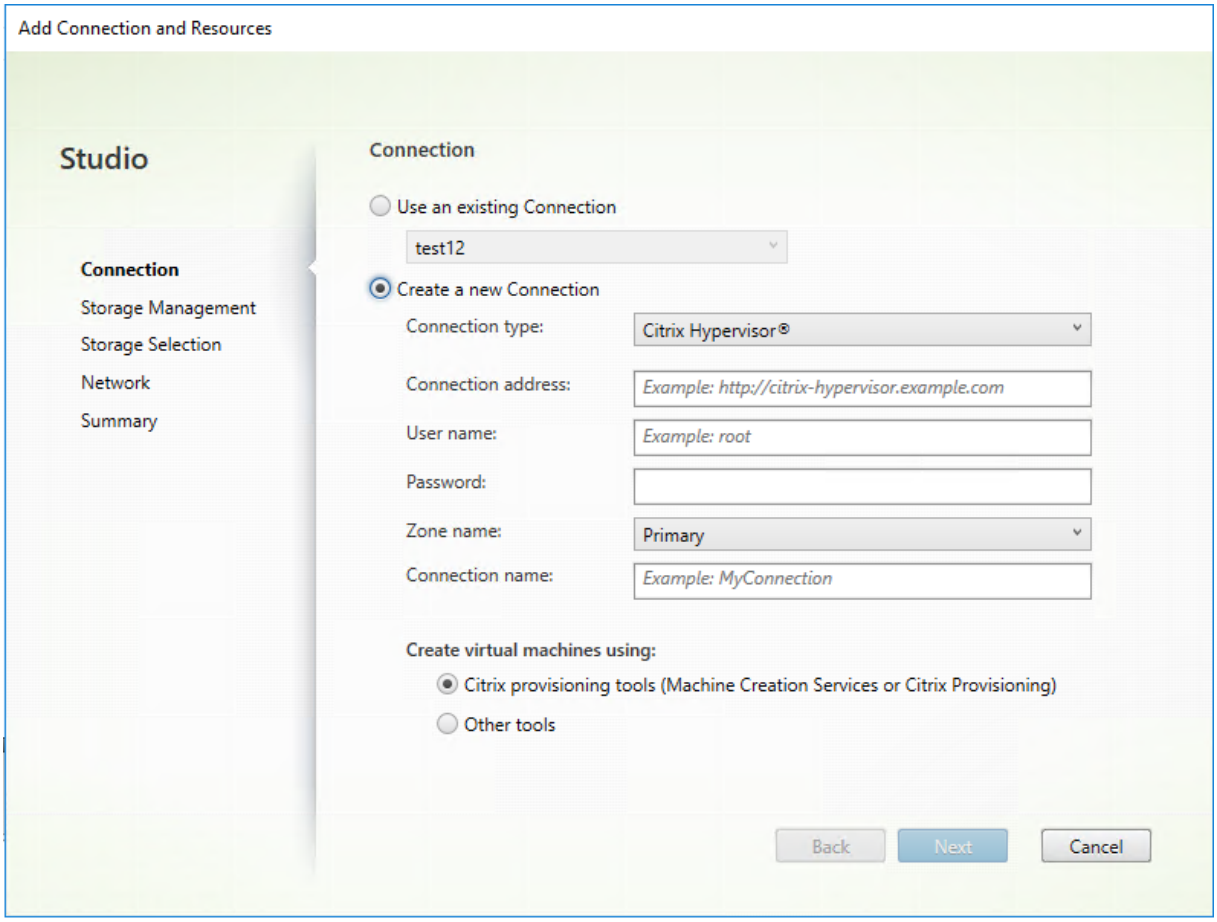
Facoltativamente, è possibile creare la prima connessione quando si crea il Sito. La procedura guidata di creazione del sito contiene le pagine relative alla connessione descritte nelle sezioni seguenti.

Se si sta creando una connessione dopo aver creato il Sito, iniziare dal passaggio 1.

> **Importante:**
>
> Le risorse dell'host (archiviazione e rete) devono essere disponibili prima della creazione di una connessione.

1. Accedere a Web Studio.
2. Selezionare **Hosting** nel riquadro a sinistra.
3. Selezionare **Add Connections and Resources** (Aggiungi connessioni e risorse) nella barra delle azioni.
4. La procedura guidata guida l'utente attraverso le pagine seguenti (il contenuto specifico della pagina dipende dal tipo di connessione selezionato). Dopo aver completato ogni pagina, fare clic su **Next** fino a raggiungere la pagina **Summary**.

Connessione



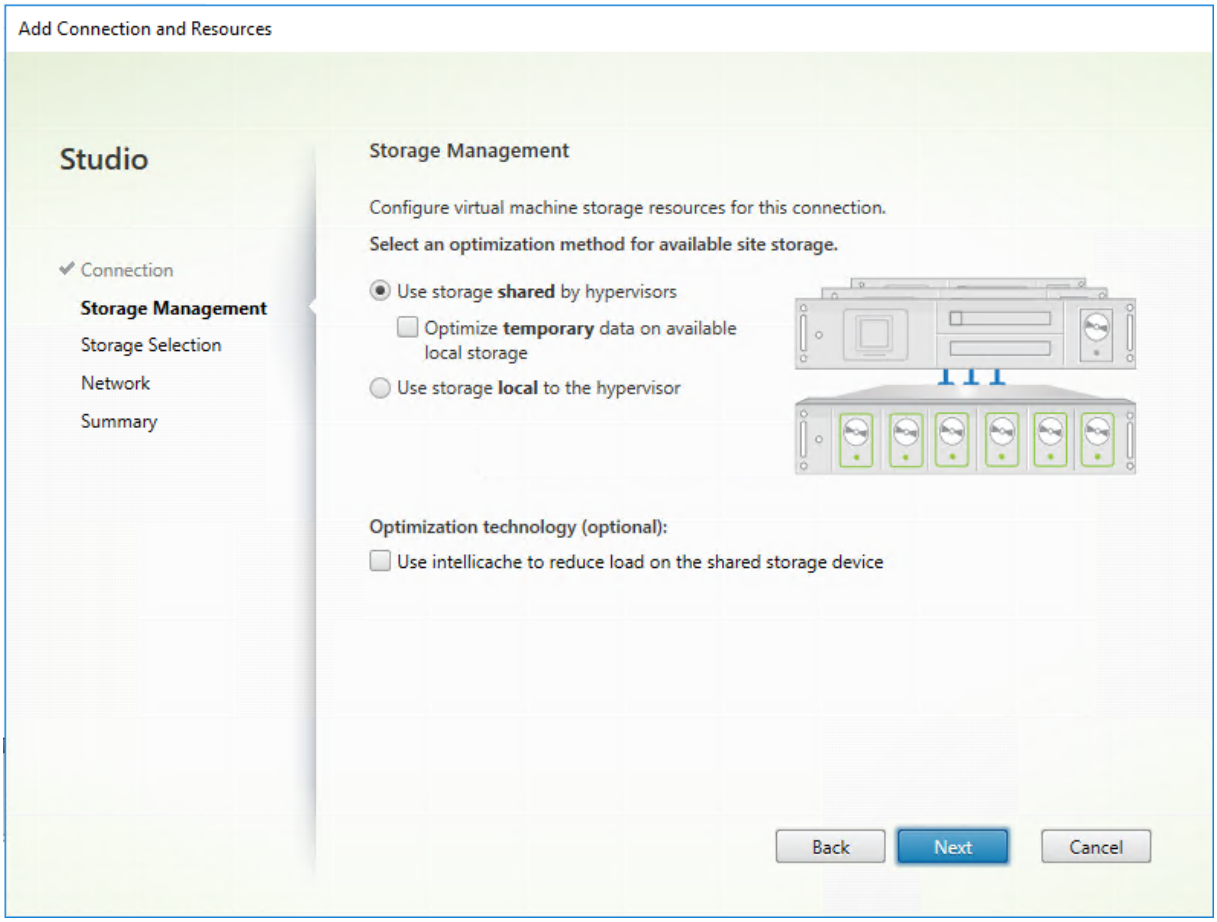
Nella pagina **Connection**:

- Per creare una connessione, selezionare **Create a new Connection** (Crea una nuova connessione). Per creare una connessione basata sulla stessa configurazione host di una connessione esistente, selezionare **Use an existing Connection** (Usa una connessione esistente) e quindi scegliere la connessione pertinente.
- Selezionare l'hypervisor che si sta utilizzando nel campo **Connection type** (Tipo di connessione). Le connessioni a host cloud pubblici sono indicate nell'elenco a discesa solo se si utilizza la licenza Hybrid Rights. In alternativa, è possibile utilizzare il comando PowerShell `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/true per ottenere quanto segue:
  - Elenco di tutti i plug-in hypervisor supportati da Citrix, inclusi i plug-in di terze parti.
  - Disponibilità del plugin hypervisor. Se lo stato di disponibilità è **false**, il motivo potrebbe essere che il plug-in dell'hypervisor non è installato correttamente o che non si ha diritto alla Hybrid Rights License.
- I campi dell'indirizzo e delle credenziali della connessione variano a seconda del tipo di connes-

sione selezionato. Inserire le informazioni richieste.

- Immettere un nome per la connessione. Questo nome viene visualizzato in Web Studio.
- Scegliere lo strumento utilizzato per creare macchine virtuali: strumenti Web Studio (come Machine Creation Services o Citrix Provisioning) o altri strumenti.

Gestione dell'archiviazione



Per informazioni sui tipi e sui metodi di gestione dell'archiviazione, vedere Archiviazione host.

Se si sta configurando una connessione a un host Hyper-V o VMware, selezionare un nome di cluster. Altri tipi di connessione non richiedono un nome di cluster.

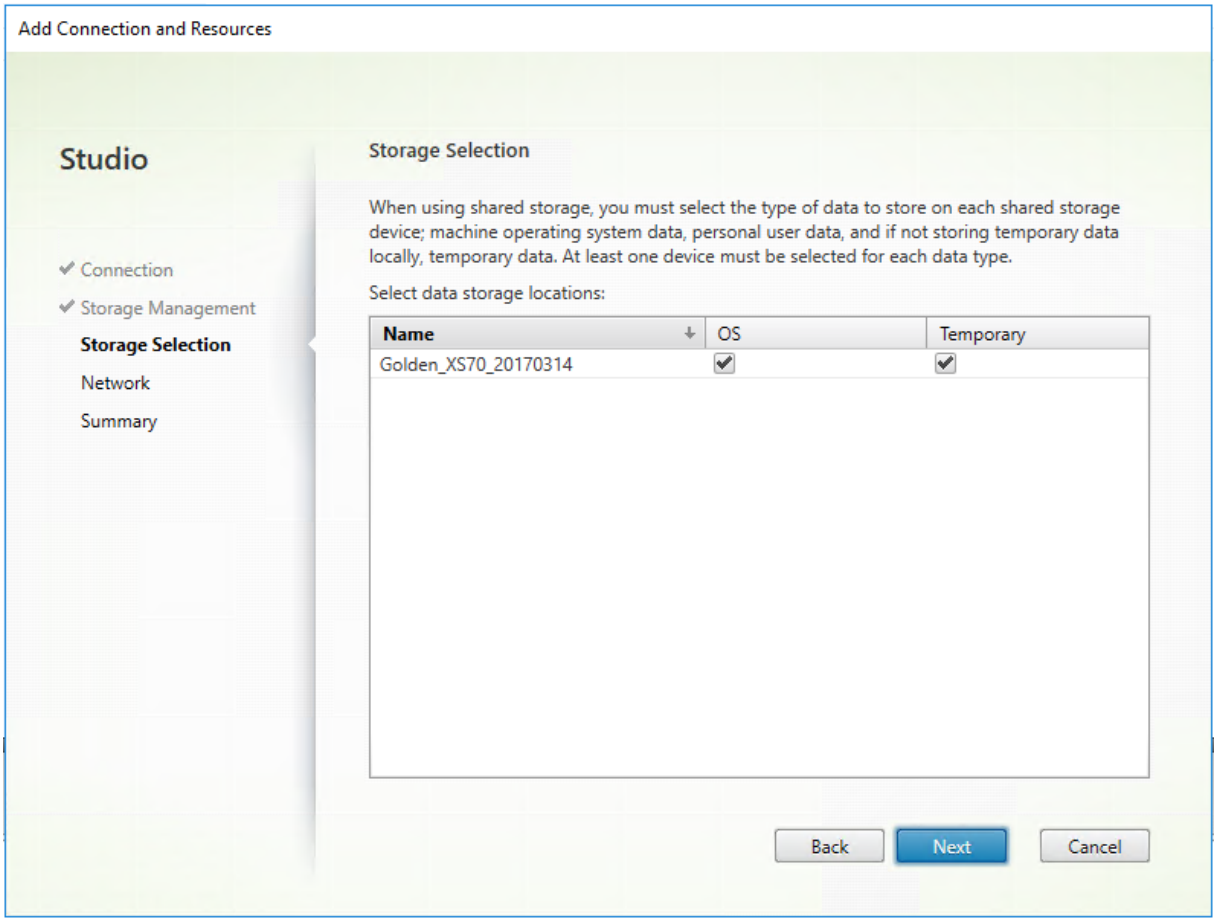
Selezionare un metodo di gestione dell'archiviazione: archiviazione condivisa dagli hypervisor o archiviazione locale per l'hypervisor.

- Se si sceglie l'archiviazione condivisa dagli hypervisor, indicare se si desidera conservare i dati temporanei sulla posizione di archiviazione locale disponibile (è possibile specificare dimensioni di archiviazione temporanea non predefinite nei cataloghi di macchine che utilizzano questa connessione). **Eccezione:** quando si utilizza Clustered Storage Volumes (CSV), Microsoft System Center Virtual Machine Manager non accetta i dischi di cache dei dati temporanei sull'

archiviazione locale. La configurazione della gestione dell'archiviazione in Web Studio non riesce.

Se si utilizza l'archiviazione condivisa in un pool Citrix Hypervisor, indicare se si desidera utilizzare IntelliCache per ridurre il carico sul dispositivo di archiviazione condiviso. Vedere Utilizzare IntelliCache per le connessioni Citrix Hypervisor.

Gestione delle risorse di archiviazione



Per ulteriori informazioni sulla selezione dell'archiviazione, vedere Archiviazione host.

Selezionare almeno un dispositivo di archiviazione host per ogni tipo di dati disponibile. Il metodo di gestione dell'archiviazione selezionato nella pagina precedente influisce sui tipi di dati selezionabili in questa pagina. Selezionare almeno un dispositivo di archiviazione per ogni tipo di dati supportato prima di passare alla pagina successiva della procedura guidata.

La parte inferiore della pagina **Storage Selection** (Selezione archiviazione) contiene ulteriori opzioni di configurazione se si sceglie l'archiviazione condivisa dagli hypervisor e si è abilitato **Optimize temporary data on available local storage** (Ottimizza i dati temporanei sullo storage locale disponibile)

nella pagina precedente. È possibile selezionare i dispositivi di archiviazione locale da utilizzare per i dati temporanei.

Viene visualizzato il numero di dispositivi di archiviazione attualmente selezionati (nell'immagine precedente "1 storage device selected"(1 dispositivo di archiviazione selezionato)). Quando si passa il mouse su quella voce, vengono visualizzati i nomi dei dispositivi selezionati.

1. Fare clic su **Select** per modificare i dispositivi di archiviazione da utilizzare.
2. Nella finestra di dialogo **Select Storage** (Seleziona archiviazione) selezionare o deselezionare le caselle di controllo del dispositivo di archiviazione e quindi fare clic su **OK**.

Rete

Nella pagina **Network** (Rete) immettere un nome per le risorse. Questo nome viene visualizzato in Web Studio per identificare la combinazione di archiviazione e rete associata alla connessione.

Selezionare una o più reti utilizzate dalle macchine virtuali.

Riepilogo

Nella pagina **Summary** controllare gli elementi selezionati. Al termine, fare clic su **Finish**.

Ricordare: l'archiviazione locale dei dati temporanei consente di configurare valori non predefiniti per la memorizzazione temporanea dei dati quando si crea il catalogo di macchine contenente macchine che utilizzano questa connessione. Vedere Creare cataloghi di macchine.

Modificare le impostazioni di connessione

Non utilizzare questa procedura per rinominare o creare una connessione. Quelle connessioni sono operazioni diverse. Modificare l'indirizzo solo se la macchina host corrente ha un nuovo indirizzo. L'immissione di un indirizzo in una macchina diversa interrompe i cataloghi delle macchine che usano quella connessione.

Non è possibile modificare le impostazioni della **GPU** per una connessione, poiché i cataloghi di macchine che accedono a questa risorsa devono utilizzare un'immagine master specifica della GPU appropriata. Creare una connessione.

1. Accedere a Web Studio.
2. Selezionare **Hosting** nel riquadro a sinistra.
3. Selezionare la connessione e quindi selezionare **Edit Connection** (Modifica connessione) nella barra delle azioni.
4. Seguire le indicazioni per le impostazioni disponibili quando si modifica una connessione.

5. Al termine, fare clic su **Apply** per applicare le modifiche apportate e mantenere aperta la finestra oppure su **Save** per applicare le modifiche e chiudere la finestra.

Pagina **Connection Properties** (Proprietà connessione):

- Per modificare l'indirizzo e le credenziali di connessione, selezionare **Edit settings…** (Modifica impostazioni) e quindi immettere le nuove informazioni.
- Per specificare i server ad alta disponibilità per una connessione Citrix Hypervisor, selezionare **Edit servers** (Modifica server) e selezionare i server. Citrix consiglia di selezionare tutti i server del pool per consentire la comunicazione con Citrix Hypervisor in caso di errore del pool master.

  > **Nota:**
  >
  > Se si utilizza HTTPS e si desidera configurare server ad alta disponibilità, non installare un certificato wildcard per tutti i server di un pool. È richiesto un certificato individuale per ogni server.

Pagina **Advanced**:

- Per un tipo di connessione con riattivazione su LAN di Microsoft System Center Configuration Manager (ConfMgr), che viene utilizzato con Accesso remoto al PC, immettere **ConfMgr Wake Proxy**, Magic Packet e informazioni sulla trasmissione dei pacchetti.
- Le impostazioni della soglia di limitazione consentono di specificare un numero massimo di azioni di alimentazione consentite su una connessione. Queste impostazioni possono essere utili quando le impostazioni di gestione dell'alimentazione consentono l'avvio di troppe o troppo poche macchine contemporaneamente. Ogni tipo di connessione ha valori predefiniti specifici appropriati per la maggior parte dei casi e questi non devono essere modificati.
- L'impostazione **Simultaneous actions (all types)** (Azioni simultanee (tutti i tipi)) specifica due valori: un numero assoluto massimo che può verificarsi contemporaneamente su questa connessione e una percentuale massima del totale di macchine che utilizzano questa connessione. È necessario specificare valori sia assoluti che percentuali. Il limite effettivo applicato è il valore più basso.

  Ad esempio, in una distribuzione con 34 macchine, se **Simultaneous actions (all types)** è impostato su un valore assoluto di 10 e un valore percentuale di 10, il limite effettivo applicato è 3 (ovvero il 10% di 34 arrotondato al numero intero più vicino, che è inferiore al valore assoluto di 10 macchine).
- Il valore contenuto in **Maximum new actions per minute** (numero massimo di nuove azioni al minuto) è un numero assoluto. Non esiste un valore percentuale.
- Immettere dati nel campo **Connection options** (Opzioni di connessione) solo sotto la guida di un rappresentante del Supporto Citrix o seguendo istruzioni esplicite della documentazione.

Pagina **Shared Tenants** (Tenant condivisi):

Aggiungere tenant e sottoscrizioni che condividono la Raccolta di calcolo di Azure con la sottoscrizione di questa connessione. Di conseguenza, quando si creano o si aggiornano i cataloghi, è possibile selezionare immagini condivise da questi tenant e sottoscrizioni.

- Inserire l'**ID applicazione** e il **segreto dell'applicazione** per l'applicazione associata a questa connessione. Con queste informazioni, è possibile autenticarsi in Azure. Si consiglia di cambiare regolarmente le chiavi per garantire la sicurezza.
- Specificare i tenant e le sottoscrizioni condivisi. È possibile aggiungere fino a otto tenant condivisi. Per ogni tenant, è possibile aggiungere fino a otto sottoscrizioni.
- Al termine, fare clic su **Save** (Salva) e su **Apply** (Applica).

Immettere le informazioni nel campo **Connection options** (Opzioni di connessione) solo sotto la guida di un rappresentante dell'assistenza Citrix.

Attivare o disattivare la modalità di manutenzione per una connessione

L'attivazione della modalità di manutenzione per una connessione impedisce che qualsiasi nuova azione di alimentazione influisca su qualsiasi macchina archiviata nella connessione. Gli utenti non possono connettersi a una macchina quando è in modalità di manutenzione. Se vi sono utenti già connessi, la modalità di manutenzione ha effetto quando si scollegano.

1. Accedere a Web Studio.
2. Selezionare **Hosting** nel riquadro a sinistra.
3. Selezionare la connessione. Per attivare la modalità di manutenzione, selezionare **Turn On Maintenance Mode** (Attiva modalità di manutenzione) nella barra delle azioni. Per disattivare la modalità di manutenzione, selezionare **Turn Off Maintenance Mode** (Disattiva modalità di manutenzione).

È inoltre possibile attivare o disattivare la modalità di manutenzione per le singole macchine. Inoltre, è possibile attivare o disattivare la modalità di manutenzione per le macchine incluse nei cataloghi macchine o nei gruppi di consegna.

Eliminare una connessione

L'eliminazione di una connessione può comportare l'eliminazione di un gran numero di macchine e la perdita di dati. Assicurarsi che i dati utente sulle macchine interessate siano sottoposti a backup o non più necessari.

Prima di eliminare una connessione, assicurarsi che:

- Tutti gli utenti vengono scollegati dalle macchine memorizzate sulla connessione.

- Nessuna sessione utente disconnessa è in esecuzione.
- La modalità di manutenzione è attivata per macchine in pool e dedicate.
- Tutte le macchine presenti nei cataloghi di macchine utilizzate dalla connessione sono spente.

Un catalogo macchine diventa inutilizzabile quando si elimina una connessione a cui fa riferimento. Se a questa connessione viene fatto riferimento da un catalogo, è possibile eliminare il catalogo. Prima di eliminare un catalogo, assicurarsi che non sia utilizzato da altre connessioni.

1. Accedere a Web Studio.
2. Selezionare **Hosting** nel riquadro a sinistra.
3. Selezionare la connessione e quindi selezionare **Delete Connection** (Elimina connessione) nella barra delle azioni.
4. Se questa connessione contiene macchine archiviate, viene chiesto se tali macchine devono essere eliminate. Se devono essere eliminate, specificare cosa fare con gli account di computer Active Directory associati.

Rinominare o verificare una connessione

1. Accedere a Web Studio.
2. Selezionare **Hosting** nel riquadro a sinistra.
3. Selezionare la connessione e quindi scegliere **Rename Connection** (Rinomina connessione) o **Test Connection** (Verifica connessione) nella barra delle azioni.

Visualizzare i dettagli di una macchina su una connessione

1. Accedere a Web Studio.
2. Selezionare **Hosting** nel riquadro a sinistra.
3. Selezionare la connessione e quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.

Il riquadro superiore contiene un elenco delle macchine a cui si accede tramite la connessione. Selezionare una macchina per visualizzarne i dettagli nel riquadro inferiore. Sono inoltre forniti i dettagli della sessione per le sessioni aperte.

Usare la funzione di ricerca per trovare rapidamente le macchine. Selezionare una ricerca salvata dall'elenco nella parte superiore della finestra o creare una ricerca. È possibile eseguire la ricerca digitando il nome della macchina intero o parte di esso oppure creare un'espressione da utilizzare per una ricerca avanzata. Per creare un'espressione, fare clic su **Unfold** (Apri) e quindi selezionare gli elementi desiderati dagli elenchi di proprietà e operatori.

Gestire le macchine su una connessione

1. Accedere a Web Studio.
2. Selezionare **Hosting** nel riquadro a sinistra.
3. Selezionare una connessione e quindi selezionare **View Machines** (Visualizza macchine) nel riquadro **Actions**.
4. Nella barra delle azioni selezionare una delle opzioni seguenti. Alcune azioni non sono disponibili in determinati stati della macchina e con determinati tipi di host di connessione.

Azione	Descrizione
Start (Avvia)	Avvia la macchina se è spenta o sospesa.
Suspend (Sospendi)	Mette in pausa la macchina senza arrestarla e aggiorna l'elenco delle macchine.
Shut down	Richiede l'arresto del sistema operativo.
Force shut down	Spegne forzatamente la macchina e aggiorna l'elenco delle macchine.
Restart (Riavvia)	Richiede al sistema operativo di arrestare e quindi riavviare la macchina. Se il sistema operativo non è in grado di eseguire la procedura, la macchina rimane nello stato corrente.
Enable maintenance mode	Interrompe temporaneamente i collegamenti a una macchina. Gli utenti non possono connettersi a una macchina che si trova in questo stato. Se vi sono utenti connessi, la modalità di manutenzione avrà effetto quando si scollegheranno. È anche possibile attivare o disattivare la modalità di manutenzione per tutte le macchine a cui si accede tramite una connessione, come descritto sopra.
Remove from Delivery Group	Rimuove la macchina dal gruppo di consegna. Ciò non la elimina dal catalogo macchine utilizzato dal gruppo di consegna. È possibile rimuovere una macchina solo quando non è connesso alcun utente. Attivare la modalità di manutenzione per impedire temporaneamente agli utenti di connettersi durante la rimozione della macchina.

Azione	Descrizione
Delete (Elimina)	Elimina una macchina. Gli utenti non vi hanno più accesso e la macchina viene eliminata dal catalogo macchine. Prima di eliminare una macchina, assicurarsi che tutti i dati utente siano sottoposti a backup o che non siano più necessari. È possibile eliminare una macchina solo quando non vi è connesso alcun utente. Attiva la modalità di manutenzione per impedire temporaneamente agli utenti di connettersi durante l'eliminazione della macchina.

Per le azioni che comportano l'arresto della macchina, se la macchina non chiude la sessione entro 10 minuti, viene spenta. Se Windows tenta di installare aggiornamenti durante l'arresto, c'è il rischio che il computer sia spento prima del completamento degli aggiornamenti.

Modificare lo spazio di archiviazione

È possibile visualizzare lo stato dei server utilizzati per l'archiviazione del sistema operativo e dei dati temporanei per le macchine virtuali che utilizzano una connessione. È inoltre possibile specificare quali server utilizzare per l'archiviazione di ciascun tipo di dati.

1. Accedere a Web Studio.
2. Selezionare **Hosting** nel riquadro a sinistra.
3. Selezionare la connessione e quindi selezionare **Edit Storage** (Modifica archiviazione) nella barra delle azioni.
4. Nel riquadro sinistro, selezionare il tipo di dati: sistema operativo o temporanei.
5. Selezionare o deselezionare le caselle di controllo di uno o più dispositivi di archiviazione per il tipo di dati selezionato.
6. Fare clic su **OK**.

Per ciascun dispositivo di archiviazione incluso nell'elenco sono indicati il nome e lo stato di archiviazione. I valori validi dello stato di archiviazione sono:

- **In use** (In uso): lo spazio di archiviazione è in uso per creare macchine.
- **Superseded** (Sostituito): lo spazio di archiviazione è in uso solo per le macchine esistenti. Non vengono aggiunte nuove macchine in questo spazio di archiviazione.
- **Not in use** (Non in uso): lo spazio di archiviazione non viene utilizzato per la creazione di macchine.

Se si deseleziona la casella di controllo di un dispositivo attualmente in stato **In use**, il suo stato diventa **Superseded**. Le macchine esistenti continueranno a utilizzare quel dispositivo di archiviazione (e possono scrivere dati su di esso), quindi è possibile che tale posizione diventi piena anche quando smette di essere utilizzata per la creazione di macchine.

Eliminare, rinominare o testare le risorse

1. Accedere a Web Studio.
2. Selezionare **Hosting** nel riquadro a sinistra.
3. Selezionare la risorsa e quindi selezionare la voce appropriata nella barra delle azioni: **Delete Resources** (Elimina risorse), **Rename Resources** (Rinomina risorse) o **Test Resources** (Verifica risorse).

Timer di connessione

È possibile utilizzare le impostazioni dei criteri per configurare tre timer di connessione:

- **Maximum connection timer** (Timer di connessione massima): determina la durata massima di una connessione ininterrotta tra un dispositivo utente e un desktop virtuale. Utilizzare le impostazioni dei criteri **Session connection timer** (Timer di connessione sessione) e **Session connection timer interval** (Intervallo del timer di connessione sessione).
- **Connection idle timer** (Timer di inattività della connessione): determina per quanto tempo viene mantenuta una connessione ininterrotta del dispositivo utente a un desktop virtuale se non è presente alcun input da parte dell'utente. Utilizzare le impostazioni dei criteri **Session idle timer** (Timer di inattività sessione) e **Session idle timer interval** (Intervallo del timer di inattività sessione).
- **Disconnect timer** (Timer di disconnessione): determina per quanto tempo un desktop virtuale disconnesso e bloccato può rimanere bloccato prima che la sessione venga scollegata. Utilizzare le impostazioni dei criteri **Disconnected session timer** (Timer sessione disconnessa) e **Disconnected session timer interval** (Intervallo del timer sessione disconnessa).

Quando si aggiorna una di queste impostazioni, assicurarsi che siano coerenti in tutta la distribuzione.

Per ulteriori informazioni, vedere la documentazione sulle impostazioni dei criteri.

Passaggi successivi

Per informazioni sulla connessione a tipi di host specifici, vedere:

- Connessione ad AWS

- Connessione a Citrix Hypervisor
- Connessione agli ambienti cloud di Google
- Connessione a Microsoft Azure
- Connessione a Microsoft System Center Virtual Machine Manager
- Connessione a Nutanix
- Connessione alle soluzioni Nutanix Cloud e dei partner
- Connessione a VMware
- Connessione al cloud VMware e alle soluzioni dei partner

Se ci si trova nel processo di distribuzione iniziale, creare un catalogo delle macchine.

Connessione ad AWS

April 3, 2024

Creare e gestire connessioni e risorse descrive le procedure guidate che creano una connessione. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud AWS.

> **Nota:**
>
> Prima di creare una connessione ad AWS, è prima necessario completare la configurazione del proprio account AWS come posizione delle risorse. Vedere Ambienti cloud AWS.

Creare una connessione

Quando si crea una connessione da Web Studio:

- È necessario fornire la chiave API e i valori della chiave segreta. È possibile esportare il file chiave contenente tali valori da AWS e quindi importarli. È inoltre necessario fornire la regione, la zona di disponibilità, il nome del VPC, gli indirizzi delle subnet, il nome di dominio, i nomi dei gruppi di sicurezza e le credenziali.
- Il file delle credenziali per l'account AWS radice (recuperato dalla console AWS) non è formattato come i file delle credenziali scaricati per gli utenti AWS standard. Pertanto, la gestione di Citrix Virtual Apps and Desktops non può utilizzare il file per popolare i campi della chiave API e della chiave segreta. Assicurarsi di utilizzare i file delle credenziali di AWS Identity Access Management (IAM).

> **Nota:**
>
> Dopo aver creato una connessione, i tentativi di aggiornamento della chiave API e della chiave segreta potrebbero non riuscire. Per risolvere il problema, controllare le restrizioni del server

> proxy o del firewall e assicurarsi che il seguente indirizzo sia contattabile: `https://*.amazonaws.com`.

Valori predefiniti della connessione host

Quando si creano connessioni host in ambienti cloud AWS, vengono visualizzati i seguenti valori predefiniti:

Opzione	Valore assoluto	Percentuale
Azioni simultanee (tutti i tipi)	125	100
Numero massimo di nuove azioni al minuto	125	

MCS supporta 100 operazioni di provisioning simultanee massime per impostazione predefinita.

URL dell'endpoint del servizio

URL dell'endpoint del servizio di zona standard

Quando si utilizza MCS, viene aggiunta una nuova connessione AWS con una chiave API e un segreto API. Con queste informazioni, insieme all'account autenticato, MCS interroga AWS per le zone supportate utilizzando la chiamata API EC2 AWS DescribeRegions. La query viene effettuata utilizzando un URL generico dell'endpoint del servizio EC2 `https://ec2.amazonaws.com/`. Utilizzare MCS per selezionare la zona per la connessione dall'elenco delle zone supportate. L'URL dell'endpoint del servizio AWS preferito viene selezionato automaticamente per la zona. Tuttavia, dopo aver creato l'URL dell'endpoint del servizio, non è più possibile impostarlo o modificarlo.

Definire le autorizzazioni IAM

Utilizzare le informazioni in questa sezione per definire le autorizzazioni IAM per Citrix Virtual Apps and Desktops in AWS. Il servizio IAM di Amazon consente account con più utenti, che possono essere ulteriormente organizzati in gruppi. Questi utenti possono disporre di autorizzazioni diverse per controllare la loro capacità di eseguire operazioni associate all'account. Per ulteriori informazioni sulle autorizzazioni IAM, vedere Riferimento alla policy JSON IAM.

Per applicare la policy delle autorizzazioni IAM a un nuovo gruppo di utenti:

1. Accedere alla Console di gestione AWS e selezionare il **servizio IAM** dall'elenco a discesa.
2. Selezionare **Create a New Group of Users** (Crea un nuovo gruppo di utenti).
3. Digitare un nome per il nuovo gruppo di utenti e selezionare **Continue** (Continua).

4. Nella pagina **Permissions** (Autorizzazioni), scegliere **Custom Policy** (Criterio personalizzato). Selezionare **Select** (Seleziona).
5. Digitare un nome per il **criterio Permissions** (Autorizzazioni).
6. Nella sezione **Policy Document** (Documento del criterio), immettere le autorizzazioni pertinenti.

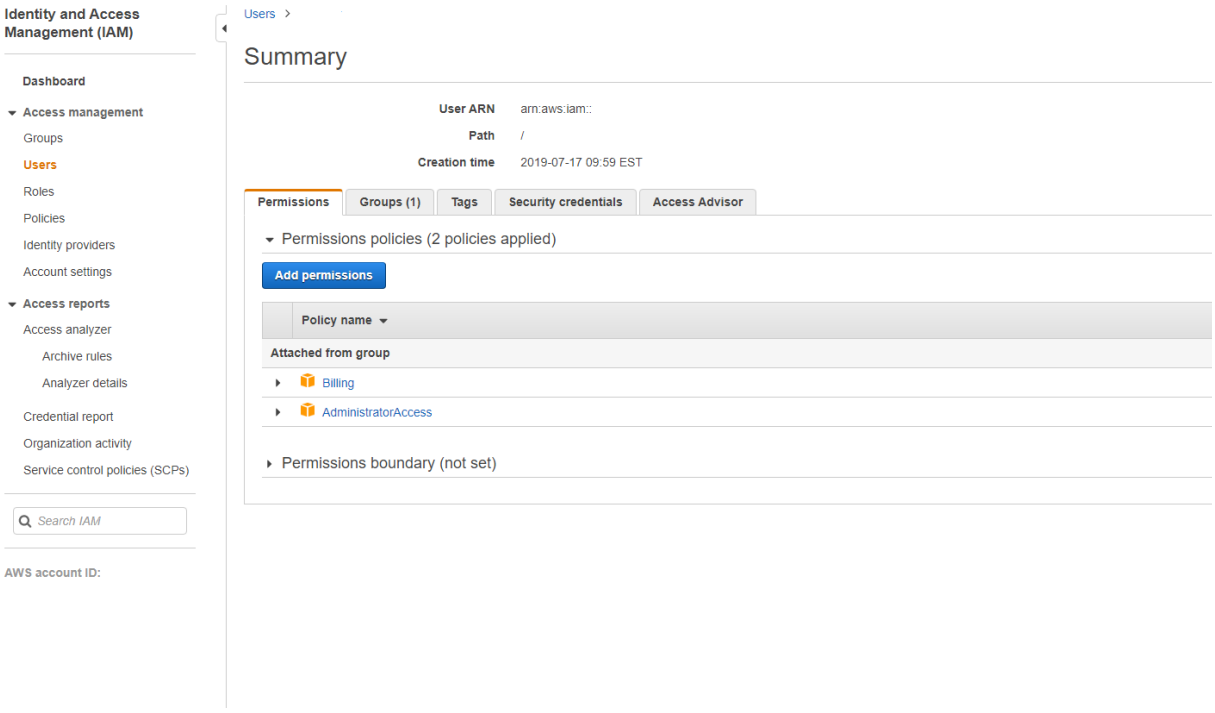
Dopo aver inserito le informazioni sul criterio, selezionare**Continue** (Continua) per completare il gruppo di utenti. Agli utenti del gruppo vengono concesse le autorizzazioni per eseguire solo le azioni richieste per Citrix Virtual Apps and Desktops.

> **Importante:**
>
> Utilizzare il testo del criterio fornito nell'esempio precedente per elencare le azioni utilizzate da Citrix Virtual Apps and Desktops per eseguire azioni all'interno di un account AWS senza limitare tali azioni a risorse specifiche. Citrix consiglia di utilizzare l'esempio a scopo di test. Per gli ambienti di produzione, è possibile scegliere di aggiungere ulteriori restrizioni sulle risorse.

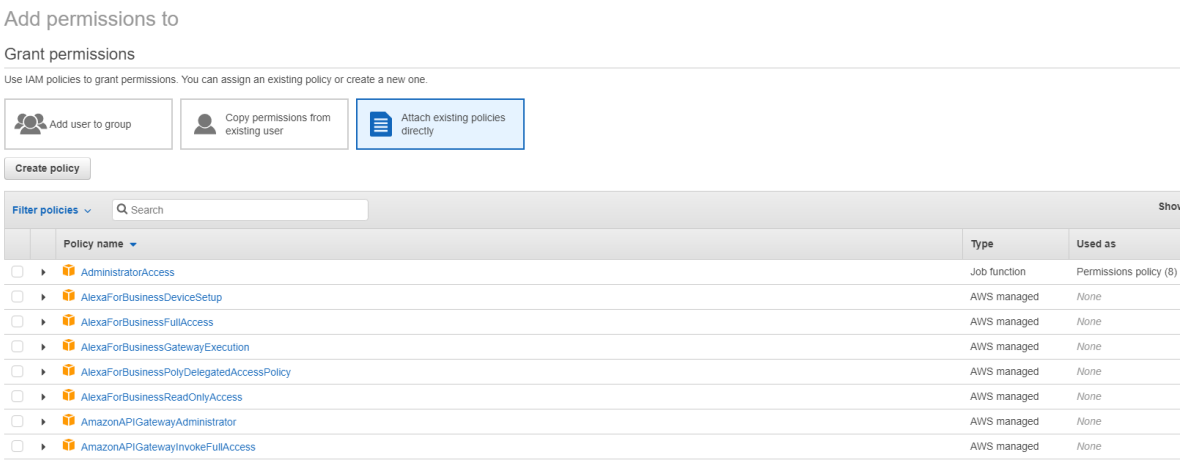
Impostare le autorizzazioni IAM

Impostare le autorizzazioni nella sezione **IAM** della Console di gestione AWS:

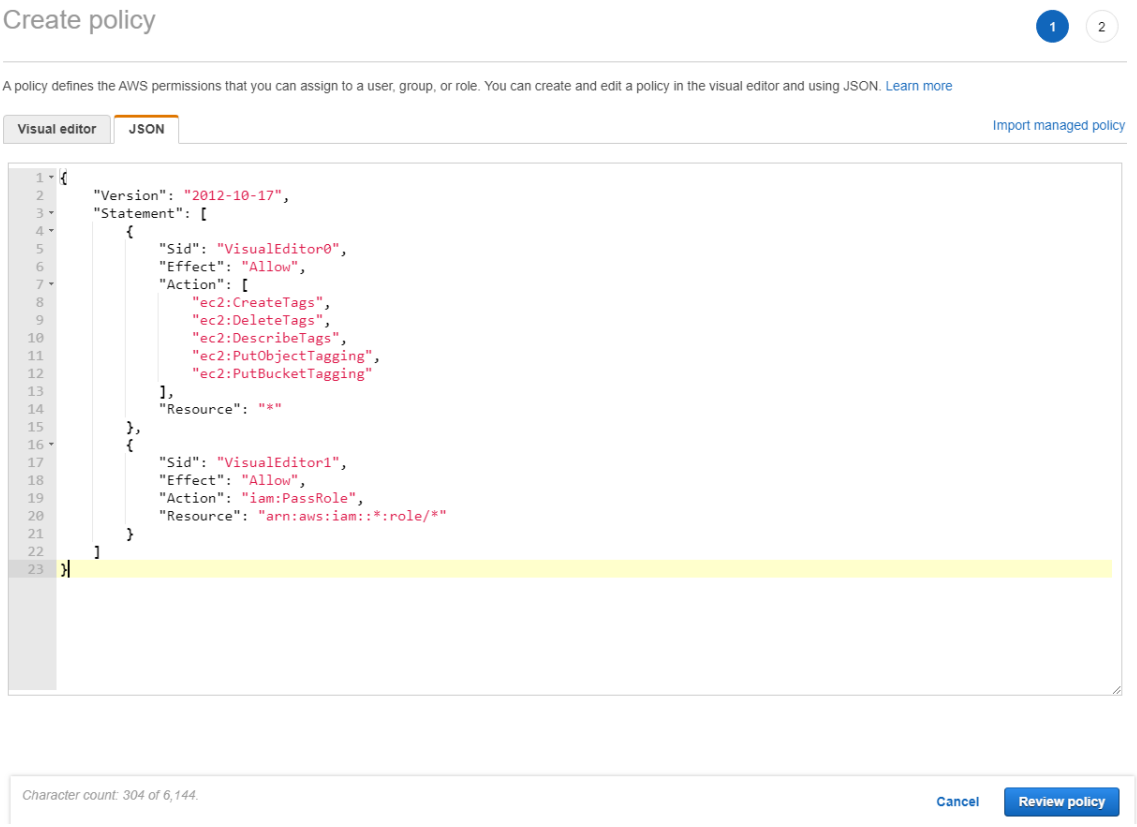
1. Nel pannello **Summary** (Riepilogo), selezionare la scheda **Permissions** (Autorizzazioni).
2. Selezionare **Add permissions** (Aggiungi autorizzazioni).



Nella schermata **Add Permissions to** (Aggiungi autorizzazioni a), concedere le autorizzazioni:



Utilizzare il seguente come esempio nella scheda **JSON**:



> **Suggerimento:**
>
> L'esempio JSON indicato potrebbe non includere tutte le autorizzazioni per l'ambiente. Per ulteriori informazioni, consultare l'articolo su come definire le autorizzazioni di gestione delle identità e degli accessi che eseguono Citrix Virtual Apps and Desktops su AWS.

Autorizzazioni AWS richieste

Questa sezione contiene l'elenco completo delle autorizzazioni AWS.

> **Nota:**
>
> L'autorizzazione *iam:PassRole* è necessaria solo per **role_based_auth**.

Creazione di una connessione host

Viene aggiunta una nuova connessione host utilizzando le informazioni provenienti da AWS.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

Gestione dell'alimentazione delle macchine virtuali

Le istanze delle macchine sono accese o spente.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateVolume",
```



```
                "ec2:DeleteVolume",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DetachVolume",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }

    ]
 }

<!--NeedCopy-->
```

Creazione, aggiornamento o eliminazione di macchine virtuali

Un catalogo delle macchine viene creato, aggiornato o eliminato con macchine virtuali di cui viene eseguito il provisioning come istanze AWS.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
```



```
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
```



```
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }

    ]
 }

<!--NeedCopy-->
```

> **Nota:**
>
> La sezione EC2 relativa ai gruppi di sicurezza è necessaria solo se occorre creare un gruppo di sicurezza di isolamento per la macchina virtuale di preparazione durante la creazione del catalogo. Una volta completata questa operazione, queste autorizzazioni non sono necessarie.

Caricamento e download diretti del disco Il caricamento diretto del disco elimina il requisito del Volume Worker per il provisioning del catalogo delle macchine e utilizza invece le API pubbliche fornite da AWS. Questa funzionalità riduce i costi associati agli account di archiviazione aggiuntivi e alla complessità di gestire le operazioni di Volume Worker.

Le seguenti autorizzazioni devono essere aggiunte al criterio:

- ebs:StartSnapshot
- ebs:GetSnapshotBlock
- ebs:PutSnapshotBlock
- ebs:CompleteSnapshot
- ebs:ListSnapshotBlocks
- ebs:ListChangedBlocks
- ec2:CreateSnapshot
- ec2:DescribeLaunchTemplates

> **Importante:**
>
> - È possibile aggiungere una macchina virtuale ai cataloghi delle macchine esistenti senza alcuna operazione di Volume Worker, come l'AMI Volume Worker e la macchina virtuale del Volume Worker.
> - Se si elimina un catalogo esistente che utilizzava Volume Worker in precedenza, vengono eliminati tutti gli artefatti, inclusi quelli correlati a Volume Worker.

Crittografia EBS dei volumi creati

EBS può crittografare automaticamente i volumi appena creati se l'AMI è crittografata o EBS è configurato per crittografare tutti i nuovi volumi. Tuttavia, per implementare la funzionalità, è necessario includere le seguenti autorizzazioni nel criterio IAM.

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

Nota:

Le autorizzazioni possono essere limitate a chiavi specifiche includendo un blocco di risorse e condizioni a discrezione dell'utente. Ad esempio, **autorizzazioni KMS con condizione**:

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123
                   -456d-a12b-a123b4cd56ef"
```



```
            ],
            "Condition": {

                "Bool": {

                    "kms:GrantIsForAWSResource": true
                 }

             }

         }

    ]
 }

<!--NeedCopy-->
```

La seguente dichiarazione dei criteri chiave è l'intero criterio chiave predefinito per le chiavi KMS necessario per consentire all'account di utilizzare i criteri IAM per delegare l'autorizzazione per tutte le azioni (kms:*) sulla chiave KMS.

```
{

"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {

"AWS": "arn:aws:iam::111122223333:root"
 }
 ,
"Action": "kms:",
"Resource": ""
 }

<!--NeedCopy-->
```

Per ulteriori informazioni, consultare la documentazione ufficiale di AWS Key Management Service.

Autenticazione basata su ruoli IAM

Le seguenti autorizzazioni vengono aggiunte per supportare l'autenticazione basata sui ruoli.

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
```



```
            }

        ]
    }

<!--NeedCopy-->
```

Criteri minimi delle autorizzazioni IAM

Il seguente JSON può essere utilizzato per tutte le funzionalità attualmente supportate. È possibile creare connessioni host, creare, aggiornare o eliminare macchine virtuali ed eseguire la gestione dell'alimentazione utilizzando questo criterio.
Il criterio può essere applicato agli utenti come spiegato nelle sezioni Definizione delle autorizzazioni IAM oppure è anche possibile utilizzare l'autenticazione basata su ruoli utilizzando la chiave di sicurezza **role_based_auth** e la chiave segreta.

> **Importante:**
>
> Per utilizzare **role_based_auth**, configurare innanzitutto il ruolo IAM desiderato su tutti i Delivery Controller del nostro sito. Utilizzando Web Studio, aggiungere la connessione di hosting e fornire role_based_auth per la chiave di autenticazione e il segreto. Una connessione di hosting con queste impostazioni utilizza quindi l'autenticazione basata su ruoli.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
```



```
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
```



```
            "Resource": "arn:aws:s3:::citrix*"
         }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
,
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
         }
,
        {

            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
         }

    ]
}

<!--NeedCopy-->
```

Nota:

- La sezione EC2 relativa a SecurityGroups è necessaria solo se occorre creare un gruppo di sicurezza di isolamento per la macchina virtuale di preparazione durante la creazione del catalogo. Una volta completata questa operazione, queste autorizzazioni non sono necessarie.

- La sezione KMS è necessaria solo quando si utilizza la crittografia del volume EBS.
- La sezione delle autorizzazioni iam:PassRole è necessaria solo per **role_based_auth**.
- È possibile aggiungere autorizzazioni specifiche a livello di risorsa anziché l'accesso completo in base ai requisiti e all'ambiente. Per maggiori dettagli, consultare i documenti AWS Demystifying EC2 Resource-Level Permissions (Sfatare i miti relativi alle autorizzazioni a livello di risorsa EC2) e Gestione degli accessi per le risorse AWS.

Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine
- Per informazioni specifiche su AWS, vedere Creare un catalogo di AWS

Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

Connessione a Citrix Hypervisor

January 7, 2024

Creare e gestire connessioni e risorse descrive le procedure guidate che creano una connessione. Le seguenti informazioni coprono i dettagli specifici degli ambienti di virtualizzazione Citrix Hypervisor.

> **Nota:**
>
> Prima di creare una connessione a Citrix Hypervisor, è prima necessario completare la configurazione del proprio account Citrix Hypervisor come posizione delle risorse. Vedere Ambienti di virtualizzazione Citrix Hypervisor.

Creare una connessione a Citrix Hypervisor

Quando si crea una connessione a Citrix Hypervisor (in precedenza XenServer), è necessario fornire le credenziali di amministratore "power"VM o un utente di livello superiore.

Citrix consiglia di utilizzare HTTPS per proteggere le comunicazioni con Citrix Hypervisor. Per utilizzare HTTPS, è necessario sostituire il certificato SSL predefinito installato su Citrix Hypervisor; vedere CTX128656.

È possibile configurare la disponibilità elevata se è abilitata sul server Citrix Hypervisor. Citrix consiglia di selezionare tutti i server del pool (da Edit High Availability) per consentire la comunicazione con il server Citrix Hypervisor in caso di errore del pool master.

È possibile selezionare un tipo di GPU e un gruppo, o pass-through, se Citrix Hypervisor supporta vGPU. Il display indica se la selezione dispone di risorse GPU dedicate.

Quando si utilizza l'archiviazione locale su uno o più host Citrix Hypervisor per l'archiviazione temporanea dei dati, assicurarsi che ogni posizione di archiviazione nel pool abbia un nome univoco. Per modificare un nome in XenCenter, fare clic con il pulsante destro del mouse sulla posizione di archiviazione e modificare la proprietà del nome.

È possibile utilizzare Citrix Provisioning (in precedenza Provisioning Services) e Machine Creation Services (MCS) per eseguire il provisioning di:

- BIOS legacy per le macchine virtuali con sistema operativo desktop o server supportate.
- UEFI per le macchine virtuali con sistema operativo desktop o server supportate, incluso l'avvio sicuro.

> **Nota:**
>
> Quando si configura MCS, sono necessarie autorizzazioni operatore pool o superiori.

Utilizzare IntelliCache per le connessioni Citrix Hypervisor

Utilizzando IntelliCache, le distribuzioni VDI ospitate sono più convenienti perché è possibile utilizzare una combinazione di archiviazione condivisa e archiviazione locale. Ciò migliora le prestazioni e riduce il traffico di rete. L'archiviazione locale memorizza nella cache l'immagine master dall'archivio condiviso, riducendo il numero di letture sulla posizione di archiviazione condivisa. Per i desktop condivisi, le scritture sui dischi diversi vengono scritte nell'archiviazione locale dell'host e non nell'archiviazione condivisa.

- L'archiviazione condivisa deve essere NFS quando si utilizza IntelliCache.
- Citrix consiglia di utilizzare un dispositivo di archiviazione locale ad alte prestazioni per garantire il trasferimento dati più rapido possibile.

Per utilizzare IntelliCache, è necessario attivarlo sia in questo prodotto che in Citrix Hypervisor.

- Durante l'installazione di Citrix Hypervisor, selezionare **Enable thin provisioning (Optimized storage for Virtual Desktops)** [Abilita thin provisioning (Archiviazione ottimizzata per Virtual Desktops)]. Citrix non supporta pool misti di server in cui IntelliCache è abilitato e server in cui non lo è. Per ulteriori informazioni, vedere la documentazione di Citrix Hypervisor.
- In Citrix Virtual Apps and Desktops, IntelliCache è disabilitato per impostazione predefinita. È possibile modificare l'impostazione solo quando si crea una connessione Citrix Hypervisor; non

è possibile disabilitare IntelliCache in un secondo momento. Quando si aggiunge una connessione Citrix Hypervisor:

- Selezionare **Shared** (Condivisa) come tipo di archiviazione.
- Selezionare la casella di controllo **Use IntelliCache**.

Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine
- Per informazioni specifiche su Citrix Hypervisor, vedere Creare un catalogo di Citrix Hypervisor

Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

Connessione agli ambienti cloud di Google

January 7, 2024

Creare e gestire connessioni e risorse descrive le procedure guidate che creano una connessione. Le seguenti informazioni coprono i dettagli specifici degli ambienti cloud di Google.

> **Nota:**
>
> Prima di creare una connessione agli ambienti cloud di Google, è prima necessario completare la configurazione del proprio account cloud Google come posizione delle risorse. Vedere Ambienti Google Cloud.

Aggiungere una connessione

Seguire le indicazioni fornite in Creare una connessione e risorse. La seguente descrizione guida l'utente nella configurazione di una connessione di hosting:

1. Da **Manage > Configuration** (Gestisci > Configurazione), selezionare **Hosting** nel riquadro di sinistra.
2. Selezionare **Add Connections and Resources** (Aggiungi connessioni e risorse) nella barra delle azioni.

3. Nella pagina **Connection** (Connessione), selezionare **Create a new Connection** (Crea una nuova connessione) e **Citrix provisioning tools** (Strumenti di provisioning Citrix), quindi selezionare **Next** (Avanti).

    - **Tipo di connessione**. Selezionare **Google Cloud** dal menu.
    - **Nome connessione**. Digitare un nome per la connessione.

4. Nella pagina **Region** (Regione), selezionare un nome di progetto dal menu, selezionare una regione contenente le risorse che si desidera utilizzare, quindi selezionare **Next** (Avanti).

5. Nella pagina **Network** (Rete) digitare un nome per le risorse, selezionare una rete virtuale dal menu, selezionare un sottoinsieme e quindi selezionare **Next** (Avanti). Il nome della risorsa aiuta a identificare la regione e la combinazione di rete. Le reti virtuali con il suffisso *(Shared)* (Condivisa) aggiunto al loro nome rappresentano i VPC condivisi. Se si configura un ruolo IAM a livello di subnet per un VPC condiviso, nell'elenco delle subnet vengono visualizzate solo le subnet specifiche del VPC condiviso.

    > **Nota:**
    >
    > - Il nome della risorsa può contenere da 1 a 64 caratteri e non può contenere solo spazi vuoti né i caratteri `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

6. Nella pagina **Summary** (Riepilogo), confermare le informazioni e quindi selezionare **Finish** (Fine) per uscire dalla finestra **Add Connection and Resources** (Aggiungi connessione e risorse).

Dopo aver creato la connessione e le risorse, vengono elencate la connessione e le risorse create. Per configurare la connessione, selezionare la connessione e quindi selezionare l'opzione applicabile nella barra delle azioni.

Allo stesso modo, è possibile eliminare, rinominare o testare le risorse create con la connessione. A tale scopo, selezionare la risorsa sotto la connessione e quindi selezionare l'opzione applicabile nella barra delle azioni.

URL dell'endpoint del servizio

È necessario avere accesso ai seguenti URL:

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Progetti Google Cloud

Esistono fondamentalmente due tipi di progetti Google Cloud:

- Progetto di provisioning: in questo caso, l'account amministratore corrente possiede i computer forniti nel progetto. Questo progetto viene anche definito progetto locale.
- Progetto VPC condiviso: progetto in cui le macchine create nel progetto di provisioning utilizzano il VPC del progetto Shared VPC. L'account amministratore utilizzato per il progetto di provisioning ha autorizzazioni limitate in questo progetto, in particolare solo autorizzazioni per utilizzare il VPC.

Creare un ambiente sicuro per il traffico gestito di GCP

È possibile consentire l'accesso privato di Google ai propri progetti Google Cloud. Questa implementazione migliora la sicurezza per la gestione dei dati sensibili. A tale scopo, è possibile effettuare una delle seguenti operazioni:

- Includere le seguenti regole di ingresso dei controlli del servizio VPC per l'account Cloud Build Service. Se si effettua questa operazione, non seguire i passaggi seguenti per creare un ambiente sicuro per il traffico gestito da GCP.

```
Ingress Rule 1
From:
Identities:
<ProjectID>@cloudbuild.gserviceaccount.com
Source > All sources allowed
To:
Projects =
All projects
Services =
Service name: All services
<!--NeedCopy-->
```

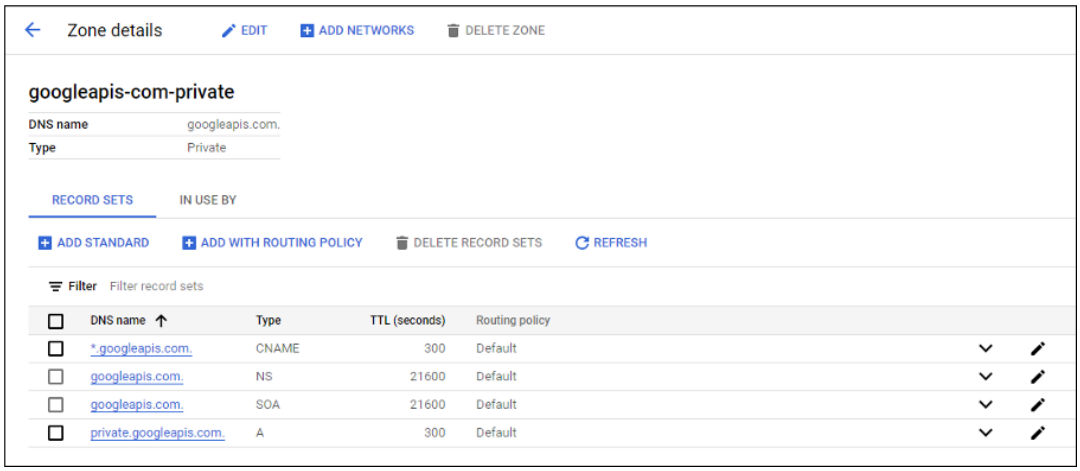
- Se si utilizza un pool di lavoratori privato, aggiungere `UsePrivateWorkerPool` in `CustomProperties`. Per informazioni sul pool di lavoratori privati, vedere Panoramica dei pool privati.

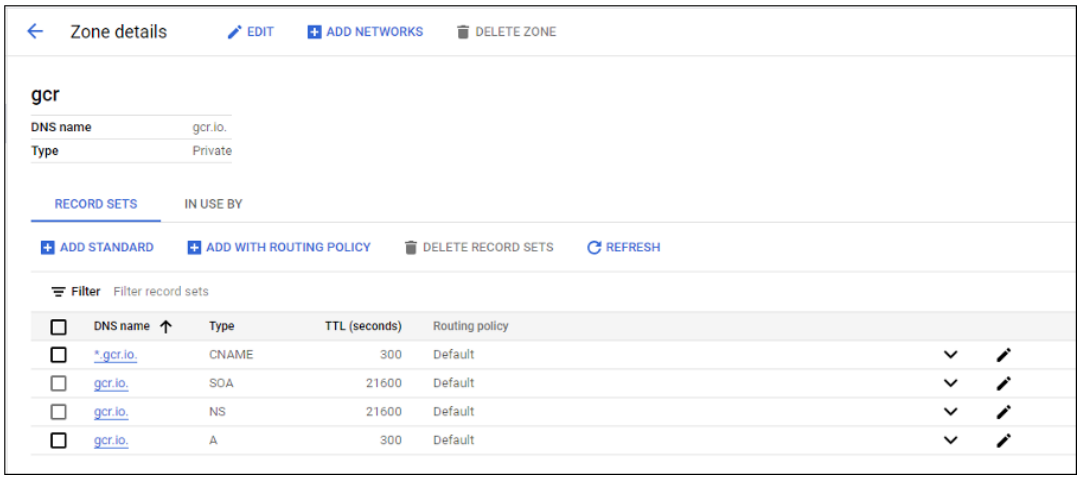
Requisiti per creare un ambiente sicuro per il traffico gestito da GCP

I requisiti per creare un ambiente sicuro per il traffico gestito GCP sono:

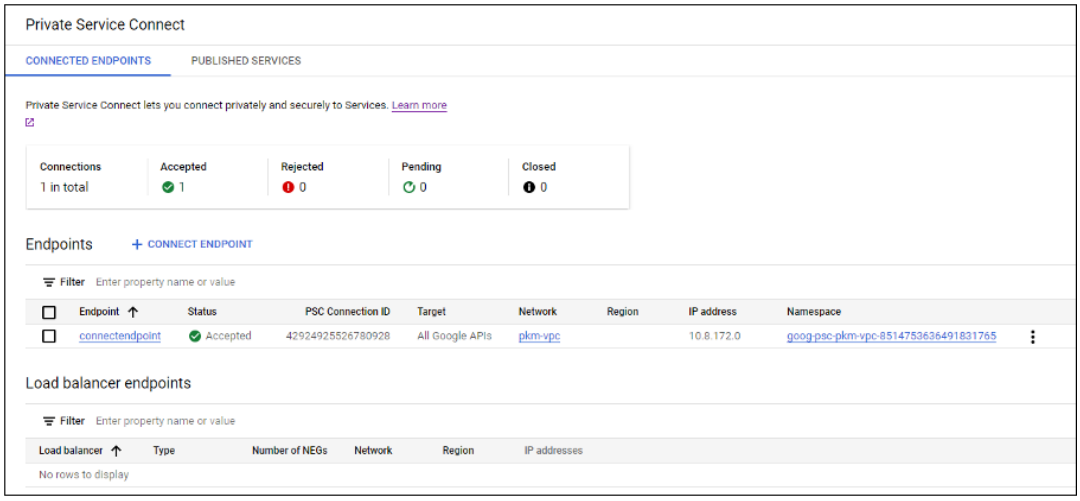
- Assicurarsi che la connessione di hosting sia in modalità di manutenzione durante l'aggiornamento delle proprietà personalizzate.
- Per utilizzare i pool di lavoratori privati, sono necessarie le seguenti modifiche:

- Per Citrix Cloud Service Account, aggiungere i seguenti ruoli IAM:
  * Account del servizio Cloud Build
  * Amministratore istanze Compute
  * Utente account di servizio
  * Creatore token account di servizio
  * Proprietario del pool di worker Cloud Build
- Creare l'account di servizio Citrix Cloud nello stesso progetto che si utilizza per creare una connessione di hosting.
- Configurare le zone DNS per **`private`**`.googleapis.com` e `gcr.io` come descritto nella Configurazione DNS.

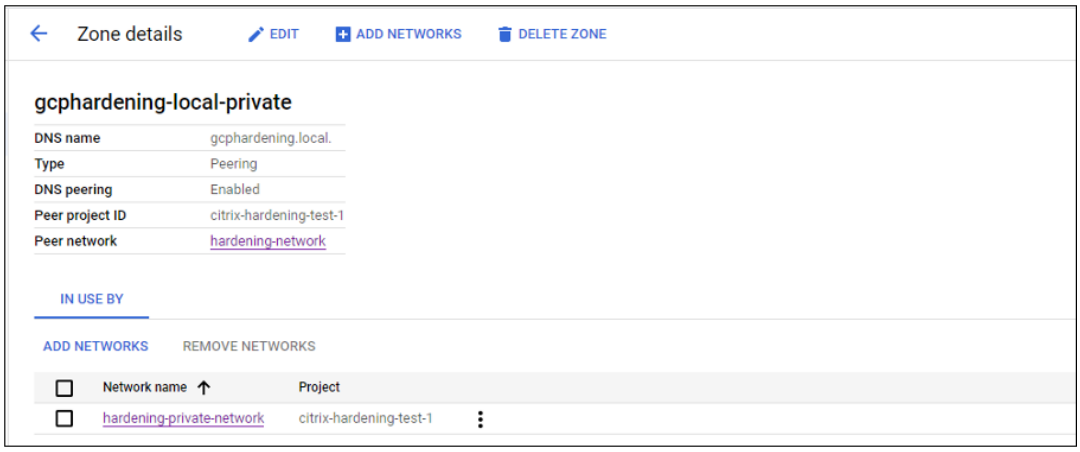




- Configurare la traduzione degli indirizzi di rete (NAT) privata o utilizzare la connessione al servizio privato. Per ulteriori informazioni, vedere Accesso alle API di Google tramite gli endpoint.



- Se si utilizza un VPC con peering, creare una zona Cloud DNS che esegue il peering del VPC con peering. Per ulteriori informazioni, vedere Creazione di una zona di peering.



- Nei controlli dei servizi VPC, impostare le regole di uscita in modo che le API e le VM possano comunicare con Internet. Le regole di ingresso sono opzionali. Ad esempio:

```
Egress Rule 1
From:
Identities:ANY_IDENTITY
To:
Projects =
All projects
Service =
Service name: All services
<!--NeedCopy-->
```

Abilitare il pool di lavoratori privati

Per abilitare il pool di lavoratori privati, impostare le proprietà personalizzate come segue sulla connessione host:

1. Aprire una finestra di PowerShell dall'host Delivery Controller o utilizzare l'SDK Remote PowerShell. Per ulteriori informazioni sull'SDK Remote PowerShell, vedere SDK e API.
2. Eseguire i seguenti comandi:
   a) `Add-PSSnapin citrix*`
   b) `cd XDHyp:\Connections\`
   c) `dir`
3. Copiare le `CustomProperties` dalla connessione a un blocco note.
4. Aggiungere l'impostazione della proprietà `<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"Value="True"/>`. Ad esempio:

```
1 ```
2 <CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance" xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation">
3 <Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
     Value="True"/>
4 </CustomProperties>
5 <!--NeedCopy--> ```
```

5. Nella finestra di PowerShell assegnare una variabile alle proprietà personalizzate modificate. Ad esempio:
   `$customProperty = '<CustomProperties...</CustomProperties>'`.
6. Eseguire `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`.
7. Eseguire `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`.
8. Eseguire `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`.
9. Eseguire quanto segue per aggiornare una connessione host esistente:

```
1 Set-Item -PassThru -Path @('XDHyp:\Connections\\<ENTER YOUR
     CONNECTION NAME HERE>') -SecurePassword $securePassword -
     UserName $gcpServiceAccount -CustomProperties $customProperty
2 <!--NeedCopy-->
```

Autorizzazioni GCP richieste

Questa sezione contiene l'elenco completo delle autorizzazioni GCP. Usare il set completo di autorizzazioni indicato nella sezione per il corretto funzionamento della funzionalità.

Creazione di una connessione host

- Autorizzazioni minime richieste per Citrix Cloud Service Account nel progetto Provisioning:

```
compute.instanceTemplates.list
compute.instances.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```

  I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

  - Amministratore Compute
  - Utente di Cloud Datastore

- Autorizzazioni aggiuntive richieste per Shared VPC for Citrix Cloud Service Account nel progetto Shared VPC:

```
compute.networks.list
compute.subnetworks.list
resourcemanager.projects.get
<!--NeedCopy-->
```

  I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

  - Utente di rete Compute

Gestione dell'alimentazione delle macchine virtuali

Autorizzazioni minime richieste per Citrix Cloud Service Account nel progetto Provisioning:

```
compute.instanceTemplates.list
compute.instances.list
compute.instances.get
compute.instances.reset
compute.instances.resume
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```


I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

- Amministratore Compute
- Utente di Cloud Datastore

Creazione, aggiornamento o eliminazione di macchine virtuali

- Autorizzazioni minime richieste per Citrix Cloud Service Account nel progetto Provisioning:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.start
```



```
compute.instances.stop
compute.instances.suspend
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
iam.serviceAccounts.actAs
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

- Amministratore Compute
- Amministratore archiviazione
- Editor Cloud Build
- Utente account di servizio
- Utente di Cloud Datastore

- Autorizzazioni aggiuntive necessarie per Shared VPC for Citrix Cloud Service Account nel progetto Shared VPC per creare un'unità di hosting utilizzando VPC e una sottorete del progetto Shared VPC:

```
compute.firewalls.list
compute.networks.list
compute.projects.get
compute.regions.list
```



```
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```

I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

- Utente di rete Compute
- Utente di Cloud Datastore

- Autorizzazioni minime richieste per l'account Cloud Build Service nel progetto Provisioning richieste dal servizio Google Cloud Build quando si scarica il disco di istruzioni di preparazione su MCS:

```
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.images.get
compute.images.list
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.getSerialPortOutput
compute.instances.list
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.machineTypes.list
compute.networks.get
compute.networks.list
compute.projects.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
logging.logEntries.create
pubsub.topics.publish
resourcemanager.projects.get
source.repos.get
source.repos.list
storage.buckets.create
storage.buckets.get
storage.buckets.list
```



```
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

- Account del servizio Cloud Build
- Amministratore istanze Compute
- Utente account di servizio

- Autorizzazioni minime richieste per l'account Cloud Compute Service nel progetto Provisioning richieste dal servizio Google Cloud Build quando si scarica il disco di istruzioni di preparazione su MCS:

```
resourcemanager.projects.get
storage.objects.create
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

- Utente di rete Compute
- Utente dell'account di archiviazione
- Utente di Cloud Datastore

- Autorizzazioni aggiuntive richieste per l'account Shared VPC for Cloud Build Service nel progetto Provisioning richieste dal servizio Google Cloud Build quando si scarica il disco di istruzioni di preparazione su MCS:

```
compute.firewalls.list
compute.networks.list
compute.subnetworks.list
compute.subnetworks.use
resourcemanager.projects.get
<!--NeedCopy-->
```

I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

- Utente di rete Compute
- Utente dell'account di archiviazione
- Utente di Cloud Datastore

- Autorizzazioni aggiuntive richieste per Cloud Key Management Service (KMS) per Citrix Cloud Service Account nel progetto Provisioning:

```
cloudkms.cryptoKeys.get
```



```
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
<!--NeedCopy-->
```

I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

- Visualizzatore KMS Compute

Autorizzazioni generali

Di seguito sono riportate le autorizzazioni per Citrix Cloud Service Account nel progetto di Provisioning per tutte le funzionalità supportate in MCS. Queste autorizzazioni garantiscono la migliore compatibilità in futuro:

```
resourcemanager.projects.get
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
```



```
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.instances.update
compute.instances.updateAccessConfig
compute.instances.updateDisplayDevice
compute.instances.updateSecurity
compute.instances.updateShieldedInstanceConfig
compute.instances.updateShieldedVmConfig
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
<!--NeedCopy-->
```


Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine
- Per informazioni specifiche su Google Cloud Platform (GCP), vedere Creare un catalogo di Google Cloud Platform

Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

Connessione a Microsoft Azure

January 7, 2024

Creare e gestire connessioni e risorse descrive le procedure guidate che creano una connessione. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud di Azure Resource Manager.

> **Nota:**
>
> Prima di creare una connessione a Microsoft Azure, è necessario completare la configurazione del proprio account Azure come posizione delle risorse. Vedere Ambienti cloud Microsoft Azure Resource Manager.

Creare entità servizio e connessioni

Prima di creare connessioni, è necessario configurare le entità servizio usate dalle connessioni per accedere alle risorse di Azure. È possibile creare una connessione in due modi:

- Creare un'entità servizio e una connessione allo stesso tempo utilizzando Web Studio
- Creare una connessione utilizzando un'entità servizio creata in precedenza

Questa sezione mostra come completare queste attività:

- Creare un'entità servizio e una connessione utilizzando Web Studio
- Creare un'entità servizio utilizzando PowerShell
- Ottenere il segreto dell'applicazione in Azure
- Creare una connessione utilizzando un'entità servizio esistente

Considerazioni

- Citrix consiglia di utilizzare Service Principal con ruolo di collaboratore. Tuttavia, consulta la sezione Autorizzazioni minime per ottenere l'elenco delle autorizzazioni minime.
- Quando si crea la prima connessione, Azure richiede di concederle le autorizzazioni necessarie. Per le connessioni future è comunque necessario autenticarsi, ma Azure ricorda il consenso precedente e non visualizza più la richiesta.
- Gli account utilizzati per l'autenticazione devono essere co-amministratori della sottoscrizione.
- L'account utilizzato per l'autenticazione deve essere un membro della directory della sottoscrizione. Esistono due tipi di account di cui tenere conto: "lavoro o scuola"e "account Microsoft personale". Vedere CTX219211 per i dettagli.
- Sebbene sia possibile utilizzare un account Microsoft esistente aggiungendolo come membro della directory della sottoscrizione, possono verificarsi complicazioni se all'utente è stato precedentemente concesso l'accesso come ospite a una delle risorse della directory. In questo caso, potrebbe essere presente una voce di segnaposto nella directory che non concede loro le autorizzazioni necessarie e viene restituito un errore.

  Correggere questo problema rimuovendo le risorse dalla directory e aggiungendole di nuovo esplicitamente. Tuttavia, utilizzare questa opzione con attenzione, perché ha effetti indesiderati su altre risorse a cui l'account può accedere.
- Esiste un problema noto per cui alcuni account vengono rilevati come ospiti della directory quando invece sono membri. Configurazioni come questa si verificano in genere con account di directory consolidati precedenti. Soluzione: aggiungere un account alla directory, che assume il valore di appartenenza corretto.
- I gruppi di risorse sono semplicemente contenitori per le risorse e possono contenere risorse provenienti da regioni diverse dalla propria. Ciò può creare potenzialmente confusione se si prevede che le risorse visualizzate nella regione di un gruppo di risorse siano disponibili.
- Assicurarsi che la rete e la subnet siano sufficientemente grandi da ospitare il numero di macchine necessarie. Ciò richiede una certa lungimiranza, ma Microsoft aiuta a specificare i valori corretti, con indicazioni sulla capacità dello spazio degli indirizzi.

Creare un'entità servizio e una connessione utilizzando Web Studio

> **Importante:**
>
> Questa funzionalità non è ancora disponibile per le sottoscrizioni di Azure in Cina e in Germania.

Con Web Studio è possibile creare sia un'entità servizio che una connessione in un unico flusso di lavoro. Le entità servizio consentono alle connessioni di accedere alle risorse di Azure. Quando si es-

egue l'autenticazione in Azure per creare un'entità servizio, un'applicazione viene registrata in Azure. Viene creata una chiave segreta (chiamata segreto del client o segreto dell'applicazione) per l'applicazione registrata. L'applicazione registrata (in questo caso una connessione) utilizza il segreto del client per l'autenticazione in Azure AD.

Prima di iniziare, assicurarsi che siano soddisfatti questi prerequisiti:

- Avere un account utente nel tenant Azure Active Directory della propria sottoscrizione.
- L'account utente Azure AD sia anche co-amministratore per la sottoscrizione di Azure che si desidera utilizzare per il provisioning delle risorse.
- Si dispone delle autorizzazioni di amministratore globale, amministratore dell'applicazione o sviluppatore di applicazioni per l'autenticazione. Queste autorizzazioni possono essere revocate dopo aver creato una connessione host. Per ulteriori informazioni sui ruoli, vedere Ruoli predefiniti di Azure AD.

Utilizzare la procedura guidata **Add Connection and Resources** (Aggiungi connessione e risorse) per creare insieme un'entità servizio e una connessione allo stesso tempo:

1. Nella pagina **Connection** (Connessione), selezionare **Create a new connetion** (Crea una nuova connessione), il tipo di connessione **Microsoft Azure** e l'ambiente Azure.
2. Selezionare gli strumenti da utilizzare per creare le macchine virtuali, quindi selezionare **Next** (Avanti).
3. Nella pagina **Connection Details** (Dettagli connessione), inserire il proprio ID sottoscrizione di Azure e un nome per la connessione. Dopo aver inserito l'ID sottoscrizione, viene abilitato il pulsante **Create new** (Crea nuova).

   > **Nota:**
   >
   > Il nome della connessione può contenere da 1 a 64 caratteri e non può contenere solo spazi vuoti né i caratteri `\/;:#.*?=<>|[]{ } "'()'`.

4. Selezionare **Create new** (Crea nuova), quindi inserire il nome utente e la password dell'account Azure Active Directory.
5. Selezionare **Sign in** (Accedi).
6. Selezionare **Accept** (Accetta) per concedere a Citrix Virtual Apps and Desktops le autorizzazioni elencate. Citrix Virtual Apps and Desktops crea un'entità servizio che consente di gestire le risorse di Azure per conto dell'utente specificato.
7. Dopo aver selezionato **Accept** (Accetta), si torna alla pagina **Connection** (Connessione) della procedura guidata.

> **Nota:**
>
> Dopo aver eseguito l'autenticazione in Azure, i pulsanti **Create new** (Crea nuova) e **Use existing** (Usa esistente) scompaiono. Viene visualizzato il testo **Connection successful** (Connessione riuscita), con un segno di spunta verde che indica la connessione riuscita alla sottoscrizione di Azure.

8. Nella pagina **Connection Details** (Dettagli connessione), selezionare **Next** (Avanti).

> **Nota:**
>
> Non è possibile passare alla pagina successiva finché non ci si autentica correttamente in Azure e non si acconsente a concedere le autorizzazioni richieste.

9. Configurare le risorse per la connessione. Le risorse comprendono la regione e la rete.
   - Nella pagina **Region** (Regione), selezionare una regione.
   - Nella pagina **Network** (Rete), procedere come segue:
     - Digitare un nome da 1 a 64 caratteri per la risorsa, per semplificare l'identificazione della combinazione di regione e rete. Il nome di una risorsa non può contenere solo spazi vuoti né i caratteri `\/;:#.*?=<>|[]{ } "'()'`.
     - Selezionare una coppia rete virtuale/gruppo di risorse (se si dispone di più di una rete virtuale con lo stesso nome, l'associazione del nome della rete con il gruppo di risorse fornisce combinazioni univoche). Se la regione selezionata nella pagina precedente non dispone di reti virtuali, tornare a quella pagina e selezionare una regione con reti virtuali.
10. Nella pagina **Summary** (Riepilogo), visualizzare un riepilogo delle impostazioni e selezionare **Finish** (Fine) per completare la configurazione.

Visualizzare l'ID dell'applicazione Dopo aver creato una connessione, è possibile visualizzare l'ID dell'applicazione utilizzata dalla connessione per accedere alle risorse di Azure.

Nell'elenco **Add Connection and Resources** (Aggiungi connessione e risorse), selezionare la connessione per visualizzare i dettagli. La scheda **Details** (Dettagli) mostra l'ID dell'applicazione.

Creare un'entità servizio utilizzando PowerShell

Per creare un'entità servizio utilizzando PowerShell, connettersi alla sottoscrizione di Azure Resource Manager e utilizzare i cmdlet PowerShell forniti nelle sezioni seguenti.

Assicurarsi di avere a portata di mano quanto segue:

- **SubscriptionId:** `SubscriptionID` di Azure Resource Manager per la sottoscrizione in cui si desidera eseguire il provisioning di VDA.
- **ActiveDirectoryID**: ID tenant dell'applicazione registrata con Azure AD.
- **ApplicationName:** nome dell'applicazione da creare in Azure AD.

I passaggi dettagliati sono i seguenti:

Connettersi alla sottoscrizione Azure Resource Manager.

```
`Connect-AzAccount`
```

1. Selezionare la sottoscrizione Azure Resource Manager in cui si desidera creare l'entità servizio.

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-
   AzSubscription
   ```

2. Creare l'applicazione nel proprio tenant AD.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. Creare un'entità servizio.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. Assegnare un ruolo all'entità servizio.

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
    $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. Dalla finestra di output della console PowerShell, prendere nota dell'ApplicationId. Fornire questo ID quando si crea la connessione host.

Ottenere il segreto dell'applicazione in Azure

Per creare una connessione utilizzando un'entità servizio esistente, è prima necessario ottenere l'ID e il segreto dell'applicazione dell'entità servizio nel portale di Azure.

I passaggi dettagliati sono i seguenti:

1. Ottenere l'**ID dell'applicazione** da Web Studio o utilizzando PowerShell.
2. Accedere al portale di Azure.
3. In Azure, selezionare **Azure Active Directory**.
4. Da **Registrazioni app** in Azure AD, selezionare la propria applicazione.
5. Andare a **Certificati e segreti**.
6. Fare clic su **Client secrets** (Segreti client).

Creare una connessione utilizzando un'entità servizio esistente

Se si dispone già di un'entità servizio, è possibile utilizzarla per creare una connessione utilizzando Web Studio.

Assicurarsi di avere a portata di mano quanto segue:

- SubscriptionId
- ActiveDirectoryID (tenant ID)
- ID applicazione
- Segreto dell'applicazione

  Per ulteriori informazioni, vedere Ottenere il segreto dell'applicazione.
- Data di scadenza del segreto

I passaggi dettagliati sono i seguenti:

Nella procedura guidata **Add Connection and Resources** (Aggiungi connessione e risorse):

1. Nella pagina **Connection** (Connessione), selezionare **Create a new connetion** (Crea una nuova connessione), il tipo di connessione **Microsoft Azure** e l'ambiente Azure.
2. Selezionare gli strumenti da utilizzare per creare le macchine virtuali, quindi selezionare **Next** (Avanti).
3. Nella pagina **Connection Details** (Dettagli connessione), inserire il proprio ID sottoscrizione di Azure e un nome per la connessione.

   > **Nota:**
   >
   > Il nome della connessione può contenere da 1 a 64 caratteri e non può contenere solo spazi vuoti né i caratteri `\/;:#.*?=<>|[]{ } "'()'`.

4. Selezionare **Use existing** (Usa esistente). Nella finestra **Existing Service Principal Details** (Dettagli entità servizio esistente), immettere le seguenti impostazioni per l'entità servizio esistente. Dopo aver inserito i dettagli, il pulsante **Save** (Salva) è abilitato. Selezionare **Save** (Salva). Non è possibile andare oltre questa pagina finché non si forniscono dettagli validi.

   - **Subscription ID** (ID sottoscrizione). Inserire il proprio ID sottoscrizione di Azure. Per ottenere l'ID sottoscrizione, accedere al portale di Azure e andare a **Sottoscrizioni > Panoramica**.
   - **Active Directory ID** (ID Active Directory) (ID tenant). Inserire l'ID Directory (tenant) dell'applicazione che si è registrata con Azure AD.

- **Application ID** (ID applicazione). Inserire l'ID applicazione (client) dell'applicazione registrata con Azure AD.
- **Application secret** (Segreto dell'applicazione). Creare una chiave segreta (segreto client). L'applicazione registrata utilizza la chiave per l'autenticazione in Azure AD. Si consiglia di cambiare le chiavi regolarmente per motivi di sicurezza. Assicurarsi di salvare la chiave, perché non è possibile recuperarla in un secondo momento.
- **Secret expiration date** (Data di scadenza del segreto). Immettere la data dopo la quale il segreto dell'applicazione scade. Si riceverà un avviso sulla console prima della scadenza della chiave segreta. Tuttavia, se la chiave segreta scade, si ricevono errori.

  > **Nota:**
  >
  > Per motivi di sicurezza, il periodo di scadenza non può essere superiore a due anni da oggi.

- **Authentication URL** (URL di autenticazione). Questo campo viene compilato automaticamente e non è modificabile.
- **Management URL** (URL di gestione). Questo campo viene compilato automaticamente e non è modificabile.
- **Storage suffix** (Suffisso di archiviazione). Questo campo viene compilato automaticamente e non è modificabile.

  L'accesso ai seguenti endpoint è necessario per creare un catalogo MCS in Azure. L'accesso a questi endpoint ottimizza la connettività tra la rete e il portale di Azure e i relativi servizi.

  - Authentication URL: https://login.microsoftonline.com/
  - Management URL: https://management.azure.com/. Questo è un URL di richiesta per le API del provider di Azure Resource Manager. L'endpoint per la gestione dipende dall'ambiente. Ad esempio, per Azure Global è https://management.azure.com/ e per Azure US Government è https://management.usgovcloudapi.net/.
  - Storage suffix: https://*.core.windows.net./. Questo (*) è un carattere jolly per il suffisso di archiviazione. Ad esempio, `https://demo.table.core.windows.net/`.

5. Dopo aver selezionato **Save** (Salva), si torna alla pagina **Connection Details** (Dettagli connessione). Selezionare **Next** (Avanti) per passare alla pagina successiva.
6. Configurare le risorse per la connessione. Le risorse comprendono la regione e la rete.

   - Nella pagina **Region** (Regione), selezionare una regione.
   - Nella pagina **Network** (Rete), procedere come segue:

- Digitare un nome da 1 a 64 caratteri per la risorsa, per semplificare l'identificazione della combinazione di regione e rete. Il nome di una risorsa non può contenere solo spazi vuoti né i caratteri `\/;:#.*?=<>|[]{ } "'()'`.
- Selezionare una coppia rete virtuale/gruppo di risorse (se si dispone di più di una rete virtuale con lo stesso nome, l'associazione del nome della rete con il gruppo di risorse fornisce combinazioni univoche). Se la regione selezionata nella pagina precedente non dispone di reti virtuali, tornare a quella pagina e selezionare una regione con reti virtuali.

7. Nella pagina **Summary** (Riepilogo), visualizzare un riepilogo delle impostazioni e selezionare **Finish** (Fine) per completare la configurazione.

Gestire le entità servizio e le connessioni

Questa sezione descrive in dettaglio come gestire le entità servizio e le connessioni:

- Configurare le impostazioni di limitazione delle richieste di Azure
- Abilitare la condivisione di immagini in Azure
- Aggiungere tenant condivisi a una connessione utilizzando Full Configuration
- Implementare la condivisione di immagini tramite PowerShell
- Gestire il segreto dell'applicazione e la data di scadenza del segreto

Configurare le impostazioni di limitazione delle richieste di Azure

Azure Resource Manager limita le richieste di sottoscrizione e tenant, instradando il traffico in base a limiti definiti, a seconda delle esigenze specifiche del provider. Per ulteriori informazioni, vedere Limitazione delle richieste di Resource Manager sul sito Microsoft. Sono previsti dei limiti per sottoscrizioni e tenant, a causa dei quali la gestione di molte macchine può diventare problematica. Ad esempio, in una sottoscrizione contenente molte macchine potrebbero verificarsi dei problemi di prestazioni relativi alle operazioni di alimentazione.

> **Suggerimento:**
>
> Per ulteriori informazioni, vedere Miglioramento delle prestazioni di Azure con Machine Creation Services.

Per contribuire a mitigare questi problemi, è possibile rimuovere la limitazione delle richieste interna di MCS per utilizzare maggiormente la quota di richieste disponibile da Azure.

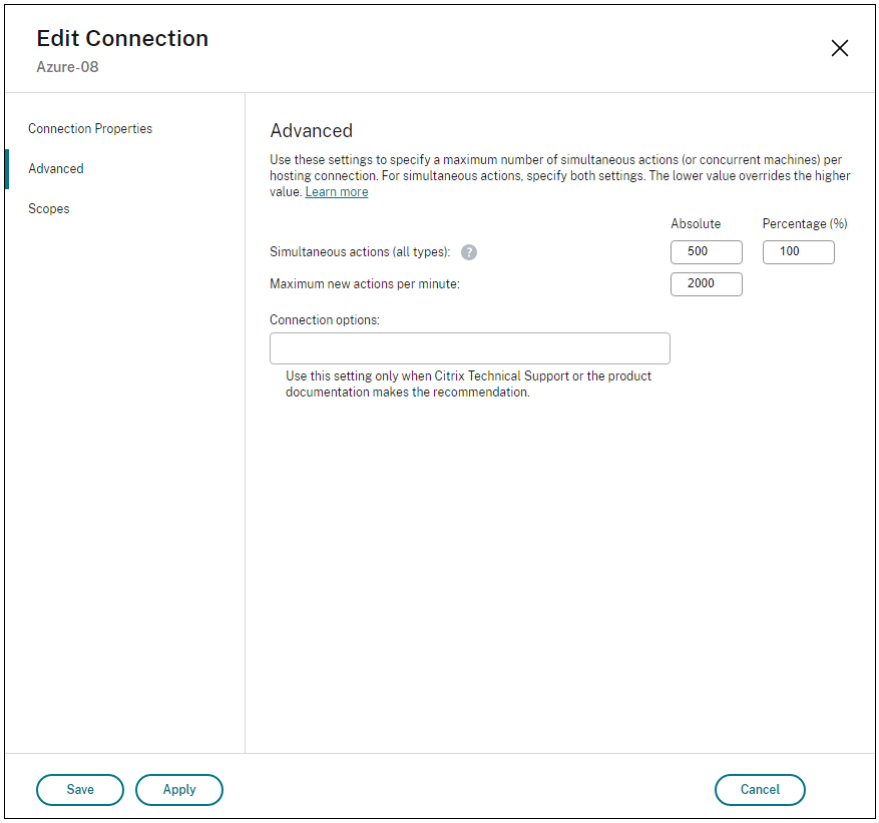
Si consigliano le seguenti impostazioni ottimali quando si accendono o si spengono le macchine virtuali in sottoscrizioni di grandi dimensioni, ad esempio quelle contenenti 1.000 macchine virtuali:

- Operazioni simultanee assolute: 500

- Numero massimo di nuove operazioni al minuto: 2.000
- Numero massimo di operazioni simultanee: 500

Utilizzare Web Studio per configurare le operazioni di Azure per una determinata connessione Azure:

1. In Web Studio, selezionare **Hosting** nel riquadro a sinistra.
2. Selezionare la connessione.
3. Nella procedura guidata **Edit Connection** (Modifica connessione), selezionare **Advanced** (Avanzate).
4. Nella pagina **Advanced** (Avanzate), utilizzare le opzioni di configurazione per specificare il numero di azioni simultanee e il numero massimo di nuove azioni al minuto, nonché eventuali opzioni di connessione aggiuntive.



MCS supporta massimo 500 operazioni simultanee per impostazione predefinita. In alternativa, è possibile utilizzare l'SDK Remote PowerShell per impostare il numero massimo di operazioni simultanee.

Utilizzare la proprietà **PowerShell** `MaximumConcurrentProvisioningOperations` per specificare il numero massimo di operazioni di provisioning simultanee di Azure. Quando si utilizza questa proprietà, considerare:

- Il valore predefinito di `MaximumConcurrentProvisioningOperations` è 500.

- Configurare il parametro `MaximumConcurrentProvisioningOperations` utilizzando il comando PowerShell `Set-item`.

Abilitare la condivisione di immagini in Azure

Quando si creano o si aggiornano cataloghi delle macchine, è possibile selezionare immagini condivise provenienti da diverse sottoscrizioni e tenant di Azure (condivise tramite la Raccolta di calcolo di Azure). Per abilitare la condivisione di immagini all'interno di tenant o fra uno e l'altro, è necessario configurare le impostazioni necessarie in Azure:

- Condividere immagini all'interno di un tenant (tra abbonamenti)
- Condividere immagini tra tenant

Condividere immagini all'interno di un tenant (tra abbonamenti) Perché sia possibile selezionare in Raccolta di calcolo di Azure un'immagine che appartiene a una sottoscrizione diversa, l'immagine deve essere condivisa con l'entità servizio (SPN) di quella sottoscrizione.

Ad esempio, se esiste un'entità servizio (SPN 1) configurata in Studio come:

Entità servizio: SPN 1

Subscription: subscription 1

Tenant: tenant 1

L'immagine è in una sottoscrizione diversa, che è configurata in Studio come:

Subscription: subscription 2

Tenant: tenant 1

Se si intende condividere l'immagine della sottoscrizione 2 con la sottoscrizione 1 (SPN 1), passare alla sottoscrizione2 e condividere il gruppo di risorse con SPN1.

L'immagine deve essere condivisa con un altro SPN utilizzando il controllo degli accessi in base al ruolo di Azure (RBAC). Azure RBAC è il sistema di autorizzazione usato per gestire l'accesso alle risorse di Azure. Per ulteriori informazioni su Azure RBAC, vedere il documento Microsoft Che cos'è il controllo degli accessi in base al ruolo di Azure. Per concedere l'accesso, si assegnano ruoli alle entità servizio nell'ambito del gruppo di risorse con il ruolo di collaboratore. Per assegnare i ruoli di Azure, è necessario disporre di un'autorizzazione `Microsoft.Authorization/roleAssignments/write`, come nel caso di un Amministratore Accesso utenti o un Proprietario. Per ulteriori informazioni sulla condivisione di immagini con un altro SPN, vedere il documento Microsoft Assegnare ruoli di Azure usando il portale di Azure.

Per informazioni sulla selezione di un'immagine da una sottoscrizione diversa mediante i comandi PowerShell, vedere Selezionare un'immagine da un'altra sottoscrizione.

Condividere immagini tra tenant Per condividere immagini tra tenant con la Raccolta di calcolo di Azure, creare una registrazione dell'applicazione.

Ad esempio, se ci sono due tenant (Tenant 1 e Tenant 2) e si desidera condividere la propria galleria di immagini con Tenant 1, allora:

1. Creare una domanda di registrazione per Tenant 1. Per ulteriori informazioni, vedere Creare la registrazione dell'app.
2. Consentire a Tenant 2 di accedere all'applicazione richiedendo l'accesso tramite un browser. Sostituire `Tenant2 ID` con l'ID tenant del Tenant 1. Sostituire `Application (client) ID` con l'ID dell'applicazione della registrazione dell'applicazione creata. Quando si sono completate le sostituzioni, incollare l'URL in un browser e seguire le istruzioni di accesso per accedere al Tenant 2. Ad esempio:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
      client_id=<Application (client) ID>&response_type=code&
      redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   <!--NeedCopy-->
   ```

   Per ulteriori informazioni, vedere Concedere l'accesso al tenant 2.
3. Concedere all'applicazione l'accesso al gruppo di risorse Tenant 2. Accedere come Tenant 2 e concedere alla registrazione dell'app l'accesso al gruppo di risorse che contiene l'immagine della raccolta. Per ulteriori informazioni, vedere Eseguire l'autenticazione delle richieste su più tenant.

Per creare un catalogo utilizzando un'immagine di un tenant diverso utilizzando i comandi PowerShell:

1. Aggiornare le proprietà personalizzate della connessione di hosting con ID tenant condivisi.
2. Selezionare un'immagine da un altro tenant.

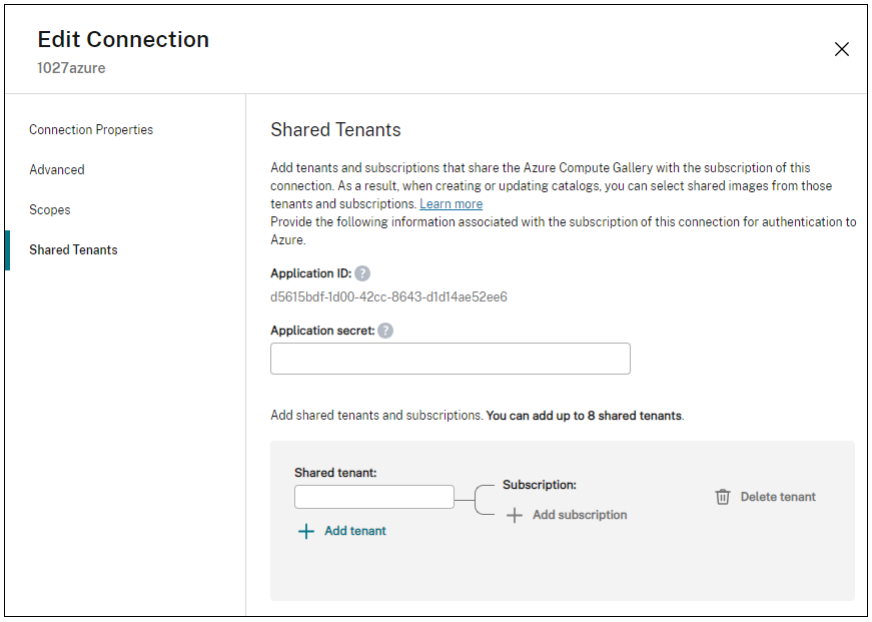
Aggiungere tenant condivisi a una connessione utilizzando Full Configuration

Quando si creano o si aggiornano cataloghi delle macchine in Web Studio, è possibile selezionare immagini condivise provenienti da diverse sottoscrizioni e tenant di Azure (condivise tramite la Raccolta di calcolo di Azure). La funzionalità richiede che vengano fornite informazioni condivise sul tenant e sulla sottoscrizione per le connessioni host associate.

> **Nota:**
>
> Assicurarsi di aver configurato le impostazioni necessarie in Azure per abilitare la condivisione di immagini tra tenant. Per ulteriori informazioni, vedere Condividere immagini tra tenant.

Completare i seguenti passaggi per una connessione:

1. In Web Studio, selezionare **Hosting** nel riquadro a sinistra.
2. Selezionare la connessione e quindi selezionare **Edit Connection** (Modifica connessione) nella barra delle azioni.



3. In **Shared Tenants** (Tenant condivisi), procedere come segue:
   - Fornire l'ID dell'applicazione e il segreto dell'applicazione associati alla sottoscrizione della connessione. Citrix Virtual Apps and Desktops utilizza queste informazioni per l'autenticazione in Azure AD.
   - Aggiungere tenant e sottoscrizioni che condividono la Raccolta di calcolo di Azure con la sottoscrizione della connessione. È possibile aggiungere fino a 8 tenant condivisi e 8 sottoscrizioni per ogni tenant.
4. Al termine, selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra oppure selezionare **OK** per applicare le modifiche e chiudere la finestra.

Implementare la condivisione di immagini tramite PowerShell

Questa sezione illustra i processi di condivisione delle immagini tramite PowerShell:

- Selezionare un'immagine da un'altra sottoscrizione
- Aggiornare le proprietà personalizzate della connessione di hosting con ID tenant condivisi
- Selezionare un'immagine da un altro tenant

Selezionare un'immagine da un'altra sottoscrizione È possibile selezionare un'immagine in Raccolta di calcolo di Azure che appartiene a una sottoscrizione condivisa diversa all'interno dello stesso tenant di Azure per creare e aggiornare i cataloghi MCS usando i comandi di PowerShell.

1. Nella cartella principale dell'unità di hosting, Citrix crea una nuova cartella di sottoscrizione condivisa chiamata `sharedsubscription`.
2. Elencare tutte le sottoscrizioni condivise di un tenant.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\sharedsubscription.folder"
<!--NeedCopy-->
```

3. Selezionare un abbonamento condiviso, quindi elencare tutti i gruppi di risorse condivise di quella sottoscrizione condivisa.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription"
<!--NeedCopy-->
```

4. Selezionare un gruppo di risorse, quindi elencare tutte le gallerie di quel gruppo di risorse.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription\ xyz.resourcegroup"
<!--NeedCopy-->
```

5. Selezionare una raccolta, quindi elencare tutte le definizioni delle immagini di quella raccolta.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resourcegroup\testgallery.gallery"
<!--NeedCopy-->
```

6. Selezionare una definizione di immagine, quindi elencare tutte le versioni dell'immagine in questione.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resourcegroup\sigtestdef.imagedefinition"
<!--NeedCopy-->
```

7. Creare e aggiornare un catalogo MCS utilizzando i seguenti elementi:

   - Gruppo di risorse
   - Raccolta
   - Definizione delle immagini della raccolta
   - Versione delle immagini della raccolta.

   Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Aggiornare le proprietà personalizzate della connessione di hosting con ID tenant condivisi
Utilizzare `Set-Item` per aggiornare le proprietà personalizzate della connessione di hosting

con ID tenant e ID di abbonamento condivisi. Aggiungere una proprietà `SharedTenants` in `CustomProperties`. Il formato di `Shared Tenants` è:

```
[{
 "Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":["7
    bb42f40-8d7f-4230-a920-be2781f6d5d9"] }
 ,{
 "Tenant":"50e83564-c4e5-4209-b43d-815c45659564","Subscriptions":["06
    ab8944-6a88-47ee-a975-43dd491a37d0"] }
 ]
<!--NeedCopy-->
```

Ad esempio:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://schemas.
   citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
   /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`" Value=`"
   123`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`" Value
   =`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
   Value=`"https://login.microsoftonline.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value=`"
   core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`
   " />
<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`" Value=`"`[
    {
  'Tenant':'123abc', 'Subscriptions':['345', '567']  }
  ]`"` />
</CustomProperties>"
-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "
   advc345" -SecurePassword
$psd
<!--NeedCopy-->
```

> **Nota:**
>
> È possibile aggiungere più di un tenant. Ogni inquilino può avere più di una sottoscrizione.

Selezionare un'immagine da un altro tenant È possibile selezionare nella Raccolta di calcolo di Azure un'immagine che appartiene a un diverso tenant di Azure per creare e aggiornare i cataloghi MCS usando i comandi di PowerShell.

1. Nella cartella principale dell'unità di hosting, Citrix crea una nuova cartella di sottoscrizione condivisa chiamata `sharedsubscription`.
2. Elencare tutte le sottoscrizioni condivise.

```
Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
```



```
<!--NeedCopy-->
```

3. Selezionare un abbonamento condiviso, quindi elencare tutti i gruppi di risorse condivise di quella sottoscrizione condivisa.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription
<!--NeedCopy-->
```

4. Selezionare un gruppo di risorse, quindi elencare tutte le gallerie di quel gruppo di risorse.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\ xyz.resourcegroup
<!--NeedCopy-->
```

5. Selezionare una raccolta, quindi elencare tutte le definizioni delle immagini di quella raccolta.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery
<!--NeedCopy-->
```

6. Selezionare una definizione di immagine, quindi elencare tutte le versioni dell'immagine in questione.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery\hij.
    imagedefinition
<!--NeedCopy-->
```

7. Creare e aggiornare un catalogo MCS utilizzando i seguenti elementi:

   - Gruppo di risorse
   - Raccolta
   - Definizione delle immagini della raccolta
   - Versione delle immagini della raccolta.

   Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Gestire il segreto dell'applicazione e la data di scadenza del segreto

Accertarsi di aver modificato il segreto dell'applicazione per una connessione prima della scadenza del segreto. Si riceverà un avviso su Web Studio prima della scadenza della chiave segreta.

Creare un segreto dell'applicazione in Azure È possibile creare un segreto dell'applicazione per una connessione tramite il portale di Azure.

1. Selezionare **Azure Active Directory**.
2. Da **Registrazioni app** in Azure AD, selezionare la propria applicazione.
3. Andare a **Certificati e segreti**.
4. Fare clic su **Segreti client > Nuovo segreto client**.
5. Fornire una descrizione del segreto e specificare una durata. Al termine, selezionare **Add** (Aggiungi).

   > **Nota:**
   >
   > Assicurarsi di salvare il segreto del client, perché non è possibile recuperarlo in un secondo momento.

6. Copiare il valore del segreto del client e la data di scadenza.
7. In Web Studio modificare la connessione corrispondente e sostituire il contenuto nei campi **Application secret** (Segreto applicazione) e **Secret expiration date** (Data di scadenza del segreto) con i valori copiati.

Modificare la data di scadenza del segreto È possibile utilizzare Web Studio per aggiungere o modificare la data di scadenza del segreto dell'applicazione in uso.

1. Nella procedura guidata **Add Connection and Resources** (Aggiungi connessione e risorse), fare clic con il pulsante destro del mouse su una connessione e fare clic su **Edit Connection** (Modifica connessione).
2. Nella pagina **Connection Properties** (Proprietà connessione), fare clic su **Secret expiration date** (Data di scadenza del segreto) per aggiungere o modificare la data di scadenza del segreto dell'applicazione in uso.

Autorizzazioni Azure richieste

Questa sezione contiene le autorizzazioni minime e generali richieste per Azure.

Autorizzazioni minime

Le autorizzazioni minime offrono un migliore controllo della sicurezza. Tuttavia, le nuove funzionalità che richiedono autorizzazioni aggiuntive non funzionano se si utilizzano solo le autorizzazioni minime.

Creazione di una connessione host Aggiungere una nuova connessione host utilizzando le informazioni ottenute da Azure.

```
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/disks/read",
<!--NeedCopy-->
```

Gestione dell'alimentazione delle macchine virtuali Accendere o spegnere le istanze della macchina.

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
<!--NeedCopy-->
```

Creazione, aggiornamento o eliminazione di macchine virtuali Creare un catalogo delle macchine, quindi aggiungere, eliminare, aggiornare le macchine ed eliminare il catalogo delle macchine.

Di seguito è riportato l'elenco delle autorizzazioni minime richieste quando l'immagine master è un disco gestito o le snapshot si trovano nella stessa area geografica della connessione di hosting.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkInterfaces/read",
```



```
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
<!--NeedCopy-->
```

Sono necessarie le seguenti autorizzazioni aggiuntive basate su autorizzazioni minime per le seguenti funzionalità:

- Se l'immagine master è un disco rigido virtuale (VHD) in un account di archiviazione situato nella stessa area geografica della connessione host:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
<!--NeedCopy-->
```

- Se l'immagine master è una ImageVersion della Raccolta immagini condivise:

```
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
<!--NeedCopy-->
```

- Se l'immagine master è un disco gestito, le snapshot o il VHD si trovano in una regione diversa dalla regione della connessione di hosting:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/delete",
<!--NeedCopy-->
```

- Se si utilizza un gruppo di risorse gestito da Citrix:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
<!--NeedCopy-->
```

- Se si colloca l'immagine master nella Raccolta immagini condivise:

```
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
<!--NeedCopy-->
```

- Se si utilizza il supporto degli host dedicati di Azure:


```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
<!--NeedCopy-->
```

- Se si utilizza la crittografia lato server (SSE) con le chiavi gestite dal cliente (CMK):

```
"Microsoft.Compute/diskEncryptionSets/read",
<!--NeedCopy-->
```

- Se si distribuiscono macchine virtuali utilizzando modelli ARM (profilo macchina):

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
<!--NeedCopy-->
```

- Se si utilizza la specifica del modello di Azure come profilo macchina:

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
<!--NeedCopy-->
```

Creazione, aggiornamento ed eliminazione di macchine con disco non gestito Di seguito è riportato l'elenco delle autorizzazioni minime richieste quando l'immagine master è un VHD e utilizza il gruppo di risorse come fornito dall'amministratore:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action"
<!--NeedCopy-->
```


Autorizzazione generale

Il ruolo di collaboratore ha accesso completo per gestire tutte le risorse. Questo set di autorizzazioni non impedisce di ottenere nuove funzionalità.

Il seguente set di autorizzazioni fornisce la migliore compatibilità in futuro, sebbene includa più autorizzazioni del necessario con il set di funzionalità corrente:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/delete",
```



```
46 "Microsoft.Resources/subscriptions/resourceGroups/read",
47 "Microsoft.Resources/subscriptions/resourceGroups/write",
48 "Microsoft.Resources/subscriptions/resourceGroups/delete",
49 "Microsoft.Storage/storageAccounts/delete",
50 "Microsoft.Storage/storageAccounts/listKeys/action",
51 "Microsoft.Storage/storageAccounts/read",
52 "Microsoft.Storage/storageAccounts/write",
53 "Microsoft.Resources/templateSpecs/read",
54 "Microsoft.Resources/templateSpecs/versions/read",
55 <!--NeedCopy-->
```

Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine
- Per informazioni specifiche su Azure, vedere Creare un catalogo di Microsoft Azure

Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

Connessione a Microsoft System Center Virtual Machine Manager

January 7, 2024

Creare e gestire connessioni e risorse descrive le procedure guidate che creano una connessione. Le seguenti informazioni riguardano dettagli specifici di Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Prima di creare una connessione a VMM, è necessario completare la configurazione del proprio account VMM come posizione delle risorse. Vedere Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager.

Creare una connessione

Se è stato utilizzato MCS per eseguire il provisioning delle macchine virtuali, eseguire le seguenti operazioni nella procedura guidata di creazione della connessione:

- Immettere l'indirizzo come nome di dominio completo del server host.

- Inserire le credenziali per l'account amministratore impostato in precedenza. Questo account deve disporre dell'autorizzazione a creare nuove macchine virtuali.
- Nella finestra di dialogo Host Details (Dettagli host) selezionare il cluster o l'host autonomo da utilizzare per la creazione di macchine virtuali.

  > **Importante**
  >
  > Cercare un cluster o un host autonomo anche se si utilizza una singola distribuzione host Hyper-V.

Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine
- Per creare cataloghi di macchine con MCS sulla condivisione di file SMB 3, vedere Creare un catalogo di Microsoft System Center Virtual Machine Manager

Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

Connessione a Nutanix

January 7, 2024

Creare e gestire connessioni e risorse descrive le procedure guidate che creano una connessione. Le seguenti informazioni coprono i dettagli specifici di Nutanix.

> **Nota:**
>
> Prima di creare una connessione a Nutanix, è necessario completare la configurazione del proprio account Nutanix come posizione delle risorse. Vedere Ambienti di virtualizzazione Nutanix.

Creare una connessione a Nutanix

Le seguenti informazioni si aggiungono alle informazioni guida di Connessioni e risorse. Per creare una connessione Nutanix, seguire la guida generale di quell'articolo, tenendo conto dei dettagli specifici di Nutanix.

Nella procedura guidata **Aggiungere connessioni e risorse**, selezionare il tipo di connessione Nutanix nella pagina **Connection**, quindi specificare l'indirizzo e le credenziali, oltre a un nome per la connessione. Nella pagina **Network** selezionare una rete per l'unità di hosting.

Sono disponibili i seguenti tipi di connessione: **Nutanix AHV**, **Nutanix AHV DRaaS** e **Nutanix AHV PC**.

- Per **Nutanix AHV** specificare l'indirizzo e le credenziali del cluster Prism Element (PE).
- Per **Nutanix AHV PC**, specificare l'indirizzo e le credenziali di Prism Central (PC).

  > **Nota:**
  >
  > Attualmente, il tipo di connessione Nutanix AHV PC viene utilizzato solo per creare una connessione a Nutanix Cloud Cluster (NC2) su Azure. Inoltre, un catalogo di macchine può essere ospitato solo su un singolo cluster in una connessione NC2 su Azure.

- Per **Nutanix AHV DRaaS**, specificare l'indirizzo e il nome utente del tenant DRaaS. Importare i propri file di credenziali Nutanix DRaaS privati e pubblici (`.pem`).

> **Suggerimento:**
>
> Se si distribuiscono macchine utilizzando Nutanix AHV (Prism Element) come risorsa, selezionare il contenitore in cui risiede il disco della macchina virtuale.

Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine
- Per informazioni specifiche su Nutanix, vedere Creare un catalogo di Nutanix

Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

Connessione alle soluzioni Nutanix Cloud e dei partner

January 7, 2024

Creare e gestire connessioni e risorse descrive le procedure guidate che creano una connessione. Le seguenti informazioni coprono i dettagli specifici delle soluzioni Nutanix Cloud e dei partner.

Citrix Virtual Apps and Desktops supporta la seguente soluzione Nutanix Cloud e dei partner:

- Nutanix Cloud Clusters su AWS

> **Nota:**
>
> Prima di creare una connessione a Nutanix Cloud e dei partner, è necessario completare la configurazione del proprio account come posizione delle risorse. Scopri le Soluzioni Nutanix Cloud e dei partner.

Connettersi a Nutanix Prism

Dopo aver creato un cluster Nutanix, connettersi a Nutanix Prism.

Per connettersi a Nutanix Prism:

1. Creare una macchina virtuale bastion nella subnet 10.0.129.0/24.
2. Creare una connessione RDP alla macchina virtuale bastion, andare all'URL del **Prism Element** copiato nella sezione precedente.
3. Accedere utilizzando le credenziali predefinite: `admin:nutanix/4u`. Ricordarsi di cambiare la password.

Creare una macchina virtuale sul cluster Nutanix

Dopo essersi connessi a **Nutanix Prism**, creare macchine virtuali sul cluster Nutanix.

Se la macchina virtuale ha bisogno di accesso a Internet

1. Andare alla console AWS.
2. Creare una nuova subnet 10.0.130.0/24 nello stesso VPC di quella creata da Nutanix CFS.
3. Aggiungere un percorso alla tabella di instradamento di questa subnet per indirizzare tutto il traffico locale al gateway NAT sopra indicato.
4. Creare una connessione RDP alla macchina virtuale bastion, andare all'URL del **Prism Element** copiato nella sezione precedente e accedere.
5. Aggiungere una nuova rete. Andare a **Settings>Network Configuration>Create Subnet** (Impostazioni> Configurazione di rete> Crea subnet). Utilizzare la stessa sottorete 10.0.130.0/24 utilizzata in AWS.
6. Creare tutte le macchine virtuali (AD, CC, VDA e così via) in quella nuova subnet.

Se la macchina virtuale non ha bisogno di accesso a Internet

1. Creare una connessione RDP alla macchina virtuale bastion, andare all'URL del **Prism Element** copiato nella sezione precedente e accedere.

2. Aggiungere una nuova rete. Andare a **Settings>Network Configuration>Create Subnet** (Impostazioni> Configurazione di rete> Crea subnet). Usare la subnet 10.0.129.0/24.
3. Creare tutte le macchine virtuali (AD, CC, VDA e così via) in quella subnet.

> **Suggerimento:**
>
> Assicurarsi che le informazioni relative all'ora e al fuso orario nelle macchine virtuali siano impostate correttamente. Questo è particolarmente importante per AD.

Creare una connessione host

1. Avviare Web Studio.
2. Selezionare il nodo di hosting e fare clic su **Add Connection and Resources** (Aggiungi connessione e risorse).
3. Nella schermata **Connection** (Connessione), selezionare **Create a new Connection** (Crea una nuova connessione) e nel campo **Connection address** (Indirizzo di connessione) immettere `https://xxx.xxx.xxx.xxx:9440`.
4. Seguire l'interfaccia utente per completare la procedura guidata.

> **Nota:**
>
> Per vedere l'opzione Nutanix in Web Studio, tutte le macchine virtuali con connettore devono avere il plug-in Nutanix installato, anche se non sono utilizzate nella zona Nutanix.

Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine
- Per informazioni specifiche su Nutanix, vedere Creare un catalogo di Nutanix

Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

Connessione a VMware

January 7, 2024

Creare e gestire connessioni e risorse descrive le procedure guidate che creano una connessione. Le seguenti informazioni coprono i dettagli specifici degli ambienti di virtualizzazione VMware.

> **Nota:**
>
> Prima di creare una connessione a VMware, è necessario completare la configurazione del proprio account VMware come posizione delle risorse. Vedere Ambienti di virtualizzazione VMware.

Creare una connessione

Nella procedura guidata di creazione della connessione:

1. Selezionare il tipo di connessione VMware.
2. Specificare l'indirizzo del punto di accesso per l'SDK di vCenter.
3. Specificare le credenziali di un account utente VMware configurato in precedenza che disponga delle autorizzazioni per la creazione di macchine virtuali. Specificare il nome utente nel formato dominio/nome utente.

Impronta digitale SSL di VMware

La funzione di identificazione personale SSL di VMware elimina la necessità di creare manualmente una connessione host a un hypervisor VMware vSphere. Non è più necessario creare manualmente una relazione di trust tra i Delivery Controllers presenti nel Sito e il certificato dell'hypervisor prima di creare una connessione.

La funzionalità di identificazione personale SSL di VMware memorizza l'identificazione personale del certificato non attendibile nel database del sito. Questa configurazione garantisce che l'hypervisor possa essere continuamente identificato come attendibile da Citrix Virtual Apps and Desktops, anche se non dai Controller.

Quando si crea una connessione host vSphere in Studio, una finestra di dialogo consente di visualizzare il certificato del computer a cui ci si connette. È quindi possibile scegliere se considerarlo affidabile.

Privilegi richiesti

Creare un account utente VMware e uno o più ruoli VMware. Basare la creazione di questi ruoli sul livello di granularità al quale è necessario assegnare autorizzazioni agli utenti. Definire i privilegi per ciascun ruolo, utilizzando l'elenco delle autorizzazioni vCenter necessarie a Citrix Virtual Apps and Desktops per eseguire le operazioni.

Per concedere autorizzazioni a un utente, associare l'utente al ruolo a livello di data center. Per ulteriori informazioni sull'impostazione delle autorizzazioni in vCenter, vedere la documentazione di VMware.

Nelle tabelle seguenti vengono illustrati i mapping tra le operazioni di Citrix Virtual Apps and Desktops e i privilegi VMware minimi richiesti.

> **Nota:**
>
> Il nome visualizzato dell'elenco delle autorizzazioni, in particolare l'*interfaccia utente*, è diverso per alcune versioni di vSphere. Ad esempio, in vSphere 6.7 l'autorizzazione *User Interface* (Interfaccia utente) è **Change Memory** (Modifica memoria) e **Change Settings** (Modifica impostazioni), anziché **Settings** (Impostazioni) e **Memory** (Memoria) come descritto nei privilegi richiesti indicati in questa pagina.

Aggiungere connessioni e risorse

SDK	Interfaccia utente
System. Anonimo, System. Read e System.View	Aggiunto automaticamente. È possibile utilizzare il ruolo di sola lettura incorporato.

Gestione dell'alimentazione

SDK	Interfaccia utente
VirtualMachine.Interact.PowerOff	Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power Off (Spegni)
VirtualMachine.Interact.PowerOn	Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power On (Accendi)
VirtualMachine.Interact.Reset	Virtual machine (Macchina virtuale) > Interaction (Interazione) > Reset (Reimposta)
VirtualMachine.Interact.Suspend	Virtual machine (Macchina virtuale) > Interaction (Interazione) > Suspend (Sospendi)

Provisioning di macchine (Machine Creation Services)

Per effettuare il provisioning delle macchine tramite MCS, le seguenti autorizzazioni sono obbligatorie:

SDK	Interfaccia utente
Datastore.AllocateSpace	Datastore > Allocate space (Alloca spazio)
Datastore.Browse	Datastore > Browse datastore (Sfoglia datastore)
Datastore.FileManagement	Datastore > Low level file operations (Operazioni file di basso livello)
Network.Assign	Network (Rete) > Assign network (Assegna rete)
Resource.AssignVMToPool	Resource (Risorsa) > Assign virtual machine to resource pool (Assegna macchina virtuale al pool di risorse)
VirtualMachine.Config.AddExistingDisk	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Add existing disk (Aggiungi disco esistente)
VirtualMachine.Config.AddNewDisk	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Add new disk (Aggiungi nuovo disco)
VirtualMachine.Config.AdvancedConfig	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Advanced (Avanzate)
VirtualMachine.Config.RemoveDisk	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Remove disk (Rimuovi disco)
VirtualMachine.Config.CPUCount	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Change CPU Count (Modifica conteggio CPU)
VirtualMachine.Config.Memory	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Change memory (Modifica memoria)
VirtualMachine.Config.Settings	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Change settings (Modifica impostazioni)
VirtualMachine.Interact.PowerOff	Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power Off (Spegni)
VirtualMachine.Interact.PowerOn	Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power On (Accendi)
VirtualMachine.Interact.Reset	Virtual machine (Macchina virtuale) > Interaction (Interazione) > Reset (Reimposta)

SDK	Interfaccia utente
VirtualMachine.Interact.Suspend	Virtual machine (Macchina virtuale) > Interaction (Interazione) > Suspend (Sospendi)
VirtualMachine.Inventory.CreateFromExisting	Virtual machine (Macchina virtuale) > Inventory (Inventario) > Create from existing (Crea da esistente)
VirtualMachine.Inventory.Create	Virtual machine (Macchina virtuale) > Inventory (Inventario) > Create new (Crea nuova)
VirtualMachine.Inventory.Delete	Virtual machine (Macchina virtuale) > Inventory (Inventario) > Remove (Rimuovi)
VirtualMachine.Provisioning.Clone	Virtual machine (Macchina virtuale) > Provisioning > Clone virtual machine (Clona macchina virtuale)
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2, vSphere 5.1, Update 1 e vSphere 6.x, Update 1: Virtual machine (Macchina virtuale) > State (Stato) > Create snapshot (Crea snapshot); vSphere 5.5: Virtual machine (Macchina virtuale) > Snapshot management (Gestione snapshot) > Create snapshot (Crea snapshot)

Aggiornamento e rollback delle immagini

SDK	Interfaccia utente
Datastore.AllocateSpace	Datastore > Allocate space (Alloca spazio)
Datastore.Browse	Datastore > Browse datastore (Sfoglia datastore)
Datastore.FileManagement	Datastore > Low level file operations (Operazioni file di basso livello)
Network.Assign	Network (Rete) > Assign network (Assegna rete)
Resource.AssignVMToPool	Resource (Risorsa) > Assign virtual machine to resource pool (Assegna macchina virtuale al pool di risorse)
VirtualMachine.Config.AddExistingDisk	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Add existing disk (Aggiungi disco esistente)

SDK	Interfaccia utente
VirtualMachine.Config.AddNewDisk	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Add new disk (Aggiungi nuovo disco)
VirtualMachine.Config.AdvancedConfig	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Advanced (Avanzate)
VirtualMachine.Config.RemoveDisk	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Remove disk (Rimuovi disco)
VirtualMachine.Interact.PowerOff	Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power Off (Spegni)
VirtualMachine.Interact.PowerOn	Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power On (Accendi)
VirtualMachine.Interact.Reset	Virtual machine (Macchina virtuale) > Interaction (Interazione) > Reset (Reimposta)
VirtualMachine.Inventory.CreateFromExisting	Virtual machine (Macchina virtuale) > Inventory (Inventario) > Create from existing (Crea da esistente)
VirtualMachine.Inventory.Create	Virtual machine (Macchina virtuale) > Inventory (Inventario) > Create new (Crea nuova)
VirtualMachine.Inventory.Delete	Virtual machine (Macchina virtuale) > Inventory (Inventario) > Remove (Rimuovi)
VirtualMachine.Provisioning.Clone	Virtual machine (Macchina virtuale) > Provisioning > Clone virtual machine (Clona macchina virtuale)

Eliminare le macchine con provisioning

SDK	**Interfaccia utente**
Datastore.Browse	Datastore > Browse datastore (Sfoglia datastore)
Datastore.FileManagement	Datastore > Low level file operations (Operazioni file di basso livello)
VirtualMachine.Config.RemoveDisk	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Remove disk (Rimuovi disco)

SDK	Interfaccia utente
VirtualMachine.Interact.PowerOff	Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power Off (Spegni)
VirtualMachine.Inventory.Delete	Virtual machine (Macchina virtuale) > Inventory (Inventario) > Remove (Rimuovi)

Profilo di storage (vSAN)

Per visualizzare, creare o eliminare i criteri di archiviazione durante la creazione di cataloghi su un datastore vSAN, sono obbligatorie le seguenti autorizzazioni:

SDK	Interfaccia utente
storage.Profile-driven storage update	PROFILE-DRIVEN STORAGE > Profile-driven storage update
storage.Profile-driven storage view	PROFILE-DRIVEN STORAGE > Profile-driven storage view

Tag e attributi personalizzati

I tag e gli attributi personalizzati consentono di allegare metadati alle macchine virtuali create nell' inventario di vSphere e semplificano la ricerca e il filtraggio di questi oggetti. Per creare, modificare, assegnare ed eliminare tag o categorie, sono obbligatorie le seguenti autorizzazioni:

SDK	Interfaccia utente
Tagging.Create	vSphere Tagging > Create vSphere Tag (Crea tag vSphere)
Tagging.Create	vSphere Tagging > Create vSphere Tag Category (Crea categoria di tag vSphere)
Tagging.Edit	vSphere Tagging > Edit vSphere Tag (Modifica tag vSphere)
Tagging.Edit	vSphere Tagging > Edit vSphere Tag Category (Modifica categoria di tag vSphere)
Tagging.Delete	vSphere Tagging > Delete vSphere Tag (Elimina tag vSphere)

SDK	Interfaccia utente
Tagging.Delete	vSphere Tagging > Delete vSphere Tag Category (Elimina categoria di tag vSphere)
Tagging.Assign	vSphere Tagging > Assign or Unassign vSphere Tag (Assegna o annulla assegnazione del tag vSphere)
Tagging.Assign	vSphere Tagging > Assign or Unassign vSphere Tag on Object (Assegna o annulla l'assegnazione di tag vSphere all'oggetto)
Global.ManageCustomFields	Global (Globali) > Manage custom attributes (Gestisci attributi personalizzati)
Global.SetCustomField	Global (Globali) > Set custom attribute (Imposta attributo personalizzato)

> **Nota:**
>
> Quando MCS crea un catalogo di macchine, assegna alle VM di destinazione speciali tag con nomi. Questi tag differenziano l'immagine master dalle VM create da MCS e impediscono l'utilizzo di macchine virtuali create da MCS per la preparazione delle immagini. È possibile identificare la differenza in base al valore dell'attributo `XdProvisioned` in vCenter. L'attributo è impostato su **True** se MCS crea macchine virtuali.

Operazioni crittografiche

I privilegi delle operazioni crittografiche controllano quali utenti possono eseguire i diversi tipi di operazioni crittografiche e su quale tipo di oggetto. vSphere Native Key Provider utilizza i privilegi `Cryptographer.*`. Per le operazioni crittografiche sono necessarie le seguenti autorizzazioni minime:

> **Nota:**
>
> Queste autorizzazioni sono necessarie per creare cataloghi di macchine MCS con VM dotata di vTPM.

SDK	Interfaccia utente
Cryptographic operations.Direct Access	Privileges > All Privileges > Cryptographic operations > Direct Access (Privilegi > Tutti i privilegi > Operazioni crittografiche > Accesso diretto)
Cryptographic operations.Add disk	Privileges > All Privileges > Cryptographic operations > Add disk (Privilegi > Tutti i privilegi > Operazioni crittografiche > Aggiungi disco)
Cryptographic operations.Clone	Privileges > All Privileges > Cryptographic operations > Clone (Privilegi > Tutti i privilegi > Operazioni crittografiche > Clone)
Cryptographic operations.Encrypt	Privileges > All Privileges > Cryptographic operations > Encrypt (Privilegi > Tutti i privilegi > Operazioni crittografiche > Crittografa)
Cryptographic operations.Encrypt new	Privileges > All Privileges > Cryptographic operations > Encrypt new (Privilegi > Tutti i privilegi > Operazioni crittografiche > Crittografa nuovo)
Cryptographic operations.Decrypt	Privileges > All Privileges > Cryptographic operations > Decrypt (Privilegi > Tutti i privilegi > Operazioni crittografiche > Decrittografa)
Operazioni crittografiche. Migrazione	Privileges > All Privileges > Cryptographic operations > Migrate (Privilegi > Tutti i privilegi > Operazioni crittografiche > Migrazione)
Operazioni crittografiche. Leggi le informazioni KMS	Privileges > All Privileges > Cryptographic operations > Read KMS information (Privilegi > Tutti i privilegi > Operazioni crittografiche > Leggi le informazioni KMS)

Provisioning delle macchine (Citrix Provisioning)

Tutti i privilegi del comando di**provisioning delle macchine (Machine Creation Services)** e i seguenti.

SDK	Interfaccia utente
VirtualMachine.Config.AddRemoveDevice	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Add or remove device (Aggiungi o rimuovi dispositivo)
VirtualMachine.Config.CPUCount	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Change CPU Count (Modifica conteggio CPU)
VirtualMachine.Config.Memory	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Memory (Memoria)
VirtualMachine.Config.Settings	Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Settings (Impostazioni)
VirtualMachine.Provisioning.CloneTemplate	Virtual machine (Macchina virtuale) > Provisioning > Clone template (Clona modello)
VirtualMachine.Provisioning.DeployTemplate	Virtual machine (Macchina virtuale) > Provisioning > Deploy template (Distribuisci modello)
vApp.Export	vApp > Export (Esporta)

> **Nota:**
>
> - Le autorizzazioni per clonare e distribuire un modello sono necessarie per fornire macchine virtuali utilizzando l'installazione guidata di Citrix Virtual Apps and Desktops e la procedura guidata Export Devices tramite la console Citrix Provisioning.
> - `vApp.Export` è necessario per creare cataloghi di macchine MCS utilizzando il profilo macchina.

Ottenere e importare un certificato

Per proteggere le comunicazioni vSphere, Citrix consiglia di utilizzare HTTPS anziché HTTP.

HTTPS richiede certificati digitali. Utilizzare un certificato digitale emesso da un'autorità di certificazione che soddisfi i criteri di sicurezza dell'organizzazione.

Se non è possibile utilizzare un certificato digitale emesso da un'autorità di certificazione, è possibile utilizzare il certificato autofirmato installato da VMware. Utilizzare questo metodo solo se i criteri di protezione dell'organizzazione lo consentono. Aggiungere il certificato VMware vCenter a ciascun Delivery Controller.

1. Aggiungere il nome di dominio completo (FQDN) del computer che esegue vCenter Server al file hosts su tale server, in `%SystemRoot%/WINDOWS/system32/Drivers/etc/`. Questo passaggio è necessario solo se il nome di dominio completo del computer che esegue vCenter Server non è già presente nel sistema dei nomi di dominio.
2. Ottenere il certificato vCenter utilizzando uno dei tre metodi seguenti:

   Dal server vCenter.

   a) Copiare il file rui.crt dal server vCenter in una posizione accessibile sui Delivery Controller.
   b) Sul controller, passare alla posizione del certificato esportato e aprire il file rui.crt.

   Scaricare il certificato utilizzando un browser Web. Se si utilizza Internet Explorer, fare clic con il pulsante destro del mouse su Internet Explorer e scegliere **Esegui come amministratore** per scaricare o installare il certificato.

   a) Aprire il browser Web e stabilire una connessione Web sicura al server vCenter (ad esempio https://server1.domain1.com).
   b) Accettare gli avvisi di sicurezza.
   c) Fare clic sulla barra degli indirizzi che visualizza l'errore del certificato.
   d) Visualizzare il certificato e fare clic sulla scheda Dettagli.
   e) Selezionare **Copy to file and export in .CER format** (Copia su file ed esporta in formato.CER), fornendo un nome quando richiesto.
   f) Salvare il certificato esportato.
   g) Passare alla posizione del certificato esportato e aprire il file .CER.

   Importare direttamente da Internet Explorer in esecuzione come amministratore.

   - Aprire il browser Web e stabilire una connessione Web sicura al server vCenter (ad esempio https://server1.domain1.com).
   - Accettare gli avvisi di sicurezza.
   - Fare clic sulla barra degli indirizzi che visualizza l'errore del certificato.
   - Visualizzare il certificato.

3. Importare il certificato nell'archivio certificati di ciascuno dei controller.

   a) Fare clic sull'opzione **Install certificate**, selezionare **Local Machine**e quindi fare clic su **Next**.
   b) Selezionare **Place all certificates in the following store** (Inserisci tutti i certificati nell'archivio seguente) e quindi fare clic su **Browse** (Sfoglia). Selezionare **Trusted People** (Persone attendibili), quindi fare clic su **OK**. Fare clic su **Next** e quindi su **Finish**.

   Se si modifica il nome del server vSphere dopo l'installazione, è necessario generare un nuovo certificato autofirmato su tale server prima di importare il nuovo certificato.

Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine
- Per informazioni specifiche su VMware, vedere Creare un catalogo di VMware

Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

Connessione al cloud VMware e alle soluzioni dei partner

January 7, 2024

Dopo aver configurato il cluster Azure VMware Solution (AVS), Google Cloud VMware Engine e il cloud VMware su AWS, creare le connessioni. Vedere Connessione a VMware per creare connessioni.

Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine
- Per informazioni specifiche su VMware, vedere Creare un catalogo di VMware

Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

Creare cataloghi di macchine

April 4, 2024

> **Importante:**
>
> A partire da Citrix Virtual Apps and Desktops 7 2006, se la distribuzione corrente utilizza una delle seguenti tecnologie, è possibile aggiornare la distribuzione alla versione corrente solo dopo aver rimosso gli elementi del ciclo di vita (EOL) che utilizzano tali tecnologie.

- Personal vDisks (PvDs)
- AppDisks
- Tipi di host cloud pubblici: Citrix CloudPlatform, Microsoft Azure Classic

Per ulteriori informazioni, vedere Rimuovere PVD, AppDisk e host non supportati.

Nota:

È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Se si desidera utilizzare connessioni a host cloud pubblici per la distribuzione, è necessaria la licenza Hybrid Rights per completare la nuova installazione o l'aggiornamento alla versione corrente.

Quando il programma di installazione rileva una o più tecnologie o connessioni host non supportate senza la licenza Hybrid Rights, l'aggiornamento viene sospeso o interrotto. Viene visualizzato un messaggio esplicativo. I registri del programma di installazione ne contengono i dettagli. Per ulteriori informazioni, vedere Aggiornare una distribuzione.

Introduzione

Le raccolte di macchine fisiche o virtuali vengono gestite in una singola entità denominata catalogo di macchine. Tutte le macchine in un catalogo hanno lo stesso tipo di sistema operativo: sistema operativo multisessione o sistema operativo a sessione singola e macchine Windows o Linux.

Web Studio guida l'utente a creare il primo catalogo di macchine dopo aver creato il sito. Dopo aver creato il primo catalogo, Web Studio guida l'utente per creare il primo gruppo di consegna. In seguito, è possibile modificare il catalogo creato e creare altri cataloghi.

Suggerimento:

L'aggiornamento di una distribuzione esistente abilita la funzionalità MCS (Machine Creation Services) Storage Optimization (MCS I/O) e non è richiesta alcuna configurazione aggiuntiva. Il Virtual Delivery Agent (VDA) e l'aggiornamento DEL Delivery Controller gestiscono l'aggiornamento della funzionalità MCS I/O.

Panoramica

Quando si crea un catalogo di macchine virtuali, è necessario specificare come eseguire il provisioning di tali macchine virtuali. È possibile utilizzare Machine Creation Services (MCS). In alternativa, è possibile utilizzare i propri strumenti per il provisioning delle macchine.

Considerare gli aspetti seguenti:

- MCS supporta un singolo disco di sistema dall'immagine della macchina virtuale. Ignora il resto dei dischi dati collegati a quell'immagine.
- Se si utilizza MCS per il provisioning di macchine virtuali, fornire un'immagine master (o un'istantanea di un'immagine) per creare macchine virtuali identiche nel catalogo. Prima di creare il catalogo, utilizzare innanzitutto gli strumenti per creare e configurare l'immagine master. Questo processo include l'installazione di un Virtual Delivery Agent (VDA) sull'immagine. Quindi creare il catalogo macchine in Web Studio. Selezionare l'immagine (o l'istantanea), specificare il numero di macchine virtuali da creare nel catalogo e configurare ulteriori informazioni.
- Se le macchine sono già disponibili, è comunque necessario creare uno o più cataloghi di macchine per tali macchine.
- Se si crea un catalogo utilizzando direttamente PowerShell SDK, è possibile specificare un modello di hypervisor (**VMTemplates**) anziché un'immagine o un'istantanea.
- L'utilizzo di un modello per il provisioning di un catalogo è considerato una funzionalità sperimentale. Quando si utilizza questo metodo, la preparazione della macchina virtuale potrebbe non riuscire. Di conseguenza, il catalogo non può essere pubblicato utilizzando il modello.

Quando si utilizza MCS o Citrix Provisioning per creare il primo catalogo, si utilizza la connessione host configurata al momento della creazione del sito. In seguito, dopo aver creato il primo catalogo e il primo gruppo di consegna, è possibile modificare le informazioni relative a tale connessione o creare altre connessioni.

Dopo aver completato la creazione guidata del catalogo, vengono eseguiti automaticamente test per verificare che sia configurato correttamente. Al termine dei test, è possibile visualizzarne il resoconto. Eseguire i test in qualsiasi momento da Web Studio.

> **Nota:**
>
> MCS non supporta Windows 10 IoT Core e Windows 10 IoT Enterprise. Per ulteriori informazioni, fare riferimento al sito Microsoft.

Per dettagli tecnici sugli strumenti di Citrix Provisioning, vedere Citrix Virtual Apps and Desktops Image Management.

Controllo licenza Servizi Desktop remoto

Attualmente Web Studio non controlla la presenza di licenze valide per Servizi Desktop remoto Microsoft durante la creazione di un catalogo di macchine che contiene computer con sistema operativo multisessione Windows. Per visualizzare lo stato della licenza di Servizi Desktop remoto Microsoft per un **sistema operativo multisessione** Windows, passare a Citrix Director. Visualizzare lo stato della

licenza Servizi Desktop remoto Microsoft nel pannello **Machine Details** (Dettagli macchina). Questo pannello si trova nella pagina **Dettagli macchina e Dettagli utente** (Machine Details and the User Details). Per ulteriori informazioni, vedere Stato della licenza Servizi Desktop remoto Microsoft.

Registrazione dei VDA

Un VDA deve essere registrato presso un Delivery Controller quando si avviano sessioni mediate. I VDA non registrati possono causare un sottoutilizzo di risorse altrimenti disponibili. Esistono vari motivi per cui un VDA potrebbe non essere registrato, molti dei quali sono risolvibili da un amministratore. Web Studio fornisce informazioni sulla risoluzione dei problemi nella creazione guidata catalogo e dopo che sono stati aggiunti computer da un catalogo a un gruppo di consegna.

Dopo che sono stati aggiunti computer esistenti mediante la procedura guidata, l'elenco dei nomi di account computer indica se ogni computer è adatto per l'aggiunta al catalogo. Passare il mouse sull'icona accanto a ogni macchina per visualizzare un messaggio informativo su quella macchina.

Se il messaggio identifica un computer problematico, rimuovere quel computer o aggiungerlo. Ad esempio, se un messaggio indica che non è stato possibile ottenere informazioni su una macchina, aggiungere comunque la macchina.

Per ulteriori informazioni, vedere:

- CTX136668 per informazioni sulla risoluzione dei problemi di registrazione VDA
- Versioni e livelli funzionali dei VDA
- Metodi di registrazione VDA

Riepilogo della creazione del catalogo MCS

Ecco una breve panoramica delle azioni MCS predefinite dopo che sono state fornite le informazioni nella creazione guidata catalogo.

- Se è stata selezionata un'immagine master (anziché un'istantanea), MCS crea un'istantanea.
- MCS crea una copia completa dell'istantanea e la posiziona in ciascuna posizione di archiviazione definita nella connessione host.
- MCS aggiunge le macchine ad Active Directory, che crea identità univoche.
- MCS crea il numero di macchine virtuali specificato nella procedura guidata, definendo due dischi per ciascuna macchina virtuale. Oltre ai due dischi per macchina virtuale, viene memorizzato anche un master nella stessa posizione di archiviazione. Se sono stati definiti più percorsi di archiviazione, ciascuno di essi ottiene i seguenti tipi di disco:
  - Copia completa dell'istantanea di sola lettura e condivisa tra le macchine virtuali appena create.

- Un disco di identità univoco da 16 MB che conferisce a ciascuna macchina virtuale un'identità univoca. Ogni macchina virtuale ottiene un disco di identità.
- Un disco di differenza univoco per archiviare le scritture effettuate nella macchina virtuale. Questo disco è sottoposto a thin provisioning (se supportato dall'archiviazione host) e aumenta fino alle dimensioni massime dell'immagine master, se necessario. Ogni macchina virtuale ottiene un disco di differenza. Il disco di differenza contiene le modifiche apportate durante le sessioni. È permanente per i desktop dedicati. Per i desktop in pool, viene eliminato e ne viene creato uno nuovo dopo ogni riavvio tramite il Delivery Controller.

In alternativa, durante la creazione di macchine virtuali per la distribuzione di desktop statici, è possibile specificare (nella pagina **Machines** della creazione guidata catalogo) duplicati di macchine virtuali spesse (copia completa). I cloni completi non richiedono la conservazione dell'immagine master in ogni archivio dati. Ogni macchina virtuale dispone di un proprio file.

Considerazioni sull'archiviazione MCS

Ci sono molti fattori da valutare quando si scelgono le soluzioni di archiviazione, le configurazioni e le capacità per MCS. Le seguenti informazioni forniscono considerazioni appropriate per la capacità di archiviazione:

Considerazioni sulla capacità:

- Dischi

  I dischi Delta o Differencing (Diff) occupano la maggior quantità di spazio nella maggior parte delle distribuzioni MCS per ogni macchina virtuale. Ogni macchina virtuale creata da MCS viene fornita con almeno 2 dischi al momento della creazione.

  - Disk0= Diff Disk: contiene il sistema operativo quando viene copiato dall'immagine di base principale.
  - Disk1 = Disco di identità: 16 MB - contiene i dati di Active Directory per ogni macchina virtuale.

  Mano mano che il prodotto si evolve, potrebbe essere necessario aggiungere altri dischi per soddisfare determinati casi d'uso e il consumo di funzionalità. Ad esempio:

  - MCS Storage Optimization crea un disco in stile cache di scrittura per ogni macchina virtuale.
  - MCS ha aggiunto la possibilità di utilizzare cloni completi invece dello scenario del disco Delta descritto nella sezione precedente.

  Anche le funzionalità dell'hypervisor potrebbero essere considerate. Ad esempio:

  - Citrix Hypervisor IntelliCache crea un disco di lettura sull'archiviazione locale per ogni Citrix Hypervisor. Questa opzione salva su IOPS rispetto all'immagine master che potrebbe essere contenuta nella posizione di archiviazione condivisa.

- Sovraccarico Hypervisor

  I diversi hypervisor utilizzano file specifici che creano un sovraccarico per le macchine virtuali. Gli hypervisor utilizzano l'archiviazione anche per la gestione e le operazioni di registrazione generali. Calcolare lo spazio per includere il sovraccarico per:

  - File di registro
  - File specifici dell'hypervisor. Ad esempio:
    * VMware aggiunge altri file alla cartella di **VM storage**. Vedere le best practice di VMware.
    * Calcola i requisiti di dimensioni totali delle macchine virtuali. Si consideri una macchina virtuale contenente 20 GB per il disco virtuale, 16 GB per il file di scambio e 100 MB per i file di registro, con un consumo totale di 36,1 GB.
  - Snapshot per XenServer; Snapshot per VMware.

- Sovraccarico del processo

  La creazione di un catalogo, l'aggiunta di un computer e l'aggiornamento di un catalogo hanno implicazioni di archiviazione uniche nel loro genere. Ad esempio:

  - La creazione iniziale del catalogo richiede la copia del disco di base da copiare in ogni posizione di archiviazione.
    * È inoltre necessario creare temporaneamente una macchina virtuale di preparazione.
  - L'aggiunta di una macchina a un catalogo non richiede la copia del disco di base in ciascuna posizione di archiviazione. La creazione del catalogo varia in base alle funzioni selezionate.
  - Aggiornare il catalogo per creare un disco di base aggiuntivo su ogni posizione di archiviazione. Gli aggiornamenti del catalogo presentano anche un picco di archiviazione temporaneo in cui ogni macchina virtuale del catalogo dispone di 2 dischi Diff per un certo periodo di tempo.

Altre considerazioni:

- **Dimensionamento RAM:** influisce sulle dimensioni di alcuni file e dischi dell'hypervisor, quali i dischi di ottimizzazione I/O, la cache di scrittura e i file istantanea.
- **Thin/Thick provisioning:** l'archiviazione NFS è preferita grazie alle funzionalità di thin provisioning.

Ottimizzazione dell'archiviazione MCS (Machine Creation Services)

Con la funzione di ottimizzazione dell'archiviazione MCS (Machine Creation Services), denominata MCS I/O:

- Il contenitore della cache di scrittura è *basato su file*, la stessa funzionalità che si trova in Citrix Provisioning. Ad esempio, il nome del file della cache di scrittura di Citrix Provisioning è `D:\vdiskdif.vhdx` e il nome del file della cache di scrittura I/O MCS è `D:\mcsdif.vhdx`.
- Si ottengono miglioramenti diagnostici includendo il supporto di un file di dettagli arresto anomalo di Windows scritto sul disco della cache di scrittura.
- MCS I/O conserva la tecnologia *cache nella RAM con overflow sul disco rigido* per fornire la soluzione ottimale di cache di scrittura multi-livello. Questa funzionalità consente all'amministratore di ottenere un equilibrio fra il costo in ciascun livello, ciascuna RAM e ciascun disco e le prestazioni per soddisfare le aspettative del carico di lavoro desiderato.

L'aggiornamento del metodo della cache di scrittura da *basato su disco* a *basato su file* richiede le seguenti modifiche:

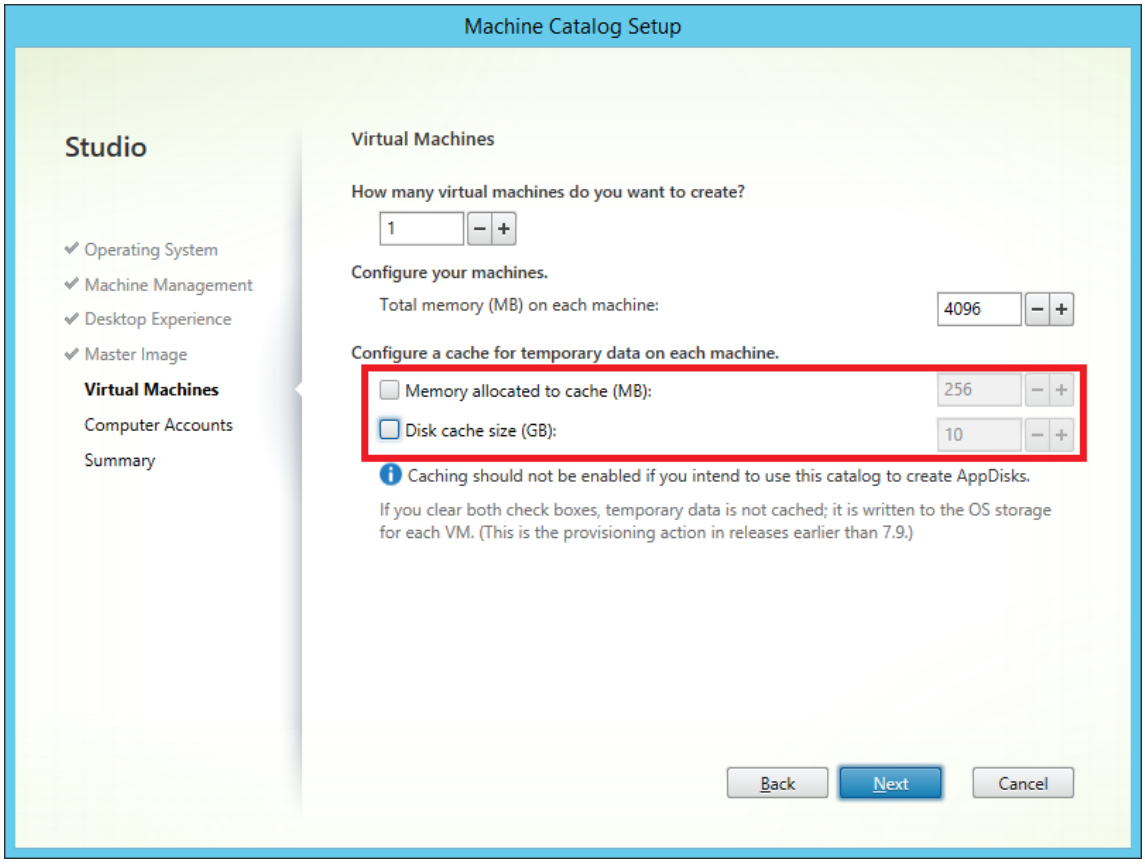
1. MCS I/O non supporta più la cache solo RAM. Specificare una dimensione del disco in Web Studio durante la creazione del catalogo macchine.
2. Il disco della cache di scrittura della macchina virtuale viene creato e formattato automaticamente al primo avvio di una macchina virtuale. Una volta che la macchina virtuale è attivata, il file della cache di scrittura `mcsdif.vhdx` viene scritto nel volume formattato `MCSWCDisk`.
3. Il file di paging viene reindirizzato al volume `MCSWCDisk` formattato. Di conseguenza, questa dimensione del disco considera la quantità totale di spazio su disco. Include il delta tra la dimensione del disco e il carico di lavoro generato più la dimensione del file di paging. Questo è in genere associato alle dimensioni della RAM della macchina virtuale.

Attivare gli aggiornamenti per l'ottimizzazione dell'archiviazione MCS Per abilitare la funzionalità di ottimizzazione dell'archiviazione I/O MCS, aggiornare il Delivery Controller e il VDA alla versione più recente di Citrix Virtual Apps and Desktops.

> **Nota:**
>
> Se si aggiorna una distribuzione esistente che ha MCS I/O abilitato, non è richiesta alcuna configurazione aggiuntiva. L'aggiornamento del VDA e del Delivery Controller gestisce l'aggiornamento di MCS I/O.

Quando si attiva l'aggiornamento dell'ottimizzazione dell'archiviazione MCS, considerare quanto segue:

- Quando si crea un catalogo di macchine, l'amministratore può configurare la RAM e le dimensioni del disco.



- L'aggiornamento di un catalogo di macchine esistente in una nuova istantanea di macchina virtuale contenente un VDA configurato per la versione 1903 determina il seguente comportamento: la nuova istantanea continua a utilizzare l'impostazione MCS I/O del catalogo esistente per la RAM e la dimensione del disco. Il disco non formattato esistente viene formattato.

> **Importante:**
>
> L'ottimizzazione dell'archiviazione MCS è stata modificata con Citrix Virtual Apps and Desktops versione 1903. Questa versione supporta la tecnologia di cache di scrittura basata su file, fornendo prestazioni e stabilità migliori. La nuova funzionalità fornita da MCS I/O potrebbe richiedere un requisito di archiviazione della cache di scrittura più elevato rispetto alle precedenti versioni di Citrix Virtual Apps and Desktops. Citrix consiglia di rivalutare le dimensioni del disco per assicurarsi che disponga di spazio sufficiente per il flusso di lavoro allocato e dimensioni extra per il file di paging. La dimensione del file di paging è in genere correlata alla quantità di RAM di sistema. Se le dimensioni del disco di catalogo esistenti non sono sufficienti, creare un catalogo di macchine e allocare un disco di cache di scrittura più grande.

Assegnare una lettera di unità specifica al disco di cache write-back MCS I/O

È possibile assegnare una lettera di unità specifica al disco della cache di scrittura I/O MCS. Questa implementazione consente di evitare conflitti tra la lettera di unità di qualsiasi applicazione utilizzata e la lettera di unità del disco di cache write-back I/O MCS. Per fare ciò, utilizzare i comandi PowerShell. Gli hypervisor supportati sono Azure, GCP, VMware, SCVMM e Citrix Hypervisor.

> **Nota:**
>
> Questa funzionalità richiede VDA versione 2305 o successiva.

Limitazioni

- Applicabile solo al sistema operativo Windows
- Lettera di unità applicabile per il disco della cache di scrittura: da `E` a `Z`
- Non applicabile quando il disco temporaneo di Azure viene usato come disco di cache di write-back
- Applicabile solo quando si crea un nuovo catalogo di macchine

Assegnare una lettera di unità al disco della cache write-back

Per assegnare una lettera di unità al disco della cache write-back:

1. Aprire la finestra di **PowerShell**.
2. Eseguire `asnp citrix*`.
3. Creare un pool di identità se non è già stato creato.
4. Creare uno schema di provisioning utilizzando il comando `New-ProvScheme` con la proprietà `WriteBackCacheDriveLetter`. Ad esempio:

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "<name>" `
-IdentityPoolName $schemeName `
-ProvisioningSchemeName $schemeName `
-InitialBatchSizeHint 1 `
-UseWriteBackCache -WriteBackCacheDiskSize 127 -
   WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
-MasterImageVM "XDHyp:\HostingUnits<name>\image.folder\abcd-
   resources.resourcegroup\
   MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa145ec77.
   manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\name\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\abcd-resources.resourcegroup
    \abcd-resources-vnet.virtualprivatecloud\default.network" }
```



```
10    `
11 -ServiceOffering "XDHyp:\HostingUnits\<name>\serviceoffering.
      folder\Standard_D2s_v5.serviceoffering" `
12 -CustomProperties '<CustomProperties xmlns="http://schemas.citrix.
      com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
13 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
      true" />
14 <Property xsi:type="StringProperty" Name="OsType" Value="Windows"
      />
15 <Property xsi:type="StringProperty" Name="StorageType" Value="
      Premium_LRS"/>
16 <Property xsi:type="StringProperty" Name="PersistWBC" Value="false
      " />
17 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
      false" />
18 <Property xsi:type="StringProperty" Name="PersistVm" Value="false"
       />
19 <Property xsi:type="StringProperty" Name="WBCDiskStorageType"
      Value="Premium_LRS" />
20 <Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
      ="false" />
21 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
      abcd-group1" />
22 <Property xsi:type="StringProperty" Name="LicenseType" Value="
      Windows_Client" />
23 <Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
       />
24 </CustomProperties>'
25 <!--NeedCopy-->
```

5. Completare la creazione del catalogo di macchine. Per ulteriori informazioni, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Preparare un'immagine master

Per informazioni sulla creazione di host di connessioni, vedere Connessioni e risorse.

L'immagine master contiene il sistema operativo, le applicazioni non virtualizzate, il VDA e altro software.

Buono a sapersi:

- Un'immagine master potrebbe anche essere nota come immagine clone, immagine dorata, macchina virtuale di base o immagine di base. I fornitori host utilizzano termini diversi.
- Assicurarsi che l'host disponga di processori, memoria e archiviazione sufficienti per supportare il numero di macchine create.

- Configurare la quantità corretta di spazio su disco rigido necessaria per desktop e applicazioni. Tale valore non può essere modificato in un secondo momento o nel catalogo macchine.
- I cataloghi di macchine Accesso remoto PC non utilizzano immagini master.
- Considerazioni sull'attivazione del servizio di gestione delle chiavi di Microsoft quando si utilizza MCS: se la distribuzione include VDA 7.x con un host XenServer 6.1 o 6.2, vSphere o Microsoft System Center Virtual Machine Manager, non è necessario riattivare manualmente Microsoft Windows o Microsoft Office.

Installare e configurare il seguente software nell'immagine master:

- Strumenti di integrazione per l'hypervisor (ad esempio Citrix VM Tools, Hyper-V Integration Services o strumenti VMware). Se si omette questo passaggio, applicazioni e desktop potrebbero non funzionare correttamente.
- Un VDA. Citrix consiglia di installare la versione più recente per consentire l'accesso alle funzionalità più recenti. La mancata installazione di un VDA nell'immagine master causa l'esito negativo della creazione del catalogo.
- Strumenti di terze parti, se necessario, come software antivirus o agenti di distribuzione software elettronici. Configurare i servizi con impostazioni appropriate per gli utenti e il tipo di computer (ad esempio l'aggiornamento delle funzionalità).
- Applicazioni di terze parti che non si stanno virtualizzando. Citrix consiglia di virtualizzare le applicazioni. La virtualizzazione riduce i costi eliminando la necessità di aggiornare l'immagine master dopo l'aggiunta o la riconfigurazione di un'applicazione. Inoltre, un numero inferiore di applicazioni installate riduce le dimensioni dei dischi rigidi dell'immagine master, risparmiando così sui costi di archiviazione.
- Client App-V con le impostazioni consigliate, se si prevede di pubblicare applicazioni App-V. Il client App-V è disponibile da Microsoft.
- Quando si utilizza MCS, se si localizza Microsoft Windows, installare le impostazioni internazionali e i Language Pack. Durante il provisioning, quando viene creata una copia istantanea, le macchine virtuali di cui viene eseguito il provisioning utilizzano le impostazioni internazionali e i Language Pack installati.

> **Importante:**
>
> Se si utilizza MCS, non eseguire Sysprep sulle immagini master.

Per preparare un'immagine master:

1. Utilizzando lo strumento di gestione dell'hypervisor, creare un'immagine master e quindi installare il sistema operativo, oltre a tutti i service pack e gli aggiornamenti. Specificare il numero di vCPU. È inoltre possibile specificare il valore vCPU se si crea il catalogo macchine utilizzando PowerShell. Non è possibile specificare il numero di vCPU quando si crea un catalogo utilizzando Web Studio. Configurare la quantità di spazio su disco rigido necessaria per desktop e applicazioni. Tale valore non può essere modificato in un secondo momento o nel catalogo.

2. Assicurarsi che il disco rigido sia collegato alla posizione del dispositivo 0. La maggior parte dei modelli di immagini master standard configura questa posizione per impostazione predefinita, ma alcuni modelli personalizzati potrebbero non farlo.
3. Installare e configurare il software di cui sopra nell'immagine master.
4. Se non si utilizza MCS, aggiungere l'immagine master al dominio di cui sono membri le applicazioni e i desktop. Assicurarsi che l'immagine master sia disponibile sull'host in cui vengono create le macchine. Se si utilizza MCS, non è necessario unire l'immagine master a un dominio. Le macchine di cui viene eseguito il provisioning vengono aggiunte al dominio specificato nella creazione guidata catalogo.
5. Citrix consiglia di creare e denominare un'istantanea dell'immagine master. Se si specifica un'immagine master anziché un'istantanea durante la creazione di un catalogo, in Web Studio viene creata un'istantanea. Non è possibile attribuirle un nome.

Attivazione dei contratti multilicenza

MCS supporta l'attivazione dei contratti multilicenza per automatizzare e gestire l'attivazione dei sistemi operativi Windows e di Microsoft Office. I tre modelli supportati da MCS per l'attivazione dei contratti multilicenza sono:

- Key Management Service (KMS)
- Attivazione basata su Active Directory (ADBA)
- Chiave di attivazione multipla (MAK)

È possibile modificare l'impostazione di attivazione dopo aver creato il catalogo delle macchine.

Key Management Service (KMS)

KMS è un servizio leggero che non richiede un sistema dedicato e può essere facilmente ospitato in cohosting su un sistema che fornisce altri servizi. Questa funzionalità è supportata in tutte le versioni di Windows supportate da Citrix. Durante la preparazione delle immagini, MCS esegue il ripristino di Microsoft Windows e Microsoft Office tramite KMS. È possibile saltare il ripristino eseguendo il comando `Set-Provserviceconfigurationdata`. Per ulteriori informazioni sul ripristino di Microsoft Windows e Microsoft Office tramite KMS durante la preparazione delle immagini, vedere MCS (Machine Creation Services): panoramica della preparazione delle immagini e rilevamento di problemi. Per ulteriori informazioni sull'attivazione di KMS, consultare Attivare tramite KMS (Key Management Service).

> **Nota:**

> Tutti i cataloghi delle macchine creati dopo l'esecuzione del comando `Set-Provserviceconfiguration` hanno le stesse impostazioni fornite nel comando.

Attivazione basata su Active Directory (ADBA)

ADBA consente di attivare le macchine tramite le relative connessioni di dominio. Le macchine vengono attivate immediatamente quando entrano a far parte del dominio. Queste macchine rimangono attivate finché rimangono unite al dominio e sono in contatto con il dominio stesso. Questa funzionalità è supportata in tutte le versioni di Windows supportate da Citrix, ad eccezione di Windows Server 2022. Per ulteriori informazioni sull'attivazione basata su Active Directory, vedere Attivazione basata su Active Directory.

Chiave di attivazione multipla (MAK)

MAK è un modo di attivare il volume e autenticare il sistema Windows con l'aiuto del server Microsoft. È necessario acquistare da Microsoft la chiave MAK, a cui è assegnato un numero fisso di conteggi di attivazione. Ogni volta che viene attivato un sistema Windows, il numero di attivazioni si riduce. Esistono due modi per attivare il sistema:

- Attivazione online: se il sistema Windows che si desidera attivare dispone di accesso a Internet, il sistema attiva automaticamente Windows al momento dell'installazione del codice prodotto. Questo processo riduce il numero di attivazioni di 1 per il MAK corrispondente.
- Attivazione offline: se il sistema Windows non è in grado di connettersi a Internet per eseguire l'attivazione online, MCS riceve un ID di conferma e un ID di installazione dal server Microsoft per attivare il sistema Windows. Questa modalità di attivazione è utile per i cataloghi di macchine non persistenti.

Requisiti chiave

- Il Delivery Controller deve avere accesso a Internet.
- Creare un nuovo catalogo se la nuova immagine da aggiornare ha una chiave MAK diversa dall'originale.
- Installare la chiave MAK sull'immagine master. Per i passaggi per installare la chiave MAK su un sistema Windows, vedere Deploy MAK Activation.
- Se non si utilizza la preparazione delle immagini:
  1. Aggiungere il valore DWORD del registro `Manual` in `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation`.
  2. Impostare il valore su 1.

Conteggi delle attivazioni Per visualizzare il numero di attivazioni rimanenti per la chiave MAK o per verificare se una macchina virtuale stia facendo uso di due o più attivazioni, utilizzare lo Strumento di gestione dell'attivazione dei contratti multilicenza (VAMT). Vedere Installare VAMT.

Attivare il sistema Windows utilizzando MAK Per attivare il sistema Windows utilizzando MAK:

1. Installare il codice prodotto sull'immagine principale. Questo passaggio richiede un conteggio delle attivazioni.
2. Creare un catalogo di macchine MCS.
3. Se non si utilizza la preparazione delle immagini:

   a) Aggiungere il valore DWORD del registro `Manual` in`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation`.
   b) Impostare il valore su `1`.

   Questo metodo disabilita l'opzione di attivazione online.
4. Aggiungere macchine virtuali al catalogo delle macchine.
5. Accendere le macchine virtuali.
6. A seconda che si tratti di attivazione online o offline, il sistema Windows viene attivato o meno.

   - Se l'attivazione è online, il sistema Windows viene attivato dopo l'installazione del codice prodotto.
   - Se l'attivazione è offline, MCS comunica con le macchine virtuali fornite per ottenere lo stato di attivazione del sistema Windows. MCS recupera quindi un ID di conferma e un ID installato dal server Microsoft. Questi ID vengono utilizzati per attivare il sistema Windows.

Risoluzione dei problemi Se la VM di cui è stato eseguito il provisioning non viene attivata con la chiave MAK installata, eseguire il comando `Get-ProvVM` o `Get-ProvScheme` in una finestra di PowerShell.

- Il comando `Get-ProvScheme`: vedere il parametro `WindowsActivationType` associato al catalogo di macchine MCS dall'ultima immagine master.
- Il comando `Get-ProvVM`. Vedere i parametri `WindowsActivationType`, `WindowsActivationStat`, `WindowsActivationStatusErrorCode` e `WindowsActivationStatusError`.

È possibile controllare l'errore e verificare i passaggi per risolvere il problema.

Creare un catalogo di macchine utilizzando Web Studio

Prima di creare un catalogo:

- Consultare questa sezione per conoscere le scelte da fare e le informazioni da fornire.
- Assicurarsi di aver creato una connessione all'hypervisor, al servizio cloud o ad altre risorse che ospitano le macchine.
- Se è stata creata un'immagine master per eseguire il provisioning delle macchine, assicurarsi di aver installato un VDA su tale immagine.

Per avviare la procedura guidata di creazione del catalogo:

1. Se questo è il primo catalogo creato, si viene guidati alla selezione corretta (ad esempio "Set up the machines and create machine catalogs to run apps and desktops"[Configura le macchine e crea cataloghi delle macchine per eseguire app e desktop]). Si apre la procedura guidata di creazione del catalogo.
2. Se è già stato creato un catalogo e si desidera crearne un altro, attenersi alla seguente procedura:

    a) Accedere a Web Studio, selezionare **Machine Catalogs** nel riquadro a sinistra, quindi selezionare **Create Machine Catalog** (Crea catalogo macchine) nella barra delle azioni.

    b) Per organizzare i cataloghi utilizzando le cartelle, creare cartelle nella cartella **Machine Catalogs** (Cataloghi delle macchine) predefinita. Per ulteriori informazioni, consultare Creare una cartella del catalogo.

    c) Selezionare la cartella in cui si desidera creare il catalogo, quindi fare clic su **Create Machine Catalog** (Crea catalogo delle macchine). Si apre la procedura guidata di creazione del catalogo.

La procedura guidata comprende i seguenti elementi. Le pagine della procedura guidata visualizzate sono diverse a seconda delle selezioni effettuate.

Sistema operativo

Ciascun catalogo contiene macchine di un solo tipo. Selezionarne uno

- **Multi-session OS:** un catalogo con sistemi operativi multisessione fornisce desktop condivisi ospitati. Le macchine possono eseguire versioni supportate dei sistemi operativi Windows o Linux, ma il catalogo non può contenere entrambi i sistemi operativi (vedere la documentazione di Linux VDA per i dettagli di quel sistema operativo).
- **Single-session OS:** un catalogo con sistemi operativi a sessione singola fornisce desktop VDI che è possibile assegnare a vari utenti diversi.

- **Remote PC Access:** un catalogo Accesso remoto PC consente agli utenti di accedere in remoto ai computer desktop dell'ufficio fisico. Accesso remoto PC non richiede una VPN per garantire la sicurezza.

Gestione macchine

Questa pagina non viene visualizzata quando si creano cataloghi di Accesso remoto PC.

La pagina **Machine Management** (Gestione macchine) indica la modalità di gestione delle macchine e lo strumento utilizzato per distribuirle.

Scegliere se le macchine presenti nel catalogo sono gestite tramite Web Studio.

- L'alimentazione delle macchine è gestita tramite Web Studio, ad esempio nel caso di macchine virtuali o PC blade. Questa opzione è disponibile solo se è già stata configurata una connessione a un host.
- L'alimentazione delle macchine non è gestita tramite Web Studio, ad esempio nel caso di macchine fisiche.

Se è stato indicato che l'alimentazione dei computer è gestita tramite Web Studio, scegliere lo strumento da utilizzare per creare macchine virtuali.

- **Citrix Machine Creation Services (MCS):** utilizza un'immagine master per creare e gestire macchine virtuali. MCS non è disponibile per le macchine fisiche.
- **Other (Altro):** uno strumento che gestisce le macchine che è già presente nel data center. Citrix consiglia di utilizzare Microsoft System Center Configuration Manager o un'altra applicazione di terze parti per garantire che le macchine nel catalogo siano coerenti.

Tipi di desktop (esperienza desktop)

Questa pagina viene visualizzata solo quando si crea un catalogo contenente macchine con sistema operativo a sessione singola.

La pagina **Desktop Experience** determina ciò che si verifica ogni volta che un utente effettua l'accesso. Selezionare una delle seguenti opzioni:

- Gli utenti si connettono a un nuovo desktop (casuale) ogni volta che accedono.
- Gli utenti si connettono allo stesso desktop (statico) ogni volta che accedono.

Immagine master

Questa pagina viene visualizzata solo quando si utilizza MCS per creare macchine virtuali.

Nella pagina **Master image** selezionare la connessione all'host, quindi selezionare l'istantanea o la macchina virtuale creata in precedenza. Se si sta creando il primo catalogo, l'unica connessione disponibile è quella configurata al momento della creazione del sito.

Ricordare:

- Quando si utilizza MCS, non eseguire Sysprep sulle immagini master.
- Se si specifica un'immagine master anziché un'istantanea, Web Studio crea un'istantanea, ma non è possibile assegnarle un nome.

Per abilitare l'utilizzo delle funzionalità più recenti del prodotto, verificare che nell'immagine master sia installata la versione più recente del VDA. Non modificare la selezione VDA minima predefinita. Tuttavia, se è necessario utilizzare una versione di VDA precedente, vedere Versioni e livelli funzionali dei VDA.

Viene visualizzato un messaggio di errore se si seleziona un'istantanea o una macchina virtuale non compatibile con la tecnologia di gestione computer selezionata in precedenza nella procedura guidata.

Macchine

Questa pagina non viene visualizzata quando si creano cataloghi di Accesso remoto PC.

Il titolo di questa pagina dipende da ciò che è stato selezionato nella pagina **Machine Management**: **Machines**, **Virtual Machines** o **VMs and users**.

Quando si utilizza MCS:

- Specificare quante macchine virtuali creare.
- Scegliere la quantità di memoria (in MB) a disposizione di ciascuna macchina virtuale.
- Ogni macchina virtuale creata dispone di un disco rigido. La sua dimensione è impostata nell'immagine master. Non è possibile modificare le dimensioni del disco rigido nel catalogo.
- Se la distribuzione contiene più di una zona, è possibile selezionare una zona per il catalogo.
- Se si creano macchine virtuali desktop statiche, selezionare una modalità di copia della macchina virtuale. Vedere Modalità di copia della macchina virtuale.
- Se si creano macchine virtuali desktop casuali che non utilizzano vDisks, è possibile configurare una cache da utilizzare per i dati temporanei su ciascuna macchina. Vedere Configurare la cache per i dati temporanei.

Quando si utilizzano altri strumenti:

Aggiungere (o importare un elenco di) nomi di account computer Active Directory. È possibile modificare il nome dell'account di Active Directory per una macchina virtuale dopo averla aggiunta/importata. Se nella pagina **Esperienza desktop** sono state specificate macchine statiche, è possibile specificare facoltativamente il nome utente di Active Directory per ogni macchina virtuale aggiunta.

Dopo aver aggiunto o importato i nomi, è possibile utilizzare il pulsante **Remove** per eliminare i nomi dall'elenco, mentre ci si trova ancora in questa pagina.

Quando si utilizzano altri strumenti (ad eccezione di MCS):

Un'icona e una descrizione comando per ogni macchina aggiunta (o importata) aiutano a identificare le macchine che potrebbero non essere idonee a essere aggiunte al catalogo o non essere in grado di registrarsi con un Delivery Controller. Per i dettagli, vedere Versioni e livelli funzionali dei VDA.

Aggiungere i SID durante la creazione di macchine virtuali

È ora possibile aggiungere il parametro `ADAccountSid` per identificare in modo univoco le macchine durante la creazione di nuove macchine virtuali.

A questo scopo:

1. Creare un catalogo con il tipo di identità supportato.
2. Aggiungere macchine al catalogo utilizzando `NewProvVM`. Ad esempio:

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID "
    )  -RunAsynchronously
<!--NeedCopy-->
```

Tuttavia, non è possibile effettuare il provisioning di una macchina con:

- Un account AD che non fa parte del pool di identità del catalogo
- Un account AD che non è in stato disponibile

Modalità di copia della macchina virtuale

La modalità di copia specificata nella pagina **Machines** determina se MCS crea duplicati sottili (copia rapida) o spessi (copia completa) dall'immagine master. (Impostazione predefinita= cloni sottili)

- Usa duplicati a copia veloce per un utilizzo più efficiente dell'archiviazione e una creazione più rapida della macchina.
- Utilizzare duplicati a copia completa per migliorare il supporto del ripristino e della migrazione dei dati, con IOPS potenzialmente ridotti dopo la creazione delle macchine.

Versioni e livelli funzionali dei VDA

Il livello funzionale di un catalogo controlla quali caratteristiche del prodotto sono disponibili per le macchine presenti nel catalogo. L'utilizzo delle funzionalità introdotte nelle nuove versioni dei

prodotti richiede un nuovo VDA. L'impostazione di un livello funzionale rende disponibili tutte le funzionalità introdotte in quella versione (e nelle successive, se il livello funzionale non cambia) per le macchine del catalogo. Tuttavia, le macchine di quel catalogo con una versione VDA precedente non possono registrarsi.

Un menu nella parte inferiore della pagina **Machines** (o **Devices**) consente di selezionare il livello VDA minimo. Questo imposta il livello funzionale minimo del catalogo. Per impostazione predefinita, per le distribuzioni locali viene selezionato il livello funzionale più recente. Se si segue la raccomandazione di Citrix di installare e aggiornare sempre i VDA e i componenti principali alla versione più recente, non è necessario modificare questa selezione. Tuttavia, se è necessario continuare a utilizzare versioni di VDA precedenti, selezionare il valore corretto.

Una versione di Citrix Virtual Apps and Desktops potrebbe non includere una nuova versione di VDA oppure il nuovo VDA non influisce sul livello funzionale. In questi casi, il livello funzionale potrebbe indicare una versione di VDA precedente ai componenti installati o aggiornati. Ad esempio, sebbene la versione 7.17 contenga un VDA 7.17, il livello funzionale predefinito ("7.9 o successivo") rimane il più attuale. Pertanto, dopo aver installato o aggiornato i componenti da 7.9-7.16 a 7.17, non è necessario modificare il livello funzionale predefinito. L'articolo Novità di ciascuna versione indica qualsiasi modifica del livello funzionale predefinito.

Il livello funzionale selezionato influisce sull'elenco delle macchine al di sopra di esso. Nell'elenco, una descrizione comando accanto a ciascuna voce indica se il VDA della macchina è compatibile con il catalogo a tale livello funzionale.

I messaggi vengono pubblicati sulla pagina se il VDA installato su ciascuna macchina non raggiunge o supera il livello minimo di funzionalità selezionato. È possibile continuare a seguire la procedura guidata. Queste macchine probabilmente non saranno in grado di registrarsi con un Controller in un secondo momento. In alternativa, è possibile:

- Rimuovere dall'elenco i computer contenenti VDA meno recenti, aggiornare i loro VDA e quindi aggiungerli nuovamente al catalogo.
- Scegliere un livello funzionale inferiore che impedisca l'accesso alle funzionalità più recenti del prodotto.

Viene anche pubblicato un messaggio se un computer non è stato aggiunto al catalogo perché è il tipo di computer sbagliato. Gli esempi includono il tentativo di aggiungere un server a un catalogo con sistemi operativi a sessione singola o l'aggiunta di una macchina con sistema operativo a sessione singola creata originariamente per l'allocazione casuale a un catalogo di macchine statiche.

> **Importante:**
>
> Alla release 1811 è stato aggiunto un livello funzionale supplementare: **1811 (o più recente)**. Tale livello è destinato all'uso con le future funzionalità di Citrix Virtual Apps and Desktops. La selezione **7.9 (o più recente)** rimane l'impostazione predefinita. Tale impostazione predefinita

> ora è valida per tutte le distribuzioni.
>
> Se si seleziona **1811 (o più recente)**, qualsiasi versione di VDA precedente presente nel catalogo non sarà in grado di registrarsi con un Controller. Tuttavia, se il catalogo contiene solo VDA versione 1811 o versioni successive supportate, questi sono tutti idonei per la registrazione. Sono inclusi i cataloghi contenenti VDA configurati per le versioni successive di Citrix Virtual Apps and Desktops, inclusa la versione 1903 e altre versioni 19XX precedenti alla versione corrente.

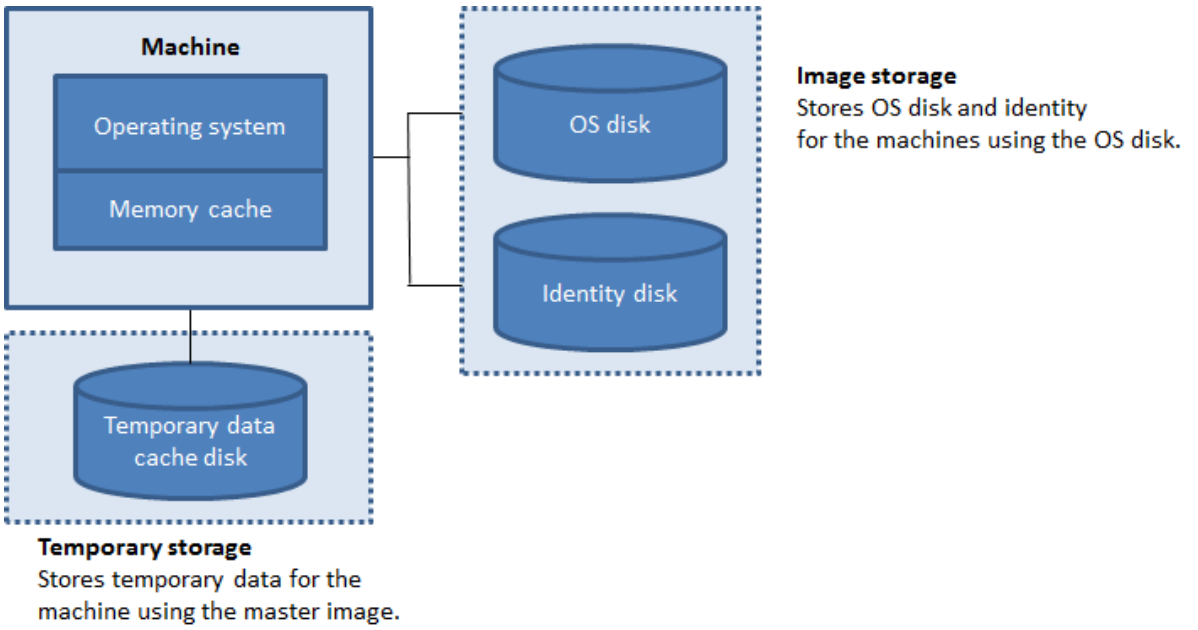
Configurare la cache per i dati temporanei

La memorizzazione nella cache locale dei dati temporanei nella macchina virtuale è facoltativa. È possibile abilitare l'uso della cache dei dati temporanei sul computer quando si utilizza MCS per gestire macchine in pool (non dedicate) in un catalogo. Se il catalogo utilizza una connessione che specifica l'archiviazione per i dati temporanei, è possibile abilitare e configurare le informazioni temporanee della cache dati quando si crea il catalogo.

> **Importante:**
>
> Questa funzione richiede un driver MCS I/O corrente. L'installazione di questo driver è un'opzione disponibile quando si installa o si aggiorna un VDA. Per impostazione predefinita, tale driver non è installato.

Specificare se i dati temporanei dovranno utilizzare l'archiviazione condivisa o locale quando si crea la connessione utilizzata dal catalogo. Per ulteriori informazioni, vedere Connessioni e risorse. Per configurare una cache per i dati temporanei su ciascun computer, è possibile utilizzare le due opzioni seguenti: **Memory allocated to cache (MB)** (Memoria allocata alla cache (MB)) e **Disk cache size (GB)** (Dimensione cache disco (GB)). Per impostazione predefinita, le due opzioni sono deselezionate. Per attivare l'opzione Memory allocated to cache (MB), selezionare la casella di controllo Disk cache size (GB). Se la casella di controllo **Disk cache size** non è selezionata, l'opzione **Memory allocated to cache** è disattivata. A seconda del tipo di connessione, i valori predefiniti per queste opzioni potrebbero differire. Generalmente, i valori predefiniti sono sufficienti per la maggior parte dei casi. Tuttavia, prendere in considerazione lo spazio necessario per:

- File di dati temporanei creati da Windows stesso, incluso il file di paging di Windows.
- Dati del profilo utente.
- Dati ShareFile sincronizzati con le sessioni degli utenti.
- Dati che potrebbero essere creati o copiati da un utente di sessione o da qualsiasi applicazione che gli utenti potrebbero installare all'interno della sessione.



Per configurare una cache per i dati temporanei su ciascun computer, tenere presente i tre scenari seguenti:

- Se non si seleziona la casella di controllo Disk cache size e la casella di controllo Memory allocated to cache, i dati temporanei non vengono memorizzati nella cache. Vengono scritti direttamente sul disco di differenza (situato nella posizione di archiviazione del sistema operativo) per ciascuna macchina virtuale (questa è l'azione di provisioning nelle versioni 7.8 e precedenti).
- Se si seleziona la casella di controllo Disk cache size e non si seleziona la casella di controllo Memory allocated to cache, i dati temporanei vengono scritti direttamente sul disco cache utilizzando una quantità minima di cache di memoria.
- Se si selezionano le caselle di controllo Disk cache size e Memory allocated to cache, i dati temporanei vengono inizialmente scritti nella cache di memoria. Quando la cache di memoria raggiunge il limite configurato (il valore di Memory allocated to cache), i dati meno recenti vengono spostati sul disco temporaneo della cache dei dati.

> **Importante:**
>
> - Se la cache del disco esaurisce lo spazio, la sessione dell'utente diventa inutilizzabile.
> - Questa funzione non è disponibile quando si utilizza una connessione host Nutanix.
> - Non è possibile modificare i valori della cache in un catalogo di computer dopo la creazione del computer.
>
> **Nota:**
>
> - La cache di memoria fa parte della quantità totale di memoria disponibile su ogni computer. Pertanto, se si attiva l'opzione Memory allocated to cache, è consigliabile aumentare la

> quantità totale di memoria su ogni computer.
> - La modifica dell'opzione Disk cache size (Dimensione della cache del disco) rispetto al valore predefinito può influire sulle prestazioni. La dimensione deve corrispondere ai requisiti dell'utente e al carico posto sulla macchina.

NIC

Questa pagina non viene visualizzata quando si creano cataloghi di Accesso remoto PC.

Se si prevede di utilizzare più schede NIC della pagina **Network Interface Cards**, associare una rete virtuale a ciascuna scheda. Ad esempio, è possibile assegnare una scheda per accedere a una rete protetta specifica e un'altra scheda per accedere a una rete utilizzata più comunemente. È inoltre possibile aggiungere o rimuovere schede di interfaccia di rete da questa pagina.

Account macchina

Questa pagina viene visualizzata solo quando si creano cataloghi di Accesso remoto PC.

Nella pagina **Machine Accounts** specificare gli account computer di Active Directory o le unità organizzative (OU) da aggiungere che corrispondono a utenti o gruppi di utenti. Non utilizzare una barra (/) in un nome di unità organizzativa.

Quando si aggiungono unità organizzative, è possibile effettuare le seguenti operazioni se il dominio non è visualizzato nell'elenco:

- Cercarlo usando una corrispondenza esatta.
- Sfogliare tutti i domini per trovarlo.

È possibile scegliere una connessione con gestione dell'alimentazione configurata in precedenza o scegliere di non utilizzare la gestione dell'alimentazione. Se si desidera utilizzare la gestione dell'alimentazione, ma non è stata ancora configurata una connessione adeguata, è possibile crearla in un secondo momento e quindi modificare il catalogo del computer per aggiornare le impostazioni di gestione dell'alimentazione.

Identità macchina

Questa pagina viene visualizzata solo quando si utilizza MCS per creare macchine virtuali.

Ogni macchina del catalogo deve avere un'identità unica. Questa pagina consente di configurare le identità per le macchine del catalogo. Le macchine vengono unite all'identità dopo il provisioning. Non è possibile modificare il tipo di identità dopo aver creato il catalogo.

Di seguito è riportato un flusso di lavoro generale per configurare le impostazioni in questa pagina:

1. Selezionare un'identità dall'elenco.
2. Indicare se creare account o utilizzare quelli esistenti e la posizione (dominio) per tali account.

È possibile selezionare una delle seguenti opzioni:

- **On-premises Active Directory** (Active Directory locale). Macchine di proprietà di un'organizzazione e che hanno effettuato l'accesso con un account Active Directory appartenente a tale organizzazione. Esistono in locale.
- **Unito ad Azure Active Directory ibrido**. Macchine di proprietà di un'organizzazione che hanno effettuato l'accesso con un account Active Directory Domain Services appartenente a tale organizzazione. Esistono nel cloud e on-premise. Per informazioni su requisiti, limitazioni e considerazioni, vedere Macchine aggiunte ad Azure Active Directory ibrido.

  > **Nota:**
  >
  > – Prima di poter utilizzare macchine aggiunte ad Azure Active Directory ibrido, assicurarsi che l'ambiente Azure soddisfi i prerequisiti. Vedere https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains.
  > – Questa opzione richiede che l'immagine master soddisfi i prerequisiti del sistema operativo. Per ulteriori informazioni, vedere la documentazione Microsoft: https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid.

> **Importante:**
>
> - Se si seleziona **On-premises Active Directory** (Active Directory on-premise) o **Hybrid Azure Active Directory joined** (Macchine aggiunte ad Azure Active Directory ibrido) come tipo di identità, ogni macchina del catalogo deve disporre di un account computer Active Directory corrispondente.

Se si creano account, è necessario disporre dell'autorizzazione per creare account computer nell'unità organizzativa in cui risiedono le macchine. Ogni macchina del catalogo deve avere un nome univoco. Specificare lo schema di denominazione degli account per le macchine che si desidera creare. Per ulteriori informazioni, vedere Schema di denominazione degli account delle macchine.

> **Nota:**
>
> Assicurarsi che i nomi delle unità organizzative non utilizzino barre (/).

Se si utilizzano account esistenti, selezionare gli account oppure fare clic su **Import** (Importa) e specificare un file .csv contenente i nomi degli account. Il contenuto del file importato deve essere nel formato seguente:

- [ADComputerAccount] ADcomputeraccountname.domain

Assicurarsi che ci siano account sufficienti per tutte le macchine che si stanno aggiungendo. L'interfaccia di Web Studio gestisce questi account. Pertanto, consentire all'interfaccia di reimpostare le password per tutti gli account o specificare la password dell'account, che deve essere la stessa per tutti gli account.

Per i cataloghi contenenti macchine fisiche o esistenti, selezionare o importare account esistenti e assegnare ciascuna macchina sia a un account computer Active Directory che a un account utente.

Schema di denominazione degli account delle macchine

Ogni macchina in un catalogo deve avere un nome univoco. È necessario specificare uno schema di denominazione degli account delle macchine quando si crea un catalogo. Utilizzare caratteri jolly (cancelletti) come segnaposto per numeri o lettere sequenziali che appaiono nel nome.

Quando si specifica uno schema di denominazione, tenere presente le seguenti regole:

- Lo schema di denominazione deve contenere almeno un carattere jolly. È necessario mettere insieme tutti i caratteri jolly.
- L'intero nome, compresi i caratteri jolly, deve contenere almeno 2 ma non più di 15 caratteri. Deve includere almeno un carattere non numerico e un carattere # (carattere jolly).
- Il nome non deve includere spazi o uno dei seguenti caratteri: `,~!@'$%^&.(){} [ \/*?"<>|=+[];:_".`.
- Il nome non può terminare con un trattino (-).

Inoltre, lasciare spazio sufficiente per l'espansione quando si specifica lo schema di denominazione. Si consideri questo esempio: se si creano 1.000 account macchina con lo schema «veryverylong#», l'ultimo nome account creato (veryverylong1000) contiene 16 caratteri. Pertanto, lo schema di denominazione comporterà uno o più nomi di macchine che superano il massimo di 15 caratteri.

È possibile indicare se i valori sequenziali sono numeri (0-9) o lettere (A-Z):

- **0-9**. Se l'opzione è selezionata, i caratteri jolly specificati vengono risolti in numeri sequenziali.

  > **Nota:**
  >
  > Se è presente un solo carattere jolly (#), i nomi degli account iniziano con 1. Se ce ne sono due, i nomi degli account iniziano con 01. Se ce ne sono tre, i nomi degli account iniziano con 001 e così via.

- **A-Z**. Se l'opzione è selezionata, i caratteri jolly specificati vengono risolti in lettere sequenziali.

Ad esempio, uno schema di denominazione PC-Sales-## (in cui l'opzione **0-9** è selezionata) genera account denominati PC-Sales-01, PC-Sales-02, PC-Sales-03 e così via.

Facoltativamente, è possibile specificare con cosa iniziano i nomi degli account.

- Se si seleziona **0-9**, gli account vengono denominati in sequenza, a partire dai numeri specificati. Immettere una o più cifre, a seconda del numero di caratteri jolly utilizzati nel campo precedente. Ad esempio, se si utilizzano due caratteri jolly, immettere due o più cifre.
- Se si seleziona **A-Z**, gli account vengono denominati in sequenza, a partire dalle lettere specificate. Immettere una o più lettere, a seconda del numero di caratteri jolly utilizzati nel campo precedente. Ad esempio, se si utilizzano due caratteri jolly, immettere due o più lettere.

Credenziali di dominio

Selezionare **Enter credentials** (Immetti credenziali) e immettere le credenziali di un amministratore con l'autorizzazione a eseguire operazioni sull'account nel dominio Active Directory di destinazione.

Utilizzare l'opzione **Check name** (Controlla nome) per verificare se il nome utente è valido o univoco. L'opzione è utile, ad esempio, quando:

- Lo stesso nome utente esiste in più domini. Viene richiesto di selezionare l'utente desiderato.
- Non si ricorda il nome del dominio. È possibile immettere il nome utente senza specificare il nome del dominio. Se il controllo viene superato, il nome del dominio viene popolato automaticamente.

> **Nota:**
>
> Se il tipo di identità selezionato in **Machine Identities** (Identità macchine) è **Hybrid Azure Active Directory joined** (Macchine aggiunte ad Azure Active Directory ibrido), le credenziali immesse devono aver ottenuto l'autorizzazione `Write userCertificate`.

Riepilogo, nome e descrizione

Nella pagina **Summary** controllare le impostazioni specificate. Immettere un nome e una descrizione per il catalogo. Queste informazioni vengono visualizzate in Web Studio.

Al termine, fare clic su **Finish** per avviare la creazione del catalogo.
Al termine, selezionare **Finish** (Fine) per avviare la creazione del catalogo.

In **Machine Catalogs** (Cataloghi delle macchine), il nuovo catalogo viene visualizzato con una barra di avanzamento in linea.

Per visualizzare i dettagli dell'avanzamento della creazione:

1. Passare il mouse sul catalogo delle macchine.
2. Nella descrizione comando visualizzata, fare clic su **View details** (Visualizza dettagli).

   Viene visualizzato un grafico di avanzamento dettagliato in cui è possibile visualizzare quanto segue:

- Cronologia dei passaggi
- Avanzamento e tempo di esecuzione del passaggio corrente
- Passaggi rimanenti

Sincronizzazione dell'ora MCS

La sincronizzazione dell'ora è determinata dall'immagine master e dal tipo di catalogo aggiunto a identità di macchine. È possibile ottenere il seguente metodo di sincronizzazione dell'ora in base all'immagine principale e al catalogo:

Immagine master	Catalogo	Metodo di sincronizzazione temporale risultante
NDJ	AD o Azure AD ibrido	Per impostazione predefinita, NT5DS. È possibile disattivare la modifica da parte di MCS delle impostazioni di sincronizzazione dell'ora utilizzando le impostazioni del registro nell'immagine master.
NDJ	NDJ o Azure AD	Uguale all'impostazione originale di sincronizzazione dell'ora
AD o Azure AD ibrido	AD o Azure AD ibrido	Uguale all'impostazione originale di sincronizzazione dell'ora
Azure AD	Azure AD	Uguale all'impostazione originale di sincronizzazione dell'ora

> **Nota:**
>
> La sincronizzazione dell'ora originale è controllata dalla seguente impostazione del registro e non può essere modificata:
>
> - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config
>
> Valore: MaxAllowedPhaseOffset, MaxNegPhaseCorrection, and MaxPosPhaseCorrection
>
> - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters
>
> Valore: Tipo

Per impedire a MCS di modificare l'impostazione di sincronizzazione dell'ora, stabilire il valore della seguente impostazione del registro nell'immagine master:

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- Nome: TimeSyncMethodKeep
- Tipo: DWORD
- 0 (oppure il valore di TimeSyncMethodKeep non è configurato): non mantiene l'impostazione originale di sincronizzazione dell'ora.
- 1: mantiene l'impostazione originale di sincronizzazione dell'ora e i valori dei parametri predefiniti.

Considerazione importante sull'impostazione di proprietà personalizzate

Le proprietà personalizzate devono essere impostate correttamente su `New-ProvScheme` e `Set-ProvScheme` negli ambienti GCP e Azure. Se si specificano proprietà o proprietà personalizzate non esistenti, viene visualizzato il seguente messaggio di errore e i comandi non vengono eseguiti.

- In Azure: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`
- In GCP: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`

Risoluzione dei problemi

> **Importante:**
>
> Dopo aver creato il catalogo macchine utilizzando Web Studio, non è più possibile utilizzare il comando PowerShell `Get-ProvTask` per recuperare le attività associate alla creazione del catalogo macchine. Questa restrizione è dovuta al fatto che Web Studio elimina tali attività dopo la creazione del catalogo di macchine indipendentemente dalla riuscita o meno della creazione del catalogo.

Citrix consiglia di raccogliere i registri per aiutare il team di supporto a fornire soluzioni. Quando si utilizza Citrix Provisioning, attenersi alla seguente procedura per generare i file di registro:

1. Nell'immagine master creare la seguente chiave del Registro di sistema con il valore 1 (come valore DWORD (32 bit)): `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`.
2. Arrestare l'immagine master e creare un'istantanea.

3. Nel Delivery Controller, eseguire il seguente comando PowerShell: `Set-ProvServiceConfigurationD -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
4. Creare un catalogo basato su tale istantanea.
5. Quando la macchina virtuale di preparazione viene creata nell'hypervisor, eseguire l'accesso ed estrarre i seguenti file dalla directory principale di C:\: Image-prep.log e PvsVmAgentLog.txt.
6. Spegnere la macchina; a quel punto viene segnalato l'errore.
7. Per riattivare l'arresto automatico dei computer di preparazione delle immagini, eseguire il seguente comando PowerShell: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`.

Problemi di preparazione delle immagini

Poiché MCS crea molte macchine da una singola immagine, vengono eseguiti alcuni passaggi per garantire che tutte le macchine siano uniche e correttamente concesse in licenza. La preparazione delle immagini fa parte del processo di creazione del catalogo. Questa preparazione assicura che tutte le macchine di chi è stato effettuato il provisioning dispongano di indirizzi IP univoci e che si annuncino correttamente al server KMS come istanze univoche. All'interno di MCS, la preparazione dell'immagine avviene dopo aver selezionato l'istantanea dell'immagine master. Ne viene eseguita una copia per consentire al catalogo di isolarsi dalla macchina selezionata. Viene creata una macchina virtuale di *preparazione*, basata sulla macchina virtuale originale, ma con la connessione di rete disconnessa. La disconnessione della connessione di rete previene eventuali conflitti con altre macchine, garantendo nel contempo che la macchina virtuale preparata sia collegata solo al disco appena copiato.

Alla macchina virtuale preparata viene collegato un piccolo disco di *istruzioni*, contenente i passaggi necessari per eseguire la preparazione dell'immagine. Questa macchina virtuale preparata si avvia e ha inizio il processo di preparazione dell'immagine. La preparazione delle immagini include i seguenti processi:

- Abilitare DHCP. L'abilitazione di DHCP garantisce che le macchine di cui viene effettuato il provisioning non causino conflitti di indirizzo IP. DHCP è abilitato su tutte le schede di rete.
- Riattivazione del servizio di gestione delle chiavi (KMS) di Microsoft Windows. La riattivazione del servizio di gestione delle chiavi garantisce che Microsoft Windows sia correttamente concesso in licenza. Il sistema operativo riattivato viene richiamato in modo che venga segnalato correttamente come nuova istanza al server licenze KMS.
- Riattivazione del servizio di gestione delle chiavi di Microsoft Office (se è installato Microsoft Office). La riattivazione di Microsoft Office garantisce che qualsiasi versione di Microsoft Office (2010+) sia registrata correttamente nel server del servizio di gestione delle chiavi. Una volta

richiamato il riattivazione di Microsoft Office, viene segnalato come nuova istanza al server licenze KMS.

> **Suggerimento:**
>
> Al termine del processo di preparazione dell'immagine, viene ottenuto il disco di istruzioni dall'hypervisor. L'hypervisor contiene le informazioni raccolte dal processo di preparazione delle immagini.

Ci sono vari motivi per cui la fase di preparazione dell'immagine può non riuscire. Viene visualizzato un messaggio di errore simile al seguente: Image Preparation Office Rearm Failed.

Questi errori sono discussi di seguito.

Abilitare DHCP Questi casi di errore sono causati da schede di rete che non supportano indirizzi IP statici. Ad esempio, versioni precedenti delle schede di rete Dell SonicWall. L'operazione non è riuscita perché una scheda SonicWall è una scheda di rete firewall, quindi l'impostazione della scheda su DHCP non ha senso in quanto supporta solo DHCP. Questo problema è stato risolto nelle versioni successive di Citrix Virtual Apps and Desktops. Tuttavia, se viene osservato in altri tipi di schede di rete, deve essere segnalato a Citrix tramite i forum o il contatto di supporto.

> **Nota:**
>
> L'impostazione di PowerShell riportata negli esempi seguenti viene applicata al sito Citrix Virtual Apps and Desktops, pertanto influisce su tutti i nuovi cataloghi e gli aggiornamenti delle immagini eseguiti nei cataloghi esistenti.

Se si verifica questo problema con altre schede di rete, è possibile risolverlo eseguendo un comando PowerShell sul Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value EnableDHCP
```

Riattivare Microsoft Office Esistono vari errori di riattivazione del servizio di gestione delle chiavi che possono verificarsi durante la fase di riattivazione di Microsoft Office. I principali errori sono:

- Alcuni runtime di Microsoft Office, ad esempio **Access Runtime**, possono richiamare la riattivazione di Office, causando l'errore.
- Non è installata una versione del servizio di gestione delle chiavi di Microsoft Office.
- Numero di riattivazioni superato.

Se l'errore è un falso positivo, è possibile risolverlo eseguendo sul Delivery Controller il seguente comando PowerShell:


```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OfficeRearm
```

Riattivare Microsoft Windows Durante la fase di riavvio di Microsoft Windows possono verificarsi vari errori del servizio di gestione delle chiavi. I principali errori sono:

- La versione di Windows installata non viene attivata tramite il servizio di gestione delle chiavi. Ad esempio, utilizza una chiave di attivazione multipla (MAK).
- Numero di riattivazioni superato.

Se la versione di Microsoft Windows è dotata della licenza corretta, è possibile annullare il riavvio del sistema operativo eseguendo sul Delivery Controller il seguente comando PowerShell:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OsRearm
```

Istanze di operazione non riuscita La macchina per la preparazione dell'immagine non è collegata alla rete come da progetto, quindi a volte la fase di preparazione dell'immagine può solo segnalare la mancata riuscita dell'operazione. Un esempio di questo tipo di errore è simile a: Preparation of the Master VM Image failed (Preparazione dell'immagine della macchina virtuale principale non riuscita). Assicurarsi che nell'immagine selezionata sia installato un sistema operativo supportato (ad esempio Windows 7) e che sia installata la versione corretta del VDA (7.0 o successiva).

I motivi principali per la mancata riuscita sono:

Virtual Delivery Agent (VDA) non è installato o è installato un VDA versione 5.x Se sull'immagine master non è installato il VDA 7.x, la preparazione dell'immagine scade dopo 20 minuti e segnala l'errore di cui sopra. Questo perché nell'immagine master non è installato alcun software per eseguire la fase di preparazione dell'immagine e segnalare la riuscita o la mancata riuscita. Per risolvere il problema, assicurarsi che sull'istantanea selezionata come immagine master sia installato il VDA (versione minima 7).

Criterio `DISKPART SAN` L'intera fase di preparazione dell'immagine può fallire a causa del criterio `DISKPART SAN` impostato sull'immagine master. Se non è impostato per portare online il disco di istruzioni per la preparazione delle immagini, la macchina viene arrestata e la preparazione delle immagini segnala un errore dopo 20 minuti. Per controllare questo sull'immagine master eseguire i seguenti comandi:

```
1 C:>; Diskpart.exe
2 DISKPART>; San
3 <!--NeedCopy-->
```


Con questo comando viene restituito il criterio corrente. Se non è *Online All*, modificarlo eseguendo il comando seguente:

```
DISKPART>; San policy=OnlineAll
```

Arrestare l'immagine master, creare un'istantanea di quella macchina e utilizzarla come immagine MCS di base.

Se la preparazione dell'immagine non riesce per un altro motivo Se la preparazione dell'immagine non riesce e non vi è alcun motivo chiaro di errore, è possibile ignorare il processo di preparazione dell'immagine durante la creazione di un catalogo MCS. Tuttavia, ignorare questo processo può causare problemi con le licenze del servizio di gestione delle chiavi e le reti (DHCP) sul sito. Utilizzare il seguente comando PowerShell:

```
1 Set-ProvServiceConfigurationData -Name
     ImageManagementPrep_DoImagePreparation -Value $false
2 <!--NeedCopy-->
```

Quando possibile, raccogliere i registri per il team di supporto Citrix o segnalare il problema a Citrix tramite i forum o tramite il contatto di supporto. Per raccogliere i registri:

1. Nell'immagine master creare la seguente chiave del Registro di sistema con il valore 1 (come "valore DWORD (32 bit)"): `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`.
2. Arrestare l'immagine master e creare un'istantanea. Sul Delivery Controller, avviare PowerShell, con gli snap-in Citrix PowerShell caricati ed eseguire `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
3. Creare un catalogo basato su tale istantanea.
4. Quando sull'hypervisor viene creata la macchina virtuale di preparazione, effettuare l'accesso ed estrarre dalla radice di C::

```
1 Image-prep.log
2 PvsVmAgentLog.txt
3 <!--NeedCopy-->
```

Arrestare la macchina. A questo punto segnalare l'errore.

Eseguire dal seguente comando PowerShell per riattivare lo spegnimento automatico delle macchine di preparazione delle immagini:

```
Remove-ProvServiceConfigurationData -Name
ImageManagementPrep_NoAutoShutdown
```


Passaggi successivi

Per informazioni sulla creazione di cataloghi di servizi cloud specifici, vedere:

- Creare un catalogo di AWS
- Creare un catalogo di Citrix Hypervisor
- Creare un catalogo di Google Cloud Platform
- Creare un catalogo di Microsoft Azure
- Creare un catalogo di Microsoft System Center Virtual Machine Manager
- Creare un catalogo di Nutanix
- Creare un catalogo di VMware

Se questo è il primo catalogo creato, Web Studio guida l'utente a creare gruppi di consegna.

Per rivedere l'intero processo di configurazione, vedere Installazione e configurazione.

Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Creare cataloghi di diversi tipi di aggiunta
- Gestire i cataloghi di macchine

Creare un catalogo di AWS

January 7, 2024

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le informazioni che seguono riguardano i dettagli specifici degli ambienti di virtualizzazione AWS.

> **Nota:**
>
> Prima di creare un catalogo di AWS, è necessario completare la creazione di una connessione ad AWS. Vedere Connessione ad AWS.

Impostazioni di rete durante la preparazione dell'immagine

Durante la preparazione dell'immagine, viene creata una macchina virtuale (VM) di preparazione basata sulla macchina virtuale originale. Questa macchina virtuale di preparazione è disconnessa dalla rete. Per disconnettere la rete dalla macchina virtuale di preparazione, viene creato un gruppo di sicurezza di rete per negare tutto il traffico in entrata e in uscita. Questo gruppo di sicurezza di

rete persiste e viene riutilizzato. Il nome del gruppo di sicurezza di rete è `Citrix.XenDesktop.IsolationGroup-GUID`, dove il GUID viene generato casualmente.

Configurare la tenancy AWS

AWS offre le seguenti opzioni di tenancy:

- Tenacy condivisa (il tipo predefinito): più istanze di Amazon EC2 di clienti diversi potrebbero risiedere sullo stesso componente hardware fisico.
- Tenancy dedicata: le istanze di EC2 vengono eseguite solo su hardware con altre istanze distribuite. Gli altri clienti non utilizzano lo stesso hardware.

È possibile utilizzare MCS per eseguire il provisioning di host AWS dedicati utilizzando PowerShell.

Configurare la tenancy dell'host AWS dedicato utilizzando PowerShell

È possibile creare un catalogo di macchine con tenancy host definita tramite PowerShell.

Un host dedicato Amazon [EC2] è un server fisico con capacità di istanza [EC2] completamente dedicata, che consente di utilizzare licenze software esistenti per socket o per macchina virtuale.

Gli host dedicati hanno un utilizzo preimpostato in base al tipo di istanza. Ad esempio, un singolo host dedicato allocato di tipi di istanza C4 Large è limitato all'esecuzione di 16 istanze. Per ulteriori informazioni, consultare il sito di AWS.

I requisiti per il provisioning sugli host AWS includono:

- Un'immagine BYOL (Bring Your Own License) importata (AMI). Con host dedicati, utilizzare e gestire le licenze esistenti.
- Un'allocazione di host dedicati con un utilizzo sufficiente per soddisfare le richieste di provisioning.
- abilitare il **posizionamento automatico**.

Per eseguire il provisioning su un host dedicato in AWS utilizzando PowerShell, utilizzare il cmdlet **New-ProvScheme** con il parametro `TenancyType` impostato su *Host*.

Per ulteriori informazioni, consultare la documentazione per gli sviluppatori Citrix.

Acquisire la proprietà dell'istanza AWS

Quando si crea un catalogo per il provisioning di macchine utilizzando Machine Creation Services (MCS) in AWS, si seleziona un'AMI per rappresentare l'immagine master/golden di quel catalogo. Da tale AMI, MCS utilizza una snapshot del disco. Nelle versioni precedenti, se si voleva avere ruoli o

tag sulle macchine si utilizzava la console AWS per impostarli individualmente. Questa funzionalità è abilitata per impostazione predefinita.

> **Suggerimento:**
>
> Per utilizzare l'acquisizione delle proprietà delle istanze AWS, è necessario disporre di una macchina virtuale associata all'AMI.

Per migliorare questo processo, **MCS legge** le proprietà dall'istanza da cui è stata presa l'AMI e applica il ruolo di Identity Access Management (IAM) e i tag della macchina alle macchine di cui è stato eseguito il provisioning per un determinato catalogo. Quando si utilizza questa funzione facoltativa, il processo di creazione del catalogo trova l'istanza dell'origine AMI selezionata che legge un insieme limitato di proprietà. Queste proprietà vengono quindi archiviate in un modello di avvio AWS, utilizzato per il provisioning di macchine per quel catalogo. Qualsiasi macchina nel catalogo eredita le proprietà dell'istanza acquisita.

Le proprietà acquisite includono:

- Ruoli IAM: applicati alle istanze di cui è stato eseguito il provisioning.
- Tag: applicati alle istanze di cui è stato eseguito il provisioning, il relativo disco e le NIC. Questi tag vengono applicati alle risorse Citrix transitorie, tra cui: bucket e oggetti S3, risorse di volume e di lavoro, AMI, snapshot e modelli di avvio.

> **Suggerimento:**
>
> L'etichettatura delle risorse Citrix transitorie è facoltativa ed è configurabile utilizzando la proprietà personalizzata `AwsOperationalResourcesTagging`.

Acquisire la proprietà dell'istanza AWS

È possibile utilizzare questa funzionalità specificando una proprietà personalizzata, `AwsCaptureInstancePro`, durante la creazione di uno schema di provisioning per una connessione di hosting AWS:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"
...<standard provscheme parameters
```

Per ulteriori informazioni, consultare la documentazione per gli sviluppatori Citrix.

> **Nota:**
>
> `AwsCaptureInstanceProperties` è obsoleto.

Applicare tag a una risorsa operativa AWS

Quando si crea un catalogo per il provisioning delle macchine in AWS utilizzando MCS, è possibile controllare se applicare il ruolo IAM e le proprietà dei tag a tali macchine. È inoltre possibile controllare

se applicare tag delle macchine alle risorse operative.

Un'Amazon Machine Image (AMI) rappresenta un tipo di appliance virtuale utilizzata per creare una macchina virtuale all'interno dell'ambiente Amazon Cloud, comunemente denominato EC2. È possibile utilizzare un'AMI per distribuire servizi che utilizzano l'ambiente EC2. Quando si crea un catalogo per eseguire il provisioning di macchine utilizzando MCS per AWS, selezionare l'**AMI** che funge da immagine golden per quel catalogo.

> **Importante:**
>
> La creazione di cataloghi mediante l'acquisizione di una proprietà di istanza e di un modello di avvio è necessaria per utilizzare la codifica delle risorse operative.

Per creare un catalogo di AWS, è necessario innanzitutto creare un'AMI per l'istanza in cui si desidera collocare l'immagine golden. MCS legge i tag di quell'istanza e li incorpora nel modello di avvio. I tag del modello di avvio vengono quindi applicati a tutte le risorse Citrix create nell'ambiente AWS, tra cui:

- Macchine virtuali
- Dischi delle macchine virtuali
- Interfacce di rete delle macchine virtuali
- Bucket S3
- Oggetti S3
- Modelli di lancio
- AMI

Applicare tag a una risorsa operativa

Per utilizzare PowerShell per etichettare le risorse:

1. Aprire una finestra di PowerShell dall'host DDC.
2. Eseguire il comando `asnp citrix` per caricare i moduli PowerShell specifici di Citrix.

Per etichettare una risorsa per una macchina virtuale di cui è stato eseguito il provisioning, utilizzare la nuova proprietà personalizzata `AwsOperationalResourcesTagging`. La sintassi di questa proprietà è la seguente:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true"...<standard provscheme parameters
>
```

Passaggi successivi

- Se questo è il primo catalogo creato, Web Studio guida l'utente a creare gruppi di consegna

- Per rivedere l'intero processo di configurazione, vedere Installazione e configurazione
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di AWS.

Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Connessione ad AWS
- Creare cataloghi di macchine

Creare un catalogo di Citrix Hypervisor

January 7, 2024

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni coprono i dettagli specifici degli ambienti di virtualizzazione Citrix Hypervisor.

> **Nota:**
>
> Prima di creare un catalogo di Citrix Hypervisor, è necessario completare la creazione di una connessione a Citrix Hypervisor. Vedere Connessione a Citrix Hypervisor.

Creare un catalogo di macchine utilizzando una connessione Citrix Hypervisor

Le macchine compatibili con GPU richiedono un'immagine master dedicata. Queste macchine virtuali richiedono driver di schede video che supportino le GPU. Configurare macchine compatibili con GPU per consentire alla macchina virtuale di operare con software che utilizza la GPU per le operazioni.

1. In XenCenter creare una VM con VGA, reti e vCPU standard.
2. Aggiornare la configurazione della VM per abilitare l'uso della GPU (Passthrough o vGPU).
3. Installare un sistema operativo supportato e abilitare RDP.
4. Installare Citrix VM Tools e driver NVIDIA.
5. Deselezionare la Console di amministrazione Virtual Network Computing (VNC) per ottimizzare le prestazioni, quindi riavviare la macchina virtuale.
6. Viene richiesto di utilizzare RDP. Utilizzando RDP, installare il VDA e riavviare la macchina virtuale.
7. Facoltativamente, creare un'istantanea della macchina virtuale come modello di base per altre immagini master GPU.

8. Utilizzando RDP, installare applicazioni specifiche del cliente che sono configurate in XenCenter e utilizzano le funzionalità GPU.

Limiti

- If a Citrix Virtual Apps and Desktops deployment with its VMs hosted on Citrix Hypervisor 8.2 uses multiple GFS2 SRs in a single MCS catalog, the VMs in the catalog cannot access the VDIs during deployment. Viene segnalato l'errore "VDI is currently in use"(VDI attualmente in uso).
- Citrix Hypervisor non supporta le macchine virtuali cloni completi MCS con SR GFS2.

Per ulteriori informazioni, vedere Vincoli.

Creare un catalogo di macchine utilizzando un profilo macchina

Quando si crea un catalogo per il provisioning delle macchine utilizzando MCS, è possibile utilizzare un profilo macchina per acquisire le proprietà hardware da una macchina virtuale e applicarle alle macchine virtuali di cui è stato appena effettuato il provisioning nel catalogo. Se il parametro `MachineProfile` non viene utilizzato, le proprietà hardware vengono acquisite dalla VM o dalla snapshot dell'immagine master.

> **Nota:**
>
> Attualmente, è possibile utilizzare solo una macchina virtuale come input del profilo macchina.

È possibile configurare in modo esplicito i seguenti parametri perché sovrascrivano i valori dei parametri nell'input del profilo macchina:

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

Per creare un catalogo con un profilo macchina:

1. Aprire la finestra di PowerShell.
2. Eseguire `asnp citrix*`.
3. Creare un pool di identità. Il pool di identità è un contenitore per gli account Active Directory (AD) per le macchine virtuali da creare. Ad esempio:

```
1 New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -
     IdentityPoolName "ExampleIdentityPool" -NamingScheme "abc1-##"
     -NamingSchemeType "Numeric" -Scope @() -ZoneUid "xxxxxxxx"
2 <!--NeedCopy-->
```


4. Creare gli account di computer AD richiesti in Active Directory.

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -
    Force
New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count
    10 -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
    -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
<!--NeedCopy-->
```

5. Eseguire il `New-ProvScheme` comando per creare un catalogo. Ad esempio:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
    -IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
     -CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
</CustomProperties>'
-MasterImageVM "XDHyp:\HostingUnits\ExampleHostingUnit\ExampleVDA.
    vm\ExampleVDA.snapshot" -ProvisioningSchemeName "ExampleCatalog
    " -Scope @() -SecurityGroup @()
-MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfile.vm"
<!--NeedCopy-->
```

6. Registrare lo schema di provisioning come catalogo del broker. Ad esempio:

```
$ConfigZone = Get-ConfigZone | Where-Object {
  $_.Name -eq "xxxxxx"  }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -
    Description "Machine profile catalog" -ProvisioningSchemeId
    fe7df345-244e-4xxxx-xxxxxxxxx -ProvisioningType Mcs -
    SessionSupport MultiSession -PersistUserChanges Discard -
    ZoneUid ($ConfigZone.Uid)
<!--NeedCopy-->
```

7. Aggiungere macchine virtuali al catalogo.

Per aggiornare un catalogo con un nuovo profilo macchina:

1. Eseguire il comando `Set-ProvScheme`. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -
    MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfileVm.vm\ExampleMachineProfileSnapshot.
    snapshot"
<!--NeedCopy-->
```

   Per ulteriori informazioni sul comando Set-ProvScheme, vedere Set-ProvScheme.

> **Nota:**
>
> - Il comando `Set-ProvScheme` in questo caso non modifica il profilo macchina delle VM esistenti nel catalogo. Solo le VM appena create aggiunte al catalogo hanno il nuovo profilo macchina.
> - Non è possibile convertire un catalogo di macchine basato su profili macchina in un catalogo di macchine non basato su profili macchina.

Passaggi successivi

- Se questo è il primo catalogo creato, Web Studio guida l'utente a creare gruppi di consegna
- Per rivedere l'intero processo di configurazione, vedere Installazione e configurazione
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di Citrix Hypervisor

Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Connessione a Citrix Hypervisor
- Creare cataloghi di macchine

Creare un catalogo di Google Cloud Platform

April 4, 2024

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni coprono i dettagli specifici degli ambienti cloud di Google.

> **Nota:**
>
> Prima di creare un catalogo di Google Cloud Platform (GCP), è necessario completare la creazione di una connessione a GCP. Vedere Connessione agli ambienti cloud di Google.

Preparare un'istanza di macchina virtuale master e un disco persistente

> **Suggerimento:**
>
> "Disco persistente"è il termine Google Cloud per il disco virtuale.

Per preparare l'istanza della macchina virtuale master, creare e configurare un'istanza di macchina virtuale con proprietà che corrispondono alla configurazione desiderata per le istanze VDA clonate nel catalogo delle macchine pianificato. La configurazione non si applica solo alle dimensioni e al tipo di istanza. Include anche attributi di istanza come metadati, tag, assegnazioni GPU, tag di rete e proprietà degli account di servizio.

Nell'ambito del processo di mastering, MCS utilizza l'istanza della macchina virtuale master per creare il *modello di istanza* di Google Cloud. Il modello di istanza viene quindi utilizzato per creare le istanze VDA clonate che costituiscono il catalogo delle macchine. Le istanze clonate ereditano le proprietà (ad eccezione delle proprietà del VPC, della subnet e del disco persistente) dell'istanza della macchina virtuale master da cui è stato creato il modello di istanza.

Dopo aver configurato le proprietà dell'istanza della macchina virtuale master in base alle proprie specifiche, avviare l'istanza e quindi preparare il disco persistente per l'istanza.

Si consiglia di creare manualmente una snapshot del disco. Ciò consente di utilizzare una convenzione di denominazione significativa per tenere traccia delle versioni, offre più opzioni per gestire le versioni precedenti dell'immagine master e consente di risparmiare tempo per la creazione del catalogo delle macchine. Se non si crea una snapshot personalizzata, MCS crea un'istantanea temporanea (che viene eliminata al termine del processo di provisioning).

Creare un catalogo di macchine

È possibile creare un catalogo di macchine in due modi:

- Creare un catalogo di macchine utilizzando Web Studio
- Creare un catalogo di macchine usando PowerShell

Creare un catalogo di macchine utilizzando Web Studio

> **Nota:**
>
> Creare le risorse prima di creare un catalogo delle macchine. Utilizzare le convenzioni di denominazione stabilite da Google Cloud durante la configurazione dei cataloghi delle macchine. Per maggiori informazioni, consultare le Linee guida per la denominazione di bucket e oggetti.

Seguire le indicazioni in Creare cataloghi delle macchine. La seguente descrizione vale esclusivamente per i cataloghi di Google Cloud.

1. Accedere a Web Studio e selezionare **Machine Catalogs** nel riquadro a sinistra.
2. Selezionare **Create Machine Catalog** (Crea catalogo delle macchine) nella barra delle azioni.
3. Nella pagina **Operating System** (Sistema operativo), selezionare **Multi-session OS** (Sistema operativo multisessione) e quindi selezionare **Next** (Avanti).

- Citrix Virtual Apps and Desktops supporta anche il sistema operativo a sessione singola.

4. Nella pagina **Machine Management** (Gestione macchine), selezionare le opzioni **Machines that are power managed** (Macchine con gestione dell'alimentazione) e **Citrix Machine Creation Services** (Servizi di creazione macchine Citrix) e fare clic su **Next** (Avanti). Se ci sono più risorse, selezionarne una dal menu.
5. Nella pagina **Master Image** (Immagine master), selezionare una macchina virtuale e il livello funzionale minimo per il catalogo, quindi selezionare **Next** (Avanti). Se si desidera utilizzare la funzionalità single-tenancy, assicurarsi di selezionare un'immagine la cui proprietà del gruppo di nodi sia configurata correttamente. Vedere Abilitare la selezione delle zone.
6. Nella pagina **Storage Types** (Tipi di archiviazione), selezionare il tipo di archiviazione utilizzato per contenere il sistema operativo per questo catalogo delle macchine. Ognuna delle seguenti opzioni di archiviazione ha caratteristiche di prezzo e prestazioni diverse (un disco di identità viene sempre creato utilizzando il disco persistente standard della zona).

   - Disco persistente standard
   - Disco persistente bilanciato
   - Disco persistente SSD

   Per ulteriori informazioni sulle opzioni di archiviazione di Google Cloud, vedere https://cloud.google.com/compute/docs/disks/.
7. Nella pagina **Virtual Machines** (Macchine virtuali), specificare quante macchine virtuali si desidera creare, visualizzare le specifiche dettagliate delle macchine virtuali e quindi selezionare **Next** (Avanti). Se si utilizzano i gruppi di nodi single-tenant per i cataloghi delle macchine, assicurarsi di selezionare **solo** le zone in cui sono disponibili i nodi single-tenant riservati. Vedere Abilitare la selezione delle zone.
8. Nella pagina **Computer Accounts** (Account computer), selezionare un account di Active Directory e quindi selezionare **Next** (Avanti).

   - Se si seleziona **Create new Active Directory accounts** (Crea nuovi account di Active Directory), selezionare un dominio e quindi immettere la sequenza di caratteri che rappresenta lo schema di denominazione per gli account delle macchine virtuali di cui è stato eseguito il provisioning creati in Active Directory. Lo schema di denominazione degli account può contenere da 1 a 64 caratteri e non può contenere spazi vuoti, caratteri non ASCII o caratteri speciali.
   - Se si seleziona **Use existing Active Directory accounts** (Usa account Active Directory esistenti), selezionare **Browse** (Sfoglia) per passare agli account delle macchine di Active Directory esistenti per le macchine selezionate.
9. Nella pagina **Domain Credentials** (Credenziali di dominio), selezionare **Enter credentials** (Immetti le credenziali), digitare il nome utente e la password, selezionare **Save** (Salva), quindi

selezionare **Next** (Avanti).

- La credenziale digitata deve disporre delle autorizzazioni per eseguire le operazioni relative agli account di Active Directory.

10. Nella pagina **Summary** (Riepilogo), confermare le informazioni, specificare un nome per il catalogo e quindi selezionare **Finish** (Fine).

> **Nota:**
>
> Il nome del catalogo può contenere da 1 a 39 caratteri e non può contenere solo spazi vuoti o caratteri `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

Il completamento della creazione del catalogo delle macchine potrebbe richiedere molto tempo. Per verificare che le macchine vengano create nei gruppi di nodi di destinazione, accedere alla console di Google Cloud.

Importare macchine di Google Cloud create manualmente

È possibile *creare una connessione a Google Cloud* e quindi *creare un catalogo contenente macchine Google Cloud*. Quindi, è possibile spegnere e riaccendere manualmente le macchine Google Cloud tramite Citrix Virtual Apps and Desktops. Con questa funzionalità, è possibile:

- Importare macchine Google Cloud con sistema operativo multisessione create manualmente in un catalogo delle macchine di Citrix Virtual Apps and Desktops.
- Rimuovere macchine Google Cloud con sistema operativo multisessione create manualmente da un catalogo Citrix Virtual Apps and Desktops.
- Utilizzare le funzionalità esistenti di gestione dell'alimentazione di Citrix Virtual Apps and Desktops per gestire l'alimentazione delle macchine Google Cloud con sistema operativo multisessione Windows. Ad esempio, impostare un programma di riavvio per tali macchine.

Questa funzionalità non richiede modifiche a un flusso di lavoro di provisioning esistente di Citrix Virtual Apps and Desktops, né la rimozione di alcuna funzionalità esistente. Si consiglia di utilizzare MCS per eseguire il provisioning delle macchine in Web Studio anziché importare le macchine Google Cloud create manualmente.

Cloud privato virtuale condiviso

I cloud privati virtuali (VPC) condivisi comprendono un progetto host, da cui vengono rese disponibili le subnet condivise, e uno o più progetti di servizio che utilizzano la risorsa. I VPC condivisi sono desiderabili per installazioni di grandi dimensioni, perché forniscono controllo, utilizzo e amministrazione centralizzati delle risorse aziendali condivise di Google Cloud. Per ulteriori informazioni, consultare il sito della documentazione di Google.

Con questa funzionalità, Machine Creation Services (MCS) supporta il provisioning e la gestione dei cataloghi delle macchine distribuiti su VPC condivisi. Questo supporto, che dal punto di vista funzionale è equivalente al supporto attualmente fornito nei VPC locali, si differenzia sotto due aspetti:

1. È necessario concedere autorizzazioni aggiuntive all'account di servizio utilizzato per creare la connessione host. Questo processo consente a MCS di accedere e utilizzare le risorse VPC condivise.
2. È necessario creare due regole firewall, una per l'ingresso e una per l'uscita. Queste regole firewall vengono utilizzate durante il processo di mastering delle immagini.

Sono necessarie nuove autorizzazioni

Per la creazione della connessione host è necessario un account di servizio Google Cloud con autorizzazioni specifiche. Queste autorizzazioni aggiuntive devono essere concesse a tutti gli account di servizio utilizzati per creare connessioni host basate su VPC condivisi.

> **Suggerimento:**
>
> Queste autorizzazioni aggiuntive non sono nuove per Citrix Virtual Apps and Desktops. Sono utilizzate per facilitare l'implementazione di VPC locali. Con i VPC condivisi, queste autorizzazioni aggiuntive consentono l'accesso ad altre risorse VPC condivise.

È necessario concedere un massimo di quattro autorizzazioni aggiuntive all'account di servizio associato alla connessione host per supportare i VPC condivisi:

1. **compute.firewalls.list**: questa autorizzazione è obbligatoria. Consente a MCS di recuperare l'elenco delle regole firewall presenti nel VPC condiviso.
2. **compute.networks.list**: questa autorizzazione è obbligatoria. Consente a MCS di identificare le reti VPC condivise disponibili per l'account di servizio.
3. **compute.subnetworks.list**: questa autorizzazione è facoltativa, a seconda di come si utilizzano i VPC. Consente a MCS di identificare le subnet all'interno dei VPC condivisi visibili. Questa autorizzazione è già richiesta quando si utilizzano VPC locali, ma deve essere assegnata anche nel progetto host del VPC condiviso.
4. **compute.subnetworks.use**: questa autorizzazione è facoltativa, a seconda di come si utilizzano i VPC. È necessario utilizzare le risorse di subnet nei cataloghi delle macchine di cui è stato eseguito il provisioning. Questa autorizzazione è già necessaria per l'utilizzo di VPC locali, ma deve essere assegnata anche nel progetto host del VPC condiviso.

Quando si utilizzano queste autorizzazioni, tenere presente che esistono diversi approcci in base al tipo di autorizzazione utilizzato per creare il catalogo delle macchine:

- Autorizzazione a livello di progetto:

  - Consente l'accesso a tutti i VPC condivisi all'interno del progetto host.
  - Richiede che le autorizzazioni 3 e 4 vengano assegnate all'account di servizio.

- Autorizzazione a livello di subnet:

  - Consente l'accesso a subnet specifiche all'interno del VPC condiviso.
  - Le autorizzazioni 3 e 4 sono intrinseche all'assegnazione a livello di subnet e quindi non devono essere assegnate direttamente all'account di servizio.

Selezionare l'approccio più adatto alle esigenze e agli standard di sicurezza della propria azienda.

> **Suggerimento:**
>
> Per ulteriori informazioni sulle differenze tra le autorizzazioni a livello di progetto e di subnet, consultare la documentazione di Google Cloud.

Regole firewall

Durante la preparazione di un catalogo delle macchine, viene preparata un'immagine della macchina che funge da disco di sistema dell'immagine master per il catalogo. Quando si verifica questo processo, il disco viene temporaneamente collegato a una macchina virtuale. Questa macchina virtuale deve essere eseguita in un ambiente isolato che impedisca tutto il traffico di rete in entrata e in uscita. Ciò si ottiene attraverso una coppia di regole firewall "nega tutto", una per il traffico in ingresso e una per il traffico in uscita. Quando si utilizzano i VCP locali di Google Cloud, MCS crea questo firewall nella rete locale e lo applica alla macchina per il mastering. Al termine del mastering, la regola firewall viene rimossa dall'immagine.

Si consiglia di ridurre al minimo il numero di nuove autorizzazioni necessarie per utilizzare i VPC condivisi. I VPC condivisi sono risorse aziendali di livello superiore e in genere dispongono di protocolli di sicurezza più rigidi. Per questo motivo, è necessario creare una coppia di regole firewall nel progetto host sulle risorse VPC condivise, una per l'ingresso e una per l'uscita. Assegnare a tali regole la massima priorità. Applicare un nuovo tag di destinazione a ciascuna di queste regole, utilizzando il valore seguente:

```
citrix-provisioning-quarantine-firewall
```

Quando MCS crea o aggiorna un catalogo delle macchine, cerca le regole del firewall contenenti questo tag di destinazione. Quindi esamina le regole per verificarne la correttezza e le applica alla macchina utilizzata per preparare l'immagine master per il catalogo. Se le regole firewall non vengono trovate o le regole vengono trovate ma non sono corrette (o le relative priorità non sono corrette), viene visualizzato un messaggio simile al seguente:

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules
for VPC <name> in project <project>. "Please ensure you have created
 'deny all'firewall rules with the network tag 'citrix-provisioning-
```



```
quarantine-firewall'and proper priority.""Refer to Citrix Documentation
 for details."
```

Configurazione del VPC condiviso

Prima di aggiungere il VPC condiviso come connessione host in Web Studio, completare i seguenti passaggi per aggiungere account di servizio dal progetto in cui si intende effettuare il provisioning:

1. Creare un ruolo IAM.
2. Aggiungere l'account di servizio utilizzato per creare una connessione host CVAD al ruolo IAM del progetto host del VPC condiviso.
3. Aggiungere l'account di servizio Cloud Build dal progetto di cui si intende eseguire il provisioning al ruolo IAM del progetto host del VPC condiviso.
4. Creare regole firewall.

Creare un ruolo IAM Determinare il livello di accesso del ruolo: *accesso a livello di progetto* o un modello più limitato utilizzando l'*accesso a livello di subnet*.

Accesso a livello di progetto per il ruolo IAM. Per il ruolo IAM a livello di progetto, includere le seguenti autorizzazioni:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

Per creare un ruolo IAM a livello di progetto:

1. Nella console di Google Cloud, andare a **IAM e amministrazione > Ruoli**.
2. Nella pagina **Ruoli**, selezionare **CREA RUOLO**.
3. Nella pagina **Crea ruolo**, specificare il nome del ruolo. Selezionare **AGGIUNGI AUTORIZZAZIONI**.
    a) Nella pagina **Aggiungi autorizzazioni**, aggiungere le autorizzazioni al ruolo, singolarmente. Per aggiungere un'autorizzazione, digitare il nome dell'autorizzazione nel campo **Filtra tabella**. Selezionare l'autorizzazione e quindi selezionare **AGGIUNGI**.
    b) Selezionare **CREA**.

Ruolo IAM a livello di subnet. Questo ruolo omette l'aggiunta delle autorizzazioni `compute.subnetworks.list` e `compute.subnetworks.use` dopo aver selezionato **CREA RUOLO**. Per questo livello di accesso IAM, le autorizzazioni `compute.firewalls.list` e `compute.networks.list` devono essere applicate al nuovo ruolo.

Per creare un ruolo IAM a livello di subnet:

1. Nella console di Google Cloud, andare a **Rete VPC** > **VPC condiviso**. Viene visualizzata la pagina **VPC condiviso**, in cui sono visualizzate le subnet delle reti VPC condivise contenute nel progetto host.
2. Nella pagina **VPC condiviso**, selezionare la subnet a cui si desidera accedere.
3. Nell'angolo in alto a destra, selezionare **AGGIUNGI MEMBRO** per aggiungere un account di servizio.
4. Nella pagina **Aggiungi membri**, completare questi passaggi:
    a) Nel campo **Nuovi membri**, digitare il nome del proprio account di servizio e quindi selezionare l'account di servizio nel menu.
    b) Selezionare il campo **Seleziona un ruolo** e quindi **Utente di rete Compute**.
    c) Selezionare **SALVA**.
5. Nella console di Google Cloud, andare a **IAM e amministrazione** > **Ruoli**.
6. Nella pagina **Ruoli**, selezionare **CREA RUOLO**.
7. Nella pagina **Crea ruolo**, specificare il nome del ruolo. Selezionare **AGGIUNGI AUTORIZZAZIONI**.
    a) Nella pagina **Aggiungi autorizzazioni**, aggiungere le autorizzazioni al ruolo, singolarmente. Per aggiungere un'autorizzazione, digitare il nome dell'autorizzazione nel campo **Filtra tabella**. Selezionare l'autorizzazione, quindi seleziona **AGGIUNGI**.
    b) Selezionare **CREA**.

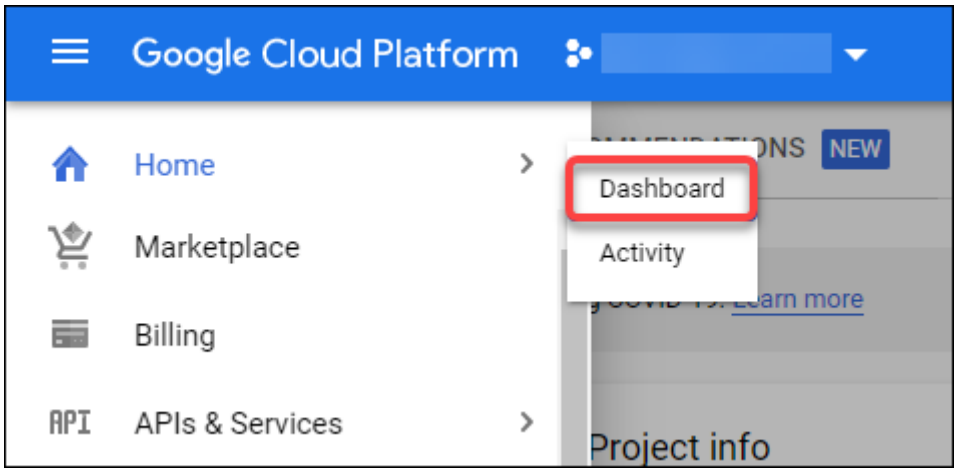
Aggiungere un account di servizio al ruolo IAM del progetto host Dopo aver creato un ruolo IAM, per aggiungere un account di servizio per il progetto host, procedere come segue:

1. Nella console di Google Cloud, accedere al progetto host e quindi a **IAM e amministrazione > IAM**.
2. Nella pagina **IAM**, selezionare **AGGIUNGI** per aggiungere un account di servizio.
3. Nella pagina **Aggiungi membri**:
    a) Nel campo **Nuovi membri**, digitare il nome del proprio account di servizio e quindi selezionare l'account di servizio nel menu.
    b) Selezionare un campo ruolo, digitare il ruolo IAM creato e quindi selezionare il ruolo nel menu.
    c) Selezionare **SALVA**.

L'account di servizio è ora configurato per il progetto host.

Aggiungere l'account del servizio di compilazione cloud al VPC condiviso Ogni sottoscrizione a Google Cloud ha un account di servizio che prende il nome dal numero ID del progetto, seguito da `cloudbuild.gserviceaccount`. Ad esempio: `705794712345@cloudbuild.gserviceaccount`.

È possibile determinare qual è il numero ID del progetto per il proprio progetto selezionando **Home page** e **Dashboard** nella console di Google Cloud:



Trovare il **numero del progetto** sotto l'area **Informazioni sul progetto** dello schermo.

Eseguire i seguenti passaggi per aggiungere l'account del servizio Cloud Build al VPC condiviso:

1. Nella console di Google Cloud, accedere al progetto host e quindi a **IAM e amministrazione** > **IAM**.
2. Nella pagina **Autorizzazioni**, selezionare **AGGIUNGI** per aggiungere un account.
3. Nella pagina **Aggiungi membri**, completare questi passaggi:

    a) Nel campo **Nuovi membri**, digitare il nome dell'account di servizio Cloud Build, quindi selezionare il proprio account di servizio nel menu.
    b) Selezionare il campo **Seleziona un ruolo**, digitare `Computer Network User`, quindi selezionare il ruolo nel menu.
    c) Selezionare **SALVA**.

Creare regole firewall Come parte del processo di mastering, MCS copia l'immagine della macchina selezionata e la utilizza per preparare il disco di sistema dell'immagine master per il catalogo. Durante il processo di mastering, MCS collega il disco a una macchina virtuale temporanea, che in seguito esegue gli script di preparazione. Questa macchina virtuale deve essere eseguita in un ambiente isolato che vieti tutto il traffico di rete in entrata e in uscita. Per creare un ambiente isolato, MCS richiede due regole firewall *"nega tutto"* (una regola di ingresso e una regola di uscita). Pertanto, creare due regole firewall nel *progetto host* come segue:

1. Nella console di Google Cloud, andare al progetto host e quindi a **Rete VPC > Firewall**.
2. Nella pagina **Firewall**, selezionare **CREA REGOLA FIREWALL**.
3. Nella pagina **Crea una regola firewall**, completare quanto segue:

    - **Name**. Digitare un nome per la regola.

- **Rete**. Selezionare la rete VPC condivisa a cui applicare la regola firewall in ingresso.
- **Priorità**. Più piccolo è il valore, maggiore è la priorità della regola. Si consiglia un valore piccolo (ad esempio, 10).
- **Direzione del traffico**. Selezionare **In entrata**.
- **Azione in caso di corrispondenza**. Selezionare **Nega**.
- **Destinazioni**. Utilizzare l'opzione predefinita, **Tag di destinazione specificati**.
- **Tag di destinazione**. Digitare `citrix-provisioning-quarantine-firewall`.
- **Filtro di origine**. Utilizzare l'opzione predefinita, **Intervalli IP**.
- **Intervalli IP di origine**. Digitare un intervallo che corrisponda a tutto il traffico. Digitare `0.0.0.0/0`.
- **Protocolli e porte**. Selezionare **Nega tutto**.

4. Selezionare **CREA** per creare la regola.
5. Ripetere i passaggi da 1 a 4 per creare un'altra regola. Per **Direzione del traffico**, selezionare **In uscita**.

Aggiungere una connessione Aggiungere una connessione agli ambienti cloud di Google. Vedere Aggiungere una connessione.

Abilitare la selezione delle zone

Citrix Virtual Apps and Desktops supporta la selezione delle zone. Con la selezione delle zone, è possibile specificare le zone in cui si desidera creare macchine virtuali. Con la selezione delle zone, gli amministratori possono posizionare nodi single-tenant nelle zone di loro scelta. Per configurare la single-tenancy, è necessario completare quanto segue su Google Cloud:

- Prenotare un nodo single-tenant di Google Cloud
- Creare l'immagine master VDA

Prenotazione di un nodo single-tenant di Google Cloud

Per prenotare un nodo single-tenant, consultare la documentazione di Google Cloud.

> **Importante:**
>
> Un modello di nodo viene utilizzato per indicare le caratteristiche prestazionali del sistema riservato nel gruppo di nodi. Tali caratteristiche includono il numero di vGPU, la quantità di memoria allocata al nodo e il tipo di macchina utilizzato per le macchine create sul nodo. Per ulteriori informazioni, consultare la documentazione di Google Cloud.

Creazione dell'immagine master VDA

Per distribuire correttamente le macchine sul nodo single-tenant, è necessario eseguire ulteriori passaggi durante la creazione di un'immagine master della macchina virtuale. Le istanze delle macchine su Google Cloud hanno una proprietà chiamata *etichette di affinità nodo*. Le istanze utilizzate come immagini master per i cataloghi distribuiti nel nodo single-tenant richiedono un'*etichetta di affinità nodo* che corrisponda al nome del **gruppo di nodi di destinazione**. Per raggiungere questo obiettivo, tenere presente quanto segue:

- Per una nuova istanza, impostare l'etichetta nella console di Google Cloud quando si crea un'istanza. Per informazioni dettagliate, consultare Impostare un'etichetta di affinità nodo durante la creazione di un'istanza.
- Per un'istanza esistente, impostare l'etichetta usando la riga di comando **gcloud**. Per informazioni dettagliate, consultare Impostare un'etichetta di affinità nodo per un'istanza esistente.

> **Nota:**
>
> Se si intende utilizzare la single-tenancy con un VPC condiviso, consultare Cloud privato virtuale condiviso.

Impostare un'etichetta di affinità nodo durante la creazione di un'istanza Per impostare l'etichetta di affinità nodo:

1. Nella console di Google Cloud, andare a **Compute Engine > Istanze VM**.
2. Nella pagina **Istanze VM**, selezionare **Crea istanza**.
3. Nella pagina **Creazione istanza**, digitare o configurare le informazioni richieste e quindi selezionare **Gestione, sicurezza, dischi, networking, single-tenancy** per aprire il pannello delle impostazioni.
4. Nella scheda **Single-tenancy**, selezionare **Sfoglia** per visualizzare i gruppi di nodi disponibili nel progetto corrente. Viene visualizzata la pagina **Nodo single-tenant**, che mostra un elenco dei gruppi di nodi disponibili.
5. Nella pagina **Nodo single-tenant**, selezionare il gruppo di nodi applicabile dall'elenco, quindi selezionare **Seleziona** per tornare alla scheda **Single-tenancy**. Il campo delle etichette di affinità nodo viene compilato con le informazioni selezionate. Questa impostazione garantisce che i cataloghi delle macchine creati dall'istanza vengano distribuiti nel gruppo di nodi selezionato.
6. Selezionare **Crea** per creare l'istanza.

Impostare un'etichetta di affinità nodo per un'istanza esistente Per impostare l'etichetta di affinità nodo:

1. Nella finestra del terminale di Google Cloud Shell, utilizzare il comando *gcloud compute instances* per impostare un'etichetta di affinità nodo. Includere le seguenti informazioni nel comando **gcloud**:

   - **Nome della macchina virtuale**. Ad esempio, utilizzare una macchina virtuale esistente denominata `s*2019-vda-base`.*
   - **Nome del gruppo di nodi**. Utilizzare il nome del gruppo di nodi creato in precedenza. Ad esempio, `mh-sole-tenant-node-group-1`.
   - **La zona in cui risiede l'istanza**. Ad esempio, la macchina virtuale risiede nella zona `*us-east-1b* zone`.

   Ad esempio, digitare il seguente comando nella finestra del terminale:

   - `gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"`

   Per ulteriori informazioni sul comando *gcloud compute instances*, consultare la documentazione di Google Developer Tools all'indirizzo https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling.

2. Passare alla pagina **Dettagli istanza VM** dell'istanza e verificare che il campo **Affinità del nodo** venga compilato con l'etichetta.

Creare un catalogo di macchine Dopo aver impostato l'etichetta di affinità nodo, configurare il catalogo delle macchine.

Chiavi di crittografia gestite dal cliente (CMEK)

È possibile utilizzare le chiavi di crittografia gestite dal cliente (CMEK) per i cataloghi MCS. Quando si utilizza questa funzionalità, si assegna il ruolo `CryptoKey Encrypter/Decrypter` di Google Cloud Key Management Service all'agente del servizio Compute Engine. L'account di Citrix Virtual Apps and Desktops deve disporre delle autorizzazioni corrette nel progetto in cui è memorizzata la chiave. Per ulteriori informazioni, consultare Aiutare a proteggere le risorse utilizzando le chiavi di Cloud KMS.

L'agente del servizio Compute Engine ha il seguente formato: `service-<Project _Number>@compute-system.iam.gserviceaccount.com`. Questo formato è diverso dall'account predefinito del servizio Compute Engine.

> **Nota:**
>
> Questo account del servizio Compute Engine potrebbe non essere visualizzato nella schermata **IAM/Autorizzazioni** di Google Cloud Console. In questi casi, utilizzare il comando `gcloud` come

> descritto in Aiutare a proteggere le risorse utilizzando le chiavi di Cloud KMS.

Assegnare autorizzazioni all'account di Citrix Virtual Apps and Desktops

Le autorizzazioni di Google Cloud KMS possono essere configurate in vari modi. È possibile fornire autorizzazioni KMS a *livello di progetto* o autorizzazioni KMS *a livello di risorsa*. Vedere Autorizzazioni e ruoli per ulteriori informazioni.

Autorizzazioni a livello di progetto Un'opzione è fornire all'account di Citrix Virtual Apps and Desktops autorizzazioni a livello di progetto per esplorare le risorse di Cloud KMS. A tale scopo, creare un ruolo personalizzato e aggiungere le seguenti autorizzazioni:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Assegnare questo ruolo personalizzato all'account di Citrix Virtual Apps and Desktops. Questo consente di sfogliare le chiavi regionali nel progetto pertinente nell'inventario.

Autorizzazioni a livello di risorsa Per l'altra opzione, le autorizzazioni a livello di risorsa, nella console di Google Cloud selezionare la `cryptoKey` utilizzata per il provisioning MCS. Aggiungere l'account di Citrix Virtual Apps and Desktops a un keyring o a una chiave utilizzata per il provisioning del catalogo.

> **Suggerimento:**
>
> Con questa opzione non è possibile sfogliare le chiavi regionali per il progetto nell'inventario perché l'account di Citrix Virtual Apps and Desktops non dispone delle autorizzazioni elenco a livello di progetto per le risorse Cloud KMS. Tuttavia, è comunque possibile eseguire il provisioning di un catalogo utilizzando CMEK specificando l'`cryptoKeyId` nelle proprietà personalizzate `ProvScheme`, come descritto di seguito.

Provisioning con CMEK utilizzando le proprietà personalizzate

Quando si crea lo schema di provisioning tramite PowerShell, specificare una proprietà `CryptoKeyId` in `ProvScheme CustomProperties`. Ad esempio:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
```



```
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="<
        yourCryptoKeyId>" />
</CustomProperties>'
<!--NeedCopy-->
```

L'`cryptoKeyId` deve essere specificato nel seguente formato:

`projectId:location:keyRingName:cryptoKeyName`

Ad esempio, se si desidera utilizzare la chiave `my-example-key` nel keyring `my-example-key-ring` nella regione `us-east1` e nel progetto con ID `my-example-project-1`, le impostazioni personalizzate `ProvScheme` saranno simili a:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
        example-project-1:us-east1:my-example-key-ring:my-example-key"
        />
</CustomProperties>'
<!--NeedCopy-->
```

Tutti i dischi e le immagini di cui è stato eseguito il provisioning tramite MCS relativi a questo schema di provisioning utilizzano questa chiave di crittografia gestita dal cliente.

> **Suggerimento:**
>
> Se si utilizzano le chiavi globali, la posizione delle proprietà del cliente deve indicare `global` e non il nome della **regione**, che nell'esempio precedente è **us-east1**. Ad esempio: `<Property xsi:type="StringProperty"Name="CryptoKeyId"Value="my-example-project-1:global:my-example-key-ring:my-example-key"/>`.

Rotazione delle chiavi gestite dal cliente

Google Cloud non supporta la rotazione delle chiavi su dischi o immagini persistenti esistenti. Una volta eseguito il provisioning di una macchina, questa viene associata alla versione della chiave in uso al momento della creazione. Tuttavia, è possibile creare una nuova versione della chiave e tale nuova chiave viene utilizzata per le macchine o le risorse di cui è stato recentemente eseguito il provisioning create quando un catalogo viene aggiornato con una nuova immagine master.

Considerazioni importanti sui keyring I keyring non possono essere rinominati o eliminati. Inoltre, si potrebbero ricevere addebiti imprevisti quando vengono configurati. Quando si elimina o si rimuove un keyring, Google Cloud visualizza un messaggio di errore:


```
Sorry, you can't delete or rename keys or key rings. We were concerned about the security implications of allowing multiple keys or key versions over time to have the same resource name, so we decided to make names immutable. (And you can't delete them, because we wouldn't be able to do a true deletion--there would still have to be a tombstone tracking that this name had been used and couldn't be reused).
We're aware that this can make things untidy, but we have no immediate plans to change this.
If you want to avoid getting billed for a key or otherwise make it unavailable, you can do so by deleting all the key versions; neither keys nor key rings are billed for, just the active key versions within the keys.
<!--NeedCopy-->
```

> **Suggerimento:**
>
> Per ulteriori informazioni, consultare Modificare o eliminare un keyring dalla console.

Compatibilità dell'accesso uniforme a livello di bucket

Citrix Virtual Apps and Desktops è compatibile con il criterio per il controllo dell'accesso uniforme a livello di bucket in Google Cloud. Questa funzionalità espande l'uso del criterio IAM che concede autorizzazioni a un account di servizio per consentire la manipolazione delle risorse, inclusi i bucket di archiviazione. Grazie al controllo dell'accesso uniforme a livello di bucket, Citrix Virtual Apps and Desktops consente di utilizzare un elenco di controllo degli accessi (ACL) per controllare l'accesso ai bucket di archiviazione o agli oggetti memorizzati in essi. Consultare Accesso uniforme a livello di bucket per informazioni generali sull'accesso uniforme a livello di bucket di Google Cloud. Per informazioni sulla configurazione, vedere Richiedere un accesso uniforme a livello di bucket.

Creare un catalogo di macchine usando PowerShell

Questa sezione descrive in dettaglio come creare cataloghi usando PowerShell:

- Creare un catalogo con un disco cache di write-back persistente
- Migliorare le prestazioni di avvio con MCSIO
- Creare un catalogo di macchine utilizzando un profilo macchina
- Creare un catalogo di macchine con il profilo della macchina come modello di istanza
- Utilizzare PowerShell per creare un catalogo con VM schermate

Creare un catalogo con un disco cache di write-back persistente

Per configurare un catalogo con il disco della cache write-back persistente, utilizzare il parametro PowerShell `New-ProvScheme CustomProperties`.

> **Suggerimento:**
>
> Utilizzare questo parametro PowerShell solo per le connessioni di hosting basate su cloud. Se si desidera eseguire il provisioning di macchine utilizzando un disco di cache write-back persistente per una soluzione locale (ad esempio, Citrix Hypervisor), PowerShell non è necessario perché il disco persiste automaticamente.

Questo parametro supporta una proprietà aggiuntiva, `PersistWBC`, utilizzata per determinare il modo in cui il disco della cache write-back persiste per le macchine di cui è stato eseguito il provisioning con MCS. La proprietà `PersistWBC` viene utilizzata solo quando viene specificato il parametro`UseWriteBackCache` e quando il parametro `WriteBackCacheDiskSize` è impostato per indicare che viene creato un disco.

> **Nota:**
>
> Questo comportamento si applica sia ad Azure che a GCP nei casi in cui il disco della cache write-back MCSIO predefinito viene eliminato e ricreato durante il ciclo di alimentazione. È possibile scegliere di rendere persistente il disco in modo da evitare l'eliminazione e la ri-creazione del disco della cache write-back MCSIO.

L'impostazione della proprietà `PersistWBC` su **`true`** elimina il disco della cache write-back quando l'amministratore di Citrix Virtual Apps and Desktops arresta la macchina dall'interfaccia di gestione.

L'impostazione della proprietà `PersistWBC` su **`false`** elimina il disco della cache write-back quando l'amministratore di Citrix Virtual Apps and Desktops arresta la macchina dall'interfaccia di gestione.

> **Nota:**
>
> Se la proprietà `PersistWBC` viene omessa, il valore predefinito della proprietà è **`false`** e la cache write-back viene eliminata quando la macchina viene arrestata dall'interfaccia di gestione.

Ad esempio, utilizzando il parametro CustomProperties per impostare `PersistWBC` su **`true`**:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```


> **Nota:**
>
> La proprietà `PersistWBC` può essere impostata solo utilizzando il cmdlet PowerShell `New-ProvScheme`. Il tentativo di modificare le `CustomProperties` di uno schema di provisioning dopo la creazione non ha alcun impatto sul catalogo macchine e sulla persistenza del disco della cache write-back quando un computer viene arrestato.

Ad esempio, impostare `New-ProvScheme` perché utilizzi la cache write-back mentre si imposta la proprietà `PersistWBC` su **`true`**:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

Migliorare le prestazioni di avvio con MCSIO

È possibile migliorare le prestazioni di avvio per i dischi gestiti di Azure e GCP quando MCSIO è abilitato. Utilizzare la proprietà personalizzata di PowerShell `PersistOSDisk` nel comando `New-ProvScheme` per configurare questa funzionalità. Le opzioni associate a `New-ProvScheme` includono:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
```



```
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="Resource <!--NeedCopy-->
``````<!--NeedCopy-->
<!--NeedCopy-->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
</CustomProperties>
<!--NeedCopy-->
```

Per abilitare questa funzionalità, impostare la proprietà personalizzata `PersistOSDisk` su **`true`**. Ad esempio:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

### Creare un catalogo di macchine utilizzando un profilo macchina

Quando si crea un catalogo per il provisioning delle macchine utilizzando Machine Creation Services (MCS), è possibile utilizzare un profilo macchina per acquisire le proprietà hardware da una macchina virtuale e applicarle alle macchine virtuali di cui è stato appena effettuato il provisioning nel catalogo. Quando il parametro `MachineProfile` non viene utilizzato, le proprietà hardware vengono

acquisite dalla VM o dalla snapshot dell'immagine master.
Alcune proprietà vengono definite in modo esplicito; ad esempio `StorageType`, `CatalogZones` e `CryptoKeyIs` vengono ignorate dal profilo del computer.

- Per creare un catalogo con un profilo macchina, utilizzare il comando `New-ProvScheme`. Ad esempio, `New-ProvScheme –MachineProfile "path to VM"`. Se non si specifica il parametro `MachineProfile`, le proprietà hardware vengono acquisite dalla VM dell'immagine master.
- Per aggiornare un catalogo con un nuovo profilo macchina, utilizzare il comando `Set-ProvScheme`. Ad esempio, `Set-ProvScheme –MachineProfile "path to new VM"`. Questo comando non modifica il profilo macchina delle VM esistenti nel catalogo. Solo le VM appena create aggiunte al catalogo hanno il nuovo profilo macchina.
- È anche possibile aggiornare l'immagine master, tuttavia, quando si aggiorna l'immagine master e le proprietà hardware non vengono aggiornate. Se si desidera aggiornare le proprietà hardware, è necessario aggiornare il profilo della macchina utilizzando il comando `Set-ProvScheme`. Queste modifiche si applicheranno solo alle nuove macchine del catalogo. Per aggiornare le proprietà hardware di una macchina esistente, è possibile utilizzare il comando `Set-ProvVMUpdateTimeWindow` con i parametri `-StartsNow` e `-DurationInMinutes -1`.

  > **Nota:**
  >
  > - `StartsNow` indica che l'ora di inizio pianificata è l'ora corrente.
  > - `DurationInMinutes` con un numero negativo (ad esempio -1) indica che non vi è alcun limite superiore nella finestra oraria della pianificazione.

### Creare un catalogo di macchine con il profilo della macchina come modello di istanza

È possibile selezionare un modello di istanza GCP come input per il profilo della macchina. I modelli di istanza sono risorse leggere in GCP, quindi sono molto convenienti.

#### Creare un nuovo catalogo di macchine con il profilo della macchina come modello di istanza

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Trovare un modello di istanza nel proprio progetto GCP usando il seguente comando:

```
cd XDHyp:\HostingUnits<HostingUnitName>\instanceTemplates.folder
<!--NeedCopy-->
```

4. Creare un nuovo catalogo di macchine con il profilo della macchina come modello di istanza utilizzando il comando NewProvScheme:

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -
    HostingUnitName <HostingUnitName> -IdentityPoolName <identity
    pool name> -MasterImageVM
XDHyp:\HostingUnits<HostingUnitName> \Base.vm\Base.snapshot -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder\mytemplate.template
<!--NeedCopy-->
```

   Per ulteriori informazioni sul comando New-ProvScheme, vedere https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/.

5. Completare la creazione del catalogo delle macchine utilizzando i comandi PowerShell. Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

#### Modificare il profilo macchine di un catalogo di macchine esistente in modo che diventi un modello di istanza

I passaggi dettagliati per modificare il profilo macchine di un catalogo di macchine esistente in modo che diventi un modello di istanza sono:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire il seguente comando:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder<TemplateName>.template
<!--NeedCopy-->
```

   Per informazioni sul comando Set-ProvScheme, vedere https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/.

### Utilizzare PowerShell per creare un catalogo con VM schermate

È possibile creare un catalogo di macchine MCS con le proprietà delle VM schermate. Una macchina virtuale schermata è rafforzata da una serie di controlli di sicurezza che forniscono l'integrità verificabile delle istanze di Compute Engine, utilizzando funzionalità avanzate di sicurezza della piattaforma quali l'avvio sicuro, un modulo di piattaforma attendibile virtuale, firmware UEFI e monitoraggio dell'integrità.

MCS supporta la creazione del catalogo utilizzando il flusso di lavoro del profilo macchina. Se si utilizza il workflow del profilo macchina, è necessario abilitare le proprietà delle VM schermate di un'istanza di macchina virtuale. È quindi possibile utilizzare questa istanza di macchina virtuale come input del profilo della macchina.

Per creare un catalogo di macchine MCS con macchina virtuale schermata utilizzando il flusso di lavoro del profilo macchina.

1. Abilitare le opzioni delle VM schermate di un'istanza di macchina virtuale nella console di Google Cloud. Vedere Avvio rapido: Abilitare le opzioni delle VM schermate.
2. Creare un catalogo di macchine MCS con il flusso di lavoro del profilo macchina utilizzando l'istanza di VM.
   a) Aprire una finestra di PowerShell.
   b) Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
   c) Creare un pool di identità se non è già stato creato.
   d) Eseguire il comando `New-ProvScheme`. Ad esempio:

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>
-HostingUnitName gcp-hostint-unit
-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    vda.vm
-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    machine.vm
<!--NeedCopy-->
```

3. Completate la creazione del catalogo di macchine.

Per aggiornare il catalogo macchine con un nuovo profilo macchina:

1. Eseguire il comando `Set-ProvScheme`. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>
-MasterImageVM XDHyp:\HostingUnits<hostin-unit>\catalog-vda.vm
-MachineProfile "DHyp:\HostingUnits<hostin-unit>\catalog-machine.
    vm
<!--NeedCopy-->
```

Per applicare la modifica effettuata in `Set-ProvScheme` alle macchine virtuali esistenti, eseguire il comando `Set-ProvVMUpdateTimeWindow`.

1. Eseguire il comando `Set-ProvVMUpdateTimeWindow`. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

2. Riavviare le macchine virtuali.

### Google Cloud Marketplace

È possibile sfogliare e selezionare le immagini offerte da Citrix su **Google Cloud Marketplace** per creare cataloghi di macchine. Attualmente, MCS supporta solo il flusso di lavoro dei profili macchina per questa funzionalità.

Per cercare il prodotto Citrix VDA VM tramite Google Cloud Marketplace, accedere a https://console.cloud.google.com/marketplace.

È possibile utilizzare un'immagine personalizzata o un'immagine Citrix Ready su **Google Cloud Marketplace** per aggiornare l'immagine di un catalogo di macchine.

> **Nota:**
>
> Se il profilo della macchina non contiene informazioni sul tipo di archiviazione, il valore viene derivato da proprietà personalizzate.

Le immagini supportate da Google Cloud Marketplace sono:

- Windows 2019 a sessione singola
- Windows 2019 multisessione
- Ubuntu

Esempio di utilizzo di un'immagine pronta per Citrix come fonte per la creazione di un catalogo di macchine:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \
-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \
-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
   win2019-single-vda-v20220819.publicimage \
-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
<!--NeedCopy-->
```

### Passaggi successivi

- Se questo è il primo catalogo creato, Web Studio guida l'utente a creare gruppi di consegna
- Per rivedere l'intero processo di configurazione, vedere Installazione e configurazione
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di Google Cloud Platform

### Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Connessione agli ambienti cloud di Google
- Creare cataloghi di macchine

# Creare un catalogo di Microsoft Azure

January 10, 2024

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud di Microsoft Azure Resource Manager.

> **Nota:**
>
> Prima di creare un catalogo di Microsoft Azure, è necessario completare la creazione di una connessione a Microsoft Azure. Vedere Connessione a Microsoft Azure.

## Provisioning on demand di Azure

Con il provisioning on demand di Azure, le macchine virtuali vengono create solo quando Citrix Virtual Apps and Desktops avvia un'azione di accensione, dopo il completamento del provisioning.

Quando si utilizza MCS per creare cataloghi delle macchine in Azure Resource Manager, la funzionalità di provisioning on demand di Azure:

- Riduce i costi di archiviazione
- Velocizza la creazione di cataloghi

Quando si crea un catalogo MCS, il portale di Azure visualizza il gruppo di sicurezza di rete, le interfacce di rete, le immagini di base e i dischi di identità nei gruppi di risorse.

Il portale di Azure non mostra una macchina virtuale finché Citrix Virtual Apps and Desktops non avvia un'azione di accensione per tale macchina. Esistono due tipi di macchine con le seguenti differenze:

- Per una macchina in pool, il disco del sistema operativo e la cache write-back esistono solo quando esiste la macchina virtuale. Quando si arresta una macchina in pool nella console, la macchina virtuale non è visibile nel portale di Azure. Si ottiene un notevole risparmio sui costi di archiviazione se si spengono regolarmente le macchine (ad esempio, al di fuori dell'orario di lavoro).
- Per una macchina dedicata, il disco del sistema operativo viene creato la prima volta che la macchina virtuale viene accesa. La macchina virtuale presente nel portale di Azure rimane in archivio fino a quando l'identità della macchina non viene eliminata. Quando si arresta una macchina dedicata nella console, la macchina virtuale è ancora visibile nel portale di Azure.

## Creare un catalogo di macchine

È possibile creare un catalogo di macchine in due modi:

- Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio
- Creare un catalogo di macchine usando PowerShell

### Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio

Un'immagine può essere un disco, una snapshot o una versione immagine di una definizione di immagine all'interno della Raccolta di calcolo di Azure utilizzata per creare le macchine virtuali in un catalogo di macchine. Prima di creare il catalogo delle macchine, creare un'immagine in Azure Resource Manager. Per informazioni generali sulle immagini, vedere Creare cataloghi delle macchine.

Durante la preparazione dell'immagine, viene creata una macchina virtuale di preparazione basata sulla macchina virtuale originale. Questa macchina virtuale di preparazione è disconnessa dalla rete. Per disconnettere la rete dalla macchina virtuale di preparazione, viene creato un gruppo di sicurezza di rete per negare tutto il traffico in entrata e in uscita. Il gruppo di sicurezza di rete viene creato automaticamente una volta per catalogo. Il nome del gruppo di sicurezza di rete è `Citrix-Deny-All-a3pgu-GUID`, dove il GUID viene generato casualmente. Ad esempio, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

Nella procedura guidata di creazione del catalogo delle macchine:

- Le pagine **Machine Type** (Tipo di macchina) e **Machine Management** (Gestione macchina) non contengono informazioni specifiche di Azure. Seguire le linee guida riportate nell'articolo Creare cataloghi di macchine.
- Nella pagina **Master Image** (Immagine master), selezionare un'immagine da utilizzare come immagine mater per tutte le macchine del catalogo. Viene visualizzata la procedura guidata **Select an image** (Seleziona un'immagine).

  1. (Applicabile solo alle connessioni configurate con immagini condivise all'interno di uno stesso tenant o tra tenant diversi) Selezionare un abbonamento in cui risiede l'immagine.
  2. Selezionare un gruppo di risorse.
  3. Passare ad Azure VHD, alla Raccolta di calcolo di Azure o alla versione immagine di Azure. Se necessario, aggiungere una nota per l'immagine selezionata.

  Quando selezionate un'immagine, tenere presente quanto segue:

  - Verificare che sull'immagine sia installato un Citrix VDA.
  - Se si seleziona un disco rigido virtuale collegato a una macchina virtuale, è necessario spegnere la VM prima di procedere al passaggio successivo.

**Nota:**

- La sottoscrizione corrispondente alla connessione (host) che ha creato le macchine nel catalogo è contrassegnata da un punto verde. Le altre sottoscrizioni sono quelle con Raccolta di calcolo di Azure condivisa con quella sottoscrizione. In queste sottoscrizioni vengono mostrate solo le gallerie condivise. Per informazioni su come configurare gli abbonamenti condivisi, vedere Condividere immagini all'interno di un tenant (tra abbonamenti) e Condividere immagini tra tenant.
- L'uso di un profilo macchina con un avvio attendibile quale **Security Type** (Tipo di sicurezza) è obbligatorio quando si seleziona un'immagine o una snapshot con avvio attendibile abilitato. È quindi possibile abilitare o disabilitare SecureBoot e vTPM specificandone i valori nel profilo macchina. L'avvio attendibile non è supportato per la Raccolta immagini condivise. Per informazioni sull'avvio attendibile di Azure, vedere https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.
- È possibile creare uno schema di provisioning utilizzando il disco del sistema operativo temporaneo su Windows con avvio attendibile. Quando si seleziona un'immagine con avvio attendibile, è necessario selezionare un profilo macchina con avvio attendibile abilitato con vTPM. Per creare cataloghi delle macchine utilizzando un disco del sistema operativo temporaneo, vedere Come creare macchine utilizzando dischi del sistema operativo temporanei.
- Quando è in corso la replica dell'immagine, è possibile procedere e selezionare l'immagine come immagine master e completare la configurazione. Tuttavia, il completamento della creazione del catalogo potrebbe richiedere più tempo durante la replica dell'immagine. MCS richiede che la replica venga completata entro un'ora a partire dalla creazione del catalogo. In caso di timeout della replica, la creazione del catalogo non riesce. È possibile verificare lo stato della replica in Azure. Riprovare se la replica è ancora in sospeso o dopo il completamento della replica.
- Quando si seleziona un'immagine master per i cataloghi delle macchine in Azure, MCS identifica il tipo di sistema operativo in base all'immagine master e al profilo macchina selezionati. Se MCS non è in grado di identificarlo, selezionare il tipo di sistema operativo corrispondente all'immagine master.
- È possibile effettuare il provisioning di un catalogo di macchine virtuali Gen2 utilizzando un'immagine Gen2 per migliorare le prestazioni in fase di avvio. Tuttavia, la creazione di un catalogo di macchine Gen2 utilizzando un'immagine Gen1 non è supportata. Allo stesso modo, non è supportata la creazione di un catalogo di macchine Gen1 utilizzando un'immagine Gen2. Inoltre, qualsiasi immagine precedente che non contiene informazioni sulla generazione è un'immagine Gen1.

Scegliere se le VM del catalogo debbano ereditare le configurazioni da un profilo macchina. Per impostazione predefinita, la casella di controllo **Use a machine profile (mandatory for Azure**

**Active Directory)** [Usa un profilo macchina (obbligatoria per Azure Active Directory)] è selezionata. Fare clic su **Select a machine profile** (Seleziona un profilo macchina) per accedere a una VM o a una specifica di modello ARM da un elenco di gruppi di risorse.

Convalidare la specifica del modello ARM per accertarsi che possa essere utilizzata come profilo macchina per creare un catalogo delle macchine. Esistono due modi per convalidare la specifica di modello ARM:

- Dopo aver selezionato la specifica del modello ARM dall'elenco dei gruppi di risorse, fare clic su **Next** (Avanti). Se la specifica del modello ARM contiene errori, vengono visualizzati messaggi di errore.
- Eseguire uno dei seguenti comandi PowerShell:
  * `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  * `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

Alcuni esempi di configurazioni che le macchine virtuali possono ereditare da un profilo macchina includono:

- Networking accelerato
- Diagnostica di avvio
- Memorizzazione nella cache del disco host (relativa ai dischi del sistema operativo e MCSIO)
- Dimensioni della macchina (se non diversamente specificato)
- Tag posizionati sulla macchina virtuale

Dopo aver creato il catalogo, è possibile visualizzare le configurazioni che l'immagine eredita dal profilo della macchina. Nel nodo **Machine Catalogs** (Cataloghi delle macchine), selezionare il catalogo per visualizzare i relativi dettagli nel riquadro inferiore. Quindi, fare clic sulla scheda **Template Properties** (Proprietà modello) per visualizzare le proprietà del profilo della macchina. La sezione **Tags** (Tag) visualizza fino a tre tag. Per visualizzare tutti i tag posizionati sulla macchina virtuale, fare clic su **View all** (Visualizza tutto).

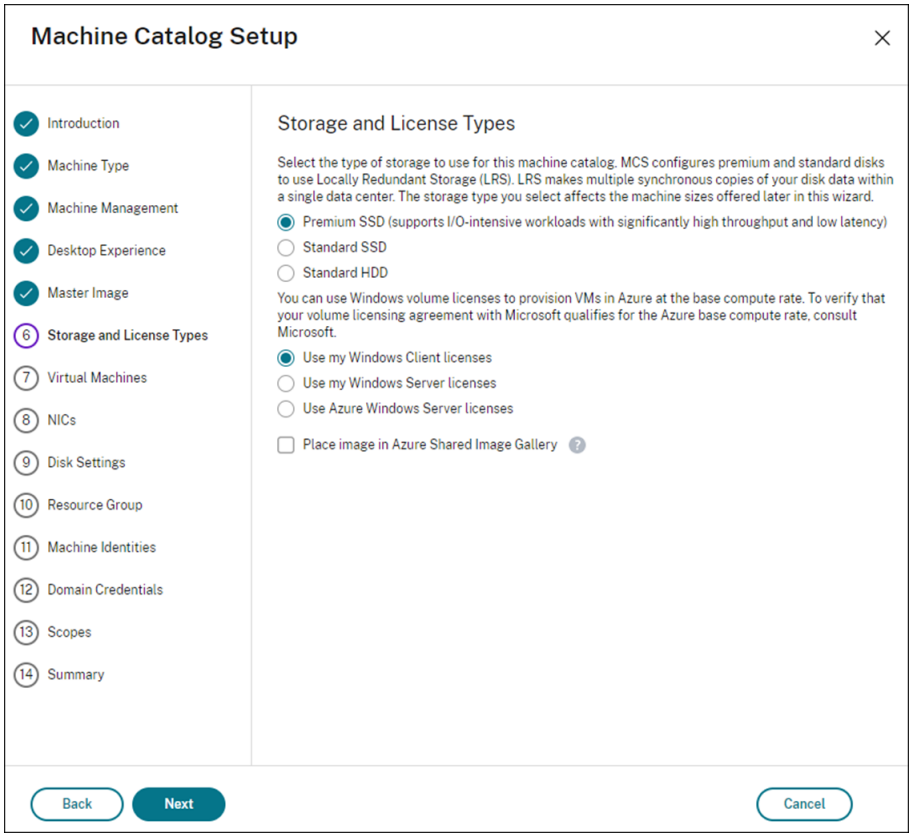
Se si desidera che MCS esegua il provisioning delle macchine virtuali in un host dedicato di Azure, abilitare la casella di controllo **Use a dedicated host group** (Utilizza un gruppo host dedicato) e quindi selezionare un gruppo host dall'elenco. Un gruppo di host è una risorsa che rappresenta una raccolta di host dedicati. Un host dedicato è un servizio che fornisce server fisici che ospitano una o più macchine virtuali. Il server dedicato alla sottoscrizione di Azure non è condiviso con altri sottoscrittori. Quando si utilizza un host dedicato, Azure garantisce che le macchine virtuali siano le uniche macchine in esecuzione su quell'host. Questa funzionalità è adatta per gli scenari in cui è necessario soddisfare i requisiti normativi o di sicurezza interni.

Per ulteriori informazioni sui gruppi di host e sulle considerazioni per il loro utilizzo, vedere Host dedicati di Azure.

> **Importante:**
>
> – Vengono visualizzati solo i gruppi di host per i quali è abilitato il posizionamento automatico di Azure.
> – L'utilizzo di un gruppo host modifica la pagina **Virtual Machines** (Macchine virtuali) mostrata più avanti nella procedura guidata. In questa pagina vengono mostrate solo le dimensioni delle macchine contenute nel gruppo host selezionato. Inoltre, le zone di disponibilità vengono selezionate automaticamente e non sono disponibili per la selezione.

- La pagina **Storage and License Types** (Tipi di archiviazione e licenze) viene visualizzata solo quando si utilizza un'immagine di Azure Resource Manager.




Sono disponibili i seguenti tipi di archiviazione da utilizzare per il catalogo delle macchine:

– **SSD premium**. Offre un'opzione di archiviazione su disco ad alte prestazioni e a bassa latenza adatta per macchine virtuali con carichi di lavoro a uso intensivo di I/O.
– **SSD standard**. Offre un'opzione di archiviazione conveniente adatta a carichi di lavoro che richiedono prestazioni costanti a livelli di IOPS inferiori.

- **HDD standard**. Offre un'opzione di archiviazione su disco affidabile e a basso costo adatta per macchine virtuali che eseguono carichi di lavoro non sensibili alla latenza.
- **Disco del sistema operativo temporaneo di Azure**. Offre un'opzione di archiviazione conveniente che riutilizza il disco locale delle macchine virtuali per ospitare il disco del sistema operativo. In alternativa, è possibile utilizzare PowerShell per creare macchine che utilizzano dischi dei sistemi operativi temporanei. Per ulteriori informazioni, vedere Dischi temporanei di Azure. Tenere presenti le seguenti considerazioni quando si utilizza un disco del sistema operativo temporaneo:
  * Il disco del sistema operativo temporaneo di Azure e l'I/O MCS non possono essere abilitati contemporaneamente.
  * Per aggiornare le macchine che utilizzano dischi dei sistemi operativi temporanei, è necessario selezionare un'immagine la cui dimensione non superi la dimensione del disco della cache o del disco temporaneo della macchina virtuale.
  * Non è possibile utilizzare l'opzione **Retain system disk during power cycles** (Conserva il disco di sistema durante i cicli di alimentazione) disponibile più avanti nella procedura guidata.

> **Nota:**
>
> Il disco di identità viene sempre creato utilizzando SSD standard indipendentemente dal tipo di archiviazione scelto.

Il tipo di archiviazione determina le dimensioni delle macchine disponibili nella pagina **Virtual Machines** (Macchine virtuali) della procedura guidata. MCS configura dischi premium e standard per l'utilizzo dell'archiviazione con ridondanza locale (LRS). LRS esegue più copie sincrone dei dati del disco all'interno di un singolo centro dati. I dischi del sistema operativo temporaneo di Azure utilizzano il disco locale delle macchine virtuali per archiviare il sistema operativo. Per informazioni dettagliate sui tipi di archiviazione di Azure e sulla replica dell'archiviazione, vedere quanto segue:

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/
- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/

Selezionare se utilizzare le licenze Windows o Linux esistenti.

- Licenze Windows: l'utilizzo di licenze Windows insieme a immagini Windows (immagini di supporto o immagini personalizzate della piattaforma Azure) consente di eseguire macchine virtuali Windows in Azure a un costo ridotto. Esistono due tipi di licenze:
  * **Licenza Windows Server**. Consente di utilizzare le licenze Windows Server o Azure Windows Server, consentendo l'utilizzo dei Vantaggi di Azure ibrido. Per i dettagli,

vedere https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. I vantaggi di Azure ibrido riducono il costo di esecuzione delle macchine virtuali in Azure alla tariffa di elaborazione di base, eliminando il costo delle licenze aggiuntive di Windows Server dalla raccolta di Azure.

* **Licenza client Windows**. Consente di trasferire le licenze di Windows 10 e Windows 11 in Azure, consentendo di eseguire macchine virtuali Windows 10 e Windows 11 in Azure senza la necessità di licenze aggiuntive. Per i dettagli, vedere Licenze di accesso client e licenze di gestione.

È possibile verificare che la macchina virtuale di cui è stato eseguito il provisioning stia utilizzando il vantaggio di licenza eseguendo il seguente comando PowerShell: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- Per il tipo di licenza Windows Server, verificare che il tipo di licenza sia **Windows_Server**. Ulteriori istruzioni sono disponibili alla pagina https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.
- Per il tipo di licenza client Windows, verificare che il tipo di licenza sia **Windows_Client**. Ulteriori istruzioni sono disponibili alla pagina https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

In alternativa, è possibile utilizzare l'SDK PowerShell `Get-Provscheme` per eseguire la verifica. Ad esempio: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. Per ulteriori informazioni su questo cmdlet, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

- Licenze Linux: con le licenze Linux BYOS (Bring-Your-Own-Subscription), non è necessario pagare per il software. La tariffa BYOS include solo la tariffa per l'hardware di elaborazione. Esistono due tipi di licenze:

  * **RHEL_BYOS**: per utilizzare correttamente il tipo RHEL_BYOS, abilitare Red Hat Cloud Access nella sottoscrizione di Azure.
  * **SLES_BYOS**: le versioni BYOS di SLES includono il supporto di SUSE.

  È possibile impostare il valore LicenseType sulle opzioni Linux in `New-ProvScheme` e `Set-ProvScheme`.

  Esempio di impostazione di LicenseType su RHEL_BYOS per `New-ProvScheme`:

```
1 New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "
    azureCatalog" -RunAsynchronously -Scope @() -SecurityGroup
    @() -CustomProperties '<CustomProperties xmlns="http://
    schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http
    ://www.w3.org/2001/XMLSchema-instance"><Property xsi:type="
    StringProperty" Name="UseManagedDisks" Value="true" /><
    Property xsi:type="StringProperty" Name="StorageAccountType
```

```
    " Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /><Property xsi:type="StringProperty" Name="
    LicenseType" Value="RHEL_BYOS" /></CustomProperties>'
<!--NeedCopy-->
```

Esempio di impostazione di LicenseType su SLES_BYOS per `Set-ProvScheme`:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
    CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.
    w3.org/2001/XMLSchema-instance"><Property xsi:type="
    StringProperty" Name="UseManagedDisks" Value="true" /><
    Property xsi:type="StringProperty" Name="StorageAccountType
    " Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /><Property xsi:type="StringProperty" Name="
    LicenseType" Value="SLES_BYOS" /></CustomProperties>'
<!--NeedCopy-->
```

> **Nota:**
>
> Se il valore `LicenseType` è vuoto, i valori predefiniti sono Azure Windows Server License (Licenza Azure Windows Server) o Azure Linux License (Licenza Azure Linux), a seconda del valore di OSType.

Esempio di impostazione di LicenseType su un valore vuoto:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
    CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.
    w3.org/2001/XMLSchema-instance"><Property xsi:type="
    StringProperty" Name="UseManagedDisks" Value="true" /><
    Property xsi:type="StringProperty" Name="StorageAccountType
    " Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /></CustomProperties>'
<!--NeedCopy-->
```

Consultare i seguenti documenti per comprendere i tipi di licenza e i relativi vantaggi:

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Raccolta di calcolo di Azure (in precedenza Raccolta immagini condivise Azure) è un repository

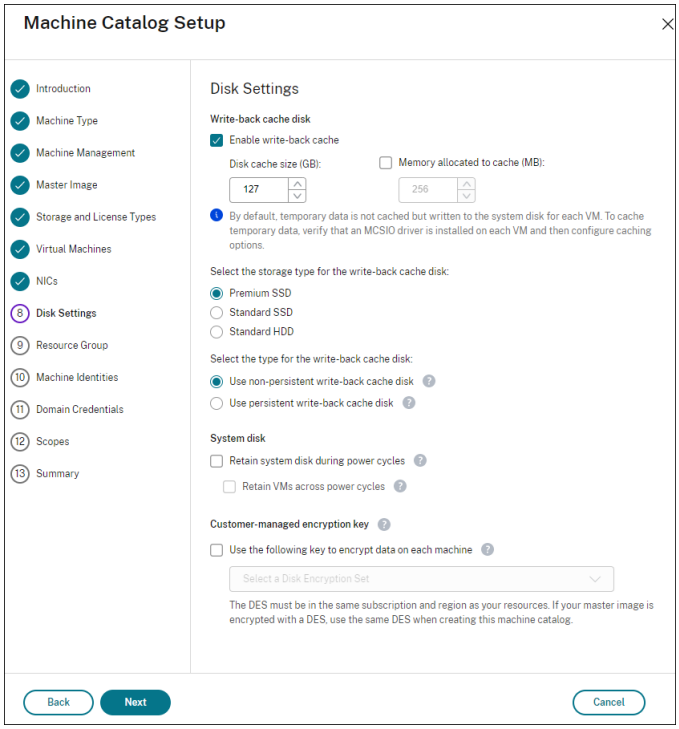
 

per la gestione e la condivisione di immagini. Consente di rendere disponibili le immagini in tutta l'organizzazione. Si consiglia di memorizzare un'immagine in SIG quando si creano cataloghi delle macchine di grandi dimensioni non persistenti, perché in questo modo è possibile reimpostare più velocemente i dischi del sistema operativo VDA. Dopo aver selezionato **Place image in Azure Compute Gallery** (Inserisci immagine nella Raccolta di calcolo di Azure), viene visualizzata la sezione **Azure Compute Gallery settings** (Impostazioni della Raccolta di calcolo di Azure), che consente di specificare altre impostazioni della Raccolta di calcolo di Azure:

  - **Ratio of virtual machines to image replicas** (Rapporto tra macchine virtuali e repliche di immagini). Consente di specificare il rapporto tra macchine virtuali e repliche di immagini che si desidera conservare in Azure. Per impostazione predefinita, Azure conserva una singola replica di immagine ogni 40 macchine non persistenti. Per le macchine persistenti, l'impostazione predefinita del numero è 1.000.
  - **Maximum replica count** (Numero massimo di repliche). Consente di specificare il numero massimo di repliche di immagini che si desidera conservare in Azure. L'impostazione predefinita è 10.

- Nella pagina **Virtual Machines** (Macchine virtuali), indicare quante macchine virtuali si desidera creare. È necessario specificarne almeno uno e selezionare una dimensione della macchina. Dopo la creazione del catalogo, è possibile modificare le dimensioni della macchina modificando il catalogo.
- La pagina **NIC** non contiene informazioni specifiche di Azure. Seguire le linee guida riportate nell'articolo Creare cataloghi di macchine.
- Nella pagina **Disk Settings** (Impostazioni disco), scegliere se abilitare la cache write-back. Con la funzione di ottimizzazione dell'archiviazione MCS abilitata, è possibile configurare le seguenti impostazioni durante la creazione di un catalogo. Queste impostazioni si applicano sia agli ambienti Azure che agli ambienti GCP.




Dopo aver abilitato la cache write-back, è possibile procedere come segue:

- Configurare le dimensioni del disco e della RAM utilizzati per la memorizzazione nella cache dei dati temporanei. Per maggiori informazioni, consultare Configurare la cache per i dati temporanei.
- Selezionare il tipo di archiviazione per il disco della cache write-back. Sono disponibili le seguenti opzioni di archiviazione per il disco della cache write-back:
  - Premium SSD (SSD premium)
  - Standard SSD (SSD standard)
  - Standard HDD (HDD standard)
- Scegliere se si desidera che il disco della cache write-back venga mantenuto per le macchine virtuali di cui è stato eseguito il provisioning. Selezionare **Enable write-back cache** (Abilita cache write-back) per rendere disponibili le opzioni. Per impostazione predefinita, l'opzione **Use non-persistent write-back cache disk** (Usa disco della cache write-back non persistente) è selezionata.
- Selezionare il tipo per il disco della cache write-back.
  - **Use persistent write-back cache disk** (Utilizza disco della cache write-back persistente). Se selezionato, il disco della cache write-back viene eliminato durante i cicli di alimentazione. Tutti i dati reindirizzati a tale disco andranno persi. Se il disco temporaneo della macchina virtuale dispone di spazio sufficiente, viene utilizzato per ospitare il disco della cache write-back per ridurre i costi. Dopo la creazione del catalogo,

è possibile verificare se le macchine di cui è stato eseguito il provisioning utilizzano il disco temporaneo. A tale scopo, fare clic sul catalogo e verificare le informazioni nella scheda **Template Properties** (Proprietà modello). Se viene utilizzato il disco temporaneo, viene visualizzato **Non-persistent Write-back Cache Disk** (Disco della cache write-back non persistente) e il relativo valore è **Yes (using VM's temporary disk)** (Sì, utilizzando il disco temporaneo della macchina virtuale). In caso contrario, viene visualizzato **Non-persistent Write-back Cache Disk** (Disco della cache write-back non persistente) e il relativo valore è **No (not using VM's temporary disk)** (No, non utilizzando il disco temporaneo della macchina virtuale).

* **Use persistent write-back cache disk** (Utilizza disco della cache write-back persistente). Se questa opzione è selezionata, il disco della cache write-back persiste per le macchine virtuali di cui è stato eseguito il provisioning. L'abilitazione dell'opzione aumenta i costi di archiviazione.

– Scegliere se conservare i dischi di sistema per i VDA durante i cicli di alimentazione.

  * **Retain system disk during power cycles** (Conserva il disco di sistema durante i cicli di alimentazione). Per impostazione predefinita, il disco di sistema viene eliminato all'arresto e ricreato all'avvio. Ciò garantisce che il disco sia sempre in uno stato pulito, ma comporta tempi di riavvio delle macchine virtuali più lunghi. Se le scritture di sistema vengono reindirizzate alla cache RAM e si verifica un overflow sul disco della cache, il disco di sistema rimane invariato. L'abilitazione di questa opzione aumenta i costi di archiviazione, ma riduce i tempi di riavvio delle macchine virtuali. Selezionare **Enable write-back cache** (Abilita cache write-back) per rendere disponibile questa opzione.
    · **Retain VMs across power cycles** (Mantieni le macchine virtuali durante i cicli di alimentazione). Selezionare questa opzione per mantenere la personalizzazione delle macchine virtuali e per abilitare l'avvio delle macchine virtuali tramite il portale di Azure.

– Scegliere se abilitare i risparmi sui costi di archiviazione. Se abilitato, risparmia sui costi di archiviazione eseguendo il downgrade del disco di archiviazione ad HDD standard all'arresto della VM. La VM torna alle impostazioni originali al momento del riavvio. L'opzione si applica sia ai dischi di archiviazione che ai dischi cache write-back. In alternativa, è anche possibile usare PowerShell. Vedere Portare il tipo di archiviazione a un livello inferiore quando una VM viene arrestata.

– Scegliere se crittografare i dati sulle macchine di cui è stato eseguito il provisioning nel catalogo. La crittografia lato server con una chiave di crittografia gestita dal cliente consente di gestire la crittografia a livello di disco gestito e di proteggere i dati sulle macchine del catalogo. Per ulteriori informazioni, vedere Crittografia lato server di Azure.

• Nella pagina **Resource Group** (Gruppo di risorse), scegliere se creare gruppi di risorse o utiliz-

zare gruppi esistenti.

  - Se si sceglie di creare gruppi di risorse, selezionare **Next** (Avanti).
  - Se si sceglie di utilizzare gruppi di risorse esistenti, selezionare i gruppi dall'elenco **Available Provisioning Resource Groups** (Gruppi di risorse di provisioning disponibili). **Da ricordare**: selezionare un numero sufficiente di gruppi per ospitare le macchine che si stanno creando nel catalogo. Se se ne scelgono troppo pochi, viene visualizzato un messaggio. Si potrebbe voler selezionare un numero superiore al minimo richiesto se si prevede di aggiungere altre macchine virtuali al catalogo in un secondo momento. Non è possibile aggiungere altri gruppi di risorse a un catalogo dopo la creazione del catalogo.

Per ulteriori informazioni, vedere Gruppi di risorse di Azure.

- Nella pagina **Machine Identities** (Identità macchine), scegliere un tipo di identità e configurare le identità per le macchine in questo catalogo. Se si selezionano le macchine virtuali come aggiunte ad **Azure Active Directory**, èpossibile aggiungerle a un gruppo di sicurezza di Azure AD. I passaggi dettagliati sono i seguenti:

  1. Nel campo **Identity type** (Tipo di identità), selezionare **Azure Active Directory joined**. Viene visualizzata l'opzione **Azure AD security group (optional)** [Gruppo di sicurezza di Azure AD (opzionale)].
  2. Fare clic su **Azure AD security group: Create new** (Gruppo di sicurezza Azure AD: Crea nuovo).
  3. Inserire un nome per il gruppo, quindi fare clic su **Create**.
  4. Seguire le istruzioni sullo schermo per accedere ad Azure.
     Se il nome del gruppo non esiste in Azure, viene visualizzata un'icona verde. In caso contrario, viene visualizzato un messaggio di errore che richiede di inserire un nuovo nome.
  5. Inserire lo schema di denominazione degli account macchina per le macchine virtuali.

  Dopo la creazione del catalogo, Citrix Virtual Apps and Desktops accede ad Azure per conto dell'utente e crea il gruppo di sicurezza e una regola di appartenenza dinamica per il gruppo. In base alla regola, le macchine virtuali con lo schema di denominazione specificato in questo catalogo vengono aggiunte automaticamente al gruppo di sicurezza.

  L'aggiunta di macchine virtuali con uno schema di denominazione diverso a questo catalogo richiede l'accesso ad Azure. Citrix Virtual Apps and Desktops può quindi accedere ad Azure e creare una regola di appartenenza dinamica basata sul nuovo schema di denominazione.

  Quando si elimina questo catalogo, l'eliminazione del gruppo di sicurezza da Azure richiede anche l'accesso ad Azure.

- Le pagine **Domain Credentials** (Credenziali di dominio) e **Summary** (Riepilogo) non contengono informazioni specifiche di Azure. Seguire le linee guida riportate nell'articolo Creare cataloghi di macchine.

Completare la procedura guidata.

### Condizioni perché il disco temporaneo di Azure sia idoneo per il disco della cache write-back

È possibile utilizzare il disco temporaneo di Azure come disco della cache write-back solo se vengono soddisfatte tutte le seguenti condizioni:

- Il disco della cache write-back non deve persistere poiché il disco temporaneo di Azure non è appropriato per i dati persistenti.
- La dimensione della macchina virtuale di Azure scelta deve includere un disco temporaneo.
- Non è necessario abilitare il disco del sistema operativo temporaneo.
- Accettare di inserire il file della cache write-back sul disco temporaneo di Azure.
- La dimensione temporanea del disco di Azure deve essere maggiore della dimensione totale di (dimensione del disco della cache write-back + spazio riservato per il file di paging + 1 GB di spazio buffer).

### Scenari relativi al disco della cache write-back non persistente

La tabella seguente descrive tre diversi scenari in cui il disco temporaneo viene utilizzato per la cache write-back durante la creazione del catalogo delle macchine.

| Scenario | Risultato |
| --- | --- |
| Tutte le condizioni per utilizzare il disco temporaneo per la cache write-back sono soddisfatte. | Il file WBC `mcsdif.vhdx` viene inserito nel disco temporaneo. |
| Lo spazio sul disco temporaneo non è sufficiente per l'utilizzo della cache write-back. | Viene creato un disco VHD `MCSWCDisk` e il file WBC `mcsdif.vhdx` viene inserito su questo disco. |
| Il disco temporaneo ha spazio sufficiente per l'utilizzo della cache write-back, ma `UseTempDiskForWBC` è impostato su **false**. | Viene creato un disco VHD `MCSWCDisk` e il file WBC `mcsdif.vhdx` viene inserito su questo disco. |

### Creare una specifica del modello di Azure

È possibile creare una specifica del modello di Azure nel portale di Azure e utilizzarla in Web Studio e nei comandi PowerShell per creare o aggiornare un catalogo di macchine MCS.

Per creare una specifica del modello di Azure per una macchina virtuale esistente:

1. Andare al portale di Azure. Selezionare un gruppo di risorse, quindi selezionare la macchina virtuale e l'interfaccia di rete. Nel menu **...** in alto, fare clic su **Export template** (Esporta modello).
2. Deselezionare la casella di controllo **Include parameters** (Includi parametri) se si desidera creare una specifica del modello di provisioning del catalogo.
3. Fare clic su **Add to library** (Aggiungi alla libreria) per modificare le specifiche del modello in un secondo momento.
4. Nella pagina **Importing template** (Modello di importazione), inserire le informazioni richieste: **Name** (nome), **Subscription** (abbonamento), **Resource Group** (Gruppo di risorse), **Location** (Posizione) e **Version** (Versione). Fare clic su **Next: Edit Template** (Avanti: Modifica modello).
5. È inoltre necessaria un'interfaccia di rete come risorsa indipendente se si desidera effettuare il provisioning di cataloghi. Pertanto, è necessario rimuovere qualsiasi elemento `dependsOn` specificato nelle specifiche del modello. Ad esempio:

   ```
   "dependsOn": [
   "[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"
   ],
   <!--NeedCopy-->
   ```

6. Creare **Review+Create** (Rivedi+Crea) e le specifiche del modello.
7. Nella pagina **Template Specs** (Specifiche del modello), verificare le specifiche del modello appena creato. Fare clic sulle specifiche del modello. Nel pannello di sinistra, fare clic su **Versions** (Versioni).
8. È possibile creare una nuova versione facendo clic su **Create new version** (Crea nuova versione). Specificare un nuovo numero di versione, apportare le necessarie modifiche alle specifiche del modello corrente e fare clic su **Review + Create** per creare la nuova versione della specifica del modello.

È possibile ottenere informazioni sulle specifiche del modello e sulla versione del modello utilizzando i seguenti comandi PowerShell:

- Per ottenere informazioni sulle specifiche del modello, eseguire:

  ```
  get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
     resourcegroup\bggTemplateSpec.templatespec
  <!--NeedCopy-->
  ```

- Per ottenere informazioni sulla versione delle specifiche del modello, eseguire:

  ```
  get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
     resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
     templatespecversion
  <!--NeedCopy-->
  ```

### Utilizzare le specifiche del modello per creare o aggiornare un catalogo

È possibile creare o aggiornare un catalogo di macchine MCS utilizzando una specifica di modello come input del profilo della macchina. A tale scopo, è possibile utilizzare i comandi Web Studio o PowerShell.

- Per Web Studio, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio
- Per PowerShell, vedere Utilizzare le specifiche del modello per creare o aggiornare un catalogo mediante PowerShell

### Crittografia lato server di Azure

Citrix Virtual Apps and Desktops supporta le chiavi di crittografia gestite dal cliente per i dischi gestiti di Azure tramite Azure Key Vault. Con questo supporto è possibile gestire i requisiti organizzativi e di conformità crittografando i dischi gestiti del catalogo delle macchine utilizzando la propria chiave di crittografia. Per ulteriori informazioni, vedere Crittografia lato server dell'archiviazione su disco di Azure.

Quando si utilizza questa funzionalità per i dischi gestiti:

- Per cambiare la chiave con cui è crittografato il disco, è necessario modificare la chiave corrente in `DiskEncryptionSet`. Tutte le risorse associate a tale modifica `DiskEncryptionSet` devono essere crittografate con la nuova chiave.
- Quando si disabilita o si elimina la chiave, tutte le macchine virtuali con dischi che utilizzano tale chiave si spengono automaticamente. Dopo lo spegnimento, le macchine virtuali non sono utilizzabili a meno che la chiave non venga nuovamente abilitata o non venga assegnata una nuova chiave. Qualsiasi catalogo che utilizza la chiave non può essere acceso e non è possibile aggiungervi macchine virtuali.

#### Considerazioni importanti quando si utilizzano chiavi di crittografia gestite dal cliente

Quando si utilizza questa funzionalità, tenere presente quanto segue:

- Tutte le risorse correlate alle chiavi gestite dal cliente (Azure Key Vault, set di crittografia dei dischi, macchine virtuali, dischi e snapshot) devono risiedere nella stessa sottoscrizione e area geografica.
- Dopo aver abilitato la chiave di crittografia gestita dal cliente, non è possibile disabilitarla in un secondo momento. Se si desidera disabilitare o rimuovere la chiave di crittografia gestita dal cliente, copiare tutti i dati su un disco gestito diverso che non utilizza la chiave di crittografia gestita dal cliente.

- I dischi creati da immagini personalizzate crittografate utilizzando la crittografia lato server e le chiavi gestite dal cliente devono essere crittografati utilizzando le stesse chiavi gestite dal cliente. Questi dischi devono trovarsi nella stessa sottoscrizione.
- Le snapshot create da dischi crittografati con crittografia lato server e chiavi gestite dal cliente devono essere crittografate con le stesse chiavi gestite dal cliente.
- I dischi, le snapshot e le immagini crittografati con chiavi gestite dal cliente non possono passare a un altro gruppo di risorse e a un'altra sottoscrizione.
- I dischi gestiti attualmente o precedentemente crittografati utilizzando Crittografia dischi di Azure non possono essere crittografati utilizzando chiavi gestite dal cliente.
- Fare riferimento al sito Microsoft per le limitazioni sui set di crittografia dei dischi per ciascuna regione.

> **Nota:**
>
> Per informazioni sulla configurazione della crittografia lato server di Azure, vedere Guida rapida: creare un insieme di credenziali delle chiavi utilizzando il portale di Azure.

### Chiave di crittografia gestita dal cliente di Azure

Quando si crea un catalogo delle macchine, è possibile scegliere se crittografare i dati sulle macchine di cui è stato eseguito il provisioning nel catalogo. La crittografia lato server con una chiave di crittografia gestita dal cliente consente di gestire la crittografia a livello di disco gestito e di proteggere i dati sulle macchine del catalogo. Un set di crittografia dei dischi (DES, Disk Encryption Set) rappresenta una chiave gestita dal cliente. Per utilizzare questa funzionalità, è necessario prima creare il DES in Azure. Un DES ha il formato seguente:

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption`

Selezionare un DES dall'elenco. Il DES selezionato deve essere nella stessa sottoscrizione e nella stessa regione delle risorse. Se l'immagine è crittografata con un DES, utilizzare lo stesso DES durante la creazione del catalogo delle macchine. Non è possibile modificare il DES dopo aver creato il catalogo.

Se si crea un catalogo con una chiave di crittografia e successivamente si disabilita il DES corrispondente in Azure, non si potrà più accendere alle macchine nel catalogo o aggiungervi macchine.

Vedere Creare un catalogo di macchine con chiave gestita dal cliente.

### Crittografia del disco di Azure sull'host

È possibile creare un catalogo di macchine MCS con crittografia in modalità host. Attualmente, MCS supporta solo il flusso di lavoro dei profili macchina per questa funzionalità. È possibile utilizzare una VM o specifiche di modello come input per il profilo di una macchina.

Questo metodo di crittografia non crittografa i dati tramite l'archiviazione di Azure. Il server che ospita la macchina virtuale crittografa i dati e quindi i dati crittografati fluiscono attraverso il server di archiviazione di Azure. Quindi, questo metodo di crittografia crittografa i dati per tutto il loro percorso dall'inizio alla fine.

**Restrizioni:**

La crittografia del disco di Azure sull'host è:

- non supportata per tutte le dimensioni delle macchine di Azure
- incompatibile con la crittografia del disco di Azure

Per creare un catalogo di macchine con funzionalità di crittografia sull'host:

1. Verificare se l'abbonamento ha la funzionalità di crittografia sull'host abilitata o meno. A questo scopo, vedere https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/. Se non è abilitata, è necessario abilitarla per l'abbonamento. Per informazioni sull'attivazione della funzionalità per l'abbonamento, vedere https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.
2. Verificare se una particolare dimensione di macchina virtuale di Azure supporta o meno la crittografia sull'host. A questo scopo, in una finestra di PowerShell, eseguire uno dei seguenti comandi:

```
PS XDHyp:\Connections<your connection>\east us.region\
   serviceoffering.folder>
<!--NeedCopy-->
```

```
PS XDHyp:\HostingUnits<your hosting unit>\serviceoffering.folder>
<!--NeedCopy-->
```

3. Creare una macchina virtuale o specifiche di modello come input per il profilo della macchina nel portale di Azure con la crittografia sull'host abilitata.
    - Se si desidera creare una macchina virtuale, selezionare una dimensione di macchina virtuale che supporti la crittografia sull'host. Dopo aver creato la macchina virtuale, viene abilitata la relativa proprietà **Encryption at host** (Crittografia sull'host).
    - Se si desidera utilizzare specifiche di modello, assegnare al parametro `Encryption at Host` il valore **true** all'interno di `securityProfile`.

4. Creare un catalogo di macchine MCS con il flusso di lavoro dei profili delle macchine, selezionando una VM o specifiche di modello.

    - Disco del sistema operativo/disco dati: viene crittografato tramite chiave gestita dal cliente e chiave gestita dalla piattaforma
    - Disco del sistema operativo temporaneo: viene crittografato solo tramite chiave gestita dalla piattaforma
    - Disco cache: viene crittografato tramite chiave gestita dal cliente e chiave gestita dalla piattaforma

    È possibile creare il catalogo delle macchine utilizzando Web Studio o eseguendo i comandi PowerShell.

### Doppia crittografia su disco gestito

È possibile creare un catalogo di macchine con doppia crittografia. In tutti i cataloghi creati con questa funzionalità tutti i dischi lato server sono crittografati con chiavi gestite dalla piattaforma e dal cliente. L'utente possiede e gestisce Azure Key Vault, Encryption Key e Disk Encryption Sets (DES).

La doppia crittografia è la crittografia lato piattaforma (impostazione predefinita) e la crittografia gestita dal cliente (CMEK). Pertanto, se si è un cliente altamente sensibile alla sicurezza e si nutre preoccupazione per il rischio associato a qualsiasi algoritmo di crittografia, implementazione o chiave compromessa, è possibile optare per questa doppia crittografia. Il sistema operativo persistente e i dischi di dati, le snapshot e le immagini sono tutti crittografati quando inattivi con doppia crittografia.

> **Nota:**
>
> - È possibile creare e aggiornare un catalogo di macchine con doppia crittografia utilizzando Web Studio e i comandi PowerShell. Per i comandi di PowerShell vedere Creare un catalogo di macchine con doppia crittografia.
> - È possibile utilizzare un flusso di lavoro non basato su profili macchina o un flusso di lavoro basato sul profilo macchina per creare o aggiornare un catalogo di macchine con doppia crittografia.
> - Se si utilizza un flusso di lavoro non basato su profili di macchina per creare un catalogo di macchine, è possibile riutilizzare il valore `DiskEncryptionSetId` archiviato.
> - Se si utilizza un profilo macchina, è possibile utilizzare una VM o un specifica di modello come input per il profilo della macchina.

**Limitazioni:**

- La doppia crittografia non è supportata per i dischi Ultra Disks o Premium SSD v2.
- La doppia crittografia non è supportata sui dischi non gestiti.

- Se si disattiva una chiave del DiskEncryptionSet associata a un catalogo, le VM del catalogo vengono disattivate.
- Tutte le risorse correlate alle chiavi gestite dal cliente (Azure Key Vault, set di crittografia dei dischi, macchine virtuali, dischi e snapshot) devono essere nella stessa sottoscrizione e area geografica.
- È possibile creare solo fino a 50 set di crittografia del disco per regione per abbonamento.
- Non è possibile aggiornare un catalogo macchine che ha già `DiskEncryptionSetId` con un `DiskEncryptionSetId` diverso.

### Gruppi di risorse di Azure

I gruppi di risorse di provisioning di Azure offrono un modo per eseguire il provisioning delle macchine virtuali che forniscono applicazioni e desktop agli utenti. È possibile aggiungere gruppi di risorse di Azure vuoti esistenti quando si crea un catalogo delle macchine MCS o quando vengono creati nuovi gruppi di risorse per conto dell'utente. Per informazioni sui gruppi di risorse di Azure, consultare la documentazione Microsoft.

#### Utilizzo dei gruppi di risorse di Azure

Non ci sono limiti al numero di macchine virtuali, dischi gestiti, snapshot e immagini per ciascun gruppo di risorse di Azure (il limite di 240 macchine virtuali per 800 dischi gestiti per ciascun gruppo di risorse di Azure è stato rimosso).

- Quando si utilizza un'entità servizio con ambito completo per creare un catalogo delle macchine, MCS crea un solo gruppo di risorse di Azure e utilizza tale gruppo per il catalogo.
- Quando si utilizza un'entità servizio con ambito limitato per creare un catalogo delle macchine, è necessario fornire un gruppo di risorse di Azure vuoto e pre-creato per il catalogo.

### Dischi temporanei di Azure

Un disco temporaneo di Azure consente di riutilizzare il disco della cache o il disco temporaneo per archiviare il disco del sistema operativo per una macchina virtuale abilitata per Azure. Questa funzionalità è utile per gli ambienti Azure che richiedono un disco SSD a prestazioni più elevate rispetto a un disco rigido standard. Per informazioni su come creare un catalogo con un disco effimero di Azure, vedere Creare un catalogo con dischi effimeri di Azure.

> **Nota:**
>
> I cataloghi persistenti non supportano i dischi del sistema operativo temporanei.

I dischi del sistema operativo temporanei richiedono che lo schema di provisioning utilizzi dischi gestiti e una Raccolta immagini condivise.

#### Memorizzazione di un disco del sistema operativo temporaneo

È possibile memorizzare un disco del sistema operativo temporaneo sul disco temporaneo della macchina virtuale o su un disco di risorse. Questa funzionalità consente di utilizzare un disco del sistema operativo temporaneo con una macchina virtuale che non ha una cache o ha una cache insufficiente. Tali macchine virtuali dispongono di un disco temporaneo o di risorse per archiviare un disco del sistema operativo temporaneo, ad esempio `Ddv4`.

Considerare quanto segue:

- Un disco temporaneo viene memorizzato nel disco della cache della macchina virtuale o nel disco temporaneo (risorsa) della macchina virtuale. Il disco della cache è preferibile rispetto al disco temporaneo, a meno che il disco della cache non sia abbastanza grande da ospitare i contenuti del disco del sistema operativo.
- Per gli aggiornamenti, una nuova immagine più grande del disco della cache ma più piccola del disco temporaneo comporta la sostituzione del disco del sistema operativo temporaneo con il disco temporaneo della macchina virtuale.

#### Ottimizzazione dell'archiviazione di dischi temporanei di Azure e Machine Creation Services (MCS) (I/O MCS)

Il disco del sistema operativo temporaneo di Azure e l'I/O MCS non possono essere abilitati contemporaneamente.

Le considerazioni importanti sono le seguenti:

- Non è possibile creare un catalogo delle macchine con il disco del sistema operativo temporaneo e l'I/O MCS abilitati contemporaneamente.
- I parametri PowerShell (`UseWriteBackCache` e `UseEphemeralOsDisk`) non hanno effetto e restituiscono un vero e proprio messaggio di errore se vengono impostati su **true** in `New-ProvScheme` o `Set-ProvScheme`.
- Per i cataloghi delle macchine esistenti creati con entrambe le funzionalità abilitate, è comunque possibile:
  - aggiornare un catalogo delle macchine
  - aggiungere o eliminare macchine virtuali
  - eliminare un catalogo delle macchine

### Raccolta di calcolo di Azure

Utilizzare la Raccolta di calcolo di Azure (in precedenza Raccolta immagini condivise di Azure) come repository di immagini pubblicate per macchine di cui è stato eseguito il provisioning con MCS in Azure. È possibile archiviare un'immagine pubblicata nella raccolta per accelerare la creazione e l'attivazione dei dischi del sistema operativo, migliorando i tempi di avvio del sistema e delle applicazioni per le macchine virtuali non persistenti. La Raccolta immagini condivise contiene i tre elementi seguenti:

- *Galleria*: le immagini sono memorizzate qui. MCS crea una raccolta per ogni catalogo delle macchine.
- *Gallery Image Definition* (Definizione dell'immagine in galleria): questa definizione include informazioni (tipo e stato del sistema operativo, regione di Azure) sull'immagine pubblicata. MCS crea una definizione di immagine per ogni immagine creata per il catalogo.
- *Gallery Image Version* (Versione immagine in galleria): ciascuna immagine di una Raccolta immagini condivise può avere più versioni e ogni versione può avere più repliche in regioni diverse. Ogni replica è una copia completa dell'immagine pubblicata.

> **Nota:**
>
> La funzionalità della Raccolta immagini condivise è compatibile solo con i dischi gestiti. Non è disponibile per i cataloghi delle macchine legacy.

Per altre informazioni, vedere Archiviare e condividere immagini in una raccolta di calcolo di Azure.

Per informazioni sulla creazione o l'aggiornamento di un catalogo di macchine utilizzando l'immagine della Raccolta di calcolo di Azure mediante PowerShell, vedere Creare o aggiornare un catalogo di macchine usando un'immagine della Raccolta di calcolo di Azure.

### Azure Marketplace

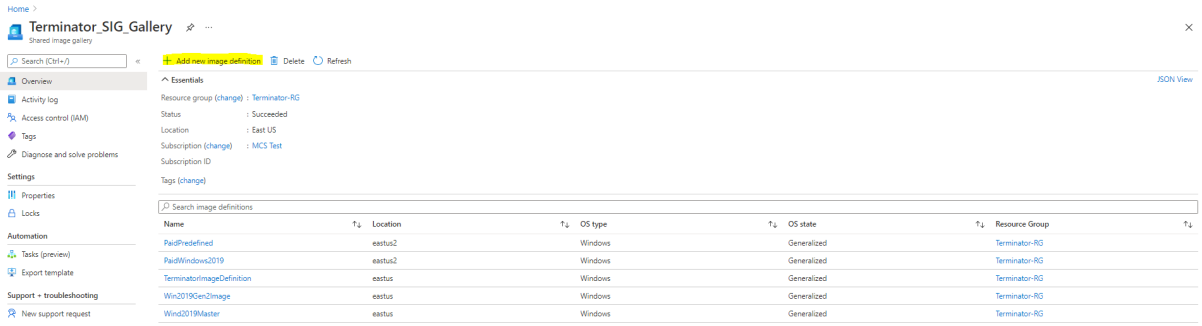
Citrix Virtual Apps and Desktops supporta l'utilizzo di un'immagine master in Azure che contiene informazioni sul piano per creare un catalogo delle macchine. Per ulteriori informazioni, vedere Microsoft Azure Marketplace.

> **Suggerimento:**
>
> Alcune immagini che si trovano in Azure Marketplace, come l'immagine standard di Windows Server, non aggiungono informazioni sul piano. La funzionalità di Citrix Virtual Apps and Desktops è dedicata alle immagini a pagamento.

### Assicurarsi che l'immagine creata nella Raccolta immagini condivise contenga informazioni sul piano di Azure

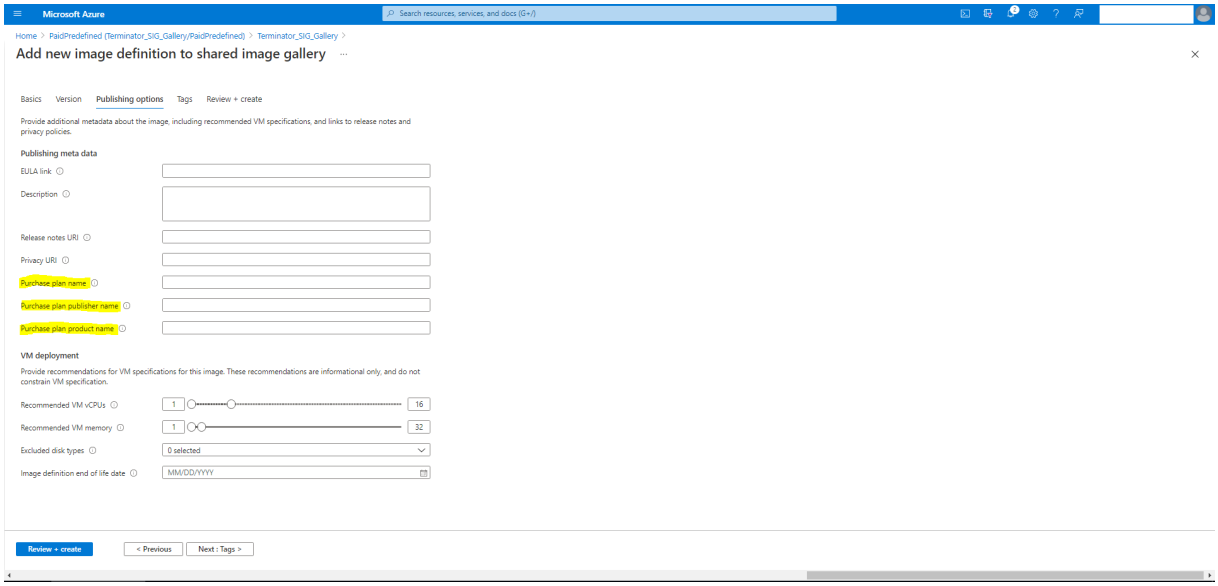
Utilizzare la procedura descritta in questa sezione per visualizzare le immagini della Raccolta immagini condivise in Web Studio. Facoltativamente, queste immagini possono essere utilizzate per un'immagine master. Per inserire l'immagine in una Raccolta immagini condivise, creare una definizione di immagine in una raccolta.



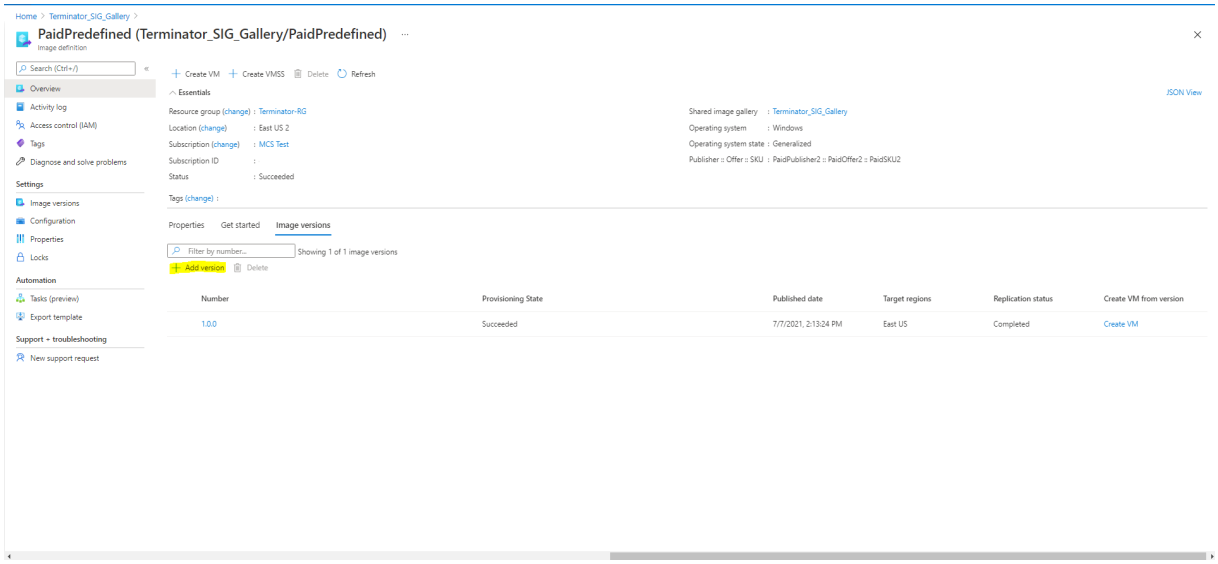

Nella pagina **Publishing options** (Opzioni di pubblicazione), verificare le informazioni sul piano di acquisto.

I campi relativi alle informazioni sul piano di acquisto sono inizialmente vuoti. Compilare questi campi con le informazioni sul piano di acquisto utilizzate per l'immagine. La mancata compilazione delle informazioni sul piano di acquisto può causare la mancata riuscita del processo del catalogo delle macchine.

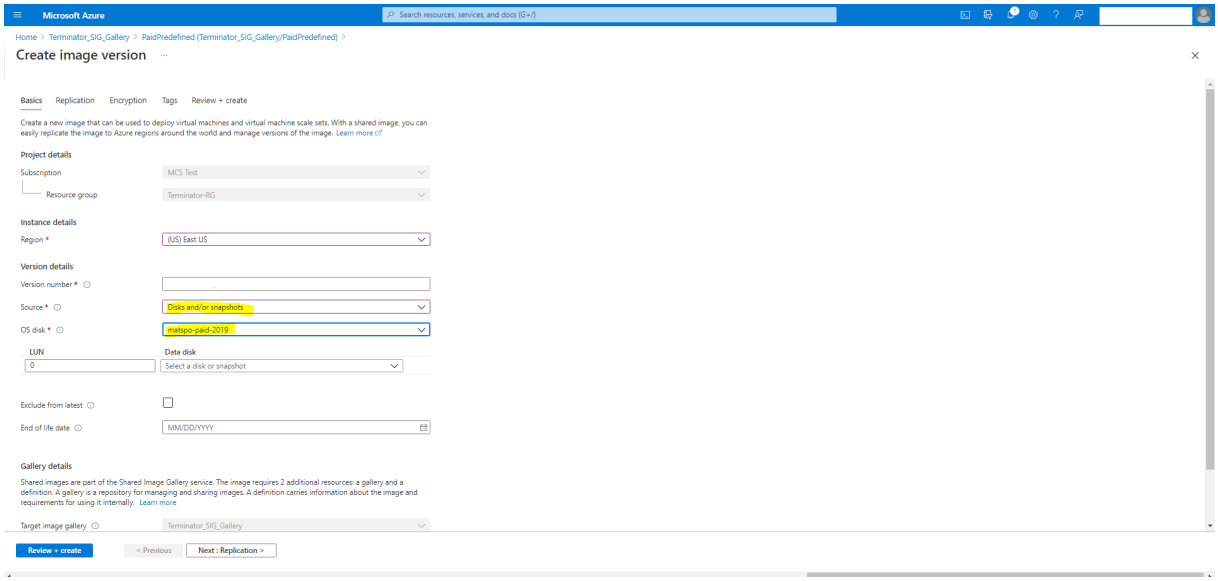



Dopo aver verificato le informazioni sul piano di acquisto, creare una versione immagine all'interno della definizione. Viene utilizzata come immagine master. Fare clic su **Add version** (Aggiungi versione):




Nella sezione **Version details** (Dettagli versione), selezionare la snapshot dell'immagine o il disco gestito come origine:




## Creare un catalogo di macchine usando PowerShell

Questa sezione descrive in dettaglio come creare cataloghi usando PowerShell:

- Creare un catalogo con un disco cache di write-back non persistente
- Creare un catalogo con disco cache di write-back persistente
- Migliorare le prestazioni di avvio con MCSIO
- Utilizzare le specifiche del modello per creare o aggiornare un catalogo mediante PowerShell
- Cataloghi di macchine con avvio attendibile
- Utilizzare i valori delle proprietà del profilo macchina
- Creare un catalogo di macchine con chiave di crittografia gestita dal cliente
- Creare un catalogo di macchine con doppia crittografia
- Creare un catalogo con dischi effimeri di Azure
- Host dedicati di Azure
- Creare o aggiornare un catalogo di macchine usando un'immagine della Raccolta di calcolo di Azure
- Configurare la Raccolta immagini condivise
- Eseguire il provisioning delle macchine in zone di disponibilità specificate
- Tipologie di archiviazione
- Posizione del file di paging
- Aggiornare l'impostazione del file di paging

### Creare un catalogo con un disco cache di write-back non persistente

Per configurare un catalogo con il disco della cache write-back non persistente, utilizzare il parametro PowerShell `New-ProvScheme CustomProperties`. La proprietà personalizzata `UseTempDiskForWBC` indica se si sta accettando di utilizzare l'archiviazione temporanea di Azure per archiviare il file della cache write-back. Questo deve essere configurato su true durante l'esecuzione di `New-ProvScheme` se si desidera utilizzare il disco temporaneo come disco della cache write-back. Se questa proprietà non viene specificata, il parametro è impostato su **False** per impostazione predefinita.

Ad esempio, utilizzando il parametro `CustomProperties` per impostare `UseTempDiskForWBC` su **true**:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
    /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
    XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
    "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="
    Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client"/> `
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="
    true"/> `
</CustomProperties>'
<!--NeedCopy-->
```

> **Nota:**
>
> Dopo aver eseguito il commit del catalogo delle macchine per l'utilizzo dell'archiviazione temporanea locale di Azure per il file della cache write-back, non può essere modificato per utilizzare l'unità disco rigido virtuale in un secondo momento.

### Creare un catalogo con disco cache di write-back persistente

Per configurare un catalogo con il disco della cache write-back persistente, utilizzare il parametro PowerShell `New-ProvScheme CustomProperties`. Questo parametro supporta una proprietà aggiuntiva, `PersistWBC`, utilizzata per determinare il modo in cui il disco della cache write-back persiste per le macchine di cui è stato eseguito il provisioning con MCS. La proprietà `PersistWBC` viene utilizzata solo quando viene specificato il parametro`UseWriteBackCache` e quando il parametro `WriteBackCacheDiskSize` è impostato per indicare che viene creato un disco.

Esempi di proprietà trovate nel parametro `CustomProperties` prima del supporto `PersistWBC` sono:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
</CustomProperties>
<!--NeedCopy-->
```

Quando si utilizzano queste proprietà, considerare che contengono valori predefiniti se le proprietà vengono omesse dal parametro `CustomProperties`. La proprietà `PersistWBC` ha due valori possibili: **true** o **false**.

L'impostazione della proprietà `PersistWBC` su **true** non elimina il disco della cache write-back quando l'amministratore di Citrix Virtual Apps and Desktops spegne la macchina utilizzando Web Studio.

L'impostazione della proprietà `PersistWBC` **su false** elimina il disco della cache write-back quando l'amministratore di Citrix Virtual Apps and Desktops arresta la macchina utilizzando Web Studio.

> **Nota:**
>
> Se la proprietà `PersistWBC` viene omessa, sarà **false** per impostazione predefinita e la cache write-back viene eliminata quando il computer viene arrestato utilizzando Web Studio.

Ad esempio, utilizzando il parametro `CustomProperties` per impostare `PersistWBC` su true:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> **Importante:**
>
> La proprietà `PersistWBC` può essere impostata solo utilizzando il cmdlet PowerShell `New-ProvScheme`. Il tentativo di modificare le `CustomProperties` di uno schema di provisioning

> dopo la creazione non ha alcun impatto sul catalogo macchine e sulla persistenza del disco della cache write-back quando un computer viene arrestato.

Ad esempio, impostare `New-ProvScheme` perché utilizzi la cache write-back mentre si imposta la proprietà `PersistWBC` su true:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

### Migliorare le prestazioni di avvio con MCSIO

È possibile migliorare le prestazioni di avvio per i dischi gestiti di Azure e GCP quando MCSIO è abilitato. Utilizzare la proprietà personalizzata di PowerShell `PersistOSDisk` nel comando `New-ProvScheme` per configurare questa funzionalità. Le opzioni associate a `New-ProvScheme` includono:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="Resource <!--NeedCopy-->
```

```
``````<!--NeedCopy-->
<!--NeedCopy-->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
    />
</CustomProperties>
<!--NeedCopy-->
```

Per abilitare questa funzionalità, impostare la proprietà personalizzata `PersistOSDisk` su **`true`**. Ad esempio:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
    /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
    UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
    /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
    Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
    =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
    GoldImages.resourcegroup\W10MCSIO-01
    _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
     CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
     adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
    folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

### Utilizzare le specifiche del modello per creare o aggiornare un catalogo mediante PowerShell

È possibile creare o aggiornare un catalogo di macchine MCS utilizzando una specifica di modello come input del profilo della macchina. A tale scopo, è possibile utilizzare i comandi Web Studio o PowerShell.

Per Web Studio, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio

Utilizzare i comandi PowerShell:

1. Aprire la finestra di **PowerShell**.
2. Eseguire `asnp citrix*`.
3. Creare o aggiornare un catalogo.

   - Per creare un catalogo:

     a) Utilizzare il comando `New-ProvScheme` con una specifica del modello come input per il profilo macchina. Ad esempio:

     ```
     New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
        image.folder/fgthj.resourcegroup/nab-ws-
        vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
        folder/fgthj.resourcegroup/test.templatespec/V1.
        templatespecversion"
     -ProvisioningSchemeName <String>
     -HostingUnitName <String>
     -IdentityPoolName <String>
     [-ServiceOffering <String>][-CustomProperties <String>
     [-LoggingId <Guid>]
     [-BearerToken <String>][-AdminAddress <String>]
     [<CommonParameters>]
     <!--NeedCopy-->
     ```

     b) Completare la creazione del catalogo di macchine.

   - Per aggiornare un catalogo, utilizzare il comando `Set-ProvScheme` con una specifica di modello come input del profilo macchina. Ad esempio:

     ```
     Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
         Us.region/vm.folder/MasterDisk.vm'
     MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
        folder/fgthj.resourcegroup/testing.templatespec/V1.
        templatespecversion'
     [-ProvisioningSchemeName] <String>
     [-CustomProperties <String>][-ServiceOffering <String>] [-
        PassThru]
     [-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <
        String>] [<CommonParameters>]
     <!--NeedCopy-->
     ```

### Cataloghi di macchine con avvio attendibile

Per creare correttamente un catalogo di macchine con avvio attendibile, utilizzare:

- Un profilo macchina con avvio attendibile
- Una dimensione di macchina virtuale che supporti l'avvio attendibile
- Una versione di macchina virtuale Windows che supporti l'avvio attendibile. Attualmente, Windows 10, 2016, 2019 e 2022 supportano l'avvio attendibile.

> **Importante:**
>
> L'avvio attendibile richiede la creazione di nuove macchine virtuali. Non è possibile abilitare l'avvio attendibile sulle macchine virtuali esistenti che erano state create inizialmente senza di esso.

Per visualizzare gli elementi di inventario offerti da Citrix Virtual Apps and Desktops e determinare se le dimensioni della macchina virtuale supportano l'avvio attendibile, eseguire il seguente comando:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando **asnp citrix*** per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire il seguente comando:

```
$s = (ls XDHyp:\HostingUnits<name of hosting unit>\serviceoffering
    .folder"<VM size>.serviceoffering)
<!--NeedCopy-->
```

4. Eseguire `$s | select -ExpandProperty Additionaldata`
5. Controllare il valore dell'attributo `SupportsTrustedLaunch`.
    - Se `SupportsTrustedLaunch` è **True**, la dimensione della macchina virtuale supporta l'avvio attendibile.
    - Se `SupportsTrustedLaunch` è **False**, la dimensione della macchina virtuale non supporta l'avvio attendibile.

Come da PowerShell di Azure, è possibile usare il seguente comando per determinare le dimensioni di macchina virtuale che supportano l'avvio attendibile:

```
(Get-AzComputeResourceSku | where {
 $\_.Locations.Contains($region) -and ($\_.Name -eq "<VM size>")  }
 )[0].Capabilities
<!--NeedCopy-->
```

Di seguito sono riportati alcuni esempi che descrivono se la dimensione della macchina virtuale supporta l'avvio attendibile dopo l'esecuzione del comando Azure PowerShell.

- *Esempio 1*: se la macchina virtuale di Azure supporta solo la generazione 1, quella macchina virtuale non supporta l'avvio attendibile. Pertanto, la funzionalità `TrustedLaunchDisabled` non viene visualizzata dopo l'esecuzione del comando Azure PowerShell.
- *Esempio 2*: se la macchina virtuale di Azure supporta solo la generazione 2 e la funzionalità`TrustedLaunchDisabled` è **True**, la dimensione della macchina virtuale di generazione 2 non è supportata per l'avvio attendibile.
- *Esempio 3*: se la macchina virtuale di Azure supporta solo la generazione 2 e la funzionalità `TrustedLaunchDisabled` non viene visualizzata dopo l'esecuzione del comando PowerShell, la dimensione della VM di generazione 2 è supportata per l'avvio attendibile.

Per ulteriori informazioni sull'avvio attendibile per le macchine virtuali Azure, vedere il documento Microsoft Avvio attendibile per le macchine virtuali di Azure.

#### Errori nella creazione di cataloghi di macchine con avvio attendibile

Si ottengono errori appropriati nei seguenti scenari durante la creazione di un catalogo di macchine con avvio attendibile:

| Scenario | Errore |
| --- | --- |
| Se si seleziona un profilo macchina durante la creazione di un catalogo non gestito | `MachineProfileNotSupportedForUnmanagedCata` |
| Se si seleziona un profilo macchina che supporta l'avvio attendibile durante la creazione di un catalogo con un disco non gestito come immagine master | `SecurityTypeNotSupportedForUnmanagedDisk` |
| Se non si seleziona il profilo macchina durante la creazione di un catalogo gestito con un' immagine master con l'avvio attendibile come tipo di sicurezza | `MachineProfileNotFoundForTrustedLaunchMaste` |
| Se si seleziona un profilo macchina con un tipo di sicurezza diverso dal tipo di protezione dell' immagine master | `SecurityTypeConflictBetweenMasterImageAndMa` |
| Se si seleziona una dimensione di macchina virtuale che non supporta l'avvio attendibile, ma utilizza un'immagine master che supporta l' avvio attendibile durante la creazione di un catalogo | `MachineSizeNotSupportTrustedLaunch` |

### Utilizzare i valori delle proprietà del profilo macchina

Il catalogo delle macchine utilizza le seguenti proprietà definite nelle proprietà personalizzate:

- Zona di disponibilità
- ID gruppo host dedicato
- ID set crittografia disco
- Tipo di sistema operativo
- Tipo di licenza
- Tipo di archiviazione

Se queste proprietà personalizzate non sono definite in modo esplicito, i valori delle proprietà vengono impostati in base alla specifica del modello ARM o alla macchina virtuale, a seconda di quale sia utilizzata come profilo macchina. Inoltre, se non è specificato `ServiceOffering`, questo viene impostato in base al profilo della macchina.

> **Nota:**
>
> Se alcune delle proprietà non sono presenti nel profilo macchina e non sono definite nelle proprietà personalizzate, vengono adottati i valori predefiniti delle proprietà laddove è applicabile.

La sezione seguente descrive alcuni scenari in `New-ProvScheme` e `Set-ProvScheme` quando `CustomProperties` hanno tutte le proprietà definite o qando i valori sono derivati da MachineProfile.

- Scenari New-ProvScheme
  - MachineProfile ha tutte le proprietà e le CustomProperties non sono definite. Esempio:

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

    ```
    1  Get-ProvScheme | select CustomProperties
    2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
          machinecreation" xmlns:xsi="http://www.w3.org/2001/
          XMLSchema-instance">
    3  <Property xsi:type="StringProperty" Name="StorageAccountType"
           Value="<mpA-value>"/>
    4  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
          -value>"/>
    5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
          "<mpA-value>"/>
    6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
          " Value="<mpA-value>"/>
    7  <Property xsi:type="StringProperty" Name="
          DedicatedHostGroupId" Value="<mpA-value>"/>
    8  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
          value>"/>
    9  </CustomProperties>
    10 <!--NeedCopy-->
    ```

  - MachineProfile ha alcune proprietà e le CustomProperties non sono definite. Esempio: MachineProfile ha solo LicenseType e OSType.

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="OSType" Value="<mpA
    -value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<mpA-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Sia MachineProfile che CustomProperties definiscono tutte le proprietà. Esempio:

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  Le proprietà personalizzate hanno la priorità. I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

  ```
  Get-ProvScheme | select CustomProperties
  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
      " Value="<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="
      DedicatedHostGroupId" Value="<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="Zones" Value="<
      CustomPropertiesA-value>"/>
  </CustomProperties>
  <!--NeedCopy-->
  ```

- Alcune proprietà sono definite in MachineProfile e alcune proprietà sono definite in CustomProperties. Esempio:

  * In CustomProperties sono definite LicenseType e StorageAccountType
  * In MachineProfile sono definite LicenseType, OSType e Zones

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<mpA
    -value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
    value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Alcune proprietà sono definite in MachineProfile e alcune proprietà sono definite in CustomProperties. Inoltre, ServiceOffering non è definito. Esempio:
  - In CustomProperties è definito StorageType
  - In MachineProfile è definito LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mp.vm"
-ServiceOffering "XDHyp:\HostingUnits\azureunit\
    serviceoffering.folder<explicit-machine-size>.
    serviceoffering"
<!--NeedCopy-->
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<explicit-machine-size>.serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="explicit-storage-type"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "value-from-machineprofile"/>
</CustomProperties>
<!--NeedCopy-->
```

- Se OsType e non si trova né in CustomProperties né in MachineProfile, allora:
  - Il valore viene letto dall'immagine master.
  - Se l'immagine master è un disco non gestito, OsType è impostato su Windows. Esempio:

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
```

```
\machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
 "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-
image.manageddisk"
```

Il valore dell'immagine master viene scritto nelle proprietà personalizzate, in questo caso Linux.

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="OSType" Value="
      Linux"/>
4  </CustomProperties>
5  <!--NeedCopy-->
```

- Scenari Set-ProvScheme
  - Un catalogo esistente con:
    - CustomProperties per `StorageAccountType` e OsType
    - MachineProfile `mpA.vm` che definisce le zone
  - Aggiornamenti:
    - MachineProfile mpB.vm che definisce StorageAccountType
    - Un nuovo insieme di proprietà personalizzate $CustomPropertiesB che definisce LicenseType e OsType

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"-CustomProperties
 $CustomPropertiesB
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<mpB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<CustomPropertiesB-value>"/>
6       </CustomProperties>
7  <!--NeedCopy-->
```

  - Un catalogo esistente con:
    - CustomProperties per `StorageAccountType` e OsType

    * MachineProfile `mpA.vm` che definisce StorageAccountType e LicenseType

- Aggiornamenti:

    * Un nuovo insieme di proprietà personalizzate $CustomPropertiesB che definisce StorageAccountType e OsType.

```
Set-ProvScheme -CustomProperties $CustomPropertiesB
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
        Value="<CustomPropertiesB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
       CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "<mp-A-value>"/>
6  </CustomProperties>
7  <!--NeedCopy-->
```

- Un catalogo esistente con:

    * CustomProperties per `StorageAccountType` e OsType
    * MachineProfile `mpA.vm` che definisce le zone

- Aggiornamenti:

    * Un MachineProfile mpB.vm che definisce StorageAccountType e LicenseType
    * `ServiceOffering` non è specificato

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
1  Get-ProvScheme | select ServiceOffering
2  serviceoffering.folder<value-from-machineprofile>.
       serviceoffering
3
4  Get-ProvScheme | select CustomProperties
5  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
6  <Property xsi:type="StringProperty" Name="StorageAccountType"
        Value="<mpB-value>"/>
7  <Property xsi:type="StringProperty" Name="OSType" Value="<
       prior-CustomProperties-value>"/>
8  <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "<mpB-value>"/>
```

```
</CustomProperties>
<!--NeedCopy-->
```

### Creare un catalogo di macchine con chiave di crittografia gestita dal cliente

I passaggi dettagliati per creare un catalogo di macchine con chiave di crittografia gestita dal cliente sono:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Inserire `cd xdhyp:/`.
4. Inserire `cd .\HostingUnits\(your hosting unit)`.
5. Immettere cd diskencryptionset.folder.
6. Immettere dir per ottenere l'elenco dei set di crittografia del disco.
7. Copiare l'ID di un set di crittografia del disco.
8. Creare una stringa di proprietà personalizzata che includa l'ID del set di crittografia del disco. Ad esempio:

```
$customProperties = "<CustomProperties xmlns=`"http://schemas.
    citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.
    org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
    Value=`"Standard_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"persistWBC`" Value=`"
    False`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value
    =`"false`" />
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
    Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
     Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/
    resourceGroups/abc/providers/Microsoft.Compute/
    diskEncryptionSets/abc-des`"/>
</CustomProperties>
<!--NeedCopy-->
```

9. Creare un pool di identità se non è già stato creato. Ad esempio:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain def.local -NamingSchemeType Numeric
<!--NeedCopy-->
```

10. Eseguire il comando New-ProvScheme: Ad esempio:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
   IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.
   resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.folder\
    def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network
    " }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\azure-res2\serviceoffering.
   folder\Standard_DS2_v2.serviceoffering"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.folder<
   def.resourcegroup><machine profile vm.vm>"
-CustomProperties $customProperties
<!--NeedCopy-->
```

11. Completate la creazione del catalogo di macchine.

### Creare un catalogo di macchine con doppia crittografia

È possibile creare e aggiornare un catalogo di macchine con doppia crittografia utilizzando Web Studio e i comandi PowerShell.

I passaggi dettagliati per creare un catalogo di macchine con doppia crittografia sono:

1. Creare un Azure Key Vault e DES con chiavi gestite dalla piattaforma e gestite dal cliente. Per informazioni su come creare un Azure Key Vault e un DES, vedere Usare il portale di Azure per abilitare la doppia crittografia dei dati inattivi per i dischi gestiti.
2. Per sfogliare i DiskEncryptionSet disponibili nella propria connessione di hosting:

   a) Aprire una finestra di **PowerShell**.
   b) Eseguire i seguenti comandi PowerShell:
      i. asnp citrix*
      ii. cd xdhyp:
      iii. cd HostingUnits
      iv. cd yourHostingUnitName (ad esempio azure-est)
      v. cd diskencryptionset.folder
      vi. dir

   È possibile utilizzare un ID del `DiskEncryptionSet` per creare o aggiornare un catalogo utilizzando proprietà personalizzate.
3. Se si desidera utilizzare il flusso di lavoro del profilo macchina, creare una VM o una specifica di modello come input per il profilo della macchina.

- Se si desidera utilizzare una VM come input del profilo macchina:
  a) Creare una macchina virtuale nel portale di Azure.
  b) Passare a **Dischi > Gestione delle chiavi** per crittografare la VM direttamente con qualsiasi `DiskEncryptionSetID`.
- Se si desidera utilizzare una specifica di modello come input del profilo della macchina:
  a) Nel modello, in `properties>storageProfile>osDisk>managedDisk`, aggiungere il parametro `diskEncryptionSet` e l'ID del DES a doppia crittografia.

4. Creare il catalogo di macchine.

   - Se si utilizza Web Studio, eseguire una delle seguenti operazioni oltre alla procedura descritta in Creare cataloghi di macchine.
     - Se non si utilizza un flusso di lavoro basato sul profilo macchina, nella pagina **Impostazioni disco** selezionare **Use the following key to encrypt data on each machine** (Usa la seguente chiave per crittografare i dati su ciascuna macchina). Quindi, selezionare il proprio DES a doppia crittografia dal menu a discesa. Continuare a creare il catalogo.
     - Se si utilizza il flusso di lavoro del profilo macchina, nella pagina **Master Image** selezionare un'immagine master e un profilo macchina. Assicurarsi che il profilo macchina abbia un ID set crittografia disco nelle sue proprietà.

     Tutte le macchine create nel catalogo sono criptate due volte dalla chiave associata al DES selezionato.

   - Se si utilizlzano i comandi di PowerShell, eseguire una delle seguenti operazioni:
     - Se non si utilizza un flusso di lavoro basato sul profilo macchina, aggiungere la proprietà personalizzata `DiskEncryptionSetId` nel comando `New-ProvScheme`. Ad esempio:

```
New-ProvScheme -CleanOnBoot -CustomProperties '<
   CustomProperties xmlns="http://schemas.citrix.com/2014/
   xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks"
    Value="true" />
<Property xsi:type="StringProperty" Name="
   StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="
   DiskEncryptionSetId" Value="/subscriptions/12345678-
   xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
   providers/Microsoft.Compute/diskEncryptionSets/
   SampleEncryptionSet" />
</CustomProperties>'
-HostingUnitName "Redacted"
-IdentityPoolName "Redacted"
```

```
-InitialBatchSizeHint 1
-MasterImageVM "Redacted"
-NetworkMapping @{
"0"="Redacted" }

-ProvisioningSchemeName "Redacted"
-ServiceOffering "Redacted"
<!--NeedCopy-->
```

- Se si utilizza un flusso di lavoro basato sul profilo macchina, utilizzare un input di profilo macchina nel comando `New-ProvScheme`. Ad esempio:

```
New-ProvScheme -CleanOnBoot
-HostingUnitName azure-east
-IdentityPoolName aio-ip
-InitialBatchSizeHint 1
-MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
   \abc.resourcegroup\fgb-vda-snapshot.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
   folder\apa-resourceGroup.resourcegroup\apa-
   resourceGroup-vnet.virtualprivatecloud\default.network"
    }

-ProvisioningSchemeName aio-test
-MachineProfile XDHyp:\HostingUnits\azure-east\
   machineprofile.folder\abc.resourcegroup\abx-mp.
   templatespec\1.0.0.templatespecversion
<!--NeedCopy-->
```

5. Completare la creazione di un catalogo utilizzando l'SDK Remote PowerShell. Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Tutte le macchine create nel catalogo sono criptate due volte dalla chiave associata al DES selezionato.

#### Convertire un catalogo non crittografato per utilizzare la doppia crittografia

È possibile aggiornare il tipo di crittografia di un catalogo di macchine (utilizzando proprietà personalizzate o il profilo macchina) solo se il catalogo in precedenza non era crittografato.

- Se non si utilizza un flusso di lavoro basato sul profilo macchina, aggiungere la proprietà personalizzata DiskEncryptionSetId nel comando `Set-ProvScheme`. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix
   .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
   /2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
   Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
```

```
        resourceGroups/Sample-RG/providers/Microsoft.Compute/
        diskEncryptionSets/SampleEncryptionSet" />
4   </CustomProperties>'
5   <!--NeedCopy-->
```

- Se si utilizza un flusso di lavoro basato sul profilo macchina, utilizzare un input di profilo macchina nel comando `Set-ProvScheme`. Ad esempio:

```
1   Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
        XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
        resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
2   <!--NeedCopy-->
```

Una volta completata l'operazione, tutte le nuove macchine virtuali aggiunte al catalogo vengono crittografate due volte dalla chiave associata al DES selezionato.

#### Verificare che il catalogo sia crittografato con doppia crittografia

- In Web Studio:
  1. Passare a **Machine Catalogs** (Cataloghi di macchine).
  2. Selezionare il catalogo da verificare. Fare clic sulla scheda **Template Properties** (Proprietà del modello) situata nella parte inferiore dello schermo.
  3. In **Azure Details** (Dettagli di Azure) verificare l'ID del set di crittografia del disco in **Disk Encryption Set**. Se l'ID DES del catalogo è vuoto, il catalogo non è crittografato.
  4. Nel portale di Azure, verificare che il tipo di crittografia del DES associato all'ID DES sia costituito da chiavi gestite dalla piattaforma e dal cliente.
- Utilizzando i comandi PowerShell:
  1. Aprire la finestra di **PowerShell**.
  2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
  3. Utilizzare `Get-ProvScheme` per ottenere le informazioni del proprio catalogo macchine. Ad esempio:

```
1   Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
2   <!--NeedCopy-->
```

  4. Recuperare la proprietà personalizzata DES Id del catalogo di macchine. Ad esempio:

```
1   <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
        Value="/subscriptions
       /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
       -RG/providers/Microsoft.Compute/diskEncryptionSets/
       SampleEncryptionSet" />
2   <!--NeedCopy-->
```

5. Nel portale di Azure, verificare che il tipo di crittografia del DES associato all'ID DES sia costituito da chiavi gestite dalla piattaforma e dal cliente.

### Creare un catalogo con dischi effimeri di Azure

Per utilizzare dischi temporanei, è necessario impostare la proprietà personalizzata `UseEphemeralOsDisk` su **true** durante l'esecuzione di `New-ProvScheme`.

> **Nota:**
>
> Se la proprietà personalizzata `UseEphemeralOsDisk` è impostata su **false** o non viene specificato un valore, tutti i VDA di cui è stato eseguito il provisioning continuano a utilizzare un disco del sistema operativo di cui è stato eseguito il provisioning.

Di seguito è riportato un esempio di set di proprietà personalizzate da utilizzare nello schema di provisioning:

```
"CustomProperties": [
            {

                "Name": "UseManagedDisks",
                "Value": "true"
             }
 ,
            {

                "Name": "StorageType",
                "Value": "Standard_LRS"
             }
 ,
            {

                "Name": "UseSharedImageGallery",
                "Value": "true"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaMaximum",
                "Value": "10"
             }
 ,
            {

```

```
                    "Name": "LicenseType",
                    "Value": "Windows_Server"
                }
    ,
                {

                    "Name": "UseEphemeralOsDisk",
                    "Value": "true"
                }

            ],
<!--NeedCopy-->
```

### Configurare un disco temporaneo per un catalogo

Per configurare un disco del sistema operativo temporaneo di Azure per un catalogo, utilizzare il parametro `UseEphemeralOsDisk` in `Set-ProvScheme`. Impostare il valore del parametro `UseEphemeralOsDisk` su **true**.

> **Nota:**
>
> Per utilizzare questa funzionalità, è necessario abilitare anche i parametri `UseManagedDisks` e `UseSharedImageGallery`.

Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties <
    CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="UseSharedImageGallery" Value=
    "true" />
<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
    true" />
</CustomProperties>'
<!--NeedCopy-->
```

### Considerazioni importanti per i dischi temporanei

Per eseguire il provisioning di dischi del sistema operativo temporanei utilizzando `New-ProvScheme`, considerare i seguenti vincoli:

- La dimensione della macchina virtuale utilizzata per il catalogo deve supportare i dischi operativi temporanei.

- La dimensione della cache o del disco temporaneo associato alla dimensione della macchina virtuale deve essere maggiore o uguale alla dimensione del disco del sistema operativo.
- La dimensione del disco temporaneo deve essere maggiore della dimensione del disco della cache.

Tenere presenti questi problemi anche quando:

- Si crea lo schema di provisioning.
- Si modifica lo schema di provisioning.
- Si aggiorna l'immagine.

### Host dedicati di Azure

È possibile utilizzare MCS per eseguire il provisioning di macchine virtuali su host dedicati di Azure. Prima di eseguire il provisioning delle macchine virtuali su host dedicati di Azure:

- Creare un gruppo host.
- Creare host nel gruppo host.
- Assicurarsi che la capacità host sia sufficiente per la creazione di cataloghi e macchine virtuali.

È possibile creare un catalogo di macchine con tenancy host definita tramite il seguente script PowerShell:

```
1 New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
     xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
     ="http://www.w3.org/2001/XMLSchema-instance">
2  <Property xsi:type="StringProperty" Name="HostGroupId" Value="
      myResourceGroup/myHostGroup" />
3  ...other Custom Properties...
4  </CustomProperties>
5 <!--NeedCopy-->
```

Quando si utilizza MCS per eseguire il provisioning di macchine virtuali su host Azure dedicati, tenere in considerazione quanto segue:

- Un *host dedicato* è una proprietà del catalogo e non può essere modificata una volta creato il catalogo. La tenancy dedicata non è attualmente supportata in Azure.
- Quando si utilizza il parametro `HostGroupId`, è necessario un gruppo host di Azure preconfigurato nella regione dell'unità di hosting.
- È necessario il posizionamento automatico di Azure. Questa funzionalità invia una richiesta di eseguire l'onboarding della sottoscrizione associata al gruppo host. Per ulteriori informazioni, vedere Set di scalabilità VM negli host dedicati di Azure - Anteprima pubblica. Se il posizionamento automatico non è abilitato, MCS genererà un errore durante la creazione del catalogo.

### Creare o aggiornare un catalogo di macchine usando un'immagine della Raccolta di calcolo di Azure

Quando si seleziona un'immagine da utilizzare per la creazione di un catalogo delle macchine, è possibile selezionare le immagini create nella Raccolta di calcolo di Azure.

Per visualizzare queste immagini, è necessario:

1. Configurare un sito Citrix Virtual Apps and Desktops.
2. Connettersi ad Azure Resource Manager.
3. Nel portale di Azure, creare un gruppo di risorse. Per ulteriori informazioni, vedere Creare una raccolta per l'archiviazione e la condivisione delle risorse.
4. Nel gruppo di risorse, creare una Raccolta di calcolo di Azure.
5. Nella Raccolta di calcolo di Azure, creare una definizione di immagine.
6. Nella definizione dell'immagine, creare una versione dell'immagine.

Usa i seguenti comandi PowerShell per creare o aggiornare un catalogo di macchine utilizzando un'immagine tratta dalla Raccolta di calcolo di Azure:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Selezionare un gruppo di risorse, quindi elencare tutte le gallerie di quel gruppo di risorse.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup")
<!--NeedCopy-->
```

4. Selezionare una raccolta, quindi elencare tutte le definizioni delle immagini di quella raccolta.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery")
<!--NeedCopy-->
```

5. Selezionare una definizione di immagine, quindi elencare tutte le versioni dell'immagine in questione.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery\sigtestimage.
    imagedefinition")
<!--NeedCopy-->
```

6. Creare e aggiornare un catalogo MCS utilizzando i seguenti elementi:

   - Gruppo di risorse
   - Raccolta

- Definizione delle immagini della raccolta
- Versione delle immagini della raccolta.

Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

### Configurare la Raccolta immagini condivise

Utilizzare il comando `New-ProvScheme` per creare uno schema di provisioning con il supporto della Raccolta immagini condivise. Utilizzare il comando `Set-ProvScheme` per abilitare o disabilitare questa funzionalità per uno schema di provisioning e per modificare il rapporto di replica e i valori massimi della replica.

Sono state aggiunte tre proprietà personalizzate agli schemi di provisioning per supportare la funzionalità Raccolta immagini condivise:

`UseSharedImageGallery`

- Definisce se utilizzare la Raccolta immagini condivise per archiviare le immagini pubblicate. Se impostata su **True**, l'immagine viene memorizzata come immagine della Raccolta immagini condivise, altrimenti viene memorizzata come snapshot.
- I valori validi sono **True** e **False**.
- Se la proprietà non è definita, il valore predefinito è **False**.

`SharedImageGalleryReplicaRatio`

- Definisce il rapporto tra macchine e repliche di versioni di immagini della raccolta.
- I valori validi sono numeri interi maggiori di 0.
- Se la proprietà non è definita, vengono utilizzati i valori predefiniti. Il valore predefinito per i dischi del sistema operativo persistenti è 1.000 e il valore predefinito per i dischi del sistema operativo non persistenti è 40.

`SharedImageGalleryReplicaMaximum`

- Definisce il numero massimo di repliche per ogni versione dell'immagine della raccolta.
- I valori validi sono numeri interi maggiori di 0.
- Se la proprietà non è definita, il valore predefinito è 10.
- Azure attualmente supporta fino a 10 repliche per una singola versione dell'immagine della raccolta. Se la proprietà è impostata su un valore maggiore di quello supportato da Azure, MCS tenta di utilizzare il valore specificato. Azure genera un errore, che viene registrato da MCS, e lascia invariato il numero di repliche corrente.

> **Suggerimento:**
>
> Quando si utilizza la Raccolta immagini condivise per archiviare un'immagine pubblicata per i cataloghi di cui è stato eseguito il provisioning con MCS, MCS imposta il numero di repliche delle versioni delle immagini della raccolta in base al numero di macchine nel catalogo, al rapporto di replica e al numero massimo di repliche. Il conteggio delle repliche viene calcolato dividendo il numero di macchine nel catalogo per il rapporto di replica (arrotondando per eccesso al valore intero più vicino) e quindi limitando il valore al numero massimo di repliche. Ad esempio, con un rapporto di replica di 20 e un massimo di 5, per 0-20 macchine viene creata una replica, per 21-40 macchine vengono create 2 repliche, per 41-60 macchine vengono create 3 repliche, per 61-80 macchine vengono create 4 repliche e per 81 macchine o più vengono create 5 repliche.

### Caso d'uso: aggiornamento del rapporto di replica e della replica massima della Raccolta immagini condivise

Il catalogo delle macchine esistente utilizza la Raccolta immagini condivise. Utilizzare il comando `Set-ProvScheme` per aggiornare le proprietà personalizzate per tutte le macchine esistenti nel catalogo e per tutte le macchine future:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

### Caso d'uso: conversione di un catalogo di snapshot in un catalogo della Raccolta immagini condivise

Per questo caso d'uso:

1. Eseguire `Set-ProvScheme` con il contrassegno `UseSharedImageGallery` impostato su **True**. Facoltativamente, includere le proprietà `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum`.
2. Aggiornare il catalogo.
3. Spegnere e riaccendere le macchine per forzare un aggiornamento.

Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

> **Suggerimento:**
>
> I parametri `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum` non sono richiesti. Al completamento del comando `Set-ProvScheme`, l'immagine della Raccolta immagini condivise non è stata ancora creata. Una volta configurato il catalogo per l'utilizzo della raccolta, la successiva operazione di aggiornamento del catalogo memorizza l'immagine pubblicata nella raccolta. Il comando di aggiornamento del catalogo crea la raccolta, l'immagine della raccolta e la versione dell'immagine. Lo spegnimento e la riaccensione delle macchine le aggiorna, a quel punto il conteggio delle repliche viene aggiornato, se appropriato. Da quel momento, tutte le macchine non persistenti esistenti vengono reimpostate utilizzando l'immagine della Raccolta immagini condivise e tutte le macchine di cui è stato eseguito il provisioning vengono create utilizzando l'immagine. La vecchia snapshot viene ripulita automaticamente entro poche ore.

### Caso d'uso: conversione di un catalogo della Raccolta immagini condivise in un catalogo di snapshot

Per questo caso d'uso:

1. Eseguire `Set-ProvScheme` con il contrassegno `UseSharedImageGallery` impostato su **False** o non definito.
2. Aggiornare il catalogo.
3. Spegnere e riaccendere le macchine per forzare un aggiornamento.

Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
<!--NeedCopy-->
```

> **Suggerimento:**
>
> A differenza dell'aggiornamento da una snapshot a un catalogo della Raccolta immagini condivise, i dati personalizzati per ogni macchina non sono ancora aggiornati per riflettere le nuove proprietà personalizzate. Eseguire il comando seguente per visualizzare le proprietà personalizzate originali della Raccolta immagini condivise: `Get-ProvVm -ProvisioningSchemeName catalog-name`. Dopo il completamento del comando `Set-ProvScheme`, la snapshot dell'immagine non è stata ancora creata. Una volta configurato il catalogo per non utilizzare la raccolta, la successiva operazione di aggiornamento del catalogo memorizza l'immagine pubblicata come snapshot. Da quel momento, tutte le macchine non persistenti esistenti vengono reimpostate utilizzando la snapshot e tutte le macchine di cui è stato eseguito il provisioning vengono create dalla snapshot. Lo spegnimento e la riaccensione delle macchine le aggiorna, a quel punto i dati della macchina personalizzati vengono aggiornati per riflettere che `UseSharedImageGallery` è impostato su **False**. Le vecchie risorse della Raccolta immagini condivise (raccolta, immagine e versione) vengono ripulite automaticamente nel giro di poche ore.

## Eseguire il provisioning delle macchine in zone di disponibilità specificate

È possibile effettuare il provisioning delle macchine in zone di disponibilità specifiche in ambienti Azure. È possibile raggiungere questo obiettivo utilizzando PowerShell.

> **Nota:**
>
> Se non viene specificata alcuna zona, MCS consente ad Azure di posizionare le macchine all'interno della regione. Se viene specificata più di una zona, MCS distribuisce in modo casuale le macchine nelle zone.

### Configurare le zone di disponibilità tramite PowerShell

Utilizzando PowerShell, è possibile visualizzare gli articoli di inventario offerti utilizzando `Get-Item`. Ad esempio, per visualizzare l'offerta di servizi *Eastern US region* `Standard_B1ls` (Regione degli Stati Uniti orientali):

```
1 $serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
     name\East US.region\serviceoffering.folder\Standard_B1ls.
     serviceoffering"
2 <!--NeedCopy-->
```

Per visualizzare le zone, utilizzare il parametro `AdditionalData` per l'elemento:

```
$serviceOffering.AdditionalData
```

Se le zone di disponibilità non sono specificate, non vi è alcun cambiamento nel modo in cui viene eseguito il provisioning delle macchine.

Per configurare le zone di disponibilità tramite PowerShell, utilizzare la proprietà personalizzata **Zones** (Zone) disponibile con l'operazione `New-ProvScheme`. La proprietà **Zones** (Zone) definisce un elenco di zone di disponibilità in cui eseguire il provisioning delle macchine. Tali zone possono includere una o più zone di disponibilità. Ad esempio, `<Property xsi:type="StringProperty"Name="Zones"Value="1, 3"/>` per le zone 1 e 3.

Utilizzare il comando `Set-ProvScheme` per aggiornare le zone per uno schema di provisioning.

Se viene fornita una zona non valida, lo schema di provisioning non viene aggiornato e viene visualizzato un messaggio di errore che fornisce istruzioni su come correggere il comando non valido.

> **Suggerimento:**
>
> Se si specifica una proprietà personalizzata non valida, lo schema di provisioning non viene aggiornato e viene visualizzato un messaggio di errore pertinente.

### Tipologie di archiviazione

Selezionare diversi tipi di archiviazione per le macchine virtuali negli ambienti di Azure che utilizzano MCS. Per le macchine virtuali di destinazione, MCS supporta:

- Disco del sistema operativo: SSD premium, SSD o HDD
- Disco della cache write-back: SSD premium, SSD o HDD

Quando si utilizzano questi tipi di archiviazione, considerare quanto segue:

- Assicurarsi che la macchina virtuale supporti il tipo di archiviazione selezionato.
- Se la configurazione utilizza un disco temporaneo di Azure, non è disponibile l'opzione per l'impostazione del disco della cache write-back.

> **Suggerimento:**
>
> `StorageType` è configurato per un tipo di sistema operativo e un account di archiviazione. `WBCDiskStorageType` è configurato per il tipo di archiviazione della cache write-back. Per un catalogo normale, è necessario `StorageType`. Se `WBCDiskStorageType` non è configurato, `StorageType` viene utilizzato come impostazione predefinita per `WBCDiskStorageType`.

Se WBCDiskStorageType non è configurato, StorageType viene utilizzato come impostazione predefinita per WBCDiskStorageType.

### Configurare i tipi di archiviazione

Per configurare i tipi di archiviazione per le macchine virtuali, utilizzare il parametro `StorageType` in `New-ProvScheme`. Impostare il valore del parametro `StorageType` su uno dei tipi di archiviazione supportati.

Di seguito è riportato un set di esempio del parametro `CustomProperties` in uno schema di provisioning:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
     <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="LicenseType" Value="
     Windows_Client" />
5 </CustomProperties>'
6 <!--NeedCopy-->
```

### Abilita l'archiviazione con ridondanza della zona

È possibile selezionare l'archiviazione con ridondanza della zona durante la creazione del catalogo. Replica il disco gestito di Azure in modo sincrono in più zone di disponibilità, il che consente di effettuare il ripristino dopo che si è verificato un errore in una zona utilizzando la ridondanza di altre.

È possibile specificare **Premium_ZRS** e **StandardSSD_ZRS** nelle proprietà personalizzate del tipo di archiviazione. L'archiviazione ZRS può essere impostata utilizzando le proprietà personalizzate esistenti o tramite il modello **MachineProfile**. L'archiviazione ZRS è supportata anche con il comando `Set-ProvVMUpdateTimeWindow` accompagnato dai parametri `-StartsNow` e `-DurationInMinutes -1`, ed è possibile modificare il computer esistente dall'archiviazione LRS a quello ZRS.

**Limitazioni:**

- Supportato solo nei dischi gestiti
- Supportato solo se si utilizzano unità a stato solido (SSD) premium e standard
- Non supportato in `StorageTypeAtShutdown`
- Disponibile solo in alcune aree geografiche.
- Le prestazioni di Azure diminuiscono quando si creano dischi ZRS su larga scala. Pertanto, alla prima accensione, accendere le macchine in batch più piccoli (meno di 300 macchine alla volta)

**Imposta l'archiviazione con ridondanza della zona come tipo di archiviazione su disco** È possibile selezionare l'archiviazione con ridondanza della zona durante la creazione iniziale del catalogo oppure aggiornare il tipo di archiviazione in un catalogo esistente.

**Seleziona l'archiviazione con ridondanza della zona utilizzando i comandi PowerShell** Quando si crea un nuovo catalogo in Azure usando il comando `New-ProvScheme` di PowerShell, utilizzare il valore `Standard_ZRS` in `StorageAccountType`.
Ad esempio:

```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    StandardSSD_ZRS" />
<!--NeedCopy-->
```

Quando lo si imposta, questo valore viene convalidato da un'API dinamica che determina se può essere utilizzato correttamente. Le seguenti eccezioni possono verificarsi se l'uso di ZRS non è valido per il proprio catalogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: la proprietà personalizzata StorageTypeAtShutdown non può essere utilizzata con l'archiviazione ZRS.
- **StorageAccountTypeNotSupportedInRegion**: questa eccezione si verifica se si tenta di utilizzare l'archiviazione ZRS in un'area di Azure che non supporta ZRS
- **ZrsRequiresManagedDisks**: è possibile utilizzare l'archiviazione con ridondanza della zona solo con dischi gestiti.

È possibile impostare il tipo di archiviazione su disco utilizzando le seguenti proprietà personalizzate:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Nota:**
>
> Durante la creazione del catalogo, viene utilizzato il disco del sistema operativo del profilo macchina `StorageType` se non sono impostate le proprietà personalizzate.

### Posizione del file di paging

Negli ambienti Azure, il file di paging viene impostato in una posizione appropriata al momento della creazione della macchina virtuale. L'impostazione del file di paging è configurata nel formato `<page file location>[min size] [max size]` (la dimensione è in MB). Per ulteriori informazioni, vedere il documento Microsoft Come determinare le dimensioni del file di paging appropriate.

Quando si crea `ProvScheme` durante la preparazione dell'immagine, MCS determina la posizione del file di paging in base a determinate regole. Dopo aver creato `ProvScheme`:

- La modifica delle dimensioni della macchina virtuale viene bloccata se la dimensione della macchina virtuale in ingresso causa una diversa impostazione del file di paging.
- L'aggiornamento del profilo macchina viene bloccato se la gamma di servizi offerti viene modificata a causa dell'aggiornamento del profilo macchina che determina una diversa impostazione del file di paging.
- Le proprietà del disco operativo effimero (EOS) e di MCSIO non possono essere modificate.

#### Determinazione della posizione del file di paging

Le funzionalità come EOS e MCSIO hanno la propria posizione prevista per il file di paging e si escludono a vicenda. La tabella mostra la posizione prevista del file di paging per ciascuna funzione:

| Funzionalità | Posizione prevista del file di paging |
|---|---|
| EOS | Disco del sistema operativo |
| MCSIO | Prima il disco temporaneo di Azure, altrimenti il Disco cache di write-back |

> **Nota:**
>
> Anche se la preparazione dell'immagine è disaccoppiata dalla creazione dello schema di provisioning, MCS determina correttamente la posizione del file di paging. Il percorso predefinito del file di paging è sul disco del sistema operativo.

#### Scenari di configurazione del file di paging

La tabella descrive alcuni possibili scenari di configurazione del file di paging durante la preparazione dell'immagine e l'aggiornamento dello schema di provisioning:

| Durante | Scenario | Risultato |
| --- | --- | --- |
| Preparazione delle immagini | Il file di paging dell'immagine di origine è impostato sul disco temporaneo, mentre la dimensione della macchina virtuale specificata nello schema di provisioning non ha un disco temporaneo | Il file di paging viene inserito nel disco del sistema operativo |
| Preparazione delle immagini | Il file di paging dell'immagine di origine è impostato sul disco del sistema operativo, mentre la dimensione della macchina virtuale specificata nello schema di provisioning ha un disco temporaneo. | Il file di paging viene inserito nel disco temporaneo |
| Preparazione delle immagini | Il file di paging dell'immagine di origine è impostato sul disco temporaneo, mentre il disco temporaneo del sistema operativo è abilitato nello schema di provisioning. | Il file di paging viene inserito nel disco del sistema operativo |
| Aggiornamento dello schema di provisioning | Si tenta di aggiornare lo schema di provisioning, la dimensione originale della macchina virtuale ha un disco temporaneo e la macchina virtuale di destinazione non ha alcun disco temporaneo. | Rifiuta la modifica con un messaggio di errore |
| Aggiornamento dello schema di provisioning | Si tenta di aggiornare lo schema di provisioning, la dimensione originale della macchina virtuale non ha un disco temporaneo e la macchina virtuale di destinazione ha un disco temporaneo | Rifiuta la modifica con un messaggio di errore |

### Aggiornare l'impostazione del file di paging

È inoltre possibile specificare l'impostazione del file di paging, inclusa la posizione e le dimensioni, utilizzando il comando PoSH in modo esplicito. Questo sostituisce il valore determinato da MCS. È possibile farlo eseguendo il comando `New-ProvScheme` e includendo le seguenti proprietà personalizzate:

- `PageFileDiskDriveLetterOverride`: lettera dell'unità disco del percorso del file di paging
- `InitialPageFileSizeInMB`: dimensione iniziale del file di paging in MB
- `MaxPageFileSizeInMB`: dimensione massima del file di paging in MB

Esempio di utilizzo delle proprietà personalizzate:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
   XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
   "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="
   PageFileDiskDriveLetterOverride" Value="d"/> `
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
   Value="2048"/> `
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
   ="8196"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client"/> `
</CustomProperties>'
<!--NeedCopy-->
```

Vincoli:

- È possibile aggiornare l'impostazione del file di paging solo quando si crea lo schema di provisioning eseguendo il comando `New-ProvScheme` e l'impostazione del file di paging non può essere modificata in seguito.
- Fornire tutte le proprietà relative dell'impostazione del file di paging (`PageFileDiskDriveLetterOver`, `InitialPageFileSizeInMB` e `MaxPageFileSizeInMB`) nelle proprietà personalizzate o non fornire alcuna di esse.
- La dimensione iniziale del file di paging deve essere compresa tra 16 MB e 16777216 MB.
- La dimensione massima del file di paging deve essere maggiore o uguale alla dimensione iniziale del file di paging e inferiore a 16777216 MB.
- Questa funzione non è supportata in Web Studio.

### Passaggi successivi

- Se questo è il primo catalogo creato, Web Studio guida l'utente a creare gruppi di consegna
- Per rivedere l'intero processo di configurazione, vedere Installazione e configurazione
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di Microsoft Azure

### Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Connessione a Microsoft Azure Resource Manager
- Creare cataloghi di macchine

## Creare un catalogo di Microsoft System Center Virtual Machine Manager

January 7, 2024

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti di virtualizzazione Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Prima di creare un catalogo di VMM, è necessario completare la creazione di una connessione a VMM. Vedere Connessione a Microsoft System Center Virtual Machine Manager.

### Creare una macchina virtuale master

1. Installare un VDA nella macchina virtuale master e selezionare l'opzione per ottimizzare il desktop per migliorare le prestazioni.
2. Creare un'istantanea della macchina virtuale master da utilizzare come backup.
3. Creare desktop virtuali.

### MCS su condivisioni di file SMB 3

Per i cataloghi di macchine creati con MCS su condivisioni di file SMB 3 per l'archiviazione nelle macchine virtuali, assicurarsi che le credenziali soddisfino i requisiti che seguono. Questi requisiti garantiscono che le chiamate dall'Hypervisor Communications Library (HCL) del Controller si connettano correttamente all'archiviazione SMB:

- Le credenziali utente VMM devono includere l'accesso completo in lettura e scrittura all'archiviazione SMB.
- Le operazioni del disco virtuale di archiviazione durante gli eventi del ciclo di vita delle macchine virtuali vengono eseguite tramite il server Hyper-V utilizzando le credenziali utente VMM.

Quando si utilizza l'archiviazione SMB, abilitare il Credential Security Support Provider (CredSSP) di autenticazione dal controller ai singoli computer Hyper-V. Utilizzare questo processo per VMM 2012 SP1 con Hyper-V in Windows Server 2012. Per ulteriori informazioni, vedere CTX137465.

L'HCL utilizza `CredSSP` per aprire una connessione alla macchina Hyper-V. Questa funzionalità passa le credenziali utente crittografate mediante Kerberos al computer Hyper-V. I comandi di **PowerShell** nella sessione sul computer Hyper-V remoto vengono eseguiti con le credenziali fornite. In questo caso, le credenziali dell'utente VMM, in modo che i comandi di comunicazione per l'archiviazione funzionino correttamente.

Le attività seguenti utilizzano script PowerShell che hanno origine nell'HCL e vengono quindi inviati al computer Hyper-V per agire sull'archiviazione SMB 3.0.

- **Consolidate master image** (Consolida immagine master): un'immagine master crea uno schema di provisioning MCS (catalogo macchine). Clona e appiattisce la macchina virtuale master pronta per la creazione di macchine virtuali dal nuovo disco creato (e rimuove la dipendenza dalla VM master originale).

  ConvertVirtualHardDisk nello spazio dei nomi root\virtualization\v2

  Esempio:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
<!--NeedCopy-->
```

- **Create difference disk** (Crea disco di differenza): crea un disco di differenza dall'immagine master generata dal consolidamento dell'immagine master. Il disco di differenza viene quindi collegato a una nuova macchina virtuale.

  CreateVirtualHardDisk nello spazio dei nomi root\virtualization\v2

  Esempio:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
<!--NeedCopy-->
```

- **Upload identity disks** (Carica dischi di identità): l'HCL non può caricare direttamente il disco di identità nell'archiviazione SMB. Pertanto, il computer Hyper-V deve caricare e copiare il disco di

identità nella posizione di archiviazione. Poiché il computer Hyper-V non è in grado di leggere il disco dal controller, l'HCL deve prima copiare il disco di identità attraverso il computer Hyper-V come segue.

1. L'HCL carica l'identità nel computer Hyper-V tramite la condivisione dell'amministratore.
2. Il computer Hyper-V copia il disco nell'archiviazione SMB tramite uno script PowerShell in esecuzione nella sessione remota di PowerShell. Nel computer Hyper-V viene creata una cartella e le autorizzazioni per tale cartella sono bloccate solo per l'utente VMM (tramite la connessione remota PowerShell).
3. L'HCL elimina il file dalla condivisione dell'amministratore.
4. Quando l'HCL termina il caricamento del disco di identità sul computer Hyper-V, la sessione remota di PowerShell copia i dischi di identità nell'archiviazione SMB. Quindi lo elimina dalla macchina Hyper-V.

La cartella del disco di identità viene ricreata se viene eliminata in modo che sia disponibile per il riutilizzo.

- **Download identity disks** (Scarica dischi di identità): come avviene nel caricamento, i dischi di identità passano attraverso il computer Hyper-V per giungere all'HCL. Il processo seguente crea una cartella che dispone solo delle autorizzazioni utente VMM sul server Hyper-V se non esiste.

  1. Il computer Hyper-V copia il disco dall'archiviazione SMB all'archiviazione Hyper-V locale tramite uno script PowerShell. Questo script viene eseguito nella sessione remota di PowerShell V3.
  2. L'HCL legge il disco dalla condivisione amministratore del computer Hyper-V in memoria.
  3. L'HCL elimina il file dalla condivisione amministratore.

## Passaggi successivi

- Se questo è il primo catalogo creato, Web Studio guida l'utente a creare gruppi di consegna
- Per rivedere l'intero processo di configurazione, vedere Installazione e configurazione
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di Microsoft System Center Virtual Machine Manager

## Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Connessione a Microsoft System Center Virtual Machine Manager
- Creare cataloghi di macchine

# Creare un catalogo di Nutanix

January 7, 2024

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti di virtualizzazione Nutanix.

> **Nota:**
>
> Prima di creare un catalogo di Nutanix, è necessario completare la creazione di una connessione a Nutanix. Vedere Connessione a Nutanix.

## Creare un catalogo di macchine utilizzando un'istantanea Nutanix

L'istantanea selezionata è il modello utilizzato per creare le macchine virtuali nel catalogo. Prima di creare il catalogo, creare immagini e istantanee in Nutanix. Per ulteriori informazioni, vedere la documentazione Nutanix.

Nella procedura guidata per la creazione del catalogo:

- Le pagine **Operating System** e **Machine Management** non contengono informazioni specifiche per Nutanix.
- La pagina **Container** o **Cluster and Container** è esclusiva di Nutanix.

  Se si distribuiscono macchine utilizzando Nutanix AHV XI come risorse, sarà visualizzata la pagina **Container**. Selezionare un contenitore in cui verranno posizionati i dischi di identità delle macchine virtuali.

  Se si distribuiscono macchine utilizzando Nutanix AHV Prism Central (PC) come risorse, sarà visualizzata la pagina **Cluster and Container**. Selezionare il cluster da utilizzare per la distribuzione delle macchine virtuali e quindi un contenitore.
- Nella pagina **Master Image** (Immagine master) selezionare l'istantanea dell'immagine. I nomi delle istantanee Acropolis devono avere il prefisso "XD_"per essere utilizzati in Citrix Virtual Apps and Desktops. Utilizzare la console Acropolis per rinominare le istantanee, se necessario. Se si rinominano le istantanee, riavviare la creazione guidata catalogo per visualizzare un elenco aggiornato.
- Nella pagina **Immagine master** (Macchine virtuali) indicare il numero di CPU virtuali e il numero di core per vCPU.
- Nella pagina **Network Cards** (Schede di rete), selezionare il tipo di NIC per filtrare le reti associate. Esistono due tipi di NIC: **VLAN** e **OVERLAY**. Selezionare una o più delle schede NIC

contenute nell'immagine master, quindi selezionare una rete virtuale associata per ciascuna scheda NIC.

- Le pagine **Machine Identities** (Identità macchina), **Domain Credentials** (Credenziali di dominio), **Credenziali di dominio** (Ambiti) e **Summary** (Riepilogo) non contengono informazioni specifiche di Nutanix.

### Limitazione

Quando si crea un catalogo MCS con una connessione host Nutanix (in particolare, il plug-in Nutanix AHV 2.7.1), le dimensioni del disco rigido delle VM fornite vengono visualizzate in modo errato in Web Studio. La dimensione visualizzata è molto inferiore (1 GB) rispetto alla dimensione di archiviazione reale (50 GB). La dimensione del disco rigido viene visualizzata correttamente sulla console Nutanix.

### Passaggi successivi

- Se questo è il primo catalogo creato, Web Studio guida l'utente a creare gruppi di consegna
- Per rivedere l'intero processo di configurazione, vedere Installazione e configurazione
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine

### Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Connessione a Nutanix
- Connessione alle soluzioni Nutanix Cloud e dei partner
- Creare cataloghi di macchine

## Creare un catalogo di VMware

January 7, 2024

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni coprono i dettagli specifici degli ambienti di virtualizzazione VMware.

> **Nota:**
>
> Prima di creare un catalogo di VMware, è necessario completare la creazione di una connessione a VMware. Vedere Connessione a VMware.

### Creare una macchina virtuale master

Utilizzare una macchina virtuale master per fornire desktop e applicazioni utente in un catalogo di macchine. Sul proprio hypervisor:

1. Installare un VDA nella macchina virtuale master, selezionando l'opzione di ottimizzazione del desktop, che migliora le prestazioni.
2. Creare un'istantanea della macchina virtuale master da utilizzare come backup.

> **Nota:**
>
> È possibile utilizzare MCS per effettuare il provisioning delle macchine virtuali nell'ambiente vSAN 8.0.

### Creare un catalogo di macchine utilizzando un profilo macchina

È possibile creare un catalogo di macchine MCS utilizzando un profilo macchina. L'origine dell'input del profilo della macchina è un modello VMware. Il profilo della macchina acquisisce le proprietà hardware da un modello VMware e le applica alle macchine virtuali di cui è appena stato effettuato il provisioning nel catalogo.

> **Nota:**
>
> - L'input dell'immagine master (istantanea) e l'input del profilo della macchina (modello VMware) devono essere entrambi abilitati o entrambi disabilitati da vTPM. Questa regola si applica sia a `New-ProvScheme` che a `Set-ProvScheme`.
> - Se l'immagine master è abilitata da vTPM, il modello VMware può provenire solo dalla stessa sorgente VM dell'immagine master.
> - Il criterio di archiviazione crittografata supporta solo la clonazione completa.

Il modello VMware presente nel profilo della macchina deve esistere durante il ciclo di vita del catalogo per consentire il provisioning delle macchine virtuali del catalogo. Senza un modello VMware, non è possibile effettuare il provisioning di nuove VM. Quando un modello VMware viene eliminato, è necessario fornire un nuovo modello utilizzando il comando `Set-ProvScheme`.

- MCS acquisisce le proprietà di un modello VMware. È possibile creare un nuovo modello VMware facendo riferimento alle proprietà archiviate del modello VMware utilizzando il comando Get-Provscheme.
- In alternativa, se sono presenti sia il catalogo delle macchine che le VM di cui è stato effettuato il provisioning, è possibile utilizzare anche una macchina con provisioning MCS per creare un nuovo modello VMware.

In base a diversi sistemi operativi, è possibile creare un catalogo macchine con diverse configurazioni:

- Se Windows 11 è installato sull'immagine master, è necessario che vTPM sia abilitato per l'immagine master. Pertanto, il modello VMware, che è un'origine del profilo della macchina, deve avere vTPM collegato.
- Se Windows 10 è installato sull'immagine master senza vTPM collegato, è possibile creare un catalogo di macchine con un modello VMware non vTPM come origine per il profilo della macchina.

Esiste un'altra configurazione in cui è possibile creare un catalogo di macchine utilizzando la modalità di copia completa del disco con un modello di profilo macchina applicato con criteri di archiviazione crittografati.

Per creare un catalogo di macchine utilizzando i comandi di PowerShell con il profilo macchina come input:

1. Aprire una finestra di **PowerShell**.
2. Eseguire `asnp citrix*`.
3. Eseguire i seguenti comandi:

    - Per creare un catalogo di macchine con il modello VMware allegato a vTPM come fonte per l'input del profilo della macchina e l'immagine master installata da Windows 11:

```
$identityPool = New-AcctIdentityPool  -IdentityPoolName "<
    string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "vSanRg"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
    snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\\<network name>.
    network" }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4
-VMMemoryMB 6144
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
    template name>.template" -TenancyType Shared
-FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
```

```
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9'
-Name "<catalog name>"
-ProvisioningType 'MCS'
-Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Per creare un catalogo di macchine con un modello VMware non vTPM come origine per il profilo della macchina e l'immagine master installata da Windows10:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###" -NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme
-CleanOnBoot -HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\\<string>.network
   " }

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
    -VMMemoryMB 8192
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
-TenancyType Shared  -FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
   ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Per creare un catalogo macchine utilizzando la modalità di copia completa del disco con modello di profilo macchina applicato con criteri di archiviazione crittografati:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme
-HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
    snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\\<string>.network
    " }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "
    XDHyp:\HostingUnits<hosting unit name><template name>.
    template"
-TenancyType Shared
-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"  -IsRemotePC $False
-MinimumFunctionalLevel 'L7_9'
-Name "<string>" -ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

Per aggiornare il profilo di una macchina, utilizzare il comando Set-ProvScheme. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
    -MachineProfile 'XDHyp:\HostingUnits<hosting unit name><template
    name>.template'
<!--NeedCopy-->
```

### Risoluzione dei problemi

Se il catalogo non viene creato, vedere CTX294978.

### Passaggi successivi

- Se questo è il primo catalogo creato, Web Studio guida l'utente a creare gruppi di consegna
- Per rivedere l'intero processo di configurazione, vedere Installazione e configurazione
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di VMware

### Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Connessione a VMware
- Creare cataloghi di macchine

## Creare cataloghi di diversi tipi di aggiunte

January 7, 2024

Utilizzando MCS, è possibile eseguire il provisioning di macchine come aggiunte ad AD locale o aggiunte ad Azure AD ibrido.

Per informazioni su come configurare le identità delle macchine in Web Studio, vedere Creare cataloghi delle macchine.

Per informazioni specifiche su come creare cataloghi uniti a identità di macchine, vedere quanto segue:

- Creare cataloghi aggiunti ad Azure Active Directory ibrido

## Creare cataloghi aggiunti ad Azure Active Directory ibrido

January 7, 2024

In questo articolo viene descritto come creare cataloghi aggiunti ad Azure Active Directory (AD) ibrido.

È possibile creare cataloghi uniti ad Azure AD utilizzando Web Studio o PowerShell.

Per informazioni su requisiti, limitazioni e considerazioni, vedere Aggiunto ad Azure Active Directory ibrido.

### Utilizzare Web Studio

Le seguenti informazioni sono un'aggiunta alle linee guida della sezione Creare cataloghi delle macchine. Per creare cataloghi aggiunti ad Azure AD ibrido, seguire le linee guida generali in quell'articolo, tenendo conto dei dettagli specifici per i cataloghi aggiunti ad Azure AD ibrido.

Nella procedura guidata per la creazione del catalogo:

- Nella pagina **Machine Identities** (Identità computer), selezionare **Hybrid Azure Active Directory joined** (Aggiunto ad Azure Active Directory ibrido). Le macchine create sono di proprietà di un'organizzazione e hanno effettuato l'accesso con un account Active Directory Domain Services appartenente a tale organizzazione. Esistono nel cloud e on-premise.

> **Nota:**
>
> Se si seleziona **Hybrid Azure Active Directory joined** (Aggiunto ad Azure Active Directory ibrido) come tipo di identità, ogni macchina del catalogo deve disporre di un account computer AD corrispondente.

### Utilizzare PowerShell

Di seguito sono riportati i passaggi di PowerShell equivalenti alle operazioni in Web Studio. Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

La differenza tra i cataloghi aggiunti ad AD locale e quelli aggiunti ad Azure AD ibrido sta nella creazione del pool di identità e degli account macchina.

Per creare un pool di identità insieme agli account per i cataloghi aggiunti ad Azure AD ibrido:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -
     Domain "corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -
     NamingScheme "HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU "CN=
     AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-d2f2-49
     d2-ab12-bae5bbd0df05"
2 New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
     -ADUserName "corp\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
     All -ADUserName "corp\admin1" -ADPassword $password
4 <!--NeedCopy-->
```

> **Nota:**
>
> `$password` è la password corrispondente per un account utente AD con autorizzazioni di scrittura.

Tutti gli altri comandi utilizzati per creare cataloghi aggiunti ad Azure AD ibrido sono gli stessi dei tradizionali cataloghi aggiunti ad AD locale.

### Visualizzare lo stato del processo di join di Azure AD ibrido

In Web Studio lo stato del processo di aggiunta ad Azure AD ibrido è visibile quando le macchine aggiunte ad Azure AD ibrido in un gruppo di consegna sono in stato di accensione. Per visualizzare lo stato, utilizzare Search (Cerca) per identificare tali macchine e quindi per ogni controllo **Machine Identity** (Identità macchina) nella scheda **Details** (Dettagli) nel riquadro inferiore. In **Machine Identity** (Identità macchina) possono essere visualizzate le seguenti informazioni:

- Aggiunto ad Azure AD ibrido
- Not yet joined to Azure AD (Non ancora aggiunta ad Azure AD)

> **Nota:**
>
> - Si potrebbe riscontrare un ritardo nell'aggiunta ad Azure AD ibrido alla prima accensione della macchina. Questo è causato dall'intervallo di sincronizzazione dell'identità della macchina predefinita (30 minuti di Azure AD Connect). La macchina si trova nello stato Hybrid Azure AD joined (Aggiunta ad Azure AD ibrido) solo dopo che le identità delle macchine sono state sincronizzate con Azure AD tramite Azure AD Connect
> - Se le macchine non si trovano nello stato Hybrid Azure AD joined (Aggiunta ad Azure AD ibrido), non vengono registrate con il Delivery Controller. Il loro stato di registrazione viene visualizzato come **Initialization** (Inizializzazione).

Inoltre, utilizzando Web Studio, è possibile scoprire perché le macchine non sono disponibili. A tale scopo, fare clic su una macchina nel nodo **Search** (Cerca), selezionare **Registration** (Registrazione) nella scheda **Details** (Dettagli) nel riquadro inferiore, quindi leggere la descrizione comando per ulteriori informazioni.

### Risoluzione dei problemi

Se l'aggiunta delle macchine ad Azure AD ibrido non va a buon fine, procedere come segue:

- Controllare se l'account della macchina è stato sincronizzato con Azure AD tramite il portale Microsoft Azure AD. Se è sincronizzato, viene visualizzato il messaggio **Not yet joined to Azure AD** (Non ancora aggiunta ad Azure AD), a indicare lo stato della registrazione in sospeso.

Per sincronizzare gli account delle macchine con Azure AD, assicurarsi che:

- L'account della macchina si trovi nell'unità organizzativa configurata per la sincronizzazione con Azure AD. Gli account macchina senza l'attributo **userCertificate** non vengono sincronizzati con Azure AD anche se si trovano nell'unità organizzativa configurata per la sincronizzazione.
- L'attributo **userCertificate** viene inserito nell'account della macchina. Utilizzare Active Directory Explorer per visualizzare l'attributo.
- Azure AD Connect deve essere stato sincronizzato almeno una volta dopo la creazione dell'account della macchina. In caso contrario, eseguire manualmente il comando `Start-ADSyncSyncCycle -PolicyType Delta` nella console PowerShell della macchina Azure AD Connect per attivare una sincronizzazione immediata.

- Verificare se la coppia di chiavi del dispositivo gestito da Citrix per il join di Azure AD ibrido è stata correttamente inviata alla macchina interrogando il valore di **DeviceKeyPairRestored** in **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix**.

  Verificare che il valore sia 1. In caso contrario, i possibili motivi sono:

  - `IdentityType` del pool di identità associato allo schema di provisioning non è impostato su `HybridAzureAD`. È possibile verificarlo eseguendo `Get-AcctIdentityPool`.
  - Il provisioning della macchina non viene eseguito utilizzando lo stesso schema di provisioning del catalogo delle macchine.
  - La macchina non è aggiunta al dominio locale. L'aggiunta a un dominio locale è un prerequisito del join di Azure AD ibrido.

- Controllare i messaggi diagnostici eseguendo il comando `dsregcmd /status /debug` sulla macchina di cui è stato eseguito il provisioning con MCS.

  Se il join di Azure AD ibrido ha esito positivo, **AzureAdJoined** e **DomainJoined** sono **YES** (Sì) nell'output della riga di comando.

  In caso contrario, fare riferimento alla documentazione di Microsoft per risolvere i problemi: https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current.

## Gestire i cataloghi di macchine

April 4, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

## Introduzione

È possibile aggiungere o rimuovere macchine da un catalogo di macchine, rinominare, modificare la descrizione o gestire gli account computer Active Directory di un catalogo.

La manutenzione dei cataloghi può anche includere la verifica che ogni computer disponga degli ultimi aggiornamenti del sistema operativo. Questi comprendono aggiornamenti degli antivirus, aggiornamenti del sistema operativo o modifiche alla configurazione.

- I cataloghi contenenti macchine casuali raggruppate create utilizzando Machine Creation Services (MCS) gestiscono le macchine aggiornando l'immagine master utilizzata nel catalogo e quindi aggiornando le macchine. Questo metodo consente di aggiornare in modo efficiente un gran numero di macchine utente.
- Per i cataloghi contenenti macchine statiche assegnate in modo permanente e per i cataloghi di macchine con accesso remoto al PC, è possibile gestire gli aggiornamenti alle macchine degli utenti al di fuori di Web Studio. Eseguire questa attività singolarmente o collettivamente utilizzando strumenti di distribuzione software di terze parti.

Per informazioni sulla creazione e la gestione delle connessioni agli hypervisor host, vedere Connessioni e risorse.

> **Nota:**
>
> MCS non supporta Windows 10 IoT Core e Windows 10 IoT Enterprise. Per ulteriori informazioni, fare riferimento al sito Microsoft.

### Informazioni sulle istanze persistenti

Quando si aggiorna un catalogo MCS creato utilizzando istanze permanenti o dedicate, tutte le nuove macchine create per il catalogo utilizzano l'immagine aggiornata. Le istanze preesistenti continuano a utilizzare l'istanza originale. Il processo di aggiornamento di un'immagine viene eseguito allo stesso modo per qualsiasi altro tipo di catalogo. Considerare quanto segue:

- Nel caso dei cataloghi dei dischi persistenti, le macchine preesistenti non vengono aggiornate alla nuova immagine, ma tutte le nuove macchine aggiunte al catalogo utilizzano la nuova immagine.

- Nel caso dei cataloghi di dischi non persistenti, l'immagine del computer viene aggiornata alla successiva reimpostazione del computer.
- Nel caso dei cataloghi di macchine persistenti, l'aggiornamento dell'immagine aggiorna anche le istanze del catalogo che la utilizzano.
- Nel caso dei cataloghi che non persistono, se si desidera utilizzare immagini diverse per macchine diverse, le immagini devono risiedere in cataloghi separati.

### Gestire i cataloghi di macchine

È possibile gestire un catalogo di macchine in due modi, come segue:

- Utilizzare Web Studio
- Utilizzare PowerShell

### Utilizzare Web Studio

Questa sezione descrive in dettaglio come gestire i cataloghi utilizzando Web Studio:

- Aggiungere macchine a un catalogo
- Eliminare macchine da un catalogo
- Modificare un catalogo
- Rinominare un catalogo
- Spostare un catalogo in una zona diversa
- Eliminare un catalogo
- Gestire gli account dei computer Active Directory in un catalogo
- Aggiornare un catalogo
- Cambiare il livello funzionale o annullare la modifica
- Clonare un catalogo
- Organizzare i cataloghi utilizzando le cartelle

### Aggiungere macchine a un catalogo

Prima di iniziare:

- Assicurarsi che l'host di virtualizzazione disponga di processori, memoria e archiviazione sufficienti per ospitare i computer aggiuntivi.
- Assicurarsi di disporre di un numero sufficiente di account computer Active Directory inutilizzati. Se si utilizzano account esistenti, il numero di computer che è possibile aggiungere è limitato dal numero di account disponibili.

- Se si utilizza Web Studio per creare account computer Active Directory per i computer aggiuntivi, è necessario disporre dell'autorizzazione di amministratore di dominio appropriata.

Per aggiungere macchine a un catalogo:

1. Accedere a Web Studio.
2. Selezionare **Machine Catalogs** nel riquadro a sinistra.
3. Selezionare un catalogo delle macchine, quindi selezionare **Add machines** (Aggiungi macchine) nella barra delle azioni.
4. Selezionare il numero di macchine virtuali da aggiungere.
5. Se gli account Active Directory esistenti non sono sufficienti per il numero di macchine virtuali che si stanno aggiungendo, selezionare il dominio e il percorso in cui vengono creati gli account. Specificare uno schema di denominazione degli account, utilizzando i marcatori hash per indicare dove compaiono numeri o lettere sequenziali. Non utilizzare una barra (/) in un nome di unità organizzativa. Un nome non può iniziare con un numero. Ad esempio, uno schema di denominazione PC-Vendite-## (in cui è selezionato 0-9) genera account computer denominati PC-Vendite-01, PC-Vendite-02, PC-Vendite-03 e così via.
6. Se si utilizzano account Active Directory esistenti, selezionare gli account oppure fare clic su **Import** e specificare un file CSV contenente i nomi di account. Assicurarsi che ci siano account sufficienti per tutte le macchine che si stanno aggiungendo. Web Studio gestisce questi account. Consentire a Web Studio di reimpostare le password per tutti gli account o specificare la password dell'account, che deve essere la stessa per tutti gli account.

Le macchine vengono create come processo in background e la creazione di molte macchine può richiedere molto tempo. La creazione delle macchine continua anche se si chiude Web Studio.

### Eliminare macchine da un catalogo

Dopo aver eliminato un computer da un catalogo di macchine, gli utenti non possono più accedervi, quindi prima di eliminare un computer, assicurarsi che si verifichino le seguenti condizioni:

- I dati utente sono stati sottoposti a backup o non sono più necessari.
- Tutti gli utenti sono disconnessi. L'attivazione della modalità di manutenzione impedisce la creazione di nuovi collegamenti a una macchina.
- Le macchine sono spente.

Per eliminare macchine da un catalogo:

1. Accedere a Web Studio.
2. Selezionare **Machine Catalogs** nel riquadro a sinistra.
3. Selezionare un catalogo, quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.

4. Selezionare una o più macchine, quindi selezionare **Delete** (Elimina) nella barra delle azioni.

Scegliere se eliminare le macchine che vengono rimosse. Se si sceglie di eliminare i computer, indicare se gli account di Active Directory per tali computer vengono mantenuti, disabilitati o eliminati.

### Modificare un catalogo

1. Nella pagina **Description** modificare la descrizione del catalogo.
2. Selezionare **Machine Catalogs** nel riquadro a sinistra.
3. Selezionare un catalogo, quindi selezionare **Edit Machine Catalog** (Modifica catalogo delle macchine) nella barra delle azioni.
4. Nella pagina **Scopes** (Ambiti), modificare gli ambiti.
5. È possibile che vengano visualizzate pagine aggiuntive a seconda del tipo di catalogo.

   Per i cataloghi creati utilizzando un'immagine di Azure Resource Manager, sono visibili le pagine seguenti. Tenere presente che le modifiche apportate si applicano solo alle macchine che verranno aggiunte al catalogo in un secondo momento. Le macchine esistenti rimangono invariate.

   - Nella pagina **Virtual Machines** (Macchine virtuali), modificare le dimensioni delle macchine e le zone di disponibilità in cui si desidera creare macchine.

     > **Nota:**
     >
     > – Sono mostrate solo le dimensioni delle macchine supportate dal catalogo.
     > – Se necessario, selezionare **Show only machine sizes used in other machine catalogs** (Mostra solo le dimensioni delle macchine utilizzate in altri cataloghi delle macchine) per filtrare l'elenco delle dimensioni delle macchine.

   - Nella pagina **Machine Profile** (Profilo macchina), scegliere se utilizzare o modificare un profilo macchina.
   - Nella pagina **License Types** (Tipi di licenza), scegliere se modificare l'impostazione delle licenze di Windows o di Linux.

   Per i cataloghi Remote PC Access (Accesso remoto PC), sono visibili le seguenti pagine:

   - Nella pagina **Power Management** (Gestione alimentazione), modificare le impostazioni di gestione dell'alimentazione e selezionare una connessione per il risparmio energia.
   - Nella pagina **Organizational Units** aggiungere o rimuovere le unità organizzative di Active Directory.

6. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e fare clic su **Save** (Salva) per uscire.

### Rinominare un catalogo

1. Accedere a Web Studio.
2. Selezionare **Machine Catalogs** nel riquadro a sinistra.
3. Selezionare un catalogo, quindi selezionare **Rename Machine Catalog** (Rinomina catalogo delle macchine) nella barra delle azioni.
4. Immettere il nuovo nome.

### Spostare un catalogo in una zona diversa

Se la distribuzione contiene più di una zona, è possibile spostare un catalogo da una zona all'altra.

Lo spostamento di un catalogo in una zona diversa, che non sia l'hypervisor contenente le macchine virtuali del catalogo, influisce sulle prestazioni.

1. Accedere a Web Studio.
2. Selezionare **Machine Catalogs** nel riquadro a sinistra.
3. Selezionare un catalogo, quindi selezionare **Move** (Sposta) nella barra delle azioni.
4. Selezionare la zona in cui si desidera spostare il catalogo.

### Eliminare un catalogo

Prima di eliminare un catalogo, assicurarsi che si verifichino le seguenti condizioni:

- Tutti gli utenti sono disconnessi e non sono in esecuzione sessioni disconnesse.
- La modalità di manutenzione è attivata per tutte le macchine del catalogo, in modo che non sia possibile effettuare nuove connessioni.
- Tutte le macchine nel catalogo sono spente.
- Il catalogo non è associato a un gruppo di consegna. In altre parole, il gruppo di consegna non contiene macchine del catalogo.

Per eliminare un catalogo:

1. Accedere a Web Studio.
2. Selezionare **Machine Catalogs** nel riquadro a sinistra.
3. Selezionare un catalogo, quindi selezionare **Delete Machine Catalog** (Elimina catalogo delle macchine) nella barra delle azioni.
4. Indicare se le macchine incluse nel catalogo vengono eliminate. Se si sceglie di eliminare i computer, indicare se gli account computer di Active Directory per tali macchine vengono mantenuti, disabilitati o eliminati.

### Gestire gli account dei computer Active Directory in un catalogo

Per gestire gli account Active Directory in un catalogo di macchine, è possibile:

- Liberare gli account macchina inutilizzati rimuovendo gli account computer Active Directory dai cataloghi di sistemi operativi a sessione singola e multisessione. Questi account possono quindi essere utilizzati per altre macchine.
- Aggiungere account in modo che quando più computer vengono aggiunti al catalogo, gli account computer siano già presenti. Non utilizzare una barra (/) in un nome di unità organizzativa.

Per gestire gli account Active Directory:

1. Accedere a Web Studio.
2. Selezionare **Machine Catalogs** nel riquadro a sinistra.
3. Selezionare un catalogo e quindi selezionare **Manage AD accounts** (Gestisci account AD) nella barra delle azioni.
4. Scegliere se aggiungere o eliminare account computer. Se si aggiungono account, specificare cosa fare con le password degli account: reimpostarle tutte o immettere una password valida per tutti gli account.

   È possibile reimpostare le password se non si conoscono le password dell'account correnti; è necessario disporre dell'autorizzazione per eseguire la reimpostazione delle password. Quando si immette una password, la password viene modificata negli account man mano che vengono importati. Quando si elimina un account, scegliere se l'account in Active Directory viene mantenuto, disattivato o eliminato.

Indicare se gli account di Active Directory vengono mantenuti, disattivati o eliminati quando si rimuovono macchine da un catalogo o si elimina un catalogo.

### Aggiornare un catalogo

Consigliamo di salvare copie o istantanee delle immagini master prima di aggiornare le macchine incluse nel catalogo. Il database conserva una cronologia delle immagini master utilizzate con ogni catalogo macchine. Eseguire il rollback o ripristinare le macchine di un catalogo per utilizzare la versione precedente dell'immagine master. Eseguire questa attività se gli utenti riscontrano problemi con gli aggiornamenti distribuiti sui loro desktop. Ciò riduce al minimo i tempi di inattività dell'utente. Non eliminare, spostare o rinominare le immagini master. Non è possibile ripristinare un catalogo per utilizzarle.

Dopo l'aggiornamento, il computer viene riavviato automaticamente.

### Aggiornare o creare un'immagine master

Prima di aggiornare il catalogo delle macchine, aggiornare un'immagine master esistente o crearne una nell'hypervisor host.

1. Nell'hypervisor, scattare un'istantanea della macchina virtuale corrente e assegnare all'istantanea un nome significativo. Questa istantanea può essere utilizzata per ripristinare (rollback) le macchine incluse nel catalogo, se necessario.
2. Se necessario, accendere l'immagine master ed effettuare l'accesso.
3. Installare gli aggiornamenti o apportare le modifiche necessarie all'immagine master.
4. Spegnere la macchina virtuale.
5. Creare un'istantanea della macchina virtuale. Assegnare un nome significativo che venga riconosciuto quando il catalogo viene aggiornato in Web Studio. Sebbene Web Studio sia in grado di creare un'istantanea, Citrix consiglia di crearla utilizzando la console di gestione dell'hypervisor. Quindi selezionare l'istantanea in Web Studio. Questo processo consente di fornire un nome e una descrizione significativi anziché un nome generato automaticamente. Per le immagini master GPU, è possibile modificare l'immagine master solo tramite la console Citrix Hypervisor.

### Cambiare l'immagine master

Per preparare l'aggiornamento e implementarlo in tutte le macchine di un catalogo:

1. Accedere a Web Studio.
2. Selezionare **Machine Catalogs** nel riquadro a sinistra.
3. Selezionare un catalogo, quindi selezionare **Change Master Image** (Cambia immagine master) nella barra delle azioni.
4. Nella pagina **Master Image** (Immagine master), selezionare l'host e l'immagine che si desidera implementare.

> **Suggerimento:**
>
> Per un catalogo creato da MCS, è possibile annotarne l'immagine aggiungendo una nota per l'immagine. Una nota può contenere fino a 500 caratteri. Ogni volta che si modifica l'immagine master, viene creata una voce correlata alla nota se si aggiunge una nota. Se si aggiorna un catalogo senza aggiungere una nota, la voce viene visualizzata come null (-). Per visualizzare la cronologia delle note per l'immagine, selezionare il catalogo, fare clic su **Template Properties** (Proprietà modello) nel riquadro inferiore e quindi fare clic su **View note history** (Visualizza cronologia note).

5. Nella pagina **Rollout Strategy** (Strategia di rollout) scegliere quando le macchine nel catalogo macchine devono essere aggiornate con la nuova immagine master: al successivo spegnimento o immediatamente.

   > **Nota:**
   >
   > La pagina **Rollout Strategy** non è disponibile per le VM persistenti perché il rollout è applicabile solo alle VM non persistenti.

6. Verificare le informazioni nella pagina **Summary** e quindi fare clic su **Finish**. Ogni macchina si riavvia automaticamente dopo l'aggiornamento.

Per tenere traccia dello stato di avanzamento dell'aggiornamento, individuare il catalogo in **Machine Catalogs** (Cataloghi delle macchine) per visualizzare la barra di avanzamento in linea e il grafico di avanzamento dettagliato.

Quando si aggiorna un catalogo utilizzando direttamente PowerShell SDK anziché Web Studio, specificare un modello di hypervisor (**VMTemplates**). Usalo come alternativa a un'immagine o a un'istantanea di un'immagine.

**Strategia di rollout:**

L'aggiornamento dell'immagine al successivo arresto avrà effetto immediato su tutti i computer non attualmente in uso, ovvero i computer che non hanno una sessione utente attiva. Un sistema in uso riceve l'aggiornamento al termine della sessione attiva corrente. Considerare quanto segue:

- Le nuove sessioni non possono essere avviate fino al completamento dell'aggiornamento sui computer applicabili.
- Le macchine con sistema operativo a sessione singola vengono immediatamente aggiornate quando la macchina non è in uso o quando gli utenti non hanno effettuato l'accesso.
- In un sistema operativo multisessione, i riavvii non vengono eseguiti automaticamente. Le macchine devono essere spente e riavviate manualmente.

> **Suggerimento:**
>
> Limitare il numero di macchine da riavviare utilizzando le impostazioni avanzate per una connessione host. Utilizzare queste impostazioni per modificare le azioni eseguite in un determinato catalogo. Le impostazioni avanzate variano a seconda dell'hypervisor.

Se si desidera abilitare la pianificazione di riavvio una tantum utilizzando PowerShell, vedere Abilitare la pianificazione del riavvio una tantum.

### Rollback dell'immagine master

Dopo aver distribuito un'immagine master aggiornata o nuova, è possibile eseguire il rollback. Questo processo potrebbe essere necessario se si verificano problemi nei computer appena aggior-

nati. Quando si esegue il rollback, le macchine incluse nel catalogo vengono ripristinate all'ultima immagine funzionante. Tutte le nuove funzionalità che richiedono l'immagine più recente non sono più disponibili. Come per il rollout, il rollback di un computer include un riavvio.

1. Accedere a Web Studio.
2. Selezionare **Machine Catalogs** nel riquadro a sinistra.
3. Selezionare il catalogo, quindi selezionare **Roll Back Master Image** (Esegui il rollback dell'immagine master) nella barra delle azioni.
4. Specificare quando applicare l'immagine master precedente alle macchine, come descritto nella sezione precedente per l'operazione di rollout.

Il rollback viene applicato solo alle macchine che devono essere ripristinate. I computer che non sono aggiornati con l'immagine master nuova o aggiornata non ricevono messaggi di notifica e non sono obbligati a scollegarsi.

Per tenere traccia dell'avanzamento del rollback, individuare il catalogo in **Machine Catalogs** (Cataloghi delle macchine) per visualizzare la barra di avanzamento in linea e il grafico di avanzamento dettagliato.

### Cambiare il livello funzionale o annullare la modifica

Modificare il livello funzionale del catalogo di macchine dopo l'aggiornamento dei VDA sui computer a una versione più recente. Citrix consiglia di aggiornare tutti i VDA alla versione più recente per consentire l'accesso a tutte le funzionalità più recenti.

Prima di modificare il livello funzionale di un catalogo di macchine:

- Avviare le macchine aggiornate in modo che si registrino con il Controller. Questo processo consente a Web Studio di determinare che le macchine nel catalogo devono essere aggiornate.

Per modificare il livello funzionale di un catalogo:

1. Accedere a Web Studio.
2. Selezionare **Machine Catalogs** nel riquadro a sinistra.
3. Selezionare il catalogo. La scheda **Details** nel riquadro inferiore visualizza le informazioni sulla versione.
4. Selezionare **Change Functional Level** (Cambia livello funzionale). Se Web Studio rileva che il catalogo deve essere aggiornato, viene visualizzato un messaggio. Seguire le istruzioni. Se uno o più computer non possono essere aggiornati, viene visualizzato un messaggio che ne spiega il motivo. Per garantire che tutte le macchine funzionino correttamente, Citrix consiglia di risolvere i problemi delle macchine prima di fare clic su **Change** per procedere.

Al termine della modifica del catalogo, è possibile ripristinare le versioni VDA precedenti delle macchine selezionando il catalogo e quindi selezionando **Undo Functional Level Change** (Annulla modifica di livello funzionale) nella barra delle azioni.

### Clonare un catalogo

Prima di clonare un catalogo, tenere presente quanto segue:

- Non è possibile modificare le impostazioni associate al sistema operativo e alla gestione della macchina. Il catalogo clonato eredita tali impostazioni dall'originale.
- Il completamento della clonazione di un catalogo può richiedere del tempo. Se necessario, selezionare **Hide progress** (Nascondi avanzamento) per eseguire la clonazione in background.
- Il catalogo clonato eredita il nome dell'originale e ha un suffisso `Copy`. È possibile modificare il nome. Vedere Rinominare un catalogo.
- Al termine della clonazione, accertarsi di assegnare il catalogo clonato a un gruppo di consegna.

1. Accedere a Web Studio, quindi selezionare **Machine Catalogs** nel riquadro a sinistra.
2. Selezionare un catalogo, quindi selezionare **Clone** (Clona) nella barra delle azioni.
3. Nella finestra **Clone Selected Machine Catalog** (Clona catalogo delle macchine selezionato), visualizzare le impostazioni per il catalogo clonato e configurare le impostazioni a seconda dei casi. Selezionare **Next** (Avanti) per passare alla pagina successiva.
4. Nella pagina **Summary** (Riepilogo), visualizzare un riepilogo delle impostazioni e selezionare **Finish** (Fine) per avviare la clonazione.
5. Se necessario, selezionare **Hide progress** (Nascondi avanzamento) per eseguire la clonazione in background.

### Organizzare i cataloghi utilizzando le cartelle

È possibile creare cartelle per organizzare i cataloghi per un facile accesso. Ad esempio, è possibile organizzare i cataloghi per tipo di immagine o per struttura organizzativa.

#### Creare una cartella del catalogo

Prima di iniziare, pianificare come organizzare i cataloghi. Considerare quanto segue:

- È possibile nidificare le cartelle fino a cinque livelli di profondità (esclusa la cartella principale predefinita).
- Una cartella del catalogo può contenere cataloghi e sottocartelle.
- Tutti i nodi in Web Studio (come i nodi **Machine Catalogs** e **Applications**) condividono un albero delle cartelle nel backend. Per evitare conflitti di nomi con altri nodi durante la ridenominazione

o lo spostamento di cartelle, si consiglia di assegnare nomi diversi alle cartelle di primo livello in nodi diversi.

Per creare una cartella del catalogo, effettuare le seguenti operazioni:

1. Selezionare **Machine Catalogs** nel riquadro a sinistra.
2. Nella gerarchia delle cartelle, selezionare una cartella e quindi selezionare **Create Folder** (Crea cartella) nella barra **Actions** (Azioni).
3. Immettere un nome per la nuova cartella, quindi fare clic su **Done** (Fine).

> **Suggerimento:**
>
> Se si crea una cartella in una posizione non prevista, è possibile trascinarla nella posizione corretta.

#### Spostare un catalogo

È possibile spostare un catalogo tra le cartelle. I passaggi dettagliati sono i seguenti:

1. Selezionare **Machine Catalogs** nel riquadro a sinistra.
2. Visualizzare i cataloghi in base alla cartella. È anche possibile attivare **View all** (Visualizza tutto) sopra la gerarchia delle cartelle per visualizzare tutti i cataloghi contemporaneamente.
3. Fare clic con il pulsante destro del mouse su un catalogo e selezionare **Move Machine Catalog** (Sposta catalogo delle macchine).
4. Selezionare la cartella in cui si desidera spostare il catalogo e quindi fare clic su **Done** (Fine).

> **Suggerimento:**
>
> È possibile trascinare un catalogo in una cartella.

#### Gestire le cartelle di un catalogo

È possibile eliminare, rinominare e spostare le cartelle del catalogo.

È possibile eliminare una cartella solo se tale cartella e le relative sottocartelle non contengono cataloghi.

Per gestire una cartella, effettuare le seguenti operazioni:

1. Selezionare **Machine Catalogs** nel riquadro a sinistra.
2. Nella gerarchia delle cartelle, selezionare una cartella, quindi selezionare un'azione nella barra **Actions** (Azioni) in base alle esigenze:
    - Per rinominare la cartella, selezionare **Rename Folder** (Rinomina cartella).

- Per eliminare la cartella, selezionare **Delete Folder** (Elimina cartella).
- Per spostare la cartella, selezionare **Move Folder** (Sposta cartella).

3. Seguire le istruzioni sullo schermo per completare i passaggi rimanenti.

### Utilizzare PowerShell

Questa sezione descrive in dettaglio come gestire i cataloghi utilizzando PowerShell:

- Recuperare gli avvisi e gli errori associati a un catalogo
- Abilitare la pianificazione del riavvio una tantum
- Aggiungere descrizioni a un'immagine
- Reimpostare il disco del sistema operativo
- Modificare le impostazioni di rete per uno schema di provisioning esistente

### Recuperare gli avvisi e gli errori associati a un catalogo

È possibile visualizzare la cronologia degli errori e degli avvisi per comprendere i problemi del catalogo delle macchine MCS e risolverli.

Utilizzando i comandi PowerShell, è possibile:

- Ottenere un elenco di errori o avvisi
- Cambiare lo stato di avviso da **New** (Nuovo) ad **Acknowledged** (Riconosciuto)
- Eliminare gli errori o gli avvisi

Per eseguire i comandi PowerShell:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.

Per ottenere un elenco di errori e avvisi:

Eseguire il comando `Get-ProvOperationEvent`.

- Senza parametri: si ricevono tutti gli errori e gli avvisi
- Con i parametri `LinkedObjectType` e `LinkedObjectUid`: si ricevono tutti gli errori e gli avvisi associati a uno schema di provisioning specifico
- Con il parametro `EventId`: si riceve un errore o un avviso specifico che corrisponde a questo ID evento
- Con il parametro `Filter`: si ricevono errori o avvisi tramite un filtro personalizzato

Per modificare lo stato degli errori o degli avvisi da **New** (Nuovo) ad **Acknowledged** (Riconosciuto):

Eseguire il comando `Confirm-ProvOperationEvent`.

- Con il parametro`EventId`: imposta lo stato di un errore o di un avviso specifico che corrisponde a questo ID evento. È possibile ottenere l'`EventId` di un errore o un avviso specifico come uscita dal comando `Get-ProvOperationEvent`
- Con i parametri `LinkedObjectType` e `LinkedObjectUid`: imposta lo stato di tutti gli errori e gli avvisi associati a uno schema di provisioning specifico
- Con il parametro `All`: imposta lo stato di tutti gli avvisi come **Acknowledged**.

Per eliminare gli errori o gli avvisi:

Eseguire il comando `Remove-ProvOperationEvent`.

- Con il parametro `EventId`: rimuove un errore o un avviso specifico che corrisponde a questo ID evento. È possibile ottenere l'`EventId` di un errore o un avviso specifico come uscita dal comando `Get-ProvOperationEvent`
- Con i parametri `LinkedObjectType` e `LinkedObjectUid`: rimuove tutti gli errori e gli avvisi associati a uno schema di provisioning specifico
- Con il parametro `All`: rimuove tutti gli errori e gli avvisi

Per ulteriori informazioni, vedere Citrix PowerShell SDK.

### Abilitare la pianificazione del riavvio una tantum

Se si desidera abilitare la pianificazione di riavvio una tantum mediante PowerShell, utilizzare i comandi PowerShell `BrokerCatalogRebootSchedule` per creare, modificare ed eliminare una pianificazione di riavvio:

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- Remove-BrokerCatalogRebootSchedule
- Rename-BrokerCatalogRebootSchedule

Ad esempio,

- Per creare un programma di riavvio delle macchine virtuali nel catalogo denominato **BankTellers** a partire dal 3 febbraio 2022, tra le 2:00 e le 4:00.

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -
    CatalogName BankTellers  -StartDate "2022-02-03" -StartTime "
    02:00" -Enabled $true -RebootDuration 120
<!--NeedCopy-->
```

- Per creare una pianificazione di riavvio delle macchine virtuali del catalogo con UID 17 a partire dal 3 febbraio 2022, tra l'1:00 e le 5:00. Dieci minuti prima del riavvio, ogni macchina virtuale è impostata per visualizzare una finestra di messaggio con il titolo "**WARNING: Reboot pending**"

(ATTENZIONE: riavvio in sospeso) e il messaggio "**Save your work**"(Salvare il lavoro) in ogni sessione utente.

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot' -
    CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -
    Enabled $true -RebootDuration 240 -WarningTitle "WARNING:
    Reboot pending" -WarningMessage "Save your work" -
    WarningDuration 10
<!--NeedCopy-->
```

- Per rinominare la pianificazione di riavvio del catalogo denominata **Old Name** in **New Name**.

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -
    NewName "New Name"
<!--NeedCopy-->
```

- Per visualizzare tutte le pianificazioni di riavvio del catalogo con UID 1, quindi rinominare la pianificazione di riavvio del catalogo con l'UID 1 in **Nuovo nome**.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
    BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
<!--NeedCopy-->
```

- Per impostare la pianificazione di riavvio del catalogo denominata **Accounting** in modo da visualizzare una finestra di messaggio con il titolo **WARNING: Reboot pending** (ATTENZIONE: riavvio in sospeso) e il messaggio **Save your work** (Salvare il lavoro) dieci minuti prima del riavvio di ciascuna macchina virtuale. Il messaggio viene visualizzato in ogni sessione utente su quella macchina virtuale.

  "'

  C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage "Save your work"-WarningDuration 10 -WarningTitle "WARNING: Reboot pending"

- Per visualizzare tutte le pianificazioni di riavvio disattivate e quindi abilitare tutte le pianificazioni di riavvio disattivate.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
    BrokerCatalogRebootSchedule -Enabled $true
<!--NeedCopy-->
```

- Per impostare la pianificazione del riavvio del catalogo con UID 17 in modo da visualizzare il messaggio **Rebooting in %m% minutes** (Riavvio in %m% minuti) quindici, dieci e cinque minuti prima del riavvio di ogni macchina virtuale.

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "
    Rebooting in %m% minutes." -WarningDuration 15 -
    WarningRepeatInterval 5
<!--NeedCopy-->
```

- Per configurare il fuso orario per il catalogo denominato **MyCatalog**.

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
<!--NeedCopy-->
```

### Aggiungere descrizioni a un'immagine

È possibile aggiungere descrizioni informative sulle modifiche correlate agli aggiornamenti delle immagini per i cataloghi delle macchine. Utilizzare questa funzionalità per aggiungere una descrizione durante la creazione di un catalogo o quando si aggiorna un'immagine master esistente per un catalogo. È inoltre possibile visualizzare le informazioni per ogni immagine master del catalogo. Utilizzare i seguenti comandi per aggiungere o visualizzare le descrizioni delle immagini:

- Per aggiungere una nota durante la creazione di un catalogo di macchine con un'immagine master, utilizzare il parametro `MasterImageNote` nel comando `NewProvScheme`. Ad esempio:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -
    HostingUnitName <name> -IdentityPoolName <name> -MasterImageVM
XDHyp:\HostingUnits<hosting unit name><vm name>.vm\Base.snapshot
    -MasterImageNote "Note"
<!--NeedCopy-->
```

- Per aggiornare l'immagine master associata a un catalogo di macchine, utilizzare il parametro `MasterImageNote` nel comando `Publish-ProvMasterVMImage`. Ad esempio:

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name> -
    MasterImageVM XDHyp:\HostingUnits<hosting unit name><vm name>.
    vm\base.snapshot -MasterImageNote "Note"
<!--NeedCopy-->
```

- Per visualizzare le informazioni di ogni immagine, utilizzare il comando Get-ProvSchemeMasterVMImageHist
  Ad esempio:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
    MyScheme -Showall
<!--NeedCopy-->
```

Per tenere traccia dell'avanzamento del rollback, individuare il catalogo in **Machine Catalogs** (Cataloghi delle macchine) per visualizzare la barra di avanzamento in linea e il grafico di avanzamento dettagliato.

Non è possibile eseguire il rollback in alcuni scenari, inclusi i seguenti (l'opzione **Roll Back Master Image** non è visibile)

- Non si ha il permesso di eseguire il rollback.
- Il catalogo non è stato creato utilizzando MCS.
- Il catalogo è stato creato utilizzando un'immagine del disco del sistema operativo.
- La snapshot utilizzata per creare il catalogo è danneggiata.

- Le modifiche apportate dall'utente alle macchine nel catalogo non sono persistenti.
- Le macchine nel catalogo sono in esecuzione.

### Reimpostare il disco del sistema operativo

Utilizzare il comando PowerShell `Reset-ProvVMDisk` per reimpostare il disco del sistema operativo di una macchina virtuale persistente in un catalogo di macchine creato da MCS. Attualmente, questa funzionalità è applicabile ad Azure, Citrix Hypervisor, Google Cloud. Ambienti di virtualizzazione VMware e SCVMM.

Per eseguire correttamente il comando PowerShell, assicurarsi che sussistano le seguenti condizioni:

- Le VM di destinazione si trovano in un catalogo MCS persistente.
- Il catalogo macchine MCS funziona correttamente.
- Ciò implica che lo schema di provisioning e l'host esistono e che lo schema di provisioning contiene le voci corrette.
- L'hypervisor non è in modalità di manutenzione.
- Le VM di destinazione sono spente e in modalità manutenzione.

Effettuare le seguenti operazioni per ripristinare il disco del sistema operativo:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando **asnp citrix*** per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire il comando PowerShell `Reset-ProvVMDisk` in uno dei seguenti modi:
   - Specificare l'elenco delle VM sotto forma di elenco separato da virgole ed eseguire il ripristino su ciascuna VM:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc"
         ,"def") -OS
     <!--NeedCopy-->
     ```

   - Specificare l'elenco di VM come output dal comando `Get-ProvVM` ed eseguire il ripristino su ciascuna VM:

     ```
     (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk
         "abc" -OS
     <!--NeedCopy-->
     ```

   - Specificare una singola VM per nome:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS
     <!--NeedCopy-->
     ```

- Creare attività di ripristino separate per ciascuna delle VM restituite dal comando `Get-ProvVM`. Questo metodo è meno efficiente perché ogni attività eseguirà gli stessi controlli ridondanti, quali il controllo della capacità dell'hypervisor e il controllo della connessione per ogni VM.

```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -OS
<!--NeedCopy-->
```

4. Viene visualizzato un prompt di conferma che elenca le VM da reimpostare insieme a un messaggio di avviso che indica che si tratta di un'operazione irreversibile. Se non si fornisce una risposta e si preme **Invio**, non vengono eseguite altre azioni.

> **Nota:**
>
> Non togliere le VM dalla modalità di manutenzione né accenderle fino al completamento del processo di ripristino.

È possibile eseguire il comando PowerShell `-WhatIf` per stampare l'azione che eseguirebbe e uscire senza eseguirla.

È anche possibile ignorare la richiesta di conferma utilizzando uno dei seguenti metodi:

- Fornire il parametro `-Force`:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Force
<!--NeedCopy-->
```

- Fornire il parametro `-Confirm:$false`:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Confirm:$false
<!--NeedCopy-->
```

- Prima di eseguire `Reset-ProvVMDisk`, modificare `$ConfirmPreference` su **None**:

```
PS C:\Windows\system32> $ConfirmPreference='None'
PS C:\Windows\system32> $ConfirmPreference
None
PS C:\Windows\system32> Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -VMName "abc" -OS
<!--NeedCopy-->
```

5. Eseguire `Get-ProvTask` per ottenere lo stato delle attività restituite dal comando `Reset-ProvVMDisk`.

### Modificare le impostazioni di rete per uno schema di provisioning esistente

È possibile modificare l'impostazione di rete per uno schema di provisioning esistente in modo che le nuove macchine virtuali vengano create nella nuova sottorete. Utilizzare il parametro `-NetworkMapping` nel comando `Set-ProvScheme` per modificare l'impostazione di rete.

> **Nota:**
>
> Questa funzionalità è supportata su Citrix Virtual Apps and Desktops 2203 LTSR CU3 e versioni successive.

Per modificare l'impostazione di rete per uno schema di provisioning esistente, procedere come segue:

1. Nella finestra di PowerShell, eseguire il comando `asnp citrix*` per caricare i moduli di PowerShell.
2. Eseguire `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` per accedere al percorso di rete che si desidera modificare.
3. Assegnare una variabile alla nuova impostazione di rete. Ad esempio:

```
$NewNetworkMap = @{
 "0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }

<!--NeedCopy-->
```

4. Eseguire `Set-ProvScheme -ProvisioningSchemeName "name"-NetworkMapping $NewNetworkMap`.
5. Eseguire `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` per verificare la nuova impostazione di rete per lo schema di provisioning esistente.

### Risoluzione dei problemi

- Per le macchine con stato "Stato di alimentazione sconosciuto", vedere CTX131267 per istruzioni.
- Per correggere le macchine virtuali che mostrano continuamente uno stato di alimentazione sconosciuto, vedere Come correggere le macchine virtuali che mostrano continuamente uno stato di alimentazione sconosciuto.

### Passaggi successivi

Per informazioni sulla gestione di cataloghi di servizi cloud specifici, vedere:

- Gestire un catalogo AWS
- Gestire un catalogo di Citrix Hypervisor
- Gestire un catalogo Google Cloud Platform
- Gestire un catalogo di Microsoft Azure
- Gestire un catalogo di Microsoft System Center Virtual Machine Manager
- Gestire un catalogo VMware

## Gestire un catalogo di AWS

January 7, 2024

In Gestire i cataloghi delle macchine sono descritte le procedure guidate per la gestione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud AWS.

> **Nota:**
>
> Prima di gestire un catalogo di AWS, è necessario completare la creazione di un catalogo di AWS. Vedere Creare un catalogo di AWS.

### Identificare le risorse create da MCS

Di seguito sono riportati i tag che MCS aggiunge alle risorse. I tag nella tabella sono rappresentati come "key":"value".

| Nome della risorsa | Tag |
|---|---|
| Disco ID | "Name": "VMName_IdentityDisk"<br>"XdConfig": "XdProvisioned=true"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Immagine | "XdConfig": "XdProvisioned=true"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| NIC | "Description": "XD NIC"<br>"XdConfig": "XdProvisioned=true"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco del sistema operativo | "Name": "VMName_rootDisk" |

| Nome della risorsa | Tag |
| --- | --- |
| | “XdConfig”: “XdProvisioned=true” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “Citrix Resource”: “” [quando AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| PrepVM | “Name”: “Preparation - CatalogName - xxxxxxxxxx” “XdConfig”: “XdProvisioned=true” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “Citrix Resource”: “” [quando AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| Snapshot pubblicata | “XdConfig”: “XdProvisioned=true” |
| | Se non si tratta di una snapshot per l’AMI Volume Worker, allora “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] |
| Modello | “XdConfig”: “XdProvisioned=true” [quando AwsCaptureInstanceProperties = true] “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “CitrixResource”: “” [quando AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| Macchina virtuale nel catalogo | “XdConfig”: “XdProvisioned=true” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “CitrixResource”: “” |

| Nome della risorsa | Tag |
| --- | --- |
| | [quando AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:id”:”lt-xxxx” [quando AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:version”: “n” [quando AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| AMI Volume Worker | “XdConfig”: “XdProvisioned=true” |
| Bootstraper Volume Worker | “Name”: “XenDesktop Temp” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixVolumeWorkerBootstrapper”: “” |
| Istanza di Volume Worker | “Name”: “Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx” “XdConfig”: “XdProvisioned=true” |

### Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Connessione ad AWS
- Creare cataloghi di macchine
- Creare un catalogo di AWS
- Gestire i cataloghi delle macchine

## Gestire un catalogo di Citrix Hypervisor

January 7, 2024

In Gestire i cataloghi delle macchine sono descritte le procedure guidate per la gestione di un catalogo di macchine. Le seguenti informazioni coprono i dettagli specifici degli ambienti di virtualizzazione Citrix Hypervisor.

> **Nota:**
>
> Prima di gestire un catalogo di Citrix Hypervisor, è necessario completare la creazione di un catalogo Citrix Hypervisor. Vedere Creare un catalogo di Citrix Hypervisor.

### Identificare le risorse create da MCS

Di seguito sono riportati i tag che MCS aggiunge alle risorse. I tag nella tabella sono rappresentati come "key":"value".

| Nome della risorsa | Tag |
|---|---|
| Disco di base pubblicato e relativa copia su ogni rete o archivio locale | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco ID | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco del sistema operativo | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Preparare una macchina virtuale | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Macchina virtuale nel catalogo | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco WBC | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |

### Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Connessione a Citrix Hypervisor
- Creare cataloghi di macchine
- Creare un catalogo di Citrix Hypervisor
- Gestire i cataloghi delle macchine

## Gestisci un catalogo di Google Cloud Platform

January 7, 2024

In Gestire i cataloghi delle macchine sono descritte le procedure guidate per la gestione di un catalogo di macchine. Le seguenti informazioni coprono i dettagli specifici degli ambienti cloud di Google.

> **Nota:**
>
> Prima di gestire un catalogo di Google Cloud Platform, è necessario completare la creazione di un catalogo di Google Cloud Platform. Vedere Creare un catalogo di Google Cloud Platform.

### Gestire un catalogo di macchine

Per aggiungere macchine a un catalogo, aggiornare le macchine ed eseguire il rollback di un aggiornamento, vedere Gestire i cataloghi delle macchine.

### Gestione dell'alimentazione

Citrix DaaS consente la gestione dell'alimentazione delle macchine Google Cloud. Utilizzare il nodo **Search** (Cerca) nel riquadro a sinistra per individuare la macchina di cui si desidera gestire l'alimentazione. Sono disponibili le seguenti azioni per l'alimentazione:

- Delete (Elimina)
- Start (Avvia)
- Restart (Riavvia)
- Force Restart (Forza riavvio)
- Shut Down (Arresta)
- Force Shutdown (Imponi arresto)
- Add to Delivery Group (Aggiungi al gruppo di consegna)
- Manage Tags (Gestisci tag)
- Turn On Maintenance Mode (Attiva la modalità di manutenzione)

È anche possibile gestire l'alimentazione delle macchine Google Cloud utilizzando Autoscale (Scalabilità automatica). A tale scopo, aggiungere le macchine Google Cloud a un gruppo di consegna e abilitare la scalabilità automatica per tale gruppo. Per ulteriori informazioni sulla scalabilità automatica, consultare Scalabilità automatica.

#### Aggiornare i computer sottoposti a provisioning utilizzando PowerShell

Il comando `Set-ProvScheme` modifica lo schema di provisioning. Tuttavia, non influisce sulle macchine esistenti. Utilizzando il comando `Set-ProvVMUpdateTimeWindow` di PowerShell, è ora possibile applicare lo schema di provisioning corrente a una macchina o a un set di macchine esistente persistente o non persistente. Attualmente, in GCP, l'aggiornamento delle proprietà supportato da questa funzionalità è il profilo del computer.

È possibile aggiornare:

- Una singola macchina virtuale
- Un elenco di macchine virtuali specifiche o di tutte le macchine virtuali esistenti associate a un ID di schema di provisioning
- Un elenco di macchine virtuali specifiche o di tutte le macchine virtuali esistenti associate a un nome di uno schema di provisioning

Per aggiornare le macchine virtuali esistenti:

1. Verificare la configurazione delle macchine esistenti. Ad esempio,

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Aggiornare lo schema di provisioning. Ad esempio,

```
`Set-ProvScheme  –ProvisioningSchemeName "my-catalog"  –
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofileinstance.vm"
<!--NeedCopy-->
```

3. Verifica se la proprietà corrente della VM corrisponde allo schema di provisioning corrente e se c'è qualche azione di aggiornamento in sospeso sulla VM. Ad esempio,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

   È anche possibile trovare macchine con una versione particolare. Ad esempio,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Aggiornare le macchine esistenti.

   - Per aggiornare tutte le macchine esistenti:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

   - Per aggiornare un elenco di macchine specifiche:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
   -1
<!--NeedCopy-->
```

   - Per aggiornare le macchine in base all'output di `Get-ProvVM`:

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
    ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

5. Trovare i computer con un aggiornamento pianificato. Ad esempio,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

6. Riavviare le macchine. Alla successiva accensione, le modifiche delle proprietà vengono applicate ai computer esistenti. È possibile verificare lo stato aggiornato utilizzando il seguente comando:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

### Modificare le proprietà personalizzate relative al disco di un catalogo esistente

È possibile modificare le seguenti proprietà personalizzate relative al disco di un catalogo esistente e delle VM esistenti del catalogo:

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

> **Nota:**
>
> - La proprietà `StorageType` è per il disco del sistema operativo
> - La proprietà `PersistOsDisk` può essere impostata solo per il catalogo non persistente con la cache di write-back abilitata

Questa implementazione consente di selezionare diversi tipi di archiviazione per i diversi dischi anche dopo aver creato un catalogo e quindi di bilanciare i costi associati ai diversi tipi di archiviazione.

Per fare ciò, utilizzare i comandi PowerShell `Set-ProvScheme` e `Set-ProvVMUpdateTimeWindow`:

1. Aprire una finestra di **PowerShell**.
2. Eseguire `asnp citrix*`.

3. Eseguire `Get-ProvVM -VMName <VM name>` per ottenere le proprietà personalizzate.
4. Modificare la stringa delle proprietà personalizzate.
   a) Copiare le proprietà personalizzate su un file di Blocco note e modificare le proprietà personalizzate.
   b) Nella finestra di **PowerShell**, incollare le proprietà personalizzate modificate dal file di Blocco note e assegnare una variabile alle proprietà personalizzate modificate. Ad esempio:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com
   /2014/xd/machinecreation xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="CatalogZones" Value
   ="" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="
   true" />
<Property xsi:type="StringProperty" Name="PersistOSDisk" Value
   ="true" />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
   Value="pd-standard" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   pd-standard" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Aggiornare il catalogo esistente. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName> -
   CustomProperties $cp
<!--NeedCopy-->
```

6. Aggiornare le macchine virtuali esistenti. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
   VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Riavviare le macchine virtuali. Alla successiva accensione, le modifiche delle proprietà personalizzate vengono applicate alle macchine virtuali esistenti.

### Proteggersi dall'eliminazione accidentale di macchine

Citrix DaaS consente di proteggere le risorse MCS su Google Cloud per impedirne l'eliminazione accidentale. Configurare la macchina virtuale di cui è stato eseguito il provisioning impostando il flag `deletionProtection` su TRUE.

Per impostazione predefinita, le macchine virtuali di cui è stato eseguito il provisioning tramite MCS o il plug-in Google Cloud vengono create con InstanceProtection abilitato. L'implementazione è ap-

plicabile sia ai cataloghi persistenti che a quelli non persistenti. I cataloghi non persistenti vengono aggiornati quando le istanze vengono ricreate dal modello. Per le macchine persistenti esistenti, è possibile impostare il flag nella console di Google Cloud. Per ulteriori informazioni sull'impostazione del flag, consultare il sito della documentazione di Google. Le nuove macchine aggiunte ai cataloghi persistenti vengono create con `deletionProtection` abilitato.

Se si tenta di eliminare un'istanza di una macchina virtuale per la quale è stato impostato il flag `deletionProtection`, la richiesta non riesce. Tuttavia, se viene concessa l'autorizzazione `compute.instances.setDeletionProtection` o il ruolo IAM **Compute Admin**, è possibile reimpostare il flag per consentire l'eliminazione della risorsa.

### Identificare le risorse create da MCS

Di seguito sono riportati i tag che MCS aggiunge alle risorse. I tag nella tabella sono rappresentati come "key":"value".

| Nome della risorsa | Tag |
|---|---|
| Disco ID | "CitrixResource": "internal" |
| Immagine | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"<br>"CitrixResource": "internal" |
| Disco del sistema operativo | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"<br>"CitrixResource": "internal" |
| PrepVM | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"<br>"CitrixResource": "internal" |
| Snapshot pubblicata | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"<br>"CitrixResource": "internal" |
| Bucket di archiviazione | "Citrixresource": "internal" |
| Modello | "CitrixResource": "internal" |
| Macchina virtuale nel catalogo | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"<br>"CitrixResource": "internal" |

| Nome della risorsa | Tag |
| --- | --- |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”. Il plug-in aggiunge anche questa etichetta per le macchine virtuali di cui è stato eseguito il provisioning tramite MCS: “citrix-provisioning-scheme-id”: “provSchemeId”. È possibile utilizzare questa etichetta per filtrare in base al catalogo nella console di GCP. |
| Disco WBC | “CitrixResource”: “internal”<br>CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |

> **Nota:**
>
> Una macchina virtuale non è visibile nell’inventario Citrix se viene aggiunto un tag **CitrixResource** per identificarla come risorsa creata da MCS. È possibile rimuovere o rinominare il tag per renderlo visibile.

### Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Connessione agli ambienti cloud di Google
- Creare cataloghi di macchine
- Creare un catalogo di Google Cloud Platform
- Gestire i cataloghi delle macchine

## Gestire un catalogo di Microsoft Azure

January 7, 2024

In Gestire i cataloghi delle macchine sono descritte le procedure guidate per la gestione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud di Microsoft Azure Resource Manager.

> **Nota:**
>
> Prima di gestire un catalogo di Microsoft Azure, è necessario completare la creazione di un catalogo di Microsoft Azure. Vedere Creare un catalogo di Microsoft Azure.

### Convertire un catalogo di macchine non basato su profili macchina in un catalogo di macchine basato su profili macchina

È possibile utilizzare una VM o una specifica modello come input del profilo macchina per convertire un catalogo di macchine non basate su profili macchina in un catalogo di macchine basate su profilo macchina. Le VM esistenti e le nuove VM aggiunte al catalogo prendono i valori delle proprietà dal profilo della macchina, a meno che non vengano sovrascritti da proprietà personalizzate esplicite.

> **Nota:**
>
> Non è possibile modificare un catalogo macchine basato su profili macchina esistente per farlo diventare non basato su profili macchina.

A questo scopo:

1. Creare un catalogo di macchine persistente o non persistente con macchine virtuali e senza un profilo macchina.
2. Aprire la finestra di **PowerShell**.
3. Eseguire il comando `Set-ProvScheme` per applicare i valori delle proprietà tratti dal profilo della macchina alle nuove VM aggiunte al catalogo macchine. Ad esempio:

```
Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    machineprofile.folder<ResourceGroupName><TemplateSpecName><
    VersionName>
<!--NeedCopy-->
```

4. Esegui il `Set-ProvVMUpdateTimeWindow` comando per applicare i valori delle proprietà dal profilo macchina alle macchine virtuali esistenti del catalogo macchine. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName xxxx -VMName <
    List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

5. Riavviare le macchine virtuali esistenti per ottenere i valori delle proprietà dal profilo macchina.

### Conservare una macchina virtuale di cui è stato eseguito il provisioning durante i cicli di alimentazione

Scegliere se conservare una macchina virtuale di cui è stato eseguito il provisioning durante il ciclo di alimentazione. Utilizzare il parametro PowerShell `New-ProvScheme CustomProperties`. Questo parametro supporta una proprietà aggiuntiva, `PersistVm`, utilizzata per determinare se una macchina virtuale di cui è stato eseguito il provisioning persiste durante il ciclo di alimentazione. Impostare la proprietà `PersistVm` su **true** per fare in modo che una macchina virtuale persista quando è spenta oppure impostare la proprietà su **false** per assicurare che la macchina virtuale non venga preservata quando è spenta.

> **Nota:**
>
> La proprietà `PersistVm` si applica solo a uno schema di provisioning con le proprietà `CleanOnBoot` e `UseWriteBackCache` abilitato. Se la proprietà `PersistVm` non è specificata per le macchine virtuali non persistenti, vengono eliminate dall'ambiente Azure quando sono spente.

Nell'esempio seguente, il parametro `New-ProvScheme CustomProperties` imposta la proprietà `PersistVm`su **true**:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   Standard_LRS" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
   resourcegroup" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client" />
</CustomProperties>
<!--NeedCopy-->
```

Nell'esempio seguente, il parametro `New-ProvScheme CustomProperties` conserva la cache di write-back impostando `PersistVM` su **true**:

```
New-ProvScheme
-AzureAdJoinType "None"
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
```

```
        UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
        StringProperty`" Name=`"StorageType`" Value=`"Standard_LRS`" /><
        Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
        false`" /><Property xsi:type=`"StringProperty`" Name=`"
        PersistOsDisk`" Value=`"true`" /><Property xsi:type=`"
        StringProperty`" Name=`"PersistVm`" Value=`"true`" /><Property xsi:
        type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"demo-
        resourcegroup`" /><Property xsi:type=`"StringProperty`" Name=`"
        LicenseType`" Value=`"Windows_Client`" /></CustomProperties>"
  -HostingUnitName "demo"
  -IdentityPoolName "NonPersistent-MCSIO-PersistVM"
  -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-test.
     resourcegroup\demo-snapshot.snapshot"
  -NetworkMapping @ {
  "0"="XDHyp:\HostingUnits\demo\virtualprivatecloud.folder\East US.
     region\virtualprivatecloud.folder\ji-test.resourcegroup\jitest-vnet
     .virtualprivatecloud\default.network" }

 -ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"
  -ServiceOffering "XDHyp:\HostingUnits\demo\serviceoffering.folder\
     Standard_B2ms.serviceoffering" -UseWriteBackCache
  -WriteBackCacheDiskSize 127
  -WriteBackCacheMemorySize 256
  <!--NeedCopy-->
```

> **Suggerimento:**
>
> La proprietà `PersistVm` determina se conservare una macchina virtuale di cui è stato eseguito il provisioning. La proprietà `PersistOsdisk` determina se mantenere il disco del sistema operativo. Per preservare una macchina virtuale di cui è stato eseguito il provisioning, conservare innanzitutto il disco del sistema operativo. Non eliminare il disco del sistema operativo senza prima eliminare la macchina virtuale. È possibile utilizzare la proprietà `PersistOsdisk` senza specificare il parametro`PersistVm`.

### Portare il tipo di archiviazione a un livello inferiore quando una VM viene arrestata

È possibile risparmiare sui costi di archiviazione cambiando il tipo di archiviazione di un disco gestito portandolo a un livello inferiore quando si spegne una VM. Per fare ciò, utilizzare la proprietà personalizzata `StorageTypeAtShutdown`.

Il tipo di archiviazione del disco passa a un livello inferiore (come specificato nella proprietà personalizzata `StorageTypeAtShutdown`) quando si arresta la macchina virtuale. Dopo aver acceso la VM, il tipo di archiviazione torna all'originale (come specificato nella proprietà personalizzata `StorageType` o nella proprietà personalizzata `WBCDiskStorageType`).

> **Importante:**

> Il disco non esiste finché la VM non viene accesa almeno una volta. Pertanto, non è possibile modificare il tipo di archiviazione quando si accende la VM per la prima volta.

#### Requisiti

- Applicabile a un disco gestito. Ciò implica impostare la proprietà personalizzata `UseManagedDisks` su true.
- Applicabile a un catalogo persistente e non persistente con un disco del sistema operativo persistente. Ciò implica impostare la proprietà personalizzata `persistOsDisk` su true.
- Applicabile a un catalogo non persistente con un disco WBC persistente. Ciò implica impostare la proprietà personalizzata `persistWBC` su true.

#### Restrizione

- Come da Microsoft, è possibile cambiare il tipo di disco solo due volte al giorno. Vedere questo documento Microsoft. Nel caso di Citrix, l'aggiornamento di `StorageType` avviene ogni volta che c'è un'azione Start o Deallocate per la VM. Pertanto, limitare il numero di azioni di alimentazione per VM a due volte al giorno. Ad esempio, un'azione di alimentazione al mattino per avviare la VM e una alla sera per deallocare la VM.

#### Cambiare il tipo di archiviazione portandolo a un livello inferiore

Prima di procedere con i passaggi, vedere Requisiti e Restrizioni.

1. Aggiungere la proprietà personalizzata `StorageTypeAtShutdown`, impostare il valore su Standard_LRS (HDD) e creare un catalogo utilizzando `New-ProvScheme`. Per informazioni sulla creazione di un catalogo utilizzando PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

   > **Nota:**
   >
   > Se `StorageTypeAtShutdown` ha un valore diverso da vuoto o Standard_LRS (HDD), l'operazione ha esito negativo.

   Esempio di impostazione di proprietà personalizzate durante la creazione di un catalogo persistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
```

```
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value=""
    />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
    />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
    />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

Esempio di impostazione di proprietà personalizzate durante la creazione di un catalogo non persistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.
    com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
    Value="Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value=""
    />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
    />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
    />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true
    />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=
    true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

> **Nota:**
>
> Quando si utilizza un profilo macchina, la proprietà personalizzata ha la precedenza sulla proprietà definita in `MachineProfile`.

2. Arrestare la macchina virtuale e controllare il tipo di archiviazione della macchina virtuale nel portale di Azure. Il tipo di archiviazione del disco passa a un livello inferiore, come specificato nella proprietà personalizzata `StorageTypeAtShutdown`.

3. Accendere la VM. Il tipo di archiviazione del disco torna al tipo di archiviazione indicato in:

    - Proprietà personalizzata `StorageType` per il disco del sistema operativo
    - Proprietà personalizzata `WBCDiskStorageType` per il disco WBC solo se specificata in `CustomProperties`. Altrimenti, torna al tipo di archiviazione indicato in `StorageType`.

#### Applicare `StorageTypeAtShutdown` a un catalogo esistente

Prima di procedere con i passaggi, vedere Requisiti e Restrizioni.

Utilizzare `Set-ProvScheme` per aggiungere una macchina virtuale a un catalogo esistente. La funzionalità si applica alle nuove VM aggiunte dopo l'esecuzione di `Set-ProvScheme`. Le macchine esistenti non sono interessate.

Esempio di impostazione di proprietà personalizzate durante l'aggiunta di una macchina virtuale a un catalogo esistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="
    Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value
    ="Standard_LRS" />
</CustomProperties>'

$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName

Set-ProvScheme -ProvisioningSchemeName $ProvScheme.
    ProvisioningSchemeName -CustomProperties $customProperties
<!--NeedCopy-->
```

#### Cambiare il tipo di archiviazione delle VM esistenti a un livello inferiore al momento dell'arresto

Prima di procedere con i passaggi, vedere Requisiti e Restrizioni.

È possibile risparmiare sui costi di archiviazione modificando il tipo di archiviazione delle macchine virtuali esistenti su un livello inferiore quando le macchine virtuali vengono arrestate. Per fare ciò, utilizzare la proprietà personalizzata `StorageTypeAtShutdown`.

Per modificare il tipo di archiviazione delle macchine esistenti in un catalogo portandolo a un livello inferiore quando le macchine virtuali vengono spente:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire `Get-Provscheme -ProvisioningSchemeName $CatalogName`.
4. Modificare la stringa delle proprietà personalizzate.

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Aggiornare lo schema di provisioning del catalogo esistente. L'aggiornamento si applica alle nuove VM aggiunte dopo l'esecuzione di `Set-ProvScheme`.

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -
    CustomProperties $customProperties
<!--NeedCopy-->
```

6. Aggiornare le VM esistenti per abilitarle `StorageTypeAtShutdown`.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName -
    StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Alla successiva accensione delle macchine, la proprietà `StorageTypeAtShutdown` delle macchine viene aggiornata. Il tipo di archiviazione cambia al successivo arresto.
8. Eseguire il comando seguente per visualizzare il valore `StorageTypeAtShutdown` di ciascuna macchina virtuale di un catalogo:

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach {
  $vmName = $\_.VMName; $storageTypeAtShutdown = ($\_.CustomVmData
       | ConvertFrom-Json).StorageTypeAtShutdown.
      DiskStorageAccountType; return New-Object psobject -Property
      @{
  "VMName" = $vmName; "StorageTypeAtShutdown" =
      $storageTypeAtShutdown  }
   }

<!--NeedCopy-->
```

### Personalizzare il comportamento di accensione in caso di mancata riuscita della modifica del tipo di archiviazione

All'accensione, il tipo di archiviazione di un disco gestito potrebbe non riuscire a passare al tipo desiderato a causa di un errore in Azure. In questi scenari, la VM rimarrebbe disattivata e si riceverebbe un messaggio di errore. Tuttavia, è possibile scegliere di accendere la VM anche quando non può essere ripristinato il tipo di archiviazione configurato oppure scegliere di mantenere spenta la VM.

- Se si configura la proprietà personalizzata `FailSafeStorageType` come **true** (impostazione predefinita) o non la si specifica nei comandi `New-ProvScheme` o `Set-ProvScheme`:
  - All'accensione, la VM si accende con il tipo di archiviazione errato.
  - All'arresto, la VM rimane spenta con il tipo di archiviazione errato.
- Se si configura la proprietà personalizzata `FailSafeStorageType` come **false** nei comandi `New-ProvScheme` o `Set-ProvScheme`:
  - All'accensione, la VM rimane spenta con un tipo di archiviazione errato.
  - All'arresto, la VM rimane spenta con un tipo di archiviazione errato.

Per creare un catalogo di macchine:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Creare un pool di identità se non è già stato creato.
4. Aggiungere la proprietà personalizzata in `New-ProvScheme`. Ad esempio:

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\Azure-Resources-1\image.folder
    \abc.resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\Azure-Resources-1\ght.folder\abc.
     resourcegroup\abc-vnet.virtualprivatecloud\default.network" }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\Azure-Resources-1\
    serviceoffering.folder\Standard_DS2_v2.serviceoffering"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix
    .com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
    /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`
    "Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown
    `" Value=`"Standard_LRS`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
    Value=`"true`" />
</CustomProperties>"
<!--NeedCopy-->
```

5. Creare il catalogo di macchine. Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Per aggiornare un catalogo di macchine esistente in modo da includere la proprietà personalizzata `FailSafeStorageType`. Questo aggiornamento non influisce sulle macchine virtuali esistenti.

1. Aggiornare la proprietà personalizzata nel comando `Set-ProvScheme`. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`"
    Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType
    `" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
    Value=`"false`" />
</CustomProperties>"
<!--NeedCopy-->
```

Per applicare la modifica effettuata in Set-ProvScheme alle macchine virtuali esistenti, eseguire il comando `Set-ProvVMUpdateTimeWindow` con i parametri `-StartsNow` e `-DurationInMinutes -1`.

1. Eseguire il comando `Set-ProvVMUpdateTimeWindow` con i parametri `-StartsNow` e `-DurationInMinutes -1`. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

2. Riavviare le macchine virtuali.

### Aggiornare le macchine di cui è stato eseguito il provisioning allo stato corrente dello schema di provisioning

Il comando `Set-ProvScheme` modifica lo schema di provisioning. Tuttavia, non influisce sulle macchine esistenti. Utilizzando il comando `Set-ProvVMUpdateTimeWindow` di PowerShell, è possibile applicare lo schema di provisioning corrente a una macchina o a un set di macchine esistente persistente o non persistente. È inoltre possibile pianificare una fascia oraria per gli aggiornamenti

della configurazione dei computer esistenti forniti da MCS. Eventuali accensioni o riavvii durante la fascia oraria pianificata applicano un aggiornamento pianificato dello schema di provisioning a una macchina. Attualmente, in Azure, è possibile aggiornare `ServiceOffering`, `MachineProfile` e le seguenti proprietà personalizzate:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

> **Nota:**
>
> - È possibile aggiornare `StorageType`, `WBCDiskStorageType` e le proprietà personalizzate `IdentityDiskStorageType` di un catalogo solo usando il disco gestito in ambienti Azure.
> - Se si esegue `Set-ProvVMUpdateTimeWindow` due volte, ha effetto il comando più recente.

È possibile aggiornare:

- Una singola macchina virtuale
- Un elenco di macchine virtuali specifiche o di tutte le macchine virtuali esistenti associate a un ID di schema di provisioning
- Un elenco di macchine virtuali specifiche o di tutte le macchine virtuali esistenti associate a un nome di schema di provisioning (nome del catalogo macchine)

Dopo aver apportato le seguenti modifiche allo schema di provisioning, l'istanza della macchina virtuale viene ricreata per i cataloghi persistenti in Azure:

- Cambiare `MachineProfile`
- Rimuovere `LicenseType`
- Rimuovere `DedicatedHostGroupId`

> **Nota:**
>
> Il disco del sistema operativo delle macchine esistenti, insieme a tutti i relativi dati, rimane invariato e al disco viene collegata una nuova VM.

Prima di aggiornare le macchine virtuali esistenti:

1. Verificare la configurazione delle macchine esistenti. Ad esempio,

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Aggiornare lo schema di provisioning. Ad esempio,

   - Con la VM come input del profilo macchina:

   ```
   Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
       MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
       machineprofile.folder<resource-group>.resourcegroup<
       virtual-machine>.vm"
   <!--NeedCopy-->
   ```

   - Con le specifiche di modello come input del profilo macchina:

   ```
   Set-ProvScheme -ProvisioningSchemeName "my-catalog"
   -MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
       machineprofile.folder<resource-group>.resourcegroup<
       template-spec>.templatespec<template-spec-version>.
       templatespecversion"
   -ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
       serviceoffering.folder<service-offering>.serviceoffering"
   <!--NeedCopy-->
   ```

   - Con solo questa offerta di servizi:

   ```
   Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
       ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
       serviceoffering.folder<service-offering>.serviceoffering"
   <!--NeedCopy-->
   ```

3. Verifica se la proprietà corrente della VM corrisponde allo schema di provisioning corrente e se c'è qualche azione di aggiornamento in sospeso sulla VM. Ad esempio,

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
       ProvisioningSchemeVersion
   <!--NeedCopy-->
   ```

   È anche possibile trovare macchine con una versione particolare. Ad esempio,

   ```
   Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
       VMName, ProvisioningSchemeVersion
   <!--NeedCopy-->
   ```

Per richiedere gli aggiornamenti delle macchine esistenti da applicare al prossimo riavvio:

1. Eseguire i seguenti comandi per aggiornare i computer esistenti e far applicare gli aggiornamenti al successivo riavvio.

   - Per aggiornare tutte le macchine esistenti: Ad esempio,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- Per aggiornare un elenco di macchine specifiche. Ad esempio,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
   -1
<!--NeedCopy-->
```

- Per aggiornare le macchine in base all'output di Get-ProvVM. Ad esempio,

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
   ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

> **Nota:**
>
> - `StartsNow` indica che l'ora di inizio pianificata è l'ora corrente.
> - `DurationInMinutes` con un numero negativo (ad esempio -1) indica che non vi è alcun limite superiore nella finestra oraria della pianificazione.

2. Trovare i computer con un aggiornamento pianificato. Ad esempio,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
   , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

3. Riavviare le macchine. Alla successiva accensione, le modifiche delle proprietà vengono applicate ai computer esistenti. È possibile verificare lo stato aggiornato utilizzando il comando che segue. Ad esempio,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

Per pianificare l'aggiornamento di una VM alle impostazioni di provisioning più recenti la prossima volta che verrà avviata nella finestra temporale pianificata:

1. Eseguire i seguenti comandi:

- Per pianificare un aggiornamento con l'ora di inizio come ora corrente

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName vm1 -StartsNow -DurationInMinutes 120
<!--NeedCopy-->
```

- Per programmare un aggiornamento durante un fine settimana

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog" -VMName "vm1" -StartTimeInUTC "10/15/2022 9:00am" -DurationInMinutes (New-TimeSpan -Days 2).TotalMinutes
<!--NeedCopy-->
```

**Nota:**

- `VMName` è opzionale. Se non specificato, l'aggiornamento è pianificato per l'intero catalogo.
- Invece di `StartTimeInUTC`, utilizzare `StartsNow` per indicare che l'ora di inizio della pianificazione è l'ora corrente.
- `DurationInMinutes` è opzionale. L'impostazione predefinita è 120 minuti. Un numero negativo (ad esempio -1) non indica alcun limite superiore nella finestra oraria della pianificazione.

2. Controllare lo stato dell'aggiornamento.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested, ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
<!--NeedCopy-->
```

3. Accendere la VM. Se si accende il computer dopo la fascia oraria pianificata, l'aggiornamento della configurazione non viene applicato. Se si accende la macchina entro la fascia oraria pianificata,
   - Se la macchina è spenta e
     - non si accende la macchina, l'aggiornamento della configurazione non viene applicato
     - si accende la macchina, viene applicato l'aggiornamento della configurazione
   - Se la macchina è accesa e
     - non si riavvia la macchina, l'aggiornamento della configurazione non viene applicato
     - si riavvia la macchina, viene applicato l'aggiornamento della configurazione

Per annullare l'aggiornamento della configurazione:

È anche possibile annullare un aggiornamento della configurazione di una singola macchina virtuale, di più macchine virtuali o di un intero catalogo. Per annullare un aggiornamento della configurazione:

1. Eseguire `Clear-ProvVMUpdateTimeWindow`. Ad esempio:
   - Per annullare l'aggiornamento della configurazione pianificato per una singola macchina virtuale:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName " my-
    catalog " -VMName " vm1 "
<!--NeedCopy-->
```

- Per annullare l'aggiornamento della configurazione pianificato per più macchine virtuali:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
    catalog" -VMName "vm1","vm2"
<!--NeedCopy-->
```

> **Nota:**
>
> Le macchine virtuali devono appartenere allo stesso catalogo.

### Aggiornare le proprietà delle singole macchine virtuali

È possibile aggiornare le proprietà delle singole macchine virtuali incluse in un catalogo di macchine MCS persistente utilizzando il comando PowerShell `Set-ProvVM`. Tuttavia, gli aggiornamenti non vengono applicati immediatamente. È necessario impostare la finestra temporale utilizzando il comando PowerShell `Set-ProvVMUpdateTimeWindow` per applicare gli aggiornamenti.

Questa implementazione consente di gestire le singole macchine virtuali in modo efficiente senza aggiornare l'intero catalogo di macchine. Attualmente, questa funzionalità è applicabile solo all'ambiente Azure.

Attualmente, le proprietà che è possibile aggiornare sono:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

Utilizzando questa funzionalità, è possibile:

- Aggiornare le proprietà di una macchina virtuale
- Conservare le proprietà aggiornate di una macchina virtuale dopo l'aggiornamento del catalogo delle macchine
- Ripristinare gli aggiornamenti di configurazione applicati a una macchina virtuale

Prima di aggiornare le proprietà di una macchina virtuale:

1. Aprire una finestra di **PowerShell**.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Verificare la configurazione del catalogo di macchine esistente. Ad esempio:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

4. Verificare la configurazione della macchina virtuale a cui si desidera applicare gli aggiornamenti. Ad esempio:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

### Aggiornare le proprietà di una macchina virtuale

Effettuare le seguenti operazioni per aggiornare le proprietà su una macchina virtuale:

1. Disattivare la macchina virtuale a cui si intende applicare gli aggiornamenti.
2. Aggiornare le proprietà della macchina virtuale. Ad esempio, se si desidera aggiornare la proprietà personalizzata del tipo di archiviazione (`StorageType`) della macchina virtuale, eseguire i comandi seguenti:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

   È possibile aggiornare contemporaneamente le proprietà di due macchine virtuali appartenenti a un catalogo di macchine. Ad esempio:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2 -
    CustomProperties "...<Property Name='StorageType' Value='
    StandardSSD_LRS' />..."
<!--NeedCopy-->
```

   > **Nota:**
   >
   > Gli aggiornamenti non vengono applicati immediatamente.

3. Ottenere l'elenco delle proprietà specificate per l'aggiornamento e la versione di configurazione. Ad esempio:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -
    VMName machine1
<!--NeedCopy-->
```

   Controllare il valore della proprietà di `Version` e le proprietà da aggiornare (in questo caso, `StorageType`).

4. Controllare la versione della configurazione. Ad esempio:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Controllare il valore della proprietà di `ProvVMConfigurationVersion`. L'aggiornamento non è ancora stato applicato. La VM è ancora nella vecchia configurazione.

5. Richiedere un aggiornamento pianificato. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

Per ulteriori informazioni, vedere Aggiornare le macchine di cui è stato eseguito il provisioning allo stato corrente dello schema di provisioning.

> **Nota:**
>
> Viene inoltre applicato qualsiasi aggiornamento dello schema di provisioning in sospeso.

6. Riavviare la macchina virtuale. Ad esempio:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

7. Controllare la versione della configurazione. Ad esempio:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Controllare il valore della proprietà di `ProvVMConfigurationVersion`. L'aggiornamento viene ora applicato. La VM ora ha la nuova configurazione.

8. Per applicare ulteriori aggiornamenti della configurazione alla macchina virtuale, arrestare la macchina virtuale e ripetere i passaggi.

### Conservare le proprietà aggiornate di una macchina virtuale dopo l'aggiornamento del catalogo delle macchine

Effettuare le seguenti operazioni per mantenere le proprietà aggiornate su una macchina virtuale:

1. Disattivare la macchina virtuale a cui si intende applicare gli aggiornamenti.
2. Aggiornare il catalogo delle macchine. Ad esempio, se si desidera modificare la dimensione della macchina virtuale (`ServiceOffering`) e il tipo di archiviazione (`StorageType`), eseguire i comandi seguenti:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -
    ServiceOffering Standard_E4_v3 -CustomProperties "...<Property
    Name='StorageType' Value='StandardSSD_LRS' />..."
```

```
<!--NeedCopy-->
```

3. Ottenere i dettagli di configurazione del catalogo di macchine. Ad esempio:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

Ora `ProvisioningSchemeVersion` è incrementato di uno. Vengono inoltre aggiornate le dimensioni e il tipo di archiviazione della VM.

4. Aggiornare le proprietà della macchina virtuale. Ad esempio, fornire un profilo macchina alla macchina virtuale.

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<template-
    spec>.templatespec<template-spec-version>.templatespecversion"
<!--NeedCopy-->
```

> **Nota:**
>
> L'input del profilo macchina ha un tag e una dimensione di VM diversa (`ServiceOffering`) specificata.

5. Ottenere l'elenco delle proprietà che la macchina virtuale avrà dopo aver unito gli aggiornamenti di configurazione effettuati sulla macchina virtuale con gli aggiornamenti del catalogo delle macchine. Ad esempio:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
    AzureCatalog -VMName machine1
<!--NeedCopy-->
```

> **Nota:**
>
> Qualsiasi aggiornamento avvenuto sulla macchina virtuale sovrascriverà gli aggiornamenti effettuati sul catalogo delle macchine.

6. Richiedere un aggiornamento pianificato per la macchina virtuale. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Riavviare la macchina virtuale. Ad esempio:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

La macchina virtuale mantiene le proprie dimensioni aggiornate derivate dal profilo macchina.

I valori dei tag specificati nel profilo macchina vengono applicati anche alla macchina virtuale. Tuttavia, il tipo di archiviazione deriva dallo schema di provisioning più recente.

8. Ottenere la versione di configurazione della VM. Ad esempio:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

`ProvisioningSchemeVersion` e `ProvVMConfigurationVersion` ora mostrano la versione più recente.

#### Ripristinare gli aggiornamenti di configurazione applicati a una macchina virtuale

1. Dopo aver applicato gli aggiornamenti a una macchina virtuale, arrestare la macchina virtuale.
2. Eseguire il comando seguente per rimuovere gli aggiornamenti applicati alla macchina virtuale. Ad esempio:

```
Set-ProvVM -RevertToProvSchemeConfiguration -
    ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

3. Richiedere un aggiornamento pianificato per la macchina virtuale. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. Riavviare la macchina virtuale. Ad esempio:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

5. Controllare la versione di configurazione della VM. Ad esempio:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Il valore `ProvVMConfigurationVersion` è ora la versione di configurazione del catalogo macchine.

### Recuperare informazioni per le macchine virtuali di Azure, le snapshot, il disco del sistema operativo e la definizione delle immagini della raccolta

È possibile visualizzare informazioni per una macchina virtuale di Azure, inclusi il disco e il tipo del sistema operativo, la snapshot e la definizione delle immagini della raccolta. Queste informazioni vengono visualizzate per le risorse sull'immagine master quando viene assegnato un catalogo delle

macchine. Utilizzare questa funzionalità per visualizzare e selezionare un'immagine Linux o Windows. Una proprietà PowerShell, `TemplateIsWindowsTemplate`, è stata aggiunta al parametro `AdditionDatafield`. Questo campo contiene informazioni specifiche di Azure: tipo di macchina virtuale, disco del sistema operativo, informazioni sulle immagini della raccolta e informazioni sul tipo di sistema operativo. L'impostazione di `TemplateIsWindowsTemplate` su **True** indica che il tipo di sistema operativo è Windows; l'impostazione di `TemplateIsWindowsTemplate` su **False** indica che il tipo di sistema operativo è Linux.

> **Suggerimento:**
>
> Le informazioni visualizzate dalla proprietà PowerShell `TemplateIsWindowsTemplate` derivano dall'API di Azure. A volte, questo campo potrebbe essere vuoto. Ad esempio, una snapshot di un disco di dati non contiene il campo `TemplateIsWindowsTemplate` perché il tipo di sistema operativo non può essere recuperato da una snapshot.

Ad esempio, impostare il parametro `AdditionData` della macchina virtuale di Azure su **True** per il tipo di sistema operativo Windows utilizzando PowerShell:

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork\image.
    folder\username-dev-testing-rg.resourcegroup\username-dev-tsvda.vm).
    AdditionalData
Key Value
ServiceOfferingDescription Standard_B2ms
HardDiskSizeGB 127
ResourceGroupName FENGHUAJ-DEV-TESTING-RG
ServiceOfferingMemory 8192
ServiceOfferingCores 2
TemplateIsWindowsTemplate True
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SupportedMachineGenerations Gen1,Gen2
<!--NeedCopy-->
```

### Identificare le risorse create da MCS

Di seguito sono riportati i tag che MCS aggiunge alle risorse. I tag nella tabella sono rappresentati come "key":"value".

| Nome della risorsa | Tag |
|---|---|
| Disco ID | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Immagine | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |

| Nome della risorsa | Tag |
| --- | --- |
| | “CitrixResource”: “Internal” |
| NIC | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| Disco del sistema operativo | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| PrepVM | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| Snapshot pubblicata | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| Gruppo di risorse | “CitrixResource”: “Internal” CitrixSchemaVersion: 2.0 |
| Account di archiviazione | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| Macchina virtuale nel catalogo | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| Disco WBC | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |

> **Nota:**
>
> Una macchina virtuale non è visibile nell’inventario Citrix se viene aggiunto un tag **CitrixResource** per identificarla come risorsa creata da MCS. È possibile rimuovere o rinominare il tag per renderlo visibile.

### Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Connessione a Microsoft Azure
- Creare cataloghi di macchine
- Creare un catalogo di Microsoft Azure
- Gestire i cataloghi delle macchine

## Gestire un catalogo di Microsoft System Center Virtual Machine Manager

January 7, 2024

In Gestire i cataloghi delle macchine sono descritte le procedure guidate per la gestione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti di virtualizzazione Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Prima di gestire un catalogo di VMM, è necessario completare la creazione di un catalogo di VMM. Vedere Creare un catalogo di Microsoft System Center Virtual Machine Manager.

### Identificare le risorse create da MCS

Di seguito sono riportati i tag che MCS aggiunge alle risorse. I tag nella tabella sono rappresentati come “key”:”value”.

| Nome della risorsa | Tag |
|---|---|
| Preparare una macchina virtuale | Stringa tag: “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>Immissione della proprietà personalizzata: “XdConfig:”XdProvisioned=True” |
| Macchina virtuale nel catalogo | Stringa tag: “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>Immissione della proprietà personalizzata: “XdConfig:”XdProvisioned=True” |

### Ulteriori informazioni

- Creare e gestire connessioni e risorse

- Connessione a Microsoft System Center Virtual Machine Manager
- Creare cataloghi di macchine
- Creare un catalogo di Microsoft System Center Virtual Machine Manager
- Gestire i cataloghi delle macchine

## Gestire un catalogo di VMware

January 7, 2024

In Gestire i cataloghi delle macchine sono descritte le procedure guidate per la gestione di un catalogo di macchine. Le seguenti informazioni coprono i dettagli specifici degli ambienti di virtualizzazione VMware.

> **Nota:**
>
> Prima di gestire un catalogo di VMware, è necessario completare la creazione di un catalogo di VMware. Vedere Creare un catalogo di VMware.

### Aggiornare l'ID della cartella di un catalogo di macchine

È possibile aggiornare l'ID della cartella di un catalogo di macchine MCS specificando `FolderId` nelle proprietà personalizzate del comando `Set-ProvScheme`. Le macchine virtuali create dopo l'aggiornamento dell'ID della cartella vengono create con questo nuovo ID della cartella. Se questa proprietà non è specificata in `CustomProperties`, le macchine virtuali vengono create nella cartella in cui si trova l'immagine master.

Eseguire la procedura seguente per aggiornare l'ID cartella di un catalogo di macchine.

1. Aprire un browser Web e immettere l'URL del **Web Client vSphere**.
2. Inserire le credenziali e fare clic su **Login** (Accedi).
3. Creare una cartella di posizionamento delle macchine virtuali in **vSphere Web Client**.
4. Aprire una finestra di PowerShell.
5. Eseguire il comando **asnp citrix*** per caricare i moduli PowerShell specifici di Citrix.
6. Specificare `FolderID` nella casella `CustomProperties` di `Set-ProvScheme`. In questo esempio, il valore dell'ID della cartella è `group-v2406`.

```
1 Set-ProvScheme -ProvisioningSchemeUid "50bb319c-2e83-4a37-9ea1-94
    f630687372" -CustomProperties "<CustomProperties xmlns=""http
    ://schemas.citrix.com/2014/xd/machinecreation"" xmlns:xsi=""
    http://www.w3.org/2001/XMLSchema-instance""><Property xsi:type=
```

```
      ""StringProperty"" Name=""FolderId"" Value=""group-v2406"" /></
      CustomProperties>"
<!--NeedCopy-->
```

7. Aggiungere una macchina virtuale al catalogo delle macchine utilizzando Studio.
8. Controllare la nuova macchina virtuale su vSphere Web Client. La nuova macchina virtuale viene creata nella nuova cartella.

#### Trovare l'ID della cartella in vSphere

Accedere a Managed Object Browser (MOB) su qualsiasi sistema server ESXi o vCenter per trovare l'ID della cartella delle VM.

Il MOB è un'applicazione server basata sul Web disponibile integrata in tutti i sistemi server ESX/ESXi e vCenter. Questa utility vSphere consente di visualizzare informazioni dettagliate su oggetti come VM, datastore e pool di risorse.

1. Aprire un browser Web e immettere `http://x.x.x.x/mob`, dove x.x.x.x è l'indirizzo IP del vCenter Server o dell'host ESX/ESXi. Ad esempio, https://10.60.4.70/mob.
2. Nella pagina **Home** di MOB, fare clic sul valore del **contenuto** della proprietà.
3. Fare clic sul valore di **rootFolder**.
4. Fare clic sul valore di **childEntity**.
5. Fare clic sul valore di **vmFolder**.
6. L'ID della cartella si trova nel valore di **childEntity**.

### Identificare le risorse create da MCS

Di seguito sono riportati i tag che MCS aggiunge alle risorse. I tag nella tabella sono rappresentati come "key":"value".

| Nome della risorsa | Tag |
|---|---|
| Preparare una macchina virtuale | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig:"XdProvisioned=True" |
| Macchina virtuale nel catalogo | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig:"XdProvisioned=True" |

### Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Connessione a VMware
- Creare cataloghi di macchine
- Creare un catalogo di VMware
- Gestire i cataloghi delle macchine

## Criteri di sicurezza

January 7, 2024

Questo articolo descrive le funzionalità di sicurezza su vari servizi cloud supportati. Le funzionalità di sicurezza includono:

- Gruppi di sicurezza
- Avvio sicuro
- Funzionalità di crittografia

## Gruppi di sicurezza

January 7, 2024

Il gruppo di sicurezza è un gruppo di regole di sicurezza finalizzate a filtrare il traffico di rete tra una risorsa e l'altra di una rete virtuale. Le regole di sicurezza consentono o negano il traffico di rete in entrata o in uscita da diversi tipi di risorse. Ogni regola specifica le seguenti proprietà:

- Name (Nome): un nome univoco all'interno del gruppo di sicurezza di rete
- Priority (Priorità): le regole vengono elaborate in ordine di priorità, con i numeri più bassi elaborati prima dei numeri più alti, perché i numeri più bassi hanno una priorità più alta
- Source or Destination (Origine o destinazione): qualsiasi numero di indirizzi IP o un singolo indirizzo IP, blocco CIDR (routing interdominio senza classi) (10.0.0.0/24, ad esempio), tag di servizio o gruppo di sicurezza dell'applicazione
- Protocol (Protocollo): i protocolli in base ai quali si aggiungono regole per ogni gruppo di sicurezza
- Direction (Direzione): se la regola si applica al traffico in entrata o in uscita
- Port range (Intervallo di porte): è possibile specificare una singola porta o un intervallo di porte
- Action (Azione): consentire o negare

Per ulteriori informazioni sugli hypervisor supportati, vedere le sezioni seguenti:

- Gruppi di sicurezza in AWS
- Gruppi di sicurezza in Microsoft Azure
- Gruppi di sicurezza in Google Cloud Platform

### Gruppi di sicurezza in AWS

I gruppi di sicurezza agiscono come firewall virtuali che controllano il traffico per le istanze nel VPC. È possibile aggiungere regole ai gruppi di sicurezza che consentono alle istanze nella subnet pubblica di comunicare con le istanze nella subnet privata. Inoltre, questi gruppi di sicurezza potranno anche essere associati a ogni istanza nel VPC. Le regole in entrata controllano il traffico in entrata verso la propria istanza e le regole in uscita controllano il traffico in uscita da essa.

Per ulteriori informazioni sulle impostazioni di rete durante la preparazione delle immagini, vedere Impostazioni di rete durante la preparazione dell'immagine.

Quando si avvia un'istanza, è possibile specificare uno o più gruppi di sicurezza. Per configurare i gruppi di sicurezza, vedere Configurare i gruppi di sicurezza.

### Gruppi di sicurezza in Microsoft Azure

Citrix Virtual Apps and Desktops supporta i gruppi di sicurezza di rete in Azure. È previsto che i gruppi di sicurezza di rete si associno alle sottoreti. Per ulteriori informazioni, vedere Gruppi di sicurezza di rete.

Per altre informazioni sul gruppo di sicurezza di rete creato durante la preparazione dell'immagine, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

### Gruppi di sicurezza in Google Cloud Platform

Durante la preparazione di un catalogo delle macchine, viene preparata un'immagine della macchina che funge da disco di sistema dell'immagine master per il catalogo. Quando si verifica questo processo, il disco viene temporaneamente collegato a una macchina virtuale. Questa macchina virtuale deve essere eseguita in un ambiente isolato che impedisca tutto il traffico di rete in entrata e in uscita. Ciò si ottiene attraverso una coppia di regole firewall "nega tutto". Per ulteriori informazioni, vedere Regole del firewall.

# Avvio sicuro

January 7, 2024

L'avvio sicuro è progettato per garantire che venga utilizzato solo software attendibile per avviare il sistema. Il firmware dispone di un database di certificati attendibili e verifica che l'immagine caricata sia firmata da uno dei certificati attendibili. Se quell'immagine carica ulteriori immagini, anche quell'immagine deve essere verificata allo stesso modo. vTPM è un'istanza software virtualizzata di un modulo TPM fisico tradizionale. vTPM consente l'attestazione misurando l'intera catena di avvio della macchina virtuale (UEFI, sistema operativo, sistema e driver).

Per ulteriori informazioni sui servizi cloud supportati, vedere quanto segue:

- Avvio sicuro in Google Cloud Platform
- Avvio sicuro in Microsoft Azure
- Avvio sicuro in VMware

## Avvio sicuro in Google Cloud Platform

È possibile effettuare il provisioning di macchine virtuali schermate su GCP. Una macchina virtuale schermata è rafforzata mediante una serie di controlli di sicurezza che forniscono l'integrità verificabile delle istanze di Compute Engine, utilizzando funzionalità avanzate di sicurezza della piattaforma quali l'avvio sicuro, un modulo di piattaforma attendibile virtuale, firmware UEFI e monitoraggio dell'integrità.

Per ulteriori informazioni sull'uso di PowerShell per creare un catalogo con macchine virtuali schermate, vedere Utilizzo di PowerShell per creare un catalogo con VM schermate.

## Avvio sicuro in Microsoft Azure

In ambienti Azure, è possibile creare cataloghi di macchine abilitati con l'avvio attendibile. Azure offre l'avvio attendibile come modo semplice per migliorare la sicurezza delle macchine virtuali di seconda generazione. L'avvio attendibile protegge da tecniche di attacco avanzate e persistenti. Alla base dell'avvio attendibile c'è l'avvio sicuro della VM. L'avvio attendibile utilizza anche vTPM per eseguire l'attestazione remota tramite il cloud. Viene utilizzato per i controlli dello stato della piattaforma e per prendere decisioni basate sull'attendibilità. È possibile abilitare singolarmente l'avvio sicuro e vTPM. Per ulteriori informazioni sulla creazione di un catalogo di macchine con avvio attendibile, vedere Cataloghi di macchine con avvio attendibile.

### Avvio sicuro in VMware

MCS supporta la creazione di un catalogo di macchine con un modello VMware allegato a vTPM come fonte per l'input del profilo macchina. Se Windows 11 è installato sull'immagine master, è necessario che vTPM sia abilitato per l'immagine master. Pertanto, il modello VMware, che è un'origine del profilo della macchina, deve avere vTPM collegato. Per ulteriori informazioni, vedere Creare un catalogo di macchine utilizzando un profilo macchina.

## Funzionalità di crittografia

January 7, 2024

Le funzionalità di crittografia proteggono il contenuto delle macchine virtuali dagli attacchi di ospiti malintenzionati su un host di macchina virtuale condiviso e dagli attacchi lanciati dal software di controllo dell'hypervisor che gestisce tutte le macchine virtuali presenti sull'host.

Per ulteriori informazioni sui servizi cloud supportati, vedere quanto segue:

- Funzionalità di crittografia in AWS
- Funzionalità di crittografia in Google Cloud Platform
- Funzionalità di crittografia in Microsoft Azure

### Funzionalità di crittografia in AWS

Questa sezione descrive le funzionalità di crittografia negli ambienti di virtualizzazione AWS.

#### Crittografia automatica

È possibile attivare la crittografia automatica dei nuovi volumi Amazon EBS e delle copie istantanee create nell'account. Per ulteriori informazioni, vedere Crittografia automatica.

### Funzionalità di crittografia in Google Cloud Platform

Questa sezione descrive le funzionalità di crittografia negli ambienti di virtualizzazione di Google Cloud Platform (GCP).

Se si necessita di un maggiore controllo sulle operazioni delle chiavi rispetto a quello consentito dalle chiavi di crittografia gestite da Google, è possibile utilizzare chiavi di crittografia gestite dal cliente. Quando si utilizza una chiave di crittografia gestita dal cliente, un oggetto viene crittografato con la

chiave da Cloud Storage nel momento in cui viene archiviato in un bucket e l'oggetto viene decrittografato automaticamente da Cloud Storage quando viene fornito ai richiedenti. Per ulteriori informazioni, vedere Chiavi di crittografia gestite dal cliente.

È possibile utilizzare le chiavi di crittografia gestite dal cliente (CMEK) per i cataloghi MCS. Per ulteriori informazioni, vedere Utilizzo di CMEK (Customer Managed Encryption Keys, chavi di crittografia gestite dal cliente).

### Funzionalità di crittografia in Microsoft Azure

Questa sezione descrive le funzionalità di crittografia negli ambienti di virtualizzazione di Azure.

#### Crittografia lato server di Azure

La maggior parte dei dischi gestiti di Azure è crittografata con la crittografia di Azure Storage, che utilizza la crittografia lato server (SSE) per proteggere i dati dell'utente e aiutarlo a rispettare gli impegni di sicurezza e conformità. Citrix Virtual Apps and Desktops supporta le chiavi di crittografia gestite dal cliente per i dischi gestiti di Azure tramite Azure Key Vault. Per ulteriori informazioni, vedere Crittografia lato server di Azure.

#### Doppia crittografia di Azure

La doppia crittografia è costituita da crittografia lato piattaforma (impostazione predefinita) e crittografia gestita dal cliente (CMEK). Pertanto, se si è un cliente altamente sensibile alla sicurezza e si nutre preoccupazione per il rischio associato a qualsiasi algoritmo di crittografia, implementazione o chiave compromessa, è possibile optare per questa doppia crittografia. Il sistema operativo persistente e i dischi di dati, le snapshot e le immagini sono tutti crittografati quando inattivi con doppia crittografia. Per ulteriori informazioni, vedere Doppia crittografia su disco gestito.

## Creare gruppi di consegna

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix

> Virtual Apps and Desktops 7 2212 o versioni precedenti.

Un gruppo di consegna è una raccolta di macchine selezionate da uno o più cataloghi di macchine. Nel gruppo di consegna è specificato quali utenti possono utilizzare tali macchine, oltre alle applicazioni e ai desktop disponibili per tali utenti.

La creazione di un gruppo di consegna rappresenta il passaggio successivo per configurare la distribuzione dopo la creazione di un sito e la creazione di un catalogo macchine. In seguito è possibile modificare le impostazioni iniziali nel primo gruppo di consegna e creare altri gruppi di consegna. Esistono anche funzionalità e impostazioni che è possibile configurare solo quando si modifica un gruppo di consegna, non quando lo si crea.

In Accesso remoto PC, quando si crea un sito, viene creato automaticamente un gruppo di consegna denominato "Remote PC Access Desktops".

Per creare un gruppo di consegna:

1. Se sono stati creati un sito e un catalogo macchine, senza un gruppo di consegna, Web Studio guida l'utente al punto di partenza corretto per crearne uno.
2. Se è già stato creato un gruppo di consegna e si desidera crearne un altro, effettuare le seguenti operazioni:
    a) Selezionare **Delivery groups** (Gruppi di consegna). Selezionare **Create Delivery Group** (Crea gruppo di consegna) nella barra delle azioni.
    b) Per organizzare i gruppi di consegna utilizzando le cartelle, creare cartelle nella cartella predefinita **Delivery Groups**. Per ulteriori informazioni, vedere Creare una cartella del gruppo di consegna.
    c) Selezionare la cartella in cui si desidera creare il gruppo, quindi fare clic su **Create Delivery Group** (Crea gruppo di consegna). Si apre la procedura guidata per la creazione del gruppo.
3. Viene avviata la procedura guidata con la pagina **Introduction**, che può essere rimossa dai futuri avvii della procedura guidata.
4. La procedura guidata guida quindi l'utente nelle pagine descritte nella sezione seguente. Al termine di ogni pagina, fare clic su **Next** fino a raggiungere la pagina finale.

### Passaggio 1. Macchine

Nella pagina **Machines** selezionare un catalogo e selezionare il numero di macchine di quel catalogo che si desidera utilizzare.

Buono a sapersi:

- Almeno una macchina di un catalogo selezionato deve rimanere inutilizzata.
- È possibile specificare un catalogo in più gruppi di consegna. Una macchina può essere utilizzata in un solo gruppo di consegna.
- Un gruppo di consegna può utilizzare macchine provenienti da più di un catalogo; tuttavia, tali cataloghi devono contenere gli stessi tipi di computer (sistema operativo multi-sessione, sistema operativo a sessione singola o Accesso remoto PC). In altre parole, non è possibile combinare tipi di macchina diversi in uno stesso gruppo di consegna. Analogamente, se la distribuzione contiene cataloghi di macchine Windows e cataloghi di macchine Linux, un gruppo di consegna può contenere macchine dell'uno o dell'altro tipo ma non di entrambi.
- Citrix consiglia di installare o aggiornare tutti i computer con la versione VDA più recente. Aggiornare i cataloghi e i gruppi di consegna in base alle esigenze. Quando si crea un gruppo di consegna, se si selezionano macchine con versioni VDA diverse installate, il gruppo di consegna è compatibile con la versione VDA meno recente. Questo è denominato *livello funzionale* del gruppo. Ad esempio, se uno dei computer ha VDA versione 7.1 e altri computer hanno la versione corrente, tutti i computer del gruppo possono utilizzare solo le funzionalità supportate in VDA 7.1. Ciò significa che alcune funzionalità che richiedono versioni successive del VDA potrebbero non essere disponibili in tale gruppo di consegna.
- Ogni computer incluso in un catalogo Accesso remoto PC viene automaticamente associato a un gruppo di consegna. Quando si crea un sito di Accesso remoto PC, vengono creati automaticamente un catalogo denominato "Remote PC Access Machines"(Macchine di accesso remoto PC) e un gruppo di consegna denominato "Remote PC Access Desktops"(Desktop Accesso remoto PC).
- Vengono eseguiti i seguenti controlli di compatibilità:
  - MinimumFunctionalLevel deve essere compatibile
  - SessionSupport deve essere compatibile
  - AllocationType deve essere compatibile per SingleSession
  - ProvisioningType deve essere compatibile
  - PersistChanges deve essere compatibile per MCS e Citrix Provisioning
  - Il catalogo RemotePC è compatibile solo con il catalogo RemotePC
  - Controllo relativo ad AppDisk

### Passaggio 2. Tipo di consegna

Questa pagina viene visualizzata solo se è stato scelto un catalogo contenente macchine statiche (assegnate) con sistema operativo a sessione singola.

Nella pagina **Delivery Type** scegliere **Applications** o **Desktops**. Non è possibile abilitare entrambi.

Se sono state selezionate macchine da un sistema operativo multi-sessione o da un catalogo casuale (in pool) di macchine con sistema operativo a sessione singola, si presume che il tipo di consegna sia

applicazioni e desktop: è possibile distribuire applicazioni, desktop o entrambi.

### Passaggio 3. Utenti

Specificare gli utenti e i gruppi di utenti che possono utilizzare le applicazioni e i desktop del gruppo di consegna.

#### Dove vengono specificati gli elenchi degli utenti

Gli elenchi degli utenti di Active Directory vengono specificati quando si crea o si modifica quanto segue:

- L'elenco di accesso utente di un sito, che non è configurato tramite Web Studio. Per impostazione predefinita, la regola dei criteri di autorizzazione applicazione include tutti gli utenti. Per ulteriori informazioni, vedere i cmdlet `BrokerAppEntitlementPolicyRule` dell'SDK di PowerShell.
- Gruppi di applicazioni (se configurati).
- Gruppi di consegna.
- Applicazioni.

L'elenco degli utenti che possono accedere a un'applicazione tramite StoreFront è formato dall'intersezione degli elenchi di utenti di cui sopra. Ad esempio, per configurare l'uso dell'applicazione A per un particolare reparto, senza limitare indebitamente l'accesso ad altri gruppi:

- Utilizzare la regola dei criteri di autorizzazione applicazione predefinita che include tutti gli utenti.
- Configurare l'elenco utenti del gruppo di consegna per consentire a tutti gli utenti della sede centrale di utilizzare una delle applicazioni specificate nel gruppo di consegna.
- Se i gruppi di applicazioni sono configurati, configurare l'elenco di utenti del gruppo di applicazioni per consentire ai membri del reparto Amministrazione e Finanza di accedere alle applicazioni dalla A alla L.
- Configurare le proprietà dell'applicazione A per limitarne la visibilità solo al personale della contabilità clienti del reparto Amministrazione e Finanza.

#### Utenti autenticati e non autenticati

Esistono due tipi di utenti: autenticati e non autenticati (quelli non autenticati sono anche detti anonimi). È possibile configurare uno o entrambi i tipi in un gruppo di consegna.

- **Autenticati:** per accedere alle applicazioni e ai desktop, gli utenti e i membri del gruppo specificati per nome devono presentare credenziali quali smart card o nome utente e password per

l'app StoreFront o Citrix Workspace. Per i gruppi di consegna contenenti computer con sistema operativo a sessione singola, è possibile importare i dati utente (un elenco di utenti) in un secondo momento modificando il gruppo di consegna.

- **Non autenticati (anonimi):** per i gruppi di consegna contenenti macchine con sistema operativo multi-sessione, è possibile consentire agli utenti di accedere alle applicazioni e ai desktop senza presentare le credenziali all'app StoreFront o Citrix Workspace. Ad esempio, nei chioschi, l'applicazione potrebbe richiedere le credenziali, ma il portale di accesso Citrix e gli strumenti non lo fanno. Viene creato un gruppo di utenti anonimi quando si installa il primo Delivery Controller.

  Per concedere l'accesso a utenti non autenticati, in ogni computer del gruppo di consegna deve essere installato un VDA per il sistema operativo Windows Server (versione minima 7.6). Quando sono abilitati gli utenti non autenticati, è necessario disporre di un archivio StoreFront non autenticato.

  Gli account utente non autenticati vengono creati su richiesta all'avvio di una sessione e sono denominati Anon*XYZ*, in cui *XYZ* è un valore univoco a tre cifre.

  Le sessioni utente non autenticate hanno un timeout di inattività predefinito di 10 minuti e vengono disconnesse automaticamente quando il client si disconnette. La riconnessione, il roaming tra i client e il controllo Workspace non sono supportati.

Nella tabella seguente vengono descritte le scelte effettuate nella pagina **Users**:

| Abilitare l'accesso per | Aggiungere/assegnare utenti e gruppi di utenti? | Attivare la casella di controllo "Give access to unauthenticated users" (Concedi accesso a utenti non autenticati)? |
|---|---|---|
| Solo utenti autenticati | Sì | No |
| Solo utenti non autenticati | No | Sì |
| Utenti autenticati e non autenticati | Sì | Sì |

### Passaggio 4. Applicazioni

Buono a sapersi:

- Non è possibile aggiungere applicazioni ai gruppi di consegna Accesso remoto PC.

- Per impostazione predefinita, le nuove applicazioni aggiunte vengono inserite in una cartella denominata Applications. È possibile specificare una cartella diversa. Per ulteriori informazioni, vedere l'articolo Gestire applicazioni.
- È possibile modificare le proprietà di un'applicazione quando la si aggiunge a un gruppo di consegna o in un secondo momento. Per ulteriori informazioni, vedere l'articolo Gestire applicazioni.
- Se si tenta di aggiungere un'applicazione e in quella cartella ne esiste già una con lo stesso nome, verrà richiesto di rinominare l'applicazione che si sta aggiungendo. Se si rifiuta, all'applicazione viene aggiunto un suffisso che la rende univoca all'interno di quella cartella di applicazioni.
- Quando si aggiunge un'applicazione a più di un gruppo di consegna, può verificarsi un problema di visibilità se non si dispone di autorizzazioni sufficienti a visualizzare l'applicazione in tutti i gruppi di consegna. In questi casi, vedere un amministratore con autorizzazioni più ampie o estendere il proprio ambito per includere tutti i gruppi di consegna a cui è stata aggiunta l'applicazione.
- Se si pubblicano due applicazioni con lo stesso nome per gli stessi utenti, modificare la proprietà Nome applicazione (per utente) in Web Studio; in caso contrario, gli utenti vedranno nomi duplicati nell'app Citrix Workspace.

Fare clic su **Add** per visualizzare le origini delle applicazioni.

- **Dal menu Start:** applicazioni individuate in un computer creato dall'immagine master nel catalogo selezionato. Quando si seleziona questa origine, viene avviata una nuova pagina con un elenco di applicazioni rilevate; selezionare quelle che si desidera aggiungere e quindi fare clic su **OK**.
- **Manually:** applicazioni situate su un VDA nel gruppo di consegna o in altre parti della rete. Selezionando questa fonte si apre una nuova pagina in cui è possibile specificare un'applicazione da aggiungere nei seguenti modi:
  - Digitare il percorso dell'eseguibile, la directory di lavoro, gli argomenti della riga di comando facoltativi e i nomi visualizzati per amministratori e utenti.
  - Selezionare un'applicazione da un VDA del gruppo di consegna. A tale scopo, fare clic su **Browse** (Sfoglia), immettere le credenziali per accedere al VDA, attendere di essere connessi al VDA e quindi selezionare un'applicazione dal VDA. Le proprietà dell'applicazione selezionata compilano automaticamente i campi della pagina.
- **Existing (esistenti):** applicazioni precedentemente aggiunte al sito, forse in un altro gruppo di consegna. Quando si seleziona questa origine, viene avviata una nuova pagina con un elenco delle applicazioni individuate. Aggiungere le applicazioni e fare clic su **OK**.
- **App-V**: applicazioni contenute in pacchetti App-V. Quando si seleziona questa origine, viene avviata una nuova pagina in cui si seleziona il server App-V o la libreria di applicazioni. Selezionare le applicazioni che si desidera aggiungere dalla visualizzazione risultante, quindi fare

clic su **OK**. Per ulteriori informazioni, vedere applications.Distribuire e rendere disponibili applicazioni App-V.

Se l'origine di un'applicazione o un'applicazione non è disponibile o valida, questa non è visibile o non è selezionabile. Ad esempio, l'origine **Existing** non è disponibile se al sito non sono state aggiunte applicazioni. Oppure un'applicazione potrebbe non essere compatibile con i tipi di sessione supportati sui computer del catalogo selezionato.

### Passaggio 5. Desktop

Il titolo di questa pagina dipende dal catalogo scelto nella pagina **Machines**:

- Se si sceglie un catalogo contenente macchine in pool, questa pagina si intitola **Desktops**.
- Se è stato scelto un catalogo contenente macchine assegnate e si è specificato "Desktops"nella pagina **Delivery Type** (Tipo di consegna), questa pagina si intitola **Desktop User Assignments** (Assegnazioni utente desktop).
- Se si sceglie un catalogo contenente macchine assegnate e si era specificato "Applications"nella pagina **Delivery Type**, questa pagina si intitola **Application Machine User Assignments** (Assegnazioni utente della macchina applicazioni).

Fare clic su **Aggiungi**. Nella finestra di dialogo:

- Nei campi Display name (Nome visualizzato) e Description (Descrizione), digitare le informazioni da visualizzare nell'app Citrix Workspace.
- Per aggiungere una restrizione di tag a un desktop, selezionare **Restrict launches to machines with this tag** (Limita lanci ai computer con questo tag), quindi selezionare il tag dall'elenco a discesa. Per ulteriori informazioni, vedere Tag.
- Utilizzare i pulsanti di opzione per avviare un desktop o per assegnare una macchina all'avvio del desktop. Gli utenti possono essere tutti coloro che possono accedere a questo gruppo di consegna oppure utenti e gruppi di utenti specifici.
- Se il gruppo contiene macchine assegnate, specificare il numero massimo di desktop per utente. Questo deve essere un valore pari a uno o maggiore di uno.
- Attivare o disattivare il desktop (per le macchine in pool) o la regola di assegnazione desktop (per le macchine assegnate). La disattivazione di un desktop interrompe la distribuzione del desktop. La disattivazione di una regola di assegnazione desktop interrompe l'assegnazione automatica del desktop agli utenti.
- Al termine, fare clic su **OK**.

#### Numero massimo di istanze di un desktop in un sito (solo PowerShell)

Per configurare il numero massimo di istanze di un desktop nel sito (solo PowerShell):

- In PowerShell utilizzare il cmdlet BrokerEntitlementPolicyRule appropriato con il parametro MaxPerEntitlementInstances. Ad esempio, il cmdlet seguente modifica la regola `tsvda-desktop` impostando il numero massimo di istanze simultanee di un desktop consentite nel sito su due. Quando sono in esecuzione due istanze del desktop, si verifica un errore se un terzo sottoscrittore tenta di avviare un desktop.

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop -MaxPerEntitlementInst
    2
  ```

- Per informazioni, utilizzare il cmdlet Get-Help. Ad esempio, `Get-Help Set-BrokerEntitlementPol -Parameter MaxPerEntitlementInstances`.

### Passaggio 6. Riepilogo

Inserire un nome per il gruppo di consegna. È inoltre possibile (facoltativamente) immettere una descrizione, che viene visualizzata nell'app Citrix Workspace e in Web Studio.

Esaminare le informazioni di riepilogo e quindi fare clic su **Finish**.

## Gestire i gruppi di consegna

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

### Introduzione

In questo articolo vengono descritte le procedure per la gestione dei gruppi di consegna dalla console di gestione. Oltre a modificare le impostazioni specificate durante la creazione del gruppo, è possibile configurare altre impostazioni non disponibili quando si crea un gruppo di consegna.

Le categorie di procedure includono: generale, utenti, macchine e sessioni. Alcune attività riguardano più di una categoria. Ad esempio l'opzione "Prevent users from connecting to machines"(Impedisci agli utenti di connettersi alle macchine) è descritta nella categoria macchine, ma influisce anche sugli utenti. Se non si riesce a trovare un'attività in una categoria, controllare in una categoria correlata.

Altri articoli contengono anche informazioni correlate:

- L'articolo Applicazioni contiene informazioni sulla gestione delle applicazioni nei gruppi di consegna.
- La gestione dei gruppi di consegna richiede le autorizzazioni predefinite dell'amministratore del gruppo di consegna. Per ulteriori informazioni, vedere Amministrazione delegata.

## Aspetti generali

- Modificare il tipo di consegna
- Modificare gli indirizzi StoreFront
- Cambiare il livello funzionale
- Gestire i gruppi di consegna di Remote PC Access
- Organizzare i gruppi di consegna utilizzando le cartelle
- Gestire App Protection

### Modificare il tipo di consegna di un gruppo di consegna

Il tipo di consegna indica ciò che il gruppo può fornire: applicazioni, desktop o entrambi.

Prima di modificare un tipo **solo un'applicazione** o **desktop e applicazioni** nel tipo **solo desktop**, eliminare tutte le applicazioni dal gruppo.

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Delivery Type** (Tipo di spedizione) selezionare il tipo di consegna desiderato.
4. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, fare clic su **Save** per applicare le modifiche e chiudere la finestra.

### Modificare gli indirizzi StoreFront

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **StoreFront** selezionare o aggiungere URL StoreFront. Questi URL vengono utilizzati dall'app Citrix Workspace, che viene installata su ogni macchina del gruppo di consegna.
4. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, fare clic su **Save** per applicare le modifiche e chiudere la finestra.

È inoltre possibile specificare gli indirizzi del server StoreFront selezionando **StoreFront** nel riquadro di sinistra.

### Cambiare il livello funzionale

Modificare il livello funzionale del gruppo di consegna dopo aver aggiornato i VDA sulle relative macchine e i cataloghi delle macchine contenenti le macchine utilizzate nel gruppo di consegna.

Prima di iniziare:

- Se si utilizza Citrix Provisioning (in precedenza Provisioning Services), aggiornare la versione VDA nella console Citrix Provisioning.
- Avviare le macchine contenenti il VDA aggiornato in modo che possano registrarsi con un Delivery Controller. Questo processo indica alla console ciò che deve essere aggiornato nel gruppo di consegna.
- Se si continua a utilizzare versioni precedenti dei VDA, le funzionalità più recenti del prodotto non sono disponibili. Per ulteriori informazioni, vedere la documentazione di aggiornamento.

Per aggiornare un gruppo di consegna:

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo e quindi fare clic su **Upgrade Delivery Group** (Aggiorna gruppo di consegna) nella barra delle azioni. L'azione **Change Functional Level** (Cambia livello funzionale) viene visualizzata solo se vengono rilevati VDA aggiornati.

Viene indicato quali macchine, se presenti, non possono passare a quel determinato livello funzionale e perché. È quindi possibile annullare l'azione di modifica, risolvere i problemi della macchina e quindi eseguire nuovamente l'azione di modifica.

Una volta completato la modifica, è possibile ripristinare le macchine ai loro stati precedenti. Selezionare il gruppo di consegna, quindi selezionare **Undo Functional Level Change** (Annulla modifica livello funzionale) nella barra delle azioni.

### Gestire i gruppi di consegna di Remote PC Access

Se una macchina contenuta in un catalogo di computer Accesso remoto PC non è assegnata, essa viene temporaneamente assegnata a un gruppo di consegna associato a tale catalogo. Questa assegnazione temporanea consente di assegnare la macchina a un utente in un secondo momento.

L'associazione fra catalogo macchine e gruppo di consegna ha un valore di priorità. La priorità determina il gruppo di consegna assegnato alla macchina quando si registra nel sistema o quando un utente necessita di un'assegnazione macchina. Più basso è il valore, maggiore è la priorità. Se un catalogo di macchine Accesso remoto PC dispone di più assegnazioni di gruppi di consegna, il software seleziona quella con la priorità più alta. Utilizzare l'SDK di PowerShell per impostare questo valore di priorità.

Quando vengono creati per la prima volta, i cataloghi di macchine Remote PC Access (Accesso remoto PC) vengono associati a un gruppo di consegna. Gli account macchina o le unità organizzative aggiunti al catalogo in un secondo momento possono essere aggiunti al gruppo di consegna. Questa associazione può essere disattivata o attivata.

Per aggiungere o rimuovere un'associazione di catalogo macchine di Accesso remoto PC con un gruppo di consegna:

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo Accesso remoto PC.
3. Nella sezione **Details**, fare clic sulla scheda **Machine Catalogs** (Cataloghi macchine) e quindi selezionare un catalogo di Accesso remoto PC.
4. Per aggiungere o ripristinare un'associazione, fare clic su **Add Desktops** (Aggiungi desktop). Per rimuovere un'associazione, fare clic su **Remove Association** (Rimuovi associazione).

### Organizzare i gruppi di consegna utilizzando le cartelle

È possibile creare cartelle per organizzare i gruppi di consegna per un facile accesso.

**Ruoli richiesti** Per impostazione predefinita, è necessario disporre del seguente ruolo integrato per creare e gestire le cartelle del gruppo di consegna: Cloud Administrator (amministratore cloud), Full Administrator (amministratore completo) o Delivery Group Administrator (amministratore del gruppo di consegna). Se necessario, è possibile personalizzare i ruoli per la creazione e la gestione delle cartelle del gruppo di consegna. Per ulteriori informazioni, consultare Autorizzazioni richieste.

**Creare una cartella del gruppo di consegna** Prima di iniziare, pianificare come organizzare i gruppi di consegna. Considerare quanto segue:

- È possibile nidificare le cartelle fino a cinque livelli (esclusa la cartella principale predefinita).
- Una cartella può contenere gruppi di consegna e sottocartelle.
- Tutti i nodi (come **Machine Catalogs** (Cataloghi di macchine), **Applications** (Applicazioni) e **Delivery groups** (Gruppi di consegna) condividono un albero delle cartelle nel back-end. Per evitare conflitti di nomi con altri nodi durante la ridenominazione o lo spostamento di cartelle, si consiglia di assegnare nomi diversi alle cartelle di primo livello in nodi diversi.

Per creare una cartella del gruppo di consegna, effettuare le seguenti operazioni:

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Nella gerarchia delle cartelle, selezionare una cartella e quindi selezionare **Create Folder** (Crea cartella) nella barra **Actions** (Azioni).
3. Immettere un nome per la nuova cartella, quindi fare clic su **Done** (Fine).

> **Suggerimento:**
>
> Se si crea una cartella in una posizione non prevista, è possibile trascinarla nella posizione corretta.

### Spostare un gruppo di consegna

È possibile spostare un gruppo di consegna da una cartella all'altra. I passaggi dettagliati sono i seguenti:

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Visualizzare i gruppi per cartella. È anche possibile attivare **View all** (Visualizza tutto) sopra la gerarchia delle cartelle per visualizzare tutti i gruppi contemporaneamente.
3. Fare clic con il pulsante destro del mouse su un gruppo, quindi selezionare **Move Delivery Group** (Sposta gruppo di consegna).
4. Selezionare la cartella in cui si desidera spostare il gruppo e quindi fare clic su **Done** (Fine).

> **Suggerimento:**
>
> È possibile trascinare un gruppo in una cartella.

### Gestire le cartelle dei gruppi di consegna

È possibile eliminare, rinominare e spostare le cartelle dei gruppi di consegna.

Tenere presente che è possibile eliminare una cartella solo se essa e le relative sottocartelle non contengono gruppi di consegna.

Per gestire una cartella, effettuare le seguenti operazioni:

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Nella gerarchia delle cartelle, selezionare una cartella, quindi selezionare un'azione nella barra **Actions** (Azioni) in base alle esigenze:
   - Per rinominare la cartella, selezionare **Rename Folder** (Rinomina cartella).
   - Per eliminare la cartella, selezionare **Delete Folder** (Elimina cartella).
   - Per spostare la cartella, selezionare **Move Folder** (Sposta cartella).
3. Seguire le istruzioni sullo schermo per completare i passaggi rimanenti.

**Autorizzazioni richieste** Nella tabella seguente sono elencate le autorizzazioni necessarie per eseguire azioni sulle cartelle dei gruppi di consegna.

| Azione | Autorizzazioni richieste |
|---|---|
| Creare cartelle dei gruppi di consegna | Creazione di cartella del gruppo di consegna |
| Eliminare le cartelle dei gruppi di consegna | Rimozione della cartella del gruppo di consegna |
| Spostare le cartelle dei gruppi di consegna | Spostamento cartella del gruppo di consegna |
| Ridenominare le cartelle dei gruppi di consegna | Modifica della cartella del gruppo di consegna |
| Spostare i gruppi di consegna nelle cartelle | Modifica della cartella del gruppo di consegna e modifica delle proprietà del gruppo di consegna |

#### Gestire App Protection

Le seguenti informazioni si riferiscono ad App protection. Fare attenzione ai seguenti dettagli:

- È necessario disporre di un diritto valido ad App Protection. Per acquistare la funzionalità App Protection, contattare il proprio rappresentante commerciale Citrix.
- App Protection richiede l'attendibilità XML. Per abilitare l'attendibilità XML, andare a **Settings > Enable XML trust** (Impostazioni > Abilita attendibilità XML).
- Per quanto riguarda anti-screen-capturing:
  - Su Windows e macOS, solo la finestra del contenuto protetto è vuota. App Protection è attiva quando una finestra protetta non è ridotta a icona.
  - Nel sistema operativo Linux, l'intera acquisizione è vuota. App Protection è attiva indipendentemente dal fatto che una finestra protetta sia ridotta a icona o meno.

Per scegliere un metodo App Protection per un gruppo di consegna, seguire questi passaggi:

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Manage app protection**, è possibile abilitare l'**Anti-keylogging e l'Anti-Screen-Capturing**.

### Utenti

- Modificare le impostazioni utente
- Aggiungere o rimuovere utenti

### Modificare le impostazioni utente in un gruppo di consegna

Il nome di questa pagina viene visualizzato come **User Settings** (Impostazioni utente) o **Basic Settings** (Impostazioni di base).

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **User Settings** (Impostazioni utente) (o **Basic Settings** [Impostazioni di base]) modificare una delle impostazioni nella tabella seguente.
4. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, fare clic su **Save** per applicare le modifiche e chiudere la finestra.

| Impostazione | Descrizione |
|---|---|
| Descrizione | Testo utilizzato da Citrix Workspace (o StoreFront) e visualizzato dagli utenti. |
| Enable delivery group | Indica se il gruppo di consegna è abilitato. |
| Time zone (Fuso orario) | Il fuso orario in cui devono risiedere le macchine di questo gruppo di consegna. L'opzione elenca i fusi orari supportati dal sito. **Nota:** la modifica del fuso orario su un gruppo di consegna potrebbe provocare il riavvio delle macchine del gruppo. Per evitare ciò, modificare le impostazioni del fuso orario solo al di fuori degli orari di produzione. |
| Enable Secure ICA | Protegge le comunicazioni da e verso le macchine del gruppo di consegna utilizzando SecureICA, che crittografa il protocollo ICA. Il livello predefinito è 128 bit. Il livello può essere modificato utilizzando l'SDK. Citrix consiglia di utilizzare più metodi di crittografia come la crittografia TLS durante l'attraversamento di reti pubbliche. Inoltre, SecureICA non controlla l'integrità dei dati. |

### Aggiungere o rimuovere utenti in un gruppo di consegna

Per informazioni dettagliate sugli utenti, vedere Utenti.

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.

2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Users** (Utenti):
    - Per aggiungere utenti, fare clic su **Add** (Aggiungi) e specificare gli utenti da aggiungere.
    - Per rimuovere utenti, selezionare uno o più utenti, quindi fare clic su **Remove** (Rimuovi).
    - Selezionare o deselezionare la casella di controllo per consentire l'accesso agli utenti non autenticati.
4. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, fare clic su **Save** per applicare le modifiche e chiudere la finestra.

**Importare o esportare elenchi utenti** Per i gruppi di consegna contenenti macchine operative fisiche a sessione singola, è possibile importare informazioni utente da un file .csv dopo aver creato il gruppo di consegna. È inoltre possibile esportare in un file .csv le informazioni utente. Il file .csv può contenere dati di una versione precedente del prodotto.

La prima riga del file CSV deve contenere due intestazioni di colonna, separate da una virgola. Assicurarsi che la prima intestazione sia `Machine Account` e la seconda sia `User Names`. È possibile includere intestazioni aggiuntive, ma non sono supportate. Le righe successive del file contengono dati separati da virgole. Le voci `Machine Account` possono essere SID o FQDN del computer o coppie di nomi di dominio e computer.

Per importare o esportare informazioni utente:

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Machine Allocation** (Allocazione macchina), selezionare l'elenco **Import** o l'elenco **Export** quindi individuare il percorso del file.
4. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, fare clic su **Save** per applicare le modifiche e chiudere la finestra.

## Macchine

- Modificare le assegnazioni delle macchine agli utenti
- Modificare il numero massimo di macchine per utente
- Aggiornare una macchina
- Aggiungere, modificare o rimuovere una restrizione di tag per un desktop
- Rimuovere una macchina
- Limitare l'accesso alle macchine
- Impedire agli utenti di connettersi a una macchina (modalità manutenzione)
- Arrestare e riavviare le macchine

- Creare e gestire pianificazioni di riavvio per le macchine
- Caricare macchine gestite
- Macchine con alimentazione gestita

#### Modificare le assegnazioni delle macchine agli utenti di un gruppo di consegna

È possibile modificare le assegnazioni delle macchine con sistema operativo a sessione singola con provisioning MCS. Non è possibile modificare le assegnazioni per macchine con sistema operativo multisessione o macchine con provisioning fornito da Citrix Provisioning.

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Desktops** o **Desktop Assignment Rules** (il titolo della pagina dipende dal tipo di catalogo macchine utilizzato dal gruppo di consegna), specificare i nuovi utenti.
4. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, fare clic su **Save** per applicare le modifiche e chiudere la finestra.

#### Modificare il numero massimo di macchine per utente contenute in un gruppo di consegna

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Desktop Assignment Rules** (Regole di assegnazione desktop) impostare il valore massimo di desktop per utente.
4. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, fare clic su **Save** per applicare le modifiche e chiudere la finestra.

#### Aggiornare una macchina di un gruppo di consegna

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi fare clic su **View Machines** nella barra delle azioni.
3. Selezionare una macchina e quindi fare clic su **Update Machines** (Aggiorna macchine) nella barra delle azioni.

Per scegliere un'immagine master diversa, selezionare **Master image** (Immagine master), quindi selezionare una snapshot.

Per applicare le modifiche e notificarlo agli utenti della macchina, selezionare **Rollout notification to end-users** (Notifica rollout agli utenti finali). Quindi specificare:

- Quando aggiornare l'immagine master: ora o al successivo riavvio

- Il tempo di distribuzione del riavvio (il tempo totale per iniziare ad aggiornare tutte le macchine del gruppo)
- Indica se gli utenti vengono avvisati del riavvio
- Il messaggio che ricevono gli utenti

#### Aggiungere, modificare o rimuovere una restrizione di tag per un desktop

L'aggiunta, la modifica e la rimozione di restrizioni ai tag possono avere effetti imprevisti sui desktop di cui si considera l'avvio. Leggere le considerazioni e le avvertenze in Tag.

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Desktops** selezionare il desktop e fare clic su **Edit**.
4. Per aggiungere una restrizione tag, selezionare **Restrict launches to machines with the tag** (Limita avvii alle macchine con il tag), quindi selezionare il tag.
5. Per modificare o rimuovere una restrizione tag, effettuare le seguenti operazioni:
   - Selezionare un tag diverso.
   - Rimuovere la restrizione tag deselezionando **Restrict launches to machines with this tag** (Limita avvii alle macchine con il tag).
6. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, fare clic su **Save** per applicare le modifiche e chiudere la finestra.

#### Rimuovere una macchina da un gruppo di consegna

La rimozione di una macchina la elimina da un gruppo di consegna. Non la elimina dal catalogo macchine utilizzato dal gruppo di consegna. Pertanto, tale macchina è disponibile per l'assegnazione a un altro gruppo di consegna.

Le macchine devono essere spente prima di poter essere rimosse. Per impedire temporaneamente agli utenti di connettersi a una macchina durante la rimozione, mettere la macchina in modalità di manutenzione prima di spegnerla.

Le macchine potrebbero contenere dati personali, quindi prestare attenzione prima di allocare la macchina a un altro utente. Considerare la possibilità di ricreare l'immagine della macchina.

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi fare clic su **View Machines** nella barra delle azioni.
3. Assicurarsi che la macchina sia spenta.

4. Selezionare il computer, quindi fare clic su **Remove from Delivery Group** (Rimuovi dal gruppo di consegna) nella barra delle azioni.

È inoltre possibile rimuovere una macchina da un gruppo di consegna tramite la connessione utilizzata dalla macchina.

#### Limitare l'accesso alle macchine di un gruppo di consegna

Qualsiasi modifica apportata per limitare l'accesso alle macchine di un gruppo di consegna sostituisce le impostazioni precedenti, indipendentemente dal metodo utilizzato. È possibile effettuare le seguenti operazioni:

- **Limitare l'accesso per gli amministratori utilizzando ambiti di amministrazione delegata:** creare e assegnare un ambito che consente agli amministratori di accedere a tutte le applicazioni e un altro ambito che consente l'accesso solo a determinate applicazioni. Per ulteriori informazioni, vedere Amministrazione delegata.
- **Limitare l'accesso agli utenti tramite espressioni dei criteri SmartAccess:** utilizzare le espressioni dei criteri per filtrare le connessioni degli utenti effettuate tramite Citrix Gateway.

  1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
  2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
  3. Nella pagina **Access Policy** (Criteri di accesso), selezionare **Connections through NetScaler Gateway** (Connessioni tramite NetScaler Gateway).
  4. Per scegliere un sottoinsieme di tali connessioni, selezionare **Connections meeting any of the following filters** (Connessioni che soddisfano uno dei seguenti filtri). Definire quindi il sito Citrix Gateway e aggiungere, modificare o rimuovere le espressioni dei criteri SmartAccess per gli scenari di accesso utente consentiti. Per ulteriori informazioni, vedere la documentazione di Citrix Gateway.
  5. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, fare clic su **Save** per applicare le modifiche e chiudere la finestra.

- **Limitare l'accesso per gli utenti tramite filtri di esclusione:** utilizzare i filtri di esclusione per i criteri di accesso impostati nell'SDK. I criteri di accesso vengono applicati ai gruppi di consegna per affinare le connessioni. Ad esempio, è possibile limitare l'accesso alla macchina a un sottoinsieme di utenti ed è possibile specificare i dispositivi utente consentiti. I filtri di esclusione affinano ulteriormente i criteri di accesso. Ad esempio, per motivi di sicurezza, è possibile negare l'accesso a un sottoinsieme di utenti o dispositivi. Per impostazione predefinita, i filtri di esclusione sono disabilitati.

  Ad esempio, un laboratorio didattico in una sottorete di rete aziendale che impedisce l'accesso da quel laboratorio a un particolare gruppo di consegna. Indipendentemente da chi utilizza

le macchine nel laboratorio, utilizzare il comando: `Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`.

Utilizzare il carattere jolly asterisco (*) per far corrispondere tutti i tag che iniziano con la stessa espressione dei criteri. Ad esempio, se si aggiunge il tag `VPDesktops_Direct` a una macchina e `VPDesktops_Test` a un altro, impostando il tag nello script `Set-BrokerAccessPolicy` a `VPDesktops_*` si applica il filtro a entrambe le macchine.

Se si è connessi tramite un browser Web o con la funzionalità di esperienza utente dell'app Citrix Workspace abilitata nello store, non è possibile utilizzare un filtro di esclusione dei nomi client.

### Impedire agli utenti di connettersi a una macchina (modalità di manutenzione) in un gruppo di consegna

Quando è necessario impedire temporaneamente che vengano effettuate nuove connessioni alle macchine, è possibile attivare la modalità di manutenzione per una o tutte le macchine di un gruppo di consegna. Questa operazione può essere effettuata prima di applicare patch o di utilizzare gli strumenti di gestione.

- Quando una macchina con sistema operativo multisessione è in modalità di manutenzione, gli utenti possono connettersi a sessioni esistenti, ma non possono avviare nuove sessioni.
- Quando una macchina con sistema operativo a sessione singola (o un PC che utilizza Accesso remoto PC) è in modalità di manutenzione, gli utenti non possono connettersi o riconnettersi. Le connessioni correnti permangono finché non si disconnettono o si scollegano.

Per attivare o disattivare la modalità di manutenzione:

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo.
3. Per attivare la modalità manutenzione per tutti i computer del gruppo di consegna, fare clic su **Turn On Maintenance Mode** (Attiva modalità di manutenzione) nella barra delle azioni.

   Per attivare la modalità di manutenzione per una macchina, fare clic su **View Machines** (Visualizza macchine) nella barra delle azioni. Selezionare un computer e quindi fare clic su **Turn On Maintenance Mode** (Attiva modalità manutenzione) nella barra delle azioni.
4. Per disattivare la modalità di manutenzione per una o tutte le macchine di un gruppo di consegna, seguire le istruzioni precedenti, ma fare clic su **Turn Off Maintenance Mode** (Disabilita modalità di manutenzione) nella barra delle azioni.

Le impostazioni di Connessione desktop remoto di Windows influiscono anche sul fatto che una macchina con sistema operativo multisessione possa essere o meno in modalità di manutenzione. La modalità di manutenzione è attiva quando si verifica una delle seguenti condizioni:

- La modalità di manutenzione è impostata su attivata, come descritto in precedenza.
- RDC è impostato su **Don't allow connections to this computer** (Non consentire connessioni al computer).
- RDC non è impostato su **Don't allow connections to this computer** (Non consentire connessioni al computer). **Remote Host Configuration User Logon Mode** (Modalità di accesso utente Configurazione host remoto) è impostato su **Allow reconnections, but prevent new logons** (Consenti riconnessioni, ma impedisci nuovi accessi) o **Allow reconnections, but prevent new logons until the server is restarted** (Consenti riconnessioni, ma impedisci nuovi accessi fino al riavvio del server).

È inoltre possibile attivare o disattivare la modalità manutenzione per:

- Una connessione che influisce sulle macchine che la utilizzano.
- Un catalogo di macchine, che influisce sulle macchine che contiene.

#### Arrestare e riavviare le macchine di un gruppo di consegna

Questa procedura non è supportata per le macchine Remote PC Access (Accesso remoto PC).

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi fare clic su **View Machines** nella barra delle azioni.
3. Selezionare il computer e quindi fare clic su una delle seguenti voci nella barra delle azioni:
    - **Force shut down** (Spegnimento forzato): spegne forzatamente la macchina e aggiorna l'elenco delle macchine.
    - **Restart** (Riavvio): richiede al sistema operativo di arrestare e quindi riavviare la macchina. Se il sistema operativo non è in grado di eseguire la procedura, la macchina rimane nello stato corrente.
    - **Force restart** (Forza riavvio): chiude forzatamente la sessione del sistema operativo e riavvia la macchina.
    - **Suspend** (Sospendi): mette in pausa la macchina senza arrestarla e aggiorna l'elenco delle macchine.
    - **Shut down** (Arresto): richiede l'arresto del sistema operativo.

Per le azioni non forzate, se la macchina non chiude la sessione entro 10 minuti, viene spenta. Se Windows tenta di installare aggiornamenti durante la chiusura della sessione, c'è il rischio che il computer sia spento prima del completamento degli aggiornamenti.

Citrix consiglia di impedire agli utenti con sistema operativo a sessione singola di selezionare **Shut down** in una sessione. Per ulteriori informazioni, vedere la documentazione relativa ai criteri Microsoft.

È inoltre possibile arrestare e riavviare i computer che utilizzano una connessione.

### Creare e gestire pianificazioni di riavvio per le macchine di un gruppo di consegna

> **Nota:**
>
> - Quando una pianificazione di riavvio viene applicata a un gruppo di consegna con AutoScale abilitato, le relative macchine vengono semplicemente spente e AutoScale provvederà ad accenderle.
> - Quando le pianificazioni di riavvio vengono applicate a macchine a sessione singola casuali, tali macchine vengono spente anziché riavviate, per risparmiare sui costi. Si consiglia di utilizzare AutoScale per accendere le macchine.
> - La modifica del fuso orario su un gruppo di consegna potrebbe provocare il riavvio delle macchine del gruppo. Per evitare ciò, modificare le impostazioni del fuso orario solo al di fuori degli orari di produzione.

Una pianificazione di riavvio specifica quando le macchine di un gruppo di consegna vengono periodicamente riavviate. È possibile creare una o più pianificazioni per un gruppo di consegna. Una pianificazione può influire su:

- Tutte le macchine del gruppo.
- Una o più macchine (ma non tutte) del gruppo. Le macchine sono identificate da un tag applicato alla macchina. Questa operazione è chiamata restrizione tag, perché il tag limita un'azione solo agli elementi che hanno il tag.

Ad esempio, supponiamo che tutte le macchine si trovino in un unico gruppo di consegna. Si desidera che ogni macchina venga riavviata una volta alla settimana e che le macchine utilizzate dal team di contabilità vengano riavviate quotidianamente. A tale scopo, impostare una pianificazione per tutte le macchine e un'altra pianificazione solo per le macchine del team contabilità.

Una pianificazione include il giorno e l'ora di inizio del riavvio e la relativa durata.

È possibile attivare o disattivare una pianificazione. La disattivazione di una pianificazione può essere utile durante i test, durante intervalli speciali o durante la preparazione delle pianificazioni prima di averne bisogno.

Non è possibile utilizzare pianificazioni per l'accensione o l'arresto automatico dalla console di gestione, solo per il riavvio.

**Sovrapposizione delle pianificazioni** Più pianificazioni possono sovrapporsi. Nell'esempio precedente, entrambe le pianificazioni influenzano le macchine del team di contabilità. Quelle macchine potrebbero essere riavviate due volte alla domenica. Il codice di pianificazione è progettato per evitare di riavviare la stessa macchina più spesso del previsto, ma non può essere garantito.

- Se le pianificazioni coincidono con precisione nei tempi di inizio e durata, è più probabile che i computer vengano riavviati una sola volta.

- Più le pianificazioni differiscono nei tempi di inizio e durata, più è probabile che si verifichino più riavvii.
- Il numero di macchine interessate da una pianificazione influisce anche sulla possibilità di sovrapposizione. Nell'esempio, la pianificazione settimanale che interessa tutti i computer potrebbe avviare il riavvio più velocemente della pianificazione giornaliera per le macchine del team di contabilità, a seconda della durata specificata per ciascuna.

Per un'analisi approfondita delle pianificazioni di riavvio, vedere Elementi interni della pianificazione del riavvio.

#### Visualizzare le pianificazioni di riavvio

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
3. Selezionare la pagina **Restart Schedule** (Pianificazione riavvii).

La pagina **Restart Schedule** contiene le seguenti informazioni per ogni pianificazione configurata:

- Nome della pianificazione.
- Eventuale limitazione tag utilizzata.
- Quante volte si verifica il riavvio della macchina.
- Se gli utenti della macchina ricevono una notifica o meno.
- Se la pianificazione è abilitata o meno.

**Aggiungere (applicare) tag** Quando si configura una pianificazione di riavvio che utilizza una restrizione tag, assicurarsi che il tag sia stato aggiunto ai computer interessato dalla pianificazione. Nell'esempio precedente, ciascuna delle macchine utilizzate dal team di contabilità ha un tag applicato. Per ulteriori informazioni, vedere Tag.

Sebbene sia possibile applicare più tag a una macchina, una pianificazione di riavvio può specificare un solo tag.

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare il gruppo contenente le macchine controllate dal programma.
3. Fare clic su **View Machines** (Visualizza macchine), quindi selezionare le macchine a cui si desidera aggiungere un tag.
4. Fare clic su **Manage Tags** (Gestisci tag) nella barra delle azioni.
5. Se il tag esiste, attivare la casella di controllo accanto al nome del tag. Se il tag non esiste, fare clic su **Create** e quindi specificare il nome del tag. Dopo aver creato il tag, attivare la casella di controllo accanto al nome del tag appena creato.
6. Fare clic su **Save** nella finestra di dialogo **Manage Tags** (Gestisci tag).

**Creare una pianificazione di riavvio**

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Gestisci tag** (Riavvia pianificazione) fare clic su **Add**.
4. Nella pagina **Add Restart Schedule** (Aggiungi pianificazione di riavvio):

    - Per abilitare la pianificazione, selezionare **Yes** (Sì). Per disabilitare la pianificazione, selezionare **No**.
    - Digitare un nome e una descrizione della pianificazione.
    - Per **Restrict to tag** (Limita ai tag), applicare una restrizione per il tag.
    - Per **Include machines in maintenance mode** (Includi macchine in modalità di manutenzione), scegliere se includere in questo programma di riavvio le macchine in modalità di manutenzione. Se invece si desidera utilizzare PowerShell, vedere Riavvii pianificati per le macchine in modalità di manutenzione.
    - Per **Restart frequency** (Frequenza di riavvio), selezionare la frequenza di riavvio: giornaliera, settimanale, mensile o una volta. Se si seleziona **Weekly** (Settimanale) o **Monthly** (Mensile), è possibile specificare uno o più giorni specifici.
    - Per **Repeats every** (Si ripete ogni), specificare la frequenza con cui si desidera eseguire la pianificazione.
    - Per **Start date** (Data di inizio), specificare una data di inizio per la prima occorrenza della pianificazione.
    - Per **Begin restart at** (Inizia il riavvio alle ore) specificare, in formato orologio 24 ore, l'ora della giornata in cui iniziare il riavvio.
    - In **Restart duration** (Durata del riavvio):

        – Se non si desidera utilizzare il riavvio naturale, selezionare **Restart all machines at the same time** (Riavvia tutti i computer contemporaneamente) o **Restart all machines within a time period** (Riavvia tutti i computer entro un periodo di tempo).

        – Se si desidera utilizzare il riavvio naturale, selezionare **Restart all machines after draining all sessions** (Riavviare tutti i computer dopo aver esaurito tutte le sessioni).

        All'avvio di una pianificazione di riavvio configurata per utilizzare il riavvio naturale:

        * Tutti i computer inattivi appartenenti al gruppo di consegna vengono riavviati immediatamente.
        * Ogni macchina appartenente a un gruppo di consegna che abbia una o più sessioni attive viene riavviata quando tutte le sessioni vengono scollegate.

> **Nota:**
>
> È possibile utilizzare questa opzione per le macchine con alimentazione gestita e anche per le macchine con alimentazione non gestita.

- In **Send notification to users** (Invia notifica agli utenti), scegliere se visualizzare un messaggio di notifica sulle macchine interessate prima dell'inizio del riavvio. Per impostazione predefinita, non viene visualizzato alcun messaggio.
- Se si sceglie di visualizzare un messaggio 15 minuti prima dell'inizio del riavvio, è possibile scegliere (in **Notification frequency** [Frequenza di notifica]) di ripetere il messaggio ogni cinque minuti dopo il messaggio iniziale. Per impostazione predefinita, il messaggio non si ripete.
- Immettere il titolo e il testo della notifica. Non è presente testo predefinito.

  Se si desidera che il messaggio includa un conto alla rovescia per il riavvio, includere la variabile **%m%**. A meno che non si scelga di riavviare tutte le macchine contemporaneamente, il messaggio viene visualizzato su ogni macchina all'ora appropriata prima del riavvio.

5. Fare clic su **Done** (Fine) per applicare le modifiche e chiudere la finestra **Add Restart Schedule** (Aggiungi pianificazione di riavvio).
6. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, fare clic su **Save** per applicare le modifiche e chiudere la finestra.

**Riavviare dopo lo svuotamento** Un altro valore della durata del riavvio è disponibile quando si utilizza PowerShell per creare o aggiornare una pianificazione di riavvio del computer (`New-BrokerRebootSchedulev2` o `Set-BrokerRebootSchedulev2`).

Quando si attiva la funzione di riavvio dopo lo svuotamento con il parametro `-UseNaturalReboot <Boolean>`, tutte le macchine vengono riavviate dopo lo svuotamento di tutte le sessioni. Quando viene raggiunto l'orario del riavvio, le macchine vengono messe in stato di scarico e quindi riavviate quando tutte le sessioni sono scollegate.

Questa funzionalità è supportata per i gruppi di consegna contenenti macchine a sessione singola o multisessione. È possibile utilizzare questa opzione per le macchine con alimentazione gestita e anche per le macchine con alimentazione non gestita.

In un ambiente locale, questa funzionalità è supportata solo quando si utilizza PowerShell. La funzionalità non è disponibile in Web Studio.

#### Modificare, rimuovere, abilitare o disattivare una pianificazione di riavvio

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.

2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Restart Schedule** (Pianificazione di riavvio) selezionare la casella di controllo relativa a una pianificazione.

    - Per modificare una pianificazione, fare clic su **Edit**. Aggiornare la configurazione della pianificazione, utilizzando le linee guida in Creare una pianificazione di riavvio.
    - Per attivare o disattivare una pianificazione, fare clic su **Edit**. Selezionare o deselezionare la casella di controllo **Enable restart schedule** (Abilita pianificazione riavvio).
    - Per rimuovere una pianificazione, fare clic su **Remove**. Confermare la rimozione. La rimozione di una pianificazione non influisce sui tag applicati alle macchine interessate.

**Riavvii pianificati ritardati a causa di un'interruzione del database**

> **Nota:**
>
> Questa funzionalità è disponibile solo in PowerShell.

Se si verifica un'interruzione del database del sito prima dell'inizio di un riavvio pianificato per le macchine (VDA) di un gruppo di consegna, i riavvii iniziano al termine dell'interruzione. Questo può avere risultati imprevisti.

Ad esempio, supponiamo di aver programmato il riavvio di un gruppo di consegna durante le ore fuori produzione (a partire dalle 03:00). Un'ora prima dell'inizio del riavvio pianificato (02:00) si verifica un'interruzione del database del sito. L'interruzione dura sei ore (fino alle 08:00). La pianificazione di riavvio inizia quando viene ripristinata la connessione tra il Delivery Controller e il database del sito. Il riavvio del VDA ora inizia cinque ore dopo la pianificazione originale, con conseguente riavvio dei VDA durante le ore di produzione.

Per evitare questa situazione, è possibile utilizzare il parametro `MaxOvertimeStartMins` per i cmdlet `New-BrokerRebootScheduleV2` e `Set-BrokerRebootScheduleV2`. Il valore specifica il numero massimo di minuti dopo l'ora di inizio pianificata in cui una pianificazione di riavvio può iniziare.

- Se la connessione al database viene ripristinata entro quell'ora (ora pianificata + `MaxOvertimeStartMins` ), inizia il riavvio del VDA.
- Se la connessione al database non viene ripristinata entro quell'ora, i riavvii del VDA non vengono avviati.
- Se questo parametro viene omesso o ha un valore zero, il riavvio pianificato inizia quando viene ripristinata la connessione al database, indipendentemente dalla durata dell'interruzione.

Per ulteriori informazioni, vedere la Guida del cmdlet. Questa funzionalità è disponibile solo in PowerShell. Non è possibile impostare questo valore quando si configura una pianificazione di riavvio in Web Studio.

#### Riavvii programmati per macchine in modalità manutenzione

> **Nota:**
>
> Questa funzionalità è disponibile solo in PowerShell. L'opzione `IgnoreMaintenanceMode` è supportata da Citrix Virtual Apps and Desktops 7 2006 e versioni successive.

Per indicare se una pianificazione di riavvio influisce sui computer in modalità manutenzione, utilizzare l'opzione `IgnoreMaintenanceMode` con i cmdlet `BrokerRebootScheduleV2`.

Ad esempio, il cmdlet seguente crea una pianificazione che riavvia i computer che sono in modalità manutenzione (oltre ai computer che non lo sono).

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup
> -IgnoreMaintenanceMode $true
```

Il cmdlet seguente modifica una pianificazione di riavvio esistente.

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode
$true
```

Per ulteriori informazioni, vedere la Guida del cmdlet. Questa funzionalità è disponibile solo in PowerShell.

#### Caricare macchine gestite nei gruppi di consegna

È possibile caricare solo le macchine gestite con sistema operativo multisessione.

La gestione del carico misura il carico del server e determina quale server selezionare nelle condizioni ambientali correnti. Questa selezione si basa su:

- **Stato della modalità di manutenzione server:** un sistema operativo multisessione viene preso in considerazione per il bilanciamento del carico solo quando la modalità di manutenzione è disattivata.
- **Indice di carico server:** determina la probabilità di ricevere connessioni di un server che distribuisce macchine con sistema operativo multisessione. L'indice è una combinazione di strumenti di valutazione del carico: il numero di sessioni e le impostazioni per le metriche delle prestazioni come CPU, disco e utilizzo della memoria. Gli strumenti di valutazione del carico sono specificati nelle impostazioni dei criteri di gestione del carico.

  Un indice di caricamento server pari a 10000 indica che il server è completamente caricato. Se non sono disponibili altri server, gli utenti potrebbero ricevere un messaggio che indica che il desktop o l'applicazione non è disponibile quando avviano una sessione.

  È possibile monitorare l'indice di caricamento in Director (Monitor), nella ricerca di Web Studio (Manage) e SDK.

Nelle visualizzazioni della console, per visualizzare la colonna **Server Load Index** (che è nascosta per impostazione predefinita), selezionare una macchina, fare clic con il pulsante destro del mouse su un'intestazione di colonna e quindi selezionare **Select Column**. Nella **categoria Machine**, selezionare **Load Index**.

Nell'SDK utilizzare il cmdlet `Get-BrokerMachine`. Per ulteriori informazioni, vedere CTX202150.

- **Concurrent logon tolerance policy setting** (Impostazione dei criteri di tolleranza di accesso simultaneo): il numero massimo di richieste simultanee di accesso al server. (questa impostazione equivale alla limitazione del carico nelle versioni XenApp 6.x).

  Quando l'impostazione di tolleranza di accesso simultaneo di tutti i server è pari o superiore all'impostazione, la richiesta di accesso successiva viene assegnata al server con meno accessi in sospeso. Se questi criteri sono soddisfatti da più di un server, viene selezionato il server con l'indice di carico più basso.

#### Macchine con alimentazione gestita in un gruppo di consegna

È possibile gestire l'alimentazione delle sole macchine virtuali con sistema operativo a sessione singola, non delle macchine fisiche (incluse le macchine Accesso remoto PC). Le macchine con sistema operativo a sessione singola con funzionalità GPU non possono essere sospese, quindi le operazioni di spegnimento non riescono. Per i computer con sistema operativo multisessione, è possibile creare una pianificazione di riavvio.

Nei gruppi di consegna contenenti macchine in pool, le macchine virtuali con sistema operativo a sessione singola possono trovarsi in uno dei seguenti stati:

- Assegnate casualmente e in uso
- Non assegnate e non connesse

Nei gruppi di consegna contenenti macchine statiche, le macchine virtuali con sistema operativo a sessione singola possono essere:

- Assegnate in modo permanente e in uso
- Assegnate in modo permanente e non connesse (ma pronte)
- Non assegnate e non connesse

Durante l'uso normale, i gruppi di consegna statici contengono in genere macchine assegnate in modo permanente e non assegnate. Inizialmente, tutte le macchine sono non assegnate, ad eccezione di quelle assegnate manualmente quando è stato creato il gruppo di consegna. Man mano che gli utenti si connettono, le macchine vengono assegnate in modo permanente. È possibile gestire completamente l'alimentazione delle macchine non assegnate in tali gruppi di consegna, ma gestire solo parzialmente quelle assegnate in modo permanente.

- **Pool e buffer:** nei gruppi di consegna in pool e i gruppi di consegna statici con macchine non allocate, un pool (in questa istanza) è un insieme di macchine non assegnate o assegnate temporaneamente che vengono mantenute alimentate, pronte per la connessione degli utenti. Un utente ottiene una macchina immediatamente dopo l'accesso. La dimensione del pool (il numero di macchine mantenute accese) è configurabile in base all'ora del giorno. Per i gruppi di consegna statici, utilizzare l'SDK per configurare il pool.

  Un buffer è un set di standby aggiuntivo di macchine non allocate che vengono attivate quando il numero di macchine presenti nel pool scende al di sotto di una determinata soglia. La soglia è una percentuale della dimensione del gruppo di consegna. Nel caso di gruppi di consegna di grandi dimensioni, quando la soglia viene superata potrebbe essere attivato un numero significativo di macchine. Quindi, pianificare attentamente le dimensioni dei gruppi di consegna o utilizzare l'SDK per regolare la dimensione predefinita del buffer.

- **Timer dello stato di alimentazione:** è possibile utilizzare i timer dello stato di alimentazione per sospendere le macchine quando è trascorso un determinato periodo di tempo dalla disconnessione degli utenti. Ad esempio, le macchine si sospendono automaticamente al di fuori dell'orario di ufficio non meno di 10 minuti dopo la disconnessione degli utenti.

  È possibile configurare i timer per i giorni feriali e i fine settimana e per intervalli di ore di punta e non di punta.

- **Gestione parziale dell'alimentazione delle macchine assegnate in modo permanente:** per le macchine assegnate in modo permanente, è possibile impostare timer dello stato di alimentazione, ma non pool o buffer. Le macchine vengono accese all'inizio di ogni periodo di punta e spente all'inizio di ogni periodo non di punta. Non si dispone del controllo fine disponibile per le macchine non assegnate sul numero di macchine che diventano disponibili per compensare le macchine che vengono consumate.

**Gestione dell'alimentazione di macchine virtuali con sistema operativo a sessione singola**

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi fare clic su **Edit Delivery Group** (Modifica gruppo di consegna) nella barra delle azioni.
3. Nella pagina **Power Management** (Gestione energia) selezionare **Weekdays** (Giorni feriali) in **Power manage machines** (Gestione dell'alimentazione delle macchine). Per impostazione predefinita, i giorni feriali sono dal lunedì al venerdì.
4. Per i gruppi di consegna casuale, in **Machines to be powered on** (Macchine da accendere), fare clic su **Edit** e quindi specificare la dimensione del pool durante i giorni feriali. Quindi, selezionare il numero di macchine da accendere.
5. In **Peak hours** (Ore di punta), impostare le ore di punta e non di punta per ogni giorno.
6. Impostare i timer dello stato di alimentazione per le ore di ore di punta e non di punta durante i giorni feriali: In **During peak hours (Durante le ore di punta) > When disconnected (Quando**

**si è disconnessi)**, specificare il ritardo (in minuti) prima di sospendere qualsiasi macchina disconnessa nel gruppo di consegna, quindi selezionare **Suspend**. In **During off-peak hours (Durante le ore non di punta) > When disconnected**, specificare il ritardo prima di spegnere qualsiasi macchina disconnessa nel gruppo di consegna, quindi selezionare **Shutdown** (Arresto). Questo timer non è disponibile per i gruppi di consegna con macchine casuali.

7. Selezionare **Weekend** in **Power manage machines**, quindi configurare le ore di punta e i timer dello stato di alimentazione per i fine settimana.
8. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, fare clic su **Save** per applicare le modifiche e chiudere la finestra.

Utilizzare l'SDK per:

- Spegnere, invece di sospendere, le macchine in risposta a timer dello stato di alimentazione o se si desidera che i timer siano basati sullo scollegamento, anziché la disconnessione.
- Modificare le definizioni predefinite di giorno feriale e di fine settimana.
- Disabilitare la gestione dell'alimentazione. Vedere CTX217289.

**Gestire l'alimentazione di macchine VDI che passano a un periodo di tempo diverso con sessioni disconnesse**

> **Importante:**
>
> Questo miglioramento si applica solo alle macchine VDI con sessioni disconnesse. Non si applica alle macchine VDI con sessioni scollegate.

Nelle versioni precedenti, una macchina VDI che passava a un periodo di tempo in cui era necessaria un'azione (azione di disconnessione= "**Suspend**"o "**Shutdown**") rimaneva alimentata. Questo scenario si verificava se la macchina si disconnetteva durante un periodo di tempo (di punta o non di punta) in cui non era richiesta alcuna azione (azione di disconnessione = "**Nothing**").

A partire da Citrix Virtual Apps and Desktops 7 1909, la macchina viene sospesa o spenta al termine del tempo di disconnessione specificato, a seconda dell'azione di disconnessione configurata per il periodo di tempo di destinazione.

Ad esempio, è possibile configurare i criteri di risparmio energia seguenti per un gruppo di consegna VDI:

- Impostare `PeakDisconnectAction` su "Nothing"
- Impostare `OffPeakDisconnectAction` su "Shutdown"
- Impostare `OffPeakDisconnectTimeout` su "10"

Per ulteriori informazioni sui criteri di risparmio energia per l'azione di disconnessione, vedere https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy e https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Nelle versioni precedenti, una macchina VDI con una sessione disconnessa durante i periodi di punta rimaneva accesa quando passava dai periodi di punta a quelli non di punta. A partire da Citrix Virtual Apps and Desktops 7 1909, le azioni dei criteri `OffPeakDisconnectAction` e `OffPeakDisconnectTimeout` vengono applicate alla macchina VDI durante la transizione da un periodo all'altro. Di conseguenza, la macchina viene spenta 10 minuti dopo la transizione al periodo fuori picco.

Se si desidera ripristinare il comportamento precedente (ovvero, non eseguire alcuna azione su macchine che passano dal periodo di punta a quello fuori picco o al periodo di punta con sessioni disconnesse), effettuare una delle seguenti operazioni:

- Impostare il valore `LegacyPeakTransitionDisconnectedBehaviour` del Registro di sistema su `1`, l'equivalente di *true* che abilita il comportamento precedente. Per impostazione predefinita, il valore è `0`, o *false*, il che attiva le azioni dei criteri per il risparmio di energia relative alla disconnessione durante la transizione da un periodo all'altro.
  - Percorso: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - Nome: `LegacyPeakTransitionDisconnectedBehaviour`
  - Tipo: `REG_DWORD`
  - Dati: `0x00000001 (1)`
- Configurare l'impostazione utilizzando il comando PowerShell`Set-BrokerServiceConfigurationD` . Ad esempio:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Una macchina deve soddisfare i seguenti criteri prima che le possano essere applicate le azioni dei criteri di risparmio energia durante la transizione da un periodo all'altro:

- Avere una sessione disconnessa.
- Non avere nessuna azione per il risparmio di energia in sospeso.
- Appartenere a un gruppo di consegna VDI (a sessione singola) che passa a un periodo di tempo diverso.
- Avere una sessione che si disconnette durante un determinato periodo di tempo (di picco o non di picco) e passa a un periodo in cui viene assegnata un'azione per il risparmio di energia.

#### Modificare la percentuale di VDA che si trovano in stato alimentato per i cataloghi

1. Regolare le ore di punta per il gruppo di consegna dalla sezione **Power management** (Gestione energia) per il gruppo di consegna.
2. Prendere nota del nome del gruppo desktop.

3. Con privilegi di amministratore, avviare PowerShell ed eseguire i comandi seguenti. Sostituire “Desktop Group Name”con il nome del gruppo desktop che ha una percentuale modificata di VDA in esecuzione.

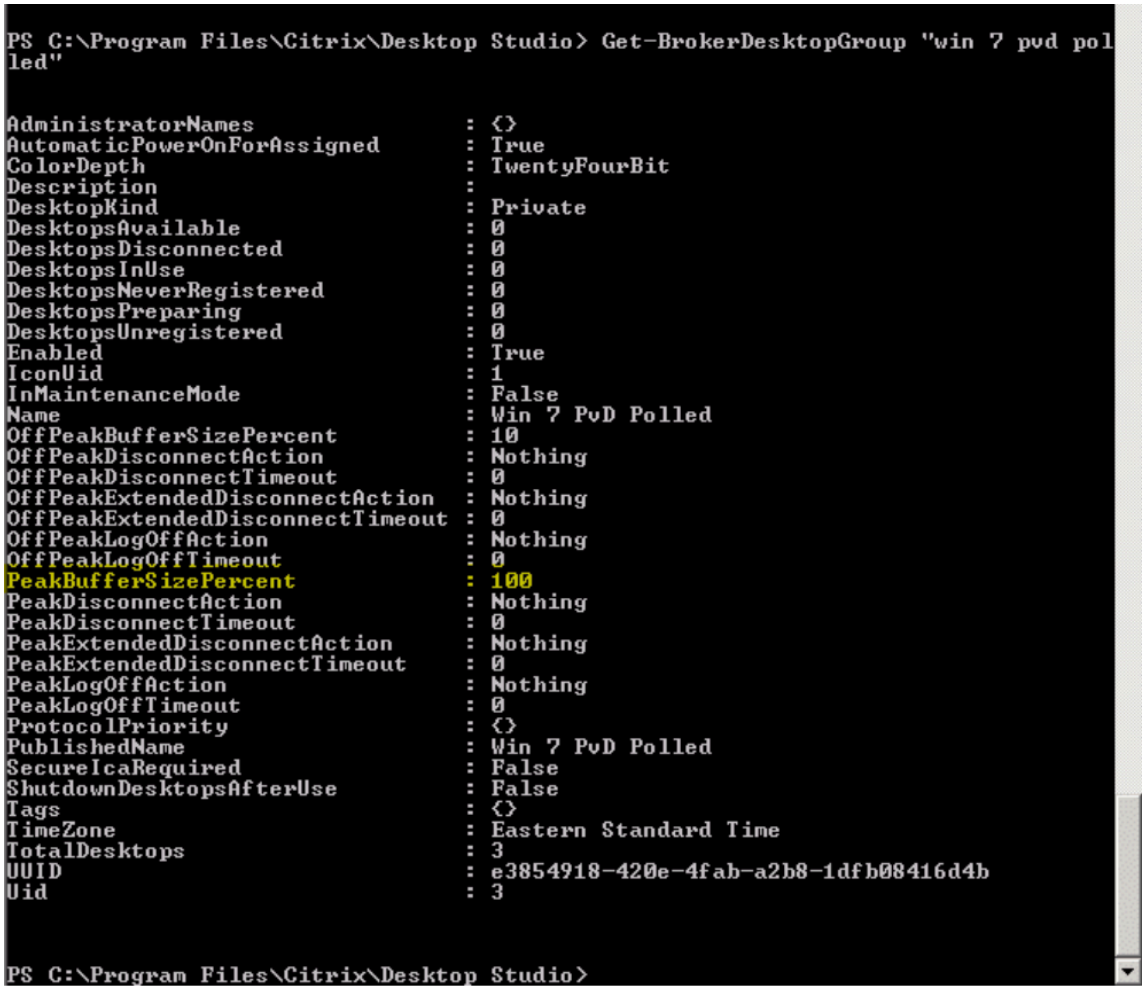
   ```
   asnp Citrix*

   # Set-BrokerDesktopGroup "Desktop Group Name"-PeakBufferSizePercent
    100
   ```

   Un valore pari a 100 indica che il 100% dei VDA è in stato pronto.

4. Verificare la soluzione eseguendo:

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```




Può occorrere fino a un’ora perché le modifiche abbiano effetto.

Per arrestare i VDA dopo che l’utente si è scollegato, immettere:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-ShutDownDesktopsAfterUse
 $True
```

Per riavviare i VDA durante le ore di punta, in modo che siano pronti per gli utenti dopo che si scollegano, immettere:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-AutomaticPowerOnForAssignedDurin
 $True
```

## Sessioni

- Scollegare o disconnettere una sessione o inviare un messaggio agli utenti
- Configurare il pre-lancio e la persistenza della sessione
- Controllare la riconnessione della sessione quando è disconnessa dalla macchina in modalità di manutenzione
- Configurare il roaming di sessione

### Scollegarsi o disconnettere una sessione

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo di consegna, quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.
3. Nel riquadro centrale selezionare il computer, selezionare **View Sessions** (Visualizza sessioni) nella barra delle azioni, quindi selezionare una sessione.
    - In alternativa, nel riquadro centrale selezionare la scheda **Session**, quindi selezionare una sessione.
4. Per scollegarsi da una sessione, selezionare **Log off** nella barra delle azioni. La sessione si chiude e l'utente è scollegato. La macchina diventa disponibile per altri utenti, a meno che non sia allocata a un utente specifico.
5. Per disconnettere una sessione, selezionare **Disconnect** nella barra delle azioni. Le applicazioni continuano a essere eseguite nella sessione e la macchina rimane allocata a quell'utente. L'utente può riconnettersi alla stessa macchina.

È possibile configurare i timer dello stato di alimentazione per i computer con sistema operativo a sessione singola in modo da gestire automaticamente le sessioni inutilizzate. Per informazioni dettagliate, vedere Macchine con alimentazione gestita.

### Inviare un messaggio a un gruppo di consegna

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo di consegna, quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.

3. Nel riquadro centrale selezionare una macchina a cui si desidera inviare un messaggio.
4. Nella barra delle azioni, selezionare **View Sessions** (Visualizza sessioni).
5. Nel riquadro centrale selezionare tutte le sessioni, quindi selezionare **Send Message** nella barra delle azioni.
6. Digitare il messaggio e fare clic su **OK**. Se necessario, è possibile specificare il livello di gravità. Le opzioni includono **Critical**, **Question**, **Warning** e **Information**.

In alternativa, è possibile inviare un messaggio utilizzando Citrix Director. Per ulteriori informazioni, vedere Inviare messaggi agli utenti.

### Configurare il pre-avvio della sessione e la permanenza della sessione in un gruppo di consegna

Queste funzionalità sono supportate solo su sistemi operativi multisessione.

Le funzioni di pre-avvio della sessione e di permanenza della sessione consentono agli utenti specificati di accedere rapidamente alle applicazioni, avviando le sessioni prima che siano richieste (pre-avvio della sessione) e mantenendo attive le sessioni delle applicazioni dopo che un utente ha chiuso tutte le applicazioni (permanenza della sessione).

Per impostazione predefinita, il pre-avvio della sessione e la permanenza della sessione non vengono utilizzati. Una sessione viene avviata (viene lanciata) quando un utente avvia un'applicazione e rimane attiva fino alla chiusura dell'ultima applicazione aperta nella sessione.

Considerazioni:

- Il gruppo di consegna deve supportare le applicazioni e le macchine devono eseguire un VDA per il sistema operativo multisessione, versione minima 7.6.
- Queste funzionalità sono supportate solo quando si utilizza l'app Citrix Workspace per Windows e richiedono anche una configurazione aggiuntiva dell'app Citrix Workspace. Per istruzioni, cercare il pre-avvio della sessione nella documentazione del prodotto per la propria versione dell'app Citrix Workspace per Windows.
- L'app Citrix Workspace per HTML5 non è supportata.
- Quando si utilizza il pre-avvio della sessione, se la macchina di un utente viene messa in modalità di sospensione o ibernazione, il pre-avvio non funziona (indipendentemente dalle impostazioni di pre-avvio della sessione). Gli utenti possono bloccare le loro macchine/sessioni. Tuttavia, se un utente si disconnette dall'app Citrix Workspace, la sessione viene terminata e il pre-avvio non è più applicabile.
- Quando si utilizza il pre-avvio della sessione, le macchine client fisiche non possono utilizzare le funzioni di gestione dell'alimentazione di sospensione o ibernazione. Gli utenti di macchine client possono bloccare le proprie sessioni, ma non devono scollegarsi.

- Il pre-avvio e la permanenza delle sessioni consumano una licenza per utilizzo simultaneo, ma solo quando sono connesse. Se si utilizza una licenza utente/dispositivo, la licenza dura 90 giorni. Le sessioni pre-avviate e in periodo di permanenza inutilizzate si disconnettono dopo 15 minuti per impostazione predefinita. Questo valore può essere configurato in PowerShell (cmdlet `New`/`Set-BrokerSessionPreLaunch`).
- Un'attenta pianificazione e il monitoraggio dei modelli di attività degli utenti sono essenziali per personalizzare queste funzionalità in modo che si completino. La configurazione ottimale trova un equilibrio fra i vantaggi della disponibilità delle applicazioni precedenti per gli utenti e il costo di mantenimento delle licenze in uso e dell'allocazione delle risorse.
- È inoltre possibile configurare il pre-avvio della sessione per un'ora pianificata nell'app Citrix Workspace.

**Per quanto tempo rimangono attive le sessioni pre-avviate e in periodo di permanenza se sono inutilizzate** Esistono diversi modi per specificare per quanto tempo una sessione inutilizzata debba rimanere attiva se l'utente non avvia un'applicazione: un timeout configurato e le soglie di caricamento del server. È possibile configurarli tutti. L'evento che si verifica prima causa la fine della sessione inutilizzata.

- **Timeout:** un timeout configurato specifica il numero di minuti, ore o giorni in cui una sessione pre-avviata o in periodo di permanenza inutilizzata rimane attiva. Se si configura un timeout troppo breve, le sessioni pre-avviate terminano prima che diano all'utente il vantaggio di un accesso più rapido alle applicazioni. Se si configura un timeout troppo lungo, potrebbero essere negate connessioni utente in ingresso perché il server non dispone di risorse sufficienti.

  È possibile abilitare questo timeout solo dall'SDK (cmdlet `New`/`Set-BrokerSessionPreLaunch`), non dalla console di gestione. Se si disattiva il timeout, questo non viene visualizzato nella visualizzazione della console per tale gruppo di consegna né nelle pagine **Edit Delivery Group** (Modifica gruppo di consegna).

- **Soglie:** la fine automatica delle sessioni pre-avviate e in periodo di permanenza in base al carico del server garantisce che le sessioni rimangano aperte il più a lungo possibile, supponendo che siano disponibili risorse server. Le sessioni pre-avviate e in periodo di permanenza inutilizzate non causano rifiuti delle connessioni, perché vengono terminate automaticamente quando sono necessarie risorse per nuove sessioni utente.

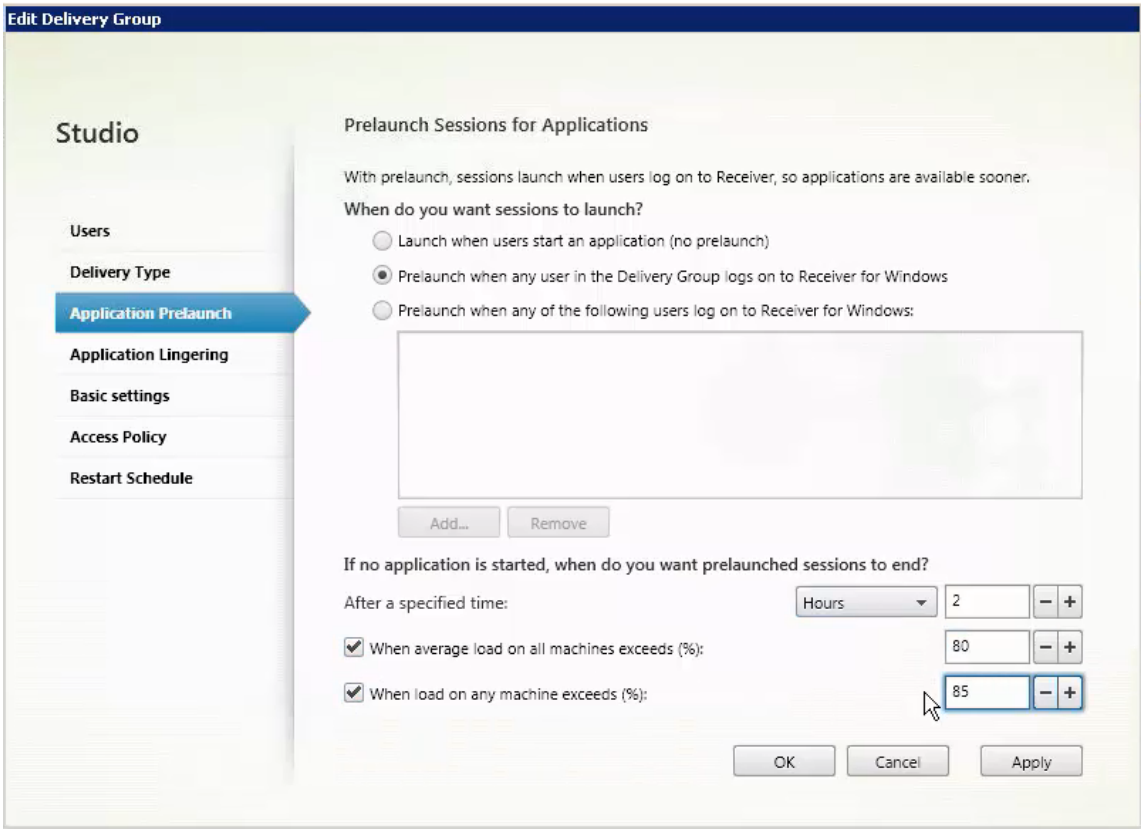
  È possibile configurare due soglie: il carico percentuale medio di tutti i server del gruppo di consegna e il carico percentuale massimo di un singolo server del gruppo. Quando viene superata una soglia, vengono terminate le sessioni che sono in stato di pre-avvio o di permanenza da più tempo. Le sessioni vengono terminate una per una a intervalli di un minuto fino a quando il carico scende al di sotto della soglia. Quando la soglia è stata superata, non vengono avviate nuove sessioni di pre-avvio.

I server con VDA non registrati con un controller e i server in modalità di manutenzione sono considerati a pieno carico. Un'interruzione non pianificata causa il completamento automatico delle sessioni in pre-avvio e in periodo di permanenza per liberare capacità.

**Per abilitare il pre-avvio della sessione**

1. Selezionare un gruppo, quindi fare clic su **Edit Delivery Group** (Modifica gruppo di consegna) nella barra delle azioni.
2. Nella pagina **Application Prelaunch** (Pre-avvio applicazioni), abilitare il pre-avvio della sessione scegliendo quando si avviano le sessioni:
   - Quando un utente avvia un'applicazione. Questa è l'impostazione predefinita. Il pre-avvio della sessione è disabilitato.
   - Quando qualsiasi utente del gruppo di consegna accede all'app Citrix Workspace per Windows.
   - Quando chiunque in un elenco di utenti e gruppi di utenti accede all'app Citrix Workspace per Windows. Assicurarsi di specificare anche utenti o gruppi di utenti se si sceglie questa opzione.




3. Una sessione pre-avviata viene sostituita con una sessione normale quando l'utente avvia un'applicazione. Se l'utente non avvia un'applicazione (la sessione pre-avviata non è utilizzata),

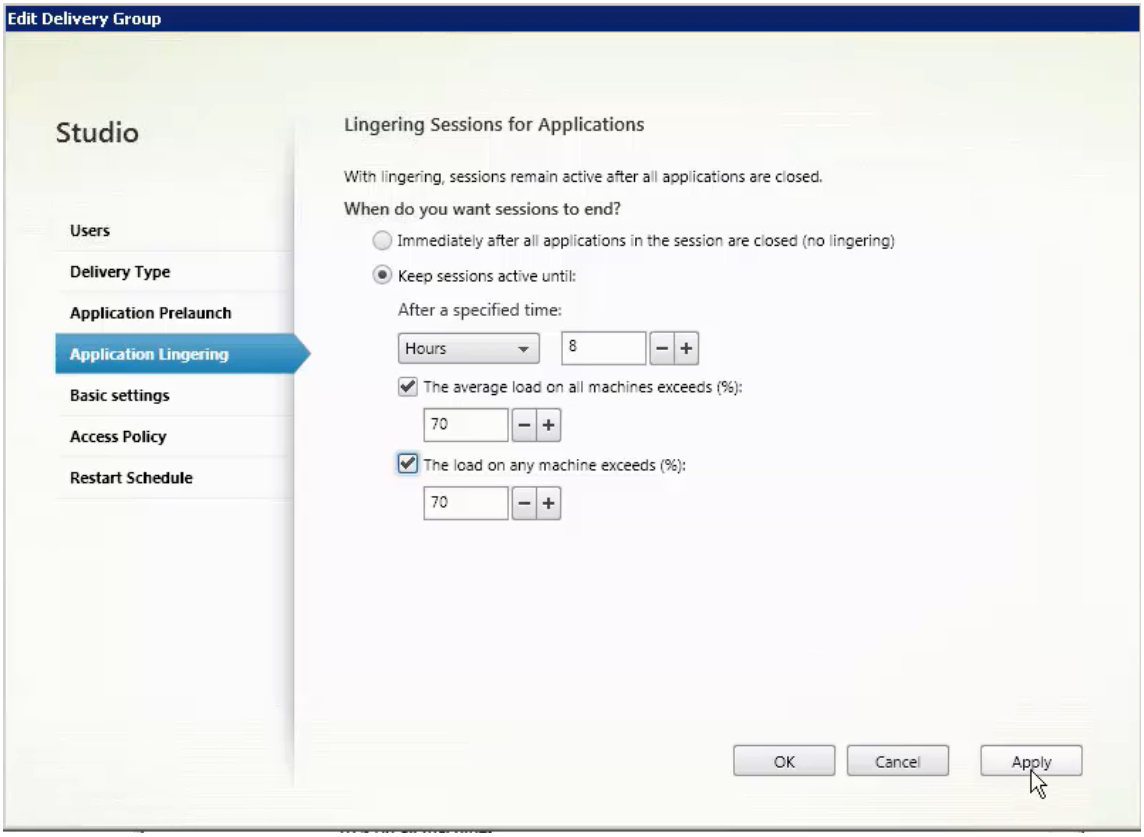
le impostazioni seguenti influiscono sul tempo in cui la sessione rimane attiva.

- Al termine di un intervallo di tempo specificato. È possibile modificare l'intervallo di tempo (1-99 giorni, 1-2376 ore o 1-142.560 minuti).
- Quando il carico medio di tutte le macchine del gruppo di consegna supera una percentuale specificata (1-99%).
- Quando il carico di qualsiasi macchina del gruppo di consegna supera una percentuale specificata (1-99%).

Riepilogo: una sessione pre-avviata rimane attiva fino a quando non si verifica uno dei seguenti eventi: un utente avvia un'applicazione, il tempo specificato è trascorso o viene superata una soglia di carico specificata.

**Per attivare la permanenza della sessione**

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi fare clic su **Edit Delivery Group** (Modifica gruppo di consegna) nella barra delle azioni.
3. Nella pagina **Application Lingering** (Permanenza applicazione), attivare la permanenza della sessione selezionando **Keep sessions active until** (Mantieni sessioni attive fino a).



4. Diverse impostazioni influiscono sul tempo in cui una sessione persistente rimane attiva se l'utente non avvia un'altra applicazione.

    - Al termine di un intervallo di tempo specificato. È possibile modificare l'intervallo di tempo: 1-99 giorni, 1-2376 ore o 1-142.560 minuti.
    - Quando il carico medio su tutte le macchine del gruppo di consegna supera una percentuale specificata: 1- 99%.
    - Quando il carico di qualsiasi macchina del gruppo di consegna supera una percentuale specificata: 1-99%.

    Riepilogo: una sessione in periodo di persistenza rimane attiva fino a quando non si verifica uno dei seguenti eventi: un utente avvia un'applicazione, il tempo specificato è trascorso o viene superata una soglia di carico specificata.

### Controllare la riconnessione della sessione quando è disconnessa dalla macchina in modalità di manutenzione

> **NOTA:**
>
> Questa funzionalità è disponibile solo in PowerShell.

È possibile controllare se le sessioni disconnesse su macchine in modalità di manutenzione possono riconnettersi alle macchine nel gruppo di consegna.

Prima della versione 2106, la riconnessione non era consentita per le sessioni desktop a sessione singola in pool che si erano disconnesse dalle macchine in modalità di manutenzione. A partire dalla versione 2106, è possibile configurare un gruppo di consegna per consentire o vietare le riconnessioni (indipendentemente dal tipo di sessione) dopo la disconnessione da una macchina in modalità di manutenzione.

Durante la creazione o la modifica di un gruppo di consegna (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`), utilizzare il parametro `-AllowReconnectInMaintenanceMode <boolean>` per consentire o vietare le riconconnessioni per le macchine scollegate da una macchina in modalità di manutenzione.

- Se è impostato su true, le sessioni possono riconnettersi alle macchine del gruppo.
- Se è impostato su false, le sessioni non possono riconnettersi alle macchine del gruppo.

Valori predefiniti:

- Sessione singola: Disabled (Disattivato)
- Multisessione: Enabled (Abilitato)

### Configurare il roaming di sessione

Per impostazione predefinita, il roaming delle sessioni è abilitato per i gruppi di consegna. Le sessioni sono in roaming fra i dispositivi client con l'utente. Quando l'utente avvia una sessione e si sposta su un altro dispositivo, viene utilizzata la stessa sessione e le applicazioni sono disponibili simultaneamente su entrambi i dispositivi. È possibile visualizzare le applicazioni su più dispositivi. Seguono le applicazioni, indipendentemente dal dispositivo o dall'esistenza di sessioni correnti. Spesso seguono anche stampanti e altre risorse assegnate all'applicazione. In alternativa, è possibile utilizzare PowerShell. Per ulteriori informazioni, vedere Roaming di sessione.

**Configurare il roaming di sessione per le applicazioni** Per configurare il roaming di sessione per le applicazioni, effettuare le seguenti operazioni:

1. Nella console, selezionare **Delivery Groups** nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit Delivery Group** (Modifica gruppo di consegna) nella barra delle azioni.
3. Nella pagina **Users** (Utenti), abilitare il roaming delle sessioni selezionando la casella di controllo **Sessions roam with users as they move between devices** (Sessioni in roaming con gli utenti mentre si spostano da un dispositivo all'altro).
    - Quando è abilitato, se un utente avvia una sessione di un'applicazione e si sposta su un altro dispositivo, la stessa sessione è in esecuzione e disponibile su entrambi i dispositivi. Quando è disabilitato, la sessione non è più accessibile da dispositivi diversi.
4. Selezionare **OK** per applicare le modifiche e chiudere la finestra.

**Configurare il roaming di sessione per i desktop** Per configurare il roaming di sessione per un desktop, effettuare le seguenti operazioni:

1. Nella console, selezionare **Delivery Groups** nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Desktops** (Desktop) selezionare il desktop e selezionare **Modifica**.
4. Abilitare il roaming della sessione selezionando la casella di controllo **Session roaming** (Roaming della sessione).

- Quando è abilitato, se un utente avvia il desktop e si sposta su un altro dispositivo, la stessa sessione è in esecuzione e le applicazioni sono disponibili su entrambi i dispositivi. Quando è disabilitato, la sessione non è più accessibile da dispositivi diversi.

Selezionare **OK** per applicare le modifiche e chiudere la finestra.

### Risoluzione dei problemi

- I VDA che non sono registrati con un Delivery Controller non vengono presi in considerazione quando si avviano sessioni mediate. Ciò si traduce in un sottoutilizzo di risorse altrimenti disponibili. Esistono vari motivi per cui un VDA potrebbe non essere registrato, molti dei quali sono risolvibili da un amministratore. La visualizzazione dei dettagli fornisce informazioni sulla risoluzione dei problemi nella creazione guidata del catalogo e dopo aver aggiunto un catalogo a un gruppo di consegna.

  Dopo aver creato un gruppo di consegna, il relativo riquadro dei dettagli indica il numero di macchine che possono essere registrate ma non lo sono. Ad esempio, una o più macchine sono accese e non in modalità manutenzione, ma non sono attualmente registrate presso un Controller. Quando si visualizza una macchina non registrata che dovrebbe esserlo, vedere la scheda **Troubleshoot** (Risoluzione dei problemi) nel riquadro dei dettagli per individuare le possibili cause e leggere le azioni correttive consigliate.

  Per i messaggi sul livello di funzionalità, vedere Versioni e livelli funzionali di VDA.

  Per informazioni sulla risoluzione dei problemi relativi alla registrazione di VDA, vedere CTX136668.

- Nella visualizzazione di un gruppo di consegna, la **versione VDA installata** nel riquadro dei dettagli potrebbe differire dalla versione effettiva installata sulle macchine. La visualizzazione Programmi e funzionalità di Windows della macchina mostra la versione VDA effettiva.
- Per le macchine con **stato di alimentazione sconosciuto**, vedere CTX131267 per informazioni.

## Creare gruppi di applicazioni

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

### Introduzione

I gruppi di applicazioni consentono di gestire raccolte di applicazioni. Creare gruppi di applicazioni per applicazioni condivise da diversi gruppi di consegna. Oppure applicazioni utilizzate da un sottoin-

sieme di utenti all'interno dei gruppi di consegna. I gruppi di applicazioni sono facoltativi e offrono un'alternativa all'aggiunta delle stesse applicazioni a più gruppi di consegna. Associare i gruppi di consegna a più di un gruppo di applicazioni e associare un gruppo di applicazioni a più di un gruppo di consegna.

L'uso di gruppi di applicazioni offre vantaggi in termini di gestione delle applicazioni e di controllo delle risorse rispetto all'uso di più gruppi di consegna.

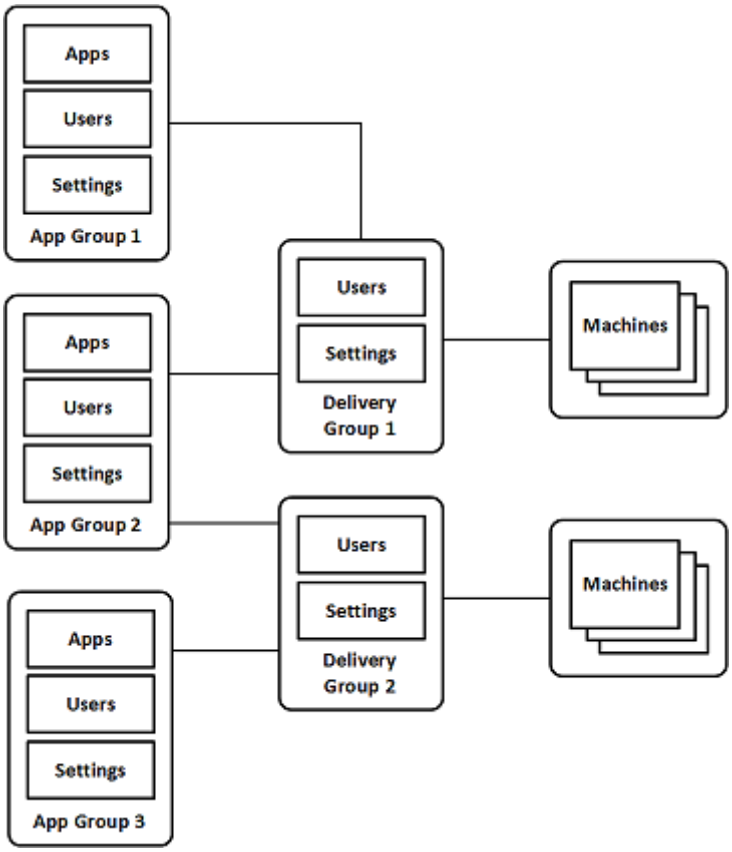
- Il raggruppamento logico delle applicazioni e le relative impostazioni consente di gestire tali applicazioni come un'unica unità. Ad esempio, non è necessario aggiungere (pubblicare) la stessa applicazione nei singoli gruppi di consegna uno alla volta.
- La condivisione della sessione tra gruppi di applicazioni consente di ridurre il consumo di risorse. In altri casi, può essere utile disabilitare la condivisione della sessione tra gruppi di applicazioni.
- È possibile utilizzare la funzione di restrizione tag per pubblicare applicazioni tratte da un gruppo di applicazioni, considerando solo un sottoinsieme di macchine in gruppi di consegna selezionati. Con le restrizioni tag, è possibile utilizzare i computer esistenti per più di un'attività di pubblicazione, risparmiando i costi associati alla distribuzione e alla gestione di macchine aggiuntive. Una restrizione tag può essere spiegata come una suddivisione (o la creazione di partizioni) delle macchine che fanno parte di un gruppo di consegna. L'utilizzo di un gruppo di applicazioni o di desktop con una restrizione tag può essere utile per isolare e risolvere i problemi di un sottoinsieme di macchine in un gruppo di consegna.

## Configurazioni di esempio

### Esempio 1:

Nell'immagine seguente è illustrata una distribuzione di Citrix Virtual Apps and Desktops che include gruppi di applicazioni:




In questa configurazione, le applicazioni vengono aggiunte ai gruppi di applicazioni, non ai gruppi di consegna. I gruppi di consegna specificano quali macchine vengono utilizzate (anche se è visibile, le macchine sono in cataloghi di macchine).

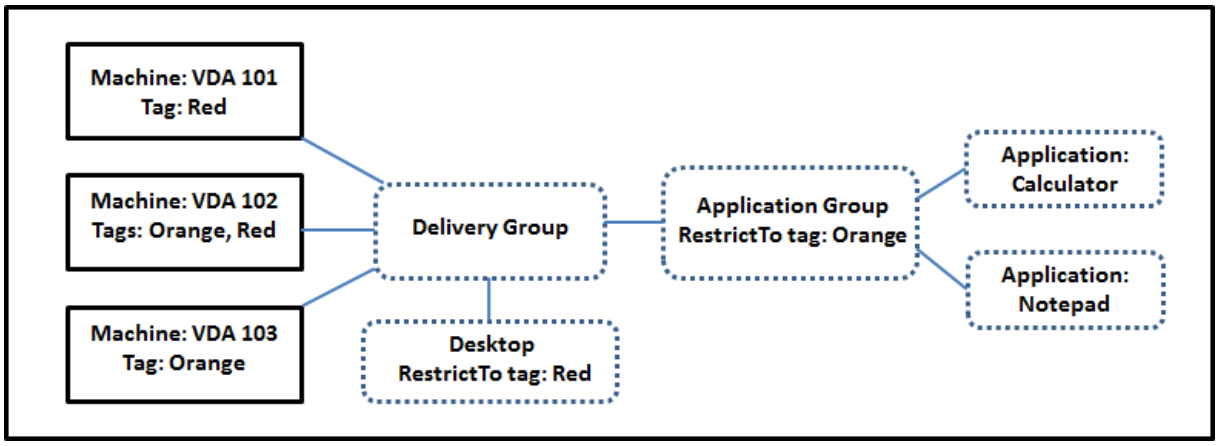
Il gruppo di applicazioni 1 è associato al gruppo di consegna 1. L'accesso alle applicazioni del gruppo di applicazioni 1 viene effettuato dagli utenti specificati nel gruppo di applicazioni 1. Questi gruppi vengono visualizzati solo fintanto che si trovano anche nell'elenco utenti del gruppo di consegna 1. Questa configurazione segue le indicazioni secondo cui l'elenco di utenti di un gruppo di applicazioni è un sottoinsieme (una restrizione) degli elenchi di utenti dei gruppi di consegna associati. Le impostazioni del gruppo di applicazioni 1 (ad esempio la condivisione della sessione dell'applicazione tra gruppi di applicazioni, i gruppi di consegna associati) si applicano alle applicazioni e agli utenti di tale gruppo. Le impostazioni del gruppo di consegna 1 si applicano agli utenti dei gruppi di applicazioni 1 e 2, poiché tali gruppi di applicazioni sono stati associati a tale gruppo di consegna.

Il gruppo di applicazioni 2 è associato a due gruppi di consegna: 1 e 2. A ciascuno di questi gruppi di consegna viene assegnata una priorità nel gruppo di applicazioni 2, che indica l'ordine in cui i gruppi di consegna vengono verificati quando viene avviata un'applicazione. I gruppi di consegna con la stessa priorità sono bilanciati dal carico. L'accesso alle applicazioni del gruppo di applicazioni 2 viene effettuato dagli utenti specificati nel gruppo di applicazioni 2. Tuttavia, devono anche essere visualizzati negli elenchi di utenti per il gruppo di consegna 1 e il gruppo di consegna 2.

**Esempio 2:**

Questo semplice layout utilizza restrizioni di tag per limitare quali macchine vengono considerate per alcuni lanci di desktop e applicazioni. Il sito dispone di un gruppo di consegna condiviso, un desktop pubblicato e un gruppo di applicazioni configurato con due applicazioni.




Sono stati aggiunti tag a ciascuna delle tre macchine (VDA 101-103).

Il gruppo di applicazioni è stato creato con la restrizione tag "Arancione". Ciascuna delle sue applicazioni viene lanciata solo su macchine che fanno parte di quel gruppo di consegna e che hanno il tag "Arancione", VDA 102 e 103.

Per esempi e indicazioni più completi sull'utilizzo delle restrizioni tag nei gruppi di applicazioni (e per i desktop), vedere Tag.

## Guida e considerazioni

Citrix consiglia di aggiungere le applicazioni a gruppi di applicazioni o a gruppi di consegna, ma non a entrambi. In caso contrario, la complessità aggiuntiva di avere applicazioni in due tipi di gruppo può rendere più difficile la gestione.

Per impostazione predefinita, un gruppo di applicazioni è abilitato. Dopo aver creato un gruppo di applicazioni, è possibile modificare il gruppo per cambiare questa impostazione. Vedere Gestire i gruppi di applicazioni.

Per impostazione predefinita, la condivisione della sessione dell'applicazione tra gruppi di applicazioni è abilitata. Vedere Condivisione della sessione tra gruppi di applicazioni.

Citrix consiglia di aggiornare i gruppi di consegna alla versione corrente. Questo processo richiede:

1. L'aggiornamento dei VDA sulle macchine utilizzate nel gruppo di consegna.
2. L'aggiornamento dei cataloghi di macchine contenenti quelle macchine.
3. L'aggiornamento del gruppo di consegna.

Per ulteriori informazioni, vedere Gestire i gruppi di consegna.

Per utilizzare i gruppi di applicazioni, la versione minima dei componenti principali è la 7.9.

La creazione di gruppi di applicazioni richiede l'autorizzazione di amministrazione delegata del ruolo predefinito di Amministratore gruppo di consegna. Per ulteriori informazioni, vedere Amministrazione delegata.

In questo articolo si fa riferimento al fatto di "associare"un'applicazione a più di un gruppo di applicazioni. Questa azione viene differenziata dall'aggiunta di istanze di tale applicazione da un'origine disponibile. Analogamente, i gruppi di consegna sono associati ai gruppi di applicazioni anziché essere aggiunte o componenti l'uno dell'altro.

## Condividere la sessione con gruppi di applicazioni

Quando la condivisione della sessione dell'applicazione è abilitata, tutte le applicazioni vengono avviate nella stessa sessione dell'applicazione. Ciò consente di risparmiare i costi associati all'avvio di più sessioni dell'applicazione e consente l'utilizzo di funzionalità dell'applicazione che comportano l'uso degli Appunti, ad esempio le operazioni di copia e incolla. Tuttavia, in alcune situazioni è possibile cancellare la condivisione della sessione.

Quando si utilizzano i gruppi di applicazioni, è possibile configurare la condivisione della sessione dell'applicazione nei tre modi seguenti che estendono il comportamento standard di condivisione della sessione che è disponibile quando si utilizzano solo gruppi di consegna:

- Condivisione della sessione abilitata tra gruppi di applicazioni.
- Condivisione della sessione abilitata solo tra applicazioni nello stesso gruppo di applicazioni.
- Condivisione della sessione disabilitata.

### Condivisione della sessione tra gruppi di applicazioni

È possibile abilitare la condivisione della sessione dell'applicazione tra gruppi di applicazioni oppure disabilitarla per limitare la condivisione della sessione dell'applicazione solo alle applicazioni dello stesso gruppo di applicazioni.

- **È utile un esempio di quando si abilita la condivisione della sessione tra gruppi di applicazioni:**

  Il gruppo di applicazioni 1 contiene applicazioni di Microsoft Office quali Word ed Excel. Il gruppo di applicazioni 2 contiene altre applicazioni quali Blocco note e Calcolatrice, ed entrambi i gruppi di applicazioni sono collegati allo stesso gruppo di consegna. Un utente che ha accesso a entrambi i gruppi di applicazioni inizia una sessione di applicazione avviando Word e quindi avvia Blocco note. Se il controller rileva che la sessione esistente dell'utente che esegue

Word è adatta all'esecuzione di Blocco note, questo viene avviato all'interno della sessione esistente. Se Blocco note non può essere eseguito dalla sessione esistente, ad esempio se la restrizione tag esclude la macchina su cui è in esecuzione la sessione, viene creata una nuova sessione su una macchine adatta anziché utilizzare la condivisione della sessione.

- **È utile un esempio di quando si disabilita la condivisione della sessione tra gruppi di applicazioni:**

  Una configurazione con un insieme di applicazioni che non interagiscono bene con le altre applicazioni installate sulle stesse macchine. Ad esempio due versioni diverse della stessa suite software o due versioni diverse dello stesso browser Web. Si preferisce non consentire a un utente di avviare entrambe le versioni nella stessa sessione.

  Creare un gruppo di applicazioni per ogni versione della suite software e aggiungere le applicazioni di ciascuna versione della suite software al gruppo di applicazioni corrispondente. Se la condivisione della sessione tra gruppi è disabilitata per ciascuno di questi gruppi di applicazioni, un utente specificato in tali gruppi può eseguire le applicazioni della stessa versione nella stessa sessione. L'utente può comunque eseguire altre applicazioni contemporaneamente, ma non nella stessa sessione. Quando si avvia una delle applicazioni di versioni diverse o qualsiasi applicazione non contenuta in un gruppo di applicazioni, tale applicazione viene avviata in una nuova sessione.

Questa funzionalità di condivisione della sessione tra gruppi di applicazioni non è una funzione sandboxing di protezione. Non è infallibile e non può impedire agli utenti di avviare applicazioni nelle loro sessioni tramite altri mezzi (ad esempio tramite Esplora risorse).

Se una macchina ha raggiunto la sua capacità massima, non vengono avviate nuove sessioni su di essa. Le nuove applicazioni vengono avviate nelle sessioni esistenti sul computer in base alle esigenze utilizzando la condivisione della sessione.

È possibile rendere solo le sessioni preavviate disponibili ai gruppi di applicazioni nei quali è consentita la condivisione della sessione dell'applicazione. Le sessioni che utilizzano la funzione di permanenza della sessione sono disponibili per tutti i gruppi di applicazioni. Queste funzionalità devono essere abilitate e configurate in ciascuno dei gruppi di consegna associati al gruppo di applicazioni. Non è possibile configurarli nei gruppi di applicazioni.

Per impostazione predefinita, la condivisione della sessione dell'applicazione tra gruppi di applicazioni è abilitata quando si crea un gruppo di applicazioni. Non è possibile modificare questa impostazione quando si crea il gruppo. Dopo aver creato un gruppo di applicazioni, è possibile modificare il gruppo per cambiare questa impostazione. Vedere Gestire i gruppi di applicazioni.

#### Disabilitare la condivisione della sessione all'interno di un gruppo di applicazioni

È possibile impedire la condivisione della sessione tra applicazioni che si trovano nello stesso gruppo di applicazioni.

- **È utile osservare l'esempio di quando si disabilita la condivisione della sessione all'interno dei gruppi di applicazioni:**

  Si desidera che gli utenti accedano a più sessioni a schermo intero simultanee di un'applicazione su monitor separati.

  È possibile creare un gruppo di applicazioni e aggiungervi le applicazioni.

Per impostazione predefinita, la condivisione della sessione delle applicazioni è abilitata quando si crea un gruppo di applicazioni. Non è possibile modificare questa impostazione quando si crea il gruppo. Dopo aver creato un gruppo di applicazioni, è possibile modificare il gruppo per cambiare questa impostazione. Vedere Gestire i gruppi di applicazioni.

### Creare un gruppo di applicazioni

Per creare un gruppo di applicazioni:

1. Accedere a Web Studio.
2. Selezionare **Applications** nel riquadro a sinistra, quindi seleziona la scheda **Application Groups** (Gruppi di applicazioni).
3. Per organizzare i gruppi di applicazioni utilizzando le cartelle, create cartelle nella cartella principale **Application Groups** (Gruppi di applicazioni).
4. Selezionare la cartella in cui si desidera creare il gruppo, quindi fare clic su **Create Application Group** (Crea gruppo di applicazioni). La procedura guidata per la creazione del gruppo viene avviata con una **pagina introduttiva**. È possibile rimuovere la pagina dai lanci futuri di questa procedura guidata.
5. Seguire la procedura guidata per configurare le impostazioni nelle pagine descritte di seguito. Al termine di ogni pagina, selezionare **Next** (Avanti) fino a raggiungere la pagina **Summary** (Riepilogo).

#### Passaggio 1. Gruppi di consegna

La pagina **Delivery Groups** elenca tutti i gruppi di consegna, con il numero di macchine contenuto da ciascuno gruppo.

- L'elenco **Compatible Delivery Groups** (Gruppi di consegna compatibili) contiene i gruppi di consegna che è possibile selezionare. I gruppi di consegna compatibili contengono macchine

con sistema operativo multisessione o a sessione singola casuali (non assegnate in modo permanente o statico).
- L'elenco **Incompatible Delivery Groups** (Gruppi di consegna non compatibili) contiene gruppi di consegna che non è possibile selezionare. Ogni voce contiene la spiegazione del perché non è compatibile, ad esempio perché contiene macchine assegnate staticamente.

Un gruppo di applicazioni può essere associato a gruppi di consegna contenenti macchine condivise (non private) in grado di distribuire applicazioni.

È inoltre possibile selezionare gruppi di consegna contenenti macchine condivise che consegnano solo desktop, se sono soddisfatte entrambe le seguenti condizioni:

- Il gruppo di consegna contiene macchine condivise ed è stato creato con una versione di XenDesktop precedente alla 7.9.
- Si ha l'autorizzazione Edit Delivery Group (Modifica gruppo di consegna).

Il tipo di gruppo di consegna viene automaticamente convertito in "desktop e applicazioni"quando viene eseguito il commit della procedura guidata di creazione del gruppo di applicazioni.

Sebbene sia possibile creare un gruppo di applicazioni a cui non sono associati gruppi di consegna (ad esempio per organizzare le applicazioni o come archiviazione delle applicazioni non attualmente utilizzate), il gruppo di applicazioni non può essere utilizzato per consegnare le applicazioni finché non specifica almeno un gruppo di consegna. Inoltre, non è possibile aggiungere applicazioni al gruppo di applicazioni dall'origine del menu **From Start** se non sono specificati gruppi di consegna.

I gruppi di consegna selezionati specificano le macchine utilizzate per consegnare le applicazioni. Selezionare le caselle di controllo accanto ai gruppi di consegna che si desidera associare al gruppo di applicazioni.

Per aggiungere una restrizione tag, selezionare **Restrict launches to machines with the tag** (Limita lanci ai computer con il tag), quindi selezionare il tag dall'elenco a discesa.

#### Passaggio 2. Utenti

Specificare gli utenti dell'applicazione nel gruppo di applicazioni. Accettare tutti gli utenti e i gruppi di utenti presenti nei gruppi di consegna selezionati nella pagina precedente oppure selezionare utenti e gruppi di utenti specifici da quei gruppi di consegna. Se si limita l'uso a utenti specificati, solo gli utenti specificati nel gruppo di consegna possono accedere alle applicazioni di questo gruppo. In sostanza, l'elenco utenti specificato nel gruppo di applicazioni fornisce un filtro per gli elenchi di utenti dei gruppi di consegna.

L'attivazione o la disabilitazione dell'utilizzo delle applicazioni da parte di utenti non autenticati è disponibile solo nei gruppi di consegna e non nei gruppi di applicazioni.

Per informazioni sulla posizione in cui vengono specificati gli elenchi di utenti in una distribuzione, vedere Dove vengono specificati gli elenchi di utenti.

#### Passaggio 3. Applicazioni

Buono a sapersi:

- Per impostazione predefinita, le nuove applicazioni aggiunte vengono inserite in una cartella denominata **Applications**. È possibile specificare una cartella diversa. Se si tenta di aggiungere un'applicazione e in quella cartella ne esiste già una con lo stesso nome, verrà richiesto di rinominare l'applicazione che si sta aggiungendo. Se si accetta il nome univoco suggerito, l'applicazione viene aggiunta con il nuovo nome. In caso contrario, è necessario rinominarlo prima di poterlo aggiungere. Per ulteriori informazioni, vedere Gestire le cartelle delle applicazioni.
- È possibile modificare le proprietà (impostazioni) di un'applicazione al momento dell'aggiunta o in un secondo momento. Vedere Modificare le proprietà dell'applicazione. Se si pubblicano due applicazioni con lo stesso nome per gli stessi utenti, modificare la proprietà **Application name (for user)** [Nome applicazione (per utente)] in Web Studio. In caso contrario, gli utenti vedranno nomi duplicati nell'app Citrix Workspace.
- Quando si aggiunge un'applicazione a più gruppi di applicazioni, può verificarsi un problema di visibilità se non si dispone di autorizzazioni sufficienti a visualizzare l'applicazione in tutti questi gruppi. In questi casi, vedere un amministratore con autorizzazioni di livello superiore o estendere il proprio ambito in modo da includere tutti i gruppi a cui è stata aggiunta l'applicazione.

Fare clic su **Add** (Aggiungi) nel menu a discesa per visualizzare le origini dell'applicazione.

- **Menu From Start:** applicazioni che vengono individuate su una macchina nei gruppi di consegna selezionati. Quando si seleziona questa origine, viene avviata una nuova pagina con un elenco delle applicazioni individuate. Selezionare le caselle di controllo delle applicazioni da aggiungere e quindi fare clic su **OK**.

  Questa origine non può essere selezionata se è stata selezionata una delle seguenti opzioni:

  - Gruppi di applicazioni a cui non sono associati gruppi di consegna.
  - Gruppi di applicazioni a cui sono associati gruppi di consegna che non contengono macchine.
  - Un gruppo di consegna che non contiene macchine.

- **Manually defined** (Definizione manuale): applicazioni situate nel sito o in un altro punto della rete. Quando si seleziona questa origine, viene avviata una nuova pagina in cui si digita il percorso dell'eseguibile, della directory di lavoro, degli argomenti della riga di comando facoltativi e dei nomi visualizzati per amministratori e utenti. Dopo aver immesso queste informazioni, fare clic su **OK**.

- **Existing** (Esistenti): applicazioni precedentemente aggiunte al sito. Quando si seleziona questa origine, viene avviata una nuova pagina con un elenco delle applicazioni individuate. Selezionare le caselle di controllo delle applicazioni da aggiungere e quindi fare clic su **OK**. Non è possibile selezionare questa origine se il sito non dispone di applicazioni.
- **App-V**: applicazioni contenute in pacchetti App-V. Quando si seleziona questa origine, viene avviata una nuova pagina in cui si seleziona **App-V server** o **Application Library**. Nella schermata risultante, selezionare le caselle di controllo delle applicazioni da aggiungere e quindi fare clic su **OK**. Per ulteriori informazioni, vedere applications.Distribuire e rendere disponibili applicazioni App-V. Questa origine non può essere selezionata (o potrebbe non essere visualizzata) se App-V non è configurato per il sito.

Come già osservato, alcune voci del menu a discesa **Add** non sono selezionabili se non esiste una fonte valida di quel tipo. Le origini non compatibili non sono elencate (ad esempio, non è possibile aggiungere gruppi di applicazioni ai gruppi di applicazioni, quindi quell'origine non è elencata quando si crea un gruppo di applicazioni).

#### Passaggio 4. Ambiti

Questa pagina viene visualizzata solo se in precedenza è stato creato un ambito personalizzato. Per impostazione predefinita, è selezionato l'ambito **All**. Per ulteriori informazioni, vedere Amministrazione delegata.

#### Passaggio 5. Riepilogo

Immettere un nome per il gruppo di applicazioni. È inoltre possibile (facoltativamente) inserire una descrizione.

Esaminare le informazioni di riepilogo e quindi fare clic su **Finish**.

## Gestire i gruppi di applicazioni

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo

> riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

## Introduzione

In questo articolo viene descritto come gestire i gruppi di applicazioni creati.

Vedere Applications (Applicazioni) per informazioni sulla gestione delle applicazioni nei gruppi di applicazioni o nei gruppi di consegna, comprese le procedure seguenti:

- Aggiungere o rimuovere applicazioni in un gruppo di applicazioni.
- Modificare le associazioni dei gruppi di applicazioni.

La gestione dei gruppi di applicazioni richiede le autorizzazioni di amministrazione delegate del ruolo predefinito Amministratore gruppo di consegna. Per ulteriori informazioni, vedere Amministrazione delegata.

## Attivare o disattivare un gruppo di applicazioni

Quando un gruppo di applicazioni è abilitato, può consegnare le applicazioni che sono state aggiunte ad esso. La disattivazione di un gruppo di applicazioni disabilita tutte le applicazioni del gruppo. Tuttavia, se tali applicazioni sono associate anche ad altri gruppi di applicazioni abilitati, possono essere recapitate da tali altri gruppi. Se l'applicazione è stata aggiunta in modo esplicito ai gruppi di consegna associati al gruppo di applicazioni, la disattivazione del gruppo di applicazioni non influisce sulle applicazioni che fanno parte di tali gruppi di consegna.

Un gruppo di applicazioni è abilitato quando lo si crea. Non è possibile modificare questa configurazione quando si crea il gruppo.

1. Selezionare **Applications** nel riquadro a sinistra, quindi seleziona la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni, quindi selezionare **Edit Application Group** (Modifica gruppo di applicazioni) nella barra delle azioni.
3. Nella pagina **Settings** (Impostazioni), selezionare o deselezionare la casella di controllo **Enable Application Group** (Abilita gruppo di applicazioni).
4. Fare clic su **Apply** per mantenere aperta la finestra oppure fare clic su **Save** per applicare le modifiche e chiudere la finestra.

### Attivare o disattivare la condivisione della sessione delle applicazioni tra gruppi di applicazioni

La condivisione della sessione tra gruppi di applicazioni è abilitata quando si crea un gruppo di applicazioni. Non è possibile modificare questa configurazione quando si crea il gruppo. Per ulteriori informazioni, vedere Condivisione della sessione tra gruppi di applicazioni.

1. Selezionare **Applications** nel riquadro a sinistra, quindi seleziona la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni, quindi selezionare **Edit Application Group** (Modifica gruppo di applicazioni) nella barra delle azioni.
3. Nella pagina **Settings** selezionare o deselezionare la casella di controllo **Enable application session sharing between Application Groups** (Abilita condivisione della sessione delle applicazioni tra gruppi di applicazioni).
4. Fare clic su **Apply** per mantenere aperta la finestra oppure fare clic su **Save** per applicare le modifiche e chiudere la finestra.

### Disabilitare la condivisione della sessione delle applicazioni all'interno di un gruppo di applicazioni

La condivisione della sessione tra applicazioni nello stesso gruppo di applicazioni è abilitata per impostazione predefinita quando si crea un gruppo di applicazioni. Se si disattiva la condivisione della sessione delle applicazioni tra gruppi di applicazioni, la condivisione della sessione tra applicazioni che appartengono allo stesso gruppo di applicazioni rimane abilitata.

È possibile utilizzare PowerShell SDK per configurare gruppi di applicazioni con la condivisione della sessione delle applicazioni disabilitata tra le applicazioni in essi contenute. In alcune circostanze questa opzione è desiderabile. Ad esempio, si potrebbe avere necessità che gli utenti avviino le applicazioni non integrate in finestre di applicazione a schermo intero su monitor separati.

Quando si disattiva la condivisione della sessione delle applicazioni all'interno di un gruppo di applicazioni, ciascuna applicazione del gruppo viene avviata in una nuova sessione dell'applicazione. Se è disponibile una sessione disconnessa adatta che esegue la stessa applicazione, questa viene riconnessa. Ad esempio, quando si avvia Blocco note con una sessione disconnessa con Blocco note in esecuzione, viene riconnessa tale sessione anziché crearne una nuova. Quando sono disponibili più sessioni disconnesse adatte, una delle sessioni viene scelta come quella a cui riconnettersi, in modo casuale ma deterministico. Quando la situazione si ripresenta nelle stesse circostanze, viene scelta la stessa sessione, ma la sessione non è necessariamente prevedibile altrimenti.

Utilizzare PowerShell SDK per disattivare la condivisione della sessione dell'applicazione per tutte le applicazioni di un gruppo di applicazioni esistente oppure per creare un gruppo con la condivisione della sessione delle applicazioni disabilitata.

#### Esempi di cmdlet PowerShell

Per disattivare la condivisione della sessione, utilizzare il cmdlet Broker PowerShell `New-BrokerApplicationGroup` o il cmdlet `Set-BrokerApplicationGroup` con il parametro `SessionSharingEnabled` impostato su `False` e il parametro `SingleAppPerSession` impostato su `True`.

- Ad esempio, per creare un gruppo di applicazioni con la condivisione della sessione delle applicazioni disabilitata per tutte le applicazioni del gruppo:

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

- Ad esempio, per disabilitare la condivisione della sessione delle applicazioni tra tutte le applicazioni di un gruppo di applicazioni esistente:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

#### Considerazioni

- Per attivare la proprietà `SingleAppPerSession`, è necessario impostare la proprietà `SessionSharingEnabled` su False. Le due proprietà non devono essere abilitate contemporaneamente. Il parametro `SessionSharingEnabled` si riferisce alla condivisione della sessione tra gruppi di applicazioni.
- La condivisione della sessione delle applicazioni funziona solo per le applicazioni che sono associate a gruppi di applicazioni ma non a gruppi di consegna. Tutte le applicazioni associate direttamente a un gruppo di consegna condividono la sessione per impostazione predefinita.
- Se un'applicazione è assegnata a più gruppi di applicazioni, assicurarsi che non vi siano impostazioni in conflitto tra i gruppi. Ad esempio, se un gruppo ha l'opzione impostata su `True` e un altro ce l'ha impostata su `False` ne deriva un comportamento imprevedibile.

### Rinominare un gruppo di applicazioni

1. Selezionare **Applications** nel riquadro a sinistra, quindi seleziona la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni e quindi selezionare **Rename Application Group** (Rinomina gruppo di applicazioni) nella barra delle azioni.
3. Specificare il nuovo nome univoco e quindi fare clic su **OK**.

### Aggiungere, rimuovere o modificare la priorità delle associazioni dei gruppi di consegna con un gruppo di applicazioni

Un gruppo di applicazioni può essere associato a gruppi di consegna contenenti macchine condivise (non private) in grado di distribuire applicazioni.

È inoltre possibile selezionare gruppi di consegna contenenti macchine condivise che consegnano solo desktop, se sono soddisfatte entrambe le seguenti condizioni:

- Il gruppo di consegna contiene macchine condivise ed è stato creato con una versione precedente alla 7.9.
- Si ha l'autorizzazione Edit Delivery Group (Modifica gruppo di consegna).

Il tipo di gruppo di consegna viene automaticamente convertito in "desktop e applicazioni"quando viene eseguito il commit della finestra di dialogo **Edit Application Group** (Modifica gruppo di applicazioni).

1. Selezionare **Applications** nel riquadro a sinistra, quindi seleziona la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni, quindi selezionare **Edit Application Group** (Modifica gruppo di applicazioni) nella barra delle azioni.
3. Selezionare la pagina **Delivery Groups** (Gruppi di consegna).
4. Per aggiungere gruppi di consegna, fare clic su **Add**. Selezionare le caselle di controllo dei gruppi di consegna disponibili (i gruppi di consegna non compatibili non possono essere selezionati). Al termine delle selezioni, fare clic su **OK**.
5. Per rimuovere i gruppi di consegna, selezionare le caselle di controllo dei gruppi da rimuovere e quindi fare clic su **Remove**. Confermare l'eliminazione quando richiesto.
6. Per modificare la priorità dei gruppi di consegna, selezionare la casella di controllo del gruppo di consegna e quindi fare clic su **Edit Priority** (Modifica priorità). Immettere la priorità (0= massima), quindi fare clic su **OK**.
7. Fare clic su **Apply** per applicare le modifiche apportate e mantenere aperta la finestra oppure su **Save** per applicare le modifiche e chiudere la finestra.

### Aggiungere, modificare o rimuovere una restrizione tag in un gruppo di applicazioni

L'aggiunta, la modifica e la rimozione di restrizioni tag può avere effetti imprevisti su quali macchine vengono considerate per il lancio delle applicazioni. Leggere le considerazioni e le avvertenze in Tag.

1. Selezionare **Applications** nel riquadro a sinistra, quindi seleziona la scheda **Application Groups** (Gruppi di applicazioni).

2. Selezionare un gruppo di applicazioni, quindi selezionare **Edit Application Group** (Modifica gruppo di applicazioni) nella barra delle azioni.
3. Selezionare la pagina **Delivery Groups** (Gruppi di consegna).
4. Per aggiungere una restrizione tag, selezionare **Restrict launches to machines with the tag** (Limita lanci ai computer con il tag), quindi selezionare il tag dall'elenco a discesa.
5. Per modificare o rimuovere una restrizione tag, selezionare un tag diverso o rimuovere completamente la restrizione tag deselezionando **Restrict launches to machines with this tag** (Limita lanci alle macchine con questo tag).
6. Fare clic su **Apply** per applicare le modifiche apportate e mantenere aperta la finestra oppure su **Save** per applicare le modifiche e chiudere la finestra.

### Aggiungere o rimuovere utenti in un gruppo di applicazioni

Per informazioni dettagliate sugli utenti, vedere Creare gruppi di applicazioni.

1. Selezionare **Applications** nel riquadro a sinistra, quindi seleziona la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni, quindi selezionare **Edit Application Group** (Modifica gruppo di applicazioni) nella barra delle azioni.
3. Selezionare la pagina **Users**. Indicare se si desidera consentire di utilizzare le applicazioni incluse nel gruppo di applicazioni a tutti gli utenti dei gruppi di consegna associati oppure solo utenti e gruppi specifici. Per aggiungere utenti, fare clic su **Add** (Aggiungi) e specificare gli utenti da aggiungere. Per rimuovere utenti, selezionare uno o più utenti, quindi fare clic su **Remove** (Rimuovi).
4. Fare clic su **Apply** per applicare le modifiche apportate e mantenere aperta la finestra oppure su **Save** per applicare le modifiche e chiudere la finestra.

### Aggiungere, modificare o rimuovere l'icona di un'applicazione in un gruppo di applicazioni

Per aggiungere, modificare o rimuovere l'icona di un'applicazione, attenersi alla seguente procedura.

1. Selezionare **Applications** nel riquadro a sinistra.
2. Nella scheda **Applications** (Applicazioni), selezionare un'applicazione e quindi scegliere **Properties** (Proprietà).

   Per apportare modifiche a livello di gruppo di applicazioni, passare alla scheda **Application Groups** (Gruppi di applicazioni), selezionare un'applicazione in un gruppo e quindi scegliere **Properties** (Proprietà).

3. Selezionare la pagina **Delivery** (Consegna), quindi selezionare **Change** (Modifica). Viene visualizzata la finestra **Select icon** (Seleziona icona).
4. Nella finestra **Select icon** (Seleziona icona), effettuare una delle seguenti operazioni:
   - Per aggiungere un'icona, selezionare **Add** (Aggiungi), quindi selezionare l'icona.
   - Per rimuovere un'icona, selezionarla e quindi selezionare **Remove** (Rimuovi).
   - Per modificare un'icona, selezionarla per l'applicazione.

   > **Importante:**
   >
   > - Non è possibile aggiungere un'icona di dimensioni superiori a 200 KB.
   > - È possibile aggiungere solo file con estensione .icon.
   > - Non è possibile rimuovere le icone incorporate.
   > - Non è possibile rimuovere l'icona di un'applicazione in uso.

5. Selezionare **Save** per applicare le modifiche e chiudere la finestra.

### Modificare gli ambiti in un gruppo di applicazioni

È possibile modificare un ambito solo se lo si è creato (non è possibile modificare l'ambito All). Per ulteriori informazioni, vedere Amministrazione delegata.

1. Selezionare **Applications** nel riquadro a sinistra, quindi seleziona la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni, quindi selezionare **Edit Application Group** (Modifica gruppo di applicazioni) nella barra delle azioni.
3. Selezionare la pagina **Scopes** (Ambiti). Selezionare o deselezionare la casella di controllo accanto a un ambito.
4. Fare clic su **Apply** per applicare le modifiche apportate e mantenere aperta la finestra oppure su **Save** per applicare le modifiche e chiudere la finestra.

### Modificare gli ambiti in un gruppo di applicazioni

È possibile modificare un ambito solo se lo si è creato (non è possibile modificare l'ambito All). Per ulteriori informazioni, vedere Amministrazione delegata.

1. Selezionare **Applications** nel riquadro a sinistra, quindi seleziona la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni, quindi selezionare **Edit Application Group** (Modifica gruppo di applicazioni) nella barra delle azioni.

3. Selezionare la pagina **Scopes** (Ambiti). Selezionare o deselezionare la casella di controllo accanto agli ambiti che si desidera modificare.
4. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra oppure **Save** per applicare le modifiche e chiudere la finestra.

## Eliminare un gruppo di applicazioni

Un'applicazione deve essere associata ad almeno un gruppo di consegna o un gruppo di applicazioni. Se dopo l'eliminazione di un gruppo di applicazioni una o più applicazioni non appartengono più a un gruppo, viene visualizzato un avviso che l'eliminazione di tale gruppo rimuove anche tali applicazioni. È quindi possibile confermare o annullare l'eliminazione.

L'eliminazione di un'applicazione non la elimina dall'origine da cui proveniva originariamente. Tuttavia, se si desidera renderla nuovamente disponibile, è necessario aggiungerla di nuovo.

1. Selezionare **Applications** nel riquadro a sinistra, quindi seleziona la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni e quindi selezionare **Delete Group** (Elimina gruppo) nella barra delle azioni.
3. Confermare l'eliminazione quando richiesto.

## Organizzare i gruppi di applicazioni utilizzando le cartelle

È possibile creare cartelle per organizzare i gruppi di applicazioni per un facile accesso.

### Ruoli richiesti

Per impostazione predefinita, è possibile creare e gestire cartelle per i gruppi di applicazioni se si dispone di uno dei seguenti ruoli predefiniti:

- Cloud Administrator (Amministratore cloud)
- Full Administrator (Amministratore completo)
- Application Group Administrator (Amministratore del gruppo di applicazioni)

È possibile delegare le azioni di gestione ad altri utenti creando ruoli personalizzati. Nella tabella seguente sono elencate le autorizzazioni richieste per ogni azione.

| Azione | Autorizzazioni richieste |
|---|---|
| Creare cartelle per gruppi di applicazioni | Create Application Group Folder |

| Azione | Autorizzazioni richieste |
| --- | --- |
| Eliminare le cartelle dei gruppi di applicazioni | Remove Application Group Folder |
| Spostare le cartelle dei gruppi di applicazioni | Move Application Group Folder |
| Rinominare le cartelle dei gruppi di applicazioni | Edit Application Group Folder |
| Spostare i gruppi di applicazioni nelle cartelle | Edit Application Group Folder, Edit Application Group Properties |

Per ulteriori informazioni, vedere Creare e gestire ruoli.

#### Creare e gestire le cartelle

È possibile utilizzare la barra Actions o il menu di scelta rapida per creare e gestire le cartelle dei gruppi di applicazioni. Inoltre, è possibile trascinare un gruppo di applicazioni o una cartella nella posizione desiderata nell'albero delle cartelle.

Buono a sapersi:

- È possibile nidificare le cartelle fino a cinque livelli (esclusa la cartella principale predefinita).
- Una cartella può contenere gruppi di applicazioni e sottocartelle. È possibile eliminare una cartella solo se essa e le relative sottocartelle non contengono gruppi di applicazioni.
- Tutti i nodi (quali cataloghi di macchine, gruppi di consegna, applicazioni e gruppi di applicazioni) condividono un albero di cartelle nel back-end. Per evitare conflitti di nomi con altre cartelle di risorse durante la ridenominazione o lo spostamento di cartelle, si consiglia di assegnare nomi diversi alle cartelle di primo livello in alberi di cartelle diversi.

## Accesso remoto al PC

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Accesso remoto PC è una funzionalità di Citrix Virtual Apps and Desktops che consente alle organizzazioni di consentire ai dipendenti di accedere facilmente alle risorse aziendali in remoto in modo

sicuro. La piattaforma Citrix rende possibile questo accesso sicuro offrendo agli utenti l'accesso ai PC fisici dell'ufficio. If users can access their office PCs, they can access all the applications, data, and resources they need to do their work. Accesso remoto PC elimina la necessità di introdurre e fornire altri strumenti per il telelavoro. Ad esempio, desktop o applicazioni virtuali e la relativa infrastruttura associata.

Accesso remoto PC utilizza gli stessi componenti Citrix Virtual Apps and Desktops che forniscono desktop e applicazioni virtuali. Di conseguenza, i requisiti e il processo di distribuzione e configurazione di Accesso remoto PC sono gli stessi richiesti per la distribuzione di Citrix Virtual Apps and Desktops per la distribuzione di risorse virtuali. Questa uniformità offre un'esperienza amministrativa coerente e unificata. Gli utenti ricevono la migliore esperienza utente utilizzando Citrix HDX per offrire la propria sessione PC da ufficio.

La funzionalità è costituita da un catalogo di macchine di tipo **Accesso remoto PC** che fornisce le seguenti funzionalità:

- Possibilità di aggiungere macchine specificando le OE. Questa capacità facilita l'aggiunta di PC in blocco.
- Assegnazione automatica degli utenti in base all'utente che accede al PC Windows dell'ufficio. Supportiamo le assegnazioni di utenti singoli e più utenti. Per impostazione predefinita, assegniamo automaticamente più utenti alla successiva macchina non assegnata. Per limitare l'assegnazione automatica a un singolo utente, accedere a Web Studio, andare a **Settings** e disattiva l'impostazione **Enable automatic assignment of multiple users for Remote PC Access** (Abilita l'assegnazione automatica di più utenti per l'accesso remoto al PC).

Citrix Virtual Apps and Desktops può gestire più casi d'uso per PC fisici utilizzando altri tipi di cataloghi di macchine. Questi casi d'uso includono:

- PC Linux fisici
- PC fisici in pool (ovvero assegnati in modo casuale, non dedicati)

> **Note:**
>
> Per i dettagli sulle versioni del sistema operativo supportate, vedere i requisiti di sistema per il VDA per il sistema operativo a sessione singola e Linux VDA.
>
> Per le distribuzioni locali, Accesso remoto PC è valido solo per le licenze Advanced o Premium di Citrix Virtual Apps and Desktops. Le sessioni consumano licenze allo stesso modo delle altre sessioni di Citrix Virtual Desktops. Per Citrix Cloud, Accesso remoto PC è valido per Citrix DaaS (in precedenza Citrix Virtual Apps and Desktops Service) e Workspace Premium Plus.

### Considerazioni

Anche se tutti i requisiti tecnici e le considerazioni che si applicano a Citrix Virtual Apps and Desktops in generale si applicano anche all'accesso remoto al PC, alcuni potrebbero essere più rilevanti o esclusivi per il caso di utilizzo fisico del PC.

> **Importante:**
>
> I sistemi fisici Windows 11 (e alcuni che eseguono Windows 10) includono funzionalità di sicurezza basate sulla virtualizzazione che fanno sì che il software VDA li rilevi erroneamente come macchine virtuali. Per mitigare questo problema, sono disponibili le seguenti opzioni:
>
> - Utilizzare l'opzione "/physicalmachine"insieme all'opzione "/remotepc"nell'ambito dell'installazione del VDA mediante la riga di comando
> - Se l'opzione sopra indicata non è stata utilizzata, dopo l'installazione del VDA aggiungere il seguente valore di registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>
> - Nome: ForceEnableRemotePC
> - Tipo: DWORD
> - Dati: 1

### Considerazioni sulla distribuzione

Durante la pianificazione della distribuzione di Accesso remoto PC, prendere alcune decisioni generali.

- È possibile aggiungere Accesso remoto PC a una distribuzione esistente di Citrix Virtual Apps and Desktops. Prima di scegliere questa opzione, considerare quanto segue:
  - I Delivery Controller o i Cloud Connector correnti sono adeguatamente dimensionati per supportare il carico aggiuntivo associato ai VDA di Accesso remoto PC?
  - I database del sito locali e i server di database sono adeguatamente dimensionati per supportare il carico aggiuntivo associato ai VDA di Accesso remoto PC?
  - I VDA esistenti e i nuovi VDA di Accesso remoto PC supereranno il numero massimo di VDA supportati per sito?
- È necessario distribuire il VDA sui PC dell'ufficio tramite un processo automatizzato. Di seguito sono riportate le opzioni disponibili:
  - Strumenti di distribuzione elettronica del software (ESD) come SCCM: installare i VDA utilizzando SCCM.
  - Script di distribuzione: installare i VDA utilizzando gli script.

- Vedere le Considerazioni sulla sicurezza di Remote PC Access (Accesso remoto PC).

> **Nota:**
>
> Quando si progetta l'accesso remoto al PC, è necessario considerare il numero di monitor fisici collegati alla GPU sul PC remoto e attualmente configurati/operativi. Anche se un monitor non viene utilizzato nella sessione Citrix, ma viene rilevato dalla GPU, la sua presenza viene conteggiata ai fini del limite massimo di monitor supportato dalla GPU.

### Considerazioni sul catalogo di macchine

Il tipo di catalogo di macchine richiesto dipende dal caso d'uso:

- Catalogo macchine Accesso remoto PC
  - PC dedicati Windows
  - PC multiutente dedicati Windows. Questo caso d'uso si applica ai PC fisici dell'ufficio a cui più utenti possono accedere da remoto in turni diversi.
  - PC Windows in pool. Questo caso d'uso si applica ai PC fisici a cui possono accedere più utenti casuali, come i laboratori informatici.
- Catalogo macchine con sistema operativo a sessione singola
  - Statico - PC Linux dedicati
  - Casuale - PC Linux in pool

Una volta identificato il tipo di catalogo di macchine, considerare quanto segue:

- Una macchina può essere assegnata a un solo catalogo di macchine alla volta.
- Per facilitare l'amministrazione delegata, è consigliabile creare cataloghi di macchine in base alla posizione geografica, al reparto o a qualsiasi altro raggruppamento che faciliti la delega dell'amministrazione di ciascun catalogo agli amministratori appropriati.
- Quando si scelgono le unità organizzative (OU) in cui risiedono gli account macchina, selezionare quelle di livello inferiore per una maggiore granularità. Se tale granularità non è richiesta, è possibile scegliere OU di livello superiore. Ad esempio, nel caso di banca/funzionari/cassieri, selezionare i **Tellers** (Cassieri) per una maggiore granularità. In caso contrario, è possibile selezionare **Officers** (Funzionari) o **Bank** (banca) in base a quanto è richiesto.
- Lo spostamento o l'eliminazione di unità organizzative dopo l'assegnazione a un catalogo di macchine Accesso remoto PC influisce sulle associazioni VDA e causa problemi per le assegnazioni future. Pertanto, assicurarsi di pianificare di conseguenza in modo che gli aggiornamenti delle assegnazioni alle unità organizzative dei cataloghi di macchine siano contabilizzati nel piano di modifica di Active Directory.

- Se non è facile scegliere unità organizzative per aggiungere macchine al catalogo macchine a causa della struttura delle unità organizzative, non è necessario selezionare alcuna unità organizzativa. È possibile utilizzare PowerShell per aggiungere macchine al catalogo in seguito. Le assegnazioni automatiche di utenti continuano a funzionare se l'assegnazione desktop è configurata correttamente nel gruppo di consegna. Uno script di esempio per aggiungere macchine al catalogo macchine insieme alle assegnazioni utente è disponibile in GitHub.
- La funzione Wake on LAN integrata è disponibile solo con il catalogo di macchine di tipo **Accesso remoto PC**.

### Considerazioni su Linux VDA

Queste considerazioni sono specifiche per Linux VDA:

- Usare Linux VDA su macchine fisiche solo in modalità non 3D. A causa delle limitazioni del driver NVIDIA, la schermata locale del PC non può essere oscurata e visualizza le attività della sessione quando è abilitata la modalità HDX 3D. Visualizzare questa schermata è un rischio per la sicurezza.
- Utilizzare cataloghi di macchine del tipo con sistema operativo a sessione singola per le macchine Linux fisiche.
- L'assegnazione automatica degli utenti non è disponibile per le macchine Linux.
- Se gli utenti sono già connessi al proprio PC localmente, i tentativi di avviare i PC da StoreFront non riescono.
- Le opzioni di risparmio energetico non sono disponibili per le macchine Linux.

### Requisiti tecnici e considerazioni

Questa sezione contiene i requisiti tecnici e le considerazioni per i PC fisici.

- I seguenti dispositivi non sono supportati:
  - Switch KVM o altri componenti che possono disconnettere una sessione.
  - PC ibridi, inclusi computer portatili e PC All-in-One e NVIDIA Optimus.
  - Macchine a doppio avvio.
- Collegare la tastiera e il mouse direttamente al PC. Il collegamento al monitor o ad altri componenti che possono essere spenti o scollegati può rendere queste periferiche non disponibili. Se è necessario collegare i dispositivi di input a componenti quali monitor, non spegnere tali componenti.
- I PC devono far parte di un dominio di Servizi di dominio Active Directory.

- Secure Boot è supportato solo su Windows 10 e Windows 11.
- Il PC deve disporre di una connessione di rete attiva. Una connessione cablata è preferibile per una maggiore affidabilità e larghezza di banda.
- Se si utilizza il Wi-Fi, effettuare le seguenti operazioni:

  1. Impostare l'alimentazione in modo che la scheda di rete wireless sia accesa.
  2. Configurare la scheda di rete wireless e il profilo di rete per consentire la connessione automatica alla rete wireless prima dell'accesso dell'utente. In caso contrario, il VDA non si registra finché l'utente non esegue l'accesso. Il PC non è disponibile per l'accesso remoto fino a quando un utente non ha effettuato l'accesso.
  3. Assicurarsi che i Delivery Controller o i connettori cloud possano essere raggiunti dalla rete Wi-Fi.

- È possibile utilizzare Accesso remoto PC sui computer portatili. Assicurarsi che il computer portatile sia collegato a una fonte di alimentazione anziché funzionare a batteria. Configurare le opzioni di alimentazione del laptop in modo che corrispondano alle opzioni di un PC desktop. Ad esempio:

  1. Disattivare la funzionalità di ibernazione.
  2. Disattivare la funzione di sospensione.
  3. Impostare l'azione di chiusura del coperchio su **Non intervenire**.
  4. Impostare l'azione di pressione del pulsante di accensione su **Arresta sistema**.
  5. Disabilitare le funzioni di risparmio energetico della scheda video e della scheda NIC.

- Accesso remoto PC è supportato sui dispositivi Surface Pro con Windows 10. Seguire le stesse linee guida per i computer portatili citati sopra.
- Se si utilizza una docking station, è possibile disancorare e reinserire i computer portatili. Quando si disancora il computer portatile, il VDA si registra nuovamente nei Delivery Controller o nei connettori cloud tramite Wi-Fi. Tuttavia, quando si reinserisce il computer portatile, il VDA non passa all'uso della connessione cablata a meno che non si disconnetta la scheda wireless. Alcuni dispositivi offrono una funzionalità integrata di disconnessione della scheda wireless dopo che è stata stabilita una connessione cablata. Gli altri dispositivi richiedono soluzioni personalizzate o utilità di terze parti per disconnettere la scheda wireless. Leggere le considerazioni sulle reti Wi-Fi menzionate in precedenza.

  Eseguire le seguenti operazioni per abilitare l'inserimento e il disancoraggio per i dispositivi di Accesso remoto PC:

  1. Nel menu **Start**, selezionare **Impostazioni > Sistema > Alimentazione e sospensione** e impostare **Sospensione** su **Mai**.
  2. In **Gestione periferiche > Schede di rete > Adattatore Ethernet** andare su **Risparmio energia** e deselezionare **Consenti al computer di spegnere il dispositivo per risparmi-**

**are energia**. Assicurarsi che l'opzione **Consenti al dispositivo di riattivare il computer** sia selezionata.

- Più utenti con accesso allo stesso PC dell'ufficio vedono la stessa icona in Citrix Workspace. Quando un utente accede a Citrix Workspace, tale risorsa appare come non disponibile se già in uso da parte di un altro utente.
- Installare l'app Citrix Workspace su ciascun dispositivo client (ad esempio, un PC di casa) che accede al PC dell'ufficio.

### Sequenza di configurazione

Questa sezione contiene una panoramica su come configurare Accesso remoto PC quando si utilizza il catalogo di macchine di **Accesso remoto PC**. Per informazioni su come creare altri tipi di cataloghi delle macchine, vedere Creare cataloghi delle macchine.

1. Solo sito locale: per utilizzare la funzionalità di riattivazione LAN integrata, configurare i prerequisiti descritti in Riattivazione LAN.
2. Se è stato creato un nuovo sito Citrix Virtual Apps and Desktops per l'accesso remoto PC:

   a) Selezionare il tipo di sito **Accesso remoto PC**.
   b) Nella pagina **Risparmio energia** scegliere di attivare o disattivare la gestione del risparmio energia per il catalogo di macchine Accesso remoto PC predefinito. È possibile modificare questa impostazione in un secondo momento modificando le proprietà del catalogo macchine. Per informazioni dettagliate sulla configurazione della riattivazione LAN, vedere Riattivazione LAN.
   c) Completare le informazioni nelle pagine **Users** e **Machine Accounts**.

   Completando questa procedura viene creato un catalogo macchine denominato **Remote PC Access Machines** e un gruppo di consegna denominato **Remote PC Access Desktops**.
3. Se si aggiungono elementi a un sito Citrix Virtual Apps and Desktops esistente:

   a) Creare un catalogo macchine di tipo **Accesso remoto PC** (pagina Operating System della procedura guidata). Per informazioni dettagliate su come creare un catalogo delle macchine, vedere Creare cataloghi delle macchine. Assicurarsi di assegnare l'unità organizzativa corretta in modo che i PC di destinazione siano resi disponibili per l'utilizzo con Accesso remoto PC.
   b) Creare un gruppo di consegna per fornire agli utenti l'accesso ai PC inclusi nel catalogo macchine. Per i dettagli su come creare un gruppo di consegna, vedere Creare gruppi di consegna. Assicurarsi di assegnare il gruppo di consegna a un gruppo di Active Directory che contenga gli utenti che richiedono l'accesso ai propri PC.

4. Distribuire il VDA nei PC dell'ufficio.

   - Si consiglia di utilizzare il programma di installazione VDA principale con sistema operativo a sessione singola (VDAWorkstationCoreSetup.exe).
   - È inoltre possibile utilizzare il programma di installazione VDA completo per sessione singola (VDAWorkstationSetup.exe) con l'opzione `/remotepc/physicalmachine`, che ottiene lo stesso risultato dell'utilizzo del programma di installazione VDA principale.

     > **Nota:**
     >
     > Per l'installazione RemotePC, utilizzare l'argomento `/physicalmachine` con `/remotepc` perché VDA si comporti come previsto in determinati scenari utente.

   - È possibile abilitare Assistenza remota di Windows per consentire ai team dell'help desk di fornire supporto remoto tramite Citrix Director. A tale scopo, utilizzare l'opzione `/enable_remote_assistance`. Per ulteriori informazioni, vedere Installare utilizzando la riga di comando.
   - Per poter visualizzare le informazioni sulla durata dell'accesso in Director, è necessario utilizzare il programma di installazione VDA completo per sessione singola e includere il componente **Citrix User Profile Management WMI Plugin**. Includere questo componente utilizzando l'opzione `/includeadditional`. Per ulteriori informazioni, vedere Installare utilizzando la riga di comando.
   - Per informazioni sulla distribuzione di VDA utilizzando SCCM, vedere Installare i VDA utilizzando SCCM.
   - Per informazioni sulla distribuzione di VDA tramite script di distribuzione, vedere Installare i VDA utilizzando gli script.

   Dopo aver completato i passaggi da 2 a 4, gli utenti vengono assegnati automaticamente ai propri computer quando effettuano l'accesso locale sui PC.

5. Chiedere agli utenti di scaricare e installare l'app Citrix Workspace su ciascun dispositivo client utilizzato per accedere al PC dell'ufficio in remoto. L'app Citrix Workspace è disponibile presso `https://www.citrix.com/downloads/` o negli store delle applicazioni per i dispositivi mobili supportati.

### Funzionalità gestite tramite il Registro di sistema

> **Attenzione:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi de-

> rivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

#### Disabilitare le assegnazioni automatiche di più utenti

In ogni Delivery Controller, aggiungere la seguente impostazione del Registro di sistema:

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- Nome: AllowMultipleRemotePCAssignments
- Tipo: DWORD
- Dati: 0

#### Modalità sospensione (versione minima 7.16)

Per consentire a un computer Accesso remoto PC di passare a uno stato di sospensione, aggiungere questa impostazione del Registro di sistema sul VDA e quindi riavviare il computer. Dopo il riavvio, vengono rispettate le impostazioni di risparmio energetico del sistema operativo. La macchina entra in modalità di sospensione dopo al termine del periodo di inattività preconfigurato. Dopo che si è svegliata, la macchina si registra nuovamente nel Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: DisableRemotePCSleepPreventer
- Tipo: DWORD
- Dati: 1

#### Gestione delle sessioni

Per impostazione predefinita, la sessione di un utente remoto viene disconnessa automaticamente quando un utente locale avvia una sessione su tale computer (premendo CTRL+ALT+CANC). Per evitare questa azione automatica, aggiungere la seguente voce del Registro di sistema nel PC dell'ufficio e quindi riavviare il computer.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: SasNotification
- Tipo: DWORD
- Dati: 1

Per impostazione predefinita, l'utente remoto ha la preferenza rispetto all'utente locale quando il messaggio di connessione non viene riconosciuto entro il periodo di timeout. Per configurare il comportamento, utilizzare questa impostazione:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaMode
- Tipo: DWORD
- Dati:
  - 1 - L'utente remoto ha sempre la preferenza se non risponde all'interfaccia utente di messaggistica nel periodo di timeout specificato. Questo comportamento è l'impostazione predefinita se questa impostazione non viene configurata.
  - 2 - L'utente locale ha la preferenza.

Il timeout per l'applicazione della modalità Accesso remoto PC è di 30 secondi per impostazione predefinita. È possibile configurare questo timeout, ma si consiglia di non impostarlo a meno di 30 secondi. Per configurare il timeout, utilizzare questa impostazione del Registro di sistema:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaTimeout
- Tipo: DWORD
- Dati: numero di secondi al timeout in valori decimali

Quando un utente desidera ottenere forzatamente l'accesso alla console: l'utente locale può premere Ctrl+Alt+Canc due volte in un intervallo di 10 secondi per ottenere il controllo locale su una sessione remota e forzare un evento di disconnessione.

Dopo la modifica del Registro di sistema e il riavvio del computer, se un utente locale preme Ctrl+Alt+Canc per accedere al PC mentre è utilizzato da un utente remoto, l'utente remoto riceve un messaggio di richiesta. Il messaggio di richiesta chiede se consentire o negare la connessione dell'utente locale. Consentendo la connessione, viene disconnessa la sessione dell'utente remoto.

### Registrazione della gestione delle sessioni

Remote PC Access ora dispone di funzionalità mediante le quali effettua una registrazione quando qualcuno tenta di accedere a un PC con una sessione ICA attiva. Ciò consente di monitorare l'ambiente alla ricerca di attività indesiderate o impreviste e di essere in grado di controllare tali eventi se è necessario indagare su eventuali incidenti.

Gli eventi vengono registrati utilizzando il Visualizzatore eventi di Windows e si trovano in **Applicazioni e servizi > Citrix > HostCore > ICA Service > Admin**.

Esistono tre eventi distinti che vengono registrati quando si utilizza Remote PC Access.

### Evento Ctrl+Alt+Canc

Questo evento appare quando l'utente locale preme Ctrl+Alt+Canc sulla tastiera della console quando è attiva una sessione remota.

### Dettagli evento

- Nome registro: Applicazione e servizi
- ID evento: 43, 44, 45
- Fonte: ICA Service

**ID evento 43** Questo ID evento viene visualizzato quando il valore del Registro di sistema SasNotification non esiste o quando il valore del Registro di sistema SasNotification è 0.

- Messaggio:

```
1           Ctrl+Alt+Del has been pressed on the endpoint.
2           The session management behavior is set to automatically
               disconnect the remote session.
```

**ID evento 44** Questo ID evento viene visualizzato quando il valore del Registro di sistema SasNotification è 1 e il valore del Registro di sistema RpcaMode è 1 o il valore del Registro di sistema RpcaMode non esiste.

- Messaggio:

```
1           Ctrl+Alt+Del has been pressed on the endpoint.
2           The session management behavior is set to notify the
               remote user. The user preference is set to remote user
               .
```

**ID evento 45** Questo ID evento viene visualizzato quando il valore del registro SasNotification è 1 e il valore del Registro di sistema RpcaMode è 2.

- Messaggio:

```
1           Ctrl+Alt+Del has been pressed on the endpoint.
2           The session management behavior is set to notify the
               remote user.
3           The user preference is set to local user.
```

### Evento disconnessione sessione remota

Questo evento viene visualizzato quando la sessione remota è stata disconnessa per vari motivi.

**Dettagli evento**

- Nome registro: Applicazione e servizi
- ID evento: 46, 47, 48
- Fonte: ICA Service

**ID evento 46** Questo ID evento viene visualizzato quando la sessione remota è stata disconnessa e quando il valore del Registro di sistema SasNotification non esiste o il valore del Registro di sistema SasNotification è 0.

- Messaggio:

```
1          The remote session for <remoteUserName> has been
              disconnected.
```

**ID evento 47** Questo ID evento viene visualizzato quando l'utente remoto accetta di disconnettere la sessione e quando il valore del Registro di sistema SasNotification è 1 e il valore del Registro di sistema RpcaMode è 1 o il valore del Registro di sistema RpcaMode è 2 o il valore del Registro di sistema RpcaMode non esiste.

- Messaggio:

```
1          The remote session for <remoteUserName> has been
              disconnected because the user accepted the request to
              disconnect the session.
```

**ID evento 48** Questo ID evento viene visualizzato quando l'utente remoto non rifiuta la richiesta di disconnessione entro il periodo di timeout specifico e quando il valore del Registro di sistema SasNotification è 1 e il valore del Registro di sistema RpcaMode è 2.

- Messaggio:

```
1          The remote session for <remoteUserName> has been
              disconnected because the user did not decline the
              disconnection request within the configured timeout
              period (<timeout period>).
```

**Evento di Ctrl+Alt+Canc premuto due volte** Questo evento appare quando Ctrl+Alt+Canc viene premuto due volte entro 10 secondi.

#### Dettagli evento

- Nome registro: Applicazione e servizi
- ID evento: 49
- Fonte: ICA Service

**ID evento 49** Questo ID evento appare quando Ctrl+Alt+Canc viene premuto due volte entro 10 secondi.

- Messaggio:

```
The remote session for <remoteUserName> has been forcibly
    disconnected.
```

### Riattivare su LAN

Accesso remoto PC supporta la funzione di riattivazione su LAN, che offre agli utenti la possibilità di accendere i PC fisici da remoto. Questa funzionalità consente agli utenti di mantenere spenti i PC dell'ufficio quando non sono in uso per risparmiare sui costi energetici. Consente inoltre l'accesso remoto quando una macchina è stata spenta inavvertitamente.

Con la funzione di riattivazione su LAN, i Magic Packet vengono inviati direttamente dal VDA in esecuzione sul PC alla sottorete in cui risiede il PC quando viene richiesto dal controller di consegna. Ciò consente alla funzione di agire senza dipendere da componenti aggiuntivi dell'infrastruttura o da soluzioni di terze parti per la distribuzione di Magic Packet.

La funzione di riattivazione su LAN è diversa dalla funzione di riattivazione su LAN basata su SCCM precedente. Per informazioni sulla riattivazione LAN basata su SCCM, vedere Riattivazione LAN - integrata con SCCM.

#### Requisiti di sistema

Di seguito sono riportati i requisiti di sistema per l'utilizzo della funzione di riattivazione su LAN:

- Piano di controllo:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 o versioni successive
- PC fisici:
  - VDA versione 2009 o successiva
  - Windows 10 o Windows 11. Per i dettagli relativi al supporto, vedere i requisiti di sistema del VDA.

- Riattivazione su LAN abilitata in BIOS/UEFI
- Riattivazione su LAN abilitata nelle proprietà della scheda di rete all'interno della configurazione di Windows

### Configurare la riattivazione su LAN

Se si utilizza Citrix Virtual Apps and Desktops in locale, la configurazione della riattivazione su LAN integrata è supportata solo utilizzando PowerShell.

Per configurare la riattivazione su LAN:

1. Creare il catalogo di macchine Accesso remoto PC se non è già disponibile.
2. Creare la connessione host di riattivazione LAN se è già disponibile.

   > **Nota:**
   >
   > Per utilizzare la funzionalità di riattivazione su LAN, se si dispone di una connessione host del tipo "Microsoft Configuration Manager Wake on LAN", creare una nuova connessione host.

3. Recuperare l'identificatore univoco della connessione host di Riattivazione LAN.
4. Associare la connessione host di riattivazione su LAN a un catalogo di macchine.

Per creare la connessione host di riattivazione su LAN:

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "\*citrix\*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                -Name $connectionName `
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties
                    >" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
    $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
```

```
22 {
23
24     Start-Sleep -s 5
25     $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
           $hypHc.HypervisorConnectionUid
26  }
27
28 <!--NeedCopy-->
```

Quando la connessione host è pronta, eseguire i seguenti comandi per recuperare l'identificatore univoco della connessione host:

```
1 $bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
2 $hypUid = $bhc.Uid
3 <!--NeedCopy-->
```

Dopo aver recuperato l'identificatore univoco della connessione, eseguire i comandi seguenti per associare la connessione al catalogo del computer Accesso remoto PC:

```
1 Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
      RemotePCHypervisorConnectionUid $hypUid
2 <!--NeedCopy-->
```

#### Considerazioni di progettazione

Quando si prevede di utilizzare la riattivazione su LAN con Accesso remoto PC, considerare quanto segue:

- Più cataloghi di macchine possono utilizzare la stessa connessione host di riattivazione su LAN.
- Perché un PC possa riattivare un altro PC, entrambi i PC devono trovarsi nella stessa sottorete e utilizzare la stessa connessione host di riattivazione su LAN. Non importa se i PC si trovano nello stesso catalogo di macchine o cataloghi diversi.
- Le connessioni host vengono assegnate a zone specifiche. Se la distribuzione contiene più di una zona, è necessaria una connessione host di riattivazione su LAN in ciascuna zona. Lo stesso vale per i cataloghi di macchine.
- I Magic Packet vengono trasmessi utilizzando l'indirizzo di trasmissione globale 255.255.255.255. Assicurarsi che l'indirizzo non sia bloccato.
- Deve essere presente almeno un PC acceso nella sottorete, per ciascuna connessione di riattivazione su LAN, per poter riattivare le macchine in quella sottorete.

#### Considerazioni operative

Di seguito sono riportate considerazioni sull'impiego della funzione di riattivazione su LAN:

- Il VDA deve registrarsi almeno una volta prima che il PC possa essere riattivato utilizzando la funzione di riattivazione su LAN integrata.
- La funzione di riattivazione su LAN può essere utilizzata solo per riattivare i PC. Non supporta altre azioni di alimentazione, ad esempio il riavvio o l'arresto.
- Dopo essere stata creata, la connessione di riattivazione su LAN è visibile in Web Studio. Tuttavia, la modifica delle sue proprietà all'interno di Web Studio non è supportata se si utilizza Citrix Virtual Apps and Desktops in locale.
- I Magic Packet vengono inviati in uno di due modi:

  1. Quando un utente tenta di avviare una sessione sul proprio PC e il VDA non è registrato
  2. Quando un amministratore invia manualmente un comando di accensione da Web Studio o PowerShell

- Poiché il controller di distribuzione non è a conoscenza dello stato di alimentazione di un PC, Web Studio visualizza **Not Supported** nello stato di alimentazione. Il controller di consegna utilizza lo stato di registrazione del VDA per determinare se un PC è acceso o spento.

## Riattivazione su LAN integrata con SCCM

La funzione di riattivazione su LAN integrata con SCCM è un'opzione alternativa di riattivazione su LAN per l'accesso remoto PC disponibile solo con Citrix Virtual Apps and Desktops locali.

### Requisiti di sistema

Di seguito sono riportati i requisiti di sistema per l'utilizzo della funzione di riattivazione su LAN integrata con SCCM:

- Citrix Virtual Apps and Desktops 1912 o versioni successive
- PC fisici:
  - VDA versione 1912 o successiva
  - Windows 10. Per i dettagli relativi al supporto, vedere i requisiti di sistema del VDA.
  - Riattivazione su LAN abilitata in BIOS/UEFI
  - Riattivazione su LAN abilitata nelle proprietà della scheda di rete all'interno della configurazione di Windows
- System Center Configuration Manager (SCCM) 2012 R2 o versione successiva

### Configurare la funzione di riattivazione su LAN integrata con SCCM

Completare i seguenti prerequisiti:

1. Configurare SCCM 2012 R2, 2016 o 2019 all'interno dell'organizzazione. Quindi distribuire il client SCCM su tutti i computer Accesso remoto PC, lasciando trascorrere il tempo necessario per l'esecuzione del ciclo di inventario SCCM pianificato o forzarne uno manualmente, se necessario.
2. Per il supporto del proxy di riattivazione, attivare l'opzione in SCCM. Per ogni sottorete dell'organizzazione che contiene PC che utilizzano la funzione Accesso remoto PC su LAN, assicurarsi che tre o più computer possano fungere da macchine sentinella.
3. Per il supporto dei Magic Packet, configurare i router e i firewall della rete perché consentano l'invio di Magic Packet, utilizzando una trasmissione diretta in sottorete o unicast.
4. Configurare la riattivazione su LAN nelle impostazioni BIOS/UEFI di ciascun PC.
5. Distribuire il VDA sui PC fisici se non lo si è già fatto.

Dopo aver soddisfatto i prerequisiti, completare la procedura seguente per consentire al Delivery Controller di comunicare con SCCM:

1. Creare una connessione host per SCCM. Per ulteriori informazioni, vedere Connessioni e risorse.
    - Selezionare **Microsoft Configuration Manager Wake on LAN** come tipo di connessione.
    - Le credenziali immesse devono includere l'accesso alle raccolte nell'ambito e devono avere il ruolo **Remote Tools Operator**.
2. Selezionare la connessione in Web Studio, quindi selezionare **Edit Connection** (Modifica connessione) e fare clic su **Advanced**.
3. Selezionare l'opzione appropriata per la gestione della riattivazione su LAN:
    - Se si utilizza il proxy di riattivazione, selezionare la prima opzione: **Microsoft System Center Configuration Manager Wake-up proxy** (Proxy di riattivazione di Microsoft System Center Configuration Manager).
    - Se si utilizzano Magic Packet, selezionare la seconda opzione: **Wake on LAN packets transmitted by the Delivery Controller** (Pacchetti di riattivazione su LAN trasmessi dal Delivery Controller).
        - Selezionare il metodo di trasmissione appropriato: **subnet-directed broadcasts** (trasmissioni dirette dalla sottorete) o **unicast**.

Dopo aver creato la connessione host, associare la connessione a un catalogo di Accesso remoto PC:

- Se si sta creando un nuovo catalogo di Accesso remoto PC, nella pagina **Operating System** della creazione guidata catalogo selezionare **Remote PC Access** come tipo di catalogo e scegliere la connessione appropriata dall'elenco a discesa.
- Per aggiungere la riattivazione da LAN a un catalogo di Accesso remoto PC esistente:
    1. Andare al nodo **Machine Catalogs** (Cataloghi macchine) in Web Studio, selezionare il catalogo macchine e quindi selezionare **Edit Machine Catalog** (Modifica catalogo macchine).

2. Selezionare la scheda **Modifica catalogo macchine** (Risparmio energia) e scegliere **Yes** per abilitare la gestione del risparmio energia per il catalogo macchine.
3. Selezionare la connessione appropriata dall'elenco a discesa e fare clic su **OK**.

## Risoluzione dei problemi

### Lo schermo nero del monitor non funziona

Se il monitor locale del PC Windows non ha lo schermo nero mentre è attiva una sessione HDX (il monitor locale mostra ciò che sta accadendo nella sessione), ciò è probabilmente dovuto a problemi del driver del fornitore della GPU. Per risolvere il problema, assegnare al driver di visualizzazione indiretta Citrix (IDD) una priorità maggiore rispetto al driver del fornitore della scheda grafica impostando il seguente valore del Registro di sistema:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Nome: CitrixIDD
- Tipo: DWORD
- Dati: 3

Per ulteriori informazioni sulle priorità della scheda video e sulla creazione del monitor, vedere l'articolo del Knowledge Center CTX237608.

### La sessione si disconnette quando si seleziona Ctrl+Alt+Canc nel computer in cui è attivata la notifica di gestione della sessione

La notifica di gestione della sessione controllata dal valore del Registro di sistema **SasNotification** funziona solo quando la modalità Accesso remoto PC è attivata sul VDA. Se il PC fisico ha il ruolo di Hyper-V o qualsiasi funzionalità di sicurezza basata sulla virtualizzazione abilitata, il PC si segnala come macchina virtuale. Se il VDA rileva che è in esecuzione su una macchina virtuale, disattiva automaticamente la modalità Accesso remoto PC. Per attivare la modalità Accesso remoto PC, aggiungere il seguente valore del Registro di sistema:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dati: 1

Riavviare il PC affinché l'impostazione abbia effetto.

#### Informazioni diagnostiche

Le informazioni diagnostiche su Accesso remoto PC vengono scritte nel registro eventi applicazioni di Windows. I messaggi informativi non vengono limitati. I messaggi di errore vengono limitati eliminando i messaggi duplicati.

- 3300 (informativo): Macchina aggiunta al catalogo
- 3301 (informativo): Macchina aggiunta al gruppo di consegna
- 3302 (informativo): Macchina assegnata all'utente
- 3303 (errore): Eccezione

#### Gestione dell'alimentazione

Se è attivata la gestione dell'alimentazione per Accesso remoto PC, le trasmissioni dirette dalla sottorete potrebbero non riuscire ad avviare i computer che si trovano in una sottorete diversa dal controller. Se è necessaria la gestione dell'alimentazione tra sottoreti che utilizzano trasmissioni dirette da sottoreti e il supporto AMT non è disponibile, provare il proxy di riattivazione o il metodo Unicast. Verificare che tali impostazioni siano abilitate nelle proprietà avanzate per la connessione di gestione dell'alimentazione.

#### La sessione remota attiva registra gli input del touchscreen locale

Quando il VDA abilita la modalità Accesso remoto PC, il computer ignora l'input del touchscreen locale durante una sessione attiva. Se il PC fisico ha il ruolo di Hyper-V o qualsiasi funzionalità di sicurezza basata sulla virtualizzazione abilitata, il PC si segnala come macchina virtuale. Se il VDA rileva che è in esecuzione su una macchina virtuale, disattiva automaticamente la modalità Accesso remoto PC. Per attivare la modalità Accesso remoto PC, aggiungere la seguente impostazione del Registro di sistema:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dati: 1

Riavviare il PC affinché l'impostazione abbia effetto.

### Altre risorse

Di seguito sono elencate altre risorse per Accesso remoto PC:

- Guida alla progettazione della soluzione: decisioni sulla progettazione di Remote PC Access (Accesso remoto PC).
- Esempi di architetture di Remote PC Access (Accesso remoto PC): architettura di riferimento per la soluzione Citrix Remote PC Access (Accesso remoto PC).

## Pubblicare contenuti

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

È possibile pubblicare un'applicazione che è semplicemente un percorso URL o UNC verso una risorsa, ad esempio un documento di Microsoft Word o un collegamento Web. Questa funzionalità è nota come contenuto pubblicato. La possibilità di pubblicare contenuti aggiunge flessibilità alla modalità di distribuzione dei contenuti agli utenti. Si traggono vantaggi dal controllo degli accessi e dalla gestione delle applicazioni esistenti. È inoltre possibile specificare se utilizzare applicazioni locali o pubblicate per aprire il contenuto.

Il contenuto pubblicato appare come le altre applicazioni in StoreFront e nell'app Citrix Workspace. Gli utenti accedono allo stesso modo in cui accedono alle applicazioni. Sul client, la risorsa si apre come al solito.

- Se un'applicazione installata localmente è appropriata, viene avviata per aprire la risorsa.
- Se è stata definita un'associazione di tipi di file, viene avviata un'applicazione pubblicata per aprire la risorsa.

È possibile pubblicare contenuti utilizzando PowerShell SDK. Non è possibile utilizzare Web Studio per pubblicare contenuti. Tuttavia, è possibile utilizzare Web Studio per modificare le proprietà dell'applicazione in un secondo momento, dopo la pubblicazione.

### Panoramica e preparazione della configurazione

Per la pubblicazione del contenuto viene utilizzato il cmdlet `New-BrokerApplication` con le seguenti proprietà chiave. Per le descrizioni di tutte le proprietà del cmdlet, vedere la Guida del cmdlet.

```
New-BrokerApplication –ApplicationType PublishedContent -
    CommandLineExecutable location -Name app-name -DesktopGroup delivery
    -group-name
<!--NeedCopy-->
```

La proprietà `ApplicationType` deve essere `PublishedContent`.

La proprietà `CommandLineExecutable` specifica la posizione del contenuto pubblicato. Sono supportati i seguenti formati, con un limite di 255 caratteri.

- Indirizzo di sito Web HTML (ad esempio http://www.citrix.com)
- File di documento su un server Web (ad esempio `https://www.citrix.com/press/pressrelease.doc`)
- Directory su un server FTP (ad esempio `ftp://ftp.citrix.com/code`)
- File di documento su un server FTP (ad esempio `ftp://ftp.citrix.com/code/Readme.txt`>)
- Percorso directory UNC (ad esempio `file://myServer/myShare or \\\\\myServer\\myShare`)
- Percorso file UNC (ad esempio `file://myServer/myShare/myFile.asf` o `\\myServer\myShare\myFile.asf`)

Assicurarsi di avere l'SDK corretto.

- Per le distribuzioni di Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops) scaricare e installare l'SDK PowerShell remoto di Citrix Virtual Apps and Desktops.
- Per le distribuzioni locali di Citrix Virtual Apps and Desktops, utilizzare PowerShell SDK installato con il Delivery Controller. L'aggiunta di un'applicazione di contenuto pubblicato richiede una versione minima 7.11 di Delivery Controller.

Nelle procedure riportate di seguito vengono utilizzati esempi. Negli esempi:

- È stato creato un catalogo di macchine.
- È stato creato un gruppo di consegna denominato `PublishedContentApps`. Il gruppo utilizza una macchina con sistema operativo multisessione inclusa nel catalogo. L'applicazione WordPad è stata aggiunta al gruppo.
- Le assegnazioni vengono eseguite per il nome del gruppo di consegna, la posizione di `CommandLineExecutable` e il nome dell'applicazione.

### Per iniziare

Nel computer contenente PowerShell SDK, aprire PowerShell.

Il cmdlet seguente aggiunge lo snap-in PowerShell SDK appropriato e assegna il record del gruppo di consegna restituito.

```
Add-PsSnapin Citrix\* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

Se si utilizza Citrix DaaS, effettuare l'autenticazione immettendo le proprie credenziali Citrix Cloud. Se ci sono più clienti, sceglierne uno.

#### Pubblicare un URL

Dopo aver assegnato il percorso e il nome dell'applicazione, il cmdlet seguente pubblica la home page di Citrix come applicazione.

```
$citrixUrl = "https://www.citrix.com/"
$appName = "Citrix Home Page"

New-BrokerApplication –ApplicationType PublishedContent –
    CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.
    Uid
<!--NeedCopy-->
```

Verificare la riuscita:

- Aprire StoreFront ed effettuare l'accesso come utente che può accedere alle applicazioni nel gruppo di consegna PublishedContentApps. Il display include l'applicazione appena creata con l'icona predefinita. Per informazioni sulla personalizzazione dell'icona, vedere https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/.
- Fare clic sull'applicazione **Citrix Home Page**. L'URL viene avviato in una nuova scheda in un'istanza in esecuzione locale del browser predefinito.

### Pubblicare risorse situate nei percorsi UNC

In questo esempio, l'amministratore ha già creato una condivisione denominata `PublishedResources`. Dopo aver assegnato i percorsi e i nomi delle applicazioni, i cmdlet seguenti pubblicano un file RTF e un file DOCX in tale condivisione come risorsa.

```
$rtfUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
$rtfAppName = "PublishedRTF"

New-BrokerApplication –ApplicationType PublishedContent
 –CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx
    "
$docxAppName = "PublishedDOCX"

New-BrokerApplication –ApplicationType PublishedContent
```

```
 – CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
<!--NeedCopy-->
```

Verificare la riuscita:

- Aggiornare la finestra StoreFront per visualizzare i documenti appena pubblicati.
- Fare clic sulle applicazioni **PublishedRTF** e **PublishedDOCX**. Ogni documento si apre in un WordPad in esecuzione locale.

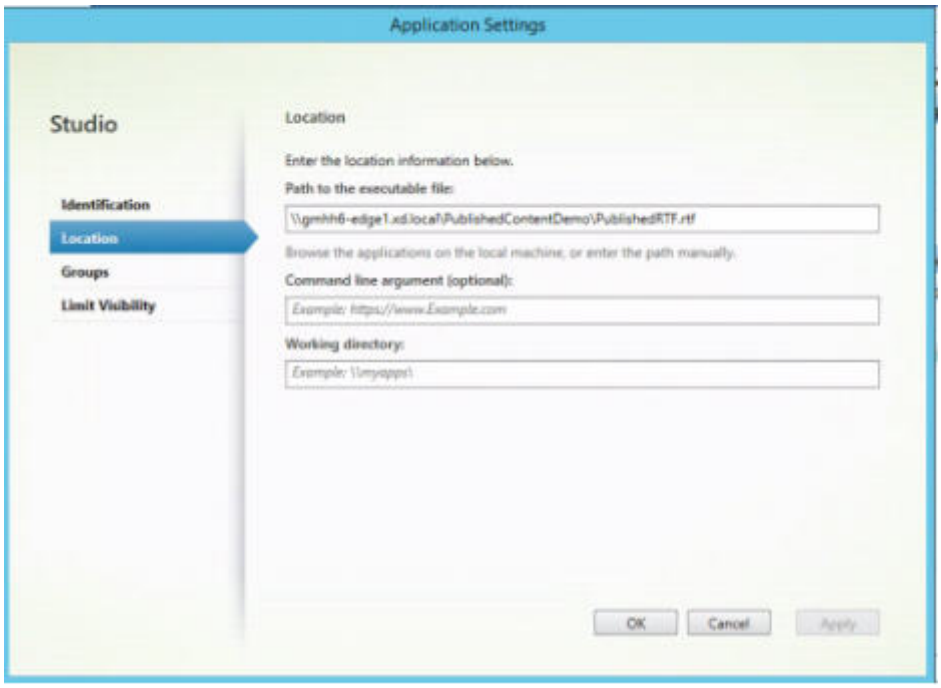
### Visualizzare e modificare le applicazioni PublishedContent

È possibile gestire il contenuto pubblicato utilizzando gli stessi metodi adottati per altri tipi di applicazione.

Per visualizzare e modificare le applicazioni `PublishedContent`, seguire questi passaggi:

1. Accedere a Web Studio e selezionare **Applications** nel riquadro a sinistra.
2. Nella scheda **Applications** (Applicazioni), selezionare un'applicazione PublishedContent e quindi scegliere **Properties** (Proprietà).

   Le proprietà dell'applicazione (ad esempio visibilità utente, associazione di gruppi e collegamento) si applicano al contenuto pubblicato. Tuttavia, non è possibile modificare l'argomento della riga di comando o le proprietà della directory di lavoro nella pagina **Location**.
3. Per modificare la risorsa, modificare il campo **Path to the executable file** (percorso al file eseguibile) in tale pagina.

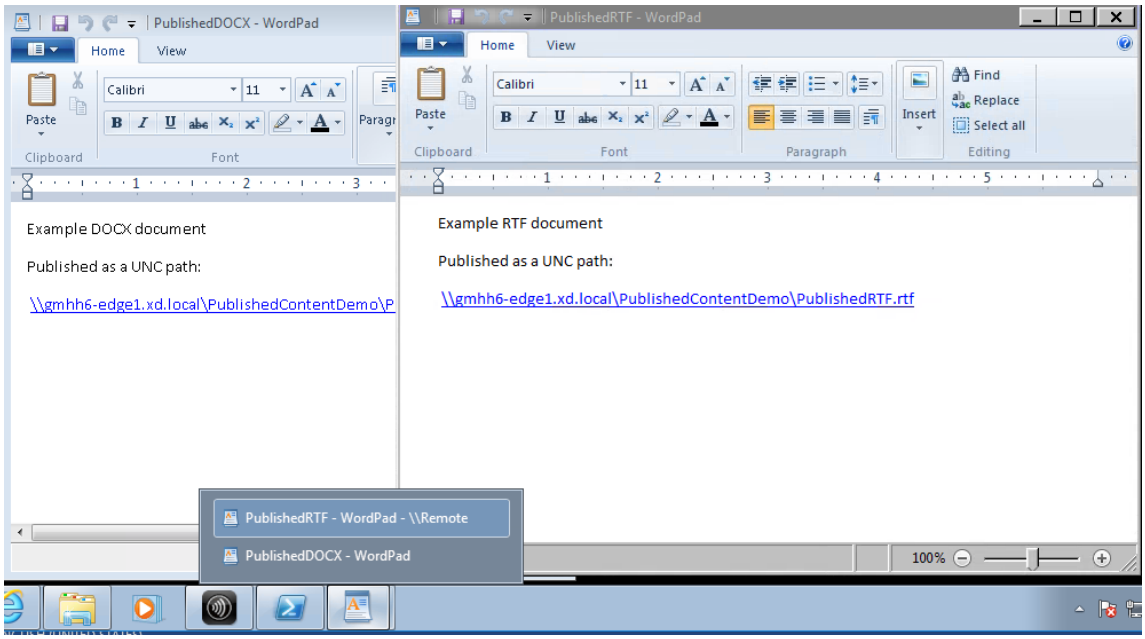


4. Per utilizzare un'applicazione pubblicata per aprire un'applicazione `PublishedContent` (anziché un'applicazione locale), seguire questi passaggi:

   In questo esempio, l'applicazione WordPad pubblicata viene modificata per creare un'associazione di tipi di file per i file RTF.

   a) Attivare la modalità di manutenzione per il gruppo di consegna.
   b) Modificare la proprietà **File Type Association** (Associazione dei tipi di file).
   c) Al termine, disattivare la modalità di manutenzione.
   d) Aggiornare StoreFront per caricare le modifiche relative all'associazione dei tipi di file e quindi fare clic sulle applicazioni **PublishedRTF** e **PublishedDocx**. Notate la differenza. **PublishedDocx** si apre ancora nel WordPad locale. Tuttavia, **PublishedRTF** ora si apre nel WordPad pubblicato a causa dell'associazione del tipo di file.




### For more information

- Creare cataloghi di macchine
- Creare gruppi di consegna
- Modificare le proprietà dell'applicazione

## VDI del server

January 7, 2024

Utilizzare la funzionalità Server VDI (Virtual Desktop Infrastructure) per distribuire un desktop da un sistema operativo server per un singolo utente.

- Gli amministratori aziendali possono fornire sistemi operativi server come desktop VDI, soluzione che può essere utile per utenti come ingegneri e progettisti.
- I Service Provider possono offrire desktop dal cloud. Tali desktop sono conformi al Microsoft Services Provider License Agreement (SPLA).

Supporto:

- Nelle distribuzioni dei servizi di Citrix DaaS (in precedenza Citrix Virtual Apps and Desktops e Citrix Virtual Apps and Desktops), Server VDI è supportato su Windows Server 2022, Windows Server 2019 e Windows Server 2016.
- Tutte le distribuzioni VDI Server supportano la tecnologia a livello di personalizzazione utente.
- Affinché VDI Server funzioni con dispositivi TWAIN quali scanner, è necessario installare la funzionalità Windows Server Desktop Experience.
- Le seguenti funzionalità non possono essere utilizzate con Server VDI:
  - Applicazioni ospitate
  - Accesso alle app locali
  - Connessioni desktop dirette (non mediate)
  - Accesso remoto al PC

### Installare e configurare Server VDI

1. Preparare il server Windows per l'installazione.
   - Utilizzare Windows Server Manager per assicurarsi che i servizi ruolo Servizi Desktop remoto non siano installati. Se sono stati installati in precedenza, rimuoverli. L'installazione dei VDA non riesce se questi servizi ruolo sono installati.
   - Assicurarsi che la proprietà **Restrict each user to a single session** (Limita ogni utente a una singola sessione) sia abilitata. Nel server Windows, modificare il Registro di sistema per l'impostazione di Terminal Server:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
     ```

     ```
     DWORD fSingleSessionPerUser = 1
     ```
2. Utilizzare l'interfaccia della riga di comando del programma di installazione di Citrix Virtual Apps and Desktops per installare un VDA su un'immagine master server o su un server supportato, specificando le opzioni `/quiet` e `/servervdi`. Per impostazione predefinita, l'interfaccia grafica del programma di installazione blocca il VDA del sistema operativo Windows a

sessione singola su un sistema operativo server. L'utilizzo della riga di comando evita questo comportamento. Utilizzare uno dei seguenti comandi:

- Distribuzioni di Citrix Virtual Apps and Desktops:
  - `XenDesktopVdaSetup.exe /quiet /servervdi`
  - `VDAWorkstationSetup.exe /quiet /servervdi`
- Distribuzioni di Citrix DaaS:
  - `VDAWorkstationSetup.exe /quiet /servervdi`

Altre opzioni:

- Utilizzare `/controllers` per specificare i Delivery Controller o i connettori cloud.
- Utilizzare `/enable_hdx_ports` per aprire le porte nel firewall, a meno che il firewall non debba essere configurato manualmente.
- Utilizzare `/mastermcsimage` (o `/masterimage`) se si sta installando il VDA su un'immagine e si utilizzerà MCS per creare macchine virtuali server da tale immagine.
- Per tutti i dettagli sulle opzioni, vedere Installare utilizzando la riga di comando.

3. Creare un catalogo di macchine per Server VDI. Nella procedura guidata per la creazione del catalogo:

   - Nella pagina **Operating System** selezionare **Single-session OS** (Sistema operativo a sessione singola).
   - Nella pagina **Summary** specificare un nome e una descrizione del catalogo di computer per gli amministratori che lo identifichino chiaramente come VDI del server. In Studio questo è l'unico elemento indicatore che il catalogo supporta Server VDI.

   Quando si utilizza la ricerca in Studio, il catalogo VDI Server viene visualizzato nella scheda **Single-session OS Machines** (Macchine con sistema operativo a sessione singola), anche se il VDA è installato su un computer multisessione.

4. Creare un gruppo di consegna e selezionare il catalogo Server VDI creato.

Se durante l'installazione dei VDA non sono stati specificati i Delivery Controller o i connettori cloud, ricordarsi di specificarli in seguito. Per i dettagli, vedere Registrazione VDA.

## Livello di personalizzazione utente

January 10, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

La funzionalità del livello di personalizzazione utente di Citrix Virtual Apps and Desktops estende le funzionalità dei cataloghi di macchine non persistenti per preservare i dati degli utenti e le applicazioni installate localmente in tutte le sessioni. Basata sulla tecnologia sottostante Citrix App Layering, la funzionalità di livello di personalizzazione utente supporta Citrix Provisioning and Machine Creation Services (MCS) in un catalogo di macchine non persistenti.

Installare i componenti del livello di personalizzazione utente insieme al Virtual Delivery Agent all'interno dell'immagine master. Un file VHD memorizza localmente le applicazioni installate dall'utente. Il disco rigido virtuale montato sull'immagine funge da disco rigido virtuale dell'utente.

> **Importante:**
>
> È possibile distribuire livelli di personalizzazione utente in App Citrix Virtual Apps and Desktops o livelli utente App Layering abilitati in un modello di immagine, non in entrambi. Non installare la funzionalità del livello di personalizzazione utente in un livello all'interno di App Layering.

Questa funzionalità sostituisce Personal vDisk (PvD), fornendo allo stesso tempo un'esperienza di lavoro persistente per gli utenti in un ambiente desktop non persistente (in pool).

Per distribuire la funzionalità del livello di personalizzazione utente, installarla e configurarla seguendo i passaggi descritti nell'articolo.

## Supporto delle applicazioni

A parte le seguenti eccezioni, tutte le applicazioni installate da un utente localmente sul desktop sono supportate nel livello di personalizzazione utente.

### Eccezioni

Le seguenti applicazioni fanno eccezione e non sono supportate nel livello di personalizzazione utente:

- Applicazioni aziendali, ad esempio MS Office e Visual Studio.
- Applicazioni che modificano lo stack di rete o l'hardware. Esempio: un client VPN.
- Applicazioni che dispongono di driver a livello di avvio. Esempio: un programma antivirus.

- Applicazioni con driver che utilizzano l'archivio driver. Esempio: un driver di stampante.

  > **Nota:**
  >
  > È possibile rendere disponibili le stampanti utilizzando Oggetti Criteri di gruppo di Windows.

*Non* consentire agli utenti di installare applicazioni non supportate localmente. Piuttosto, installare queste applicazioni direttamente sull'immagine master.

#### Applicazioni che richiedono un account utente locale o amministratore

Quando un utente installa un'applicazione localmente, l'app entra nel livello utente. Se l'utente aggiunge o modifica un utente o un gruppo locale, le modifiche non persistono oltre la sessione.

> **Importante:**
>
> Aggiungere qualsiasi utente o gruppo locale richiesto nell'immagine master.

### Requisiti

La funzionalità del livello di personalizzazione utente richiede i seguenti componenti:

- Citrix Virtual Apps and Desktops 7 1909 o versioni successive
- Virtual Delivery Agent (VDA), versione 1912 o successiva
- Citrix Provisioning, versione 1909 o successiva
- Condivisione file di Windows (SMB) o File di Azure con autenticazione AD locale abilitata

È possibile distribuire la funzionalità di livello di personalizzazione utente nelle seguenti versioni di Windows quando il sistema operativo viene distribuito come singola sessione. Il supporto è limitato a un singolo utente in una singola sessione.

- Windows 11 Enterprise x64
- Windows 10 Enterprise x64, versione 1607 o successiva
- Windows 10 multisessione (File di Azure supportato)
- Windows Server 2016 (File di Azure supportato)
- Windows Server 2019 (File di Azure supportato)

Per Citrix Virtual Apps and Desktops 7, l'uso di File di Azure con livelli di personalizzazione utente è supportato nei client Windows Server 2019, Windows Server 2016v e Windows 10.

> **Nota:**
>
> se si utilizza un sistema operativo server, è supportato solo Server VDI. Per i dettagli sulla distribuzione, vedere l'articolo VDI del server.

> Il livello di personalizzazione utente supporta un solo utente alla volta per macchina e quindi il computer si deve riavviare per reimpostare i dischi. Non è possibile utilizzare il livello di personalizzazione utente con sistemi operativi server multisessione, ma solo con sistemi server a sessione singola. Il livello di personalizzazione utente funziona solo con desktop non persistenti.

Disinstallare la funzionalità del livello di personalizzazione utente, se installata. Riavviare l'immagine master prima di installare l'ultima versione.

## Configurare la condivisione di file

La funzionalità del livello di personalizzazione utente richiede l'archiviazione SMB (Server Message Block) di Windows. Per creare una condivisione file Windows, attenersi alla procedura usuale per il sistema operativo Windows in uso.

Per informazioni dettagliate sull'utilizzo dei File di Azure con cataloghi basati su Azure, consultare Configurare l'archiviazione di File di Azure per i livelli di personalizzazione utente.

## Consigli

Seguire i suggerimenti riportati in questa sezione per una distribuzione corretta del livello di personalizzazione utente.

### Microsoft System Center Configuration Manager (SCCM)

Se si utilizza SCCM con la funzionalità del livello di personalizzazione utente, seguire le linee guida Microsoft per la preparazione dell'immagine in un ambiente VDI. Per ulteriori informazioni, fare riferimento a questo articolo di Microsoft TechNet.

### Dimensione del livello utente

Un livello utente è un disco con thin-provisioning che si espande man mano che viene utilizzato lo spazio sul disco. La dimensione predefinita consentita per un livello utente è 10 GB, il minimo consigliato.

> **Nota:**
>
> Durante l'installazione, se il valore è impostato su zero (0), la dimensione del livello utente predefinita è impostata su 10 GB.

Se si desidera modificare la dimensione del livello utente, è possibile immettere un valore diverso per il criterio **User Layer Size**. Vedere **Passaggio 5: Creare criteri personalizzati per i gruppi di consegna**, in **Facoltativo: fare clic su Seleziona accanto a Dimensione livello utente in GB.**

#### Strumenti per sovrascrivere la dimensione del livello utente (facoltativo)

È possibile ignorare la dimensione del livello utente utilizzando uno strumento di Windows per definire una quota sulla condivisione file a livello utente.

Utilizzare uno dei seguenti strumenti di quota Microsoft per impostare una quota rigida nella directory del livello utente denominata **Users** (Utenti):

- Gestione risorse file server (FSRM)
- Gestione quote

> **Nota:**
>
> L'aumento della quota influisce sui nuovi livelli utente ed espande quelli esistenti. La diminuzione della quota influisce solo sui nuovi livelli utente. I livelli utente esistenti non diminuiscono mai di dimensioni.

### Distribuire un livello di personalizzazione utente

Quando si distribuisce la funzionalità di personalizzazione utente, è possibile definirne i criteri in Web Studio. Assegnare quindi i criteri al gruppo di consegna associato al catalogo macchine in cui viene distribuita la funzionalità.

Se si lascia l'immagine master senza configurazione del livello di personalizzazione utente, i servizi rimangono inattivi e non interferiscono con le attività di creazione.

Se si impostano i criteri nell'immagine master, i servizi tentano di eseguire e montare un livello utente all'interno dell'immagine master. L'immagine master mostrerebbe comportamenti inaspettati e instabilità.

Per distribuire la funzionalità del livello di personalizzazione utente, completare i passaggi seguenti nell'ordine seguente:

- Passaggio 1: verificare la disponibilità di un ambiente Citrix Virtual Apps and Desktops.
- Passaggio 2: Preparare l'immagine master.
- Passaggio 3: Creare un catalogo macchine.
- Passaggio 4: Creare un gruppo di consegna.
- Passaggio 5: Creare criteri personalizzati per il gruppo di consegna.

> **Nota:**
>
> l'accesso per la prima volta dopo l'aggiornamento di Windows 10 sull'immagine richiede più tempo del solito. Il livello dell'utente deve essere aggiornato per la nuova versione di Windows 10, il che aumenta il tempo di accesso.

**Passaggio 1: Verificare che sia disponibile un ambiente Citrix Virtual Apps and Desktops**

Assicurarsi che il proprio ambiente Citrix Virtual Apps and Desktops sia disponibile per l'utilizzo con questa nuova funzionalità. Per informazioni dettagliate sull'installazione, vedere Installare e configurare Citrix Virtual Apps and Desktops.

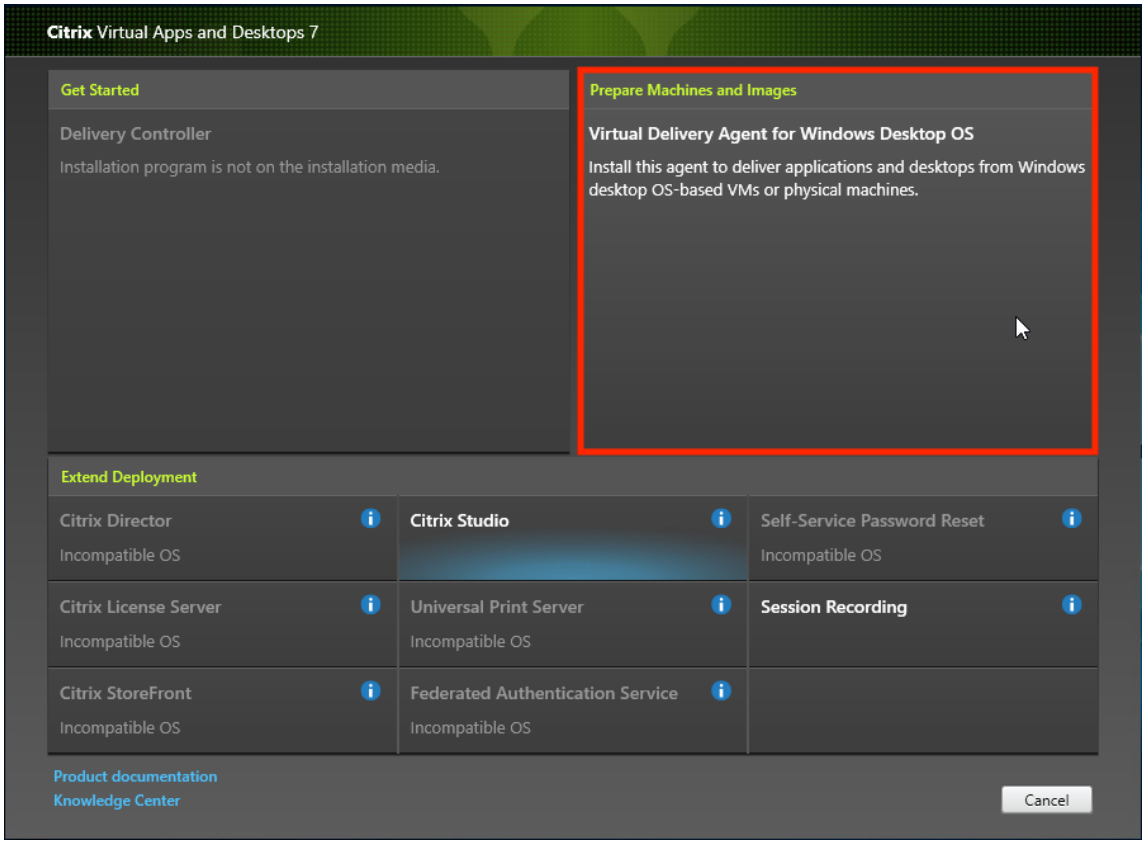
**Passaggio 2: Preparare l'immagine master**

Per preparare l'immagine master:

1. Individuare l'immagine master. Installare le applicazioni aziendali dell'organizzazione e tutte le altre app che gli utenti generalmente trovano utili.
2. Se si sta distribuendo Server VDI, attenersi alla procedura descritta nell'articolo Server VDI. Assicurarsi di includere il componente facoltativo, il **livello di personalizzazione utente**. Per i dettagli, vedere le Opzioni della riga di comando per l'installazione di un VDA.
3. Se si utilizza Windows 10, installare Virtual Delivery Agent (VDA) 1912 o versione successiva. Se è già installata una versione precedente del VDA, disinstallare prima la versione precedente. Quando si installa la nuova versione, assicurarsi di selezionare e installare il componente opzionale, **Citrix User Personalization Layer**, come segue:

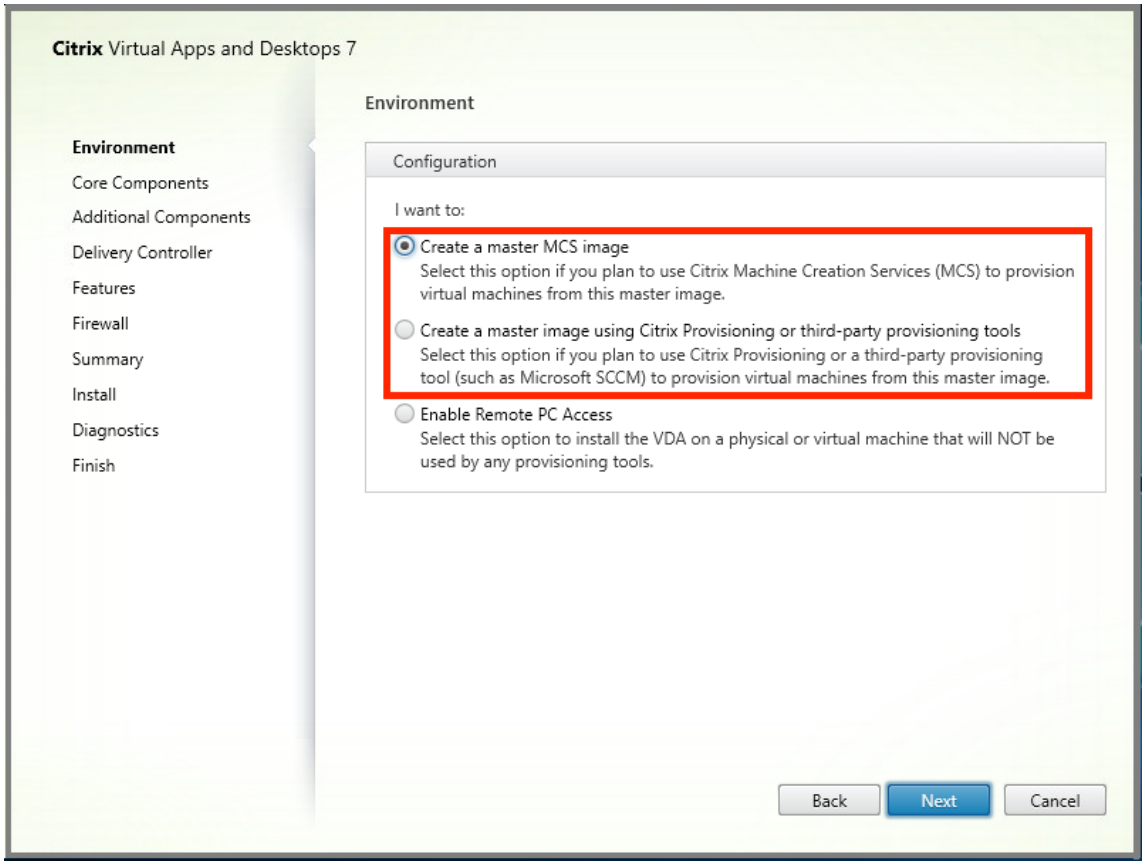
    a) Fare clic sul riquadro **Virtual Delivery Agent for Windows Desktop OS**:




a) **Environment** (Ambiente): selezionare **Create a master MCS image** (Creare un'immagine MCS master) o **Create a master image using Citrix Provisioning or third-party provisioning tools** (Creare un'immagine master utilizzando Citrix Provisioning o strumenti di provisioning di terze parti).

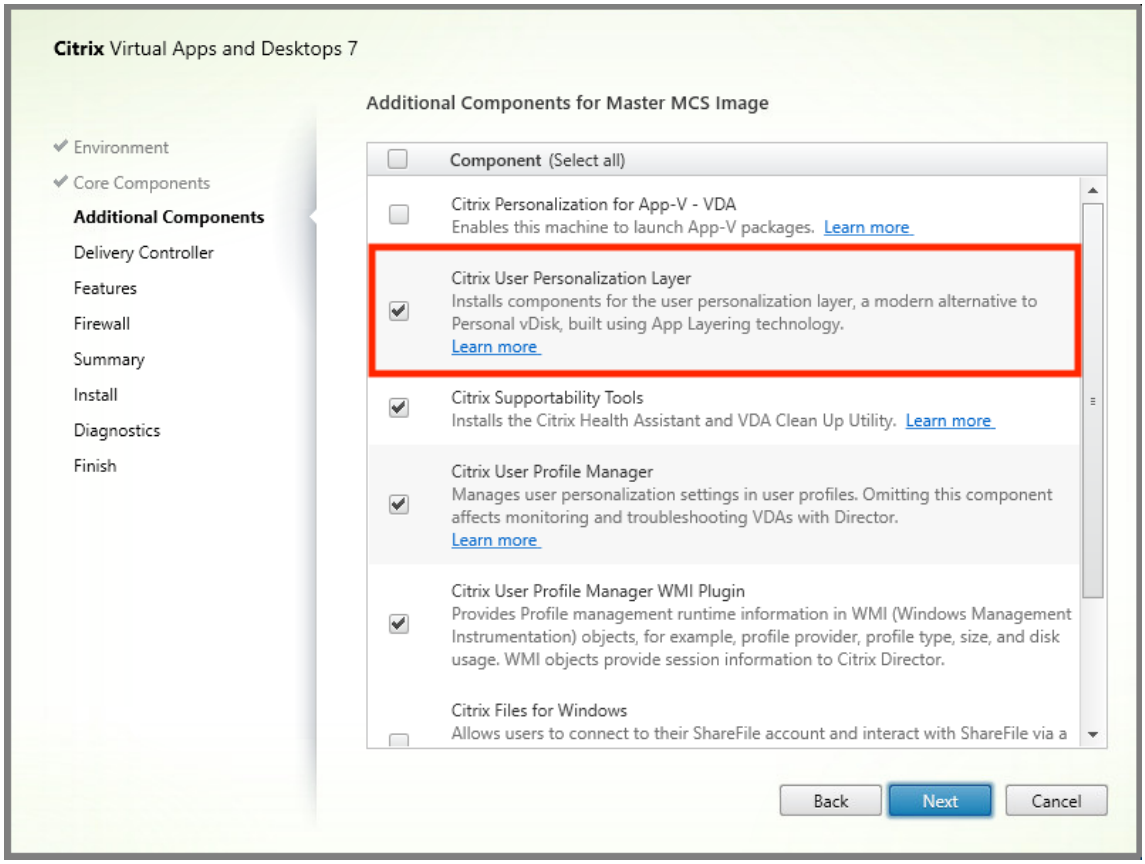
 




a) **Core components** (Componenti principali): fare clic su **Next**.

b) **Additional components** (Componenti aggiuntivi): inserire un segno di spunta in **Citrix User Personalization Layer**.




a) Fare clic sulle schermate di installazione rimanenti, configurando il VDA in base alle esigenze, e fare clic su **Install**. L'immagine si riavvia una o più volte durante l'installazione.

4. Lasciare disabilitata l'opzione **Windows updates**. Il programma di installazione del livello di personalizzazione utente disattiva gli aggiornamenti di Windows nell'immagine. Lasciare disabilitati gli aggiornamenti.

L'immagine è pronta per essere caricata in Web Studio.

> **Nota:**
>
> se si desidera semplicemente aggiornare il livello di personalizzazione utente (UPL), è possibile farlo con una versione più recente di UPL e il pacchetto autonomo. Non è necessario aggiornare il VDA.

### Passaggio 3: Creare un catalogo macchine

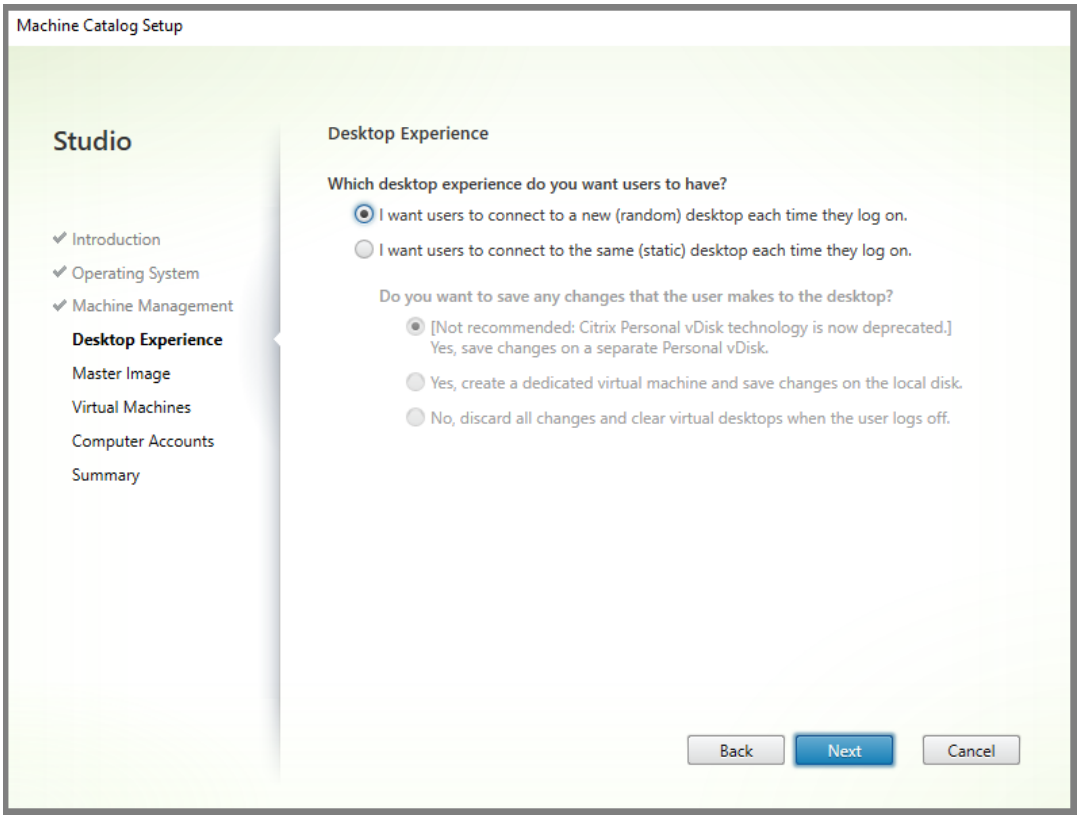
In Web Studio, seguire la procedura per creare un catalogo di macchine. Utilizzare le seguenti opzioni durante la creazione del catalogo:

1. Selezionare **Operating System** (Sistema operativo) e impostarlo su **Single-session OS** (Sistema operativo a sessione singola).

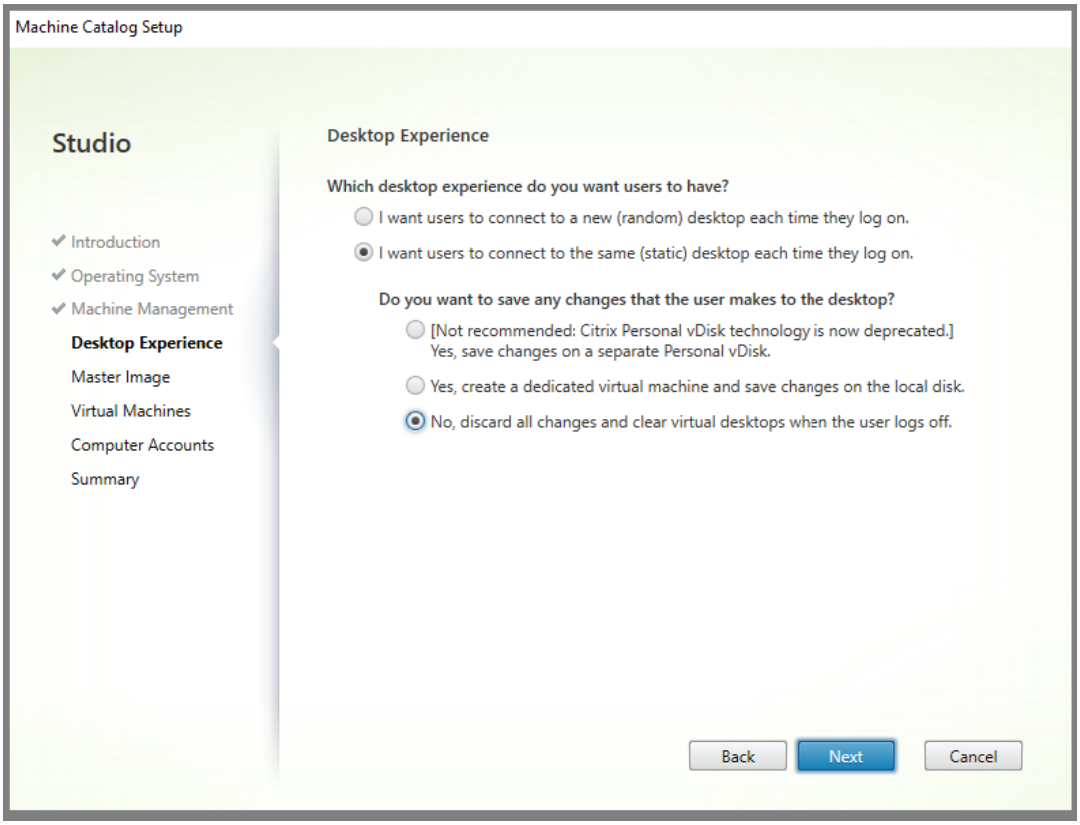
2. Selezionare **Machine Management** (Gestione macchine) e impostarlo su **Machines that are power managed** (Macchine con alimentazione gestita). Ad esempio, macchine virtuali o PC blade.
3. Selezionare **Desktop Experience** (Esperienza desktop) e impostarla sul tipo di catalogo **in pool casuale** o **in pool statico**, come negli esempi seguenti:

   - **In pool casuale:**




   - **In pool statico:** se si seleziona l'esperienza in pool statico, configurare i desktop in modo da eliminare tutte le modifiche e cancellare i desktop virtuali quando l'utente si scollega, come mostrato nello screenshot seguente:




> **Nota:**
>
> Il livello di personalizzazione utente non supporta i cataloghi in pool statico configurati per utilizzare Citrix Personal vDisk o assegnati come macchine virtuali dedicate.

4. Se si utilizza MCS, selezionare **Immagine master** e l'istantanea per l'immagine creata nella sezione precedente.
5. Configurare le rimanenti proprietà del catalogo in base alle esigenze dell'ambiente.

### Passaggio 4: Creare un gruppo di consegna

Creare e configurare un **gruppo di consegna**, comprendente i computer del catalogo macchine creato. Per ulteriori informazioni, vedere Creare gruppi di consegna.

### Passaggio 5: Creare criteri personalizzati per i gruppi di consegna

Per abilitare il montaggio dei livelli utente all'interno di Virtual Delivery Agent, utilizzare i parametri di configurazione per specificare:

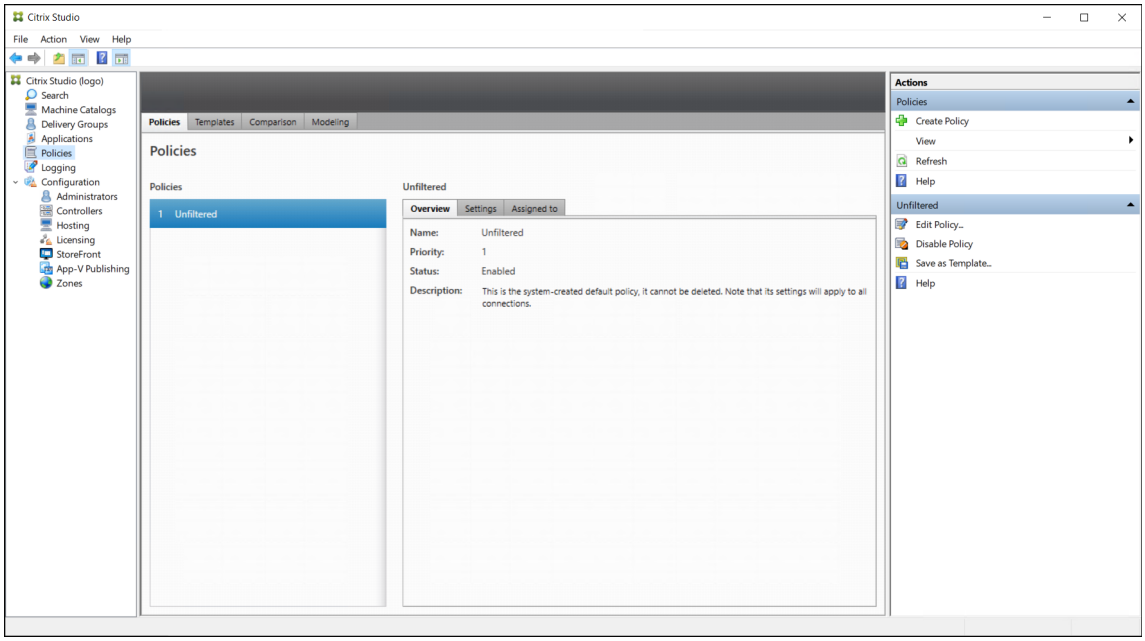
- In quale posizione sulla rete accedere ai livelli utente.

- Fino a che dimensione consentire ai dischi del livello utente di ingrandirsi.

Definire i parametri come criteri Citrix personalizzati in Web Studio e assegnarli al gruppo di consegna.

1. Accedere a Web Studio e selezionare **Policies** nel riquadro a sinistra:

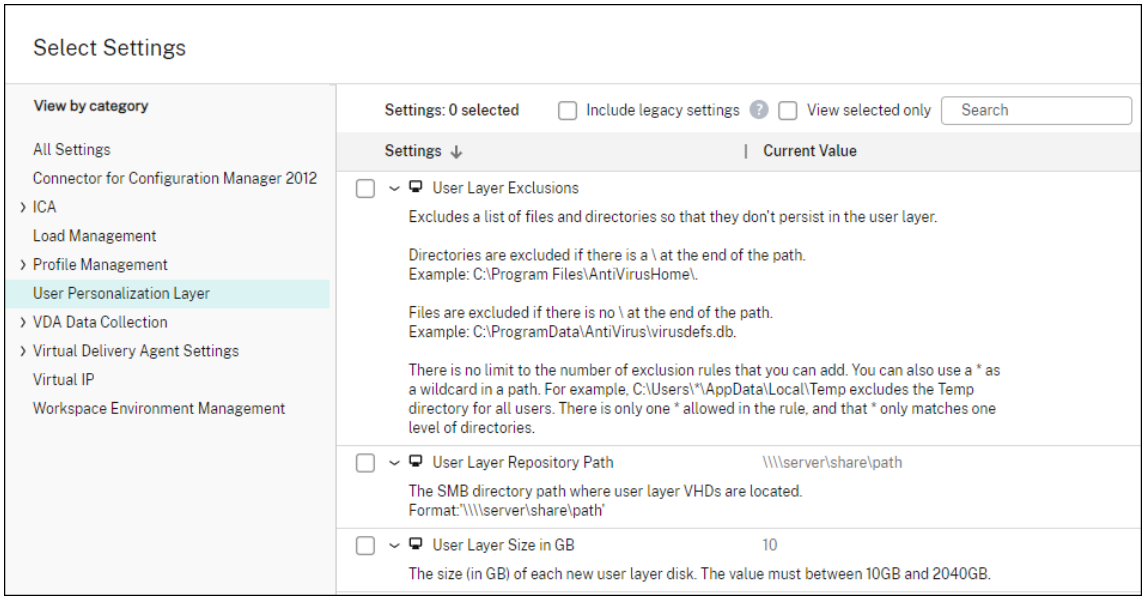



2. Selezionare **Create Policy** (Crea criterio) nella barra delle azioni. Viene visualizzata la finestra Create Policy (Crea criterio).
3. Digitare "user layer"(livello utente) nel campo di ricerca. Nell'elenco dei criteri disponibili vengono visualizzati i tre criteri seguenti:

   - Esclusioni a livello utente
   - User Layer Repository Path (Percorso del repository del livello utente)
   - User Layer Size GB (Dimensione livello utente GB)

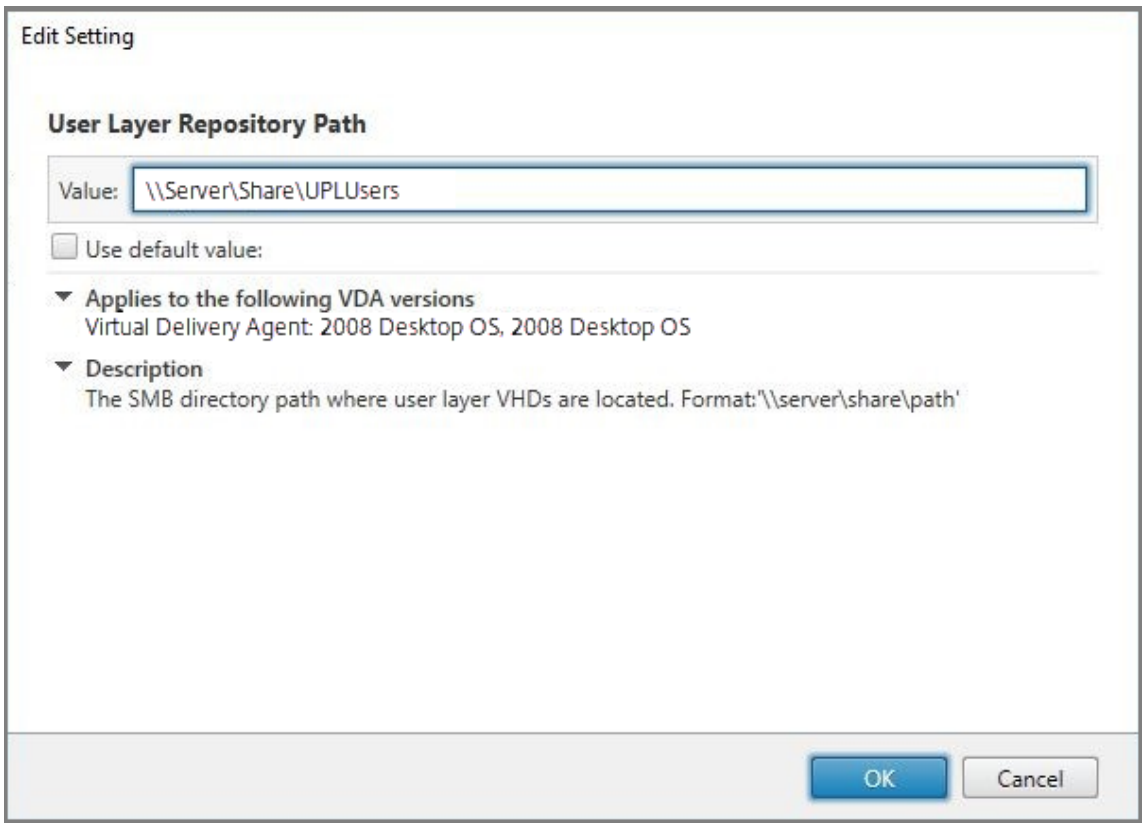
   > **Nota:**
   >
   > L'aumento delle dimensioni influisce sui nuovi livelli utente ed espande i livelli utente esistenti. La riduzione delle dimensioni influisce solo sui nuovi livelli utente. I livelli utente esistenti non diminuiscono mai di dimensioni.




4. Selezionare la casella di controllo accanto a **User Layer Repository Path** (Percorso del repository del livello utente) e fare clic su **Edit** (Modifica). Viene visualizzata la finestra Edit Setting (Modifica impostazione).
5. Immettere un percorso nel campo **Value** e fare clic su **Save**:
   - **Formato del percorso:** `\\server-name-or-address\share-name\folder`
   - **Esempio di percorso:** `\\Server\Share\UPLUsers`
   - **Esempio di percorsi risultanti:** per un utente chiamato **Alex** in **CoolCompanyDomain**, il percorso sarebbe: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

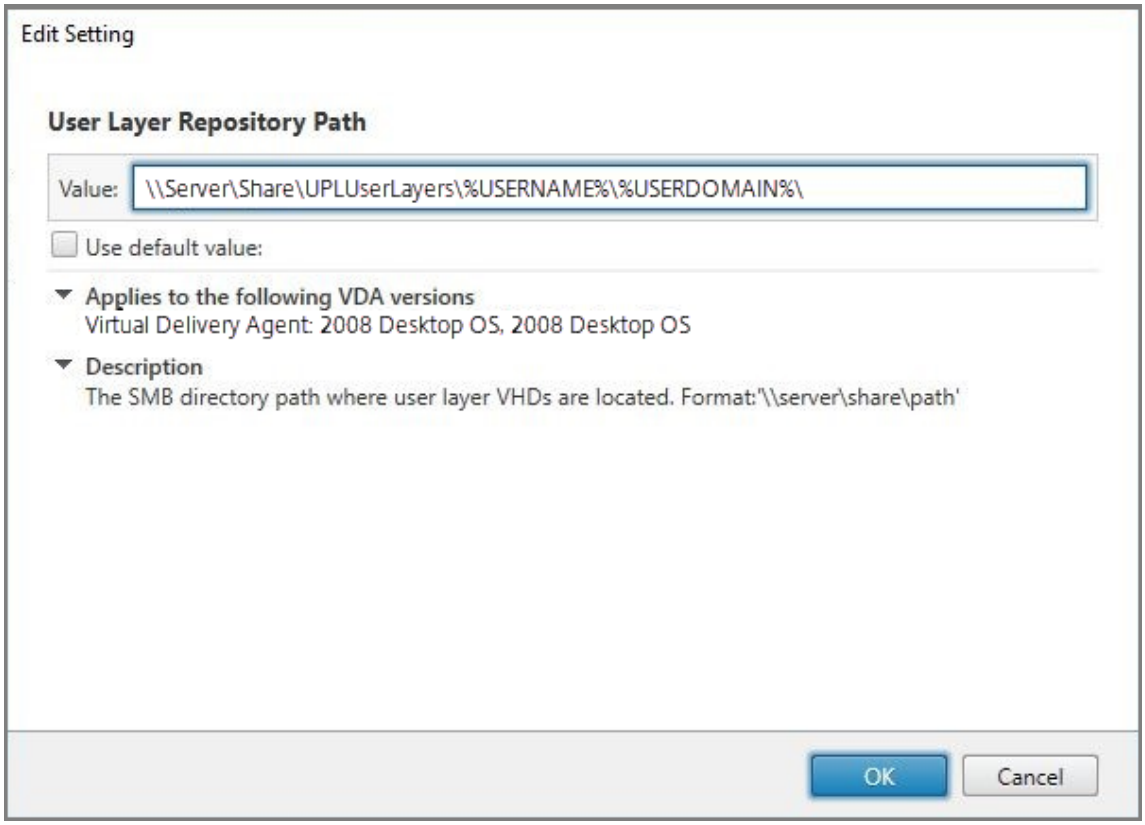



È possibile personalizzare il percorso utilizzando le variabili %USERNAME% e %USERDOMAIN%, le variabili di ambiente della macchina e gli attributi di Active Directory (AD). Quando sono espanse, queste variabili danno luogo a percorsi espliciti.

Esempio di variabili di ambiente:

- **Formato del percorso:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **Esempio di percorso:** `\\Server\Share\UPLUserLayers\\%USERNAME%\\%USERDOMAIN%`
- **Esempio di percorsi risultanti:** per un utente chiamato **Alex** in **CoolCompanyDomain**, il percorso sarebbe: `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`

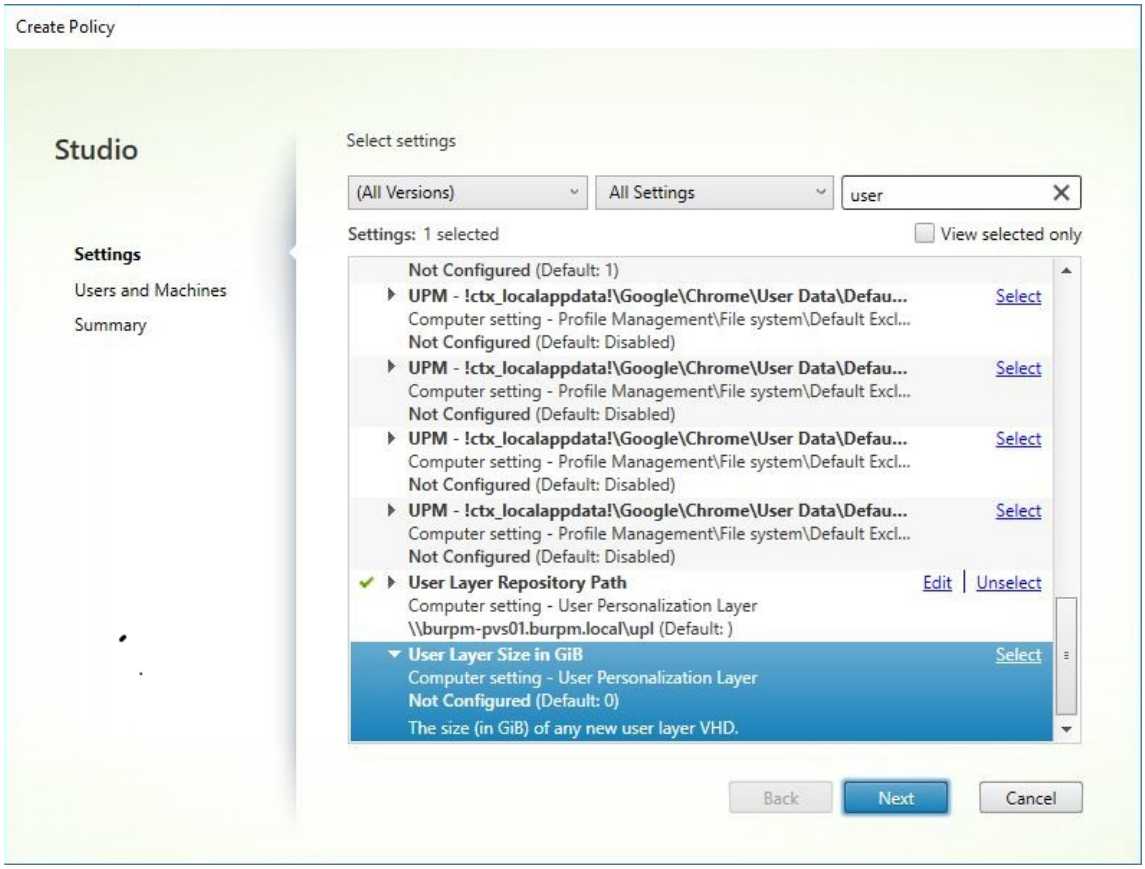



Esempio di attributi AD personalizzati:

- Formato del percorso: `\\Server-name-or-address\share-name\AD-attribute`
- Esempio di percorso: `\\Server\share\\#sAMAccountName#`
- Esempio di percorsi risultanti: `\\Server\share\JohnSmith` (se #sAMAccount-Name# si risolve in JohnSmith per l'utente corrente)

6. Facoltativo: selezionare la casella di controllo accanto a **User Layer Size in GB** (Dimensione del livello utente in GB) e fare clic su **Edit** (Modifica):

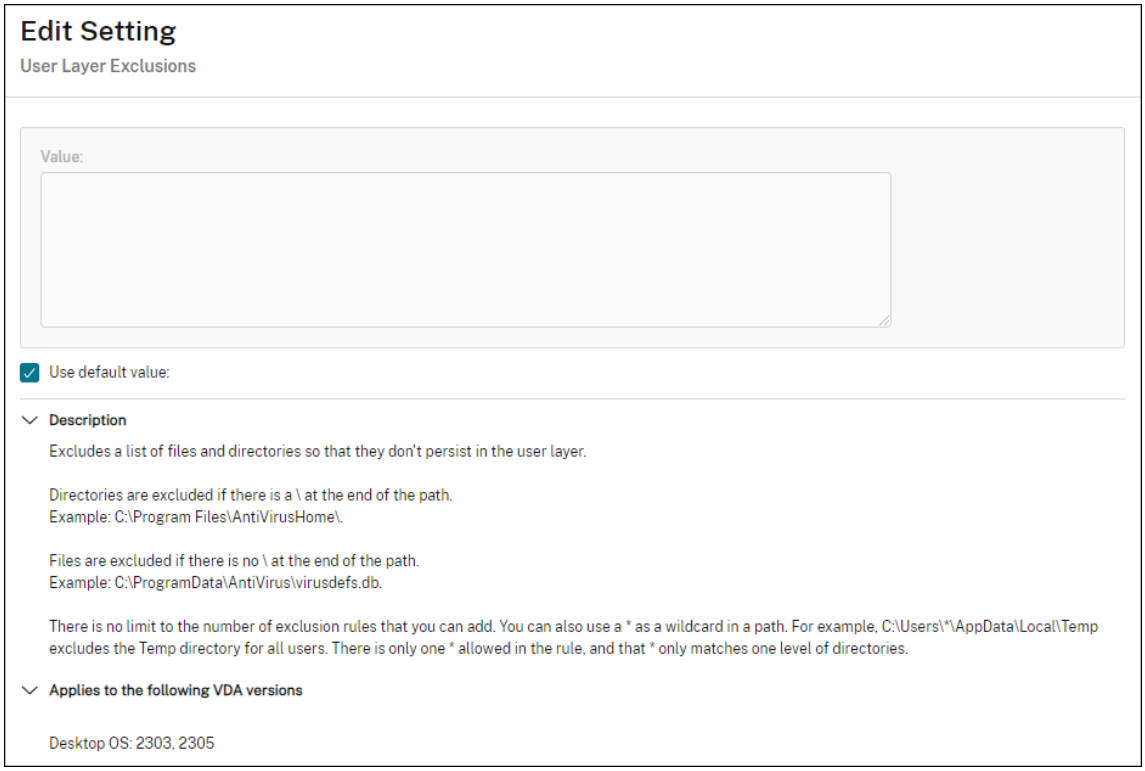



(Percorso del repository del livello utente)

Viene visualizzata la finestra Edit Settingsi.

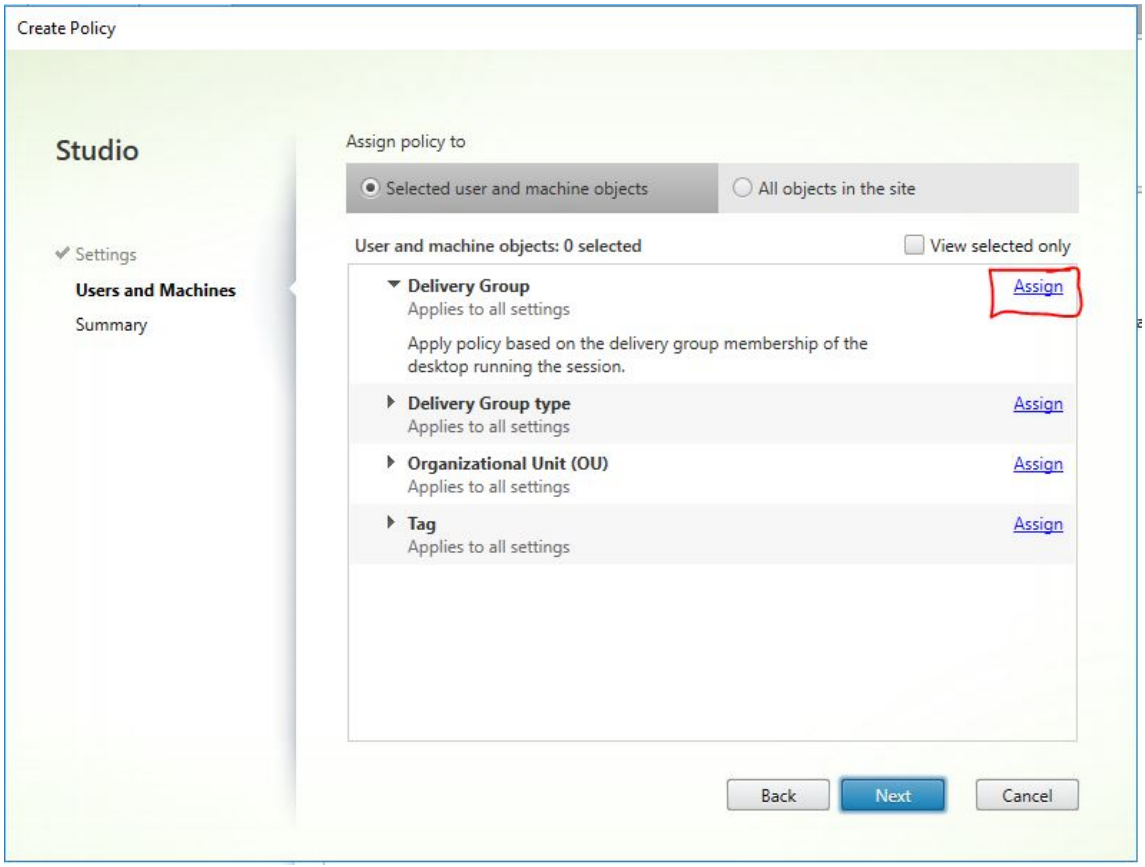
7. Facoltativo: modificare il valore predefinito di **10 GB** alla dimensione massima che ogni livello utente può raggiungere. Fare clic su **Salva**.
8. Facoltativo: selezionare la casella di controllo accanto a **User Layer Exclusions** (Esclusioni a livello utente) e fare clic su **Edit** (Modifica).




9. Facoltativo: specificare i file e le cartelle da escludere, quindi fare clic su **Save**. Per ulteriori informazioni, vedere la documentazione di Citrix App Layering.
10. Fare clic su **Next** per configurare utenti e macchine a cui effettuare l'assegnazione. Fare clic sul collegamento **Delivery Group Assign** (Assegna a gruppo di consegna) evidenziato in questa immagine:

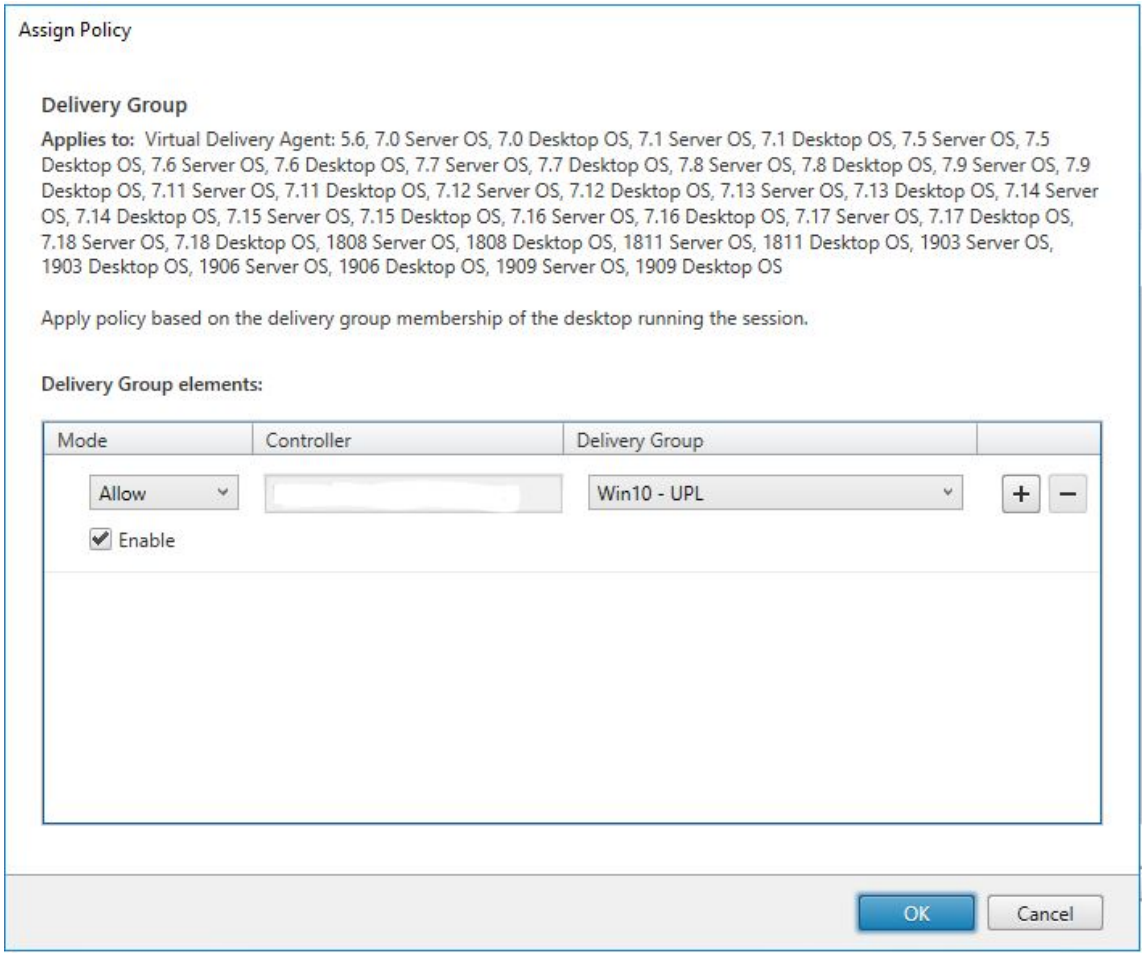
 




(Percorso del repository del livello utente)

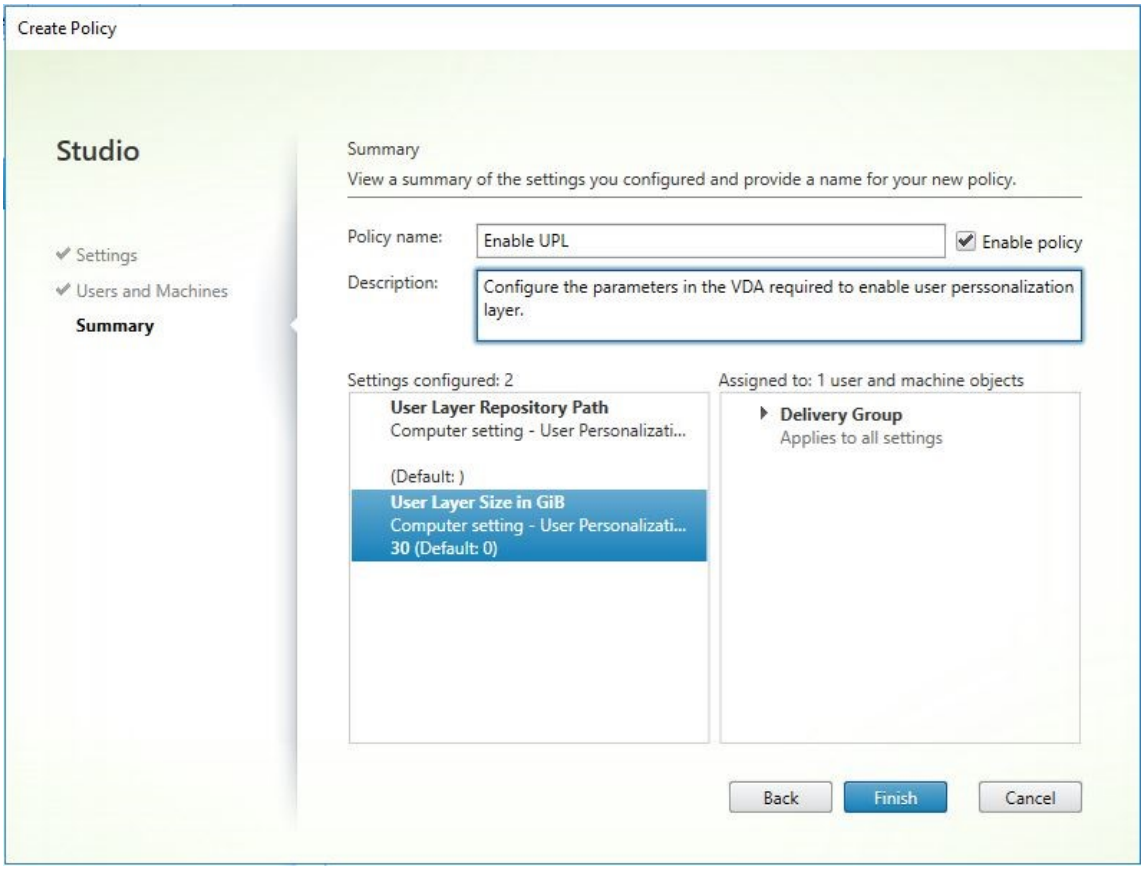
11. Nel menu **Delivery Group** selezionare il gruppo di consegna creato nella sezione precedente. Fare clic su **OK**.




12. Immettere un nome per il criterio. Fare clic sulla casella di controllo per attivare il criterio e quindi fare clic su **Finish**.




### Configurare le impostazioni di protezione nella cartella del livello utente

In qualità di amministratore di dominio, è possibile specificare più di una posizione di archiviazione per i livelli utente. Creare una sottocartella `\Users` per ciascun percorso di archiviazione (inclusa la posizione predefinita). Proteggere ogni posizione utilizzando le seguenti impostazioni.

| Nome impostazione | Valore | Si applica a |
|---|---|---|
| Proprietario autore | Modifica | Solo sottocartelle e file |
| Diritti del proprietario | Modifica | Solo sottocartelle e file |
| Utenti o gruppo | Crea cartella/Aggiunta dati;<br>Visita cartella/Esegui file;<br>Elenca cartella/Leggi dati;<br>Leggi attributi | Solo cartella selezionata |
| Sistema | Controllo completo | Cartella selezionata, sottocartelle e file relativi |

| Nome impostazione | Valore | Si applica a |
| --- | --- | --- |
| Amministratori di dominio e gruppo di amministrazione selezionato | Controllo completo | Cartella selezionata, sottocartelle e file relativi |

### Messaggi del livello utente

Quando un utente non è in grado di accedere al livello utente, riceve uno di questi messaggi di notifica.

- **Livello utente in uso**

  ```
  We were unable to attach your user layer because it is in use.
  Any changes you make to application settings or data will not be
  saved. Be sure to save any work to a shared network location.<!--
  NeedCopy-->
  ```

- **Livello utente non disponibile**

  ```
  We were unable to attach your user layer. Any changes you make to
   application settings or data will not be saved. Be sure to save
  any work to a shared network location.<!--NeedCopy-->
  ```

- **Il sistema non ripristinato dopo lo scollegamento dell'utente**

  ```
  This system was not shut down properly. Please log off immediately
   and contact your system administrator.<!--NeedCopy-->
  ```

### File di registro da utilizzare per la risoluzione dei problemi

Il file di registro ulayersvc.log contiene l'output del software del livello di personalizzazione utente in cui vengono registrate le modifiche.

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log
2 <!--NeedCopy-->
```

### Limiti

Tenere presenti le seguenti limitazioni durante l'installazione e l'utilizzo della funzionalità di livello di personalizzazione utente.

- *Non* tentare di distribuire il software del livello di personalizzazione utente su un livello all'interno di App Layering. Distribuire i livelli di personalizzazione degli utenti in Citrix Virtual Apps and Desktops oppure abilitare i livelli utente in un modello di immagine App Layering, non entrambe le cose. Entrambi i processi producono i livelli utente necessari.
- *Non* configurare la funzionalità di livello di personalizzazione utente con i cataloghi di macchine persistenti.
- *Non* utilizzare gli host di sessione.
- *Non* aggiornare il catalogo macchine con un'immagine che esegue una nuova installazione del sistema operativo (anche la stessa versione di Windows 10). La procedura consigliata consiste nell'applicare aggiornamenti al sistema operativo all'interno della stessa immagine master utilizzata durante la creazione del catalogo macchine.
- *Non* utilizzare driver di avvio, né altre personalizzazioni di avvio anticipato.
- *Non* eseguire la migrazione dei dati PvD alla funzionalità del livello di personalizzazione utente.
- *Non* eseguire la migrazione dei livelli utente esistenti dal prodotto App Layering completo alla funzionalità del livello di personalizzazione utente.
- *Non* modificare il percorso SMB del livello utente per accedere ai livelli utente creati utilizzando un'immagine del sistema operativo master diversa.
- Quando un utente si disconnette da una sessione e quindi effettua nuovamente l'accesso, la nuova sessione viene eseguita su un computer diverso all'interno del pool. In un ambiente VDI, Microsoft Software Center vede un'applicazione come **Installed** nel primo computer, ma **Unavailable** (Non disponibile) sul secondo computer.

  Per scoprire lo stato effettivo dell'applicazione, istruire l'utente a selezionare l'applicazione nel Software Center e fare clic su **Install**. SCCM aggiorna quindi lo stato al valore effettivo.
- Software Center si arresta occasionalmente immediatamente dopo l'avvio all'interno di un VDA con la funzionalità di livello di personalizzazione utente abilitata. Per evitare questo problema, seguire i consigli di Microsoft per l'implementazione di SCCM in un ambiente VDI XenDesktop. Assicurarsi inoltre che il servizio `ccmexec` sia in esecuzione prima di avviare Software Center.
- Nei criteri di gruppo (impostazioni computer), le impostazioni dei livelli utente sostituiscono le impostazioni applicate all'immagine master. Pertanto, le modifiche apportate nelle impostazioni computer utilizzando un oggetto criteri di gruppo non sono sempre presenti per l'utente al successivo accesso alla sessione.

  Per risolvere questo problema, creare uno script di accesso utente che invia il comando:

  ```
  gpupdate /force
  ```

  Ad esempio, un cliente imposta il seguente comando per l'esecuzione ad ogni accesso utente:

```
gpudate /Target:Computer /force
```

Per ottenere risultati ottimali, applicare le modifiche delle impostazioni computer direttamente al livello utente, dopo che l'utente ha effettuato l'accesso.

- Un account utente di dominio non deve essere l'ultimo utente ad aver effettuato l'accesso a un'immagine master. Altrimenti le macchine fornite in provisioning da quell'immagine avranno problemi.
- I certificati personalizzati non persistono quando UPL è abilitato in un ambiente Azure AD puro, a causa di un problema sottostante di Windows in esecuzione su Azure. Se Microsoft risolve questo problema in un miglioramento futuro, aggiorneremo questo articolo.

## Rimuovere componenti

January 7, 2024

Per rimuovere componenti, Citrix consiglia di utilizzare la funzionalità di Windows per la rimozione o la modifica dei programmi. In alternativa, è possibile rimuovere i componenti utilizzando la riga di comando o uno script sul supporto di installazione.

Quando si rimuovono i componenti, i prerequisiti non vengono rimossi e le impostazioni del firewall non vengono modificate. Ad esempio, quando si rimuove un Delivery Controller, il software SQL Server e i database non vengono rimossi.

Se è stato aggiornato un controller da una distribuzione precedente che includeva l'interfaccia Web, è necessario rimuovere il componente con interfaccia Web separatamente. Non è possibile utilizzare il programma di installazione per rimuovere l'interfaccia Web.

Per informazioni sulla rimozione di funzionalità non menzionate di seguito, vedere la documentazione della funzionalità.

### Preparazione

Prima di rimuovere un Controller, rimuoverlo dal sito. Per i dettagli, vedere Rimuovere un controller.

Chiudere Studio e Director prima di rimuoverli.

### Rimuovere i componenti utilizzando la funzionalità di Windows per rimuovere o modificare programmi

Dalla funzionalità di Windows per la rimozione o la modifica di programmi:

- Per rimuovere un Controller, Studio, Director, License Server o StoreFront, fare clic con il pulsante destro del mouse su **Citrix Virtual Apps *versione*** o **Citrix Virtual Apps and Desktops *versione*** e selezionare **Disinstalla**. Viene avviato il programma di installazione. Selezionare i componenti da rimuovere.

  In alternativa, è possibile rimuovere StoreFront facendo clic con il pulsante destro del mouse su **Citrix StoreFront** e selezionando **Disinstalla**.

- Per rimuovere un VDA, fare clic con il pulsante destro del mouse su **Citrix Virtual Delivery Agent *versione*** e selezionare **Disinstalla**. Il programma di installazione si avvia ed è possibile selezionare i componenti da rimuovere. Il computer si riavvia automaticamente dopo la rimozione, per impostazione predefinita.

- Per rimuovere Universal Print Server, fare clic con il pulsante destro del mouse su **Citrix Universal Print Server** e selezionare**Disinstalla**.

### Rimuovere i componenti principali utilizzando la riga di comando

Dalla directory `\x64\XenDesktop Setup`, eseguire il comando `XenDesktopServerSetup.exe`.

- Per rimuovere uno o più componenti, specificare le opzioni `/remove` e `/components`.
- Per rimuovere tutti i componenti, specificare l'opzione `/removeall`.

Per informazioni sui comandi e sui parametri, vedere Installare utilizzando la riga di comando.

Ad esempio, il comando seguente rimuove Web Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components
webstudio
```

### Rimuovere i VDA utilizzando la riga di comando

Dalla directory `\x64\XenDesktop Setup`, eseguire il comando `XenDesktopVdaSetup.exe`.

- Per rimuovere uno o più componenti, utilizzare le opzioni `/remove` e `/components`. Ad esempio, per rimuovere l'app VDA e Citrix Workspace, utilizzare `/remove /components vda,plugin`.
- L'opzione `/removeall` rimuove solo il VDA. Non rimuove l'app Citrix Workspace.

Per informazioni sui comandi e sui parametri, vedere Installare utilizzando la riga di comando.

Il computer si riavvia automaticamente dopo la rimozione, per impostazione predefinita.

Per rimuovere i VDA utilizzando uno script in Active Directory, vedere Installare o rimuovere i VDA utilizzando degli script.

# Aggiornamento e migrazione

January 7, 2024

## Introduzione

L'aggiornamento modifica la distribuzione in Citrix Virtual Apps and Desktops 7 versione corrente (CR) senza dover configurare nuove macchine o siti. Questo è noto come aggiornamento sul posto.

L'aggiornamento consente di accedere alle funzionalità e alle tecnologie più recenti per le quali si è idonei. Gli aggiornamenti possono anche contenere correzioni, chiarimenti e miglioramenti delle versioni precedenti.

### Panoramica dell'aggiornamento

1. Vedere l'articolo Aggiornare una distribuzione prima di iniziare l'aggiornamento. Questa è la fonte di informazioni principale per imparare a prepararsi per un aggiornamento e per implementarlo.
2. Assicurarsi che le date attuali di Customer Success Services siano valide e non siano scadute. Per ulteriori informazioni, vedere l'articolo Customer Success Services renewal licenses.
3. Completare la guida alla preparazione.
4. Eseguire i programmi di installazione per aggiornare i componenti principali.
5. Aggiornare i database di sistema e il sito.
6. Aggiornare i VDA sulle immagini (o direttamente sulle macchine).
7. Aggiornare gli altri componenti.

Ogni fase di preparazione e aggiornamento è descritta in dettaglio in Aggiornare una distribuzione.

## Versioni che è possibile aggiornare

È possibile eseguire l'aggiornamento a Citrix Virtual Apps and Desktops 2203 LTSR da:

- XenApp e XenDesktop 7.15 LTSR da CU5 a CU8
- Virtual Apps and Desktops 1912 con o senza CU, fino a CU5 incluso
- Versioni CR attualmente supportate di Citrix Virtual Apps and Desktops

È possibile fare riferimento alla Guida all'aggiornamento Citrix per un elenco delle versioni di Citrix Virtual Apps and Desktops (e XenApp e XenDesktop) da cui è possibile eseguire l'aggiornamento.

### Domande frequenti

In questa sezione si trovano le risposte ad alcune domande frequenti sull'aggiornamento di Citrix Virtual Apps and Desktops.

- **Qual è l'ordine corretto per aggiornare l'ambiente Virtual Apps and Desktops?**

  Per un'illustrazione e una descrizione della sequenza di aggiornamento consigliata, vedere Sequenza di aggiornamento e Procedura di aggiornamento.

- **Il mio sito comprende svariati Delivery Controller (in diverse zone). Cosa succede se aggiorno solo alcuni di essi? Devo aggiornare tutti i Controller presenti nel sito durante la stessa sessione di manutenzione?**

  La procedura migliore consiste nell'aggiornare tutti i Delivery Controller durante la stessa sessione di manutenzione, poiché vari servizi presenti in ciascun Controller comunicano tra loro. Mantenere versioni diverse potrebbe causare problemi. Durante una sessione di manutenzione, si consiglia di aggiornare metà dei Controller, aggiornare il sito e quindi aggiornare i Controller rimanenti (per ulteriori informazioni, vedere Procedura di aggiornamento).

- **Posso passare direttamente alla versione più recente o devo eseguire aggiornamenti incrementali?**

  È quasi sempre possibile eseguire l'aggiornamento alla versione più recente saltando le versioni intermedie, a meno che non sia esplicitamente indicato nell'articolo **Novità** della versione a cui si effettua l'aggiornamento. Vedere la Guida all'aggiornamento.

- **Un cliente può eseguire l'aggiornamento da un ambiente LTSR (Long Term Service Release) a una versione corrente?**

  Sì. I clienti non sono tenuti a continuare a utilizzare una LTSR per un periodo prolungato. I clienti possono spostare un ambiente LTSR a una versione corrente, in base ai requisiti e alle caratteristiche dell'azienda.

- **Sono consentite versioni miste dei componenti?**

  All'interno di ogni sito, Citrix consiglia di aggiornare tutti i componenti alla stessa versione. Sebbene sia possibile utilizzare versioni precedenti di alcuni componenti, così facendo potrebbero non essere disponibili tutte le funzionalità della versione più recente. Per ulteriori informazioni, vedere Considerazioni sull'ambiente misto.

- **Con quale frequenza deve essere aggiornata una versione corrente?**

Le versioni correnti raggiungono la fine della manutenzione (EOM) 6 mesi dopo la data di rilascio. Citrix consiglia ai clienti di adottare l'ultima versione corrente. Le versioni correnti raggiungono la fine del ciclo di vita (EOL) 18 mesi dopo la data di rilascio. Per ulteriori informazioni, vedere Ciclo di vita della versione corrente.

- **Cosa è consigliato: aggiornamento a LTSR o CR?**

  Le versioni correnti (CR) offrono le funzionalità di virtualizzazione di app, desktop e server più recenti e innovative. Questo permette di continuare a utilizzare tecnologia all'avanguardia e di rimanere un passo avanti rispetto alla concorrenza.

  Le LTSR (Long Term Service Release) sono ideali per ambienti di produzione aziendali di grandi dimensioni che preferiscono mantenere la stessa versione di base per un periodo prolungato.

  Per ulteriori informazioni, vedere Opzioni di manutenzione.

- **Devo aggiornare le mie licenze?**

  Assicurarsi che la data della licenza corrente non sia scaduta e che sia valida per la versione a cui si sta eseguendo l'aggiornamento. Vedere CTX111618. Per informazioni sul rinnovo, vedere Licenze di rinnovo di Customer Success Services.

- **Quanto tempo richiede un aggiornamento?**

  Il tempo necessario per aggiornare una distribuzione varia a seconda dell'infrastruttura e della rete. Quindi, non possiamo fornire una durata esatta.

- **Quali sono le migliori pratiche?**

  Assicurarsi di comprendere e seguire la guida alla preparazione.

- **Quali sistemi operativi sono supportati?**

  L'articolo Requisiti di sistema relativo alla versione a cui si sta eseguendo l'aggiornamento elenca i sistemi operativi supportati.

  Se la distribuzione corrente utilizza sistemi operativi non più supportati, vedere Sistemi operativi precedenti.

- **Quali versioni di VMware vSphere (vCenter + ESXi) sono supportate?**

  CTX131239 elenca gli host e le versioni supportati, oltre a collegamenti a problemi noti.

- **La mia versione quando raggiunge l'EOL?**

  Controllare la matrice del prodotto.

- **Quali sono i problemi noti dell'ultima versione?**

  - Citrix Virtual Apps and Desktops
  - StoreFront
  - Citrix Provisioning

- Citrix License Server
- App Citrix Workspace per Windows

### Ulteriori informazioni

Gli aggiornamenti della distribuzione Long Term Service Release (LTSR) utilizzano gli aggiornamenti cumulativi (CU). Un CU aggiorna i componenti di base di LTSR e ogni CU include il proprio metainstaller.

Ogni CU ha una documentazione dedicata. Ad esempio, per LTSR 7.15, seguire il collegamento alla pagina **What's new** (Novità) di LTSR per visualizzare l'ultimo CU. Ogni pagina CU include informazioni sulla versione supportata, istruzioni e un collegamento al pacchetto di download del CU.

## Migrazione

### Migrazione al cloud

È possibile utilizzare lo strumento di configurazione automatica per Citrix Virtual Apps and Desktops per eseguire la migrazione della distribuzione locale nel cloud. Per ulteriori informazioni, vedere Migrazione al cloud.

### Migrazione legacy

La migrazione consente di spostare i dati da una distribuzione precedente a una versione più recente. Il processo include l'installazione di componenti più recenti e la creazione di un nuovo sito, l'esportazione di dati dalla farm precedente e quindi l'importazione dei dati nel nuovo sito.

Non sono disponibili strumenti o script supportati per la migrazione delle versioni XenApp e XenDesktop o per la migrazione delle versioni precedenti di Citrix Virtual Apps and Desktops. L'*aggiornamento* è supportato per le versioni di Citrix Virtual Apps and Desktops elencate nella Guida all'aggiornamento Citrix e descritte in questa documentazione del prodotto.

Per i contenuti di migrazione XenApp 6.x precedenti, vedere quanto segue. Né gli script né gli articoli sono supportati né sottoposti a manutenzione.

- Gli script di migrazione open source per le versioni XenApp 6.x sono disponibili all'indirizzo https://github.com/citrix/xa65migrationtool. Citrix non supporta né sottopone a manutenzione questi script di migrazione
- Modifiche di 7.x
- Aggiornamento di un worker XenApp 6.5 a un nuovo VDA
- Migrazione di XenApp 6.x

# Aggiornare una distribuzione

April 3, 2024

## Introduzione

È possibile aggiornare determinate distribuzioni a versioni più recenti senza dover prima configurare nuovi computer o siti. Questo metodo è chiamato aggiornamento sul posto. Per informazioni su quali versioni di Citrix Virtual Apps and Desktops è possibile aggiornare, vedere la Guida all'aggiornamento Citrix.

Prima di effettuare l'aggiornamento a una qualsiasi delle versioni di Citrix Virtual Apps and Desktops, assicurarsi che le date attuali di Customer Success Services siano valide e non siano scadute. Per ulteriori informazioni, vedere l'articolo Customer Success Services renewal licenses.

Per avviare un aggiornamento, eseguire il programma di installazione dalla nuova versione per aggiornare i componenti principali installati in precedenza, i VDA e determinati altri componenti. Quindi aggiornare i database e il sito.

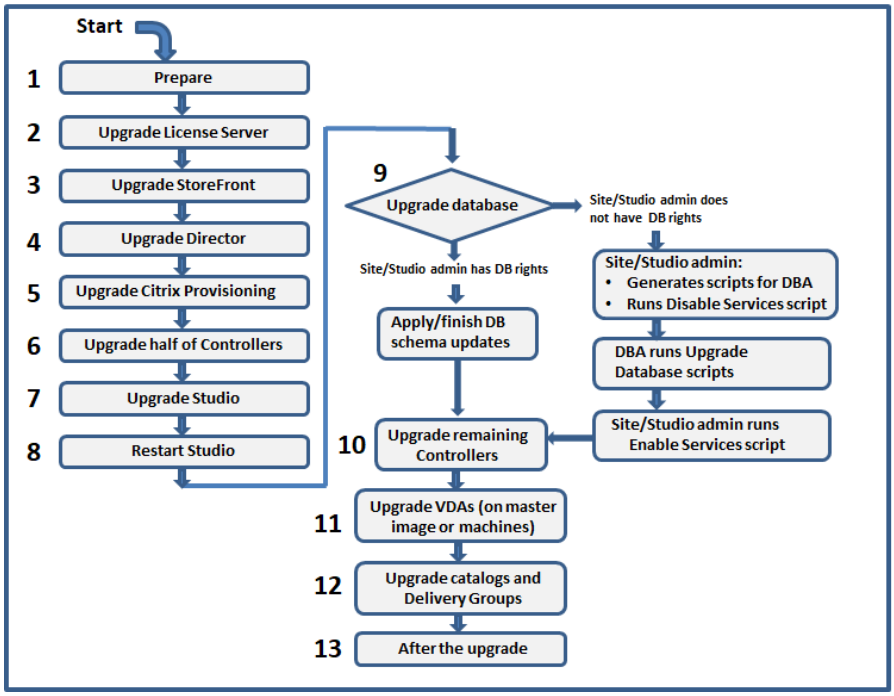
È possibile aggiornare qualsiasi componente che può essere installato con il programma di installazione completo del prodotto (e i programmi di installazione di VDA autonomi), se è disponibile una versione più recente. Per altri componenti non installati con il programma di installazione completo del prodotto (ad esempio Citrix Provisioning e Profile Management), vedere la documentazione del componente per indicazioni. Per gli aggiornamenti degli host, vedere la documentazione appropriata.

Esaminare tutte le informazioni contenute in questo articolo prima di iniziare un aggiornamento.

## Sequenza di aggiornamento

Il diagramma seguente mostra i passaggi della sequenza di aggiornamento. La procedura di aggiornamento contiene i dettagli di ogni passaggio del diagramma.




> **Nota:**
>
> Per evitare errori, è necessario aggiornare tutti i Delivery Controller e il database prima di eseguire qualsiasi attività relativa al provisioning e al gruppo di consegna, come la creazione di un nuovo catalogo di macchine, l'eliminazione di un catalogo di macchine, l'aggiornamento di una macchina in un gruppo di consegna e così via.

## Licenze Hybrid Rights

Le licenze Hybrid Rights sono licenze di abbonamento a termine che vengono fornite, in aggiunta alla sottoscrizione al servizio cloud, quando un cliente effettua la transizione da una licenza perpetua a una sottoscrizione a un servizio cloud. È anche possibile acquistare un componente aggiuntivo Hybrid Rights con le sottoscrizioni DaaS.

Se si dispone di una licenza Hybrid Rights con un attributo SaaS, quando si effettua l'aggiornamento a Citrix Virtual Apps and Desktops LTSR 2203 e versioni successive, si acquisisce il diritto ad accedere a funzionalità non disponibili con Citrix Virtual Apps and Desktops LTSR 1912. Queste funzionalità includono il provisioning e l'hosting di carichi di lavoro in cloud pubblici, come Microsoft Azure, AWS EC2 e Google Cloud. Prima di distribuire il nuovo file di licenza, aggiornare il server di licenza alla versione più recente.

Se si ha accesso a una licenza Hybrid Rights senza attributo SaaS, seguire questi passaggi per accedere alla nuova licenza Hybrid Rights con attributo SaaS:

> **Nota:**
>
> - Si riceverà un'email con un nuovo codice di licenza. Per ulteriori informazioni, vedere Use license access code.
> - Le licenze esistenti vengono revocate. Le licenze revocate devono essere eliminate dai server licenze e seguite dall'installazione di una nuova licenza. Per ulteriori informazioni, vedere Deleting license files.

1. Andare al portale di gestione licenze citrix.com Manage Licenses e scaricare il nuovo file di licenza Hybrid Rights con i diritti di provisioning cloud abilitati (attributo SaaS). Per ulteriori informazioni, vedere Download licenses. L'immagine seguente mostra il file di licenza Hybrid Rights con attributo SaaS nella sezione Increments.

```
INCREMENT XDT_PLT_CCS CITRIX 2022.1201 01-dec-2022 5 \
    VENDOR_STRING=;LT=RetailS;GP=720;PSL=10;CL=VDS,VDA,VDE,VDP,SaaS:SA=0;ODP=0;NUDURMIN=2880;NUDURMAX=525600;AP=ADMIN/INT/14
    OVERDRAFT=1 DUP_GROUP=V ISSUED=18-dec-2005 NOTICE="Citrix \
    Systems Inc." SN=RetailSSaaS SIGN="..."
```

2. Installare il file di licenza Hybrid Rights sul License Server. Per ulteriori informazioni, vedere Installare licenze.
3. Se c'è una variazione delle edizioni o del modello della licenza, assicurarsi di eseguire il comando broker per impostare l'edizione e il modello e quindi avviare l'aggiornamento sul posto. Per ulteriori informazioni sui comandi Broker, vedere la sezione SDK PowerShell Broker.

Per ulteriori informazioni sul supporto dei cloud pubblici con Citrix Virtual Apps and Desktops Current Releases e Long Term Service Release, vedere CTX270373.

### Procedura di aggiornamento

La maggior parte dei componenti principali del prodotto può essere aggiornata eseguendo il programma di installazione del prodotto sul computer contenente il componente.

Se un computer contiene più componenti (ad esempio Studio e License Server), tutti i componenti del computer vengono aggiornati se il supporto del prodotto contiene versioni più recenti del software.

Per utilizzare i programmi di installazione:

- Per eseguire l'interfaccia grafica completa del programma di installazione del prodotto, accedere la computer e quindi inserire il supporto o montare l'unità ISO per la nuova versione. Fare doppio clic su **AutoSelect**.
- Per utilizzare l'interfaccia della riga di comando, inserire il comando appropriato. Vedere Installare utilizzando la riga di comando.

#### Passaggio 1: preparazione

Prima di iniziare un aggiornamento, assicurarsi di essere pronti. Leggere e completare tutte le attività necessarie:

- Rimuovere PVD, AppDisks e host non supportati
- VDA con componenti PvD o AppDisks
- Limiti
- Considerazioni sull'ambiente misto
- Sistemi operativi precedenti
- Preparazione
- Test preliminari sul sito
- Controllo della versione di SQL Server

#### Passaggio 2: aggiornamento di License Server

Se l'installazione ha una nuova versione del software Citrix License Server, aggiornare questo componente prima di qualsiasi altro.

Se non è ancora stato determinato se il License Server è compatibile con la nuova versione, è essenziale eseguire il programma di installazione sul License Server prima di aggiornare qualsiasi altro componente principale.

#### Passaggio 3: aggiornamento di StoreFront

Se il supporto di installazione contiene una nuova versione del software StoreFront, eseguire il programma di installazione sul computer contenente il server StoreFront.

- Nell'interfaccia grafica, scegliere **Citrix StoreFront** nella sezione **Estendi distribuzione**.
- Dalla riga di comando, eseguire `CitrixStoreFront-x64.exe`, che è disponibile nella cartella `x64` del supporto di installazione di Citrix Virtual Apps and Desktops.

#### Passaggio 4: aggiornamento di Director

Se il supporto di installazione contiene una nuova versione del software Director, eseguire il programma di installazione sul computer che contiene Director.

#### Passaggio 5: aggiornamento di Citrix Provisioning

Il supporto di installazione di Citrix Provisioning è disponibile separatamente da quello di Citrix Virtual Apps and Desktops. Per informazioni su come installare e aggiornare il software del server e del

dispositivo di destinazione di Citrix Provisioning, vedere la documentazione del prodotto Citrix Provisioning.

#### Passaggio 6: aggiornamento di metà dei Delivery Controller

Ad esempio, se il sito dispone di quattro controller, eseguire il programma di installazione su due di essi.

Lasciare attiva metà dei controller consente agli utenti di accedere al sito. I VDA possono registrarsi con i controller rimanenti. Potrebbero esserci momenti in cui il sito ha una capacità ridotta perché sono disponibili meno controller. L'aggiornamento causa solo una breve interruzione nello stabilire nuove connessioni client durante le fasi finali di aggiornamento del database. I controller aggiornati non possono elaborare le richieste fino a quando non viene aggiornato l'intero sito.

Se il tuo sito dispone di un solo controller, non è utilizzabile durante l'aggiornamento.

I test preliminari sul sito vengono eseguiti sul primo controller, prima dell'avvio dell'aggiornamento effettivo. Per ulteriori informazioni, vedere Test preliminari sul sito.

#### Passaggio 7: aggiornamento di Studio

- Se Web Studio non è già stato aggiornato (perché si trovava sulla stessa macchina di un altro componente), eseguire il programma di installazione sulla macchina contenente Studio.

  > **Nota:**
  >
  > Dopo l'aggiornamento di Web Studio, le informazioni sulla versione potrebbero non essere aggiornate immediatamente. È possibile che venga richiesto di aggiornare Web Studio anche se è già aggiornato. Per risolvere il problema, accedere al server Web Studio, aprire Gestione Internet Information Services (IIS), passare a Pagina iniziale > Siti > Sito Web predefinito e selezionare **Riavvia** nel riquadro Gestione del sito Web.

- Se Web Studio e StoreFront sono installati sulla stessa macchina e si desidera aggiornarli entrambi a questa versione, consigliamo di installare Web Studio su una macchina diversa per l'aggiornamento. Per ulteriori informazioni, vedere Installare Web Studio.

  In alternativa, se si preferisce mantenere Web Studio e StoreFront sulla stessa macchina, sostituire il contenuto di `web.config` in `C:\Program Files\Citrix\Web Studio\Site` con quanto segue dopo l'aggiornamento di Web Studio.

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <rewrite>
```

```
            <rules>
                <rule name="Redirect to https" stopProcessing="true">
                    <match url="(.*)" />
                    <conditions>
                        <add input="{
HTTPS }
" pattern="^OFF$" />
                    </conditions>
                    <action type="Redirect" url="https://{
HTTP_HOST }
{
REQUEST_URI }
" appendQueryString="false" />
                </rule>
                <rule name="Redirect from studio" stopProcessing="true"
                    >
                    <match url="^studio/?$" />
                    <action type="Redirect" url="/citrix/" redirectType
                        ="Permanent" />
                </rule>
                <rule name="Redirect from webstudio" stopProcessing="
                    true">
                    <match url="^webstudio/?$" />
                    <action type="Redirect" url="/citrix/" redirectType
                        ="Permanent" />
                </rule>
                <rule name="Angular Routes" stopProcessing="true">
                    <match url="^(search|machinecatalogs|deliverygroups
                        |applications|policies|logging|administrators|
                        hosting|storefront|appvpublishing|settings|
                        backuprestore|zones|licensing|spa|login|logged-
                        out|site-error|permission-error|orchserver-error
                        )" />
                    <conditions logicalGrouping="MatchAll">
                        <add input="{
REQUEST_FILENAME }
" matchType="IsFile" negate="true" />
                        <add input="{
REQUEST_FILENAME }
" matchType="IsDirectory" negate="true" />
                    </conditions>
                    <action type="Rewrite" url="/citrix/" />
                </rule>
            </rules>
        </rewrite>
        <staticContent>
            <clientCache cacheControlMode="DisableCache" />
        </staticContent>
    </system.webServer>
</configuration>
<!--NeedCopy-->
```

#### Passaggio 8: riavvio di Studio

Riavviare Web Studio aggiornato. Il processo di aggiornamento riprende automaticamente.

#### Passaggio 9: aggiornamento del database e del sito

> **Nota:**
>
> Per evitare errori, è necessario aggiornare tutti i Delivery Controller e il database prima di eseguire qualsiasi attività relativa al provisioning e al gruppo di consegna, come la creazione di un nuovo catalogo di macchine, l'eliminazione di un catalogo di macchine, l'aggiornamento di una macchina in un gruppo di consegna e così via.

Vedere Preparazione per informazioni sulle autorizzazioni necessarie per aggiornare lo schema dei database di SQL Server.

- Se si dispone di autorizzazioni sufficienti per aggiornare lo schema del database di SQL Server, è possibile avviare un aggiornamento automatico del database. Continuare con Aggiornare automaticamente il database e il sito.
- Se non si dispone di autorizzazioni sufficienti per il database, è possibile avviare un aggiornamento manuale che utilizza script e procedere con l'aiuto dell'amministratore del database (un utente che dispone delle autorizzazioni necessarie). Per un aggiornamento manuale, l'utente di Studio genera gli script e quindi esegue gli script che abilitano e disabilitano i servizi. L'amministratore del database esegue altri script che aggiornano lo schema del database, utilizzando l'utilità SQLCMD o SQL Server Management Studio in modalità SQLCMD. Continuare con Aggiornare manualmente il database e il sito.
- Se si dispone di una distribuzione multizona e si desidera aggiornare automaticamente il database e il sito, Citrix consiglia di eseguire l'aggiornamento dbschema nella stessa zona in cui sono ospitati i database SQL server del sito. In caso contrario, l'aggiornamento automatico del database e del sito potrebbe non riuscire.

Citrix consiglia vivamente di eseguire il backup del database prima dell'aggiornamento. Vedere CTX135207. Durante un aggiornamento del database, i servizi del prodotto sono disattivati. Durante questo periodo, i controller non possono mediare nuove connessioni per il sito, quindi è bene pianificare attentamente.

#### Aggiornare automaticamente il database e il sito

1. Avviare Studio appena aggiornato.
2. Indicare che si desidera avviare automaticamente l'aggiornamento del sito e confermare di essere pronti.

L'aggiornamento del database e del sito procede.

#### Aggiornare manualmente il database e il sito

1. Avviare Studio appena aggiornato.
2. Indicare che si desidera aggiornare manualmente il sito. La procedura guidata verifica la compatibilità di License Server e chiede conferma.
3. Confermare di aver eseguito il backup del database.

   La procedura guidata genera e visualizza gli script insieme a un elenco di controllo dei passaggi di aggiornamento. Se lo schema di un database non è stato modificato dopo l'aggiornamento della versione del prodotto, tale script non viene generato. Ad esempio, se lo schema del database di registrazione non cambia, lo script `UpgradeLoggingDatabase.sql` non viene generato.
4. Eseguire i seguenti script nell'ordine indicato.

   - `DisableServices.ps1`: l'utente di Studio esegue questo script PowerShell su un controller per disabilitare i servizi del prodotto.
   - `UpgradeSiteDatabase.sql`: l'amministratore del database esegue questo script SQL sul server che contiene il database del sito
   - `UpgradeMonitorDatabase.sql`: l'amministratore del database esegue questo script SQL sul server che contiene il database di monitoraggio.
   - `UpgradeLoggingDatabase.sql`: l'amministratore del database esegue questo script SQL sul server che contiene il database di registrazione della configurazione. Eseguire questo script solo se il database cambia (ad esempio, dopo aver applicato un hotfix).
   - `EnableServices.ps1`: l'utente di Studio esegue questo script PowerShell su un controller per abilitare i servizi del prodotto.

   Dopo aver completato l'aggiornamento del database e aver attivato i servizi del prodotto, Studio esegue automaticamente il test dell'ambiente e della configurazione, quindi genera un report HTML. Se vengono identificati problemi, è possibile ripristinare il backup del database. Dopo aver risolto i problemi, è possibile aggiornare nuovamente il database.
5. Dopo aver completato le attività indicate nell'elenco di controllo, fare clic su **Fine aggiornamento**.

#### Passaggio 10: aggiornamento dei Delivery Controller rimanenti

Da Studio appena aggiornato, selezionare **Citrix Studio** *nome-sito* nel riquadro di navigazione. Nella scheda **Attività comuni** selezionare **Aggiornamento dei Delivery Controller rimanenti**.

> **Nota:**
>
> Per rendere disponibile **Upgrade remaining Delivery Controllers** (Aggiorna i controller di consegna rimanenti), creare almeno un catalogo di macchine e un gruppo di consegna per il sito.

Dopo aver completato l'aggiornamento e aver confermato il completamento, chiudere Studio e riaprirlo. Studio potrebbe richiedere un aggiornamento del sito aggiuntivo per registrare i servizi del controller nel sito o per creare un ID zona se non esiste.

#### Passaggio 11: aggiornamento dei VDA

> **Importante:**
>
> Se si sta aggiornando un VDA alla versione 1912 o successiva, vedere Aggiornamento dei VDA a 1912 o versioni successive.

Eseguire il programma di installazione del prodotto su macchine contenenti VDA.

Se sono stati utilizzati Machine Creation Services e un'immagine master per creare macchine, passare all'host e aggiornare il VDA sull'immagine master. È possibile utilizzare uno qualsiasi dei programmi di installazione di VDA disponibili.

- Per istruzioni sull'interfaccia grafica, vedere Installare i VDA.
- Per informazioni sulla riga di comando, vedere Installare utilizzando la riga di comando.

Se è stato utilizzato Citrix Provisioning per creare macchine, vedere la documentazione del prodotto Citrix Provisioning per informazioni sull'aggiornamento.

#### Passaggio 12: aggiornamento dei cataloghi di macchine e dei gruppi di consegna

- Aggiornare i cataloghi che utilizzano macchine con VDA aggiornati.
- Aggiornare i cataloghi che utilizzano macchine con VDA aggiornati.
- Aggiornare i gruppi di consegna che utilizzano macchine con VDA aggiornati.

#### Passaggio 13: dopo l'aggiornamento

Dopo aver completato un aggiornamento, è possibile effettuare un test del sito appena aggiornato. Da Studio selezionare **Citrix Studio nome-sito** nel riquadro di navigazione. Nella scheda **Attività comuni** selezionare **Test sito**. Questi test vengono eseguiti automaticamente dopo l'aggiornamento del database, ma è possibile eseguirli nuovamente in qualsiasi momento.

I test potrebbero non riuscire per un controller su Windows Server 2016 quando viene utilizzato un Microsoft SQL Server Express locale per il database del sito, se il servizio SQL Server Browser non viene avviato. Per evitare il problema:

- Abilitare il servizio Browser SQL Server (se necessario) e quindi avviarlo.
- Riavviare il servizio SQL Server (SQLEXPRESS).

Aggiornare gli altri componenti della distribuzione. Per informazioni, vedere la documentazione dei prodotti seguenti:

- StoreFront
- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- Profile Management
- Citrix Provisioning
- Registrazione della sessione
- Workspace Environment Management

Se è necessario sostituire il software Microsoft SQL Server Express LocalDB con una versione successiva, vedere Sostituire SQL Server Express LocalDB.

### Aggiornamento Dbschema

Quando si aggiorna la propria distribuzione, è possibile aggiornare diversi schemi di database. La tabella seguente elenca quali schemi di database vengono aggiornati durante il processo:

| From\To | 1912 CU1 | 1912 CU2 | 1912 CU3 | 1912 CU4 | 1912 CU5 | 2203 |
|---|---|---|---|---|---|---|
| 7.15 RTM or 7.15 CU releases | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config; Logging |
| 1912 RTM | Config | Site, Config | Site, Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config; Logging |
| 1912 CU1 | | Site | Site, Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config; Logging |
| 1912 CU2 | | | Site, Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config; Logging |
| 1912 CU3 | | | | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config; Logging |
| 1912 CU4 | | | | | Site, Config | Site; Monitor; Config; Logging |
| 1912 CU5 | | | | | | Site; Monitor; Config; Logging |
| 2112 | | | | | | Site; Monitor; Config |

Definizione dei termini:

- Sito: archivio dati del sito. L'aggiornamento di Dbschema viene effettuato nell'archivio dati del sito.
- Monitor: archivio dati di monitoraggio. L'aggiornamento di Dbschema viene effettuato nell'archivio dati di monitoraggio.
- Config: tabella di configurazione. La versione di Desktop Studio, le informazioni sulle licenze o entrambe vengono aggiornate nella tabella Configuration.
- Registrazione: registrazione dell'archivio dati. L'aggiornamento di Dbschema viene effettuato nell'archivio dati di registrazione.

### Aggiornare vDAS alla versione 2203 o successiva

Se il componente Personal vDisk (PvD) è stato installato su un VDA, tale VDA non può essere aggiornato alla versione 2203 o successiva. Per utilizzare il nuovo VDA, è necessario disinstallare il VDA corrente e quindi installare il nuovo VDA.

Questa istruzione si applica anche se non PvD non è stato mai usato.

Ecco come il componente PvD potrebbe essere stato installato nelle versioni precedenti:

- Nell'interfaccia grafica del programma di installazione VDA, PvD era un'opzione nella pagina **Componenti aggiuntivi**. Nelle versioni 7.15 LTSR e 7.x precedenti questa opzione era attivata per impostazione predefinita. Quindi, se sono state accettate le impostazioni predefinite (o se l'opzione è stata abilitata esplicitamente in qualsiasi versione), PvD è stato installato.
- Sulla riga di comando, l'opzione `/baseimage` ha installato PvD. Se è stata specificata questa opzione o è stato utilizzato uno script che la conteneva, è stato installato PvD.

Se non è noto se sul VDA è installato PvD, eseguire il programma di installazione per il nuovo VDA (2203 o successivo) sulla macchina o sull'immagine.

- Se PvD è installato, viene visualizzato un messaggio che indica che è presente un componente incompatibile.
  - Dall'interfaccia grafica, fare clic su **Cancel** nella pagina contenente il messaggio, quindi confermare che si desidera chiudere il programma di installazione.
  - Dall'interfaccia della riga di comando, il comando fallisce semplicemente con il messaggio visualizzato.
- Se PvD non è installato, l'aggiornamento procede.

#### Cosa fare

Se nel VDA non è installato PvD, seguire la normale procedura di aggiornamento.

Se nel VDA è installato PvD:

1. Disinstallare l'attuale VDA.
2. Installare il nuovo VDA.

Se si desidera continuare a utilizzare PvD sui computer Windows 10 (1607 e versioni precedenti, senza aggiornamenti), VDA 7.15 LTSR è l'ultima versione supportata.

> **Nota:**
>
> *È possibile usare Personal vDisk con i desktop Windows 7 in XenApp e XenDesktop 7.15 LTSR?*
>
> Citrix ha escluso Personal vDisk (PvD) da XenApp e XenDesktop 7.6 LTSR, modifica che è stata

> annunciata in gennaio 2016. Inoltre, Citrix ha annunciato la deprecazione della tecnologia PvD e consiglia ai clienti di iniziare a utilizzare Citrix App Layering in futuro. Citrix App Layering (versione 4.4 e successive) è un componente compatibile di XenApp e XenDesktop 7.15 LTSR. Tuttavia, per aiutare i clienti che hanno le distribuzioni PvD esistenti su Windows 7 a migrare alla tecnologia Citrix App Layering, Citrix ha deciso di fornire supporto limitato nel tempo per le distribuzioni PvD per i desktop Windows 7 tramite XenApp e XenDesktop 7.15 LTSR Cumulative Updates (CU) fino al 14 gennaio 2020. Il componente PvD verrà rimosso dai CU LTSR e non sarà supportato dopo il 14 gennaio 2020. Inoltre, l'uso di PvD per Windows 7 dopo il 14 gennaio 2020 renderà i siti LTSR non conformi. PvD per Windows 10 continua anche ad essere escluso da 7.15 LTSR. Pertanto, i clienti non devono utilizzarlo con i loro siti LTSR 7.15.

### Rimuovere PvD, AppDisks e host non supportati

Le tecnologie e i tipi di host seguenti non sono supportati nelle distribuzioni di Citrix Virtual Apps and Desktops 7 versione corrente:

- **Personal vDisks (PvD)** per la memorizzazione dei dati accanto alle VM degli utenti nei cataloghi. La funzionalità del livello di personalizzazione utente gestisce ora la persistenza dell'utente.
- **AppDisks** per la gestione delle applicazioni utilizzate nei gruppi di consegna.
- **Tipi di host:** Azure Classic, CloudPlatform (il prodotto Citrix originale).
  - Per i tipi di host supportati in questa versione, vedere Requisiti di sistema.
  - Per informazioni su modi alternativi per continuare a utilizzare ARM e AWS, vedere CTX270373.

Se la distribuzione corrente utilizza PvD o AppDisks o dispone di connessioni a tipi di host non supportati (ad esempio, Microsoft Azure Classic), è possibile eseguire l'aggiornamento alla versione 2006 (o versioni successive supportate) solo dopo aver rimosso gli elementi che utilizzano tali tecnologie. Se la distribuzione corrente utilizza connessioni a host cloud pubblici (ad esempio, AWS), assicurarsi di avere una licenza Hybrid Rights prima di eseguire l'aggiornamento. Quando il programma di installazione rileva una o più tecnologie o connessioni host non supportate senza la licenza Hybrid Rights, l'aggiornamento viene sospeso o interrotto e viene visualizzato un messaggio esplicativo. I registri del programma di installazione ne contengono i dettagli.

Per garantire l'esito positivo dell'aggiornamento, vedere e seguire le istruzioni applicabili per rimuovere gli elementi non supportati.

- Rimuovere PvD
- Rimuovere AppDisks
- Rimuovere gli elementi host non supportati

Anche se non è stato utilizzato PvD o AppDisks nella distribuzione, è possibile che gli MSI correlati siano stati inclusi in un'installazione o un aggiornamento VDA precedente. Prima di poter aggiornare

i VDA alla versione 2006 (o a una versione successiva supportata), è necessario rimuovere tale software, anche se non è mai stato utilizzato. Quando si utilizza l'interfaccia grafica, tale rimozione può essere eseguita automaticamente oppure è possibile includere le opzioni di rimozione quando si utilizza l'interfaccia CLI. Per ulteriori informazioni, vedere Aggiornamento dei VDA con componenti PvD o AppDisks.

#### Rimuovere PvD

Un aggiornamento della distribuzione non può avere esito positivo fino a quando non vengono rimossi tutti i computer configurati per l'utilizzo di PvD. Ciò influisce sui cataloghi e i gruppi di consegna.

Per rimuovere PvD da gruppi e cataloghi:

1. Da Studio, se un gruppo di consegna contiene macchine di un catalogo che utilizza PvD, rimuovere tali macchine dal gruppo.
2. Da Studio, eliminare tutti i cataloghi contenenti macchine che utilizzano PvD.

**Aggiornamenti dei VDA:** l'aggiornamento della distribuzione non rileva se i VDA hanno i componenti AppDisk o PvD installati. Tuttavia, i programmi di installazione dei VDA lo fanno. Per ulteriori informazioni, vedere VDA con componenti PvD o AppDisks.

Se si prevede di utilizzare App Layering anziché PvD, vedere Migrazione di PvD ad App Layering per informazioni sullo spostamento dei dati.

#### Rimuovere AppDisks

Un aggiornamento della distribuzione non può procedere fino a quando non si rimuove AppDisks da tutti i gruppi di consegna che li utilizzano e quindi rimuovere gli AppDisks stessi.

1. Selezionare **Gruppi di consegna** nel riquadro di spostamento di Studio.
2. Selezionare un gruppo e quindi fare clic su **Gestisci AppDisks** nel riquadro azioni.
3. Fare clic sull'azione che rimuove AppDisk dal gruppo.
4. Ripetere i passaggi 2 e 3 per ogni gruppo di consegna che utilizza AppDisks.
5. Selezionare **AppDisks** nel riquadro di spostamento Studio.
6. Selezionare un AppDisk e fare clic sull'azione che elimina AppDisk.
7. Ripetere i passaggi 5 e 6 per ogni AppDisk.

**Aggiornamenti dei VDA:** l'aggiornamento della distribuzione non rileva se i VDA hanno i componenti AppDisk o PvD installati. Tuttavia, i programmi di installazione dei VDA lo fanno. Per ulteriori informazioni, vedere VDA con componenti PvD o AppDisks.

### Rimuovere gli elementi host non supportati

Un aggiornamento della distribuzione alla versione 2006 (o versione successiva supportata) non può continuare se il sito dispone di connessioni a tipi di host non supportati, ad esempio Citrix CloudPlatform o Microsoft Azure Classic. Completare le seguenti attività prima di tentare un aggiornamento.

Da Studio:

- Eliminare tutte le connessioni agli host non supportati.
- Se un gruppo di consegna contiene macchine di un catalogo creato con un'immagine master da un host non supportato, rimuovere tali macchine dal gruppo.
- Eliminare tutti i cataloghi creati utilizzando un'immagine master da un host non supportato.

### VDA con componenti PvD o AppDisks

Se i componenti che abilitano le tecnologie PvD e AppDisks sono installati su un VDA, tale VDA non può essere aggiornato fino a quando tali componenti non vengono rimossi.

> **Nota:**
>
> Durante l'aggiornamento alla versione 1912, è necessario disinstallare il VDA corrente e quindi installare il nuovo VDA. In questa versione, viene chiesto se si desidera che Citrix rimuova il componente e quindi continui l'aggiornamento.

I componenti AppDisk e PvD potrebbero essere stati installati nelle versioni precedenti dei VDA, anche se non tali tecnologie non son state mai utilizzate:

- Interfaccia grafica: nei programmi di installazione dei VDA, la pagina **Componenti aggiuntivi** conteneva l'opzione **Citrix AppDisk/Personal vDisk**. Nelle versioni 7.15 LTSR e 7.x precedenti questa opzione era attivata per impostazione predefinita. Quindi, se si accettavano le impostazioni predefinita (o si era abilitata esplicitamente l'opzione in qualsiasi versione che la offriva), quel componente veniva installato.
- CLI: specificando l'opzione `/baseimage`, il componente veniva installato.

**Cosa fare** Se il programma di installazione dei VDA non rileva i componenti AppDisks o PvD nel VDA attualmente installato, l'aggiornamento procede come di consueto.

Se il programma di installazione rileva componenti AppDisks o PvD nel VDA attualmente installato:

- Interfaccia grafica: l'aggiornamento va in pausa. Viene visualizzato un messaggio in cui si chiede se si desidera rimuovere automaticamente i componenti non supportati. Se si fa clic su **OK**, i componenti vengono rimossi automaticamente e l'aggiornamento procede.
- CLI: per evitare errori di comando, includere le seguenti opzioni nel comando:

- /remove_appdisk_ack
- /remove_pvd_ack

### Limiti

Agli aggiornamenti si applicano le seguenti limitazioni:

- **Installazione selettiva dei componenti:** se si installano o si aggiornano componenti nella nuova versione, ma si sceglie di non aggiornare altri componenti (su macchine diverse) che richiedono l'aggiornamento, Studio visualizza un promemoria. Ad esempio, supponiamo che un aggiornamento includa nuove versioni del controller e di Studio. Si aggiorna il controller ma non si esegue il programma di installazione sul computer in cui è installato Studio. Studio non consente di continuare a gestire il sito fino a quando non si aggiorna Studio.

  Non è necessario aggiornare i VDA, ma Citrix consiglia di aggiornare tutti i VDA per consentire l'utilizzo di tutte le funzionalità disponibili.
- **Versione anticipata o anteprima tecnologia:** non è possibile eseguire l'aggiornamento da una versione anticipata, un'anteprima tecnologica o una versione di anteprima.
- **Componenti su sistemi operativi precedenti:** non è possibile installare VDA correnti su sistemi operativi non più supportati da Microsoft o Citrix. Per ulteriori informazioni, vedere Sistemi operativi precedenti.
- **Ambienti/siti misti:** se è necessario continuare a eseguire siti di versioni precedenti e siti della versione corrente, vedere Considerazioni sull'ambiente misto.
- **Selezione di prodotti:** quando si esegue l'aggiornamento da una versione precedente, non si sceglie né si specifica il prodotto (Citrix Virtual Apps o Citrix Virtual Apps and Desktops) che è stato configurato durante l'installazione.

### Considerazioni sull'ambiente misto

Quando si esegue l'aggiornamento, Citrix consiglia di aggiornare tutti i componenti e i VDA in modo da poter accedere a tutte le funzionalità nuove e migliorate dell'edizione e della versione.

Ad esempio, sebbene sia possibile utilizzare i VDA correnti nelle distribuzioni contenenti versioni precedenti del controller, è possibile che le nuove funzionalità della versione corrente non siano disponibili. Possono verificarsi problemi di registrazione dei VDA anche quando si utilizzano versioni non correnti.

In alcuni ambienti potrebbe non essere possibile aggiornare tutti i VDA alla versione più recente. In tal caso, quando si crea un catalogo di macchine, è possibile specificare la versione VDA installata sui computer (questo è il cosiddetto livello funzionale). Per impostazione predefinita, questa impostazione

specifica la versione minima consigliata di VDA. Il valore predefinito è sufficiente per la maggior parte delle distribuzioni. Prendere in considerazione la possibilità di modificare l'impostazione indicando una versione precedente solo se il catalogo contiene VDA precedenti al valore predefinito. Non è consigliato far coesistere versioni diverse di VDA in un catalogo macchine.

Se viene creato un catalogo con l'impostazione della versione VDA minima predefinita e uno o più computer dispone di un VDA precedente alla versione predefinita, tali computer non potranno registrarsi con il controller e non funzioneranno.

Per ulteriori informazioni, vedere Versioni VDA e livelli funzionali.

#### Più siti con versioni diverse

Quando l'ambiente contiene siti con versioni di prodotto diverse (ad esempio, un sito XenDesktop 7.18 e un sito Citrix Virtual Apps and Desktops 1909), Citrix consiglia di utilizzare StoreFront per aggregare applicazioni e desktop di versioni diverse del prodotto. Per ulteriori informazioni, vedere la documentazione di StoreFront.

In un ambiente misto, continuare a utilizzare le versioni di Studio e Director per ciascuna versione, ma assicurarsi che le versioni diverse siano installate su computer separati.

### Sistemi operativi precedenti

Supponiamo che sia stata installata una versione precedente di un componente su un computer che eseguiva una versione del sistema operativo supportata. Ora, si intende utilizzare una versione più recente del componente, ma tale sistema operativo non è più supportato per la versione corrente del componente.

Si supponga, ad esempio, che sia stato installato un server VDA su un computer con Windows Server 2008 R2. Ora si desidera aggiornare tale VDA alla versione corrente, ma Windows Server 2008 R2 non è supportato nella versione corrente a cui si sta eseguendo l'aggiornamento.

Se si tenta di installare o aggiornare un componente in un sistema operativo non più consentito, viene visualizzato un messaggio di errore, ad esempio "Cannot be installed on this operating system"("Impossibile installare su questo sistema operativo").

Queste considerazioni si applicano all'aggiornamento delle versioni correnti e LTSR (Long Term Service Release). Non influiscono sull'applicazione di CU a una versione LTSR.

Seguire i collegamenti per scoprire quali sistemi operativi sono supportati:

- Citrix Virtual Apps and Desktops (versione corrente):
  - Delivery Controller, Studio, Director, VDA, Universal Print Server
  - Federated Authentication Service

  - Per StoreFront, Reimpostazione della password self-service e Registrazione della sessione, vedere l'articolo sui requisiti di sistema per la versione corrente.

- Per le LTSR, vedere gli elenchi dei componenti per la versione LTSR e il CU (selezionare la versione LTSR dalla pagina principale della documentazione del prodotto Citrix Virtual Apps and Desktops).

#### Sistemi operativi non validi

Nella tabella seguente sono elencati i sistemi operativi precedenti non validi per l'installazione/aggiornamento dei componenti nella versione corrente. Indica l'ultima versione valida del componente supportata per ogni sistema operativo elencato e la versione del componente in cui l'installazione e l'aggiornamento non sono più validi.

I sistemi operativi indicti nella tabella includono service pack e aggiornamenti.

| Sistema operativo | Componente/funzione | Ultima versione valida | Installazione/aggiornamento non possibile a partire dalla versione |
|---|---|---|---|
| Windows 7 e Windows 8 | VDA | 7.15 LTSR | 7.16 |
| Windows 7 e Windows 8 | Altri componenti del programma di installazione | 7.17 | 7.18 |
| Versioni di Windows 10 precedenti alla 1607 | VDA | 7.15 LTSR | 7.16 |
| Versione di Windows 10 x86 | VDA | 1906.2.0 | 1909 |
| Windows Server 2008 R2 | VDA | 7.15 LTSR | 7.16 |
| Windows Server 2008 R2 | Altri componenti del programma di installazione | 7.17 | 7.18 |
| Windows Server 2012 | VDA | 7.15 LTSR | 7.16 |
| Windows Server 2012 | Altri componenti del programma di installazione | 7.17 | 7.18 |
| Windows Server 2012 R2 | Altri componenti del programma di installazione* | 1912 LTSR | 2003 |

| Sistema operativo | Componente/funzione | Ultima versione valida | Installazione/aggiornamento non possibile a partire dalla versione |
|---|---|---|---|
| Windows Server 2012 R2 | VDI del server | 7.15 LTSR | 7.16 |

Windows XP e Windows Vista non sono validi per nessun componente o tecnologia 7.x.n

*Si applica a Delivery Controller, Studio, Director e VDA.

### Cosa si può fare

Sono disponibili delle scelte. È possibile effettuare le seguenti operazioni:

- Continuare a utilizzare il sistema operativo corrente
- Ricreare l'immagine della macchina o aggiornarla
- Aggiungere nuove macchine e quindi rimuovere quelle vecchie

**Continuare a utilizzare il sistema operativo corrente** Questi metodi sono fattibili per i VDA. Se si desidera continuare a utilizzare macchine con il sistema operativo precedente, è possibile scegliere una delle seguenti opzioni:

- Continuare a utilizzare la versione del componente installata.
- Scaricare la versione più recente valida del componente e quindi aggiornare il componente a tale versione (si presuppone che l'ultima versione valida del componente non sia già installata).

Ad esempio, si dispone di un VDA 7.14 su un computer con Windows 7 SP1. L'ultima versione di VDA valida sui sistemi operativi Windows 7 è XenApp e XenDesktop 7.15 LTSR. È possibile continuare a utilizzare 7.14 o scaricare un VDA LTSR 7.15 e quindi aggiornare il VDA a quella versione. Queste versioni di VDA precedenti funzionano in distribuzioni contenenti Delivery Controller con versioni più recenti. Ad esempio, un VDA LTSR 7.15 può connettersi a un controller Citrix Virtual Apps and Desktops 7 1808.

**Ricreare l'immagine della macchina o aggiornarla** Questi metodi sono fattibili per i VDA e per altre macchine che non dispongono di componenti di base (ad esempio Delivery Controller) installati. Scegliere una delle seguenti opzioni:

- Dopo aver messo il computer fuori servizio (attivando la modalità di manutenzione e consentendo la chiusura di tutte le sessioni), è possibile ricrearne l'immagine su una versione supportata del sistema operativo Windows e quindi installare la versione più recente del componente.

- Per aggiornare il sistema operativo senza ricreare l'immagine, disinstallare il software Citrix prima di aggiornare il sistema operativo, inclusi gli aggiornamenti interni al sistema operativo. Ad esempio, da Windows 10 versione 1903 a Windows 10 versione 1909. In caso contrario, il software Citrix sarà in uno stato non supportato. Installare quindi il nuovo componente.
- Per aggiornare il sistema operativo in una macchina VDA senza creare una nuova immagine, è necessario innanzitutto installare una versione del VDA supportata nel sistema operativo a cui si sta effettuando l'aggiornamento o aggiornare il VDA dopo l'aggiornamento del sistema operativo. In caso contrario, il software Citrix sarà in uno stato non supportato.

**Aggiungere nuove macchine e quindi rimuovere quelle vecchie** Questo metodo può essere utilizzato se è necessario aggiornare il sistema operativo su macchine contenenti un Delivery Controller o un altro componente principale.

Citrix raccomanda che tutti i controller di un sito abbiano lo stesso sistema operativo. La seguente sequenza di aggiornamento riduce al minimo l'intervallo quando diversi controller hanno diversi sistemi operativi.

1. Eseguire una snapshot di tutti i Delivery Controller presenti nel sito e quindi eseguire il backup del database del sito.
2. Installare nuovi Delivery Controller su server puliti con sistemi operativi supportati. Ad esempio, installare un Controller su due computer Windows Server 2016.
3. Aggiungere i nuovi Controller al sito.
4. Rimuovere i Controller in esecuzione su sistemi operativi non validi per la versione corrente. Ad esempio, rimuovere due Controller su due computer Windows Server 2008 R2. Seguire i consigli per rimuovere i controller in Delivery Controller.

## Preparazione

Prima di iniziare un aggiornamento, esaminare le informazioni riportate di seguito e completare le attività necessarie.

> **Nota:**
>
> Sebbene l'aggiornamento dei VDA avvenga successivamente nella sequenza di aggiornamento, è consigliabile scegliere un programma di installazione e rivedere la procedura prima di iniziare l'aggiornamento, in modo da sapere cosa aspettarsi.

### Scegliere un programma di installazione e un'interfaccia

Utilizzare il programma di installazione completo dell'ISO del prodotto per aggiornare i componenti. È possibile aggiornare i VDA utilizzando il programma di installazione del prodotto intero o uno dei

programmi di installazione VDA autonomi. Tutti i programmi di installazione offrono la possibilità di utilizzare l'interfaccia grafica o la riga di comando.

Per ulteriori informazioni, vedere Programmi di installazione.

**Dettagli dell'installazione:** dopo aver completato qualsiasi lavoro di preparazione e quando si è pronti per avviare il programma di installazione, l'articolo sull'installazione mostra cosa sarà visualizzato (se si utilizza l'interfaccia grafica) o cosa digitare (se si utilizza la riga di comando).

- Installare/aggiornare i componenti principali utilizzando l'interfaccia grafica
- Installare/aggiornare i componenti principali utilizzando la riga di comando
- Installare/aggiornare i VDA utilizzando l'interfaccia grafica
- Installare/aggiornare i VDA utilizzando la riga di comando

Se è stato originariamente installato un VDA a sessione singola con il programma di installazione `VDAWorkstationCoreSetup.exe`, Citrix consiglia di utilizzare quello per aggiornarlo. Se si utilizza il programma di installazione dell'intero VDA o il programma di installazione `VDAWorkstationSetup.exe` per aggiornare il VDA, i componenti originariamente esclusi potrebbero essere installati, a meno che non vengano espressamente omessi o esclusi dall'aggiornamento.

Quando si aggiorna un VDA alla versione corrente, vi sarà un riavvio del computer durante il processo di aggiornamento. Questo requisito è iniziato con la versione 7.17 e non può essere evitato. L'aggiornamento riprende automaticamente dopo il riavvio (a meno che non venga specificato `/noresume` nella riga di comando).

#### Azioni riguardanti i database

Eseguire il backup dei database di registrazione del sito, di monitoraggio e di configurazione. Seguire le istruzioni in CTX135207. Se vengono rilevati problemi dopo l'aggiornamento, è possibile ripristinare il backup.

Per informazioni sull'aggiornamento delle versioni di SQL Server non più supportate, vedere Controllo della versione di SQL Server. Questo si riferisce a SQL Server utilizzato per i database di registrazione del sito, del monitoraggio e della configurazione.

Microsoft SQL Server Express LocalDB viene installato automaticamente, per l'utilizzo con la cache host locale. Se è necessario sostituire una versione precedente, la nuova versione deve essere SQL Server Express LocalDB 2019. Per informazioni dettagliate sulla sostituzione di SQL Server Express LocalDB con una nuova versione dopo l'aggiornamento dei componenti e del sito, vedere Sostituire SQL Server Express LocalDB.

#### Assicurarsi che le proprie licenze Citrix siano aggiornate

Per una panoramica completa della gestione delle licenze Citrix, vedere Attivare, aggiornare e gestire le licenze Citrix.

È possibile utilizzare il programma di installazione completo del prodotto per aggiornare License Server. In alternativa, è possibile scaricare e aggiornare i componenti della licenza separatamente. Vedere Eseguire l'aggiornamento.

Prima di eseguire l'aggiornamento, assicurarsi che la data di Customer Success Services/Software Maintenance/Subscription Advantage sia valida per la nuova versione del prodotto. La data deve essere almeno 2021.11.15.

#### Assicurarsi che la propria versione di Citrix License Server sia compatibile

Assicurarsi che Citrix License Server sia compatibile con la nuova versione. Ci sono due modi per farlo:

- Prima di aggiornare qualsiasi altro componente Citrix, eseguire il programma di installazione `XenDesktopServerSetup.exe` dal layout ISO sulla macchina contenente un Delivery Controller. In caso di problemi di incompatibilità, il programma di installazione lo segnala insieme ai passaggi consigliati per risolvere i problemi.
- Dalla directory `XenDesktop Setup` del supporto, eseguire il comando `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`. Il display indica se il License Server è compatibile. Se il License Server non è compatibile, aggiornarlo.

#### Eseguire il backup di eventuali modifiche di StoreFront

Prima di iniziare un aggiornamento, se sono state apportate modifiche ai file contenuti in `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`, ad esempio *default.ica* e *usernamepassword.tfrm*, eseguirne il backup per ciascuno store. Dopo l'aggiornamento è possibile ripristinarli per reintegrare le modifiche.

#### Chiudere applicazioni e console

Prima di avviare un aggiornamento, chiudere tutti i programmi che potrebbero causare blocchi di file, incluse le console di amministrazione e le sessioni di PowerShell.

Il riavvio del computer garantisce che tutti i blocchi di file vengano cancellati e che non vi siano aggiornamenti di Windows in sospeso.

Prima di avviare un aggiornamento, arrestare e disattivare qualsiasi servizio agente di monitoraggio di terze parti.

#### Assicurarsi di disporre delle autorizzazioni appropriate

Oltre ad essere un utente di dominio, è necessario essere un amministratore locale dei computer in cui si stanno aggiornando i componenti del prodotto.

Il database del sito e il sito possono essere aggiornati automaticamente o manualmente. Per un aggiornamento automatico del database, le autorizzazioni dell'utente di Studio devono includere la possibilità di aggiornare lo schema del database di SQL Server (ad esempio, il ruolo database di `db_securityadmin` o `db_owner`). Per ulteriori informazioni, vedere Database.

Se l'utente di Studio non dispone di tali autorizzazioni, l'avvio di un aggiornamento manuale del database genera script. L'utente di Studio esegue alcuni script da Studio. L'amministratore del database esegue altri script, utilizzando uno strumento come SQL Server Management Studio.

#### Altre attività di preparazione

- Eseguire il backup dei modelli e aggiornare gli hypervisor, se necessario
- Completare qualsiasi altra attività di preparazione dettata dal piano di continuità aziendale.

### Test preliminari sul sito

Quando si aggiornano i Delivery Controller e un sito, i test preliminari del sito vengono eseguiti prima dell'effettivo inizio dell'aggiornamento. Questi test verificano che:

- Il database del sito possa essere raggiunto e che ne sia stato eseguito il backup
- Le connessioni ai servizi Citrix essenziali funzionino correttamente
- L'indirizzo di Citrix License Server sia disponibile
- Sia possibile raggiungere il database di registrazione della configurazione
- Assicurarsi di avere una licenza Hybrid Rights se si intende aggiungere connessioni a host cloud pubblici (ad esempio, AWS). In caso contrario, il test preliminare del sito si interrompe o si arresta e viene visualizzato un messaggio esplicativo.

Dopo l'esecuzione dei test, è possibile visualizzare un report dei risultati. È quindi possibile correggere eventuali problemi rilevati ed eseguire nuovamente i test. La mancata esecuzione dei test preliminari del sito e della successiva risoluzione di eventuali problemi può influire sul funzionamento del sito.

Il report contenente i risultati del test è un file HTML (`PreliminarySiteTestResult.html`) nella stessa directory dei registri di installazione. Tale file viene creato se non esiste. Se il file esiste, il suo contenuto viene sovrascritto.

#### Eseguire i test

- Quando si utilizza l'interfaccia grafica del programma di installazione per eseguire l'aggiornamento, la procedura guidata include una pagina in cui è possibile avviare i test e quindi visualizzare il report. Dopo aver eseguito i test, visualizzato il report e risolto eventuali problemi rilevati, è possibile eseguire nuovamente i test. Al termine dei test, fare clic su Avanti per continuare la procedura guidata.
- Quando si utilizza l'interfaccia della riga di comando per eseguire l'aggiornamento, i test vengono eseguiti automaticamente. Per impostazione predefinita, se un test non riesce, l'aggiornamento non viene eseguito. Dopo aver visualizzato il report e aver risolto i problemi, eseguire nuovamente il comando.

Citrix consiglia di eseguire sempre i test preliminari del sito e risolvere eventuali problemi prima di continuare l'aggiornamento del controller e del sito. Il potenziale beneficio giustifica ampiamente il tempo impiegato per la riesecuzione dei test. Tuttavia, è possibile ignorare questa azione consigliata.

- Quando si esegue l'aggiornamento con l'interfaccia grafica, è possibile scegliere di saltare i test e continuare il processo di aggiornamento.
- Quando si esegue l'aggiornamento dalla riga di comando, non è possibile saltare i test. Per impostazione predefinita, un test del sito non riuscito fa chiudere il programma di installazione senza eseguire l'aggiornamento. Nella maggior parte dei casi, se si include l'opzione `/ignore_site_test_failure`, eventuali test non riusciti vengono ignorati e l'aggiornamento procede (vedere Controllo della versione di SQL Server per le eccezioni).

#### Quando si aggiornano più controller

Quando si avvia un aggiornamento su un controller e quindi si avvia un aggiornamento di un altro controller che si trova nello stesso sito (prima del completamento del primo aggiornamento):

- Se i test preliminari del sito sono stati completati sul primo controller, la pagina dei test preliminari del sito non viene visualizzata nella procedura guidata dell'altro controller.
- Se i test del primo controller sono in corso quando si avvia l'aggiornamento dell'altro controller, la pagina dei test del sito viene visualizzata nella procedura guidata dell'altro controller. Tuttavia, se i test del primo controller terminano, vengono conservati solo i risultati del test del primo controller.

#### Errori di test non correlati allo stato di salute del sito

- Se i test preliminari del sito non riescono per un problema di memoria insufficiente, rendere disponibile più memoria e quindi eseguire nuovamente i test.

- Se si dispone dell'autorizzazione per l'aggiornamento, ma non per eseguire test del sito, i test preliminari del sito non riescono. Per risolvere il problema, eseguire nuovamente il programma di installazione con un account utente che disponga dell'autorizzazione per eseguire i test.

### Controllo della versione di SQL Server

Una distribuzione corretta di Citrix Virtual Apps and Desktops richiede una versione supportata di Microsoft SQL Server per i database di registrazione del sito, del monitoraggio e della configurazione. L'aggiornamento di una distribuzione Citrix con una versione di SQL Server non più supportata può causare problemi di funzionalità e il sito non sarà supportato.

Per informazioni su quali versioni di SQL Server sono supportate per la versione Citrix a cui si sta eseguendo l'aggiornamento, vedere l'articolo Requisiti di sistema relativo a tale versione.

Durante l'aggiornamento di un Controller, il programma di installazione di Citrix verifica la versione di SQL Server attualmente installata utilizzata per i database di registrazione del sito, del monitoraggio e della configurazione.

- Se la verifica determina che la versione di SQL Server attualmente installata non è una versione supportata nella versione Citrix a cui si sta eseguendo l'aggiornamento:

  - Interfaccia grafica: l'aggiornamento si ferma e viene visualizzato un messaggio. Fare clic su **Accetto** e quindi su **Annulla** per chiudere il programma di installazione Citrix. Non è possibile procedere all'aggiornamento.
  - Interfaccia della riga di comando: il comando non riesce (anche se il comando includeva l'opzione /`ignore_db_check_failure`).

  Aggiornare la versione di SQL Server e quindi avviare nuovamente l'aggiornamento Citrix.

- Se la verifica non è in grado di determinare quale versione di SQL Server è attualmente installata, verificare se la versione attualmente installata è supportata nella versione a cui si sta eseguendo l'aggiornamento (Requisiti di sistema).

  - Interfaccia grafica: l'aggiornamento si ferma e viene visualizzato un messaggio.

    * Se la versione di SQL Server attualmente installata è supportata, fare clic su **Accetto** per chiudere il messaggio e quindi su **Avanti** per continuare l'aggiornamento Citrix.
    * Se la versione di SQL Server attualmente installata non è supportata, fare clic su **Accetto** per chiudere il messaggio e quindi fare clic su **Annulla** per terminare l'aggiornamento Citrix. Aggiornare SQL Server a una versione supportata e quindi avviare nuovamente l'aggiornamento Citrix.

  - Interfaccia della riga di comando: il comando non riesce e viene visualizzato un messaggio. Dopo aver chiuso il messaggio:

    * Se la versione di SQL Server attualmente installata è supportata, eseguire nuovamente il comando con l'opzione `/ignore_db_check_failure`.
    * Se la versione di SQL Server attualmente installata non è supportata, aggiornare SQL Server a una versione supportata. Eseguire nuovamente il comando per avviare l'aggiornamento Citrix.

#### Aggiornamento di SQL Server

Se si aggiungono nuovi server SQL Server e si esegue la migrazione del database del sito, è necessario aggiornare le stringhe di connessione.

Se il sito utilizza attualmente SQL Server Express per il database del sito (che Citrix ha installato automaticamente durante la creazione del sito):

1. Installare la versione più recente di SQL Server Express.
2. Scollegare il database.
3. Collegare il database al nuovo SQL Server Express.
4. Effettuare la migrazione delle stringhe di connessione.

Per ulteriori informazioni, vedere Configurazione delle stringhe di connessione e la documentazione del prodotto Microsoft SQL Server.

### Sostituzione di SQL Server Express LocalDB

Microsoft SQL Server Express LocalDB è una funzionalità di SQL Server Express utilizzata dalla cache host locale in modo autonomo. La cache host locale non richiede componenti di SQL Server Express diversi da SQL Server Express LocalDB.

Se è stata installata una versione di Delivery Controller precedente alla 1912 e quindi si aggiorna la distribuzione alla versione 1912 o successiva, Citrix non aggiorna automaticamente la versione di SQL Server Express LocalDB. Perché no? Perché potrebbero essere presenti componenti non Citrix che fanno affidamento su SQL Server Express LocalDB. Se si dispone di componenti non Citrix che utilizzano SQL Server Express LocalDB, assicurarsi che l'aggiornamento di SQL Server Express LocalDB non interferisca con tali componenti. Per aggiornare (sostituire) la versione di SQL Server Express LocalDB, seguire le istruzioni riportate in questa sezione.

- **Quando si aggiornano i Delivery Controller a Citrix Virtual Apps and Desktops versione 1912 o 2003:** l'aggiornamento di SQL Server Express LocalDB è facoltativo. La cache host locale funziona correttamente, senza perdita di funzionalità, indipendentemente dal fatto che si aggiorni o meno SQL Server Express LocalDB. È stata aggiunta la possibilità di passare a una versione più recente di SQL Server Express LocalDB in caso di timori sulla fine del supporto da parte di Microsoft per SQL Server Express LocalDB 2014.

- **Quando si aggiornano i Delivery Controller a versioni più recenti del 2003 di Citrix Virtual Apps and Desktops:** la versione supportata è SQL Server Express LocalDB 2019. Se è stato originariamente installato un Delivery Controller precedente alla versione 1912 e da allora SQL Server Express LocalDB non è stato sostituito con la versione più recente, è necessario sostituire il software del database a questo punto. In caso contrario, la cache host locale non funzionerà.

Cosa occorre:

- Il supporto di installazione di Citrix Virtual Apps and Desktops (per la versione a cui si è eseguito l'aggiornamento). Il supporto contiene una copia di Microsoft SQL Server Express LocalDB 2019.
- Uno strumento Sysinternals di Windows scaricabile da Microsoft.

Procedura:

1. Completare l'aggiornamento dei componenti, dei database e del sito Citrix Virtual Apps and Desktops. Tali aggiornamenti del database influiscono sui database di registrazione del sito, del monitoraggio e della configurazione. Non influiscono sul database della cache host locale che utilizza SQL Server Express LocalDB.
2. Sul Delivery Controller, scaricare `PsExec` da Microsoft. Vedere il documento Microsoft PsExec v2.2.
3. Arrestare il servizio Citrix High Availability.
4. Dal prompt dei comandi eseguire `PsExec` e passare all'account Servizio di rete.

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE"cmd
   ```

   Facoltativamente, è possibile utilizzare `whoami` per verificare che il prompt dei comandi sia in esecuzione come account del servizio di rete.

   ```
   whoami
   ```

   ```
   nt authority\networkservice
   ```

5. Spostarsi nella cartella contenente SqlLocalDB.

   ```
   cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
   ```

6. Arrestare ed eliminare `CitrixHA` (LocalDB).

   ```
   SqlLocalDB stop CitrixHA
   ```

   ```
   SqlLocalDB delete CitrixHA
   ```

7. Rimuovere i file correlati in `C:\Windows\ServiceProfiles\NetworkService`.

   ```
   HADatabaseName.*
   HADatabaseName_log.*
   HAImportDatabaseName.*
   HAImportDatabaseName_log.*
   <!--NeedCopy-->
   ```

Suggerimento: la distribuzione potrebbe non avere `HAImportDatabaseName.*` e `HAImportDatabaseName_log.*`

8. Disinstallare SQL Server Express LocalDB 2014 dal server, utilizzando la funzionalità di Windows per la rimozione di programmi.
9. Installare SQL Server Express LocalDB 2019. Nella cartella `Support > SQLLocalDB` del supporto di installazione di Citrix Virtual Apps and Desktops, fare doppio clic su `sqllocaldb.msi`. Per completare l'installazione potrebbe essere richiesto un riavvio. Il nuovo SQLLocalDB risiede in `C:\Program Files\Microsoft SQL Server\150\Tools\Binn`.
10. Avviare il servizio Citrix High Availability.
11. Assicurarsi che il database della cache host locale sia stato creato su ogni Delivery Controller. Ciò conferma che il servizio High Availability (broker secondario) può subentrare, se necessario.
    - Nel server del Controller, passare a `C:\Windows\ServiceProfiles\NetworkService`.
    - Verificare che vengano creati `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf`.

## Sicurezza

January 7, 2024

Citrix Virtual Apps and Desktops offre una soluzione progettata per essere sicura che consente di personalizzare l'ambiente in base alle proprie esigenze di sicurezza.

Un problema di sicurezza che l'IT deve affrontare con i lavoratori mobili è la perdita o il furto dei dati. Grazie all'hosting di applicazioni e desktop, Citrix Virtual Apps and Desktops separa in modo sicuro i dati sensibili e la proprietà intellettuale dai dispositivi endpoint conservando tutti i dati in un centro dati. Quando sono abilitati criteri che consentono il trasferimento dei dati, tutti i dati vengono crittografati.

I centri dati Citrix Virtual Apps and Desktops semplificano inoltre la risposta agli incidenti con un servizio centralizzato di monitoraggio e gestione. Director consente all'IT di monitorare e analizzare i dati a cui si accede in tutta la rete, mentre Studio consente all'IT di applicare patch e correggere la maggior parte delle vulnerabilità nel centro dati anziché risolvere i problemi localmente su ciascuno dei dispositivi degli utenti finali.

Citrix Virtual Apps and Desktops semplifica inoltre gli audit e la conformità alle normative, poiché gli addetti alle indagini possono utilizzare un audit trail centralizzato per determinare chi ha effettuato l'

accesso ad applicazioni e dati. Director raccoglie i dati storici relativi agli aggiornamenti del sistema e all'utilizzo dei dati utente accedendo ai log di configurazione e all'API OData.

L'amministrazione delegata consente di impostare i ruoli di amministratore per controllare l'accesso a Citrix Virtual Apps and Desktops a livello granulare. Ciò consente all'organizzazione di offrire a determinati amministratori l'accesso completo alle attività, alle operazioni e agli ambiti, mentre altri amministratori hanno accesso limitato.

Citrix Virtual Apps and Desktops offre agli amministratori un controllo granulare sugli utenti applicando criteri a diversi livelli della rete, dal livello locale al livello di unità organizzativa. Questo controllo dei criteri determina se un utente, un dispositivo o un gruppo di utenti e dispositivi possono connettersi, stampare, copiare/incollare o mappare unità locali, in modo da ridurre al minimo i problemi di sicurezza relativi ai lavoratori temporanei di terze parti. Gli amministratori possono inoltre utilizzare la funzione Desktop Lock in modo che gli utenti finali possano utilizzare solo il desktop virtuale, impedendo qualsiasi accesso al sistema operativo locale del dispositivo dell'utente finale.

Gli amministratori possono aumentare la sicurezza su Citrix Virtual Apps o Citrix Virtual Desktops configurando il Sito per utilizzare il protocollo TLS (Transport Layer Security) del Controller o tra utenti finali e Virtual Delivery Agent (VDA). Il protocollo può anche essere abilitato in un sito per fornire autenticazione server, crittografia del flusso di dati e controlli di integrità dei messaggi per una connessione TCP/IP.

Citrix Virtual Apps and Desktops supporta inoltre l'autenticazione a più fattori per Windows o per un'applicazione specifica. L'autenticazione a più fattori può essere utilizzata anche per gestire tutte le risorse fornite da Citrix Virtual Apps and Desktops. Questi metodi includono:

- Token
- Smart card
- RADIUS
- Kerberos
- Biometria

Citrix Virtual Desktops può essere integrato con molte soluzioni di sicurezza di terze parti, dalla gestione delle identità al software antivirus. Un elenco dei prodotti supportati è disponibile all'indirizzo http://www.citrix.com/ready.

Alcune versioni di Citrix Virtual Apps and Desktops sono certificate per lo standard Common Criteria. Per un elenco di tali standard, vedere https://www.commoncriteriaportal.org/cc/.

## Autenticazione FIDO2 e WebAuthn

January 7, 2024

## Autorizzazione locale e autenticazione virtuale tramite FIDO2 e WebAuthn

Gli utenti possono autenticarsi alle applicazioni che sfruttano FIDO2 o WebAuthn nella loro sessione virtuale utilizzando chiavi di sicurezza FIDO2 e dispositivi biometrici integrati con TPM 2.0 e Windows Hello.

Per ulteriori informazioni su FIDO2, vedere FIDO2: WebAuthn & CTAP.

Per informazioni sull'utilizzo di questa funzione, vedere FIDO2 redirection.

> **NOTA**
>
> Tenere presente che questa funzionalità non supporta l'accesso alla sessione virtuale utilizzando WebAuthn o FIDO2. Questa funzionalità consente di utilizzare questi metodi di autenticazione solo nelle applicazioni all'interno della sessione virtuale.
>
> Questa funzionalità non è supportata negli scenari a doppio hop.

## Matrice di supportabilità

| Sistema operativo host della sessione | Autenticazione delle applicazioni Web | Autenticazione delle applicazioni UWP |
|---|---|---|
| Windows Server 2016 | Supportato tramite reindirizzamento USB | Non supportato |
| Windows Server 2019 | Supportata | Non supportato |
| Windows Server 2022 | Supportata | Supportata |
| Windows 10 | Supportata | Supportata |
| Windows 11 | Supportata | Supportata |

Per ulteriori informazioni, leggere i requisiti riportati di seguito.

## Autenticazione delle applicazioni Web

### Requisiti

Di seguito sono riportati i requisiti per l'utilizzo dell'autenticazione FIDO2 e WebAuthn con le applicazioni Web:

#### Piano di controllo Citrix

- Citrix Virtual Apps and Desktops 2009 o versioni successive

**Host della sessione**

- Sistema operativo
  - Windows 10 1809 o versione successiva
  - Windows Server 2019 o versione successiva
- VDA
  - Windows: versione 2009 o successiva

**Dispositivo client**

- Sistema operativo
  - Windows 10 1809 o versione successiva
  - Linux: fare riferimento all'app Workspace per i requisiti di sistema Linux
- App Workspace
  - Windows: versione 2009.1 o successiva
  - Linux: versione 2303 o successiva

**Requisiti del browser Web**

- Solo browser a 64 bit

**Metodi di autenticazione supportati**

- Chiave di sicurezza FIDO2
- Windows Hello
  - TPM 2.0
  - Biometria integrata
    - Riconoscimento facciale
    - Scanner per impronte digitali
  - WebAuthn

## Autenticazione delle applicazioni UWP

Con il rilascio di Citrix Virtual Apps and Desktops 2112, Citrix supporta l'autenticazione WebAuthn e FIDO2 nelle applicazioni UWP.

Applicazioni come Microsoft Teams, Microsoft Outlook per Office 365 e OneDrive utilizzano un'applicazione UWP per l'autenticazione come collegamento ad Azure Active Directory. Citrix ora supporta l'utilizzo di FIDO2 per autenticare tali applicazioni.

### Requisiti

Di seguito sono riportati i requisiti per l'utilizzo dell'autenticazione FIDO2 e WebAuthn con le applicazioni UWP:

#### Piano di controllo Citrix

- Citrix Virtual Apps and Desktops 2112 o versioni successive

#### Host della sessione

- Sistema operativo
  - Windows 10 1809 o versione successiva
  - Windows Server 2022 o versione successiva
- VDA
  - Windows: versione 2112 o successiva

#### Dispositivo client

- Sistema operativo
  - Windows 10 1809 o versione successiva
  - Linux: fare riferimento all'app Workspace per i requisiti di sistema Linux
- App Workspace
  - Windows: versione 2009.1 o successiva
  - Linux: versione 2303 o successiva

#### Metodi di autenticazione supportati

- Chiave di sicurezza FIDO2
- Windows Hello
  - TPM 2.0
  - Biometria integrata
    - Riconoscimento facciale
    - Scanner per impronte digitali
  - WebAuthn

> **Nota:**
>
> Negli scenari in cui il reindirizzamento FIDO2 non è disponibile perché la funzionalità non è supportata dal client o dal VDA o dal sistema operativo, le chiavi FIDO2 basate su USB possono essere reindirizzate utilizzando il reindirizzamento USB.
> È anche possibile utilizzare il reindirizzamento USB per reindirizzare le chiavi FIDO2 basate su USB in scenari in cui è disponibile il reindirizzamento FIDO2. In questo caso, è necessario disabilitare il reindirizzamento FIDO2 e configurare le regole di reindirizzamento USB appropriate.
> Consultare la documentazione sulle regole del dispositivo di reindirizzamento USB per informazioni dettagliate su come configurare le regole di reindirizzamento USB.

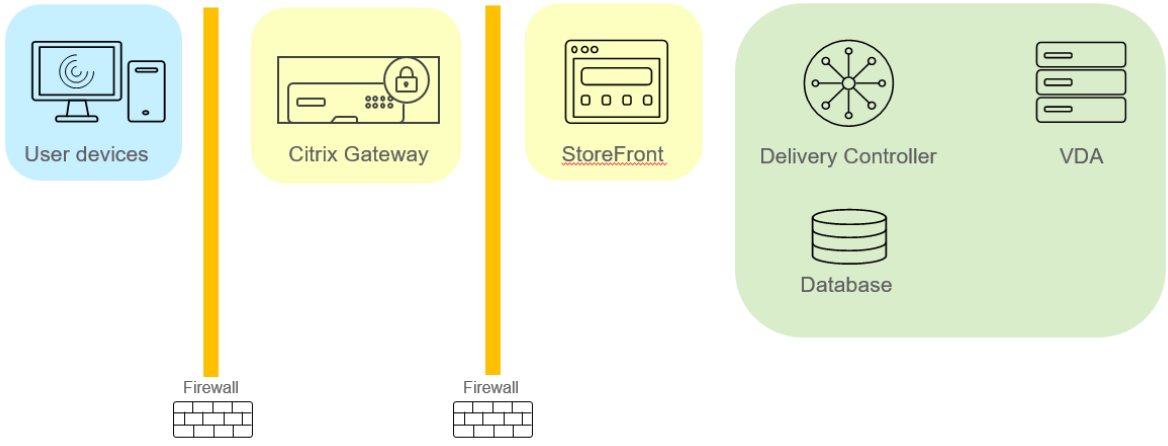
## Integrazione di Citrix Virtual Apps and Desktops con Citrix Gateway

January 7, 2024

I server StoreFront vengono distribuiti e configurati per gestire l'accesso alle risorse e ai dati pubblicati. Per l'accesso remoto, si consiglia di aggiungere Citrix Gateway davanti a StoreFront.

> **Nota:**
>
> Per la procedura di configurazione dettagliata per l'integrazione di Citrix Virtual Apps and Desktops con Citrix Gateway, vedere la documentazione di StoreFront.

Nel diagramma seguente viene illustrato un esempio di distribuzione Citrix semplificata che include Citrix Gateway. Citrix Gateway comunica con StoreFront per proteggere le app e i dati forniti da Citrix Virtual Apps and Desktops. I dispositivi utente eseguono l'app Citrix Workspace per creare una connessione sicura e accedere alle app, ai desktop e ai file.



Gli utenti accedono e si autenticano utilizzando Citrix Gateway. Citrix Gateway viene distribuito e protetto nel DMZ. È configurata l'autenticazione a due fattori. In base alle loro credenziali, agli utenti vengono fornite le risorse e le applicazioni pertinenti. Le applicazioni e i dati si trovano su server appropriati (non visualizzati nel diagramma). Server separati utilizzati per applicazioni e dati sensibili che necessitano di protezione.

## Considerazioni sulla sicurezza e procedure consigliate

January 7, 2024

> **Nota:**
>
> L'organizzazione potrebbe dover soddisfare standard di sicurezza specifici per soddisfare i requisiti normativi. Questo documento non copre questo argomento, perché tali norme di sicurezza cambiano nel tempo. Per informazioni aggiornate sugli standard di sicurezza e sui prodotti Citrix, vedere http://www.citrix.com/security/.

### Procedure consigliate per la sicurezza

Tenere aggiornati tutti i computer dell'ambiente con le patch di sicurezza. Un vantaggio è che è possibile utilizzare i thin client come terminali, il che semplifica questo compito.

Proteggere tutte le macchine del proprio ambiente con software antivirus.

Prendere in considerazione l'utilizzo di software antimalware specifico per la piattaforma.

Quando si installa il software, installarlo nei percorsi predefiniti forniti.

- Se si installa il software in una posizione di file diversa dal percorso predefinito fornito, valutare la possibilità di aggiungere al percorso del file ulteriori misure di sicurezza, quali autorizzazioni limitate.

Tutte le comunicazioni di rete devono essere adeguatamente protette e crittografate in conformità con i criteri di sicurezza. È possibile proteggere tutte le comunicazioni tra i computer con Microsoft Windows utilizzando IPSec. Per ulteriori informazioni su come eseguire questa operazione, vedere la documentazione del sistema operativo. Inoltre, la comunicazione tra dispositivi utente e desktop è protetta tramite Citrix SecureICA, che è configurato per impostazione predefinita per la crittografia a 128 bit. È possibile configurare SecureICA durante la creazione o l'aggiornamento di un gruppo di consegna.

> **Nota:**
>
> Citrix SecureICA fa parte del protocollo ICA/HDX ma non è un protocollo di sicurezza di rete conforme agli standard come Transport Layer Security (TLS). È inoltre possibile proteggere le comunicazioni di rete tra dispositivi utente e desktop utilizzando TLS. Per configurare TLS, vedere Transport Layer Security (TLS).

Applicare le procedure consigliate di Windows per la gestione degli account. Non creare un account su un modello o un'immagine prima che venga duplicato da Machine Creation Services o Provisioning Services. Non pianificare le attività utilizzando account di dominio con privilegi archiviati. Non creare manualmente account computer di Active Directory condivisi. Queste pratiche aiuteranno a impedire a un attacco mediante computer di ottenere password di account persistenti locali e quindi utilizzarle per accedere a immagini condivise MCS/PVS appartenenti ad altri utenti.

### Firewall

Proteggere tutte le macchine del proprio ambiente con firewall perimetrali, anche ai confini delle enclave, a seconda dei casi.

Tutte le macchine dell'ambiente devono essere protette da un firewall personale. Quando si installano componenti di base e i VDA, è possibile decidere che le porte necessarie per la comunicazione di componenti e funzionalità vengano automaticamente aperte se viene rilevato il servizio Windows Firewall (anche se il firewall non è abilitato). È inoltre possibile scegliere di configurare manualmente tali porte firewall. Se si utilizza un firewall diverso, è necessario configurarlo manualmente.

Se si esegue la migrazione di un ambiente convenzionale a questa release, potrebbe essere necessario riposizionare un firewall perimetrale esistente o aggiungere nuovi firewall perimetrali. Supponiamo, ad esempio, che vi sia un firewall perimetrale tra un client convenzionale e un server database ubicato nel centro dati. Quando si utilizza questa versione, il firewall perimetrale deve essere posizionato in modo che il desktop virtuale e il dispositivo utente si trovino su un lato e i server del database e i controller di consegna nel data center si trovino dall'altro lato. Pertanto, è consigliabile creare un'enclave all'interno del data center per contenere i server di database e i controller. Prendere inoltre in considerazione di predisporre protezione tra il dispositivo utente e il desktop virtuale.

> **Nota:**
>
> Le porte TCP 1494 e 2598 vengono utilizzate per ICA e CGP ed è pertanto probabile che siano aperte in corrispondenza dei firewall in modo che gli utenti esterni al data center possano accedervi. Citrix consiglia di non utilizzare queste porte per qualsiasi altra cosa, per evitare la possibilità di lasciare inavvertitamente aperte agli attacchi delle interfacce amministrative. Le porte 1494 e 2598 sono ufficialmente registrate presso la Internet Assigned Number Authority (http://www.iana.org/).

**Sicurezza delle applicazioni**

Per impedire agli utenti non amministratori di eseguire azioni dannose, è consigliabile configurare le regole di Windows AppLocker per programmi di installazione, applicazioni, eseguibili e script sull'host VDA e sul client Windows locale.

## Gestire i privilegi utente

Concedere agli utenti solo le funzionalità di cui hanno bisogno. I privilegi di Microsoft Windows continuano ad essere applicati ai desktop nel modo consueto: configurare i privilegi tramite Assegnazione diritti utente e le appartenenze ai gruppi tramite Criteri di gruppo. Un vantaggio di questa versione è che è possibile concedere a un utente diritti amministrativi su un desktop senza concedere anche il controllo fisico sul computer su cui è memorizzato il desktop.

Quando si pianificano i privilegi dei desktop, tenere presente quanto segue:

- Per impostazione predefinita, quando gli utenti non privilegiati si connettono a un desktop, vedono il fuso orario del sistema che esegue il desktop anziché il fuso orario del proprio dispositivo utente. Per informazioni su come consentire agli utenti di visualizzare l'ora locale durante l'utilizzo dei desktop, vedere l'articolo Gestire i gruppi di consegna.
- Un utente che è amministratore di un desktop ha il controllo completo su tale desktop. Se un desktop è in pool anziché dedicato, l'utente deve essere attendibile rispetto a tutti gli altri utenti del desktop, inclusi gli utenti futuri. Tutti gli utenti del desktop devono essere consapevoli del potenziale rischio permanente per la sicurezza dei loro dati presentato da questa situazione. Questa considerazione non si applica ai desktop dedicati, che hanno un solo utente; tale utente non deve essere amministratore su nessun altro desktop.
- Un utente amministratore di un desktop in genere può installare software su quel desktop, incluso software potenzialmente dannoso. L'utente può inoltre monitorare o controllare il traffico su qualsiasi rete connessa al desktop.

## Gestire i diritti di accesso

I diritti di accesso sono necessari sia per gli account utente che per gli account computer. Come per i privilegi di Microsoft Windows, i diritti di accesso continuano ad essere applicati ai desktop nel modo consueto: configurare i diritti di accesso tramite Assegnazione diritti utente e le appartenenze ai gruppi tramite Criteri di gruppo.

I diritti di accesso a Windows sono: accedere locale, accesso tramite Servizi Desktop remoto, accesso in rete (accesso al computer dalla rete), accesso come processo batch e accesso come servizio.

Per gli account computer, concedere ai computer solo i diritti di accesso necessari. È richiesto il diritto di accesso "Accedi al computer dalla rete":

- In corrispondenza dei VDA, per gli account computer dei Delivery Controller
- In corrispondenza dei Delivery Controller, per gli account computer dei VDA. Vedere Individuazione controller basata su unità organizzativa di Active Directory.
- Nei server StoreFront, per gli account computer di altri server che appartengono allo stesso gruppo di server StoreFront

Per gli account utente, concedere agli utenti solo i diritti di accesso necessari.

Secondo Microsoft, per impostazione predefinita al gruppo Utenti Desktop remoto viene concesso il diritto di accesso "Consenti accesso tramite Servizi Desktop remoto"(ad eccezione dei controller di dominio).

I criteri di protezione dell'organizzazione potrebbero indicare esplicitamente che il gruppo deve essere rimosso da tale diritto di accesso. Considerare il seguente approccio:

- Virtual Delivery Agent (VDA) per il sistema operativo multisessione utilizza Servizi Desktop remoto Microsoft. È possibile configurare il gruppo Utenti Desktop remoto come gruppo con restrizioni e controllare l'appartenenza al gruppo tramite i criteri di gruppo di Active Directory. Per ulteriori informazioni, vedere la documentazione di Microsoft.
- Per altri componenti di Citrix Virtual Apps and Desktops, incluso il VDA per il sistema operativo a sessione singola, il gruppo Utenti Desktop remoto non è richiesto. Pertanto, per questi componenti, il gruppo Utenti Desktop remoto non richiede il diritto di accesso "Consenti accesso tramite Servizi Desktop remoto"; è possibile rimuoverlo. Inoltre:
  - Se si amministrano tali computer tramite Servizi Desktop remoto, assicurarsi che i corrispondenti amministratori siano già membri del gruppo Amministratori.
  - Se non si amministrano tali computer tramite Servizi Desktop remoto, è consigliabile disabilitare Servizi Desktop remoto in tali computer.

Sebbene sia possibile aggiungere utenti e gruppi al diritto di accesso "Nega accesso tramite Servizi Desktop remoto", l'utilizzo dei diritti di negazione accesso non è generalmente raccomandato. Per ulteriori informazioni, vedere la documentazione di Microsoft.

### Configurare i diritti utente

L'installazione di Delivery Controller crea i seguenti servizi di Windows:

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): gestisce gli account computer Microsoft Active Directory per le macchine virtuali.
- Citrix Analytics (NT SERVICE\CitrixAnalytics): raccoglie informazioni sull'utilizzo della configurazione del sito ad uso di Citrix, se tale raccolta è stata approvata dall'amministratore del sito. Invia quindi queste informazioni a Citrix, per contribuire a migliorare il prodotto.

- Citrix App Library (NT SERVICE\CitrixAppLibrary): supporta la gestione e il provisioning di AppDisks, l'integrazione AppDNA e la gestione di App-V.
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): seleziona i desktop virtuali o le applicazioni disponibili per gli utenti.
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): registra tutte le modifiche della configurazione e altre modifiche di stato apportate al sito dagli amministratori.
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): repository a livello di sito per la configurazione condivisa.
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): gestisce le autorizzazioni concesse agli amministratori.
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): gestisce gli autotest degli altri servizi dei Delivery Controller.
- Citrix Host Service (NT SERVICE\CitrixHostService): archivia le informazioni sulle infrastrutture hypervisor utilizzate in una distribuzione Citrix Virtual Apps o Citrix Virtual Desktops e offre anche funzionalità utilizzate dalla console per enumerare le risorse in un pool di hypervisor.
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): orchestra la creazione di macchine virtuali desktop.
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): raccoglie le metriche per Citrix Virtual Apps o Citrix Virtual Desktops, archivia le informazioni cronologiche e fornisce un'interfaccia di query per la risoluzione dei problemi e gli strumenti di reporting.
- Citrix Storefront Service (NT SERVICE\ CitrixStorefront): supporta la gestione di StoreFront. (Non fa parte del componente StoreFront stesso.)
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): supporta le operazioni di gestione privilegiata di StoreFront. (Non fa parte del componente StoreFront stesso.)
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): propaga i dati di configurazione dal database del sito principale alla cache host locale.
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): seleziona i desktop virtuali o le applicazioni disponibili per gli utenti, quando il database del sito principale non è disponibile.

L'installazione di Delivery Controller crea anche i seguenti servizi di Windows. Questi vengono creati anche quando vengono installati con altri componenti Citrix:

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): supporta la raccolta di informazioni diagnostiche che saranno utilizzate dal supporto Citrix.
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): raccoglie informazioni diagnostiche per che saranno analizzate da Citrix, in modo che i risultati dell'analisi e le relative raccomandazioni possano essere visualizzati dagli amministratori per facilitare la diagnosi dei problemi del sito.

L'installazione di Delivery Controller crea anche il seguente servizio Windows. Questo non è attualmente utilizzato. Se è stato abilitato, disabilitarlo.

- Citrix Remote Broker Provider (NT SERVICE\XaXdCloudProxy)

L'installazione di Delivery Controller crea anche i servizi di Windows seguenti. Questi non sono attualmente utilizzati, ma devono essere abilitati. Non disabilitarli.

- Citrix Orchestration Service (NT SERVICE\CitrixOrchestration)
- Citrix Trust Service (NT SERVICE\CitrixTrust)

Ad eccezione di Citrix Storefront Privileged Administration Service, a questi servizi viene concesso il diritto Accedi come servizio e i privilegi Regolazione limite risorse memoria per un processo, Generazione di controlli di protezione e Sostituzione di token a livello di processo. Non è necessario modificare questi diritti utente. Questi privilegi non vengono utilizzati dal Delivery Controller e sono disattivati automaticamente.

### Configurare le impostazioni del servizio

Ad eccezione del servizio Citrix Storefront Privileged Administration e del servizio Citrix Telemetry, i servizi Windows Delivery Controller elencati sopra nella sezione Configurare i diritti utente sono configurati per l'accesso come identità del SERVIZIO DI RETE. Non modificare queste impostazioni di servizio.

Citrix Config Synchronizer Service necessita dell'account NETWORK SERVICE per appartenere al gruppo Local Administrator sul Delivery Controller. Ciò consente alla cache host locale di funzionare correttamente.

Il servizio Citrix Storefront Privileged Administration è configurato per accedere al sistema locale (NT AUTHORITY\SYSTEM). Questo è necessario per le operazioni di Delivery Controller StoreFront che normalmente non sono disponibili per i servizi (inclusa la creazione di siti Microsoft IIS). Non modificare le impostazioni del servizio.

Citrix Telemetry Service è configurato per l'accesso con la propria identità specifica del servizio.

È possibile disattivare il Citrix Telemetry Service. A eccezione di questo servizio e dei servizi che sono già disabilitati, non disabilitare alcun altro di questi servizi Windows di Delivery Controller.

### Configurare le impostazioni del registro

Non è più necessario abilitare la creazione di nomi di file e cartelle 8.3 sul file system VDA. La chiave del Registro di sistema **NtfsDisable8dot3NameCreation** può essere configurata per disabilitare la creazione di nomi di file e cartelle 8.3. È inoltre possibile configurarla utilizzando il comando **fsutil.exe behavior set disable8dot3**.

## Implicazioni per la sicurezza dello scenario di distribuzione

L'ambiente utente può contenere dispositivi utente non gestiti dall'organizzazione e completamente sotto il controllo dell'utente oppure dispositivi utente gestiti e amministrati dall'organizzazione. Le considerazioni sulla sicurezza per questi due ambienti sono generalmente diverse.

### Dispositivi utente gestiti

I dispositivi utente gestiti sono sotto il controllo amministrativo; sono sotto il controllo dell'utente o il controllo di un'altra organizzazione attendibile. È possibile configurare e fornire dispositivi utente direttamente agli utenti; in alternativa, è possibile fornire terminali su cui viene eseguito un singolo desktop in modalità a schermo intero. Seguire le procedure consigliate generali per la sicurezza descritte sopra per tutti i dispositivi utente gestiti. Questa versione ha il vantaggio che il software installato sul dispositivo utente è minimo.

Un dispositivo utente gestito può essere configurato per essere utilizzato in modalità a schermo intero o in modalità finestra:

- Modalità a schermo intero: gli utenti accedono ad esso con la solita schermata di accesso a Windows. Le stesse credenziali utente vengono quindi utilizzate per accedere automaticamente a questa versione.
- Gli utenti visualizzano il proprio desktop in una finestra: gli utenti accedono innanzitutto al dispositivo utente, quindi accedono a questa versione tramite un sito Web fornito con la release.

### Dispositivi utente non gestiti

Non si può presumere che i dispositivi utente non gestiti e amministrati da un'organizzazione attendibile siano sotto il controllo amministrativo. Ad esempio, è possibile consentire agli utenti di ottenere e configurare i propri dispositivi, ma gli utenti potrebbero non seguire le procedure di sicurezza generali consigliate sopra descritte. Questa versione ha il vantaggio di consentire la distribuzione di desktop in modo sicuro ai dispositivi utente non gestiti. Questi dispositivi dovrebbero comunque ancora una protezione antivirus di base che sconfigga i keylogger e altri attacchi di input simili.

### Considerazioni sull'archiviazione dei dati

Quando si utilizza questa versione, è possibile impedire agli utenti di archiviare i dati sui dispositivi utente che sono fisicamente sotto il loro controllo. Tuttavia, è comunque necessario considerare le implicazioni dell'archiviazione dei dati degli utenti sui desktop. Non è buona norma per gli utenti archiviare i dati sui desktop; i dati devono essere conservati su file server, server di database o altri repository in cui possono essere adeguatamente protetti.

L'ambiente desktop può essere costituito da vari tipi di desktop, ad esempio desktop in pool e dedicati. Gli utenti non devono mai archiviare dati su desktop condivisi tra utenti, ad esempio desktop in pool. Se gli utenti archiviano dati su desktop dedicati, tali dati devono essere rimossi se il desktop viene successivamente reso disponibile ad altri utenti.

#### Ambienti in versione mista

Gli ambienti in versione mista sono inevitabili durante alcuni aggiornamenti. Seguire le procedure consigliate e ridurre al minimo il tempo di coesistenza di componenti Citrix di versioni diverse. Negli ambienti con versioni miste, i criteri di protezione, ad esempio, potrebbero non essere applicati in modo uniforme.

> **Nota:**
>
> Questo è tipico di altri prodotti software; l'utilizzo di una versione precedente di Active Directory applica solo parzialmente i Criteri di gruppo alle versioni successive di Windows.

Lo scenario seguente descrive un problema di protezione che può verificarsi in uno specifico ambiente Citrix in versioni miste. Quando Citrix Receiver 1.7 viene utilizzato per connettersi a un desktop virtuale che esegue VDA in XenApp e XenDesktop 7.6 Feature Pack 2, l'impostazione **Allow file transfer between desktop and client** (Consenti trasferimento file fra desktop e client) è abilitata nel sito ma non può essere disattivata da un Delivery Controller che esegue XenApp e XenDesktop 7.1. Non riconosce l'impostazione del criterio, che è stata rilasciata nella versione successiva del prodotto. Questa impostazione di criterio consente agli utenti di caricare e scaricare file sul proprio desktop virtuale, presentando un problema di sicurezza. Per ovviare a questo problema, aggiornare il Delivery Controller (o un'istanza autonoma di Studio) alla versione 7.6 Feature Pack 2 e quindi utilizzare Criteri di gruppo per disattivare l'impostazione dei criteri. In alternativa, utilizzare i criteri locali su tutti i desktop virtuali interessati.

### Considerazioni sulla sicurezza di Accesso remoto PC

Accesso remoto PC implementa le seguenti funzionalità di sicurezza:

- L'utilizzo delle smart card è supportato.
- Quando una sessione remota si connette, il monitor del PC dell'ufficio appare vuoto.
- Accesso remoto PC reindirizza tutti gli input da tastiera e mouse alla sessione remota, ad eccezione di CTRL+ALT+CANC e delle smart card e dei dispositivi biometrici USB.
- SmoothRoaming è supportato solo per un singolo utente.
- Quando un utente dispone di una sessione remota connessa a un PC dell'ufficio, solo tale utente può riprendere l'accesso locale al PC dell'ufficio. Per riprendere l'accesso locale, l'utente preme Ctrl-Alt-Canc sul PC locale e quindi accede con le stesse credenziali utilizzate

dalla sessione remota. L'utente può anche riprendere l'accesso locale inserendo una smart card o sfruttando la biometria, se il sistema dispone di un'integrazione appropriata di provider di credenziali di terze parti. Questo comportamento predefinito può essere ignorato attivando il cambio rapido utente tramite oggetti Criteri di gruppo (GPO) o modificando il Registro di sistema.

> **Nota:**
>
> Citrix consiglia di non assegnare privilegi di amministratore VDA agli utenti di sessione generali.

#### Assegnazioni automatiche

Per impostazione predefinita, Accesso remoto PC supporta l'assegnazione automatica di più utenti a un VDA. In XenDesktop 5.6 Feature Pack 1, gli amministratori possono ignorare questo comportamento utilizzando lo script RemotePCAccess.ps1 di PowerShell. Questa versione utilizza una voce del Registro di sistema per consentire o vietare più assegnazioni automatiche di PC remoti; questa impostazione si applica all'intero sito.

> **Attenzione:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Per limitare le assegnazioni automatiche a un singolo utente:

In ogni controller del sito, impostare la seguente voce del Registro di sistema:

```
HKEY\_LOCAL\_MACHINE\Software\Citrix|DesktopServer
Name: AllowMultipleRemotePCAssignments
Type: REG_DWORD
Data: 0 = Disable multiple user assignment, 1 = (Default) Enable
    multiple user assignment.
```

Se sono presenti assegnazioni utente esistenti, rimuoverle utilizzando i comandi SDK affinché il VDA sia successivamente idoneo per una singola assegnazione automatica.

- Rimuovere tutti gli utenti assegnati dal VDA: `$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- Rimuovere il VDA dal gruppo di consegna: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

Riavviare il PC dell'ufficio fisico.

### Attendibilità XML

L'impostazione di attendibilità XML si applica alle distribuzioni che utilizzano:

- StoreFront locale.
- Tecnologia di autenticazione degli abbonati (utenti) che non richiede password. Esempi di tali tecnologie sono le soluzioni mediante pass-through di dominio, smart card, SAML e Veridium.

L'attivazione dell'impostazione di attendibilità XML consente agli utenti di autenticare e quindi avviare correttamente le applicazioni. Il Delivery Controller considera attendibili le credenziali inviate da StoreFront. Attivare questa impostazione solo quando sono state protette le comunicazioni tra i controller di consegna e StoreFront (utilizzando firewall, IPsec o altri sistemi di protezione consigliati).

Questa impostazione è disabilitata per impostazione predefinita.

Utilizzare l'SDK PowerShell per Citrix Virtual Apps and Desktops per controllare, abilitare o disabilitare l'impostazione di attendibilità XML.

- Per verificare il valore corrente dell'impostazione di attendibilità XML, eseguire `Get-BrokerSite` ed esaminare il valore di `TrustRequestsSentToTheXMLServicePort`.
- Per abilitare l'attendibilità XML, eseguire `Set-BrokerSite -TrustRequestsSentToTheXmlServi $true`.
- Per disattivare l'attendibilità XML, eseguire `Set-BrokerSite -TrustRequestsSentToTheXmlServ $false`.

## Smart card

January 7, 2024

Le smart card e le tecnologie equivalenti sono supportate nell'ambito delle linee guida descritte in questo articolo. Per utilizzare smart card con Citrix Virtual Apps o Citrix Virtual Desktops:

- Avere chiari i criteri di sicurezza dell'organizzazione relativi all'utilizzo delle smart card. Tali criteri potrebbero, ad esempio, indicare come vengono emesse le smart card e come devono proteggerle gli utenti. Alcuni aspetti di questi criteri potrebbero dover essere rivalutati in un ambiente Citrix Virtual Apps o Citrix Virtual Desktops.
- Determinare quali tipi di dispositivi utente, sistemi operativi e applicazioni pubblicate devono essere utilizzati con le smart card.
- Prendere dimestichezza con la tecnologia smart card e l'hardware e il software del fornitore di smart card prescelto.
- Sapere come distribuire i certificati digitali in un ambiente distribuito.

> **Nota:**
>
> La registrazione con smart card non è supportata con smart card veloci. La registrazione di smart card potrebbe funzionare quando la smart card veloce è disabilitata, ma questo dipende dal tipo di smart card e middleware. Contattare il fornitore di smart card e middleware per informazioni sulla loro integrazione con Citrix Virtual Apps and Desktops e per ricevere supporto per la registrazione di smart card nelle sessioni virtuali.

### Tipi di smart card

Le smart card aziendali e consumer hanno in comune le dimensioni, i connettori elettrici e i lettori.

Le smart card per uso aziendale contengono certificati digitali. Queste smart card supportano l'accesso a Windows e possono essere utilizzate anche con applicazioni per la firma digitale e la crittografia di documenti ed e-mail. Citrix Virtual Apps and Desktops supporta questi utilizzi.

Le smart card per uso consumer non contengono certificati digitali, ma contengono un segreto condiviso. Queste smart card possono supportare i pagamenti (ad esempio una carta di credito con chip che richiede la firma o con chip che richiede un PIN). Non supportano l'accesso a Windows o le tipiche applicazioni Windows. Per l'utilizzo con queste smart card sono necessarie applicazioni Windows specializzate e un'infrastruttura software adatta (inclusa, ad esempio, una connessione a una rete di carte di pagamento). Contattare il rappresentante Citrix per informazioni sul supporto di queste applicazioni specializzate in Citrix Virtual Apps o Citrix Virtual Desktops.

Per le smart card aziendali, esistono equivalenti compatibili che possono essere utilizzati in modo simile.

- Un token USB equivalente a una smart card si collega direttamente a una porta USB. Questi token USB sono solitamente delle dimensioni di un'unità flash USB, ma possono essere piccoli come una scheda SIM per telefono cellulare. Essi sono visualizzati come la combinazione di una smart card e un lettore di smart card USB.
- Una smart card virtuale che utilizza un TPM (Trusted Platform Module) di Windows viene visualizzata come smart card. Queste smart card virtuali sono supportate in Windows 8 e Windows 10, mediante l'app Citrix Workspace (versione minima Citrix Receiver 4.3).
  - Le versioni di Citrix Virtual Apps and Desktops (precedentemente XenApp e XenDesktop) precedenti a XenApp e XenDesktop 7.6 FP3 non supportano le smart card virtuali.
  - Per ulteriori informazioni sulle smart card virtuali, vedere Panoramica delle smart card virtuali.

  **Nota:** il termine "smart card virtuale"viene utilizzato anche per descrivere un certificato digitale memorizzato nel computer dell'utente. Questi certificati digitali non sono strettamente equivalenti alle smart card.

Il supporto delle smart card Citrix Virtual Apps and Desktops si basa sulle specifiche standard Microsoft Personal Computer/Smart Card (PC/SC). Un requisito minimo è che le smart card e i dispositivi smart card devono essere supportati dal sistema operativo Windows sottostante e devono essere approvati dai Microsoft Windows Hardware Quality Labs (WHQL) per essere utilizzati su computer che eseguono sistemi operativi Windows idonei. Per ulteriori informazioni sulla conformità hardware PC/SC, vedere la documentazione Microsoft. Altri tipi di dispositivi utente potrebbero essere conformi allo standard PS/SC. Per ulteriori informazioni, vedere il programma Citrix Ready.

In genere, è necessario un driver di periferica separato per ogni smart card o equivalente di ciascun fornitore. Tuttavia, se le smart card sono conformi a uno standard come lo standard PIV (Personal Identity Verification) NIST, potrebbe essere possibile utilizzare un singolo driver di periferica per una serie di smart card. Il driver di periferica deve essere installato sia sul dispositivo utente che su Virtual Delivery Agent (VDA). Il driver di periferica viene spesso fornito come parte di un pacchetto middleware smart card disponibile da un partner Citrix; il pacchetto middleware smart card offre funzionalità avanzate. Il driver di periferica potrebbe anche essere descritto come provider di servizi di crittografia (CSP), Key Storage Provider (KSP) o minidriver.

Le seguenti combinazioni di smart card e middleware per sistemi Windows sono state testate da Citrix come esempi rappresentativi del loro tipo. Tuttavia, è possibile utilizzare anche altre smart card e middleware. Per ulteriori informazioni sulle smart card e sui middleware compatibili con Citrix, vedere http://www.citrix.com/ready.

| Middleware | Carte abbinate |
|---|---|
| Gemalto Mini Driver per scheda .NET | Gemalto .NET v2+ |

Per informazioni sull'utilizzo delle smart card con altri tipi di dispositivi, vedere la documentazione dell'app Citrix Workspace relativa a tale dispositivo.

### Accesso remoto al PC

Le smart card sono supportate solo per l'accesso remoto ai PC fisici dell'ufficio che eseguono Windows 10, Windows 8 o Windows 7.

Le seguenti smart card sono state testate con Accesso remoto PC:

| Middleware | Carte abbinate |
|---|---|
| Minidriver Gemalto .NET | Gemalto .NET v2+ |

### Smart card veloce

La smart card veloce è un miglioramento rispetto al reindirizzamento delle smart card HDX PC/SC esistente. Migliora le prestazioni quando le smart card vengono utilizzate in situazioni WAN ad alta latenza. Quando la latenza è elevata, il miglioramento delle prestazioni può essere significativo (ad esempio, 15 secondi per un accesso veloce con smart card Windows rispetto a più di 1 minuto con il reindirizzamento della smart card basata su PC/SC).

La smart card veloce è abilitata per impostazione predefinita sui computer host con Windows VDA attualmente supportati. Per disattivare la smart card veloce sul lato host, ad esempio per scopi diagnostici, impostare l'impostazione del Registro di sistema "Disable Cryptographic Redirection"su qualsiasi valore diverso da zero:

```
HKLM\SOFTWARE\Citrix\SmartCard
CryptographicRedirectionDisable (DWORD)
<!--NeedCopy-->
```

Sul lato client, per abilitare la smart card veloce, includere il parametro ICA SmartCardCryptographicRedirection nel file *default.ica* del sito StoreFront associato:

```
[WFClient]
SmartCardCryptographicRedirection=On
```

Inoltre, sul lato client, la smart card veloce può essere attivata forzatamente o disattivata forzatamente (ad esempio, per scopi diagnostici) con le seguenti impostazioni del registro:

- HKLM\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (come DWORD con valore diverso da zero)

oppure

- HKLM\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (come DWORD con valore diverso da zero)

L'hive del Registro di sistema a 32 bit deve essere specificato (utilizzando `WOW6432Node`) se il computer client è a 64 bit.

Limitazioni:

- Solo l'app Citrix Workspace per Windows supporta le smart card veloci. Se si configurano smart card veloci nel file default.ica, le app Citrix Workspace che non sono per Windows funzionano comunque con il reindirizzamento PC/SC esistente.
- Gli unici scenari a doppio hop supportati dalle smart card veloci sono ICA > ICA con smart card veloce abilitata su entrambi gli hop. Poiché la smart card veloce non supporta gli scenari ICA > RDP a doppio hop, questi scenari non funzionano.
- Le smart card veloci non supportano CNG (Cryptography Next Generation). Pertanto, le smart card veloci non supportano le smart card ECC (Elliptic Curve Cryptography).

- Le smart card veloci supportano solo operazioni di contenitori di chiavi di sola lettura.
- La smart card veloce non supporta la modifica del PIN della smart card.

A partire dalla versione VDA 2203 e dall'app Citrix Workspace versione 2202 per Windows (o successiva), la smart card veloce è compatibile con Cryptography Next Generation (CNG). Inoltre, le smart card Elliptic Curve Cryptography (ECC) sono supportate con le seguenti curve: P-256, P-384, P-521 bit, sia per ECDSA che per ECDH.

A partire dalla versione 2203 del VDA, la smart card veloce aggiunge la possibilità di memorizzare nella cache il PIN della smart card tra le applicazioni dalla stessa sessione di accesso dell'utente. Ad esempio, se l'impostazione **Session PIN Caching** (memorizzazione nella cache dei PIN di sessione) è attivata e l'utente finale aveva precedentemente fornito il PIN della smart card a Outlook, quando Word viene quindi utilizzato per firmare un documento, Word utilizza il PIN della smart card già memorizzato nella cache (inviato ad Outlook). L'impostazione **Session PIN Caching** migliora l'esperienza dell'utente riducendo il numero di volte che l'utente deve inserire il PIN della propria smart card. Inoltre, se la smart card viene utilizzata per accedere al VDA, il PIN di accesso della smart card di Windows può essere salvato facoltativamente nella **cache dei PIN della sessione**. Questo può migliorare ulteriormente l'esperienza dell'utente.

**Session PIN Caching** è disabilitata per impostazione predefinita. Può essere abilitata e controllata con le seguenti impostazioni di registro sul VDA:

In HKLM\SOFTWARE\Citrix\SmartCard:

- `EnablePinSessionCache` come DWORD (diversa da zero per abilitare)
- `EnableLogonPinSessionCache` come DWORD (diversa da zero per abilitare)
- `PinSessionCacheEntryStaleTimeout` come DWORD (numero di secondi prima che una voce diventi obsoleta, il valore predefinito è 1 ora)

### Tipi di lettori di smart card

Un lettore di smart card può essere integrato nel dispositivo utente o essere collegato al dispositivo utente a parte (in genere tramite USB o Bluetooth). Sono supportati lettori di schede contatto conformi alle specifiche Chip/Smart Card Interface Devices (CCID) USB. Contengono uno slot o un dispositivo di scorrimento in cui l'utente inserisce la smart card. Lo standard Deutsche Kreditwirtschaft (DK) definisce quattro classi di lettori di schede contatto.

- I lettori di smart card di classe 1 sono i più comuni e di solito contengono solo uno slot. I lettori di smart card di classe 1 sono supportati, di solito con un driver di periferica CCID standard fornito con il sistema operativo.
- I lettori di smart card di classe 2 contengono inoltre un tastierino sicuro a cui non è possibile accedere dal dispositivo utente. I lettori di smart card di classe 2 potrebbero essere integrati in una tastiera con tastierino sicuro integrato. Per i lettori di smart card di classe 2, contattare il

rappresentante Citrix; potrebbe essere necessario un driver di periferica specifico per abilitare la funzionalità tastierino sicuro.
- I lettori di smart card di classe 3 contengono anche un display sicuro. I lettori di smart card di classe 3 non sono supportati.
- I lettori di smart card di classe 4 contengono anche un modulo di transazione sicuro. I lettori di smart card di classe 4 non sono supportati.

> **Nota:**
>
> La classe del lettore di smart card non è correlata alla classe di periferica USB.

I lettori di smart card devono essere installati con un driver di periferica corrispondente sul dispositivo utente.

Per informazioni sui lettori di smart card supportati, vedere la documentazione dell'app Citrix Workspace in uso. Nella documentazione dell'app Citrix Workspace, le versioni supportate sono in genere elencate in un articolo sulla smart card o nell'articolo sui requisiti di sistema.

### Esperienza utente

Il supporto delle smart card è integrato in Citrix Virtual Apps and Desktops, utilizzando uno specifico canale virtuale per smart card ICA/HDX abilitato per impostazione predefinita.

Importante: non utilizzare il reindirizzamento USB generico per i lettori di smart card. Questa opzione è disattivata per impostazione predefinita per i lettori di smart card e non è supportata se attivata.

È possibile utilizzare più smart card e più lettori sullo stesso dispositivo utente, ma se è in uso l'autenticazione pass-through, è necessario inserire una sola smart card quando l'utente avvia un desktop o un'applicazione virtuale. Quando una smart card viene utilizzata all'interno di un'applicazione (ad esempio, per le funzioni di firma digitale o crittografia), potrebbero essere visualizzate altre richieste di inserire una smart card o immettere un PIN. Ciò può verificarsi se sono state inserite più smart card contemporaneamente.

- Se viene chiesto agli utenti di inserire una smart card quando la smart card è già presente nel lettore, è necessario selezionare Annulla.
- Se viene richiesto agli utenti di immettere il PIN, questi devono mmetterlo nuovamente.

È possibile reimpostare i PIN utilizzando un sistema di gestione delle schede o un'utilità fornitore.

> **Importante:**
>
> All'interno di una sessione Citrix Virtual Apps o Citrix Virtual Desktops, l'utilizzo di una smart card con l'applicazione Microsoft Remote Desktop Connection non è supportato. Questo è talvolta descritto come uso "doppio hop".

### Prima di distribuire le smart card

- Ottenere un driver di periferica per il lettore di smart card e installarlo sul dispositivo utente. Molti lettori di smart card possono utilizzare il driver di periferica CCID fornito da Microsoft.
- Ottenere un driver di dispositivo e un software CSP (provider di servizi di crittografia) dal fornitore di smart card e installarli su dispositivi utente e desktop virtuali. Il driver e il software CSP devono essere compatibili con Citrix Virtual Apps and Desktops; controllare la documentazione del fornitore per verificare la compatibilità. Per i desktop virtuali che utilizzano smart card che supportano e utilizzano il modello minidriver, i minidriver smart card si scaricano automaticamente, ma è anche possibile ottenerli da http://catalog.update.microsoft.com o dal proprio fornitore. Inoltre, se è richiesto il middleware PKCS#11, ottenerlo dal fornitore della scheda.
- Importante: Citrix consiglia di installare e testare i driver e il software CSP su un computer fisico prima di installare il software Citrix.
- Aggiungere Citrix Receiver per URL Web all'elenco Siti attendibili per gli utenti che utilizzano smart card in Internet Explorer con Windows 10. In Windows 10, Internet Explorer non viene eseguito in modalità protetta per impostazione predefinita per i siti attendibili.
- Assicurarsi che l'infrastruttura a chiave pubblica (PKI) sia configurata in modo appropriato. Ciò include la verifica che il mapping dal certificato all'account sia configurato correttamente per l'ambiente Active Directory e che la convalida del certificato utente possa essere eseguita correttamente.
- Assicurarsi che la distribuzione soddisfi i requisiti di sistema degli altri componenti Citrix utilizzati con le smart card, tra cui Citrix Workspace app e StoreFront.
- Assicurare l'accesso nel proprio sito ai seguenti server:
  - Il controller di dominio Active Directory per l'account utente associato a un certificato di accesso sulla smart card
  - Delivery Controller
  - Citrix StoreFront
  - Citrix Gateway/Citrix Access Gateway 10.x
  - VDA
  - (Facoltativo per l'accesso remoto al PC): Microsoft Exchange Server

### Abilitare l'uso delle smart card

**Passaggio 1.** Rilasciare smart card agli utenti in base ai criteri di emissione della carta.

**Passaggio 2.** (Facoltativo) Impostare le smart card per consentire agli utenti l'accesso remoto al PC.

**Passaggio 3.** Installare e configurare il Delivery Controller e StoreFront (se non è già installato) per la comunicazione remota delle smart card.

**Passaggio 4.** Abilitare StoreFront per l'utilizzo di smart card. Per ulteriori informazioni, vedere Configurare l'autenticazione smart card nella documentazione di StoreFront.

**Passaggio 5.** Abilitare Citrix Gateway/Access Gateway per l'utilizzo delle smart card. Per ulteriori informazioni, vedere Configuring Authentication and Authorization (Configurare l'autenticazione e l'autorizzazione) e Configuring Smart Card Access with the Web Interface (Configurare l'accesso alle smart card con l'interfaccia Web) nella documentazione di NetScaler.

**Passaggio 6.** Abilitare i VDA per l'utilizzo di smart card.

- Assicurarsi che il VDA disponga delle applicazioni e degli aggiornamenti necessari.
- Installare il middleware.
- Configurare la comunicazione remota delle smart card, consentendo la comunicazione dei dati delle smart card tra l'app Citrix Workspace su un dispositivo utente e una sessione desktop virtuale.

**Passaggio 7.** Abilitare i dispositivi utente (incluse le macchine aggiunte a un dominio o non aggiunte a un dominio) per l'utilizzo delle smart card. Per ulteriori informazioni, vedere Configure smart card authentication (Configurare l'autenticazione smart card) nella documentazione di StoreFront.

- Importare il certificato radice dell'autorità di certificazione e il certificato dell'autorità di certificazione emittente nel keystore del dispositivo.
- Installare il middleware delle smart card del fornitore.
- Installare e configurare l'app Citrix Workspace per Windows, assicurandosi di importare icaclient.adm utilizzando la Console Gestione Criteri di gruppo e abilitare l'autenticazione smart card.

**Passaggio 8.** Testare la distribuzione. Assicurarsi che la distribuzione sia configurata correttamente avviando un desktop virtuale con la smart card di un utente di prova. Verificare tutti i possibili meccanismi di accesso (ad esempio, l'accesso al desktop tramite Internet Explorer e l'app Citrix Workspace).

### Tenere traccia del numero di inserimenti del lettore di smart card

Con la comunicazione remota mediante smart card, è possibile utilizzare la funzione SCardGetStatusChange per tenere traccia del numero di volte in cui una smart card è stata inserita o rimossa da un lettore. La funzione aggiorna una serie di strutture dati SCARD_READERSTATE, una per ogni lettore monitorato. La parola alta (16 bit) del campo dwEventState di ogni SCARD_READERSTATE contiene il numero di lettori. Per ulteriori informazioni, vedere gli articoli Microsoft SCardGetStatusChangeA function e SCARD_READERSTATEA structure.

L'impostazione **Reader Insert Count Reporting** (Report conteggio inserimenti lettore) è disattivata per impostazione predefinita. Per attivare il tracciamento, aggiungere la seguente chiave del Registro di sistema:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

Nome: EnableReaderInsertCountReporting

Tipo: DWORD

Valore: qualsiasi valore diverso da zero

Quando la sessione si disconnette, il conteggio viene ripristinato a zero.

**Reader Insert Count Reporting** (Report conteggio inserimenti lettore) è compatibile con il middleware smart card di terze parti.

## Distribuzioni con smart card

January 7, 2024

I seguenti tipi di distribuzioni con smart card sono supportati da questa versione del prodotto e dagli ambienti misti contenenti questa versione. Altre configurazioni potrebbero funzionare, ma non sono supportate.

| Tipo | Connettività StoreFront |
|---|---|
| Computer aggiunti a un dominio locale | Connessione diretta |
| Accesso remoto da computer aggiunti a un dominio | Connessione tramite Citrix Gateway |
| Computer non aggiunti a un dominio | Connessione diretta |
| Accesso remoto da computer non aggiunti a un dominio | Connessione tramite Citrix Gateway |
| Computer e thin client non aggiunti a un dominio che accedono al sito Desktop Appliance | Connessione tramite siti Desktop Appliance |
| Computer aggiunti a un dominio e thin client che accedono a StoreFront tramite l'URL dei servizi XenApp | Connessione tramite gli URL dei servizi XenApp |

I tipi di distribuzione sono definiti dalle caratteristiche del dispositivo utente a cui è collegato il lettore di smart card:

- Se il dispositivo è aggiunto o meno a un dominio.
- Come il dispositivo è connesso a StoreFront.
- Quale software viene utilizzato per visualizzare desktop virtuali e applicazioni.

In queste distribuzioni è inoltre possibile utilizzare applicazioni abilitate per smart card come Microsoft Word e Microsoft Excel. Tali applicazioni consentono agli utenti di firmare o crittografare digitalmente i documenti.

### Autenticazione bimodale

Ove possibile in ciascuna di queste distribuzioni, Receiver supporta l'autenticazione bimodale offrendo all'utente la possibilità di scegliere tra l'utilizzo di una smart card e l'immissione del nome utente e della password. Ciò è utile se non è possibile utilizzare la smart card (ad esempio, l'utente l'ha lasciata a casa o il certificato di accesso è scaduto).

Poiché gli utenti di dispositivi non aggiunti a un dominio accedono direttamente a Receiver per Windows, è possibile consentire agli utenti di ricorrere all'autenticazione esplicita. Se si configura l'autenticazione bimodale, agli utenti viene inizialmente richiesto di accedere utilizzando smart card e PIN, ma con la possibilità di selezionare l'autenticazione esplicita in caso di problemi relativi alle smart card.

Se si distribuisce Citrix Gateway, gli utenti accedono ai propri dispositivi e ricevono una richiesta da Receiver per Windows di eseguire l'autenticazione a Citrix Gateway. Questo vale sia per i dispositivi aggiunti a un dominio che per quelli che non lo sono. Gli utenti possono accedere a Citrix Gateway utilizzando la smart card e il PIN o con credenziali esplicite. Ciò consente di fornire agli utenti l'autenticazione bimodale per gli accessi a Citrix Gateway. Configurare l'autenticazione pass-through da Citrix Gateway a StoreFront e delegare la convalida delle credenziali a Citrix Gateway per gli utenti di smart card in modo che vengano autenticati automaticamente su StoreFront.

### Considerazioni su più foreste Active Directory

In un ambiente Citrix, le smart card sono supportate all'interno di una singola foresta. Gli accessi con smart card a più foreste richiedono un trust tra foreste bidirezionale diretto per tutti gli account utente. Non sono supportate distribuzioni a più foreste più complesse che coinvolgono smart card (ovvero, dove i trust sono solo unidirezionali o di tipi diversi).

È possibile utilizzare le smart card in un ambiente Citrix che include desktop remoti. Questa funzione può essere installata localmente (sul dispositivo utente a cui è connessa la smart card) o in remoto (sul desktop remoto a cui il dispositivo utente si connette).

### Criteri di rimozione delle smart card

Il criterio di rimozione smart card impostato sul prodotto determina cosa accade se la smart card viene rimossa dal lettore durante una sessione. Il criterio di rimozione delle smart card viene configurato e gestito dal sistema operativo Windows.

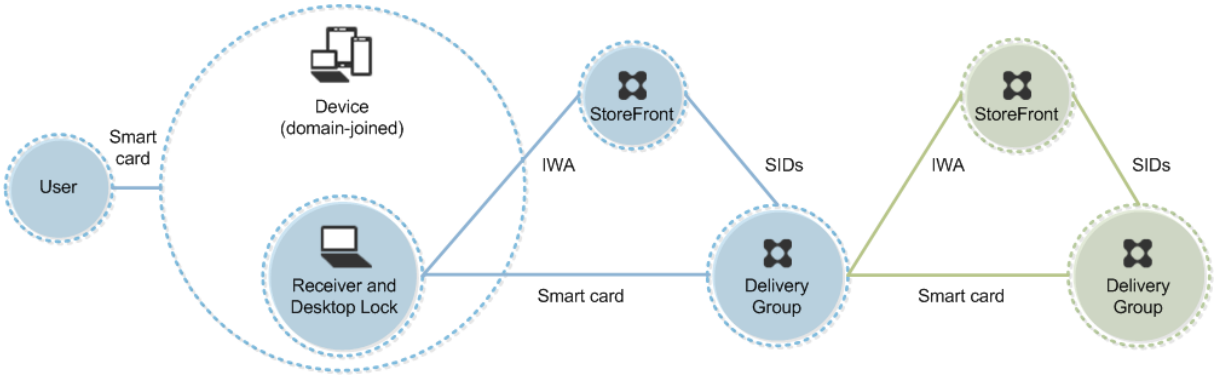
| Impostazione dei criteri | Comportamento desktop |
|---|---|
| No action | No action. |
| Lock workstation | La sessione desktop viene disconnessa e il desktop virtuale viene bloccato. |
| Force logoff | L'utente è costretto a scollegarsi. Se la connessione di rete viene persa e questa impostazione è attivata, la sessione potrebbe essere disconnessa e l'utente potrebbe perdere dati. |
| Disconnect if a remote Terminal Services session | La sessione viene disconnessa e il desktop virtuale viene bloccato. |

### Controllare la revoca dei certificati

Se il controllo della revoca dei certificati è abilitato e un utente inserisce una smart card con un certificato non valido in un lettore di schede, tale utente non può autenticarsi o accedere al desktop o all'applicazione correlata al certificato. Ad esempio, se il certificato non valido viene utilizzato per la decrittografia dei messaggi di posta elettronica, il messaggio di posta elettronica rimane crittografato. Se altri certificati presenti sulla scheda, ad esempio quelli utilizzati per l'autenticazione, sono ancora validi, tali funzioni rimangono attive.

### Esempio di distribuzione: computer aggiunti a un dominio

Questa distribuzione include dispositivi utente aggiunti a un dominio che eseguono Desktop Viewer e si connettono direttamente a StoreFront.




Un utente accede a un dispositivo utilizzando una smart card e un PIN. Il destinatario autentica l'utente a un server Storefront utilizzando l'autenticazione integrata di Windows (IWA). StoreFront passa gli identificatori di sicurezza utente (SID) a Citrix Virtual Apps o Citrix Virtual Desktops. Quando

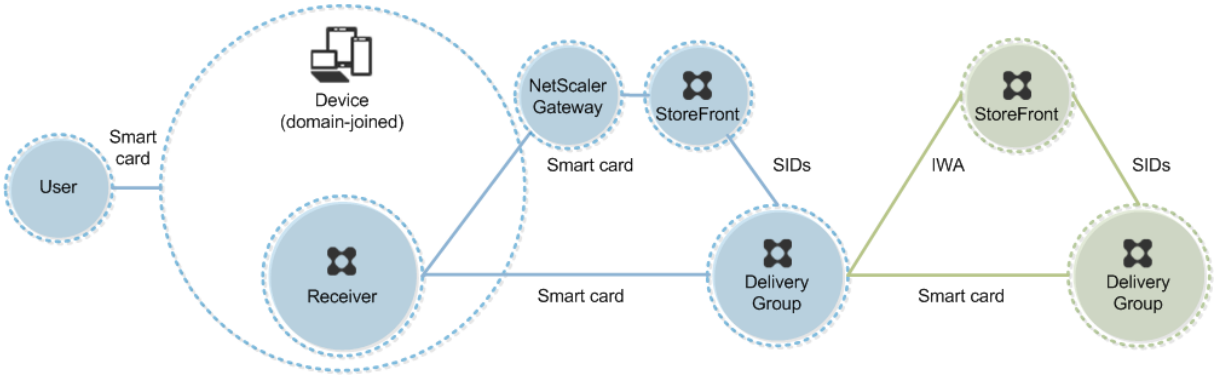
 

l'utente avvia un desktop virtuale o un'applicazione, non gli viene richiesto nuovamente il PIN perché in Receiver è configurata la funzionalità Single Sign-On.

Questa distribuzione può essere estesa a un doppio hop con l'aggiunta di un secondo server StoreFront e di un server che ospita applicazioni. Receiver del desktop virtuale esegue l'autenticazione al secondo server StoreFront. Per questa seconda connessione è possibile utilizzare qualsiasi metodo di autenticazione. La configurazione mostrata per il primo hop può essere riutilizzata nel secondo hop o utilizzata solo nel secondo hop.

### Esempio di distribuzione: accesso remoto da computer aggiunti a un dominio

Questa distribuzione include dispositivi utente aggiunti a un dominio che eseguono Desktop Viewer e si connettono a StoreFront tramite Citrix Gateway/Access Gateway.




Un utente accede a un dispositivo utilizzando una smart card e un PIN, quindi esegue nuovamente l'accesso a Citrix Gateway/Access Gateway. Questo secondo accesso può avvenire con smart card e PIN o con un nome utente e una password perché Receiver consente l'autenticazione bimodale in questa distribuzione.

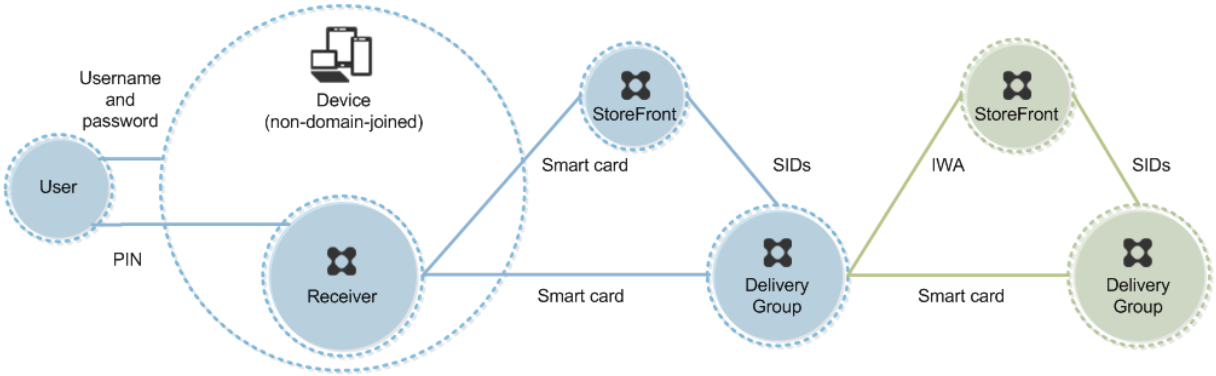
L'utente è connesso automaticamente a StoreFront, che passa gli identificatori di sicurezza utente (SID) a Citrix Virtual Apps o Citrix Virtual Desktops. Quando l'utente avvia un desktop virtuale o un'applicazione, non gli viene richiesto di nuovo un PIN perché in Receiver è configurata la funzionalità Single Sign-On.

Questa distribuzione può essere estesa a un doppio hop con l'aggiunta di un secondo server StoreFront e di un server che ospita applicazioni. Receiver del desktop virtuale esegue l'autenticazione al secondo server StoreFront. Per questa seconda connessione è possibile utilizzare qualsiasi metodo di autenticazione. La configurazione mostrata per il primo hop può essere riutilizzata nel secondo hop o utilizzata solo nel secondo hop.

### Esempio di distribuzione: computer non aggiunti a un dominio

Questa distribuzione include dispositivi utente non aggiunti a un dominio che eseguono Desktop Viewer e si connettono direttamente a StoreFront.




Un utente accede a un dispositivo. In genere, l'utente immette un nome utente e una password ma, poiché il dispositivo non è aggiunto a un dominio, le credenziali per questo accesso sono facoltative. Poiché in questa distribuzione è possibile l'autenticazione bimodale, Receiver richiede all'utente una smart card e un PIN oppure un nome utente e una password. Receiver esegue quindi l'autenticazione in Storefront.

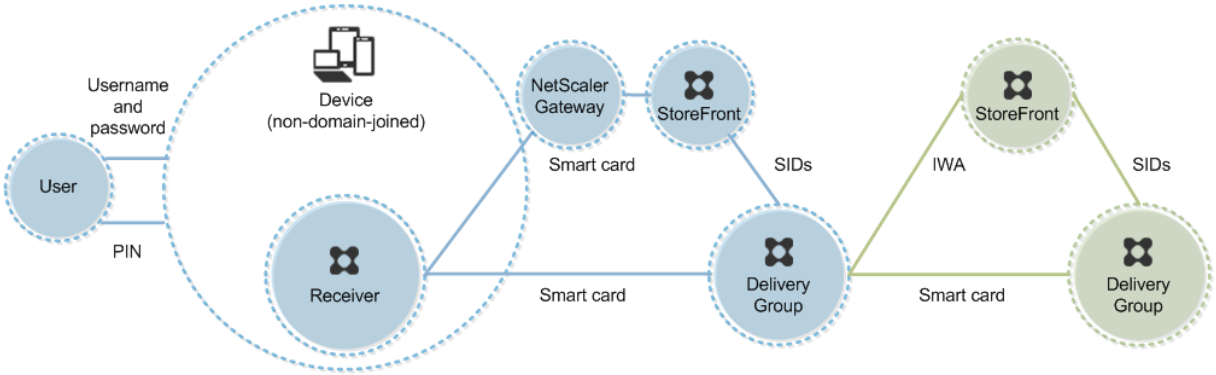
StoreFront passa gli identificatori di sicurezza utente (SID) a Citrix Virtual Apps o Citrix Virtual Desktops. Quando l'utente avvia un desktop virtuale o un'applicazione, gli viene richiesto nuovamente il PIN perché la funzionalità Single Sign-On non è disponibile in questa distribuzione.

Questa distribuzione può essere estesa a un doppio hop con l'aggiunta di un secondo server StoreFront e di un server che ospita applicazioni. Receiver del desktop virtuale esegue l'autenticazione al secondo server StoreFront. Per questa seconda connessione è possibile utilizzare qualsiasi metodo di autenticazione. La configurazione mostrata per il primo hop può essere riutilizzata nel secondo hop o utilizzata solo nel secondo hop.

### Esempio di distribuzione: accesso remoto da computer non aggiunti a un dominio

Questa distribuzione include dispositivi utente non aggiunti a un dominio che eseguono Desktop Viewer e si connettono direttamente a StoreFront.




Un utente accede a un dispositivo. In genere, l'utente immette un nome utente e una password ma, poiché il dispositivo non è aggiunto a un dominio, le credenziali per questo accesso sono facoltative. Poiché in questa distribuzione è possibile l'autenticazione bimodale, Receiver richiede all'utente una smart card e un PIN oppure un nome utente e una password. Receiver esegue quindi l'autenticazione in Storefront.

StoreFront passa gli identificatori di sicurezza utente (SID) a Citrix Virtual Apps o Citrix Virtual Desktops. Quando l'utente avvia un desktop virtuale o un'applicazione, gli viene richiesto nuovamente il PIN perché la funzionalità Single Sign-On non è disponibile in questa distribuzione.

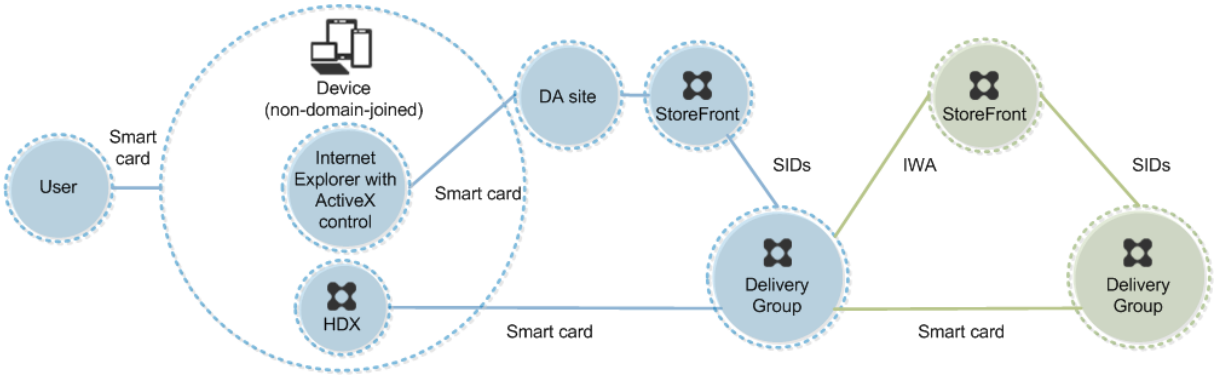
Questa distribuzione può essere estesa a un doppio hop con l'aggiunta di un secondo server StoreFront e di un server che ospita applicazioni. Receiver del desktop virtuale esegue l'autenticazione al secondo server StoreFront. Per questa seconda connessione è possibile utilizzare qualsiasi metodo di autenticazione. La configurazione mostrata per il primo hop può essere riutilizzata nel secondo hop o utilizzata solo nel secondo hop.

### Esempio di distribuzione: computer non aggiunti a un dominio e thin client che accedono al sito Desktop Appliance

Questa distribuzione riguarda dispositivi utente non aggiunti a un dominio che possono eseguire Desktop Lock e connettersi a StoreFront tramite i siti Desktop Appliance.

Desktop Lock è un componente separato rilasciato con Citrix Virtual Apps, Citrix Virtual Desktops e VDI-in-a-Box. Si tratta di un'alternativa a Desktop Viewer ed è progettato principalmente per computer Windows reimpiegati e thin client Windows. Desktop Lock sostituisce la shell di Windows e Task Manager in questi dispositivi utente, impedendo agli utenti di accedere ai dispositivi sottostanti. Con Desktop Lock, gli utenti possono accedere ai desktop di Windows Server Machine e ai desktop di Windows Desktop Machine. L'installazione di Desktop Lock è facoltativa.




Un utente accede a un dispositivo con una smart card. Se Desktop Lock è in esecuzione sul dispositivo, questo è configurato per l'avvio di un sito Desktop Appliance tramite Internet Explorer in esecuzione in modalità Kiosk. Un controllo ActiveX nel sito richiede all'utente di immettere un PIN e lo invia a StoreFront. StoreFront passa gli identificatori di sicurezza utente (SID) a Citrix Virtual Apps o Citrix Virtual Desktops. Viene avviato il primo desktop disponibile nell'elenco alfabetico di un gruppo desktop assegnato.

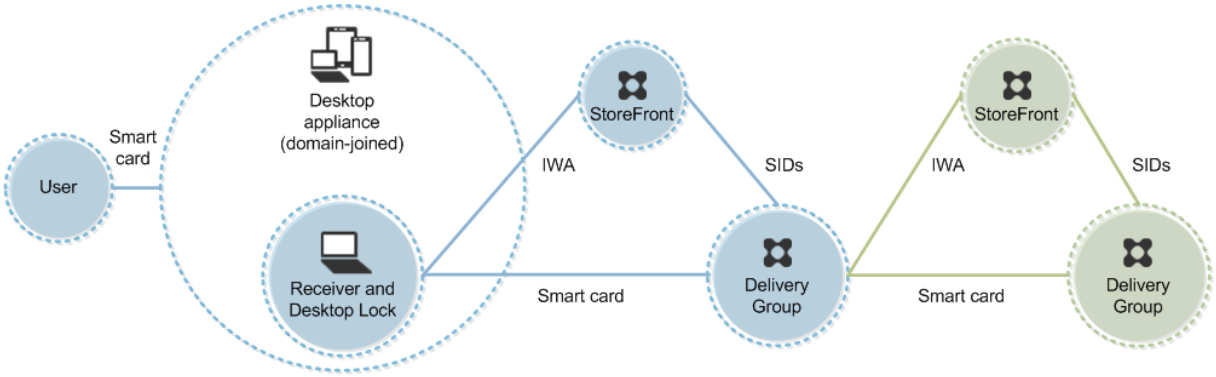
Questa distribuzione può essere estesa a un doppio hop con l'aggiunta di un secondo server StoreFront e di un server che ospita applicazioni. Receiver del desktop virtuale esegue l'autenticazione al secondo server StoreFront. Per questa seconda connessione è possibile utilizzare qualsiasi metodo di autenticazione. La configurazione mostrata per il primo hop può essere riutilizzata nel secondo hop o utilizzata solo nel secondo hop.

### Esempio di distribuzione: computer aggiunti a un dominio e thin client che accedono a StoreFront tramite l'URL dei servizi XenApp

Questa distribuzione riguarda i dispositivi utente aggiunti a un dominio che eseguono Desktop Lock e si connettono a StoreFront tramite URL di servizi XenApp.

Desktop Lock è un componente separato rilasciato con Citrix Virtual Apps, Citrix Virtual Desktops e VDI-in-a-Box. Si tratta di un'alternativa a Desktop Viewer ed è progettato principalmente per computer Windows reimpiegati e thin client Windows. Desktop Lock sostituisce la shell di Windows e Task Manager in questi dispositivi utente, impedendo agli utenti di accedere ai dispositivi sottostanti. Con Desktop Lock, gli utenti possono accedere ai desktop di Windows Server Machine e ai desktop di Windows Desktop Machine. L'installazione di Desktop Lock è facoltativa.




Un utente accede a un dispositivo utilizzando una smart card e un PIN. Se è in esecuzione sul dispositivo, Desktop Lock autentica l'utente a un server Storefront utilizzando l'autenticazione integrata di Windows (IWA). StoreFront passa gli identificatori di sicurezza utente (SID) a Citrix Virtual Apps o Citrix Virtual Desktops. Quando l'utente avvia un desktop virtuale, non gli viene richiesto nuovamente il PIN perché in Receiver è configurata la funzionalità Single Sign-On.

Questa distribuzione può essere estesa a un doppio hop con l'aggiunta di un secondo server StoreFront e di un server che ospita applicazioni. Receiver del desktop virtuale esegue l'autenticazione al secondo server StoreFront. Per questa seconda connessione è possibile utilizzare qualsiasi metodo di autenticazione. La configurazione mostrata per il primo hop può essere riutilizzata nel secondo hop o utilizzata solo nel secondo hop.

## Autenticazione pass-through e Single Sign-On con smart card

January 7, 2024

### Autenticazione pass-through

L'autenticazione pass-through con smart card ai desktop virtuali è supportata sui dispositivi utente che eseguono Windows 10, Windows 8 e Windows 7 SP1 Enterprise Edition e Professional Edition.

L'autenticazione pass-through con smart card alle applicazioni ospitate è supportata nei server che eseguono Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 e Windows Server 2008 R2 SP1.

Per utilizzare l'autenticazione pass-through con le applicazioni ospitate da smart card, assicurarsi di abilitare l'utilizzo di Kerberos quando si configura il pass-through con smartcard come metodo di autenticazione per il sito.

Nota: la disponibilità dell'autenticazione pass-through con smart card dipende da molti fattori, tra cui, a titolo esemplificativo e non esaustivo:

- Criteri di sicurezza dell'organizzazione relativi all'autenticazione pass-through.
- Tipo di middleware e configurazione.
- Tipi di lettori di smart card.
- Criteri di memorizzazione nella cache dei PIN di middleware.

L'autenticazione pass-through con smart card è configurata su Citrix StoreFront. Per ulteriori informazioni, vedere la documentazione di StoreFront.

### Single Sign-On

Single Sign-On è una funzionalità Citrix che implementa l'autenticazione pass-through con l'avvio del desktop virtuale e delle applicazioni. È possibile utilizzare questa funzionalità nelle distribuzioni di smart card aggiunte a un dominio direttamente a StoreFront e da NetScaler a StoreFront aggiunte a un dominio per ridurre il numero di volte in cui gli utenti immettono il PIN. Per utilizzare Single Sign-On in questi tipi di distribuzione, modificare i seguenti parametri nel file default.ica, che si trova sul server StoreFront:

- Distribuzioni smart card direttamente a StoreFront aggiunte a un dominio - Impostare DisableCtrlAltDel su Disattivato
- Distribuzioni smart card da NetScaler a StoreFront aggiunte a un dominio - Impostare UseLocalUserAndPassword su Attivato

Per ulteriori istruzioni sull'impostazione di questi parametri, vedere la documentazione di StoreFront o di Citrix Gateway.

La disponibilità della funzionalità Single Sign-On dipende da molti fattori, tra cui, a titolo esemplificativo ma non esaustivo:

- Criteri di sicurezza dell'organizzazione relativi al Single Sign-On.
- Tipo di middleware e configurazione.
- Tipi di lettori di smart card.
- Criteri di memorizzazione nella cache dei PIN di middleware.

> **Nota:**
>
> Quando un utente accede a Virtual Delivery Agent (VDA) su un computer con un lettore di smart card collegato, potrebbe essere visualizzato un riquadro di Windows che rappresenta la precedente modalità di autenticazione riuscita, ad esempio smart card o password. Di conseguenza, quando è attivato l'accesso Single Sign-On, potrebbe essere visualizzato il riquadro Single Sign-On. Per accedere, l'utente deve selezionare **Switch Users** (Cambia utente) per selezionare un altro riquadro, in quanto il riquadro Single Sign-On non funzionerà.

# TLS (Transport Layer Security)

January 7, 2024

Citrix Virtual Apps and Desktops supporta il protocollo TLS (Transport Layer Security) per le connessioni basate su TCP tra i componenti. Citrix Virtual Apps and Desktops supporta anche il protocollo DTLS (Datagram Transport Layer Security) per connessioni ICA/HDX basate su UDP, mediante trasporto adattivo.

TLS e DTLS sono simili e supportano gli stessi certificati digitali. La configurazione di un sito Citrix Virtual Apps o Citrix Virtual Desktops per l'utilizzo di TLS lo configura anche per l'utilizzo di DTLS. Utilizzare le procedure descritte di seguito. I passaggi sono comuni sia a TLS che a DTLS, tranne dove indicato:

- Ottenere, installare e registrare un certificato server in tutti i Delivery Controller e configurare una porta con il certificato TLS. Per i dettagli, vedere Installare i certificati del server TLS nei controller.

  Facoltativamente, è possibile modificare le porte utilizzate dal controller per l'ascolto del traffico HTTP e HTTPS.

- Abilitare le connessioni TLS tra l'app Citrix Workspace e i Virtual Delivery Agent (VDA) completando le seguenti attività:

  - Configurare TLS sui computer in cui sono installati i VDA (per comodità, di seguito le macchine in cui sono installati i VDA saranno semplicemente chiamati "VDA"). Per informazioni generali, vedere Impostazioni TLS sui VDA. Si consiglia vivamente di utilizzare lo script PowerShell fornito da Citrix per configurare TLS/DTLS. Per i dettagli, vedere Configurare TLS su un VDA utilizzando lo script PowerShell. Tuttavia, se si desidera configurare TLS/DTLS manualmente, vedere Configurare manualmente TLS su un VDA.

  - Configurare TLS nei gruppi di consegna contenenti i VDA eseguendo un set di cmdlet PowerShell in Studio. Per i dettagli, vedere Configurare TLS nei gruppi di consegna.

    Requisiti e considerazioni:

    * L'abilitazione delle connessioni TLS tra utenti e VDA è valida solo per i siti XenApp 7.6 e XenDesktop 7.6, oltre alle versioni successive supportate.
    * Configurare TLS nei gruppi di consegna e nelle VDA dopo aver installato i componenti, creato un sito, creato cataloghi di macchine e creato gruppi di consegna.
    * Per configurare TLS nei gruppi di consegna, è necessario disporre dell'autorizzazione per modificare le regole di accesso del controller. Un amministratore completo dispone di questa autorizzazione.

- Per configurare TLS sui VDA, è necessario essere un amministratore di Windows nel computer in cui è installato il VDA.
- Sui VDA in pool di cui viene eseguito il provisioning da Machine Creation Services o Provisioning Services, l'immagine della macchina VDA viene reimpostata al riavvio, causando la perdita delle impostazioni TLS precedenti. Eseguire lo script di PowerShell ogni volta che il VDA viene riavviato per riconfigurare le impostazioni TLS.

> **Avviso:**
>
> Per le attività che includono l'utilizzo del Registro di sistema di Windows, la modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Per informazioni sull'abilitazione di TLS al database del sito, vedere CTX137556.

## Installare i certificati del server TLS nei controller

Per HTTPS, il servizio XML supporta le funzionalità TLS utilizzando i certificati server, non i certificati client. Questa sezione descrive l'acquisizione e l'installazione di certificati TLS nei controller di consegna. Gli stessi passaggi possono essere applicati a Cloud Connectors per crittografare il traffico STA e XML.

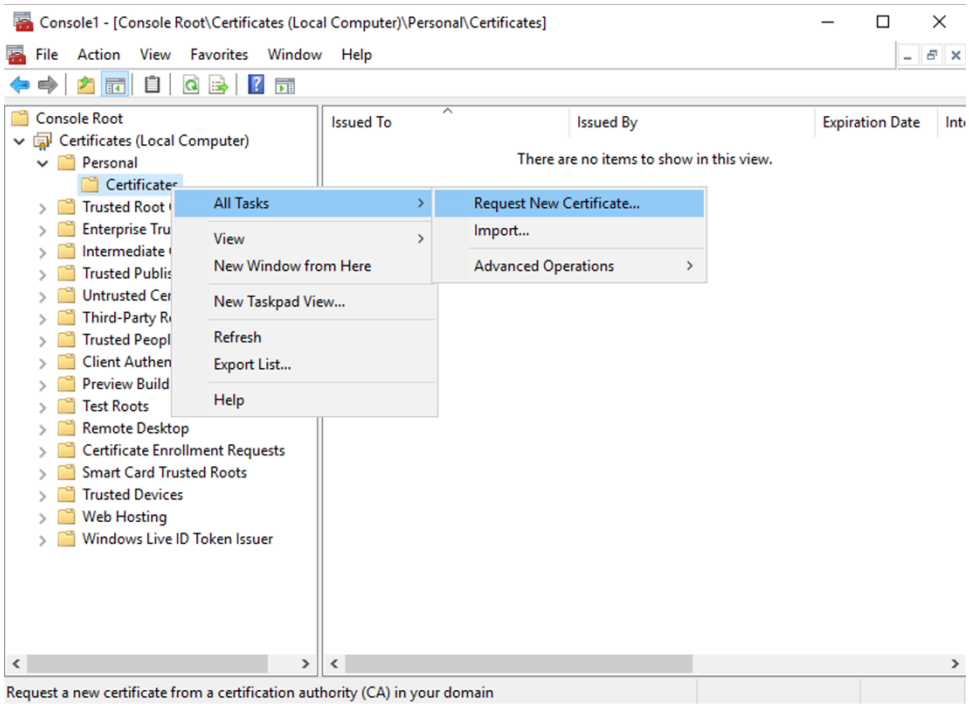
Sebbene esistano diversi tipi di autorità di certificazione e metodi per richiedere il certificato da loro, in questo articolo viene descritta l'Autorità di certificazione Microsoft. L'Autorità di certificazione Microsoft deve disporre di un modello di certificato pubblicato con uno scopo di autenticazione server.

Se l'Autorità di certificazione Microsoft è integrata in un dominio Active Directory o nella foresta attendibile a cui si aggiungono i controller di consegna, è possibile acquisire un certificato dalla procedura guidata Registrazione certificati snap-in Certificati di MMC.

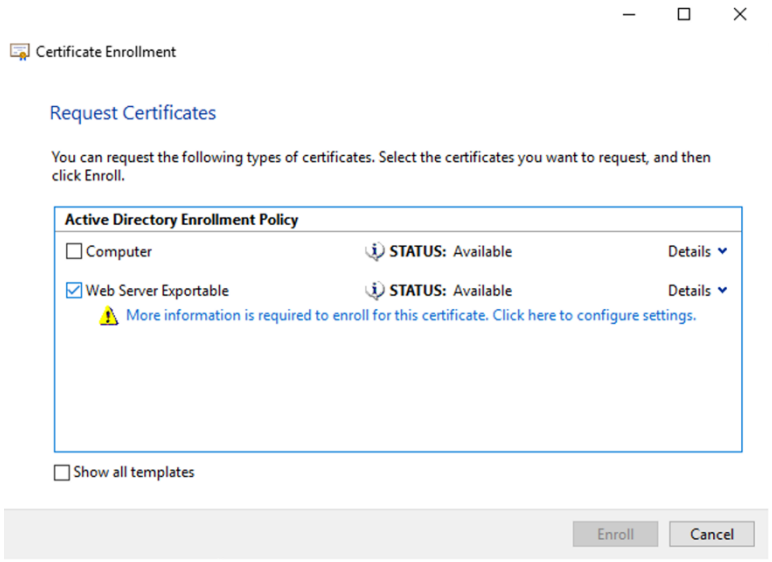
### Richiesta e installazione di un certificato

1. Nel Delivery Controller aprire la console MMC e aggiungere lo snap-in Certificati. Quando richiesto, selezionare Account del computer.
2. Espandere **Personale > Certificati**, quindi utilizzare il comando di menu contestuale **Tutte le attività > Richiedi nuovo certificato** .




3. Fare clic su **Avanti** per iniziare e **Avanti** per confermare che si sta acquisendo il certificato dalla registrazione di Active Directory.
4. Selezionare il modello per il certificato di autenticazione server. Se il modello è stato impostato per fornire automaticamente i valori per Oggetto, è possibile fare clic su **Registra** senza fornire ulteriori dettagli.



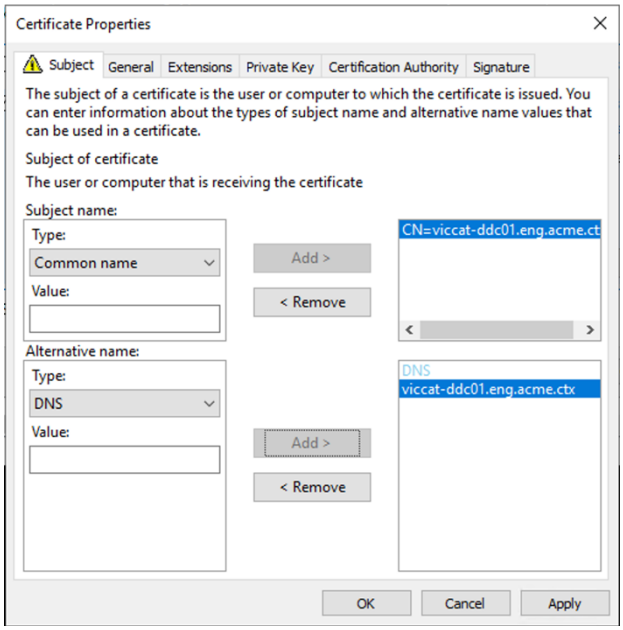

5. Per fornire ulteriori dettagli per il modello di certificato, fare clic sul pulsante freccia **Dettagli** e configurare quanto segue:

   **Nome oggetto**: selezionare Nome comune e aggiungere il nome di dominio completo del De-

livery Controller.

**Nome alternativo**: selezionare DNS e aggiungere il nome di dominio completo del Delivery Controller.




### Configurazione della porta del listener SSL/TLS

1. Aprire una finestra di comando di PowerShell come amministratore del computer.
2. Eseguire i seguenti comandi per ottenere il GUID dell'applicazione del servizio Broker:

```
New-PSDrive -Name HKCR -PSProvider Registry -Root
    HKEY_CLASSES_ROOT

$Service_Guid = Get-ChildItem HKCR:\Installer\Products -Recurse -
    Ea 0 | Where-Object {
  $key = $\_; $\_.GetValueNames() | ForEach-Object {
  $key.GetValue($\_)  }
  | Where-Object {
  $\_ -like 'Citrix Broker Service'  }
   }
  | Select-Object Name

$Service_Guid.Name -match "[A-Z0-9]*$"

$Guid = $Matches[0]

[GUID]$Formatted_Guid = $Guid

Remove-PSDrive -Name HKCR

```

```
19 Write-Host "Broker Service Application GUID: $($Formatted_Guid)" -
       ForegroundColor Yellow
20 <!--NeedCopy-->
```

3. Eseguire i seguenti comandi nella stessa finestra di PowerShell per ottenere l'identificazione personale del certificato installato in precedenza:

```
1 $HostName = ([System.Net.Dns]::GetHostByName(($env:computerName)))
      .Hostname
2
3 $Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-
      Object {
4  $_.Subject -match ("CN=" + $HostName) }
5  ).Thumbprint -join ';'
6
7 Write-Host -Object "Certificate Thumbprint for $($HostName): $(
      $Thumbprint)" -Foreground Yellow
8 <!--NeedCopy-->
```

4. Eseguire i seguenti comandi nella stessa finestra di PowerShell per configurare la porta SSL/TLS del servizio Broker e utilizzare il certificato per la crittografia:

```
1 $IPV4_Address = Test-Connection -ComputerName $HostName -Count 1
      | Select-Object -ExpandProperty IPV4Address
2
3 $IPPort = "$($IPV4_Address):443"
4
5 $SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint
      appid={
6  $Formatted_Guid }
7  "
8
9 $SSLxml | netsh
10
11 . netsh http show sslcert
12 <!--NeedCopy-->
```

Se configurato correttamente, l'output dell'ultimo comando `.netsh http show sslcert` evidenzia che il listener utilizza la `IP:port` corretta e che `Application ID` corrisponde al GUID dell'applicazione del servizio Broker.

Se i server considerano attendibile il certificato installato nei controller di consegna, è ora possibile configurare i controller di consegna StoreFront e i binding STA Citrix Gateway in modo da utilizzare HTTPS anziché HTTP.

> **Nota:**
>
> Se il controller è installato in Windows Server 2016 e StoreFront è installato in Windows Server 2012 R2, è necessario apportare una modifica alla configurazione del Controller, per modificare l'ordine dei pacchetti di crittografia TLS. Questa modifica della configurazione non è necessaria

> per Controller e StoreFront con altre combinazioni di versioni di Windows Server.

L'elenco dell'ordine dei pacchetti di crittografia deve includere i pacchetti di crittografia `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` o `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` (o entrambi) e questi pacchetti di crittografia devono precedere eventuali pacchetti di crittografia `TLS_DHE_`.

1. Utilizzando l'Editor Criteri di gruppo Microsoft, andare a **Configurazione computer > Modelli amministrativi > Rete > Impostazioni di configurazione SSL**.
2. Modificare il criterio "Ordine dei pacchetti di crittografia SSL". Per impostazione predefinita, questo criterio è impostato su "Non configurato". Impostare questo criterio su Abilitato.
3. Disporre i pacchetti nell'ordine corretto; rimuovere eventuali pacchetti di crittografia che non si desidera utilizzare.

Assicurarsi che `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` o `TLS_ECDHE_RSA_WITH_AES_128_CB` preceda eventuali pacchetti di crittografia `TLS_DHE_`.

Su Microsoft MSDN, vedere anche Prioritizing Schannel Cipher Suites.

### Modificare le porte HTTP o HTTPS

Per impostazione predefinita, il servizio XML del controller è in ascolto sulla porta 80 per il traffico HTTP e la porta 443 per il traffico HTTPS. Sebbene sia possibile utilizzare porte non predefinite, tenere presenti i rischi per la sicurezza derivanti dall'esposizione di un controller a reti non attendibili. La distribuzione di un server StoreFront standalone è preferibile alla modifica delle impostazioni predefinite.

Per modificare le porte HTTP o HTTPS predefinite utilizzate dal controller, eseguire il seguente comando da Studio:

```
BrokerService.exe -WIPORT \<http-port> -WISSLPORT \<https-port>
```

dove <`http-port`> è il numero di porta per il traffico HTTP e <`https-port`> è il numero di porta per il traffico HTTPS.

> **Nota:**
>
> Dopo aver modificato una porta, Studio potrebbe visualizzare un messaggio relativo alla compatibilità delle licenze e all'aggiornamento. Per risolvere il problema, registrare nuovamente le istanze del servizio utilizzando la seguente sequenza di cmdlet PowerShell:

```
1 Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding
     XML_HTTPS |
2 Unregister-ConfigRegisteredServiceInstance
3 Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
```

```
Register-ConfigServiceInstance
<!--NeedCopy-->
```

#### Applicare solo il traffico HTTPS

Se si desidera che il servizio XML ignori il traffico HTTP, creare la seguente impostazione del Registro di sistema in HKLM\Software\Citrix\DesktopServer\ sul controller e quindi riavviare il servizio Broker.

Per ignorare il traffico HTTP, creare DWORD XmlServicesEnableNonSsl e impostarlo su 0.

È possibile creare un valore DWORD del Registro di sistema corrispondente per ignorare il traffico HTTPS: DWORD XmlServicesEnableSsl. Assicurarsi che non sia impostato su 0.

### Impostazioni TLS sui VDA

Un gruppo di consegna non può avere una combinazione di alcuni VDA con TLS configurato e altri VDA senza TLS configurato. Prima di configurare TLS per un gruppo di consegna, assicurarsi di aver già configurato TLS per tutti i VDA in tale gruppo di consegna

Quando si configura TLS sui VDA, le autorizzazioni per il certificato TLS installato vengono modificate, dando al servizio ICA l'accesso in lettura alla chiave privata del certificato e informando il servizio ICA dei seguenti elementi:

- **Quale certificato presente nell'archivio certificati utilizzare per TLS**.
- **Quale numero di porta TCP utilizzare per le connessioni TLS**.

  Windows Firewall (se abilitato) deve essere configurato per consentire la connessione in ingresso su questa porta TCP. Questa configurazione viene eseguita automaticamente quando si utilizza lo script PowerShell.
- **Quali versioni del protocollo TLS consentire.**

  > **Importante:**
  >
  > Citrix consiglia di esaminare il proprio utilizzo di SSLv3 e riconfigurare tali distribuzioni per rimuovere il supporto per SSLv3, ove appropriato. Vedere CTX200238.

  Le versioni del protocollo TLS supportate seguono una gerarchia (da inferiore a superiore): SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3. Specificare la versione minima consentita. Sono consentite tutte le connessioni di protocollo che utilizzano tale versione o una versione superiore.

  Ad esempio, se si specifica TLS 1.1 come versione minima, sono consentite connessioni di protocollo TLS 1.1 e TLS 1.3. Se si specifica SSL 3.0 come versione minima, sono consentite le connessioni di tutte le versioni supportate. Se si specifica TLS 1.3 come versione minima, sono consentite solo le connessioni TLS 1.3.

DTLS 1.0 corrisponde a TLS 1.1 e DTLS 1.3 corrisponde a TLS 1.3.

- **Quali pacchetti di crittografia TLS consentire.**

  Un pacchetto di crittografia seleziona la crittografia utilizzata per una connessione. I client e i VDA possono supportare diverse serie di pacchetti di crittografia. Quando un client (l'app Citrix Workspace o StoreFront) si connette e invia un elenco di pacchetti di crittografia TLS supportati, il VDA fa corrispondere uno dei pacchetti di crittografia del client a uno dei pacchetti di crittografia presenti nel suo elenco di pacchetti di crittografia configurati e accetta la connessione. Se non esiste un pacchetto di crittografia corrispondente, il VDA rifiuta la connessione.

  Il VDA supporta tre serie di pacchetti di crittografia (noti anche come modalità di conformità): GOV(erno), COM(merciale) e ALL. I pacchetti di crittografia accettabili dipendono anche dalla modalità FIPS di Windows; vedere http://support.microsoft.com/kb/811833 per informazioni sulla modalità FIPS di Windows. La tabella seguente elenca i pacchetti di crittografia di ciascuna serie:

| **Pacchetto di crittografia TLS/DTLS** | **ALL** | **COM** | **GOV** | **ALL** | **COM** | **GOV** |
|---|---|---|---|---|---|---|
| **Modalità FIPS** | Disattivata | Disattivata | Disattivata | Attiva | Attiva | Attiva |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384* | X | | X | X | | X |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | X | | X | X | | X |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | X | | X | X | X | |

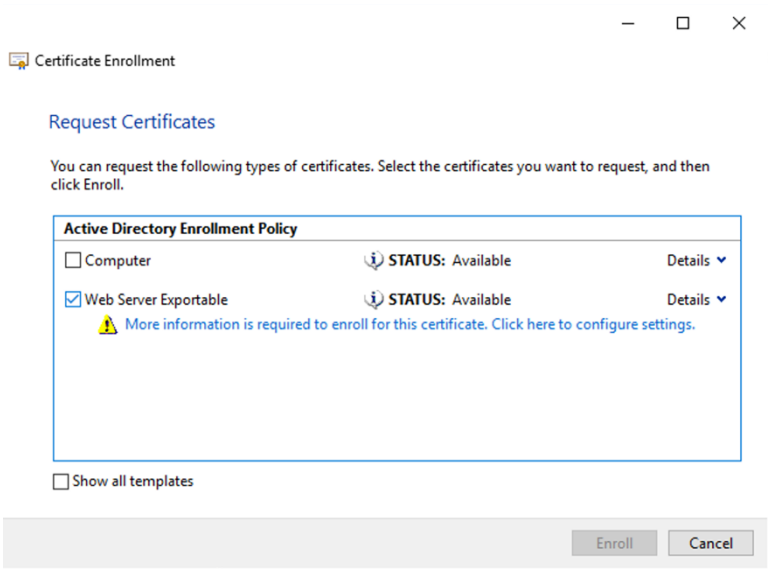
*Non supportata in Windows Server 2012 R2.

> **Nota:**
>
> Il VDA non supporta i pacchetti di crittografia DHE (ad esempio, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 e TLS_DHE_RSA_WITH_AES_128_CBC_SHA). Se selezionati da Windows, potrebbero non essere utilizzati da Receiver.
>
> Se si utilizza un Citrix Gateway, vedere la documentazione di Citrix ADC per informazioni sul supporto dei pacchetti di crittografia per la comunicazione back-end. Per informazioni sul supporto della suite di cifratura TLS, vedere Crittografie disponibili sugli apparecchi Citrix ADC. Per informazioni sul supporto della suite di cifratura DTLS, vedere Supporto della crittografia DTLS.

**Richiesta e installazione di un certificato**

1. Nel VDA, aprire la console MMC e aggiungere lo snap-in Certificati. Quando richiesto, selezionare Account del computer.
2. Espandere **Personal > Certificates**, quindi utilizzare il comando di menu contestuale **All Tasks > Request New Certificate** (Tutte le attività > Richiedi nuovo certificato).
3. Fare clic su **Avanti** per iniziare e **Avanti** per confermare che si sta acquisendo il certificato dalla registrazione di Active Directory.
4. Selezionare il modello per il certificato di autenticazione server. Sia il **computer** Windows predefinito che il **server Web esportabile** sono accettabili. Se il modello è stato impostato per fornire automaticamente i valori del Subject (Oggetto), è possibile fare clic su **Enroll** (Registra) senza fornire ulteriori dettagli.

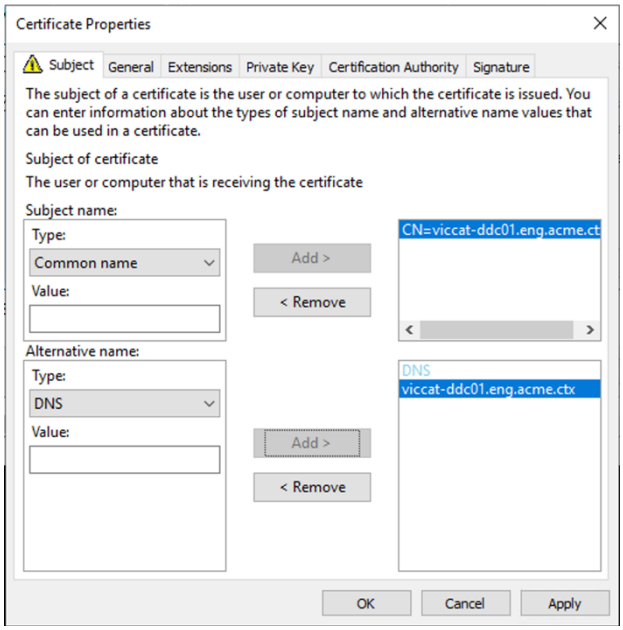



5. Per fornire ulteriori dettagli per il modello di certificato, fare clic su **Details** e configurare quanto segue:

   **Subject name** (Nome oggetto): selezionare il tipo **Common name** (Nome comune) e aggiungere il nome di dominio completo del VDA

   **Alternative name** (Nome alternativo): selezionare il tipo **DNS** e aggiungere il nome di dominio completo del VDA



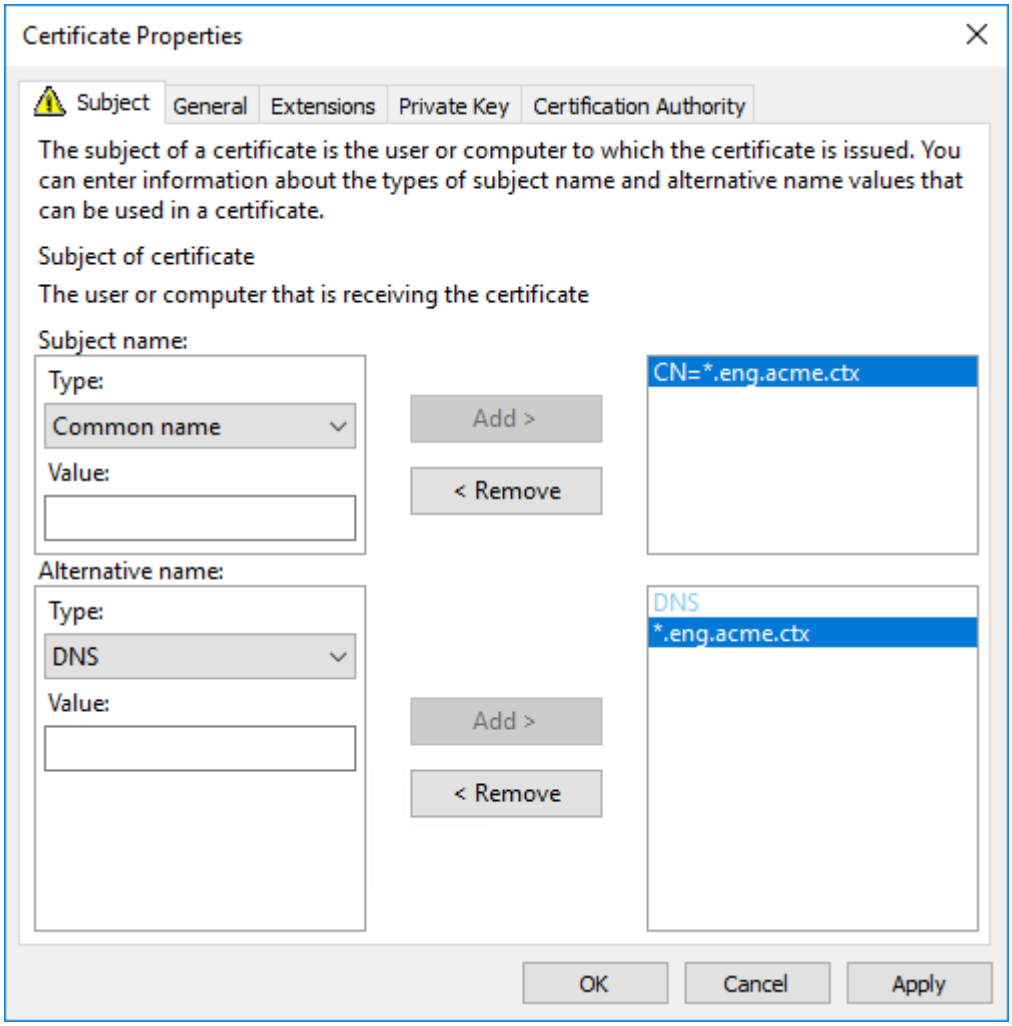

> **Nota:**
>
> Utilizzare la registrazione automatica dei certificati di Active Directory Certificate Services per automatizzare l'emissione e la distribuzione di certificati nei VDA. Questo è descritto in https://support.citrix.com/article/CTX205473.

È possibile utilizzare certificati con caratteri jolly per consentire a un singolo certificato di proteggere più VDA:

**Subject name** (Nome oggetto): selezionare il tipo **Common name** (Nome comune) e immettere il *.primary.domain dei VDA

**Alternative name** (Nome alternativo): selezionare il tipo **DNS** e aggiungere il *.primary.domain dei VDA

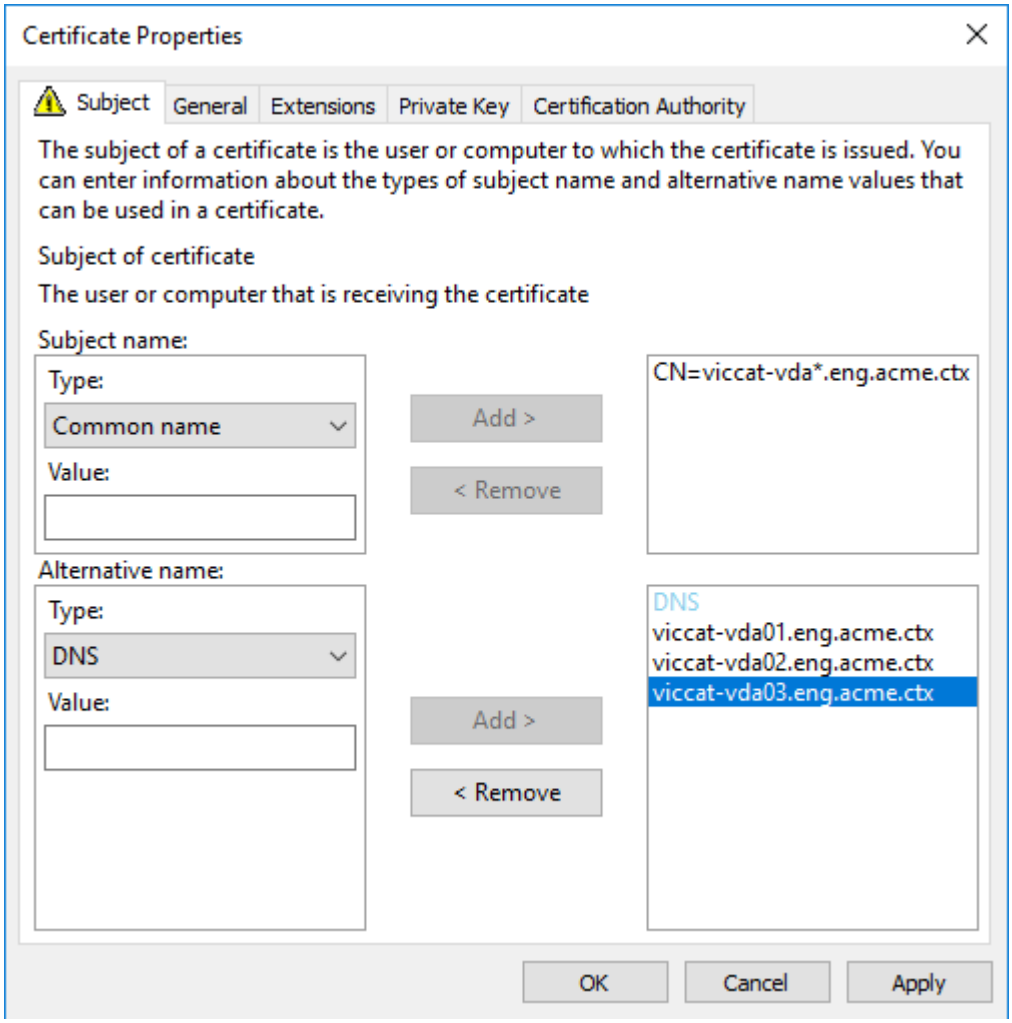



È possibile utilizzare i certificati SAN per consentire a un singolo certificato di proteggere più VDA specifici:

**Subject name** (Nome oggetto): selezionare il tipo **Common name** (Nome comune) e immettere una stringa per aiutare a identificare l'utilizzo del certificato

**Alternative name** (Nome alternativo): selezionare il tipo **DNS** e aggiungere una voce per il nome di dominio completo di ogni VDA. Ridurre al minimo il numero di nomi alternativi per garantire una negoziazione TLS ottimale.

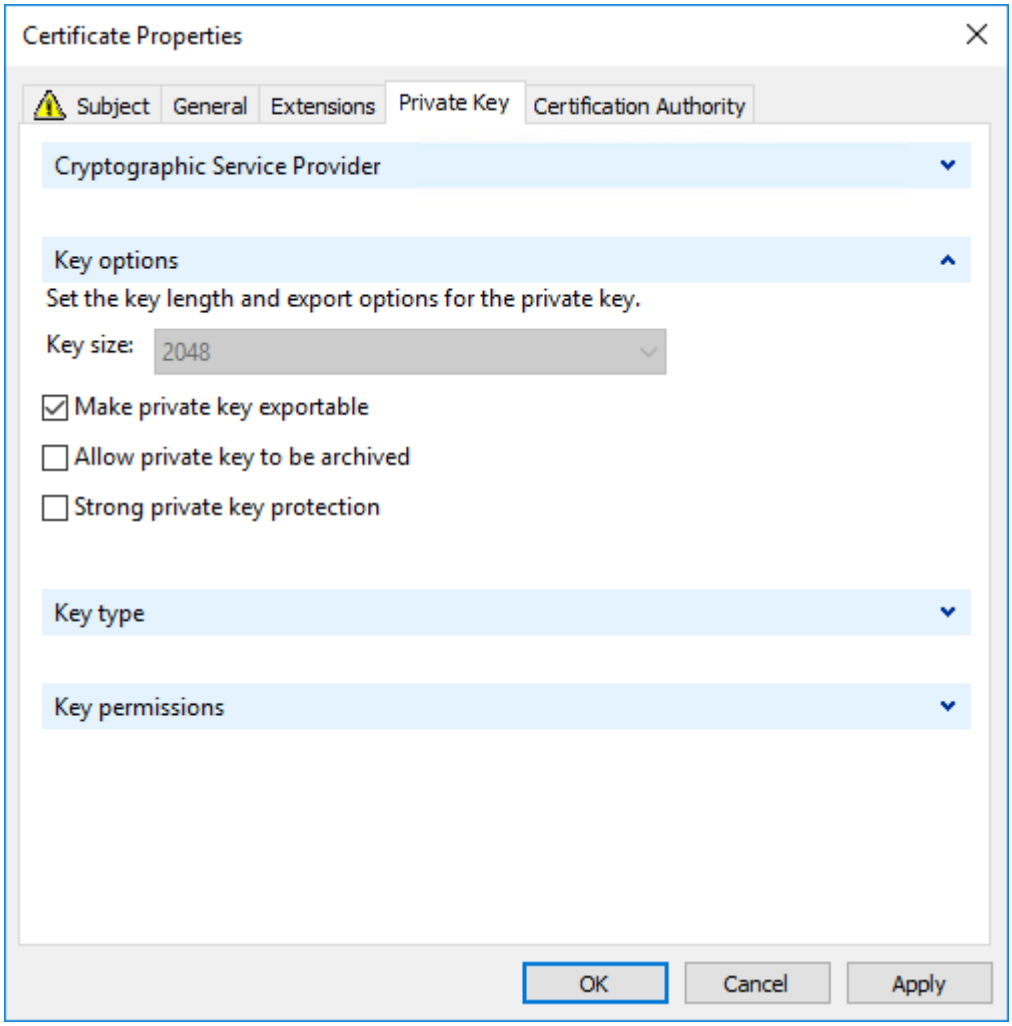
 




**Nota:**

Sia i certificati jolly che i certificati SAN richiedono che sia selezionata l'opzione **Make private key exportable** (Rendi esportabile la chiave privata) nella scheda Private Key:




**Configurare TLS su un VDA utilizzando lo script PowerShell**

Installare il certificato TLS nell'area Computer locale > Personale > Certificati dell'archivio certificati. Se in tale posizione risiedono più certificati, fornire l'identificazione personale del certificato allo script PowerShell.

> **Nota:**
>
> A partire da XenApp e XenDesktop 7.16 LTSR, lo script PowerShell trova il certificato corretto in base al nome di dominio completo del VDA. Non è necessario fornire l'identificazione personale quando è presente un solo certificato per il nome di dominio completo del VDA.

Lo script Enable-VdaSSL.ps1 abilita o disabilita il listener TLS su un VDA. Questo script è disponibile nella cartella *Supporto* > *Strumenti* > *SslSupport* del supporto di installazione.

Quando si abilita TLS, i pacchetti di crittografia DHE sono disattivati. I pacchetti di crittografia ECDHE non sono interessati.

Quando si attiva TLS, lo script disabilita tutte le regole di Windows Firewall esistenti per la porta TCP specificata. Aggiunge quindi una nuova regola che consente al servizio ICA di accettare connessioni in ingresso solo sulle porte TLS TCP e UDP. Disabilita inoltre le regole di Windows Firewall per:

- Citrix ICA (impostazione predefinita: 1494)
- Citrix CGP (impostazione predefinita: 2598)
- Citrix WebSocket (impostazione predefinita: 8008)

L'effetto è che gli utenti possono connettersi solo utilizzando TLS o DTLS. Non possono utilizzare ICA/HDX, ICA/HDX con affidabilità di sessione o HDX su WebSocket, senza TLS o DTLS.

> **Nota:**
>
> DTLS non è supportato con ICA/HDX Audio su UDP Real-Time Transport o con ICA/HDX Framehawk.

Vedere Porte di rete.

Lo script contiene le seguenti descrizioni della sintassi, oltre ad esempi aggiuntivi; è possibile utilizzare uno strumento come Notepad ++ per rivedere queste informazioni.

> **Importante:**
>
> Specificare il parametro Enable o Disable e il parametro CertificateThumbPrint. Gli altri parametri sono facoltativi.

**Sintassi** `Enable-VdaSSL { -Enable | -Disable } -CertificateThumbPrint "<thumbprint>"[-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]`

| Parametro | Descrizione |
|---|---|
| Abilita | Installa e abilita il listener TLS sul VDA. Questo parametro o il parametro Disable è obbligatorio. |
| Disable | Disattiva il listener TLS sul VDA. Questo parametro o il parametro Enable è obbligatorio. Se si specifica questo parametro, non sarà valido nessun altro parametro. |

| Parametro | Descrizione |
| --- | --- |
| CertificateThumbPrint “” | Identificazione personale del certificato TLS nell'archivio certificati, racchiuso tra virgolette. Lo script utilizza l'identificazione personale specificata per selezionare il certificato che si desidera utilizzare. Se questo parametro viene omesso, viene selezionato un certificato non corretto. |
| SSLPort | Porta TLS. Predefinito: 443 |
| SSLMinVersion “” | Versione minima del protocollo TLS, racchiusa tra virgolette. Valori validi: “TLS_1.0” (impostazione predefinita), “TLS_1.1”e “TLS_1.3”. |
| SSLCipherSuite “” | Pacchetto di crittografia TLS, racchiuso tra virgolette. Valori validi: “GOV”, “COM”e “ALL” (impostazione predefinita). |

**Esempi** Lo script seguente installa e abilita il valore di versione del protocollo TLS. L'identificazione personale (rappresentata da “12345678987654321”in questo esempio) viene utilizzata per selezionare il certificato da utilizzare.

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

Lo script seguente installa e abilita il listener TLS e specifica la porta TLS 400, il pacchetto di crittografia GOV e un valore minimo del protocollo TLS 1.2. L'identificazione personale (rappresentata da “12345678987654321”in questo esempio) viene utilizzata per selezionare il certificato da utilizzare.

```
Enable-VdaSSL -Enable
-CertificateThumbPrint "12345678987654321"
-SSLPort 400 -SSLMinVersion "TLS_1.3"
-SSLCipherSuite "All"
```

Lo script seguente disabilita il listener TLS sul VDA.

```
Enable-VdaSSL -Disable
```

#### Configurare manualmente TLS su un VDA

Quando si configura manualmente TLS su un VDA, si concede l'accesso in lettura generico alla chiave privata del certificato TLS per il servizio appropriato su ogni VDA: NT SERVICE\PorticaService per un

VDA per il sistema operativo Windows a sessione singola o NT SERVICE\TermService per un VDA per sistema operativo multisessione Windows. Sulla macchina in cui è installato il VDA:

**PASSAGGIO 1.** Avviare Microsoft Management Console (MMC): Start > Esegui > mmc.exe.

**PASSAGGIO 2.** Aggiungere lo snap-in Certificati a MMC:

1. Selezionare File > Aggiungi/Rimuovi snap-in.
2. Selezionare Certificati, quindi fare clic su Aggiungi.
3. Quando viene visualizzata la richiesta "Lo snap-in gestirà sempre certificati per:"scegliere "Account del computer"e quindi fare clic su Avanti.
4. Quando viene visualizzata la richiesta "Selezionare il computer da gestire con lo snap-in" scegliere "Computer locale", quindi fare clic su Fine.

**PASSAGGIO 3**. In Certificati (computer locale) > Personale > Certificati fare clic con il pulsante destro del mouse sul certificato e quindi selezionare Tutte le attività > Gestisci chiavi private.

**PASSAGGIO 4.** Nell'Editor dell'elenco di controllo di accesso è visualizzato "Permissions for (FriendlyName) private keys"(Autorizzazioni per chiavi private di (FriendlyName)) dove (FriendlyName) è il nome del certificato TLS. Aggiungere uno dei seguenti servizi e assegnargli l'accesso in lettura:

- Per un VDA per sistema operativo Windows a sessione singola, "PORTICASERVICE"
- Per un VDA per sistema operativo Windows multisessione, "TERMSERVICE"

**PASSAGGIO 5.** Fare doppio clic sul certificato TLS installato. Nella finestra di dialogo del certificato, selezionare la scheda Dettagli e quindi scorrere verso il basso. Fare clic su Identificazione personale.

**PASSAGGIO 6.** Eseguire regedit e passare a HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.

1. Modificare la chiave di identificazione personale SSL e copiare il valore dell'identificazione personale del certificato TLS in questo valore binario. È possibile ignorare senza problemi gli elementi sconosciuti presenti nella finestra di dialogo Modifica valore binario (ad esempio "0000" e caratteri speciali).
2. Modificare la chiave SSLEnabled e impostare il valore DWORD su 1. Per disabilitare SSL in un secondo momento, impostare il valore DWORD su 0.
3. Se si desidera modificare le impostazioni predefinite (facoltativo), utilizzare quanto segue nello stesso percorso del Registro di sistema:

   SSLPort DWORD —numero di porta SSL. Predefinito: 443.

   SSLMinVersion DWORD –1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.3. Predefinito: 2 (TLS 1.0).

   SSLCipherSuite DWORD —1 = GOV, 2 = COM, 3 = ALL. Predefinito: 3 (ALL).

**PASSAGGIO 7.** Assicurarsi che le porte TLS TCP e UDP siano aperte in Windows Firewall se non sono la 443 predefinita. Quando si crea la regola in ingresso in Windows Firewall, assicurarsi che le relative proprietà abbiano le voci "Consenti connessione"e "Abilitato"selezionate.

**PASSAGGIO 8.** Verificare che nessun'altra applicazione o servizio (ad esempio IIS) stia utilizzando la porta TLS TCP.

**PASSAGGIO 9.** Per i VDA per il sistema operativo Windows multisessione, riavviare il computer affinché le modifiche abbiano effetto. Non è necessario riavviare i computer contenenti VDA per il sistema operativo Windows a sessione singola.

> **Importante:**
>
> È necessario un passaggio aggiuntivo quando il VDA è in Windows Server 2012 R2, Windows Server 2016 o Windows 10 Anniversary Edition o versione successiva supportata. Ciò influisce sulle connessioni da Citrix Receiver per Windows (versioni da 4.6 a 4.9), dall'app Citrix Workspace per HTML5 e dall'app Citrix Workspace per Chrome. Sono incluse anche le connessioni che utilizzano Citrix Gateway.
>
> Questo passaggio è necessario anche per tutte le connessioni che utilizzano Citrix Gateway, per tutte le versioni di VDA, se è configurato TLS tra Citrix Gateway e il VDA. Ciò influisce su tutte le versioni di Citrix Receiver.

Nel VDA (Windows Server 2012 R2, Windows Server 2016 o Windows 10 Anniversary Edition o versione successiva), utilizzando l'Editor Criteri di gruppo, accedere a Configurazione computer> Criteri > Modelli amministrativi > Rete > Impostazioni di configurazione SSL > Ordine dei pacchetti di crittografia SSL. Selezionare il seguente ordine:

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

> **Nota:**
>
> I primi sei elementi specificano anche la curva ellittica, P384 o P256. Assicurarsi che "curve25519"non sia selezionato. La modalità FIPS non impedisce l'uso di "curve25519" .

Quando questa impostazione di Criteri di gruppo è configurata, il VDA seleziona un pacchetto di crittografia solo se viene visualizzato in entrambi gli elenchi: l'elenco Criteri di gruppo e l'elenco per la modalità di conformità selezionata (COM, GOV o ALL). Il pacchetto di crittografia deve essere visualizzato anche nell'elenco inviato dal client (app Citrix Workspace o StoreFront).

Questa configurazione di Criteri di gruppo influisce anche su altre applicazioni e servizi TLS sul VDA. Se le applicazioni richiedono pacchetti di crittografia specifici, potrebbe essere necessario aggiungerle a questo elenco di Criteri di gruppo.

> **Importante:**
>
> Anche se le modifiche ai Criteri di gruppo vengono visualizzate quando vengono applicate, le modifiche apportate ai Criteri di gruppo per la configurazione TLS hanno effetto solo dopo il riavvio del sistema operativo. Pertanto, nel caso dei desktop in pool, applicare le modifiche ai Criteri di gruppo per la configurazione TLS all'immagine di base.

#### Configurare TLS nei gruppi di consegna

Completare questa procedura per ogni gruppo di consegna contenente VDA configurati per le connessioni TLS.

1. Da Studio aprire la console PowerShell.
2. Eseguire **asnp Citrix.*** per caricare i cmdlet del prodotto Citrix.
3. Eseguire **Get-BrokerAccessPolicyRule -DesktopGroupName '*<nome-gruppo di consegna>*'| Set-BrokerAccessPolicyRule -HdxSslEnabled $true**.
4. Eseguire **Set-BrokerSite -DnsResolutionEnabled $true**.

#### Risoluzione dei problemi

Se si verifica un errore di connessione, controllare il registro eventi di sistema sul VDA.

Quando si utilizza l'app Citrix Workspace per Windows, se viene visualizzato un errore di connessione che indica un errore TLS, disabilitare Desktop Viewer e quindi riprovare a connettersi. Sebbene la connessione non riesca ancora, potrebbe essere fornita una spiegazione del problema TLS sottostante. Ad esempio, è stato specificato un modello non corretto al momento di richiedere un certificato all'autorità di certificazione.

La maggior parte delle configurazioni che utilizzano HDX Adaptive Transport funziona correttamente con DTLS, incluse quelle che utilizzano le versioni più recenti dell'app Citrix Workspace, di Citrix Gateway e del VDA. Alcune configurazioni che utilizzano DTLS tra l'app Citrix Workspace e Citrix Gateway e che utilizzano DTLS tra Citrix Gateway e il VDA richiedono ulteriori azioni.

È necessaria un'azione aggiuntiva se:

- La versione Citrix Receiver supporta HDX Adaptive Transport e DTLS: Receiver per Windows (4.7, 4.8, 4.9), Receiver per Mac (12.5, 12.6, 12.7), Receiver per iOS (7.2, 7.3.x) o Receiver per Linux (13.7)

e si applica anche una delle seguenti condizioni:

- la versione Citrix Gateway supporta DTLS nel VDA, ma la versione VDA non supporta DTLS (versione 7.15 o precedente),
- la versione VDA supporta DTLS (versione 7.16 o successiva), ma la versione Citrix Gateway non supporta DTLS per VDA.

Per evitare che le connessioni che partono da Citrix Receiver non funzionino, effettuare una delle seguenti operazioni:

- aggiornare Citrix Receiver a Receiver per Windows versione 4.10 o successiva, Receiver per Mac 12.8 o versioni successive o Receiver per iOS versione 7.5 o successiva; oppure
- aggiornare Citrix Gateway a una versione che supporti DTLS nel VDA; oppure
- aggiornare il VDA alla versione 7.16 o successiva; oppure
- disabilitare DTLS al VDA; oppure
- disabilitare HDX Adaptive Transport.

> **Nota:**
>
> Un aggiornamento adatto per Receiver per Linux non è ancora disponibile. Receiver per Android (versione 3.12.3) non supporta HDX Adaptive Transport e DTLS tramite Citrix Gateway e pertanto non è interessato.
>
> Per disattivare DTLS sul VDA, modificare la configurazione del firewall del VDA in modo da disabilitare la porta UDP 443. Vedere Porte di rete.

### Comunicazione tra Controller e VDA

La protezione a livello di messaggio Windows Communication Framework (WCF) protegge la comunicazione tra il controller e il VDA. Non è richiesta una protezione supplementare a livello di trasporto tramite TLS. La configurazione WCF utilizza Kerberos per l'autenticazione reciproca tra il controller e il VDA. La crittografia utilizza AES in modalità CBC con una chiave a 256 bit. L'integrità dei messaggi utilizza SHA-1.

Secondo Microsoft, i protocolli di sicurezza utilizzati da WCF sono conformi agli standard di OASIS (Organization for the Advancement of Structured Information Standards), tra cui WS-SecurityPolicy 1.2. Inoltre, Microsoft afferma che WCF supporta tutti i pacchetti di algoritmi elencati in Security Policy 1.2.

La comunicazione tra il Controller e il VDA utilizza il pacchetto di algoritmi basic256, i cui algoritmi sono come indicato sopra.

#### Reindirizzamento video TLS e HTML5 e reindirizzamento dei contenuti del browser

È possibile utilizzare il reindirizzamento video HTML5 e il reindirizzamento dei contenuti del browser per reindirizzare i siti Web HTTPS. Il JavaScript inserito in tali siti Web deve stabilire una connessione TLS al servizio di reindirizzamento video HTML5 Citrix HDX in esecuzione sul VDA. A tale scopo, il servizio di reindirizzamento video HTML5 genera due certificati personalizzati nell'archivio certificati presente sul VDA. L'arresto del servizio rimuove i certificati.

Il criterio di reindirizzamento video HTML5 è disabilitato per impostazione predefinita.

Il reindirizzamento del contenuto del browser è abilitato per impostazione predefinita.

Per ulteriori informazioni sul reindirizzamento video HTML5, vedere Impostazioni dei criteri multimediali.

## Transport Layer Security (TLS) su Universal Print Server

January 7, 2024

Il protocollo TLS (Transport Layer Security) è supportato per le connessioni basate su TCP tra Virtual Delivery Agent (VDA) e Universal Print Server.

> **Avviso:**
>
> Per le attività che includono l'utilizzo del Registro di sistema di Windows, la modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

### Tipi di connessioni di stampa tra VDA e Universal Print Server

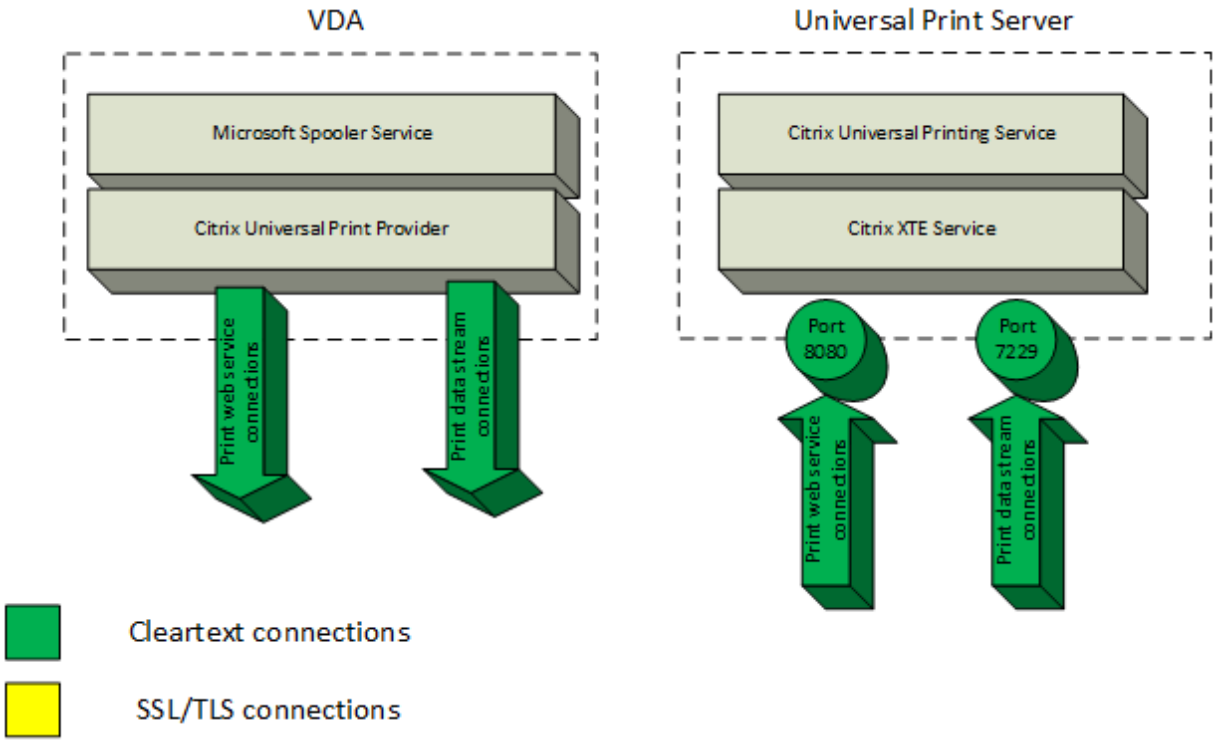
#### Connessioni in formato Cleartext

Le seguenti connessioni relative alla stampa provengono dal VDA e si connettono alle porte di Universal Print Server. Queste connessioni vengono effettuate solo quando il criterio **SSL enabled** (abilitato SSL) è impostato su **Disabled** (impostazione predefinita).

- Connessioni del servizio Web di stampa Cleartext (porta TCP 8080)
- Connessioni (CGP) del flusso di dati di stampa Cleartext (porta TCP 7229)

Nell'articolo del supporto tecnico Microsoft Panoramica del servizio e requisiti delle porte di rete per Windows vengono descritte le porte utilizzate dal servizio spooler di stampa di Microsoft Windows. Le impostazioni SSL/TLS di cui a questo documento non si applicano alle connessioni NETBIOS e RPC effettuate dal servizio Spooler di stampa Windows. Il VDA utilizza il provider di stampa di rete Windows (win32spl.dll) come fallback se il criterio di **Universal Print Server enable** (Abilitazione di Universal Print Server) è impostato su **Enabled with fallback to Windows'native remote printing** (Abilitato con fallback alla stampa remota nativa di Windows).

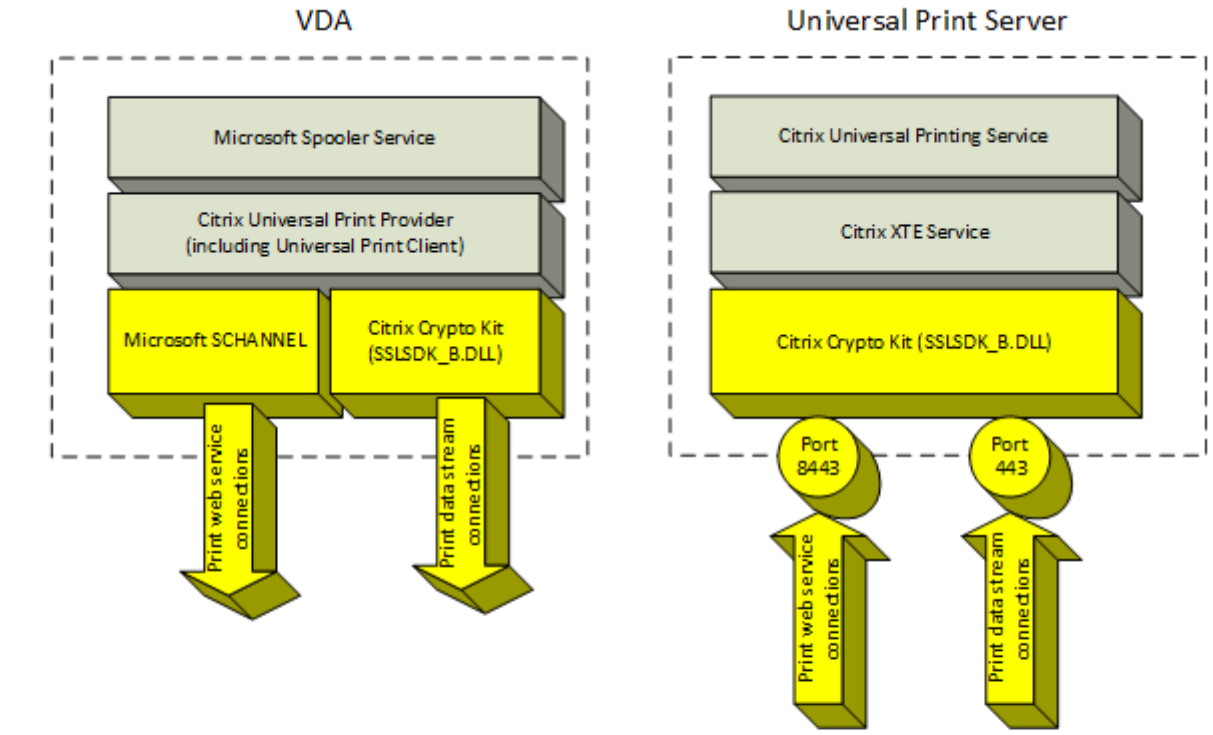


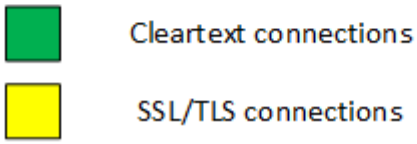

**Connessioni crittografate**

Queste connessioni SSL/TLS relative alla stampa provengono dal VDA e si connettono alle porte dell' Universal Print Server. Queste connessioni vengono effettuate solo quando il criterio **SSL enabled** è impostato su **Enabled**.

- Connessioni di servizio Web di stampa crittografate (porta TCP 8443)
- Connessioni (CGP) del flusso di dati di stampa crittografate (porta TCP 443)




**Configurazione client SSL/TLS**

Il VDA funziona come client SSL/TLS.

Utilizzare Criteri di gruppo Microsoft e il Registro di sistema per configurare Microsoft SCHANNEL SSP per le connessioni crittografate al servizio Web di stampa (porta TCP 8443). Nell'articolo del supporto tecnico Microsoft TLS Registry Settings vengono descritte le impostazioni del Registro di sistema per Microsoft SCHANNEL SSP.

Utilizzando l'Editor Criteri di gruppo su VDA (Windows Server 2016 o Windows 10), andare a **Configurazione computer> Modelli amministrativi > Rete > Impostazioni di configurazione SSL > Ordine dei pacchetti di crittografia SSL**. Selezionare il seguente ordine:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> **Nota:**
>
> Quando è configurata questa impostazione di Criteri di gruppo, il VDA seleziona un pacchetto di crittografia per le connessioni del servizio Web di stampa crittografate (porta predefinita: 8443) solo se le connessioni vengono visualizzate in entrambi gli elenchi dei pacchetti di crittografia SSL:
>
> - Elenco degli ordini dei pacchetti di crittografia SSL di Criteri di gruppo
> - Elenco corrispondente all'impostazione dei criteri dei pacchetti di crittografia SSL selezionati (COM, GOV o ALL)
>
> Questa configurazione di Criteri di gruppo influisce anche su altre applicazioni e servizi TLS sul VDA. Se le applicazioni richiedono pacchetti di crittografia specifici, potrebbe essere necessario aggiungerle a questo elenco di ordine dei pacchetti di crittografia dei Criteri di gruppo.
>
> **Importante:**
>
> Le modifiche apportate ai Criteri di gruppo per la configurazione TLS hanno effetto solo dopo il riavvio del sistema operativo.
>
> Utilizzare un criterio Citrix per configurare le impostazioni SSL/TLS per le connessioni (CGP) del flusso di dati di stampa crittografate (porta TCP 443).

#### Configurazione server SSL/TLS

Universal Print Server funziona come server SSL/TLS.

Utilizzare lo script `Enable-UpsSsl.ps1` PowerShell per configurare le impostazioni SSL/TLS.

#### Installare il certificato del server TLS su Universal Print Server

Per HTTPS, Universal Print Server supporta le funzionalità TLS utilizzando certificati server. I certificati client non vengono utilizzati. Utilizzare Servizi certificati Active Directory Microsoft o un'altra autorità di certificazione per richiedere un certificato per Universal Print Server.

Tenere presente le seguenti considerazioni quando si registra/richiede un certificato utilizzando Servizi certificati Active Directory Microsoft:

1. Inserire il certificato nell'archivio certificati **personali** del computer locale.

2. Impostare l'attributo **Nome comune** del nome distinto del soggetto (DN) del certificato sul nome di dominio completo (FQDN) di Universal Print Server. Specificare questo valore nel modello di certificato.
3. Impostare il provider di servizi di crittografia (CSP) utilizzato per generare la richiesta di certificato e la chiave privata per **Microsoft Enhanced RSA e AES Cryptographic Provider (Encryption)**. Specificare questo valore nel modello di certificato.
4. Impostare la dimensione della chiave su almeno 2048 bit. Specificare questo valore nel modello di certificato.

### Configurazione di SSL su Universal Print Server

Il servizio XTE su Universal Print Server è in ascolto delle connessioni in ingresso. Funziona come server SSL quando SSL è abilitato. Le connessioni in ingresso sono di due tipi: connessioni al servizio Web di stampa, che contengono comandi di stampa, e connessioni del flusso di dati di stampa, che contengono processi di stampa. SSL può essere abilitato su queste connessioni. SSL protegge la riservatezza e l'integrità di queste connessioni. Per impostazione predefinita, SSL è disabilitato.

Lo script PowerShell utilizzato per configurare SSL si trova sul supporto di installazione e ha il nome di file seguente: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1`.

### Configurare i numeri di porta di ascolto su Universal Print Server

Queste sono le porte predefinite per il servizio XTE:

- Porta TCP del servizio Web di stampa Cleartext (HTTP): 8080
- Porta TCP del flusso di dati di stampa (CGP): 7229
- Porta TCP del servizio Web di stampa crittografato (HTTPS): 8443
- Porta TCP del flusso di dati di stampa (CGP) crittografato: 443

Per modificare le porte utilizzate dal servizio XTE su Universal Print Server, eseguire i seguenti comandi in PowerShell come amministratore (vedere la sezione successiva per le note sull'utilizzo dello script PowerShell Enable-UpsSsl.ps1):

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` o `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

### Impostazioni TLS su Universal Print Server

Se si dispone di più server di stampa universali in una configurazione con bilanciamento del carico, assicurarsi che le impostazioni TLS siano configurate in modo coerente su tutti gli Universal Print Server.

Quando si configura TLS su Universal Print Server, le autorizzazioni per il certificato TLS installato vengono modificate, dando al servizio di stampa universale l'accesso in lettura alla chiave privata del certificato e informando il servizio di stampa universale dei seguenti elementi:

- Quale certificato presente nell'archivio certificati utilizzare per TLS.
- Quali numeri di porta TCP utilizzare per le connessioni TLS.

Windows Firewall (se abilitato) deve essere configurato per consentire le connessioni in ingresso su queste porte TCP. Questa configurazione viene eseguita per l'utente quando si utilizza lo script PowerShell Enable-UpsSsl.ps1.

- Quali versioni del protocollo TLS consentire.

Universal Print Server supporta i protocolli TLS versioni 1.2, 1.1 e 1.0. Specificare la versione minima consentita.

La versione predefinita del protocollo TLS è 1.2.

- Quali pacchetti di crittografia TLS consentire.

Un pacchetto di crittografia seleziona gli algoritmi crittografici utilizzati per una connessione. I VDA e Universal Print Server possono supportare diversi set di pacchetti di crittografia. Quando un VDA si connette e invia un elenco di pacchetti di crittografia TLS supportati, Universal Print Server fa corrispondere uno dei pacchetti di crittografia del client a uno dei pacchetti di crittografia presenti nel proprio elenco di pacchetti di crittografia configurati e accetta la connessione. Se non esiste un pacchetto di crittografia corrispondente, Universal Print Server rifiuta la connessione.

Universal Print Server supporta i seguenti set di pacchetti di crittografia denominati GOV(erno), COM(merciale) e ALL per le modalità OPEN, FIPS e SP800-52 nativo Crypto Kit. I pacchetti di crittografia accettabili dipendono anche dall'impostazione dei criteri **Modalità FIPS SSL** e dalla modalità FIPS di Windows. Per informazioni sulla modalità FIPS di Windows, vedere questo articolo del supporto Microsoft.

| Pacchetto di crittografia (in ordine di priorità decrescente) | OPEN ALL | OPEN COM | OPEN GOV | FIPS ALL | FIPS COM | FIPS GOV | SP800-52 ALL | SP800-52 COM | SP800-52 GOV |
|---|---|---|---|---|---|---|---|---|---|
| TLS_ECDHE_RSA_AES256_GCM_SHA384 | X | | | X | | X | X | | X |
| TLS_ECDHE_RSA_AES256_CBC_SHA384 | X | | | X | | X | X | | X |
| TLS_ECDHE_RSA_AES256_CBC_SHA | X | | | X | X | | X | X | |

**Configurare TLS su un Universal Print Server utilizzando lo script PowerShell**

Installare il certificato TLS nell'area **Computer locale > Personale > Certificati** dell'archivio certificati. Se in tale posizione risiedono più certificati, fornire l'identificazione personale del certificato allo script `Enable-UpsSsl.ps1` PowerShell.

> **Nota:**
>
> Lo script PowerShell trova il certificato corretto in base al nome di dominio completo di Universal Print Server. Non è necessario fornire l'identificazione personale del certificato quando è presente un solo certificato per il nome di dominio completo di Universal Print Server.

Lo script `Enable-UpsSsl.ps1` abilita o disabilita le connessioni TLS provenienti dal VDA verso Universal Print Server. Questo script è disponibile nella cartella **Supporto > Strumenti > SslSupport** del supporto di installazione.

Quando si attiva TLS, lo script disabilita tutte le regole di Windows Firewall esistenti per le porte TCP dello Universal Print Server. Aggiunge quindi nuove regole che consentono al servizio XTE di accettare le connessioni in ingresso solo sulle porte TLS TCP e UDP. Disabilita inoltre le regole di Windows Firewall per:

- Connessioni del servizio Web di stampa in formato Cleartext (impostazione predefinita: 8080)
- Connessioni (CGP) del flusso di dati di stampa in formato Cleartext (impostazione predefinita: 7229)

L'effetto è che il VDA può effettuare queste connessioni solo quando si utilizza TLS.

> **Nota:**
>
> L'attivazione di TLS non influisce sulle connessioni RPC/SMB dello spooler di stampa Windows originate dal VDA e che vanno a Universal Print Server.
>
> **Importante:**
>
> Specificare **Enable** o **Disable** come primo parametro. Il parametro CertificateThumbprint è facoltativo se solo un certificato contenuto nell'archivio certificati del Personal Computer locale dispone del nome di dominio completo dello Universal Print Server. Gli altri parametri sono facoltativi.

### Sintassi

```
1 Enable-UpsSSL.ps1 -Enable [-HTTPPort <port>] [-CGPPort <port>] [-
      HTTPSPort <port>] [-CGPSSLPort <port>] [-SSLMinVersion <version>] [-
      SSLCipherSuite <name>] [-CertificateThumbprint <thumbprint>] [-
      FIPSMode <Boolean>] [-ComplianceMode <mode>]
2 Enable-UpsSSL.ps1 -Disable [-HTTPPort <portnum>] [-CGPPort <portnum>]
```

| Parametro | Descrizione |
|---|---|
| Abilita | Abilita SSL/TLS sul server XTE. Questo parametro o il parametro Disable è obbligatorio. |
| Disable | Disattiva SSL/TLS sul server XTE. Questo parametro o il parametro Enable è obbligatorio. |
| CertificateThumbprint "<thumbprint>" | Identificazione personale del certificato TLS nell'archivio certificati personali del computer locale, racchiuso tra virgolette. Lo script utilizza l'identificazione personale specificata per selezionare il certificato che si desidera utilizzare. |
| HTTPPort <port> | Porta del servizio Web di stampa Cleartext (HTTP/SOAP). Predefinito: 8080 |
| CGPPort <port> | Porta (CGP) del flusso di dati di stampa Cleartext. Predefinito: 7229 |
| HTTPSPort <port> | Porta del servizio Web di stampa crittografato (HTTPS/SOAP). Predefinito: 8443 |
| CGPSSLPort <port> | Porta (CGP) del flusso di dati di stampa crittografato. Predefinito: 443 |

| Parametro | Descrizione |
| --- | --- |
| SSLMinVersion "<version>" | Versione minima del protocollo TLS, racchiusa tra virgolette. Valori validi: “TLS_1.0”, “TLS_1.1” e “TLS_1.2”. Impostazione predefinita: TLS_1.2. |
| SSLCipherSuite "<name>" | Nome del pacchetto di crittografia TLS, racchiuso tra virgolette. Valori validi: “GOV”, “COM”e “ALL”(impostazione predefinita). |
| FIPSMode <Boolean> | Attiva o disabilita la modalità FIPS 140 nel server XTE. Valori validi: $true per abilitare la modalità FIPS 140, $false per disabilitare la modalità FIPS 140. |

#### Esempi

Lo script seguente abilita TLS. L’identificazione personale (rappresentata da “12345678987654321”in questo esempio) viene utilizzata per selezionare il certificato da utilizzare.

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

Lo script seguente disabilita TLS.

```
Enable-UpsSsl.ps1 –Disable
```

### Configurazione della modalità FIPS

L’abilitazione della modalità FIPS (Federal Information Processing Standards) degli Stati Uniti garantisce che venga utilizzata solo la crittografia compatibile con FIPS 140 per le connessioni crittografate di Universal Print Server.

Configurare la modalità FIPS sul server prima di configurare la modalità FIPS sul client.

Vedere il sito della documentazione di Microsoft per l’attivazione/disattivazione della modalità FIPS di Windows.

#### Attivazione della modalità FIPS sul client

Sul Delivery Controller, eseguire Web Studio e impostare l’impostazione del criterio **SSL FIPS Mode** Citrix su **Enabled**. Abilitare il criterio Citrix.

Eseguire questa operazione su ciascun VDA:

1. Attivare la modalità FIPS di Windows.
2. Riavviare il VDA.

#### Attivazione della modalità FIPS sul server

Eseguire questa operazione su ciascun Universal Print Server:

1. Attivare la modalità FIPS di Windows.
2. Eseguire questo comando PowerShell come amministratore: `stop-service CitrixXTEServer, UpSvc`
3. Eseguire lo script `Enable-UpsSsl.ps1` con i parametri `-Enable -FIPSMode $true`.
4. Riavviare Universal Print Server.

#### Disabilitazione della modalità FIPS sul client

In Web Studio impostare l'impostazione del criterio **SSL FIPS Mode** Citrix su **Disabled**. Abilitare il criterio Citrix. È inoltre possibile eliminare l'impostazione del criterio Citrix **SSL FIPS Mode**.

Eseguire questa operazione su ciascun VDA:

1. Disattivare la modalità FIPS di Windows.
2. Riavviare il VDA.

#### Disattivare la modalità FIPS sul server

Eseguire questa operazione su ciascun Universal Print Server:

1. Disattivare la modalità FIPS di Windows.
2. Eseguire questo comando PowerShell come amministratore: `stop-service CitrixXTEServer, UpSvc`
3. Eseguire lo script `Enable-UpsSsl.ps1` con i parametri `-Enable -FIPSMode $false`.
4. Riavviare Universal Print Server.

### Configurare la versione del protocollo SSL/TLS

La versione predefinita del protocollo SSL/TLS è TLS 1.2. TLS 1.2 è l'unica versione del protocollo SSL/TLS consigliata per l'uso in produzione. Per la risoluzione dei problemi, potrebbe essere necessario modificare temporaneamente la versione del protocollo SSL/TLS in un ambiente non di produzione.

SSL 2.0 e SSL 3.0 non sono supportati su Universal Print Server.

#### Impostare la versione del protocollo SSL/TLS sul server

Eseguire questa operazione su ciascun Universal Print Server:

1. Eseguire questo comando PowerShell come amministratore: `stop-service CitrixXTEServer , UpSvc`
2. Eseguire lo script `Enable-UpsSsl.ps1` con i parametri di versione `-Enable -SSLMinVersion`. Ricordare di reimpostarlo su TLS 1.2 al termine del test.
3. Riavviare Universal Print Server.

#### Impostare la versione del protocollo SSL/TLS sul client

Eseguire questa operazione su ciascun VDA:

1. Nel Delivery Controller, impostare il criterio **SSL Protocol Version** (Versione protocollo SSL) sulla versione di protocollo desiderata e abilitare il criterio.
2. Nell'articolo del supporto tecnico Microsoft TLS Registry Settings vengono descritte le impostazioni del Registro di sistema per Microsoft SCHANNEL SSP. Abilitare il lato client **TLS 1.0, TLS 1.1 o TLS 1.2** utilizzando le impostazioni del Registro di sistema.

   > **Importante:**
   >
   > Ricordare di ripristinare le impostazioni del Registro di sistema ai valori originali al termine del test.

3. Riavviare il VDA.

### Risoluzione dei problemi

Se si verifica un errore di connessione, controllare il file di registro C:\Programmi (x86)\Citrix\XTE\logs\error.log sullo Universal Print Server.

Il messaggio di errore **SSL handshake from client failed** (Handshake SSL dal client non riuscito) viene visualizzato in questo file di registro se l'handshake SSL/TLS non riesce. Tali errori possono verificarsi se la versione del protocollo SSL/TLS sul VDA e quella sull'Universal Print Server non corrispondono.

Utilizzare il nome di dominio completo di Universal Print Server nelle seguenti impostazioni dei criteri che contengono nomi host di Universal Print Server:

- Session printers (Stampanti di sessione)
- Printer assignments (Assegnazioni stampante)
- Universal Print Servers for load balancing (Universal Print Server per il bilanciamento del carico)

Verificare che il clock di sistema (data, ora e fuso orario) sia corretto sugli Universal Print Server e sui VDA.

## Sicurezza dei canali virtuali

January 7, 2024

Per impostazione predefinita, la funzione Virtual channel allow list (Elenco degli elementi consentiti dei canali virtuali) è abilitata. Di conseguenza, solo i canali virtuali Citrix possono essere aperti nelle sessioni delle app e dei desktop virtuali. Se è necessario utilizzare canali virtuali personalizzati, sviluppati internamente o di terze parti, questi devono essere aggiunti esplicitamente all'elenco dei consentiti.

### Aggiungere canali virtuali all'elenco dei consentiti

Per aggiungere un canale virtuale all'elenco dei consentiti, è necessario:

1. Il nome del canale virtuale definito nel codice, che può contenere fino a sette caratteri. Ad esempio, `CTXCVC1`.
2. I percorsi dei processi che aprono il canale virtuale sulla macchina VDA. Ad esempio, `C:\Program Files\Application\run.exe`.

Una volta che si dispone delle informazioni richieste, è necessario aggiungere il canale virtuale all'elenco consentiti utilizzando l'impostazione dei criteri Elenco consentiti canali virtuali. Per aggiungere un canale virtuale all'elenco, immettere il nome del canale virtuale seguito da una virgola e quindi il percorso del processo che accede al canale virtuale. Se sono presenti più processi, questi possono essere aggiunti separati da virgole.

Utilizzando gli esempi precedenti, è necessario aggiungere all'elenco quanto segue:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

Se sono presenti più processi, è necessario aggiungere all'elenco quanto segue:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

È supportato l'uso di caratteri jolly (*). È possibile utilizzare i caratteri jolly quando i nomi delle directory o degli eseguibili cambiano in base alla versione dell'applicazione o se il componente di terze parti viene installato nei profili degli utenti.

È possibile utilizzare i caratteri jolly per quanto segue:

- Per sostituire il nome completo della directory. Ad esempio: `C:\Program Files\Application\*\run1.exe`
- Per sostituire parte del nome della directory. Ad esempio: `C:\Program Files\Application\v*\run1.exe`
- Per sostituire il nome dell'eseguibile. Ad esempio: `C:\Program Files\Application\v1.2\*.exe`
- Per sostituire parte del nome dell'eseguibile. Ad esempio: `C:\Program Files\Application\v1.2\run*.exe`

Si applicano le seguenti restrizioni:

- Il carattere jolly può essere utilizzato solo per sostituire una singola directory. Ad esempio, se l'eseguibile si trova in `C:\Program Files\Application\v1.2\run1.exe`
  - Consentiti: `C:\Program Files\Application\*\run1.exe`
  - Non consentiti: `C:\Program Files\*\run1.exe`
- Le voci devono contenere l'estensione del file.
  - Consentiti: `C:\Program Files\Application\v1.2\*.exe`
  - Non consentiti: `C:\Program Files\Application\v1.2\*`
- Tutti i percorsi devono essere locali.

> **Nota:**
>
> I percorsi di rete non sono consentiti dalla versione CVAD 2109 in poi.

### Considerazioni sui canali virtuali Citrix

Tutti i canali virtuali Citrix integrati sono affidabili e possono essere aperti senza ulteriori configurazioni. Tuttavia, ci sono due funzionalità che richiedono voci esplicite nell'elenco dei consentiti a causa di dipendenze esterne:

- Reindirizzamento multimediale
- HDX RealTime Optimization Pack per Skype for Business

#### Reindirizzamento multimediale

Per l'inserimento nell'elenco consentiti sono necessarie queste informazioni:

- Nome del canale virtuale: CTXMM
- Processo: percorso del lettore multimediale utilizzato nella macchina VDA. Ad esempio C:\Programmi (x86)\Windows Media Player\wmplayer.exe

- Inserimento nell'elenco consentiti: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

#### HDX RealTime Optimization Pack per Skype for Business

Per l'inserimento nell'elenco consentiti sono necessarie queste informazioni:

- Nome del canale virtuale: CTXRMEP
- Processo: percorso per l'eseguibile Skype for Business nel computer VDA, che può variare nelle diverse versioni di Skype for Business o se è stato utilizzato un percorso di installazione personalizzato. Ad esempio C:\Programmi\Microsoft Office\root\Office16\lync.exe.
- Inserimento nell'elenco consentiti: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

### Ottenere nomi e processi dei canali virtuali

Il modo più semplice per ottenere il nome del canale virtuale e il processo che lo apre sulla macchina VDA è ottenere le informazioni dallo sviluppatore o dal fornitore di terze parti che ha fornito il canale virtuale.

In alternativa, è possibile ottenere queste informazioni applicando i registri della funzionalità e seguendo questi passaggi:

1. Una volta installati i componenti client e server del canale virtuale personalizzato, avviare un'applicazione virtuale o un desktop virtuale.
2. Nel registro eventi di sistema della macchina VDA, cercare il nome del canale virtuale personalizzato e il processo che ha tentato di aprirlo nel seguente evento:
    - In un VDA a sessione singola, ID evento 2002 dall'origine Picadd.
    - In un VDA multisessione, ID evento 14 dall'origine Rpm.
3. Scollegarsi dalla sessione.
4. Aggiungere una voce nell'impostazione del criterio dell'elenco di elementi consentiti del canale virtuale per il canale virtuale e il processo identificati.
5. Avviare l'applicazione virtuale o il desktop virtuale per verificare che il canale virtuale personalizzato si apra correttamente.

### Il canale virtuale consente la registrazione dell'elenco

I seguenti eventi vengono registrati nel registro eventi della macchina VDA a sessione singola:

| | |
|---|---|
| Nome del registro | Sistema |
| ID | 2001 |
| Origine | Picadd |
| Livello | Informazioni |
| Descrizione | Il canale virtuale personalizzato <vcName> è stato aperto per processo <processName> |

| | |
|---|---|
| Nome del registro | Sistema |
| ID | 2002 |
| Origine | Picadd |
| Livello | Avviso |
| Descrizione | Il canale virtuale personalizzato <vcName> non può essere aperto dal processo <processName> |

| | |
|---|---|
| Nome del registro | Sistema |
| ID | 2003 |
| Origine | Picadd |
| Livello | Informazioni |
| Descrizione | <username> ha aperto il canale virtuale personalizzato <vcName> |

| | |
|---|---|
| Nome del registro | Sistema |
| ID | 2004 |
| Origine | Picadd |
| Livello | Avviso |
| Descrizione | <username> ha provato ad aprire il canale virtuale personalizzato <vcName> |

I seguenti eventi vengono registrati nel registro eventi della macchina VDA multisessione:

| | |
|---|---|
| Nome del registro | Sistema |
| ID | 13 |
| Origine | Rpm |
| Livello | Informazioni |
| Descrizione | Il canale virtuale personalizzato <vcName> è stato aperto per processo <processName> |

| | |
|---|---|
| Nome del registro | Sistema |
| ID | 14 |
| Origine | Rpm |
| Livello | Avviso |
| Descrizione | Il canale virtuale personalizzato <vcName> non può essere aperto dal processo <processName> |

| | |
|---|---|
| Nome del registro | Sistema |
| ID | 15 |
| Origine | Rpm |
| Livello | Informazioni |
| Descrizione | <username> ha aperto il canale virtuale personalizzato <vcName> |

| | |
|---|---|
| Nome del registro | Sistema |
| ID | 16 |
| Origine | Rpm |
| Livello | Avviso |
| Descrizione | <username> ha provato ad aprire il canale virtuale personalizzato <vcName> |

### Canali virtuali di terze parti noti

Di seguito sono riportate le soluzioni di terze parti note che utilizzano canali virtuali Citrix personalizzati. Questo elenco non include tutte le soluzioni che utilizzano un canale virtuale Citrix personalizzato.

- Cerner
- Cisco WebEx Teams
- Software desktop virtuale Cisco WebEx Meetings
- Epic Warp Drive
- Estensioni client Midmark IQPath
- Estensioni client Nuance PowerMic
- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings per VDI
- Ultima IA-Connect

Per ottenere informazioni dettagliate sull'aggiunta dei canali virtuali associati all'elenco consentiti, rivolgersi ai fornitori delle soluzioni. In alternativa, attenersi alla procedura descritta nella sezione Ottenere nomi e processi dei canali virtuali.

## Trasporto HDX

January 7, 2024

Citrix HDX rappresenta un ampio set di tecnologie che offrono un'esperienza ad alta definizione agli utenti di applicazioni e desktop centralizzati, su qualsiasi dispositivo e su qualsiasi rete.

HDX è progettato in base a tre principi tecnici:

- Reindirizzamento intelligente
- Compressione adattiva
- Deduplicazione dei dati

Applicati in diverse combinazioni, questi ottimizzano l'IT e l'esperienza utente, riducono il consumo di larghezza di banda e aumentano la densità degli utenti per server di hosting.

All'interno dell'offerta HDX, è possibile connettersi tramite un protocollo di trasporto esclusivo e proprietario, utilizzare il numero massimo di unità di trasmissione per stabilire le sessioni e ottimizzare la connettività con Citrix SD-WAN.

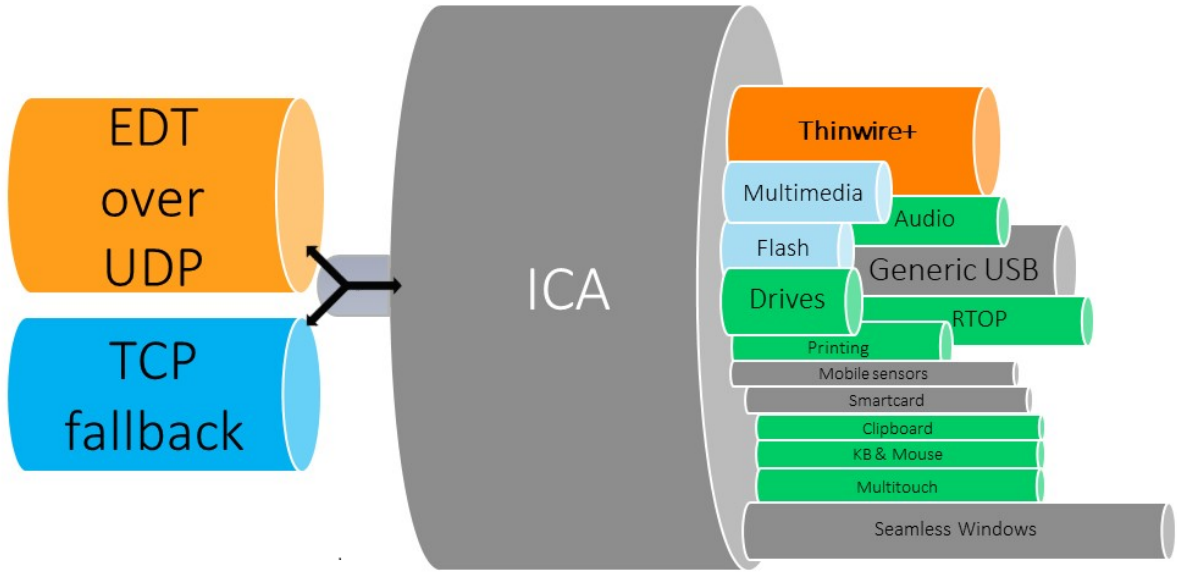
## Trasporto adattivo

January 7, 2024

Adaptive Transport (Trasporto adattivo) è un meccanismo di Citrix Virtual Apps and Desktops che offre la possibilità di utilizzare Enlightened Data Transport (EDT) come protocollo di trasporto per le connessioni ICA. Adaptive Transport (Trasporto adattivo) passa a TCP quando EDT non è disponibile.

EDT è un protocollo di trasporto proprietario di Citrix basato su User Datagram Protocol (UDP). Offre un'esperienza utente superiore su connessioni impegnative a lungo raggio, mantenendo al contempo la scalabilità del server. EDT migliora il throughput dei dati per tutti i canali virtuali ICA su reti inaffidabili, offrendo un'esperienza utente migliore e più coerente.

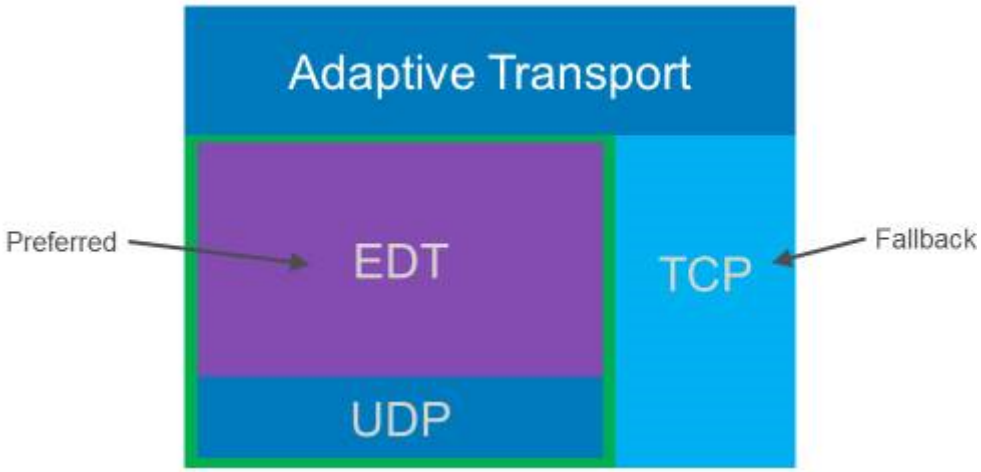



Quando Adaptive Transport (Trasporto adattivo) è impostato su **Preferred** (Preferito), EDT viene utilizzato come protocollo di trasporto principale e TCP viene utilizzato per il fallback. Per impostazione predefinita, Adaptive Transport (Trasporto adattivo) è impostato su **Preferred** (Preferito). È possibile impostare Adaptive Transport (Trasporto adattivo) sulla **modalità Diagnostica** per scopi di test, il che consente solo EDT e disabilita il fallback su TCP.

Con l'app Citrix Workspace per Windows, Mac e iOS, si cerca di stabilire le connessioni EDT e TCP in parallelo durante la connessione iniziale, la riconnessione dell'affidabilità della sessione e la riconnessione automatica del client. In questo modo si riduce il tempo di connessione se il trasporto UDP sottostante non è disponibile e deve essere utilizzato TCP. Se Adaptive Transport (Trasporto adattivo) è impostato su **Preferred** (Preferito) e la connessione viene stabilita tramite TCP, Adaptive Transport (Trasporto adattivo) continua a tentare di passare a EDT ogni cinque minuti.

Con l'app Citrix Workspace per Linux e Android, vengono tentate prima le connessioni EDT. Se la connessione non ha esito positivo, l'app Citrix Workspace tenta di connettersi tramite TCP dopo il timeout della richiesta EDT.




### Requisiti di sistema

Di seguito sono riportati i requisiti per l'utilizzo di Adaptive Transport (Trasporto adattivo) e EDT:

- Piano di controllo
  - Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops)
  - Citrix Virtual Apps and Desktops 1912 o versioni successive
- Virtual Delivery Agent
  - Versione 1912 o successiva (consigliata 2203 o successiva)
  - La versione 2012 è il minimo richiesto per l'utilizzo di EDT con Citrix Gateway Service
- StoreFront
  - Versione 3.12.x
  - Versione 1912.0.x
- App Citrix Workspace
  - Windows: versione 2105 o successiva
  - Linux: versione 2109 o successiva
  - Mac: versione 2108 o successiva
  - iOS: ultima versione disponibile nell'Apple App Store
  - Android: ultima versione disponibile in Google Play
- Citrix Gateway (ADC)
  - 13.1.17.42 o successivo (consigliato)
  - 13.0.52.24 o versioni successive
  - 12.1.56.22 o versioni successive

- Firewall (dal punto di vista del VDA)
  - UDP 1494 in entrata, se l'affidabilità della sessione è disabilitata
  - UDP 2598 in entrata, se l'affidabilità della sessione è abilitata
  - UDP 443 in entrata, se l'SSL del VDA è abilitato per la crittografia ICA (DTLS)
  - UDP 443 in uscita, se si utilizza il servizio Citrix Gateway. Per ulteriori informazioni, consultare la documentazione del servizio Citrix Gateway.

### Considerazioni

- Abilitare l'affidabilità della sessione per utilizzare EDT MTU Discovery (Rilevamento MTU EDT) e utilizzare EDT con Citrix Gateway e il servizio Citrix Gateway.
- Assicurarsi che l'MTU EDT sia adeguatamente impostata per evitare la frammentazione. In caso contrario, le prestazioni potrebbero peggiorare o le sessioni potrebbero non essere avviate in alcune situazioni. Per ulteriori informazioni, vedere la sezione EDT MTU Discover.
- Per informazioni dettagliate su requisiti e considerazioni sull'utilizzo di EDT con il servizio Citrix Gateway, vedere HDX Adaptive Transport con supporto EDT per il servizio Citrix Gateway.
- Per informazioni dettagliate sulla configurazione di Citrix Gateway per supportare EDT, vedere Configurare Citrix Gateway per supportare Enlightened Data Transport e HDX Insight.
- IPv6 non è attualmente supportato.

### Configurazione

Adaptive Transport (Trasporto adattivo) è abilitato per impostazione predefinita. È possibile configurare le seguenti opzioni utilizzando l'impostazione **HDX Adaptive Transport** (Trasporto adattivo HDX) nel criterio Citrix.

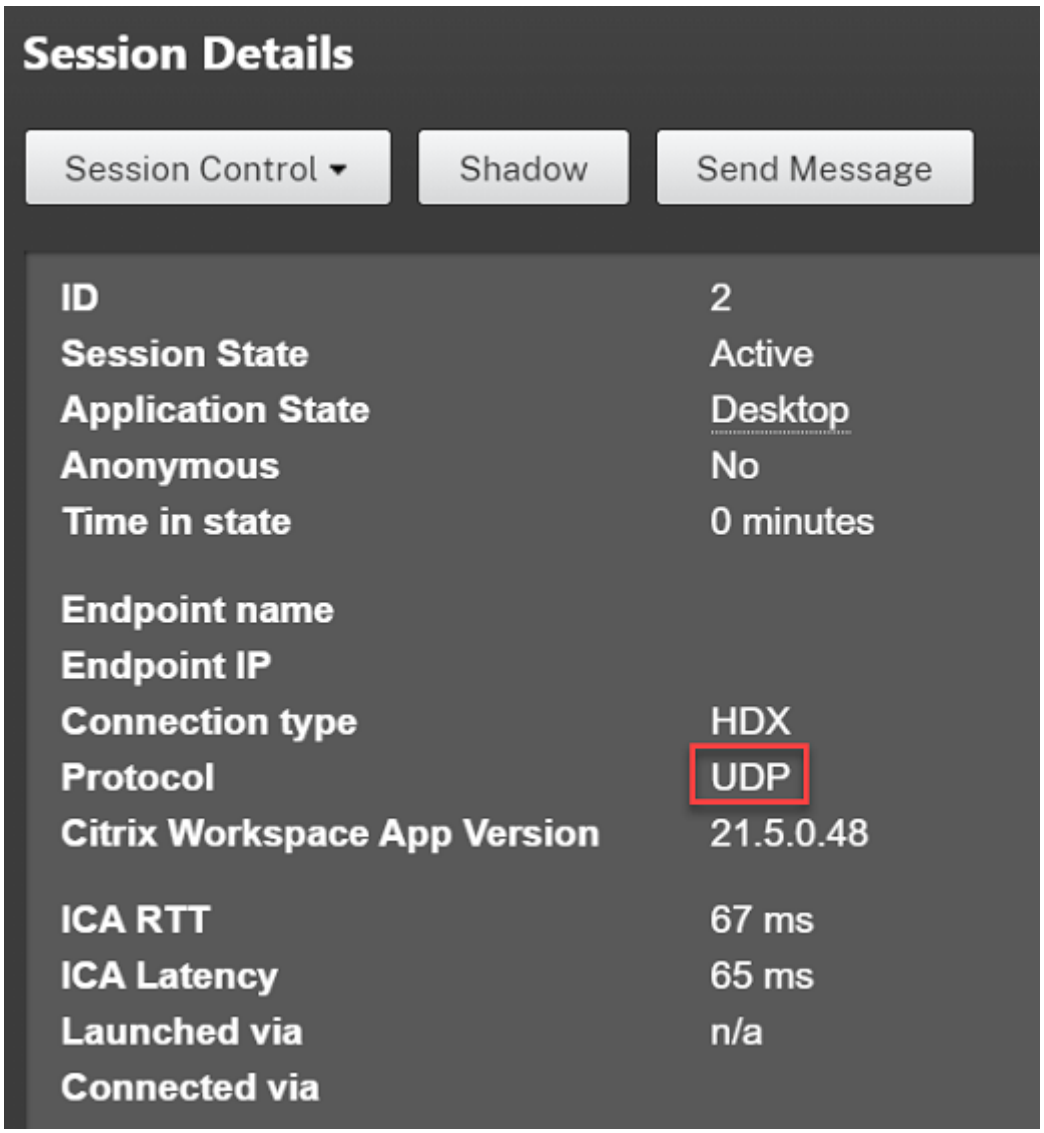
- **Preferred** (Preferito). Questa è l'impostazione predefinita. Adaptive Transport (Trasporto adattivo) è abilitato e utilizza EDT come protocollo di trasporto preferito, con fallback su TCP.
- **Diagnostic mode** (Modalità diagnostica). Adaptive Transport (Trasporto adattivo) è abilitato e forza l'uso di EDT. Il fallback su TCP è disabilitato. Questa impostazione è consigliata solo per il testing e la risoluzione dei problemi.
- **Off**. Adaptive Transport (Trasporto adattivo) è disabilitato e per il trasporto viene utilizzato solo TCP.

Per confermare che EDT viene utilizzato come protocollo di trasporto per la sessione, è possibile utilizzare Director o l'utilità della riga di comando CtxSession.exe sul VDA.

In Director, cercare la sessione e selezionare **Details** (Dettagli). Se **Connection type** (Tipo di connessione) è impostato su **HDX** e **Protocol** (Protocollo) su **UDP**, viene utilizzato EDT come protocollo di trasporto per la sessione. Se **Connection type** (Tipo di connessione) è impostato su **RDP**, ICA non è

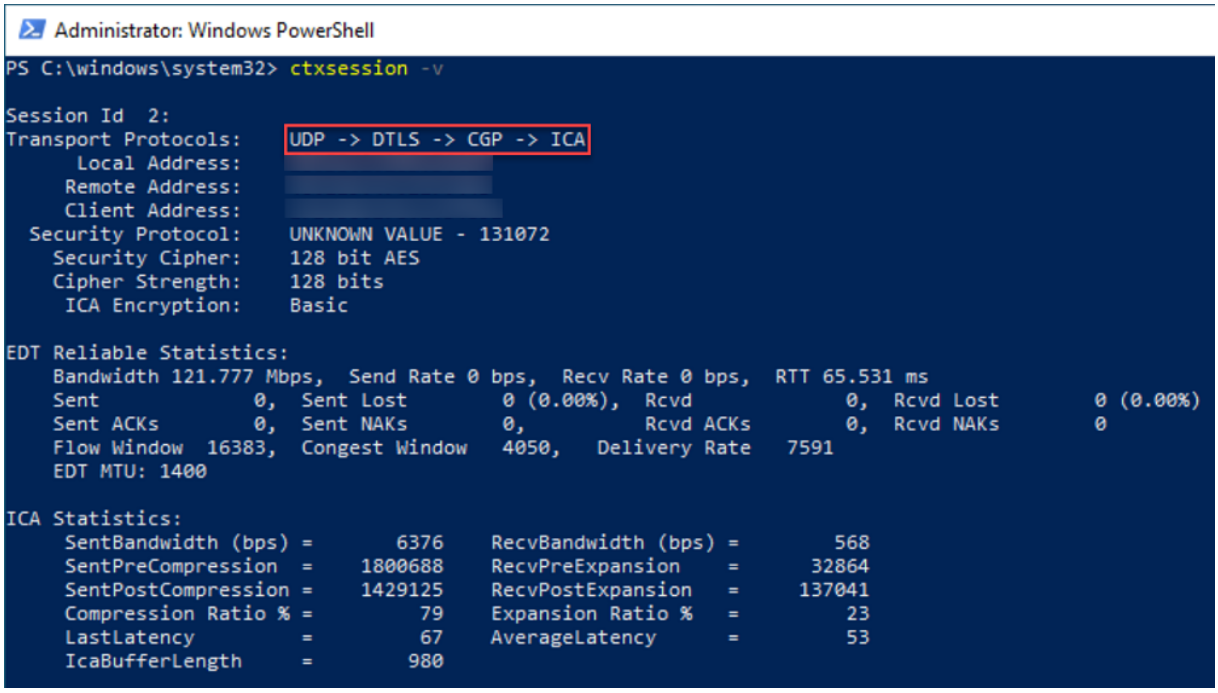
in uso e il campo **Protocol** (Protocollo) visualizza N/A. Per ulteriori informazioni, vedere Monitorare le sessioni.




Per utilizzare l'utilità CtxSession.exe, avviare un prompt dei comandi o PowerShell all'interno della sessione ed eseguire `ctxsession.exe`. Per visualizzare statistiche dettagliate, eseguire `ctxsession.exe -v`. Se EDT è in uso, il protocollo di trasporto mostra uno dei valori seguenti:

- **UDP > ICA** (affidabilità della sessione disabilitata)
- **UDP > CGP > ICA** (affidabilità della sessione abilitata)
- **UDP > DTLS > CGP > ICA** (a ICA è applicata la crittografia DTLS end-to-end)




### EDT MTU Discovery (Rilevamento MTU EDT)

MTU Discovery (Rilevamento MTU) consente a EDT di determinare automaticamente l'unità di trasmissione massima (MTU) quando si stabilisce una sessione. In questo modo si evita la frammentazione dei pacchetti EDT che potrebbe comportare un deterioramento delle prestazioni o l'impossibilità di stabilire una sessione.

> **Importante:**
>
> - L'affidabilità della sessione deve essere abilitata per consentire a MTU Discovery di funzionare.
> - MTU Discovery con Multi-Stream ICA è disponibile con VDA versione 2209 e successive.

#### Per controllare EDT MTU Discovery (Rilevamento MTU EDT) sul VDA

MTU Discovery (Rilevamento MTU) è abilitato per impostazione predefinita. Per disabilitare questa funzionalità, eliminare il valore del Registro di sistema **EDT MTU Discovery** (Rilevamento MTU EDT) e riavviare il VDA. Per ulteriori informazioni, vedere l'impostazione EDT MTU Discovery (Rilevamento MTU EDT) nell'elenco delle funzionalità HDX gestite tramite il Registro di sistema.

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi de-

> rivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

#### Requisiti di sistema

- Citrix Virtual Delivery Agent (VDA) 2003
- App Citrix Workspace 2002 per Windows
- Affidabilità della sessione abilitata. Per ulteriori informazioni sull'affidabilità della sessione, vedere Impostazioni dei criteri di affidabilità delle sessioni.

### Problemi noti

Adaptive Transport (Trasporto adattivo) ed EDT presentano i seguenti problemi:

- La frammentazione dei pacchetti può causare un peggioramento delle prestazioni o addirittura il mancato avvio delle sessioni. È possibile regolare l'MTU EDT per evitare che questo si verifichi. Utilizzare MTU Discovery (Rilevamento MTU) o la soluzione alternativa descritta in CTX231821.
- È possibile che venga visualizzata una schermata grigia o nera quando si avvia una sessione da un client Windows se MTU Discovery (Rilevamento MTU) è abilitato. Per risolvere questo problema, eseguire l'aggiornamento all'app Workspace per Windows 2105 o versioni successive o all'app Workspace per Windows 1912 CU4 o versioni successive.
- Il fallback su TCP potrebbe non riuscire sui client Linux e Android durante la connessione tramite Citrix Gateway o il servizio Citrix Gateway. Questo si verifica quando è presente una negoziazione EDT corretta tra il client e il gateway e la negoziazione EDT non riesce tra il gateway e il VDA. Per risolvere questo problema, eseguire l'aggiornamento all'app Workspace per Linux 2104 o versioni successive e all'app Workspace per Android 21.5 o versioni successive.
- I percorsi di rete asimmetrici possono causare la mancata riuscita di MTU Discovery (Rilevamento MTU) per le connessioni che non passano tramite Citrix Gateway o il servizio Citrix Gateway. Per risolvere questo problema, eseguire l'aggiornamento a VDA versione 2103 o successiva. [CVADHELP-16654]
- Quando si utilizza Citrix Gateway, i percorsi di rete asimmetrici possono impedire il funzionamento di MTU Discovery (Rilevamento MTU). Ciò è dovuto a un problema di Gateway che causa la mancata propagazione del bit Don't Fragment (DF) (Non frammentare) nell'intestazione dei pacchetti EDT. Una correzione per questo problema è disponibile a partire dalla versione 13.1 build 17.42 del firmware. Per informazioni dettagliate su come abilitare la correzione, vedere la documentazione di Citrix Gateway. [CGOP-18438]

- MTU Discovery (Rilevamento MTU) potrebbe non funzionare per gli utenti che si connettono tramite una rete DS-Lite. Alcuni modem non rispettano il bit DF quando l'elaborazione dei pacchetti è abilitata, impedendo a MTU Discovery (Rilevamento MTU) di rilevare la frammentazione. In questa situazione, queste sono le opzioni disponibili:
  - Disabilitare l'elaborazione dei pacchetti sul modem dell'utente.
  - Disabilitare MTU Discovery (Rilevamento MTU) e utilizzare una MTU hardcoded, come descritto in CTX231821.
  - Disabilitare Adaptive Transport (Trasporto adattivo) per obbligare le sessioni a utilizzare TCP. Se solo un sottoinsieme di utenti è interessato, prendere in considerazione la possibilità di disabilitarlo sul lato client in modo che altri utenti possano continuare a utilizzare EDT.

### Risoluzione dei problemi

Per risolvere i problemi relativi ad Adaptive Transport (Trasporto adattivo) ed EDT, suggeriamo quanto segue:

1. Esaminare attentamente e convalidare i requisiti, le considerazionie i problemi noti.
2. Verificare che siano presenti criteri Citrix in Studio o nell'oggetto Criteri di gruppo che sovrascrivono l'impostazione **HDX Adaptive Transport** (Trasporto adattivo HDX) desiderata.
3. Verificare se sul client sono presenti impostazioni che sovrascrivono l'impostazione HDX Adaptive Transport (Trasporto adattivo HDX) desiderata. Può trattarsi di una preferenza dell'oggetto Criteri di gruppo, di un'impostazione configurata utilizzando il modello amministrativo dell'app Workspace opzionale o di una configurazione manuale dell'impostazione **HDXoverUDP** nel Registro di sistema o nel file di configurazione del client.
4. Sui computer VDA multisessione, assicurarsi che i listener UDP siano attivi. Aprire un prompt dei comandi sulla macchina del VDA ed eseguire `netstat -a -p udp`. Per ulteriori informazioni, vedere Come confermare il protocollo HDX Enlightened Data Transport.
5. Avviare una sessione diretta internamente, bypassando Citrix Gateway, e controllare il protocollo in uso. Se la sessione utilizza EDT, il VDA è pronto per utilizzare EDT per le connessioni esterne tramite Citrix Gateway.
6. Se EDT funziona per le connessioni interne dirette e non per le sessioni che passano attraverso Citrix Gateway:
   - Assicurarsi che l'affidabilità della sessione sia abilitata
   - Assicurarsi che su Gateway sia abilitato DTLS
7. Verificare se sono state configurate le regole firewall appropriate sia nei firewall di rete che nei firewall in esecuzione sulle macchine con i VDA.

8. Verificare se le connessioni degli utenti richiedono una MTU non standard. Le connessioni con una MTU effettiva inferiore a 1500 byte causano la frammentazione dei pacchetti EDT, che a sua volta può influire sulle prestazioni o addirittura causare errori di avvio della sessione. Questo problema è comune quando si utilizzano VPN, alcuni punti di accesso Wi-Fi e reti mobili, come 4G e 5G. Per informazioni su come risolvere questo problema, vedere la sezione Rilevamento MTU.

### Interoperabilità con Citrix SD-WAN

L'ottimizzazione WAN Citrix SD-WAN (WANOP) offre la compressione tokenizzata tra le sessioni (deduplicazione dei dati), inclusa la cache video basata su URL, offrendo una notevole riduzione della larghezza di banda. La riduzione si verifica se due o più persone nella sede dell'ufficio guardano lo stesso video recuperato dal client oppure trasferiscono o stampano parti significative dello stesso file o documento. Inoltre, eseguendo i processi per la riduzione dei dati ICA e la compressione dei processi di stampa sull'appliance della filiale, WANOP offre l'offload della CPU del server VDA e consente una maggiore scalabilità del server di Citrix Virtual Apps and Desktops.

Attualmente, SD-WAN WANOP non supporta EDT. Tuttavia, non è necessario disabilitare Adaptive Transport (Trasporto adatttivo) se SD-WAN WANOP è in uso. Quando un utente avvia una sessione che passa attraverso una SD-WAN con WANOP abilitato, imposta automaticamente la sessione in modo che utilizzi TCP come protocollo di trasporto. Le sessioni non WANOP continuano a utilizzare EDT quando possibile.

## HDX Direct (anteprima tecnica)

January 7, 2024

Quando si accede alle risorse fornite da Citrix, HDX Direct consente ai dispositivi client di stabilire una connessione diretta sicura con il VDA se esiste una linea di vista diretta.

> **Importante:**
>
> HDX Direct è attualmente disponibile in anteprima tecnica. Per inviare commenti o segnalare problemi, utilizzare questo modulo.

### Requisiti

Di seguito sono riportati i requisiti per l'uso di HDX Direct:

- Piano di controllo

  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2303 o versioni successive
- Virtual Delivery Agent (VDA)
  - Windows: versione 2303 o successiva
- App Workspace
  - Windows: versione 2303 o successiva
- Livello di accesso
  - Citrix Workspace
  - Citrix Gateway Service
  - NetScaler Gateway
- Firewall
  - Macchina VDA
    - TCP 443 in entrata (ICA su TCP)
    - UDP 443 in entrata (ICA su EDT)
  - Rete

| Protocollo | Porta | Origine | Destinazione |
|---|---|---|---|
| TCP | 443 | Client | VDA |
| UDP | 443 | Client | VDA |

### Configurazione

HDX Direct è disabilitato per impostazione predefinita. È possibile configurare questa funzionalità utilizzando l'impostazione HDX Direct nei criteri Citrix.

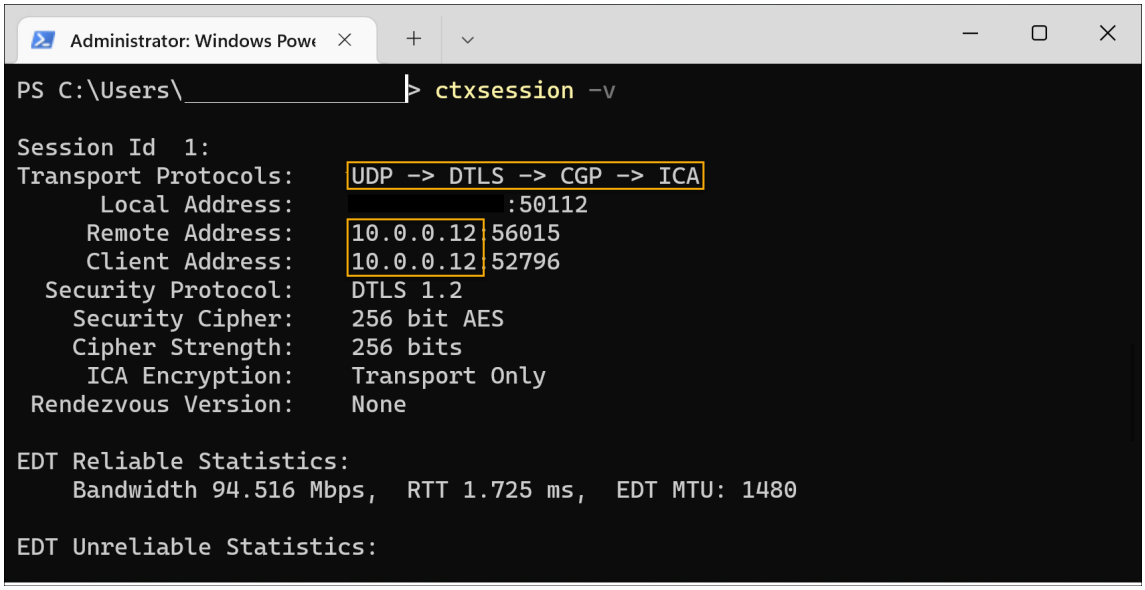
- **Allowed** (Consentito): HDX Direct è abilitato e tenta di stabilire una connessione diretta all'host della sessione quando è connessa una sessione.
- **Prohibited** (Vietato): impostazione predefinita. HDX Direct è disabilitato e impedisce al client di tentare di connettersi direttamente all'host della sessione quando è connesso tramite un gateway.

Per confermare che HDX Direct ha stabilito correttamente una connessione diretta, utilizzare l'utilità CtxSession.exe sulla macchina VDA.

Per utilizzare l'utilità CtxSession.exe, avviare un prompt dei comandi o PowerShell all'interno della sessione ed eseguire ctxsession.exe -v. Se è stata correttamente stabilita una connessione HDX Direct, verrà visualizzato quanto segue:

- Protocollo di trasporto
  - UDP > DTLS > CGP > ICA (se si utilizza EDT)
  - TCP > SSL > CGP > ICA (se si utilizza TCP)
- L'indirizzo remoto e l'indirizzo del client sono gli stessi




## Considerazioni

Di seguito sono riportate considerazioni sull'utilizzo di HDX Direct:

- Quando si utilizzano macchine non persistenti per app e desktop virtuali, non abilitare HDX Direct nell'immagine master/modello per evitare di generare certificati per la macchina virtuale (VM) master.

## Come funziona

HDX Direct consente ai client di stabilire una connessione diretta con l'host della sessione quando è disponibile una comunicazione diretta. Quando le connessioni dirette vengono effettuate utilizzando HDX Direct, viene utilizzata la crittografia a livello di rete (TLS/DTLS) per proteggerle, sfruttando certificati autofirmati.

Esistono tre fasi che coprono diverse parti della funzionalità: pre-avvio, avvio e post-avvio.

#### Fase di pre-avvio

Questa è la fase iniziale, che riguarda la creazione e la gestione dei certificati. Queste attività sono gestite dai seguenti servizi sulla macchina VDA, entrambi impostati per essere eseguiti automaticamente all'avvio della macchina:

- Servizio Citrix ClxMtp: responsabile della generazione e della rotazione dei certificati CA.
- Citrix Certificate Manager Service: responsabile della generazione e della gestione del certificato CA root autofirmato, delle chiavi dei certificati della macchina e dei certificati della macchina.

Di seguito è riportata una panoramica del processo di gestione dei certificati:

1. I servizi vengono avviati all'avvio della macchina.
2. Il servizio Citrix ClxMtp crea le chiavi se non ne è già stata creata alcuna.
3. Il servizio Citrix Certificate Manager verifica se HDX Direct è abilitato. In caso contrario, il servizio si interrompe da solo.
4. Se HDX Direct è abilitato, Citrix Certificate Manager Service verifica se esiste un certificato CA root autofirmato. In caso contrario, viene creato un certificato root autofirmato.
5. Una volta disponibile un certificato CA root, il servizio Citrix Certificate Manager verifica se esiste un certificato macchina autofirmato. In caso contrario, il servizio genera le chiavi e crea un nuovo certificato utilizzando il nome di dominio completo della macchina.
6. Se esiste un certificato della macchina creato dal servizio Citrix Certificate Manager e il nome dell'oggetto non corrisponde al FQDN della macchina, viene generato un nuovo certificato.

> **Nota:**
>
> Il servizio Citrix Certificate Manager genera certificati RSA che sfruttano chiavi a 2048 bit.

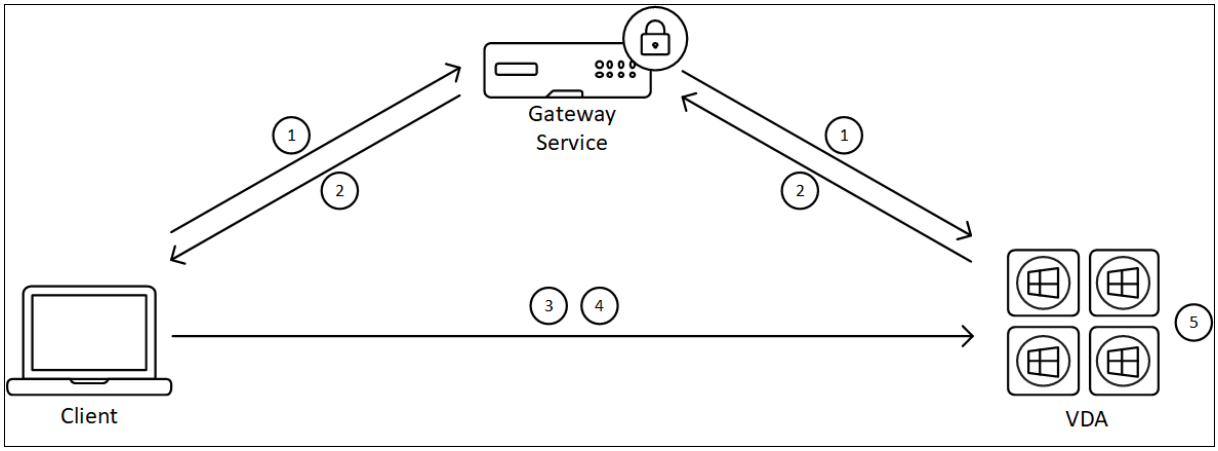
#### Fase di avvio

Per riuscire a stabilire una connessione HDX Direct sicura, il client deve considerare attendibili i certificati utilizzati per proteggere la sessione. Per ottenere questo risultato, il VDA invia al Broker le informazioni sul certificato durante l'intermediazione di una sessione. Successivamente, il Broker invia queste informazioni a Workspace per includerle nel file ICA inviato al client per avviare la sessione.

#### Fase post-avvio

Una volta che una sessione è stata mediata con successo, la sessione viene avviata. Di seguito è riportata una panoramica del processo di connessione di HDX Direct:




1. Il client stabilisce una connessione con il VDA tramite il servizio Gateway.
2. Dopo una connessione riuscita, il VDA invia al client il nome di dominio completo della macchina VDA e un elenco dei relativi indirizzi IP.
3. Il client analizza gli indirizzi IP per verificare se può raggiungere direttamente il VDA.
4. Se è in grado di raggiungere il VDA direttamente con uno qualsiasi degli indirizzi IP condivisi, il client stabilisce una connessione diretta sicura con il VDA.
5. Una volta stabilita correttamente la connessione diretta, la sessione viene trasferita alla nuova connessione e la connessione al servizio gateway termina.

### Problemi noti

Di seguito sono riportati i problemi noti relativi a HDX Direct:

- La connessione HDX Direct potrebbe non riuscire quando Rendezvous è disabilitato.
- La connessione HDX Direct potrebbe non riuscire quando si avviano sessioni da un sito Citrix Virtual Apps and Desktops 2303 locale.
- L'app Workspace potrebbe bloccarsi se il VDA è in esecuzione su Windows 11.

## Dispositivi

January 7, 2024

HDX offre un'esperienza utente ad alta definizione su qualsiasi dispositivo, in qualsiasi luogo. Gli articoli della sezione Dispositivi descrivono i seguenti dispositivi:

- Mappatura delle unità client
- Dispositivo USB generico
- Dispositivi mobili e touch screen

- Dispositivi seriali
- Tastiere speciali
- Dispositivi TWAIN
- Webcam
- Dispositivi WIA

### Dispositivo USB ottimizzato e generico

Un dispositivo USB ottimizzato è un dispositivo per il quale l'app Citrix Workspace ha un supporto specifico. Ad esempio, la possibilità di reindirizzare le webcam utilizzando il canale virtuale HDX Multimedia. Un dispositivo generico è un dispositivo USB per il quale non esiste un supporto specifico nell'app Citrix Workspace.

Per impostazione predefinita, il reindirizzamento USB generico non può reindirizzare i dispositivi USB con supporto ottimizzato per i canali virtuali a meno che non vengano inseriti in modalità Generica.

In generale, si ottengono prestazioni migliori per i dispositivi USB in modalità Ottimizzata rispetto alla modalità Generica. Tuttavia, ci sono casi in cui un dispositivo USB non dispone di funzionalità complete in modalità ottimizzata. Potrebbe essere necessario passare alla modalità Generica per ottenere l'accesso completo alle sue funzioni.

Con i dispositivi di archiviazione di massa USB, è possibile utilizzare la mappatura dell'unità client oppure il reindirizzamento USB generico oppure entrambi, controllati dalle politiche Citrix. Le principali differenze sono:

Se sia il reindirizzamento USB generico che i criteri di mappatura delle unità client sono attivati e viene inserito un dispositivo di archiviazione di massa prima o dopo l'avvio di una sessione, questo viene reindirizzato utilizzando il mapping delle unità client.

Quando queste condizioni sono vere, il dispositivo di archiviazione di massa viene reindirizzato utilizzando il reindirizzamento USB generico:

- Sono abilitati sia il reindirizzamento USB generico che i criteri di mappatura delle unità client.
- Un dispositivo è configurato per il reindirizzamento automatico.
- Viene inserito un dispositivo di archiviazione di massa prima o dopo l'avvio di una sessione.

Per ulteriori informazioni, vedere http://support.citrix.com/article/CTX123015.

| Funzionalità | Mappatura unità client | Reindirizzamento USB generico |
|---|---|---|
| Attivato per impostazione predefinita | Sì | No |
| Accesso in sola lettura configurabile | Sì | No |

| Funzionalità | Mappatura unità client | Reindirizzamento USB generico |
|---|---|---|
| Accesso ai dispositivi crittografati | Sì, se la crittografia viene sbloccata prima dell'accesso al dispositivo nella sessione virtuale. | Solo Citrix Virtual Desktops |

## Client Drive Mapping (CDM)

January 7, 2024

Client Drive Mapping rende le unità di archiviazione presenti sull'endpoint client disponibili all'interno di una sessione Citrix HDX per consentire il trasferimento di file e cartelle dal client all'host della sessione e viceversa. Questa funzionalità è abilitata per impostazione predefinita con privilegi di lettura e scrittura. Per impedire agli utenti di aggiungere o modificare file e cartelle nei dispositivi client mappati, attivare l'impostazione dei criteri **Read-only client drive access (Accesso alle unità client di sola lettura)**. Quando si aggiunge questa impostazione a un criterio, assicurarsi che l'impostazione **Client drive redirection** (Reindirizzamento unità client) sia impostata su **Allowed** (Consentita) e sia anche aggiunta al criterio.

Come precauzione di sicurezza, le unità degli endpoint vengono mappate senza l'autorizzazione di esecuzione per impostazione predefinita. Per consentire agli utenti di eseguire gli eseguibili direttamente dalle unità client mappate, modificare il valore del registro **ExecuteFromMappedDrive** nell'host della sessione. Per dettagli, vedere Unità client mappate nella sezione **Funzionalità HDX gestite tramite il Registro di sistema**.

### Requisiti

Di seguito sono riportati i requisiti per l'utilizzo del CDM:

#### Piano di controllo Citrix

- Citrix Virtual Apps and Desktops 1912 o versioni successive
- Citrix DaaS

#### Host della sessione

- Sistema operativo

  - Windows 10 1809 o versione successiva
  - Windows Server 2016 o versione successiva
  - Linux: fare riferimento all'app Workspace per i requisiti di sistema di Linux VDA
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 o versioni successive
  - Linux: fare riferimento alla documentazione di Linux VDA

#### Dispositivo client

- Sistema operativo
  - Windows 10 1809 o versione successiva
  - Linux: fare riferimento all'app Workspace per i requisiti di sistema Linux

### Criteri correlati

Vedere la sezione Riferimento alle impostazioni dei criteri per le impostazioni CDM.

### Scenari a doppio hop

CDM è supportato negli scenari a doppio hop. Per impostazione predefinita, l'unità dell'endpoint client è mappata alla sessione del secondo hop e le unità del primo hop non sono disponibili. Tuttavia, questo può essere impostato in modo che le unità del primo hop vengano mappate nella sessione del secondo hop anziché nelle unità dell'endpoint client.

Per configurare questa funzionalità, modificare il seguente valore di registro:

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced
- Nome del valore: NativeDriveMapping
- Tipo di valore: REG_SZ
- Dati del valore:
  - True: mappa le unità della prima sessione di hop nella seconda sessione di hop
  - False: mappa le unità dell'endpoint client nella seconda sessione di hop

> **Nota:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di

> sistema prima di modificarlo.

## Dispositivi USB generici

January 7, 2024

La tecnologia HDX offre **supporto ottimizzato** per i dispositivi USB più diffusi. Questi dispositivi includono:

- Monitor
- Mouse
- Tastiere
- Telefoni VoIP
- Cuffie
- Webcams
- Scanner
- Videocamere
- Stampanti
- Drive
- Lettori di smart card
- Tablet da disegno
- Signature pad

Il supporto ottimizzato offre una migliore esperienza utente con migliori prestazioni ed efficienza della larghezza di banda su una WAN. Il supporto ottimizzato è solitamente l'opzione migliore, soprattutto in ambienti con latenza elevata o sensibili alla sicurezza.

La tecnologia HDX offre il **reindirizzamento USB generico** per dispositivi speciali che non dispongono di alcun supporto ottimizzato o nei casi in cui non è adatto. Per ulteriori informazioni sul reindirizzamento USB generico, vedere Reindirizzamento USB generico.

Per ulteriori informazioni sui dispositivi USB e sull'app Citrix Workspace per Windows, vedere Configurare il reindirizzamento dei dispositivi USB compositi e [Configurazione del supporto USB].(/en-us/citrix-workspace-app-for-windows/configure/config-xdesktop/config-usb-support.html)

## Supporto dei dispositivi client mobili e con touch screen

January 7, 2024

Citrix Virtual Apps and Desktops consente agli utenti di accedere alle applicazioni e ai desktop pubblicati da dispositivi client mobili e con touch screen.

## Requisiti

### Piano di controllo Citrix

- Citrix Virtual Apps and Desktops 7.15 o versioni successive
- Citrix DaaS

### Host della sessione

- Sistema operativo
  - Windows 10 1903 o versione successiva
  - Windows Server 2016 o versione successiva
- VDA
  - Windows: versione 7.15 o successiva

### Dispositivo client

- Sistema operativo
  - Windows 10 1809 o versione successiva
- App Citrix Workspace per Windows versione 1808 o successiva

## Modalità tablet per dispositivi touch screen che utilizzano Windows Continuum

Continuum è una funzionalità di Windows 10 che si adatta al modo in cui viene utilizzato il dispositivo client. Quando il VDA rileva la presenza di una tastiera o di un mouse su un client abilitato al tocco, mette il client in modalità desktop. Se non è presente una tastiera o un mouse, il VDA mette il client in modalità tablet/mobile. Questo rilevamento si verifica durante la connessione e la riconnessione della sessione e anche durante la sessione quando la tastiera o il mouse sono collegati o scollegati.

Questa funzionalità è abilitata per impostazione predefinita. Per disabilitare questa funzionalità, configurare le impostazioni dei criteri Tablet mode toggle policy settings (Impostazioni dei criteri di abilitazione/disabilitazione della modalità tablet).

Oltre ai requisiti per i dispositivi con touch screen sopra menzionati, per Windows Continuum sono necessari i seguenti requisiti:

**Citrix Hypervisor**

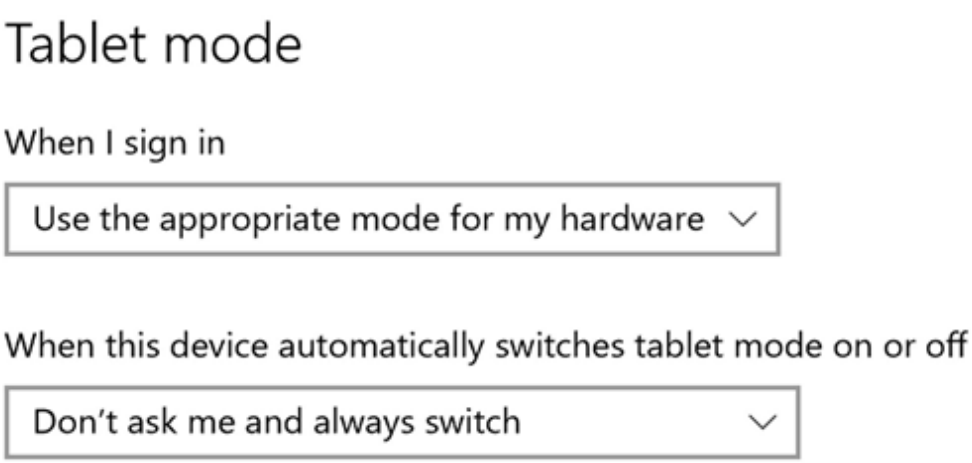
- Citrix Hypervisor 8.2 o versione successiva
- Eseguire il comando CLI di XenServer per consentire il passaggio laptop/tablet:
  **xe vm-param-set uuid=<VM_UUID> platform:acpi_laptop_slate=1**

> **Importante:**
>
> L'aggiornamento dell'immagine di base per un catalogo di macchine esistente dopo aver modificato l'impostazione dei metadati non influisce sulle VM precedentemente sottoposte a provisioning. Dopo aver modificato l'immagine di base della VM di XenServer, creare un catalogo, scegliere l'immagine di base ed eseguire il provisioning di una nuova macchina MCS (Machine Creation Services).

**Host della sessione**

- Sistema operativo
  - Windows 10 1903 o versione successiva
  - Windows 11
- VDA
  - Windows: versione 7.16 o successiva
  - **A causa delle attuali limitazioni nelle configurazioni del sistema operativo, dopo aver avviato la prima sessione ICA e riavviato il VDA l'utente dovrà impostare dai menu a discesa le seguenti opzioni:**
    - **Settings > System > Tablet Mode** (Impostazioni > Sistema > Modalità tablet)
      - Use the appropriate mode for my hardware (Utilizza la modalità appropriata per il mio hardware)
      - Don't ask me and always switch (Non mostrare più questo messaggio e cambia sempre modalità)




La **modalità tablet** offre un'interfaccia utente più adatta ai touch screen:

- Pulsanti leggermente più grandi.
- La schermata di avvio e tutte le app avviate vengono aperte a schermo intero.
- La barra delle applicazioni contiene un pulsante Indietro.
- Icone eliminate dalla barra delle applicazioni.

Accesso a Esplora file.

Windows 10 carica il driver GPIO sulla macchina virtuale di destinazione in base a questo BIOS aggiornato. Viene utilizzato per passare dalla modalità tablet alla modalità desktop e viceversa all'interno della macchina virtuale.

L'app Citrix Workspace per HTML5 non supporta le funzionalità di Windows Continuum.

La **modalità desktop** offre l'interfaccia utente tradizionale in cui si interagisce allo stesso modo in cui si usa il PC con una tastiera e un mouse.

### Penne Microsoft Surface Pro e Surface Book

Supportiamo la funzionalità penna standard con le applicazioni basate su Windows Ink. Il supporto include puntamento, cancellazione, pressione della penna, segnali Bluetooth e altre funzionalità a seconda del firmware del sistema operativo e del modello di penna. Ad esempio, la pressione della penna può essere fino a 4096 livelli. Questa funzionalità è abilitata per impostazione predefinita.

Di seguito sono riportati i requisiti per il supporto delle funzionalità della penna:

#### Piano di controllo Citrix

- Citrix Virtual Apps and Desktops 1903 o versioni successive
- Citrix DaaS

#### Host della sessione

- Sistema operativo
  - Windows 10 1809 o versione successiva
  - Windows Server 2016 o versione successiva
- VDA
  - Windows: versione 1903 o successiva

#### Dispositivo client

- Sistema operativo
  - Windows 10 1809 o versione successiva
- App Citrix Workspace per Windows versione minima 1902

Per una dimostrazione di Windows Ink e della funzionalità penna, fare clic sul seguente elemento grafico:


Per disabilitare o abilitare questa funzione, vedere Penne Microsoft Surface Pro e Surface Book nell'elenco delle funzionalità gestite tramite il Registro di sistema.

### Problemi noti

Di seguito sono riportati i problemi noti relativi al supporto della penna:

- A causa delle limitazioni del sistema operativo in Windows Server 2k22, gli utenti non saranno in grado di impostare scelte rapide della penna o apportare modifiche alle impostazioni penna/inchiostro del Pannello di controllo durante la connessione alle applicazioni o ai desktop del server 2k22.
- Le scelte rapide della penna non vengono rispettate da un client Windows 11 abilitato alla penna a causa delle limitazioni del sistema operativo.

## Porte seriali

January 7, 2024

La maggior parte dei nuovi PC non dispone di porte seriali (COM) integrate. Le porte sono facili da aggiungere utilizzando convertitori USB. Le applicazioni adatte alle porte seriali spesso comprendono sensori, controller, vecchi lettori di assegni, pad e così via. Alcuni dispositivi con porta COM virtuale USB utilizzano driver specifici del fornitore al posto dei driver forniti da Windows (usbser.sys). Questi driver consentono di forzare la porta COM virtuale del dispositivo USB in modo che non cambi anche se viene collegata a socket USB diversi. Questa operazione può essere eseguita da **Gestione dispositivi > Porte (COM e LPT) > Proprietà** o dall'applicazione che controlla il dispositivo.

Il mapping delle porte COM client consente di utilizzare i dispositivi collegati alle porte COM dell'endpoint dell'utente durante le sessioni virtuali. È possibile utilizzare questi mapping come qualsiasi altro mapping di rete.

Per ogni porta COM, un driver nel sistema operativo assegna un nome di collegamento simbolico, ad esempio COM1 e COM2. Le applicazioni utilizzano quindi il collegamento per accedere alla porta.

> **Importante:**
>
> Poiché un dispositivo può collegarsi all'endpoint utilizzando direttamente USB, non significa che possa essere reindirizzato utilizzando il reindirizzamento USB generico. Alcuni dispositivi USB funzionano come porte COM virtuali, alle quali le applicazioni possono accedere allo stesso modo della porta seriale fisica. Il sistema operativo può astrarre le porte COM e trattarle come condivisioni file. Due protocolli comuni per la COM virtuale sono CDC ACM o MCT. In caso di connessione tramite una porta RS-485, le applicazioni potrebbero non funzionare affatto. Usare un convertitore RS-485-RS232 per utilizzare RS-485 come porta COM.
>
> **Importante:**
>
> Alcune applicazioni riconoscono il dispositivo (ad esempio un signature pad) in modo coerente solo se è collegato a COM1 o COM2 sulla workstation client.

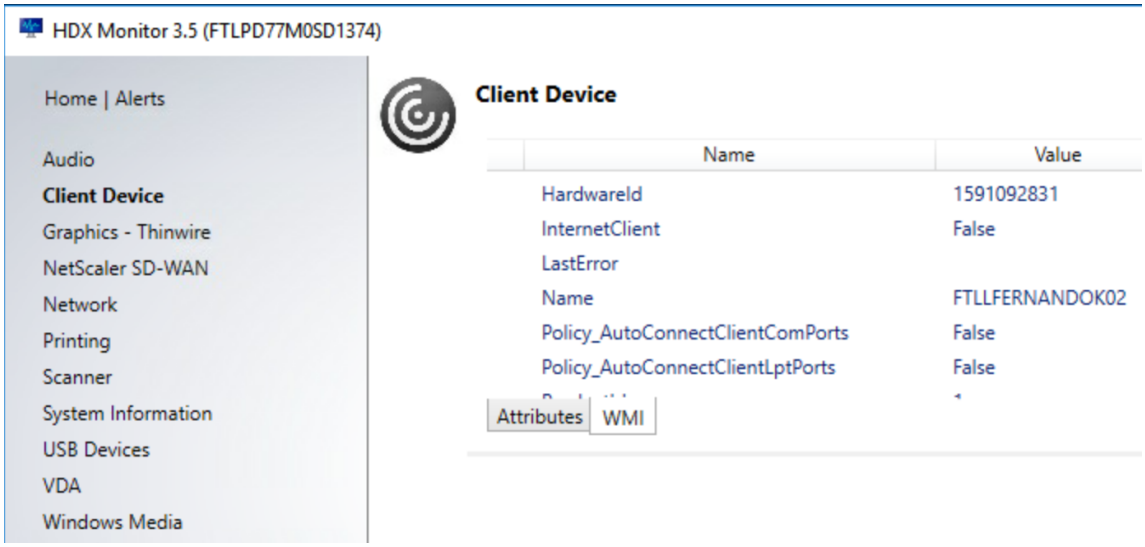
### Mappare una porta COM client a una porta COM server

È possibile mappare le porte COM client a una sessione Citrix in tre modi:

- Criteri di Studio. Per ulteriori informazioni sui criteri, vedere Impostazioni dei criteri di reindirizzamento delle porte.
- Prompt dei comandi VDA.
- Strumento di configurazione Desktop remoto (Servizi terminal).

1. Abilitare il **reindirizzamento della porta COM client** e i **criteri di Studio per la connessione automatica delle porte COM client**. Dopo l'applicazione, sono disponibili alcune informazioni in HDX Monitor.




2. Se la **connessione automatica delle porte COM client** non riesce a mappare la porta, è possibile mappare manualmente la porta o utilizzare script di accesso. Accedere al VDA e in una finestra del prompt dei comandi digitare:

   NET USE COMX: \\CLIENT\COMZ:

   oppure

   NET USE COMX: \\CLIENT\CLIENTPORT:COMZ:

   **X** è il numero della porta COM sul VDA (le porte da 1 a 9 sono disponibili per il mapping). **Z** è il numero della porta COM client che si desidera mappare.

   Per confermare che l'operazione ha avuto esito positivo, digitare **NET USE** al prompt dei comandi VDA. L'elenco visualizzato contiene unità mappate, porte LPT e porte COM mappate.

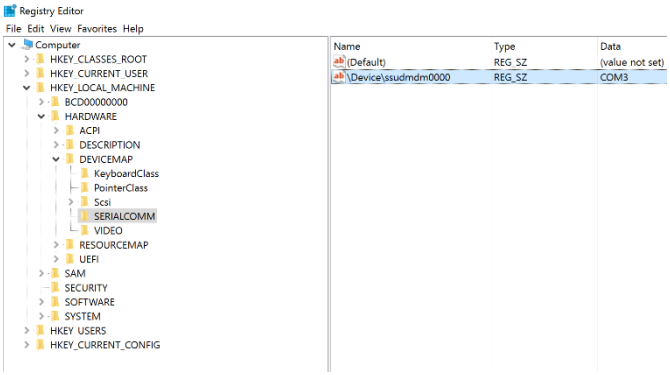

3. Per utilizzare questa porta COM in un desktop virtuale o in un'applicazione, installare l'applicazione del dispositivo utente e puntare al nome della porta COM mappata. Ad esempio, se si esegue il mapping di COM1 sul client a COM3 sul server, installare l'applicazione del dispositivo della porta COM nel VDA e puntare a COM3 durante la sessione. Utilizzare questa porta COM mappata come una porta COM sul dispositivo utente.

> **Importante:**
>
> Il mapping delle porte COM non è compatibile con TAPI. Non è possibile mappare i dispositivi TAPI (Telephony Application Programming Interface) di Windows alle porte COM client. TAPI definisce un modo standard di controllare le funzioni telefoniche per dati, fax e chiamate vocali per le applicazioni. TAPI gestisce la segnalazione, comprese la composizione, la risposta e la fine delle chiamate. Inoltre, gestisce servizi supplementari come l'attesa, il trasferimento e le chiamate in conferenza.

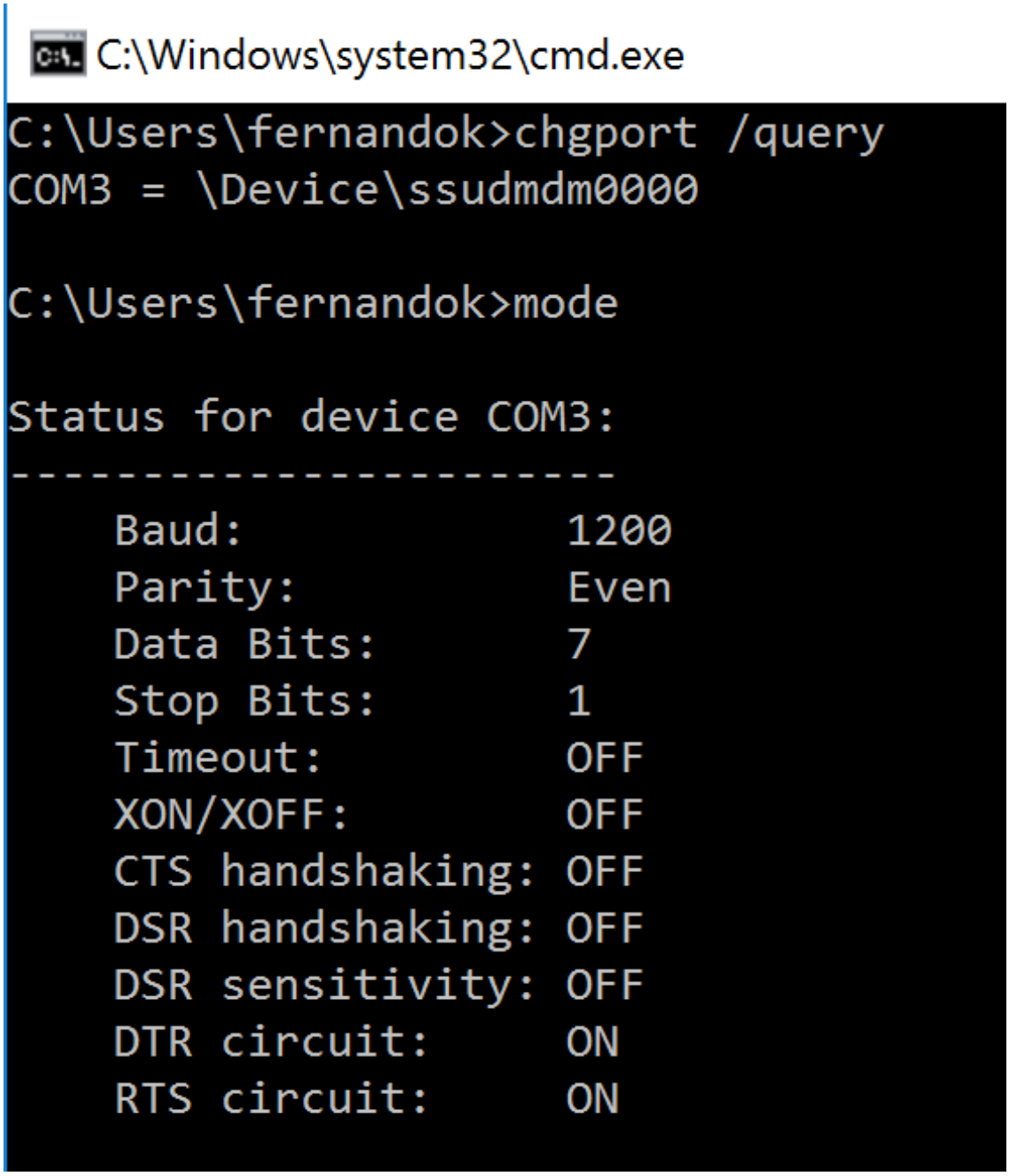
## Risoluzione dei problemi

1. Assicurarsi di poter accedere al dispositivo direttamente dall'endpoint, evitando Citrix. Se la porta non è mappata al VDA, non si è connessi a una sessione Citrix. Seguire le istruzioni per la risoluzione dei problemi fornite con il dispositivo e verificare innanzitutto che funzioni localmente.
   Quando un dispositivo è connesso a una porta COM seriale, viene creata una chiave del Registro di sistema nell'hive mostrato qui:



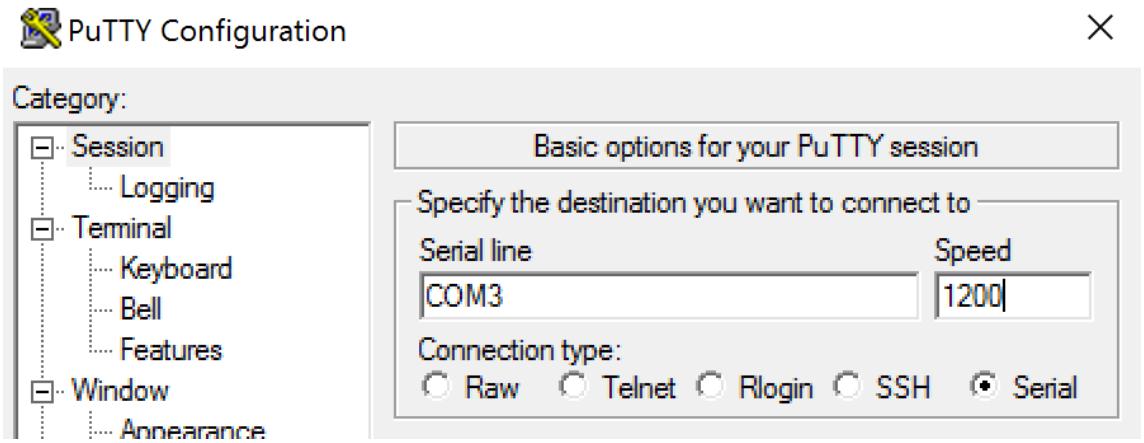

   È inoltre possibile trovare queste informazioni dal prompt dei comandi eseguendo **chgport /query**.




Se le istruzioni per la risoluzione dei problemi relativi al dispositivo non sono disponibili, provare ad aprire una sessione PuTTY. Scegliere **Session (Sessione)** e in **Serial line (Linea seriale)** specificare la porta COM.




È possibile eseguire **MODE** in una finestra di comando locale. L'output potrebbe visualizzare la porta COM in uso e il baud/parità/bit di dati/bit di stop, necessari nella sessione PuTTY. Se la connessione PuTTY ha esito positivo, premere **Invio** per visualizzare il feedback del dispositivo. Qualsiasi carattere digitato potrebbe essere ripetuto sullo schermo o ricevere una risposta. Se questo passaggio non riesce, non è possibile accedere al dispositivo da una sessione virtuale.

2. Mappare la porta COM locale al VDA (utilizzando i criteri o **NET USE COMX: \\CLIENT\COMZ:**) e ripetere le stesse procedure PuTTY del passaggio precedente, ma questa volta dal PuTTY del VDA. Se PuTTY non mostra l'errore **Unable to open connection to COM1. Unable to open serial port (Impossibile aprire la connessione a COM1. Impossibile aprire la porta seriale)**, un altro dispositivo potrebbe utilizzare COM1.

3. Eseguire **chgport /query**. Se il driver seriale Windows incorporato nel VDA assegna automaticamente \Device\Serial0 a una porta COM1 del VDA, effettuare le seguenti operazioni:
   A. Aprire CMD sul VDA e digitare **NET USE.**

   B. Eliminare gli eventuali mapping esistenti (ad esempio, COM1) sul VDA.

   **NET USE COM1 /DELETE**

   C. Mappare il dispositivo al VDA.

   **NET USE COM1: \\CLIENT\COM3:**

   D. Puntare l'applicazione sul VDA su COM3.

   Infine, provare a mappare la porta COM locale (ad esempio, COM3) a una porta COM diversa sul VDA (diversa da COM1, ad esempio COM3). Assicurarsi che l'applicazione punti a questa porta:
   **NET USE COM3: \\CLIENT\COM3**

4. Se ora è visibile la porta mappata, PuTTY funziona ma non vengono trasferiti dati, potrebbe trattarsi di una race condition. L'applicazione potrebbe connettersi e aprire la porta prima che venga mappata, bloccando il mapping. Provare a eseguire una delle seguenti operazioni:

   - Aprire una seconda applicazione pubblicata sullo stesso server. Attendere alcuni secondi

perché la porta venga mappata, quindi aprire l'applicazione reale che tenta di utilizzare la porta.

- Abilitare i criteri di reindirizzamento della porta COM dall'Editor Criteri di gruppo in Active Directory anziché da Studio. Tali criteri sono il **reindirizzamento delle porte COM client** e la **connessione automatica delle porte COM client**. I criteri applicati in questo modo potrebbero essere elaborati prima dei criteri di Studio, garantendo che la porta COM sia mappata. I criteri Citrix vengono inviati al VDA e archiviati in: `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
- Utilizzare questo script di accesso per l'utente oppure, invece di pubblicare l'applicazione, pubblicare uno script .bat che elimina innanzitutto qualsiasi mapping sul VDA, rimappa la porta COM virtuale e quindi avvia l'applicazione:

```
@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \\CLIENT\COM1:
NET USE COM2: \\CLIENT\COM2:
MODE COM1: BAUD=1200 (or whatever value needed)
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (or whatever value needed)
START C:\Program Files\<Your Software Path>\
```

5. Come ultima alternativa, è possibile utilizzare lo strumento Process Monitor di Sysinternals. Quando si esegue lo strumento sul VDA, trovare e filtrare oggetti come COM3, picaser.sys, CdmRedirector, ma soprattutto <tua_app>.exe. Eventuali errori potrebbero essere visualizzati come Accesso negato o simile.

## Tastiere speciali

January 7, 2024

### Tastiere Bloomberg

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di

> sistema prima di modificarlo.

Citrix Virtual Apps and Desktops supporta la tastiera Starboard Bloomberg modello 4, modello 5 (e il modello precedente 3). Questa tastiera consente ai clienti del settore finanziario di utilizzare le funzionalità speciali della tastiera per accedere ai dati del mercato finanziario e fare trading rapidamente.

> **Importante:**
>
> Si consiglia di utilizzare la tastiera Bloomberg con una sola sessione. Si sconsiglia di utilizzare la tastiera con più sessioni simultanee (un client per più sessioni).

La tastiera Bloomberg è un dispositivo USB composito composto da più dispositivi USB in un'unica shell fisica:

- Tastiera.
- Lettore di impronte digitali.
- Dispositivo audio con tasti per aumentare e diminuire il volume e disattivare l'altoparlante e il microfono. Questo dispositivo include altoparlante integrato, microfono, jack per il microfono e auricolare.
- Hub USB per collegare tutti questi dispositivi al sistema.

**Requisiti:**

- La sessione a cui si connette l'app Citrix Workspace per Windows deve supportare i dispositivi USB.
- Versione minima dell'app Citrix Workspace 2207 per Linux per supportare la tastiera Bloomberg modello 5.
- Versione minima dell'app Citrix Workspace 2109 per Windows per supportare la tastiera Bloomberg modello 5.
- App Citrix Workspace (versione minima 1808) per Windows o Citrix Receiver per Windows (versione minima 4.8) per supportare la tastiera Bloomberg modello 3 e 4.
- App Citrix Workspace (versione minima 1808) per Windows o Citrix Receiver per Windows (versione minima 4.12) per utilizzare la modalità KVM (due cavi USB con uno instradato tramite KVM) per il modello 4.

Per informazioni sulla configurazione delle tastiere Bloomberg nell'app Citrix Workspace per Windows, vedere Configurazione delle tastiere Bloomberg.

Per abilitare il supporto per la tastiera Bloomberg, vedere Tastiere Bloomberg nell'elenco delle funzionalità gestite tramite il Registro di sistema.

**Verificare il supporto:**

Per determinare se il supporto della tastiera Bloomberg è abilitato nell'app Citrix Workspace, verificare se Desktop Viewer segnala correttamente i dispositivi della tastiera Bloomberg.

Scenario desktop:

Aprire Desktop Viewer. Se il supporto per la tastiera Bloomberg è abilitato, Desktop Viewer mostra tre dispositivi sotto l'icona USB:

Per la tastiera Bloomberg 5:

- Modulo biometrico Bloomberg LP Bloomberg
- Tastiera Bloomberg LP (dispositivo composito con due interfacce)
- Audio tastiera Bloomberg LP (dispositivo composito con tre interfacce)

Per tastiere Bloomberg 3 e 4:

- Scanner di impronte digitali Bloomberg
- Funzionalità della tastiera Bloomberg
- Tastiera Bloomberg LP 2013

Solo per lo scenario con applicazioni integrate:

Aprire il menu **Connection Center** dall'icona dell'area di notifica dell'app Citrix Workspace. Se il supporto per la tastiera Bloomberg è abilitato, i tre dispositivi vengono visualizzati nel menu **Devices** (Dispositivi).

Il segno di spunta accanto a ciascuno di questi dispositivi indica che sono utilizzati in remoto nella sessione.

## Dispositivi TWAIN

January 7, 2024

### Requisiti

- Lo scanner deve essere conforme a TWAIN.
- Installare i driver TWAIN sul dispositivo locale. Non sono necessari sul server.
- Collegare lo scanner localmente (ad esempio, tramite USB).
- Verificare che lo scanner utilizzi il driver TWAIN locale e non il servizio Acquisizione di immagini di Windows.
- Verificare che non vi siano criteri applicati all'account utente utilizzato per il test e che limitino la larghezza di banda all'interno della sessione ICA. Ad esempio, il limite della larghezza di banda di reindirizzamento USB del client.

Per informazioni sulle impostazioni dei criteri, vedere Impostazioni dei criteri dei dispositivi TWAIN.

# Webcams

January 7, 2024

### Streaming con webcam ad alta definizione

Le webcam possono essere utilizzate dalle applicazioni di videoconferenza in esecuzione all'interno della sessione virtuale. L'applicazione sul server seleziona il formato e la risoluzione della webcam in base ai tipi di formato supportati. Quando si avvia una sessione, il client invia le informazioni della webcam al server. Scegliere una webcam dall'applicazione di videoconferenza. Quando sia la webcam che l'applicazione supportano il rendering ad alta definizione, l'applicazione utilizza una risoluzione ad alta definizione. Supportiamo risoluzioni webcam fino a 1920x1080.

Questa funzionalità richiede Citrix Receiver per Windows, versione minima 4.10. Per un elenco delle piattaforme di app Citrix Workspace che supportano il reindirizzamento della webcam HDX, vedere Matrice delle funzionalità dell'app Citrix Workspace.

Per ulteriori informazioni sullo streaming con webcam ad alta definizione, vedere Videoconferenze HDX e compressione video della webcam.

È possibile utilizzare una chiave del Registro di sistema per disabilitare e abilitare la funzionalità e quindi configurare una risoluzione specifica. Per informazioni, vedere Streaming della webcam ad alta definizione e risoluzione della webcam ad alta definizione nell'elenco delle funzionalità gestite tramite il Registro di sistema.

# Dispositivi WIA

January 7, 2024

### Requisiti

- Lo scanner deve essere conforme a WIA.
- Installare i driver WIA sul dispositivo locale. Non sono necessari sul server.
- Collegare lo scanner localmente (ad esempio, tramite USB).
- Verificare che lo scanner utilizzi il servizio Acquisizione di immagini di Windows e non il driver TWAIN.

- Verificare che non vi siano criteri applicati all'account utente utilizzato per il test e che limitino la larghezza di banda all'interno della sessione ICA. Ad esempio, il limite della larghezza di banda di reindirizzamento USB del client.

#### Windows Image Acquisition application allow list (Elenco di elementi consentiti dell'applicazione Acquisizione di immagini di Windows)

Un elenco di elementi consentiti permette di controllare quali applicazioni sul VDA possono accedere al reindirizzamento dello scanner di Acquisizione di immagini di Windows. L'Editor del Registro di sistema utilizza l'input dell'impostazione dell'elenco di elementi consentiti su ogni VDA che contiene l'Acquisizione di immagini di Windows. Per impostazione predefinita, nessuna applicazione ha accesso ad Acquisizione di immagini di Windows.

Per regolare l'acquisizione di immagini Windows per le applicazioni sul VDA, vedere l'impostazione Windows Image Acquisition application allow list nell'elenco delle funzionalità gestite tramite il Registro di sistema.

Per informazioni sulle impostazioni dei criteri, vedere Impostazioni dei criteri dei dispositivi WIA.

## Grafica

January 7, 2024

La grafica Citrix HDX include una vasta gamma di tecnologie di accelerazione grafica e codifica che ottimizza la distribuzione di applicazioni grafiche avanzate da Citrix Virtual Apps and Desktops. Le tecnologie grafiche offrono la stessa esperienza dell'utilizzo di un desktop fisico quando si lavora in remoto con applicazioni virtuali che fanno uso intensivo della grafica.

È possibile utilizzare software o hardware per il rendering grafico. Il rendering software richiede una libreria di terze parti chiamata rasterizzatore software. Ad esempio, Windows include il rasterizzatore WARP per la grafica basata su DirectX. A volte, è possibile utilizzare un renderer software alternativo. Il rendering hardware (accelerazione hardware) richiede un processore grafico (GPU).

HDX Graphics offre una configurazione di codifica predefinita ottimizzata per i casi d'uso più comuni. Utilizzando i criteri Citrix, gli amministratori IT possono anche configurare varie impostazioni correlate alla grafica per soddisfare i diversi requisiti e fornire l'esperienza utente desiderata.

### Thinwire

Thinwire è la tecnologia di visualizzazione predefinita Citrix utilizzata in Citrix Virtual Apps and Desktops.

La tecnologia di visualizzazione remota consente la trasmissione della grafica generata su un computer, in genere attraverso una rete, a un altro computer per la visualizzazione. La grafica viene generata come risultato di input dell'utente, ad esempio le sequenze di tasti o le azioni del mouse.

### HDX 3D Pro

Le funzionalità HDX 3D Pro di Citrix Virtual Apps and Desktops consentono di fornire desktop e applicazioni che offrono prestazioni ottimali utilizzando un'unità di elaborazione grafica (GPU) per l'accelerazione hardware. Queste applicazioni includono applicazioni grafiche professionali 3D basate su OpenGL e DirectX. Il VDA standard supporta solo l'accelerazione GPU di DirectX.

#### Accelerazione GPU per il sistema operativo Windows a sessione singola

Utilizzando HDX 3D Pro, è possibile distribuire applicazioni a uso intensivo della grafica nell'ambito di desktop o applicazioni ospitati su computer con sistema operativo a sessione singola. HDX 3D Pro supporta computer host fisici (tra cui workstation desktop, blade e rack) e le tecnologie di virtualizzazione GPU Passthrough e GPU offerte da Citrix Hypervisor, vSphere e Hyper-V (solo passthrough).

Utilizzando GPU Passthrough, è possibile creare macchine virtuali con accesso esclusivo a hardware dedicato per l'elaborazione grafica. È possibile installare più GPU nell'hypervisor e assegnare VM a ciascuna di queste GPU in modo individuale.

Utilizzando la virtualizzazione GPU, più macchine virtuali possono accedere direttamente alla potenza di elaborazione grafica di una singola GPU fisica.

#### Accelerazione GPU per il sistema operativo Windows multisessione

HDX 3D Pro consente di eseguire il rendering di applicazioni ricche di grafica in esecuzione in sessioni di sistema operativo multisessione Windows sulla GPU (unità di elaborazione grafica) del server. Spostando il rendering OpenGL, DirectX, Direct3D e WPF (Windows Presentation Foundation) sulla GPU del server, il rendering grafico non rallenta la CPU del server. Inoltre, il server è in grado di elaborare più grafica perché il carico di lavoro è diviso tra CPU e GPU.

### Framehawk

> **Importante:**
>
> A partire da Citrix Virtual Apps and Desktops 7 1903, Framehawk non è più supportato. Utilizzare invece Thinwire con il trasporto adattivo abilitato.

Framehawk è una tecnologia di visualizzazione remota per lavoratori mobili su connessioni wireless a banda larga (Wi-Fi e reti cellulari 4G/LTE). Framehawk supera le sfide dell'interferenza spettrale e della propagazione multipath e offre un'esperienza utente fluida e interattiva agli utenti di app virtuali e desktop.

### Filigrana di sessione basata su testo

Le filigrane di sessione basate su testo aiutano a scoraggiare e abilitare il furto dei dati di tracciabilità. Queste informazioni tracciabili vengono visualizzate sul desktop della sessione come deterrente per

coloro che utilizzano fotografie e acquisizioni dello schermo per rubare i dati. È possibile specificare una filigrana che è testo sovrapposto. La filigrana può essere visualizzata sull'intera schermata della sessione senza modificare il contenuto del documento originale. Le filigrane di sessione basate su testo richiedono il supporto VDA.

### Informazioni correlate

- HDX 3D Pro
- Accelerazione GPU per il sistema operativo Windows a sessione singola
- Accelerazione GPU per il sistema operativo Windows multisessione
- Framehawk
- Thinwire
- Filigrana di sessione basata su testo

## High Dynamic Range (HDR) a 10 bit

January 7, 2024

Con le sessioni di desktop virtuale High Dynamic Range (HDR) a 10 bit, è possibile utilizzare funzionalità di codifica e decodifica avanzate per eseguire il rendering di immagini e video di alta qualità con una gamma estesa di colori e un contrasto e una luminosità più elevati. In aggiunta, è possibile personalizzare il livello di luminanza del bianco, i dati EDID (Extended Display Identification Data) e la qualità visiva, per migliorare l'esperienza utente.

### Requisiti di sistema

Endpoint:

- App Citrix Workspace per Windows 2209 o versioni successive
- GPU NVIDIA con supporto della decodifica HEVC a 10 bit sull'endpoint
- Monitor HDR a 10 bit supportati

Server:

- VDA con sistema operativo Windows a sessione singola 2209 o versione successiva
- GPU NVIDIA con supporto della codifica HEVC 444 a 10 bit sul VDA

## Criteri richiesti

Endpoint:

- Abilitare la decodifica H.265 per la grafica

Server:

- Ottimizzare per carichi di lavoro grafici 3D
- Graphics Status Indicator (opzionale)

## Configurazioni server

Quando si avvia una sessione Citrix su un monitor endpoint abilitato per HDR a 10 bit, la sessione HDR è abilitata per impostazione predefinita. Nelle sessioni HDR con più monitor, tutti i monitor degli endpoint devono avere l'HDR a 10 bit abilitato. Le sessioni HDR sono supportate in entrambe le modalità finestra e a schermo intero.

### Livello di bianco di riferimento

Questa impostazione definisce il livello di luminanza del bianco in base al valore nit. Controlla la luminosità relativa dello schermo HDR all'interno della sessione. Il valore predefinito è 80 nit. Impostare la seguente chiave di registro per definire un valore nit diverso:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Tipo: REG_DWORD
- Nome: RefWhiteLevel

Per attivare l'impostazione, è necessario ridimensionare la sessione oppure disconnetterla e riavviarla.

### Sostituzione EDID

È possibile configurare il VDA perché utilizzi l'EDID del monitor endpoint per le sessioni HDR. Ciò consente di sfruttare appieno le funzionalità di visualizzazione del monitor abbinando la gamma cromatica e la gamma di luminanza. Per impostazione predefinita, le sessioni HDR presuppongono che il display sia compatibile con HDR1000.
È possibile esportare l'EDID del monitor degli endpoint utilizzando NVIDIA o altri strumenti. Applicarlo al VDA utilizzando la seguente chiave di registro:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Tipo: REG_BINARY

- Nome: EDIDOverride

Quando si archivia l'EDID nel registro, non deve contenere virgole, spazi o caratteri speciali. Per attivare l'override di EDID, scollegarsi e avviare una nuova sessione.

#### Esperienza visiva senza perdite

Attivare i seguenti criteri per un'esperienza visiva senza perdite:

- Allow visually lossless compression (Consenti compressione senza perdite visiva)
- Qualità visiva: Always Lossless (Sempre senza perdite) o Build to Lossless (Compila per senza perdite)

Dopo aver impostato i criteri, è possibile controllare la qualità della sessione HDR mediante l'indicatore di stato grafico utilizzando il cursore della qualità dell'immagine o passando alla modalità pixel perfetti.

#### Altre considerazioni

- Sulle GPU virtuali, è possibile avviare sessioni HDR a 10 bit su un massimo di quattro monitor.
- La sessione Citrix torna alla modalità non HDR a 8 bit nei seguenti casi:
  - Se qualsiasi monitor degli endpoint non ha l'HDR a 10 bit abilitato
  - Abilitare la condivisione dello schermo
  - Impostare un layout di visualizzazione virtuale sul VDA
  - Passare alla modalità pixel perfetti senza impostare il criterio "Allow Visually Lossless Compression"(Consenti compressione visivamente senza perdite)

## HDX 3D Pro

January 7, 2024

Le funzionalità HDX 3D Pro di Citrix Virtual Apps and Desktops consentono di fornire desktop e applicazioni che offrono prestazioni ottimali utilizzando un'unità di elaborazione grafica (GPU) per l'accelerazione hardware. Queste applicazioni includono applicazioni grafiche professionali 3D basate su OpenGL e DirectX. Il VDA standard supporta solo l'accelerazione GPU di DirectX.

Per le impostazioni dei criteri HDX 3D Pro, vedere Ottimizzazione per carichi di lavoro grafici 3D.

Tutte le app Citrix Workspace supportate possono essere utilizzate con grafica 3D. Per ottenere prestazioni ottimali con carichi di lavoro 3D complessi, monitor ad alta risoluzione, configurazioni

multi-monitor e applicazioni con frequenza dei fotogrammi elevata, si consiglia di utilizzare le versioni più recenti dell'app Citrix Workspace per Windows e dell'app Citrix Workspace per Linux. Per ulteriori informazioni sulle versioni supportate dell'app Citrix Workspace, vedere Le tappe del ciclo di vita dell'app Citrix Workspace.

Esempi di applicazioni professionali 3D includono:

- Applicazioni di progettazione, produzione e ingegneria assistita da computer (CAD/CAM/CAE)
- Software per il sistema informativo geografico (GIS)
- PACS (Picture Archiving Communication System) per diagnostica per immagini medicale
- Applicazioni che utilizzano le ultime versioni di OpenGL, DirectX, NVIDIA CUDA, OpenCL e WebGL
- Applicazioni non grafiche a uso intensivo di calcolo che utilizzano GPU CUDA (Compute Unified Device Architecture) NVIDIA per l'elaborazione parallela

HDX 3D Pro offre la migliore esperienza utente su qualsiasi larghezza di banda:

- Sulle connessioni WAN: offre un'esperienza utente interattiva sulle connessioni WAN con larghezze di banda fino a 1,5 Mbps.
- Connessioni LAN: offre un'esperienza utente equivalente a quella di un desktop locale sulle connessioni LAN.

  È possibile sostituire workstation complesse e costose con dispositivi utente più semplici spostando l'elaborazione grafica nel data center per una gestione centralizzata.

HDX 3D Pro fornisce accelerazione GPU per le macchine con sistema operativo Windows a sessione singola e macchine con sistema operativo multisessione Windows. Per ulteriori informazioni, vedere Accelerazione GPU per il sistema operativo Windows a sessione singola e Accelerazione GPU per il sistema operativo multisessione Windows.

HDX 3D Pro è compatibile con le tecnologie di virtualizzazione GPU passthrough e GPU offerte dai seguenti hypervisor, oltre al bare metal:

- Citrix Hypervisor
  - Passthrough GPU con NVIDIA GRID, AMD e Intel GVT-d
  - Virtualizzazione GPU con NVIDIA GRID, AMD e Intel GVT-G
  - Vedere la compatibilità hardware in Elenco di compatibilità hardware di Hypervisor.

Utilizzare lo strumento HDX Monitor per convalidare il funzionamento e la configurazione delle tecnologie di visualizzazione HDX e per diagnosticare e risolvere i problemi HDX. Lo strumento è disponibile nella cartella **Support** sul supporto di installazione di Citrix Virtual Apps and Desktops.

# Accelerazione GPU per il sistema operativo multisessione Windows

January 7, 2024

HDX 3D Pro consente di eseguire il rendering di applicazioni ad utilizzo intensivo di grafica in esecuzione in sessioni di sistema operativo multisessione Windows sulla GPU (unità di elaborazione grafica) del server. Spostando il rendering OpenGL, DirectX, Direct3D e WPF (Windows Presentation Foundation) sulla GPU del server, il rendering grafico non rallenta la CPU del server. Inoltre, il server è in grado di elaborare più grafica perché il carico di lavoro è diviso tra CPU e GPU.

Poiché Windows Server è un sistema operativo multiutente, più utenti possono condividere una GPU accessibile da Citrix Virtual Apps senza la necessità di virtualizzazione GPU (vGPU).

Per le procedure che includono la modifica del Registro di sistema, procedere con cautela: la modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

## Condivisione GPU

Condivisione GPU consente il rendering hardware GPU delle applicazioni OpenGL e DirectX nelle sessioni desktop remote. Ha le seguenti caratteristiche:

- Può essere utilizzato su macchine bare metal o virtuali per aumentare la scalabilità e le prestazioni delle applicazioni.
- Consente a più sessioni simultanee di condividere le risorse GPU (la maggior parte degli utenti non richiede le prestazioni di rendering di una GPU dedicata).
- Non richiede impostazioni speciali.

Una GPU può essere assegnata alla macchina virtuale Windows Server in modalità pass-through completa o GPU virtuale (vGPU) in base ai requisiti del fornitore di Hypervisor e GPU. Sono supportate anche distribuzioni bare metal su computer Windows Server fisici.

Condivisione GPU non necessita di alcuna scheda grafica specifica.

- Per le macchine virtuali, selezionare una scheda grafica compatibile con Hypervisor in uso. Per un elenco degli hardware compatibili con Citrix Hypervisor, vedere Elenco di compatibilità hardware di Hypervisor.
- Quando è in esecuzione su bare metal, si consiglia di avere una scheda di visualizzazione singola abilitata dal sistema operativo. Se nell'hardware sono installate più GPU, disattivarle tutte tranne una utilizzando Gestione periferiche.

La scalabilità tramite la condivisione GPU dipende da diversi fattori:

- Le applicazioni in esecuzione
- La quantità di RAM video che consumano
- La potenza di elaborazione della scheda grafica

Alcune applicazioni gestiscono l'insufficienza di RAM video meglio di altre. Se l'hardware viene sovraccaricato, potrebbe verificarsi un'instabilità o un arresto anomalo del driver della scheda grafica. Limitare il numero di utenti simultanei per evitare questo tipo di problemi.

Per confermare che l'accelerazione della GPU si stia verificando, utilizzare uno strumento di terze parti, ad esempio GPU-Z. GPU-Z è disponibile all'indirizzo http://www.techpowerup.com/gpuz/.

- Accesso a un codificatore video ad alte prestazioni per GPU NVIDIA e processori grafici Intel Iris Pro. Un'impostazione dei criteri (abilitata per impostazione predefinita) controlla questa funzione e consente l'uso della codifica hardware per la codifica H.264 (se disponibile). Se tale hardware non è disponibile, il VDA effettua un fallback sulla codifica basata su CPU utilizzando il codec video software. Per ulteriori informazioni, vedere Impostazioni dei criteri di grafica.

### Rendering DirectX, Direct3D e WPF

Il rendering DirectX, Direct3D e WPF è disponibile solo sui server con una GPU che supporta una versione DDI (Display Driver Interface) 9ex, 10 o 11.

- In Windows Server 2008 R2, DirectX e Direct3D non richiedono impostazioni speciali per l'utilizzo di una singola GPU.
- In Windows Server 2012 e versioni successive, le sessioni di Servizi Desktop remoto nel server Host sessione Desktop remoto utilizzano il Driver rendering base Microsoft come scheda predefinita. Per utilizzare la GPU nelle sessioni di Servizi Desktop remoto in Windows Server 2012 e versioni successive, attivare l'impostazione **Usa la scheda grafica predefinita per l'hardware per tutte le sessioni di Servizi Desktop remoto** nel Criterio di gruppo **Criteri del computer locale** > **Configurazione computer** > **Modelli amministrativi** > **Componenti di Windows** > **Servizi Desktop remoto** > **Host sessione Desktop remoto**> **Ambiente sessione remota**.
- Per abilitare il rendering delle applicazioni WPF utilizzando la GPU del server, creare le impostazioni nel Registro di sistema del server che esegue sessioni del sistema operativo multisessione Windows. Per informazioni sulle impostazioni del Registro di sistema, vedere Rendering Windows Presentation Foundation (WPF) nell'elenco delle funzionalità gestite tramite il Registro di sistema.

### Accelerazione GPU per applicazioni CUDA o OpenCL

L'accelerazione GPU delle applicazioni CUDA e OpenCL in esecuzione in una sessione utente è disabilitata per impostazione predefinita.

Per utilizzare le funzionalità POC di accelerazione CUDA, abilitare le impostazioni del Registro di sistema. Per informazioni, vedere Accelerazione GPU per applicazioni CUDA o OpenCL nell'elenco delle funzionalità gestite tramite il Registro di sistema.

## Accelerazione GPU per il sistema operativo Windows a sessione singola

January 7, 2024

Con HDX 3D Pro, è possibile distribuire applicazioni a uso intensivo della grafica nell'ambito di desktop o applicazioni ospitati su computer con sistema operativo a sessione singola. HDX 3D Pro supporta computer host fisici (tra cui workstation desktop, blade e rack) e le tecnologie di virtualizzazione GPU Passthrough e GPU offerte da Citrix Hypervisor, vSphere, Nutanix e Hyper-V (solo passthrough).

HDX 3D Pro offre le seguenti funzionalità:

- Compressione profonda adattiva basata su H.264 o H.265 per prestazioni WAN e wireless ottimali. HDX 3D Pro utilizza la compressione H.264 a schermo intero basata su CPU come tecnica di compressione predefinita per la codifica. La codifica hardware con H.264 viene utilizzata con schede NVIDIA, Intel e AMD che supportano NVENC. La codifica hardware con H.265 viene utilizzata con schede NVIDIA che supportano NVENC.
- Opzione di compressione senza perdita di dati per casi d'uso specializzati. HDX 3D Pro offre anche un codec senza perdita di dati basato su CPU per supportare applicazioni in cui è richiesta una grafica con pixel perfetti, come per l'imaging medicale. La compressione senza perdita di dati vera e propria è consigliata solo per casi d'uso specializzati in quanto consuma più risorse di rete e di elaborazione.

  Quando si utilizza la compressione senza perdita di dati:

  - L'indicatore senza perdita, un'icona dell'area di notifica, notifica l'utente se lo schermo visualizzato è un frame con perdita di dati o un frame senza perdita di dati. Questa icona aiuta quando l'impostazione del criterio **Qualità visiva** specifica **Compila per senza perdite**. L'indicatore senza perdita diventa verde quando i fotogrammi inviati sono senza perdita di dati.
  - L'interruttore senza perdita di dati consente all'utente di passare alla modalità Sempre senza perdite in qualsiasi momento all'interno della sessione. Per selezionare o deselezionare **Senza perdite in qualsiasi momento all'interno di una sessione**, fare clic con

il pulsante destro del mouse sull'icona e fare clic su **Passa al pixel perfetto** oppure utilizzare la scelta rapida da tastiera ALT+MAIUSC+1.

Per la compressione senza perdita di dati: HDX 3D Pro utilizza il codec lossless per la compressione indipendentemente dal codec selezionato tramite criterio.

Per la compressione con perdita di dati: HDX 3D Pro utilizza il codec originale, quello predefinito o quello selezionato tramite criterio.

Le impostazioni dell'interruttore senza perdita di dati non vengono mantenute per le sessioni successive. Per utilizzare un codec senza perdita per ogni connessione, selezionare **Sempre senza perdite** nell'impostazione dei criteri **Qualità visiva**.

- È possibile ignorare la scelta rapida da tastiera predefinita ALT+MAIUSC+1 per selezionare o deselezionare Senza perdite all'interno di una sessione. Configurare una nuova impostazione del Registro di sistema in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator.
  - Nome: HKEY_LOCAL_MACHINE_HotKey, Type: String
  - Il formato per configurare una combinazione di collegamenti è C=0|1, A=0|1, S=0|1, W=0|1, K=val. Le chiavi devono essere separate da virgola ",". L'ordine delle chiavi non ha importanza.
  - A, C, S, W e K sono chiavi, dove C = Control, A = ALT, S = SHIFT, W=Win e K = una chiave valida. I valori consentiti per K sono 0-9, a-z e qualsiasi codice chiave virtuale.
  - Ad esempio:
    - Per F10, impostare K=0x79
    - Per Ctrl + F10, impostare C=1, K=0x79
    - Per Alt + A, impostare A=1, K=a o A=1, K=A o K=A, A=1
    - Per Ctrl + Alt + 5, impostare C=1, A=1, K=5 o A=1, K=5, C=1
    - Per Ctrl + Maiusc + F5 impostare A=1, S=1, K=0x74

> **Attenzione:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

- Supporto di più monitor e di monitor ad alta risoluzione. Per i sistemi operativi a sessione singola, HDX 3D Pro supporta dispositivi utente con un massimo di quattro monitor. Gli utenti possono disporre i monitor in qualsiasi configurazione e combinare monitor con diverse risoluzioni e orientamenti. Il numero di monitor è limitato dalle funzionalità della GPU del computer host, dal dispositivo utente e dalla larghezza di banda disponibile. HDX 3D Pro supporta tutte le risoluzioni dei monitor ed è limitato solo dalle funzionalità della GPU sul computer host.

- Risoluzione dinamica. È possibile ridimensionare il desktop virtuale o la finestra dell'applicazione a qualsiasi risoluzione. **Nota**: l'unico metodo supportato per modificare la risoluzione è ridimensionare la finestra della sessione VDA. La modifica della risoluzione dalla sessione VDA (utilizzando **Pannello di controllo > Aspetto** e **personalizzazione > Schermo > Risoluzione dello schermo) non è supportata**.
- Supporto per l'architettura vGPU NVIDIA. HDX 3D Pro supporta schede vGPU NVIDIA. Per informazioni, consultare vGPU NVIDIA per il passthrough della GPU e la condivisione della GPU. La vGPU NVIDIA consente a più VM di avere accesso diretto e simultaneo a una singola GPU fisica, utilizzando gli stessi driver grafici NVIDIA che sono stati distribuiti sui sistemi operativi non virtualizzati.
- Supporto per VMware vSphere e VMware ESX tramite Virtual Direct Graphics Acceleration (vDGA): è possibile utilizzare HDX 3D Pro con vDGA per carichi di lavoro sia RDS che VDI.
- Supporto per VMware vSphere/ESX utilizzando vGPU NVIDIA e AMD MxGPU.
- Supporto per Microsoft HyperV utilizzando DDA (Discrete Device Assignment) in Windows Server 2016.
- Supporto per la grafica dei data center con famiglia di processori Intel Xeon E3. HDX 3D Pro supporta più monitor (fino a 3), cancellazione del contenuto della console, risoluzione personalizzata e frequenza dei fotogrammi elevata con la famiglia di processori Intel supportata. Per ulteriori informazioni, vedere http://www.citrix.com/intel e http://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- Supporto per AMD RapidFire sulle schede server AMD FirePro serie S. HDX 3D Pro supporta più monitor (fino a 6), cancellazione del contenuto della console, risoluzione personalizzata e frequenza dei fotogrammi elevata. Nota: il supporto HDX 3D Pro per AMD MxGPU (virtualizzazione GPU) funziona solo con VMware vSphere vGPU. Citrix Hypervisor e Hyper-V sono supportati con il passthrough della GPU. Per ulteriori informazioni, vedere Soluzione di virtualizzazione AMD.
- Accesso a un codificatore video ad alte prestazioni per GPU NVIDIA, GPU AMD e processori grafici Intel Iris Pro. Un'impostazione di criterio (attivata per impostazione predefinita) controlla questa funzionalità. La funzione consente l'utilizzo della codifica hardware per la codifica H.264 (ove disponibile). Se tale hardware non è disponibile, il VDA torna alla codifica basata su CPU utilizzando il codec video software. Per ulteriori informazioni, vedere Impostazioni dei criteri di grafica.

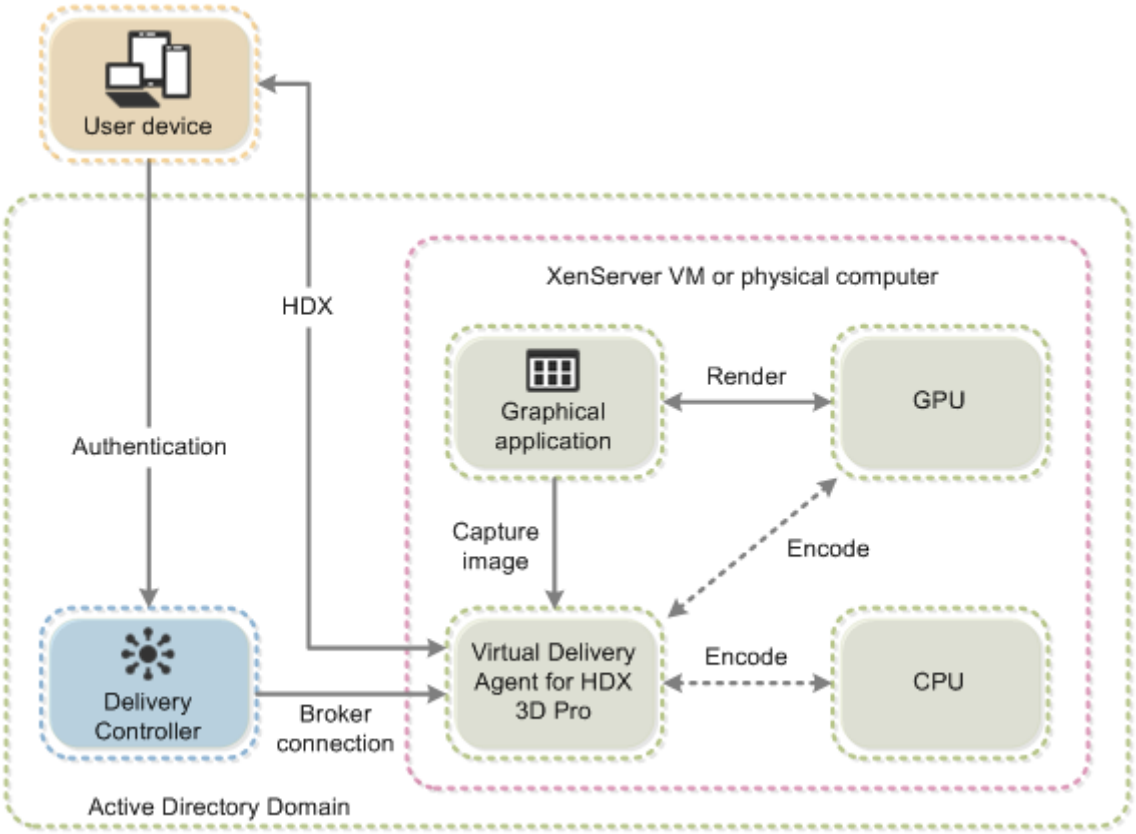
Come illustrato nella figura seguente:

- Quando un utente effettua l'accesso all'app Citrix Workspace e accede all'applicazione virtuale o al desktop, il controller autentica l'utente. Il controller contatta quindi il VDA per HDX 3D Pro per mediare una connessione al computer che ospita l'applicazione grafica.

Il VDA per HDX 3D Pro utilizza l'hardware appropriato sull'host per comprimere le viste del desktop completo o solo dell'applicazione grafica.

- Le viste del desktop o dell'applicazione e le interazioni utente con esse vengono trasmesse tra il computer host e il dispositivo utente. Questa trasmissione avviene tramite una connessione HDX diretta tra l'app Citrix Workspace e il VDA per HDX 3D Pro.




### Ottimizzare l'esperienza utente con HDX 3D Pro

Quando più utenti condividono una connessione con larghezza di banda limitata (ad esempio, in una succursale), è consigliabile utilizzare l'impostazione del criterio **Limite larghezza di banda sessione complessiva** per limitare la larghezza di banda disponibile per ciascun utente. L'utilizzo di questa impostazione garantisce che la larghezza di banda disponibile non oscilli notevolmente quando gli utenti accedono e si scollegano. Poiché HDX 3D Pro si regola automaticamente per utilizzare tutta la larghezza di banda disponibile, grandi variazioni della larghezza di banda disponibile nel corso delle sessioni utente possono influire negativamente sulle prestazioni.

Ad esempio, se 20 utenti condividono una connessione a 60 Mbps, la larghezza di banda disponibile per ciascun utente può variare tra 3 Mbps e 60 Mbps, a seconda del numero di utenti simultanei. Per ottimizzare l'esperienza utente in questo scenario, determinare la larghezza di banda richiesta per utente nei periodi di punta e limitare sempre gli utenti a tale cifra.

Per gli utenti di un mouse 3D, si consiglia di aumentare la priorità del canale virtuale di Reindirizzamento USB generico a 0. Per informazioni sulla modifica della priorità del canale virtuale, vedere l'articolo del Knowledge Center CTX128190.

# Thinwire

January 7, 2024

## Introduzione

Thinwire, parte della tecnologia Citrix HDX, è la tecnologia di visualizzazione predefinita Citrix utilizzata in Citrix Virtual Apps and Desktops.

La tecnologia di visualizzazione remota consente la trasmissione della grafica generata su un computer, in genere attraverso una rete, a un altro computer per la visualizzazione.

Una soluzione di visualizzazione remota che funziona correttamente offre un'esperienza utente altamente interattiva simile a quella di un PC locale. Thinwire realizza questa esperienza utilizzando una serie di tecniche di analisi e compressione delle immagini complesse ed efficienti. Thinwire ottimizza la scalabilità dei server e consuma meno larghezza di banda rispetto ad altre tecnologie di telecomunicazione.

Grazie a questo equilibrio, Thinwire soddisfa la maggior parte dei casi d'uso aziendali generali e viene utilizzato come tecnologia di visualizzazione remota predefinita in Citrix Virtual Apps and Desktops.

## HDX 3D Pro

Nella configurazione predefinita, Thinwire può fornire grafica 3D o altamente interattiva e utilizzare un'unità di elaborazione grafica (GPU), se presente. Tuttavia, si consiglia di attivare la modalità HDX 3D Pro utilizzando i criteri **Optimize for 3D graphics workload** (Ottimizza per i carichi di lavoro con grafica 3D) o **Qualità visiva > Compila per senza perdite** per scenari in cui sono presenti GPU. Questi criteri configurano Thinwire per utilizzare un codec video (H.264 o H.265) per codificare l'intero schermo utilizzando l'accelerazione hardware se è presente una GPU. Così facendo offre un'esperienza più fluida per la grafica professionale 3D. Per ulteriori informazioni, vedere H.264 Build to lossless (H.264 Compila per senza perdite), HDX 3D Pro e Accelerazione GPU per il sistema operativo Windows a sessione singola.

## Requisiti

Thinwire è ottimizzato per i sistemi operativi moderni, tra cui Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10 e Windows 7. Per Windows Server 2008 R2, è consigliata la modalità grafica legacy. Utilizzare i Modelli di criteri Citrix integrati, il sistema operativo legacy ad alta scalabilità server e ottimizzato per il sistema operativo legacy WAN per fornire le combinazioni di impostazioni dei criteri consigliate da Citrix per questi casi d'uso.

> **Nota:**
>
> In questa versione non è supportata la modalità grafica legacy. È inclusa per la compatibilità con le versioni precedenti quando si utilizza XenApp 7.15 LTSR, XenDesktop 7.15 LTSR e le versioni di VDA precedenti con Windows 7 e Windows 2008 R2.

- L'impostazione dei criteri che guida il comportamento di Thinwire, **Use video codec for compression**, è disponibile nelle versioni di VDA contenute in Citrix Virtual Apps and Desktops 7 1808 o versioni successive e XenApp e XenDesktop 7.6 FP3 e versioni successive. L'opzione **Use video codec when preferred** è l'impostazione predefinita sulle versioni di VDA di Citrix Virtual Apps and Desktops 7 1808 o successive e XenApp e XenDesktop 7.9 e versioni successive.
- Tutte le app Citrix Workspace supportano Thinwire. Alcune app Citrix Workspace potrebbero supportare funzionalità di Thinwire che altre non supportano, ad esempio, grafica a 8 bit o 16 bit per ridurre l'utilizzo della larghezza di banda. Il supporto di tali funzionalità viene negoziato automaticamente dall'app Citrix Workspace.
- Thinwire utilizza più risorse server (CPU, memoria) in scenari multi-monitor e ad alta risoluzione. È possibile ottimizzare la quantità di risorse utilizzate da Thinwire. Tuttavia, l'utilizzo della larghezza di banda potrebbe aumentare di conseguenza.
- In scenari a bassa larghezza di banda o ad alta latenza, è possibile abilitare la grafica a 8 o 16 bit per migliorare l'interattività. La qualità visiva potrebbe essere influenzata, soprattutto con profondità di colore a 8 bit.

## Metodi di codifica

Thinwire può operare in due diverse modalità di codifica a seconda dei criteri e delle funzionalità del client:

- Schermo intero Thinwire H.264 o H.265
- Thinwire con H.264 o H.265 selettivo

La tecnologia remota GDI legacy utilizza il driver remoto XPDM e non un codificatore bitmap Thinwire.

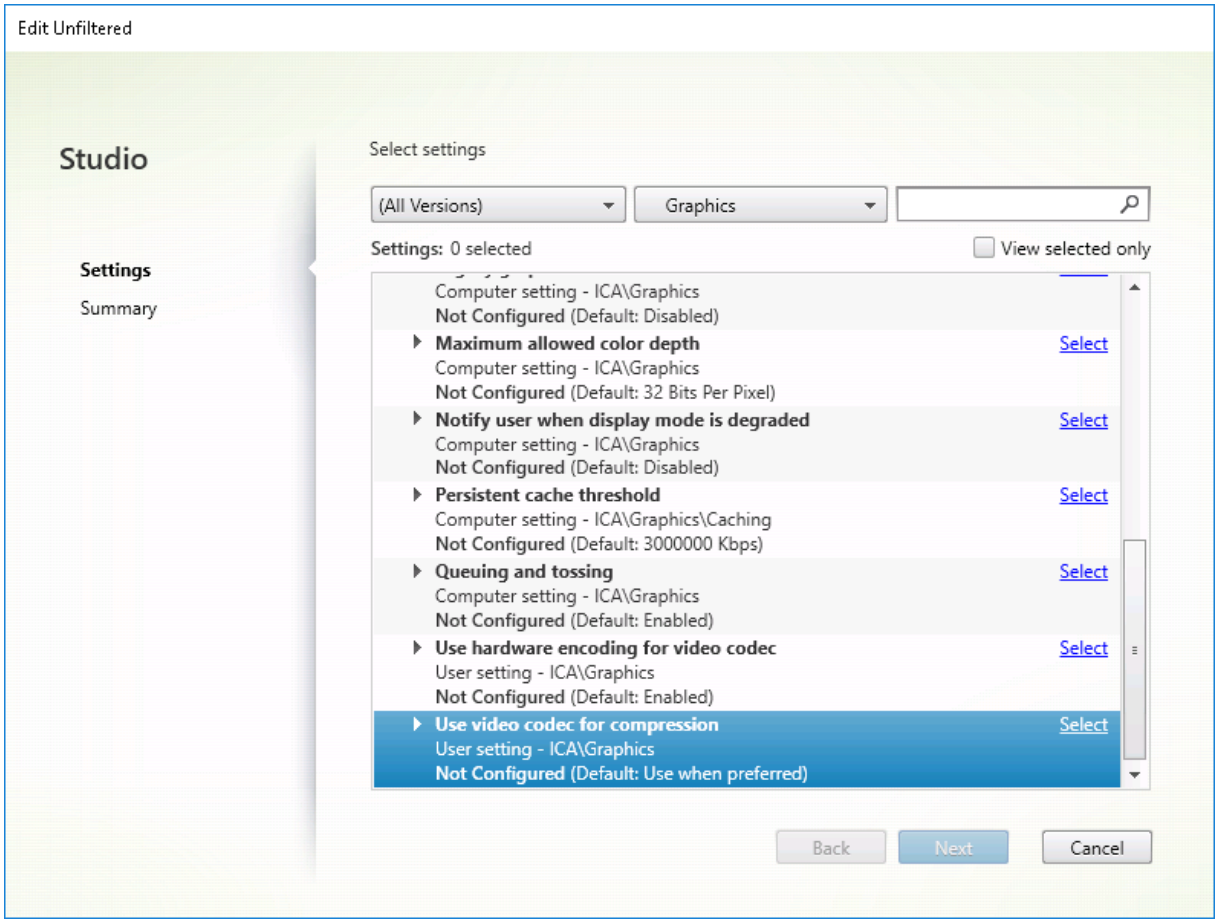
### Configurazione

Thinwire è la tecnologia di visualizzazione remota predefinita.

La seguente impostazione dei criteri di grafica imposta il valore predefinito e fornisce alternative per i diversi casi d'uso:

- Use video codec for compression (Usa codec video per la compressione)
  - **Use video codec when preferred** (Usa video codec quando preferito). Questa è l'impostazione predefinita. Non è richiesta alcuna configurazione aggiuntiva. Mantenere questa impostazione come predefinita garantisce che Thinwire sia selezionato per tutte le connessioni Citrix e sia ottimizzato per scalabilità, larghezza di banda e qualità dell'immagine superiore per i carichi di lavoro desktop tipici. Questo è funzionalmente equivalente a **For actively changing regions** (Per cambiare attivamente le regioni).
- Altre opzioni di questa impostazione di criteri continuano a utilizzare Thinwire con altre tecnologie per diversi casi d'uso. Ad esempio:
  - **For actively changing regions**. La tecnologia di visualizzazione adattiva di Thinwire identifica le immagini in movimento (video, 3D in movimento) e utilizza H.264 o H.265 solo nella parte dello schermo in cui si muove l'immagine.
  - **For the entire screen** (Per l'intero schermo). Fornisce Thinwire con schermo intero H.264 o H.265 per l'ottimizzazione migliorando l'esperienza utente e la larghezza di banda in caso di utilizzo intensivo della grafica 3D. Nel caso di H.264 4:2:0 (il criterio **Visually lossless** (Visivamente senza perdite) è disabilitato), l'immagine finale non è a pixel perfetto (senza perdite) e potrebbe non essere adatta per determinati scenari. In questi casi, prendere in considerazione l'utilizzo alternativo di H.264 Build to lossless (H.264 Compila per senza perdite).




È possibile utilizzare diverse altre impostazioni dei criteri, incluse le seguenti impostazioni dei criteri di visualizzazione visiva per ottimizzare le prestazioni della tecnologia di visualizzazione remota. Thinwire li supporta tutti.

- Profondità di colore preferita per grafiche semplici
- Target frame rate (Frequenza fotogrammi target)
- Qualità visiva

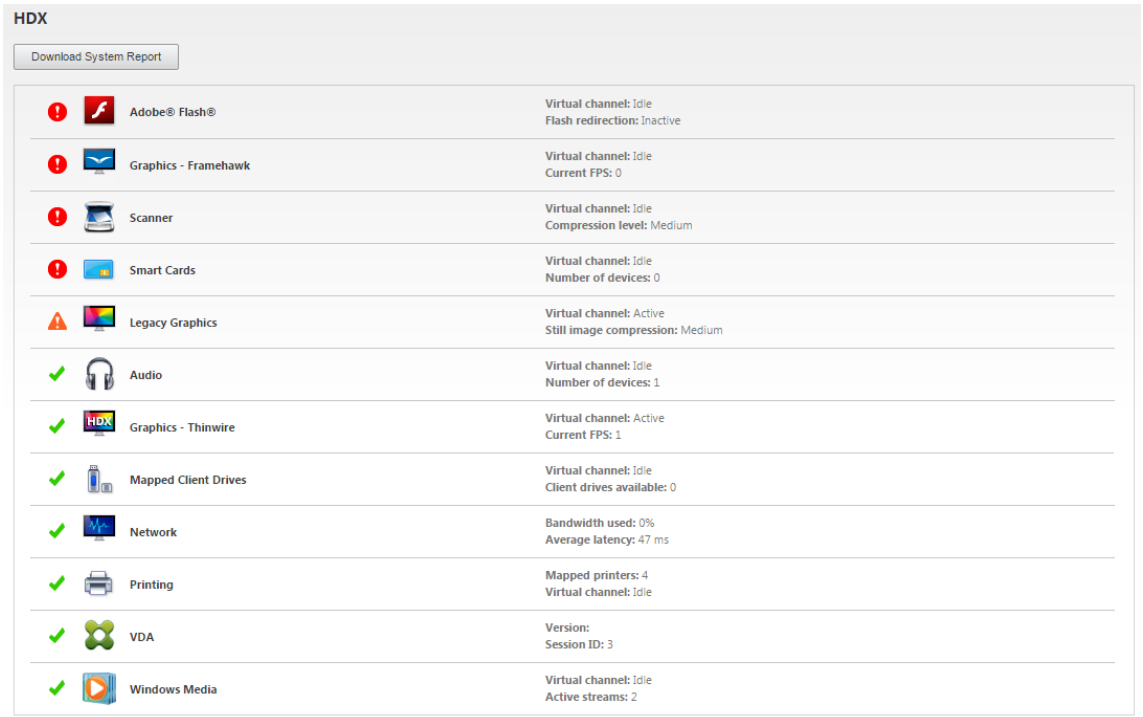
Per ottenere le combinazioni di impostazioni dei criteri per diversi casi di utilizzo aziendale consigliate da Citrix, utilizzare i Modelli di criteri Citrix incorporati. I modelli **High Server Scalability** (Elevata scalabilità del server) e **Very High Definition User Experience** (Esperienza utente ad altissima definizione) utilizzano entrambi Thinwire con la combinazione ottimale di impostazioni dei criteri per le priorità dell'organizzazione e le aspettative degli utenti.

### Monitorare Thinwire

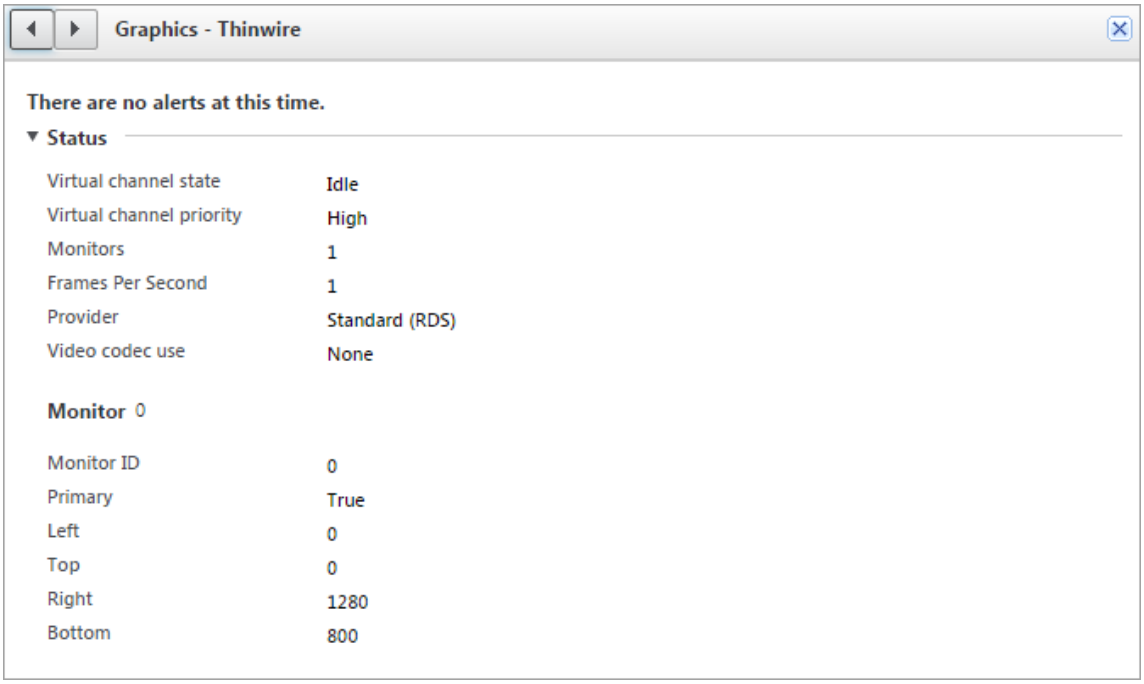
È possibile monitorare l'utilizzo e le prestazioni di Thinwire da Citrix Director. La vista dei dettagli del canale virtuale HDX contiene informazioni utili per la risoluzione dei problemi e il monitoraggio di Thinwire in qualsiasi sessione. Per visualizzare le metriche relative a Thinwire:

1. In Director cercare un utente, un computer o un endpoint, aprire una sessione attiva e fare clic su **Dettagli**. In alternativa, è possibile selezionare **Filtri** > **Sessioni** > **Tutte le sessioni**, aprire una sessione attiva e fare clic su **Dettagli**.
2. Scorrere verso il basso fino al pannello **HDX**.




3. Selezionare **Graphics - Thinwire**.



### Codec di compressione senza perdite (MDRLE)

In una tipica sessione desktop, la maggior parte delle immagini è grafica semplice o contiene regioni di testo. Thinwire determina la posizione di queste regioni e seleziona queste aree per la codifica senza perdita di dati utilizzando il codec 2DRLE. Sul lato client dell'app Citrix Workspace, questi elementi vengono decodificati utilizzando il decodificatore 2DRLE lato app Citrix Workspace per la visualizzazione delle sessioni.

In XenApp e XenDesktop 7.17, abbiamo aggiunto un codec MDRLE con rapporto di compressione più elevato che consuma meno larghezza di banda nelle sessioni desktop tipiche rispetto al codec 2DRLE. Questo nuovo codec non influisce sulla scalabilità del server.

La larghezza di banda inferiore di solito comporta un miglioramento dell'interattività delle sessioni (specialmente su collegamenti condivisi o vincolati) e una riduzione dei costi. Ad esempio, il consumo di larghezza di banda previsto quando si utilizza il codec MDRLE è di circa il 10-15% in meno rispetto a XenApp e XenDesktop 7.15 LTSR per i carichi di lavoro tipici di Office.

Non è richiesta configurazione per il codec MDRLE. Se l'app Citrix Workspace supporta la decodifica MDRLE, il VDA utilizza la codifica VDA MDRLE e la decodifica MDRLE dell'app Citrix Workspace. Se l'app Citrix Workspace non supporta la decodifica MDRLE, il VDA effettua automaticamente il fallback alla codifica 2DRLE.

**Requisiti di MDRLE:**

- VDA Citrix Virtual Apps and Desktops versione minima 7 1808.
- VDA XenApp e XenDesktop versione minima 7.17.
- App Citrix Workspace per Windows versione minima 1808
- Citrix Receiver per Windows versione minima 4.11

### Modalità progressiva

Citrix Virtual Apps and Desktops 1808 ha introdotto la modalità progressiva che è abilitata per impostazione predefinita. In condizioni di rete vincolate (impostazione predefinita: larghezza di banda <2 Mbps o latenza >200 ms), Thinwire ha aumentato la compressione del testo e delle immagini statiche per migliorare l'interattività durante l'attività dello schermo. Il testo e le immagini fortemente compressi diventano quindi progressivamente più nitidi, in modo casuale, quando l'attività dello schermo si interrompe. Questo tipo di compressione e di aumento della nitidezza migliorano l'interattività generale, riducendo al contempo l'efficienza della cache e aumentando l'utilizzo della larghezza di banda.

A partire da Citrix Virtual Apps and Desktops 1906, la modalità progressiva è disabilitata per impostazione predefinita. Ora adottiamo un approccio diverso. La qualità delle immagini fisse è ora basata sulle condizioni della rete e fluttua tra un valore minimo e massimo predefiniti per

ogni impostazione della **qualità visiva**. Poiché non esiste una fase esplicita di nitidezza, Thinwire ottimizza la distribuzione delle immagini e mantiene l'efficienza della cache, offrendo al contempo quasi tutti i vantaggi della modalità progressiva.

#### Modifica del comportamento in modalità progressiva

È possibile modificare lo stato della modalità progressiva con la chiave del Registro di sistema. Per informazioni, vedere Modalità progressiva nell'elenco delle funzionalità gestite tramite il Registro di sistema.

### H.264 Build to lossless (H.264 Compila per senza perdite)

**Compila per senza perdite** è una speciale configurazione di Thinwire che ottimizza la distribuzione grafica per l'interattività e la qualità dell'immagine finale. È possibile attivare questa impostazione impostando il criterio **Qualità visiva** su **Compila per senza perdite**.

Compila per senza perdite comprime lo schermo utilizzando H.264 (o H.265) durante l'attività dello schermo e lo rende più nitido fino a pixel perfetti (senza perdite) quando l'attività si interrompe. La qualità dell'immagine H.264 (o H.265) si adatta alle risorse disponibili per mantenere la frequenza dei fotogrammi migliore possibile. La fase di aumento della nitidezza viene eseguita gradualmente, dando una risposta immediata se l'utente inizia l'attività sullo schermo poco dopo l'inizio della fase. Ad esempio, selezionando un modello e ruotandolo.

H.264 **Compila per senza perdite** offre tutti i vantaggi di H.264 o H.265 a schermo intero, inclusa l'accelerazione hardware, ma con l'ulteriore vantaggio di uno schermo finale garantito senza perdita di dati. Questo è fondamentale per i carichi di lavoro di tipo 3D che richiedono un'immagine finale con pixel perfetti. Ad esempio, nella manipolazione della diagnostica per immagini medicale. Inoltre, H.264 **Compila per senza perdite** utilizza meno risorse rispetto allo schermo intero H.264 4:4:4. Di conseguenza, l'uso di **Compila per senza perdite** di solito si traduce in una frequenza di fotogrammi più elevata rispetto a Visivamente senza perdite H.264 4:4:4.

> **Nota:**
>
> Oltre al criterio **Qualità visiva**, impostare il criterio **Use video codec** (Usa codec video) su **Use when preferred** (Usa quando preferito) (impostazione predefinita) o **For actively changing regions** (Per cambiare attivamente le regioni). È possibile ripristinare la condizione senza H.264 Compila per senza perdite impostando il criterio **Use video codec** su **Do not use video codec** (Non utilizzare codec video). In questo modo le immagini in movimento vengono codificate con JPEG anziché H.264 (o H.265).

# Filigrana di sessione basata su testo

January 7, 2024

Le filigrane di sessione basate su testo aiutano a scoraggiare e abilitare il furto dei dati di tracciabilità. Queste informazioni tracciabili vengono visualizzate sul desktop della sessione come deterrente per coloro che utilizzano fotografie e acquisizioni dello schermo per rubare i dati. È possibile specificare una filigrana che sia uno strato di testo, che viene visualizzato sull'intera schermata della sessione senza modificare il contenuto del documento originale. Le filigrane di sessione basate su testo richiedono il supporto VDA.

> **Importante:**
>
> l'applicazione di filigrana di sessione basata su testo non è una funzionalità di sicurezza. La soluzione non impedisce completamente il furto di dati, ma funge da deterrente e fornisce un certo livello di tracciabilità. Sebbene non garantiamo la completa tracciabilità delle informazioni quando si utilizza questa funzione, si consiglia di combinare questa funzionalità con altre soluzioni di sicurezza, come necessario.

La filigrana di sessione è testo e viene applicata alla sessione che viene consegnata all'utente. La filigrana di sessione contiene informazioni per il rilevamento del furto di dati. I dati più importanti sono l'identità dell'utente che ha effettuato l'accesso alla sessione corrente in cui è stata acquisita l'immagine dello schermo. Per tenere traccia della perdita di dati in modo più efficace, includere altre informazioni come l'indirizzo del protocollo Internet del server o del client e un tempo di connessione.

Per regolare l'esperienza utente, utilizzare le Impostazioni dei criteri per la Filigrana di sessione per configurare il posizionamento e l'aspetto della filigrana sullo schermo.

**Requisiti:**

Virtual Delivery Agent:

Sistema operativo multisessione 7.17
Sistema operativo a sessione singola 7.17

**Limitazioni:**

- Le filigrane di sessione non sono supportate nelle sessioni in cui vengono utilizzate funzionalità quali Accesso alle app locali, reindirizzamento dei supporti Windows, MediaStream, reindirizzamento dei contenuti del browser e reindirizzamento video HTML5. Per utilizzare la filigrana di sessione, assicurarsi che queste funzionalità siano disabilitate.
- La filigrana di sessione non è supportata e non viene visualizzata se la sessione è in esecuzione in modalità hardware accelerata a schermo intero (codifica H.264 o H.265 a schermo intero).

- Se si impostano questi criteri HDX, le impostazioni della filigrana non hanno effetto e non viene visualizzata una filigrana nella visualizzazione della sessione.

**Use hardware encoding for video codec** (Usa codifica hardware per il codec video) su **Enabled**
**Use video codec for compression** (Usa codec video per la compressione) su **For the entire screen** (Per l'intero schermo)

- Se si impostano questi criteri HDX, il comportamento non è determinato e la filigrana potrebbe non essere visualizzata.

  **Use hardware encoding for video codec** su **Enabled**
  **Use video codec for compression** su **Use video codec when preferred** (Usa video codec quando preferito)

  Per garantire la visualizzazione della filigrana, impostare **Use hardware encoding for video codec** su **Disabled** oppure impostare **Use video codec for compression** su **For actively changing regions** (Per cambiare attivamente le regioni) o **Do not use video codec** (Non utilizzare codec video).
- La filigrana di sessione supporta solo la modalità grafica Thinwire.
- Se si utilizza la funzione Registrazione sessione, la sessione registrata non include la filigrana.
- Se si utilizza l'assistenza remota di Windows, la filigrana non viene visualizzata.
- Se un utente preme il tasto **Stamp** per catturare lo schermo, la schermata catturata sul lato VDA non include le filigrane. Si consiglia di adottare misure per evitare che l'immagine acquisita venga copiata.

## Condivisione dello schermo

January 7, 2024

La condivisione dello schermo consente a un utente di condividere con altri una sessione di Citrix Virtual Desktop, incluso il controllo dei contenuti dello schermo, della tastiera e del mouse.

### Requisiti di sistema

- Windows: VDA con sistema operativo a sessione singola o multisessione
- Linux: vedere la documentazione di Linux VDA per maggiori informazioni sulla condivisione di sessioni Linux.
- È possibile condividere solo le sessioni desktop.

- Deve esserci connettività di rete tra il VDA che ospita la sessione e le macchine che si connettono alle sessioni condivise. I requisiti delle porte di rete si basano sulle porte ICA in uso (TCP/UDP 1494 o 2598) e sulla configurazione dei criteri di condivisione dello schermo (da TCP 52525 a 52625 per impostazione predefinita).

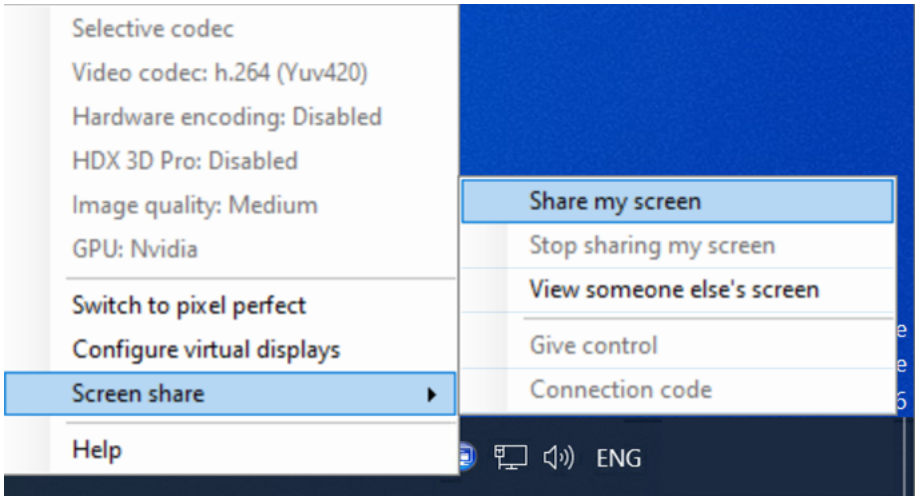
### Configurazione

La condivisione dello schermo deve essere abilitata utilizzando i criteri Citrix. La condivisione dello schermo è disabilitata per impostazione predefinita. Configurare i criteri di condivisione dello schermo per abilitare o disabilitare la funzione e assegnare l'intervallo di porte di rete utilizzabili.

Abilitare il criterio dell'indicatore di stato della grafica per visualizzare l'interfaccia utente che include i controlli per la condivisione e la connessione alle sessioni.

### Condividere una sessione

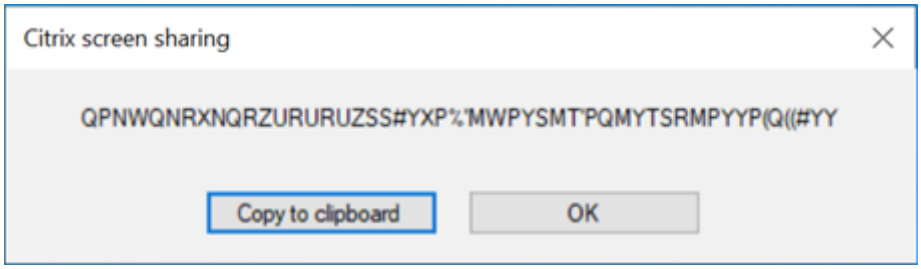
Per condividere una sessione, cercare l'icona dell'indicatore di stato della grafica HDX nell'area di notifica di Windows. Fare clic su di essa con il tasto destro per visualizzare il menu e selezionare **Screen share > Share my screen** (Condivisione schermo > Condividi il mio schermo).




Fare clic su **Copy to clipboard** (Copia negli Appunti) o selezionare e copiare manualmente l'intera stringa visualizzata nella finestra di dialogo. La stringa può quindi essere incollata nell'applicazione desiderata, ad esempio un client di posta elettronica o di messaggistica istantanea, per essere distribuita ad altri utenti.

Fare clic su **OK** o sulla **x** per chiudere la finestra di dialogo. Il codice di connessione può essere recuperato dall'opzione di menu **Screen share > Connection code** (Condivisione schermo > Codice di connessione) in qualsiasi momento mentre la sessione è condivisa.

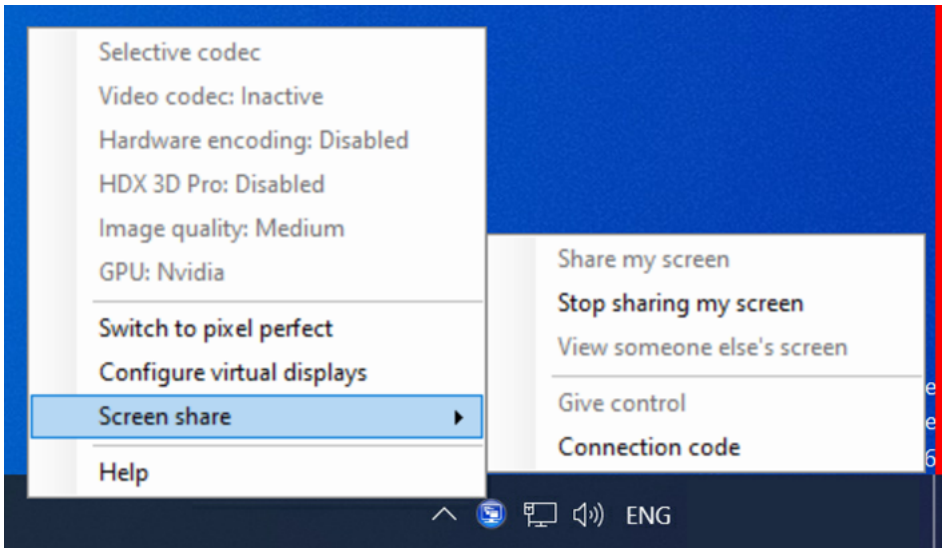
 




Intorno allo schermo appare un contorno rosso ad indicare che la sessione è ora condivisa ed è visibile da altri.

I controlli della tastiera e del mouse possono anche essere condivisi con altri utenti utilizzando l'opzione di menu **Screen share > Give control** (Condivisione schermo > Concedi il controllo).

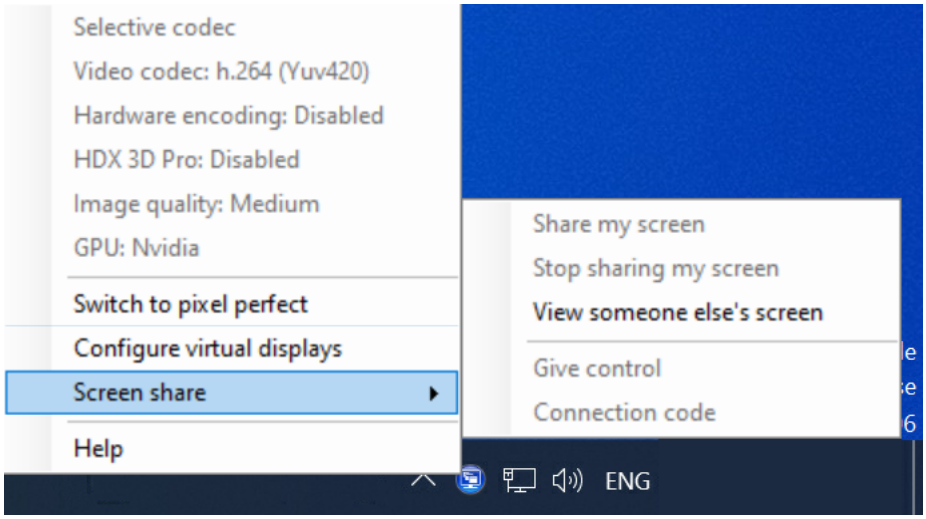
Utilizzare l'opzione di menu **Screen share > Stop sharing my screen** (Condivisione schermo > Interrompi la condivisione dello schermo) per interrompere la condivisione della sessione e disconnettere tutti gli utenti.



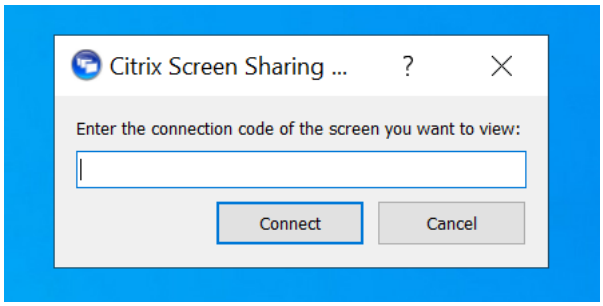

## Connettersi a una sessione condivisa

Per connettersi alle sessioni di un altro utente, cercare l'icona dell'indicatore di stato della grafica HDX nell'area di notifica di Windows. Fare clic su di essa con il tasto destro per visualizzare il menu e selezionare **Screen share > View someone else's screen** (Condivisione schermo > Visualizza lo schermo di qualcun altro).



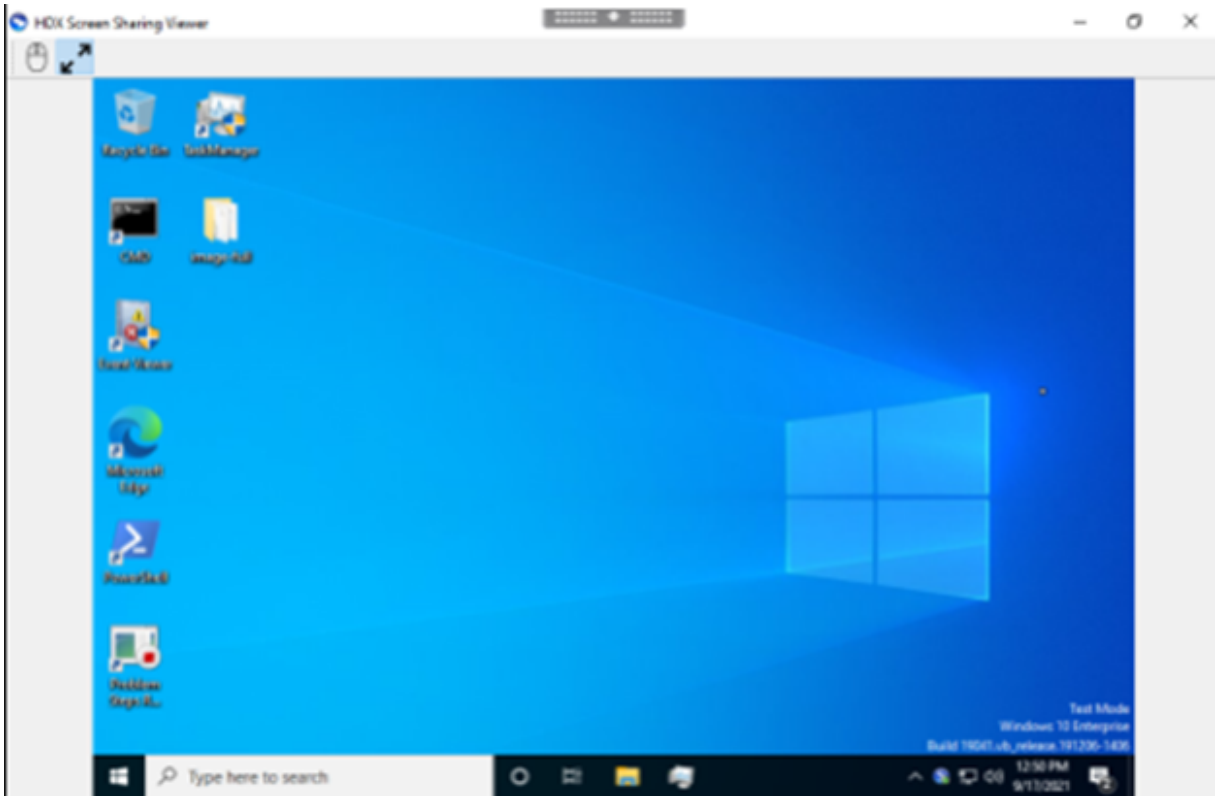

Immettere o incollare la stringa di connessione fornita dall'utente che ha condiviso la sessione nella casella di testo. Fare clic su **Connect** per stabilire la connessione.




È possibile richiedere i controlli da tastiera e mouse facendo clic sull'icona del mouse nell'angolo in alto a sinistra della finestra **HDX Screen Sharing Viewer**.

Chiudere la finestra **HDX Screen Sharing Viewer** per disconnettersi dalla sessione condivisa in qualsiasi momento.




### Altre considerazioni

- L'applicazione di visualizzazione della condivisione dello schermo è inclusa nel VDA in *C:\Programmi\Citrix\HDX\bin\TwPlayer.exe* e potrebbe essere distribuita come applicazione pubblicata utilizzando un Virtual Apps Server. Questo modello di distribuzione alternativo consente la collaborazione con utenti che non hanno accesso a un desktop virtuale.
- Il numero di utenti autorizzati a connettersi a una sessione condivisa può essere limitato utilizzando l'intervallo di porte di rete nei criteri di condivisione dello schermo. È richiesta una porta per utente. L'intervallo predefinito consente un massimo di 100 utenti.
- Tutti i monitor collegati alla sessione sono condivisi. Non è possibile selezionare singoli monitor.
- Il codec video H.265 non è supportato.

## Layout del display virtuale

January 7, 2024

L'interfaccia utente di configurazione del display virtuale consente di definire un layout di visualizzazione virtuale per i monitor di sessione sul VDA, all'interno di una sessione live. Questa funzione

consente di dividere in modo indipendente ogni monitor di sessione in più monitor virtuali. È possibile dividerlo in un totale di 8 monitor virtuali sul desktop remoto. Inoltre, è possibile aggiornare il monitor principale della sessione e le impostazioni DPI per i display.

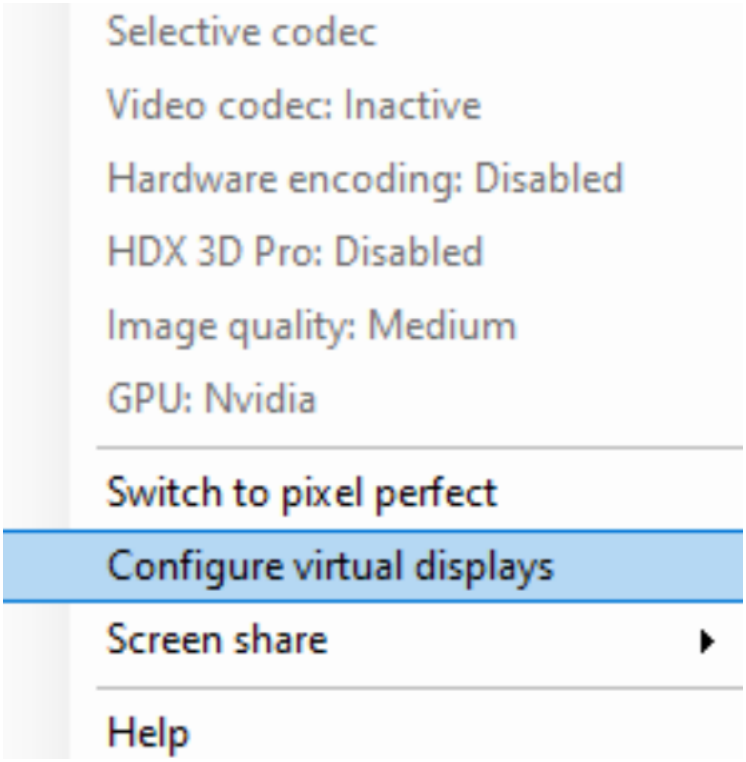
La configurazione del display virtuale definita viene memorizzata per utente per dispositivo client. La configurazione si applica a tutte le connessioni successive provenienti da un determinato client per a un determinato utente. Viene mantenuta durante il ridimensionamento della sessione, la disconnessione o riconnessione della sessione e lo scollegamento o l'accesso alla sessione. Il ripristino del layout dello schermo virtuale configurato si verifica al momento del ridimensionamento di una sessione e alla modifica del numero di monitor di sessione.

### Requisiti di sistema

- Windows: VDA con sistema operativo a sessione singola o multisessione
- Il criterio Graphics status indicator (Indicatore di stato della grafica) deve essere abilitato.
- È possibile configurare solo le sessioni desktop.

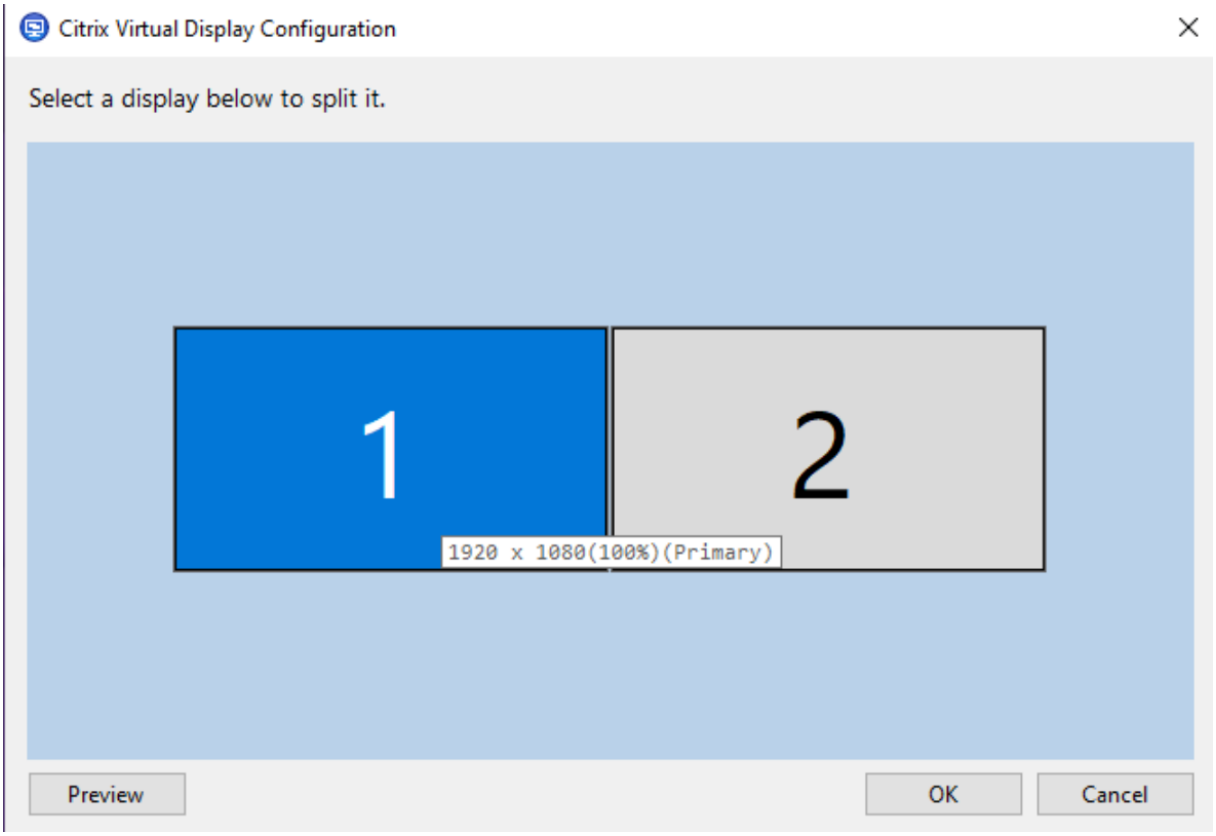
### Configurazione

Per configurare il layout dello schermo virtuale, fare clic con il pulsante destro del mouse sull'icona dell'indicatore di stato della grafica e selezionare l'opzione Configure virtual displays (Configura gli schermi virtuali). Viene avviata l'interfaccia utente di configurazione degli schermi virtuali.

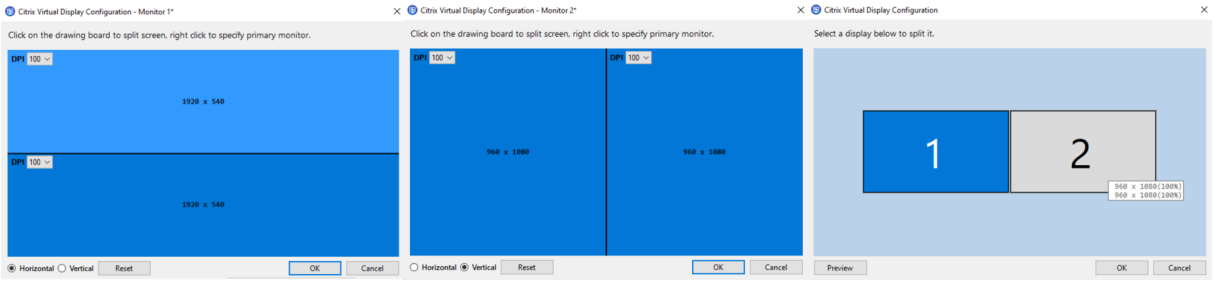


L'interfaccia utente mostra il layout degli schermi della sessione corrente; il colore blu indica il monitor principale della sessione. È possibile visualizzare la descrizione delle impostazioni dello schermo quando si passa il mouse su di esso. La descrizione fornisce informazioni sul layout dello schermo virtuale corrente definito su un dato monitor di sessione.

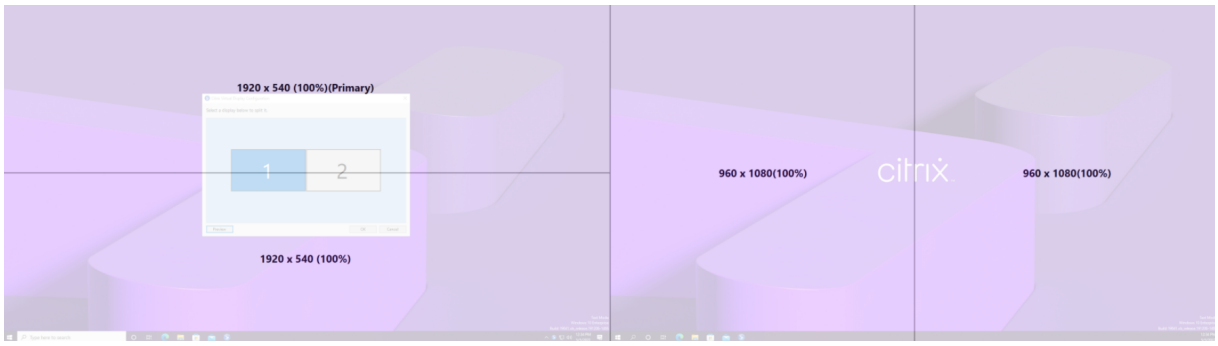



Selezionare uno schermo per passare a un'interfaccia utente interattiva, che consente di configurare schermi virtuali per il monitor di sessione selezionato. È possibile tracciare linee orizzontali o verticali per separare lo schermo in monitor virtuali. Lo schermo viene diviso in base alle percentuali specificate delle risoluzioni del monitor della sessione. Fare clic con il pulsante destro del mouse su uno schermo virtuale per contrassegnarlo come monitor principale e utilizzare l'elenco a discesa DPI per impostare un fattore di ridimensionamento preferito per lo schermo virtuale. Dopo aver definito un layout di visualizzazione virtuale, fare clic su **OK** per salvare temporaneamente il layout o su **Cancel** per annullare eventuali modifiche. È possibile utilizzare **Reset** per annullare la configurazione e ripristinare il layout originale del monitor di sessione.

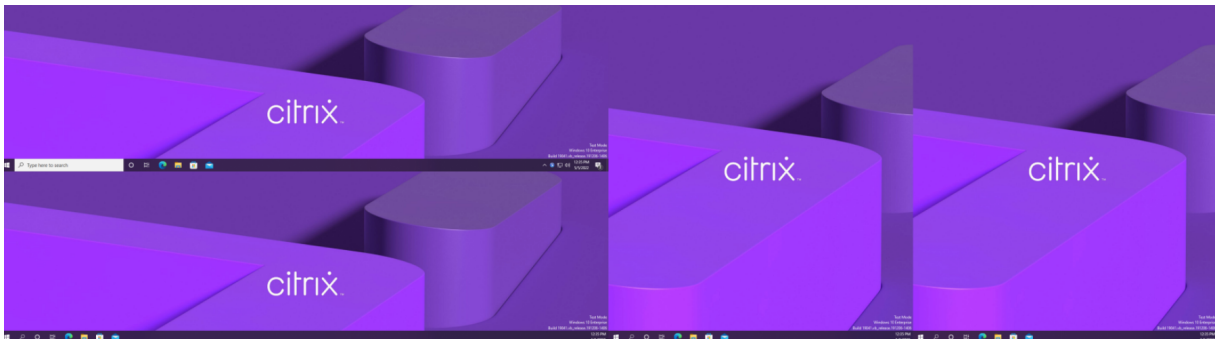


Per visualizzare in anteprima il layout di visualizzazione virtuale attualmente configurato, fare clic sul pulsante **Preview**. Viene visualizzata una finestra per evidenziare la posizione e la risoluzione previste dei display virtuali nella sessione.




Fare clic su **OK** per applicare e salvare immediatamente il layout dello schermo virtuale. Fare clic su **Cancel** per chiudere l'interfaccia utente e annullare tutte le modifiche.



### Altre considerazioni

- La risoluzione minima dello schermo virtuale richiesta è 640 x 480.
- Il DPI dello schermo virtuale definito tramite l'interfaccia utente dipende dal supporto del ridimensionamento del sistema operativo per la risoluzione dello schermo specificata.
- Non utilizzare questa funzione contemporaneamente alla funzione di visualizzazione virtuale esistente nell'app Citrix Workspace.
- La funzionalità di anteprima non è supportata su Server 2016.

## Contenuti multimediali

January 7, 2024

Lo stack tecnologico HDX supporta la distribuzione di applicazioni multimediali attraverso due approcci complementari:

- Distribuzioni multimediali di rendering lato server
- Reindirizzamento multimediale di rendering lato client

Questa strategia garantisce la possibilità di offrire una gamma completa di formati multimediali, con un'ottima esperienza utente, ottimizzando al contempo la scalabilità dei server per ridurre il costo per utente.

Con la distribuzione multimediale con rendering server, i contenuti audio e video vengono decodificati e renderizzati sul server Citrix Virtual Apps and Desktops dall'applicazione. Il contenuto viene quindi compresso e distribuito mediante il protocollo ICA all'app Citrix Workspace sul dispositivo dell'utente. Questo metodo fornisce il più alto tasso di compatibilità con varie applicazioni e formati multimediali. Poiché l'elaborazione video richiede un uso intensivo dell'elaborazione, la distribuzione multimediale con rendering del server beneficia notevolmente dell'accelerazione hardware integrata. Ad esempio, il supporto di DirectX Video Acceleration (DXVA) alleggerisce la CPU eseguendo la decodifica H.264 in hardware separato. Le tecnologie Intel Quick Sync, AMD RapidFire e NVIDIA NVENC forniscono codifica H.264 con accelerazione hardware.

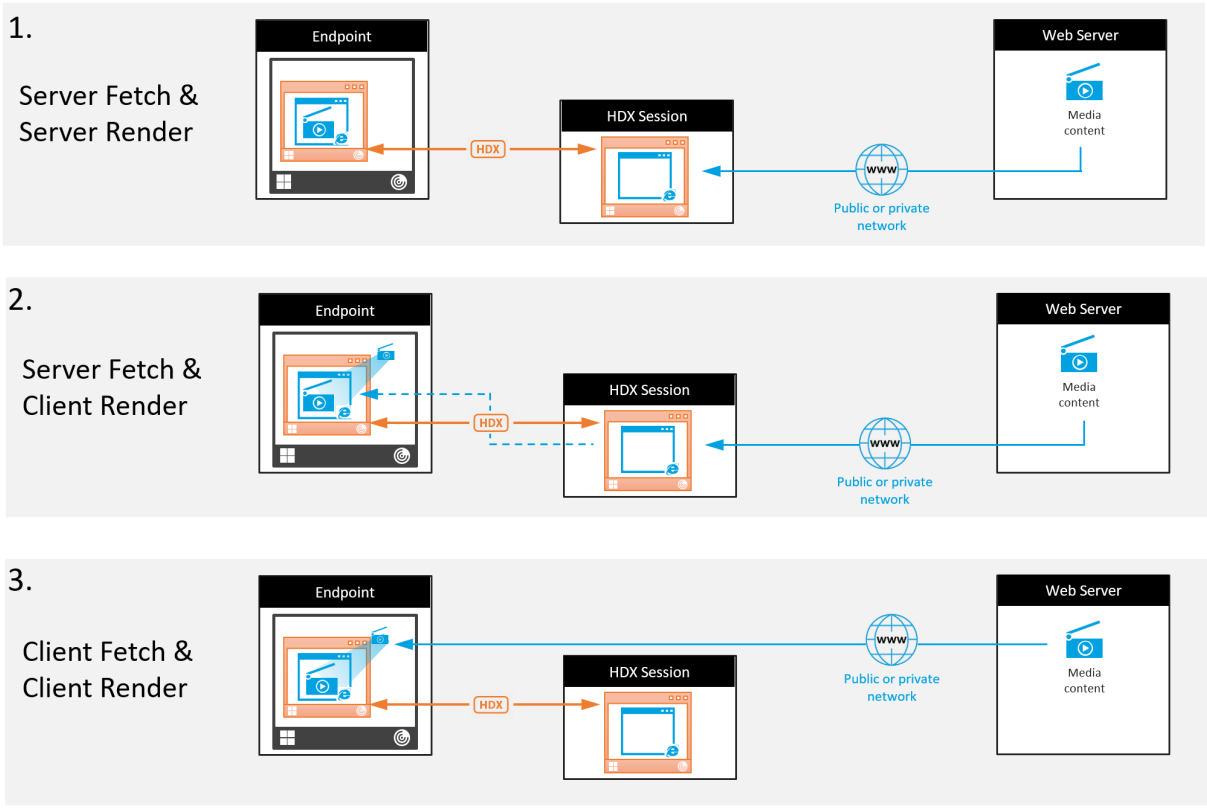
Poiché la maggior parte dei server non offre alcuna accelerazione hardware per la compressione video, la scalabilità del server viene influenzata negativamente se tutta l'elaborazione video viene eseguita sulla CPU del server. È possibile mantenere un'elevata scalabilità del server, reindirizzando molti formati multimediali al dispositivo utente per il rendering locale.

- Il reindirizzamento di Windows Media consente di alleggerire il server per un'ampia varietà di formati multimediali generalmente associati a Windows Media Player.
- Il video HTML5 è diventato di uso generale e Citrix ha introdotto una tecnologia di reindirizzamento per questo tipo di contenuti. Si consiglia il reindirizzamento dei contenuti del browser per siti Web che utilizzano HTML5, HLS, DASH o WebRTC.
- È possibile applicare le tecnologie generali di reindirizzamento dei contatti da host a client e l'accesso delle app locali ai contenuti multimediali.

Mettendo insieme queste tecnologie, se non si configura il reindirizzamento, HDX esegue il rendering lato server.
Se si configura il reindirizzamento, HDX utilizza Server Fetch e Client Render o Client Fetch e Client Render. Se tali metodi non riescono, HDX torna al rendering lato server in base alle esigenze ed è soggetto ai criteri di prevenzione del fallback.

## Esempi di scenari




**Scenario 1. (Server Fetch e Server Rendering):**

1. Il server recupera il file multimediale dalla sua origine, lo decodifica e quindi presenta il contenuto a una periferica audio o a un dispositivo di visualizzazione.
2. Il server estrae l'immagine o l'audio presentati rispettivamente dal dispositivo di visualizzazione o dalla periferica audio.
3. Il server lo comprime facoltativamente e quindi lo trasmette al client.

Questo approccio comporta un costo elevato in termini di CPU, un costo elevato di larghezza di banda (se l'immagine/audio estratto non è compresso in modo efficiente) e ha una bassa scalabilità del server.

I canali virtuali Thinwire e Audio gestiscono questo approccio. Il vantaggio di questo approccio è che riduce i requisiti hardware e software per i client. Utilizzando questo approccio la decodifica avviene sul server e funziona per una più ampia varietà di dispositivi e formati.

**Scenario 2. (Server Fetch e Client Render):**

Questo approccio si basa sulla possibilità di intercettare il contenuto multimediale prima che venga decodificato e presentato al dispositivo audio o di visualizzazione. Il contenuto audio/video compresso viene invece inviato al client dove viene quindi decodificato e presentato localmente. Il van-

taggio di questo approccio è che vengono scaricati sui dispositivi client, risparmiando cicli della CPU sul server.

Tuttavia, introduce anche alcuni requisiti hardware e software aggiuntivi per il client. Il client deve essere in grado di decodificare ciascun formato che potrebbe ricevere.

**Scenario 3. (Client Fetching e Client Rendering):**

Questo approccio si basa sulla possibilità di intercettare l'URL del contenuto multimediale prima che venga recuperato dall'origine. L'URL viene inviato al client in cui il contenuto multimediale viene recuperato, decodificato e presentato localmente. Questo approccio è concettualmente semplice. Il suo vantaggio è che risparmia sia cicli della CPU sul server che larghezza di banda, perché il server invia solo comandi di controllo. Tuttavia, il contenuto multimediale non è sempre accessibile ai client.

**Framework e piattaforma:**

I sistemi operativi a sessione singola (Windows, Mac OS X e Linux) forniscono framework multimediali che consentono lo sviluppo più rapido di applicazioni multimediali. Questa tabella elenca alcuni dei framework multimediali più popolari. Ogni framework divide l'elaborazione multimediale in più fasi e utilizza un'architettura basata su pipeline.

| Framework | Piattaforma |
|---|---|
| DirectShow | Windows (98 e versioni successive) |
| Media Foundation | Windows (Vista e versioni successive) |
| Gstreamer | Linux |
| Quicktime | Mac OS X |

### Supporto a doppio hop con tecnologie di reindirizzamento dei supporti

| | | |
|---|---|---|
| | Reindirizzamento audio | No |
| | Browser content redirection (Reindirizzamento del contenuto del browser) | No |
| | Reindirizzamento webcam HDX | Sì |
| | Reindirizzamento video HTML5 | Sì |
| | Reindirizzamento di Windows Media | Sì |

# Funzionalità audio

January 7, 2024

È possibile configurare e aggiungere le seguenti impostazioni dei criteri Citrix a un criterio che ottimizza le funzionalità audio HDX. Per i dettagli sull'utilizzo, nonché le relazioni e le dipendenze con altre impostazioni dei criteri, vedere Impostazioni dei criteri audio, Impostazioni dei criteri di larghezza di banda e Impostazioni dei criteri per le connessioni multi-flusso.

## Audio adattivo

Con l'audio adattivo, non è necessario configurare manualmente i criteri di qualità audio sul VDA. L'audio adattivo ottimizza le impostazioni per l'ambiente in uso e sostituisce i formati di compressione audio obsoleti per offrire un'esperienza utente eccellente.

L'audio adattivo è abilitato per impostazione predefinita. Per disabilitare l'audio adattivo, vedere Impostazioni dei criteri audio.

> **Importante:**
>
> Si consiglia di fornire l'audio utilizzando User Datagram Protocol (UDP) anziché TCP quando sono necessarie applicazioni audio in tempo reale. Solo Windows Virtual Delivery Agent (VDA) supporta l'audio su UDP.
>
> La crittografia audio UDP tramite DTLS è disponibile solo tra Citrix Gateway e l'app Citrix Workspace. Pertanto, a volte potrebbe essere preferibile utilizzare il trasporto TCP. TCP supporta la crittografia TLS end-to-end dal VDA all'app Citrix Workspace.
>
> Per ulteriori informazioni sull'audio adattivo e sull'audio UDP, vedere Trasporto in tempo reale dell'audio su UDP e intervallo delle porte UDP audio.

## Supporto dell'audio tramite protocollo EDT Lossy (anteprima)

Il protocollo EDT Lossy supporta l'audio. Questa funzionalità potenzia l'esperienza utente per lo streaming in tempo reale e migliora la qualità audio rispetto a EDT quando gli utenti si connettono tramite reti con elevata latenza e perdita di pacchetti.

### Anteprima pubblica

Questa funzionalità è disabilitata per impostazione predefinita nella versione 2308. Per partecipare all'anteprima pubblica, compilare il modulo Audio over EDT Lossy preview form (modulo di anteprima dell'Audio su EDT Lossy.

#### Requisiti di sistema

Assicurarsi di disporre dei seguenti prodotti nelle versioni minime che supportano EDT Lossy:

- Citrix Virtual Delivery Agent (VDA) 2308
- App Citrix Workspace per Windows 2309

Inoltre, devono essere abilitate le seguenti funzionalità:

- Criteri di HDX Adaptive Transport.
- (Facoltativo) Per le connessioni remote, è richiesto Citrix Gateway Service.

> **Nota:**
>
> Se le condizioni di cui sopra non sono soddisfatte, l'audio viene inviato tramite il trasporto EDT Reliable.

#### Informazioni aggiuntive

EDT Lossy è un protocollo di trasporto tollerante alle perdite che consente la perdita di pacchetti durante la trasmissione senza inviare nuovamente i contenuti multimediali, garantendo un'esperienza più in tempo reale per gli utenti.
Enlightened Data Transport (EDT) è un protocollo di trasporto proprietario di Citrix che offre un'esperienza utente superiore su connessioni impegnative a lungo raggio, mantenendo al contempo la scalabilità del server. La modalità tollerante alle perdite è una funzionalità del servizio Citrix Gateway che utilizza EDT Lossy come protocollo di trasporto per mantenere una connessione stabile anche in caso di congestione della rete. Ciò garantisce un'esperienza coerente e stabile per i lavoratori remoti. In condizioni normali, EDT ed EDT Lossy forniscono risultati simili. Tuttavia, in condizioni di rete con perdita di pacchetti, EDT Lossy offre un'esperienza audio migliore rispetto a EDT. In questo modo diventa una funzionalità essenziale per i lavoratori remoti che si affidano a contenuti multimediali in tempo reale per il proprio lavoro.

### Audio quality (Qualità audio)

In generale, una qualità audio più elevata consuma più larghezza di banda e prevede un maggiore utilizzo della CPU del server, inviando più dati audio ai dispositivi utente. La compressione audio consente di bilanciare la qualità del suono rispetto alle prestazioni generali della sessione. Utilizzare le impostazioni dei criteri Citrix per configurare i livelli di compressione da applicare ai file audio.

Per impostazione predefinita, l'opzione **Audio quality policy (Criteri di qualità audio)** è impostata su High - high definition audio (Elevata - Audio ad alta definizione) quando si utilizza il trasporto TCP. Il criterio è impostato su Medium - optimized-for-speech (Medio - ottimizzato per il riconoscimento vocale) quando viene utilizzato il trasporto UDP (opzione consigliata). L'impostazione **High Definition**

**audio (Audio ad alta definizione)** fornisce audio stereo ad alta fedeltà, ma consuma più larghezza di banda rispetto ad altre impostazioni di qualità. Non utilizzare questa qualità audio per applicazioni di chat vocale o chat video non ottimizzate (come i softphone). Il motivo è che potrebbe introdurre nel percorso audio una latenza che non è adatta per le comunicazioni in tempo reale. Si consiglia di impostare il criterio su Optimized for speech (Ottimizzato per il parlato) per l'audio in tempo reale, indipendentemente dal protocollo di trasporto selezionato.

Quando la larghezza di banda è limitata, ad esempio nelle connessioni via satellite o dial-up, la riduzione della qualità audio a **Low (Bassa)** consuma la minore larghezza di banda possibile. In questo caso, creare criteri separati per gli utenti con connessioni a larghezza di banda ridotta in modo che non vi siano ripercussioni negative per gli utenti con connessioni a larghezza di banda elevata.

Per i dettagli sulle impostazioni, vedere Impostazioni dei criteri audio. Ricordarsi di abilitare le impostazioni audio del client sul dispositivo utente.

Linee guida sulla larghezza di banda per la riproduzione e la registrazione audio:

- Audio adattivo (impostazione predefinita)
  - Bitrate: adattivo variabile
  - Numero di canali: 2 (stereo) per la riproduzione, 1 (mono) per l'acquisizione dal microfono
  - Frequenza: 48000 Hz
  - Profondità di bit: 16 bit
- High quality (Alta qualità)
  - Velocità in bit: ~100 kbps (min 75, max 175 kbps) per la riproduzione/~70 kbps per l'acquisizione del microfono
  - Numero di canali: 2 (stereo) per la riproduzione, 1 (mono) per l'acquisizione del microfono
  - Frequenza: 44100 Hz
  - Profondità di bit: 16 bit
- Qualità media (consigliata per VoIP)
  - Velocità in bit: ~16 kbps (min 20, max 40 kbps) per la riproduzione, ~16 kbps per l'acquisizione del microfono
  - Numero di canali: 1 (mono) sia per la riproduzione che per l'acquisizione
  - Frequenza: 16.000 Hz (banda larga)
  - Profondità di bit: 16 bit
- Bassa qualità
  - Velocità in bit: ~11 kbps (min 10; max 25 kbps) per la riproduzione, ~11 kbps per l'acquisizione del microfono
  - Numero di canali: 1 (mono) sia per la riproduzione che per l'acquisizione
  - Frequenza: 8000 Hz (banda stretta)
  - Profondità di bit: 16 bit

### Client audio redirection (Reindirizzamento audio client)

Per consentire agli utenti di ricevere audio da un'applicazione su un server tramite altoparlanti o altri dispositivi audio sul dispositivo utente, lasciare l'impostazione **Client audio redirection (Reindirizzamento audio client)** su **Allowed (Consentito)**. Questa è l'impostazione predefinita.

La mappatura audio client comporta un carico extra sui server e sulla rete. Tuttavia, il divieto di reindirizzamento audio client disabilita tutte le funzionalità audio HDX.

Per i dettagli sulle impostazioni, vedere Impostazioni dei criteri audio. Ricordarsi di abilitare le impostazioni audio client sul dispositivo utente.

### Client microphone redirection (Reindirizzamento microfono client)

Per consentire agli utenti di registrare audio utilizzando dispositivi di input come i microfoni sul dispositivo utente, lasciare l'impostazione **Client microphone redirection (Reindirizzamento microfono client)** sul valore predefinito Allowed (Consentito).

Per motivi di sicurezza, i dispositivi utente avvisano gli utenti quando server non considerati attendibili tentano di accedere ai microfoni. Gli utenti possono scegliere di accettare o rifiutare l'accesso prima di utilizzare il microfono. Gli utenti possono disabilitare questo avviso sull'app Citrix Workspace.

Per i dettagli sulle impostazioni, vedere Impostazioni dei criteri audio. Ricordarsi di abilitare le impostazioni audio del client sul dispositivo utente.

### Audio Plug N Play

L'impostazione dei criteri Audio Plug N Play consente o impedisce l'utilizzo di più dispositivi audio per registrare e riprodurre suoni. Questa impostazione è **abilitata** per impostazione predefinita. Audio Plug N Play consente di riconoscere i dispositivi audio. I dispositivi vengono riconosciuti anche se non sono collegati solo dopo l'avvio della sessione utente.

Questa impostazione si applica solo alle macchine con sistema operativo Windows multisessione.

Per i dettagli sulle impostazioni, vedere Impostazioni dei criteri audio.

### Limite di larghezza di banda di reindirizzamento audio e percentuale limite di larghezza di banda di reindirizzamento audio

L'impostazione del criterio relativo al limite della larghezza di banda di reindirizzamento audio specifica la larghezza di banda massima (in kilobit al secondo) per la riproduzione e la registrazione di audio in una sessione.

L'impostazione Audio redirection bandwidth limit percent (Percentuale limite della larghezza di banda di reindirizzamento audio) specifica la larghezza di banda massima per il reindirizzamento audio come percentuale della larghezza di banda totale disponibile.

Per impostazione predefinita, per entrambe le impostazioni viene specificato zero (nessun massimo). Se entrambe le impostazioni sono configurate, viene utilizzata quella con il limite di larghezza di banda più basso.

Per i dettagli sulle impostazioni, vedere Impostazioni dei criteri di larghezza di banda. Ricordarsi di abilitare le impostazioni audio del client sul dispositivo utente.

### Trasporto in tempo reale dell'audio su UDP e intervallo delle porte UDP audio

Per impostazione predefinita, è consentito il trasporto in tempo reale dell'audio su UDP (User Datagram Protocol), se selezionato al momento dell'installazione. Si apre una porta UDP sul server per le connessioni che utilizzano il trasporto in tempo reale dell'audio su UDP. In caso di congestione della rete o perdita di pacchetti, si consiglia di configurare UDP/RTP per l'audio per garantire la migliore esperienza utente possibile. Per l'audio in tempo reale come applicazioni softphone, l'audio UDP è preferibile a EDT. UDP consente la perdita di pacchetti senza ritrasmissione, garantendo che non venga aggiunta alcuna latenza nelle connessioni con perdita di pacchetti elevata.

> **Importante:**
>
> Quando Citrix Gateway non è nel percorso, i dati audio trasmessi con UDP non vengono crittografati. Se Citrix Gateway è configurato per accedere alle risorse di Citrix Virtual Apps and Desktops, il traffico audio tra il dispositivo endpoint e Citrix Gateway è protetto utilizzando il protocollo DTLS.

L'intervallo di porte UDP audio specifica l'intervallo di numeri di porta utilizzato dal VDA di Windows per scambiare i dati dei pacchetti audio con il dispositivo utente.

Per impostazione predefinita, l'intervallo è compreso tra 16500 e 16509.

> **Nota:**
>
> Se il trasporto in tempo reale dell'audio su UDP non è richiesto per l'audio adattivo, Citrix consiglia di configurare l'impostazione dei criteri su Disabled. Ciò consente di evitare che i client dell'app Citrix Workspace richiedano connessioni UDP aperte o attivino finestre di dialogo di configurazione del firewall client dell'app Citrix Workspace indesiderate.

Per informazioni sulle impostazioni relative ad Audio over UDP real-time transport (Audio con trasporto UDP in tempo reale), vedere Impostazioni dei criteri audio. Per informazioni dettagliate sull'intervallo di porte UDP audio, vedere Impostazioni dei criteri di connessione multi-stream. Ricordarsi di abilitare le impostazioni audio del client sul dispositivo utente.

L'audio su UDP richiede il VDA di Windows. Per i criteri supportati su Linux VDA, vedere Elenco di supporto dei criteri.

### Criteri di impostazione audio per i dispositivi utente

1. Caricare i modelli di criteri di gruppo seguendo Configurazione del modello amministrativo Oggetto Criteri di gruppo.
2. Nell'Editor Criteri di gruppo espandere **Modelli amministrativi > Citrix Components (Componenti Citrix) > Citrix Workspace > Citrix Components (Esperienza utente)**.
3. Per **Client audio settings (Impostazioni audio client)**, selezionare **Not Configured** (Non configurate), **Enabled (Abilitate)**o **Disabled (Disabilitate)**.
    - **Not Configured (Non configurate)**. Per impostazione predefinita, il reindirizzamento audio è abilitato utilizzando l'audio di alta qualità o le impostazioni audio personalizzate precedentemente configurate.
    - **Enabled**. Abilita il reindirizzamento audio utilizzando le opzioni selezionate.
    - **Disabled**. Disabilita il reindirizzamento audio.
4. Se si seleziona **Enabled (Abilitate)**, scegliere una qualità audio. Per l'audio UDP, utilizzare **Medium (Medio)** (impostazione predefinita).
5. Solo per l'audio UDP, selezionare **Enable Real-Time Transport (Abilita trasporto in tempo reale)**, quindi impostare l'intervallo di porte in ingresso da aprire nel firewall locale di Windows.
6. Per utilizzare l'audio UDP con Citrix Gateway, selezionare **Allow Real-Time Transport Through gateway (Consenti trasporto in tempo reale tramite gateway)**. Configurare Citrix Gateway con DTLS. Per ulteriori informazioni, vedere questo articolo.

In qualità di amministratore, se non si dispone del controllo sui dispositivi endpoint per apportare queste modifiche, utilizzare gli attributi default.ica di StoreFront per abilitare l'audio UDP. Ad esempio, per i dispositivi BYOD o i computer di casa.

1. Sul computer StoreFront, aprire C:\inetpub\wwwroot\Citrix\ <Store Name>\App_Data\default.ica con un editor come Blocco note.
2. Inserire le voci seguenti nella sezione [Application] (Applicazione).

    ; This text enables Real-Time Transport

    EnableRtpAudio=true

    ; This text allows Real-Time Transport Through gateway

    EnableUDPThroughGateway=true

    ; This text sets audio quality to Medium

    AudioBandwidthLimit=1

; UDP Port range

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509

Se si abilita l'audio UDP (User Datagram Protocol) modificando default.ica, l'audio UDP è abilitato per tutti gli utenti che utilizzano tale archivio.

### Evitare l'eco durante le conferenze multimediali

Gli utenti delle conferenze audio o video potrebbero sentire un'eco. Gli echi di solito si verificano quando altoparlanti e microfoni sono troppo vicini l'uno all'altro. Per questo motivo, si consiglia l'uso di cuffie per le conferenze audio e video.

HDX fornisce un'opzione di cancellazione dell'eco (attivata per impostazione predefinita) che riduce al minimo qualsiasi eco. L'efficacia della cancellazione dell'eco è sensibile alla distanza tra gli altoparlanti e il microfono. Assicurarsi che i dispositivi non siano troppo vicini o troppo lontani l'uno dall'altro.

È possibile modificare un'impostazione del Registro di sistema per disabilitare l'annullamento dell'eco. Per informazioni, vedere Evitare l'eco durante le conferenze multimediali nell'elenco delle funzionalità gestite tramite il Registro di sistema.

### Softphone

Un softphone è un software che funge da interfaccia telefonica. È possibile utilizzare un softphone per effettuare chiamate via Internet da un computer o un altro dispositivo smart. Utilizzando un softphone, è possibile comporre numeri di telefono ed eseguire altre funzioni correlate al telefono utilizzando uno schermo.

Citrix Virtual Apps and Desktops supporta diverse alternative per la distribuzione di softphone.

- **Modalità di controllo**. Il softphone ospitato controlla un telefono fisico. In questa modalità, nessun traffico audio passa attraverso il server di Citrix Virtual Apps and Desktops.
- **Supporto dei softphone ottimizzati HDX RealTime (consigliato)**. Il motore multimediale viene eseguito sul dispositivo utente e il traffico VoIP scorre peer-to-peer. Per esempi, vedere:
  - Ottimizzazione di HDX per Microsoft Teams
  - HDX RealTime Optimization Pack, che ottimizza la distribuzione di Microsoft Skype for Business
  - Cisco Jabber Softphone per VDI (precedentemente noto come VXME)
  - Cisco Webex Meetings per VDI

  - Avaya VDI Equinox (già noto come VDI Communicator)
  - Plugin Zoom VDI
  - Genesys PureEngage Cloud
  - Dispositivo di dettatura Nuance Dragon PowerMic

- **Accesso alle app locali**. Una funzionalità di Citrix Virtual Apps and Desktops che consente a un'applicazione come un softphone di venire eseguita localmente sul dispositivo utente Windows, pur apparendo perfettamente integrata con il relativo desktop virtuale/pubblicato. Questa funzionalità consente l'offload di tutte le elaborazioni audio sul dispositivo dell'utente. Per ulteriori informazioni, vedere Accesso alle app locali e reindirizzamento URL.
- **Supporto per softphone generico HDX RealTime.** Voice over Internet Protocol-over-ICA.

***Supporto dei softphone generici***

Il supporto dei softphone generici consente di ospitare un softphone non modificato su XenApp o XenDesktop nel centro dati. Il traffico audio passa attraverso il protocollo Citrix ICA (preferibilmente utilizzando UDP/RTP) e raggiunge il dispositivo utente che esegue l'app Citrix Workspace.

Il supporto generico di softphone è una funzionalità di HDX RealTime. Questo approccio alla distribuzione di softphone è particolarmente utile quando:

- Non è disponibile una soluzione ottimizzata per la distribuzione del softphone e l'utente non utilizza un dispositivo Windows in cui è possibile utilizzare l'accesso alle app locali.
- Il motore multimediale necessario per la distribuzione ottimizzata del softphone non è installato sul dispositivo utente o non è disponibile per la versione del sistema operativo in esecuzione sul dispositivo utente. In questo scenario, Generic HDX RealTime fornisce una valida soluzione di fallback.

Vi sono due considerazioni da fare sulla distribuzione di softphone utilizzando Citrix Virtual Apps and Desktops:

- Come l'applicazione softphone viene distribuita al desktop virtuale/pubblicato.
- Come viene inviato l'audio da e verso le cuffie, il microfono e gli altoparlanti dell'utente o il telefono USB.

Citrix Virtual Apps and Desktops include numerose tecnologie per supportare la distribuzione generica di softphone:

- Codec ottimizzato per il parlato per la codifica rapida dell'audio in tempo reale e l'efficienza della larghezza di banda.
- Stack audio a bassa latenza.
- Buffer del jitter lato server per migliorare l'audio quando la latenza di rete è variabile.
- Tagging dei pacchetti (DSCP e WMM) per la qualità del servizio.
  - Tagging DSCP per pacchetti RTP (Livello 3)

- Tagging WMM per Wi-Fi

Anche le versioni dell'app Citrix Workspace per Windows, Linux, Chrome e Mac possono utilizzare VoIP. L'app Citrix Workspace per Windows offre le seguenti funzionalità:

- Buffer del jitter lato client: assicura un audio fluido anche quando la latenza di rete è variabile.
- Cancellazione dell'eco: consente una maggiore variazione della distanza tra il microfono e gli altoparlanti per i lavoratori che non utilizzano cuffie.
- Audio plug-n-play: non è necessario che i dispositivi audio siano collegati prima di iniziare una sessione. Possono essere collegati in qualsiasi momento.
- Routing dei dispositivi audio: gli utenti possono indirizzare la suoneria agli altoparlanti, ma il percorso vocale verso le cuffie.
- ICA multi-stream: consente un routing flessibile basato sulla qualità del servizio sulla rete.
- ICA supporta quattro flussi TCP e due flussi UDP. Uno dei flussi UDP supporta l'audio in tempo reale su RTP.

Per un riepilogo delle funzionalità dell'app Citrix Workspace, vedere Matrice delle funzionalità di Citrix Receiver.

***Consigli per la configurazione del sistema***

*Hardware e software client*:
per una qualità audio ottimale, si consiglia l'ultima versione dell'app Citrix Workspace e una cuffia di buona qualità con cancellazione dell'eco acustico (AEC). Le versioni dell'app Citrix Workspace per Windows, Linux e Mac supportano VoIP. Inoltre, Dell Wyse offre il supporto VoIP per ThinOS (WTOS).

*Considerazioni sulla CPU*:
monitorare l'utilizzo della CPU sul VDA per determinare se è necessario assegnare due CPU virtuali a ciascuna macchina virtuale. Voce e video in tempo reale richiedono un uso intensivo di dati. La configurazione di due CPU virtuali riduce la latenza di commutazione dei thread. Pertanto, si consiglia di configurare due vCPU in un ambiente VDI Citrix Virtual Desktops.

Avere due CPU virtuali non significa necessariamente raddoppiare il numero di CPU fisiche, perché le CPU fisiche possono essere condivise tra le sessioni.

Anche Citrix Gateway Protocol (CGP), utilizzato per la funzionalità di affidabilità delle sessioni, aumenta il consumo della CPU. Nelle connessioni di rete di alta qualità, è possibile disabilitare questa funzionalità per ridurre il consumo di CPU sul VDA. Nessuno dei passaggi precedenti potrebbe essere necessario su un server potente.

*Audio UDP*:
l'audio su UDP fornisce un'eccellente tolleranza alla congestione della rete e alla perdita di pacchetti. Si consiglia di utilizzarlo al posto di TCP quando è disponibile.

*Configurazione LAN/WAN*:
una corretta configurazione della rete è fondamentale per una buona qualità dell'audio in tempo

reale. In genere, è necessario configurare reti LAN virtuali (VLAN) perché i pacchetti broadcast eccessivi possono introdurre instabilità. I dispositivi abilitati per IPv6 potrebbero generare molti pacchetti broadcast. Se il supporto IPv6 non è necessario, è possibile disabilitare IPv6 su tali dispositivi. Eseguire questa configurazione per supportare la qualità del servizio.

*Impostazioni per l'uso delle connessioni WAN*:
è possibile utilizzare la chat vocale sulle connessioni LAN e WAN. In una connessione WAN, la qualità audio dipende dalla latenza, dalla perdita di pacchetti e dall'instabilità sulla connessione. Se si distribuiscono softphone agli utenti con una connessione WAN, si consiglia di utilizzare NetScaler SD-WAN tra il centro dati e l'ufficio remoto. In tal modo si mantiene un'alta qualità del servizio. NetScaler SD-WAN supporta ICA multi-flusso, tra cui UDP. Inoltre, per un singolo flusso TCP è possibile distinguere le priorità dei vari canali virtuali ICA per garantire che i dati audio in tempo reale ad alta priorità ricevano un trattamento preferenziale.

Utilizzare Director o HDX Monitor per convalidare la configurazione HDX.

*Connessioni utente remote*:
Citrix Gateway supporta DTLS per fornire traffico UDP/RTP in modo nativo (senza incapsulamento in TCP).
Aprire i firewall in modo bidirezionale per il traffico UDP sulla porta 443.

*Selezione del codec e consumo di larghezza di banda*:
tra il dispositivo utente e il VDA nel centro dati, si consiglia di utilizzare l'impostazione del codec **Optimized-for-Speech (Ottimizzato per il parlato)**, nota anche come audio di qualità media. Tra la piattaforma VDA e l'IP-PBX, il softphone utilizza qualsiasi codec configurato o negoziato. Ad esempio:

- G711 offre una buona qualità della voce, ma ha un requisito di larghezza di banda che va da 80 kilobit al secondo fino a 100 kilobit al secondo per chiamata (a seconda dei sovraccarichi di Network Layer2).
- G729 offre una buona qualità della voce e ha un requisito di larghezza di banda ridotta che va da 30 kilobit al secondo fino a 40 kilobit al secondo per chiamata (a seconda dei sovraccarichi Network Layer 2).

***Distribuire applicazioni softphone al desktop virtuale***

Esistono due metodi con cui è possibile distribuire un softphone al desktop virtuale XenDesktop:

- L'applicazione può essere installata nell'immagine desktop virtuale.
- L'applicazione può essere trasmessa in streaming sul desktop virtuale utilizzando Microsoft App-V. Questo approccio presenta vantaggi di gestibilità perché l'immagine del desktop virtuale viene mantenuta pulita. Dopo essere stata trasmessa al desktop virtuale, l'applicazione viene eseguita in tale ambiente come se fosse installata nel modo consueto. Non tutte le applicazioni sono compatibili con App-V.

#### *Distribuire audio da e verso il dispositivo utente*

HDX RealTime generico supporta due metodi di trasmissione audio da e verso il dispositivo utente:

- **Canale virtuale audio Citrix**. Generalmente consigliamo il canale virtuale audio Citrix perché è progettato specificamente per il trasporto audio.
- **Reindirizzamento USB generico**. Supporta dispositivi audio con pulsanti o display (o entrambi), HID (Human Interface Device), se il dispositivo utente è su una connessione LAN o è disponibile una connessione simile a LAN verso il server di Citrix Virtual Apps and Desktops.

#### *Canale virtuale audio Citrix*

Il canale virtuale audio Citrix bidirezionale (CTXCAM) consente di trasmettere l'audio in modo efficiente sulla rete. HDX RealTime generico acquisisce l'audio dalla cuffia o dal microfono dell'utente e lo comprime. Quindi, lo invia tramite ICA all'applicazione softphone sul desktop virtuale. Allo stesso modo, l'uscita audio del softphone viene compressa e inviata nella direzione opposta alla cuffia o agli altoparlanti dell'utente. Questa compressione è indipendente dalla compressione utilizzata dal softphone stesso (come G.729 o G.711). Viene eseguita utilizzando il codec Optimized-for-Speech (Ottimizzato per il parlato, qualità media). Le sue caratteristiche sono ideali per VoIP. Offre un tempo di codifica rapido e consuma solo circa 56 kilobit al secondo di larghezza di banda della rete (28 Kbps in ogni direzione) nei momenti di picco. Questo codec deve essere selezionato esplicitamente nella console di Studio perché non è il codec audio predefinito. Il codec predefinito è HD Audio (Audio HD, alta qualità). Questo codec è eccellente per colonne sonore stereo ad alta fedeltà, ma è più lento da codificare rispetto al codec ottimizzato per il parlato.

#### *Reindirizzamento USB generico*

La tecnologia di reindirizzamento USB generico Citrix (canale virtuale CTXGUSB) fornisce un mezzo generico per la gestione remota di dispositivi USB, inclusi dispositivi compositi (audio più HID) e dispositivi USB isocroni. Questo approccio è limitato agli utenti connessi tramite LAN. Questo perché il protocollo USB tende a essere sensibile alla latenza di rete e richiede una notevole larghezza di banda di rete. Il reindirizzamento USB isocrono funziona bene quando si utilizzano alcuni softphone. Questo reindirizzamento offre un'eccellente qualità della voce e bassa latenza. Tuttavia, il canale virtuale Citrix Audio è preferibile perché è ottimizzato per il traffico audio. L'eccezione principale è il caso in cui si utilizza un dispositivo audio con pulsanti. Ad esempio, un telefono USB collegato al dispositivo utente che è collegato al centro dati tramite LAN. In questo caso, il reindirizzamento USB generico supporta i pulsanti del telefono o della cuffia che controllano le funzionalità inviando un segnale al softphone. Non si verifica alcun problema con i pulsanti che funzionano localmente sul dispositivo.

### Strumento della riga di comando per la diagnostica audio

Lo strumento della riga di comando di diagnostica audio sul VDA può essere utilizzato per interrogare i dati della sessione relativi alle politiche audio, alla configurazione e al trasporto dei dati.

#### Utilizzo

Aprire un prompt dei comandi ed eseguire `CtxAudioCmdTool.exe` dalla cartella `C:\Program Files\Citrix\HDX\bin`.

- Eseguendo lo strumento come amministratore è possibile visualizzare tutte le informazioni audio delle sessioni ICA attive.
- Eseguendo lo strumento come utente non amministratore è possibile visualizzare le informazioni audio della sessione ICA dell'utente corrente.

#### Output

Lo strumento offre varie impostazioni di configurazione che possono aiutare a diagnosticare problemi relativi all'audio all'interno di una sessione.

| Sezione | Descrizione |
|---|---|
| Informazioni sui criteri | Criteri audio applicate alle sessioni correnti. |
| Informazioni sulle impostazioni | Impostazioni di configurazione relative all'audio memorizzate nel registro. |
| Informazioni sullo stato | Stato, versione, codec e trasporto dell'audio applicati alle sessioni correnti. |
| Informazioni sui dispositivi | Nomi dei dispositivi, relativi ruoli e stati utilizzati nella sessione. |

> **Nota:**
>
> L'output varia a seconda che lo strumento venga eseguito su un VDA multisessione (TS) o su un VDA a sessione singola (WSVDA).

### Limitazione

Installare un dispositivo audio sul client, abilitare il reindirizzamento audio e avviare una sessione RDS. I file audio potrebbero non venire riprodotti e viene visualizzato un messaggio di errore.

Come soluzione alternativa, aggiungere la chiave del Registro di sistema sul computer RDS e quindi riavviare la macchina. Per informazioni, vedere Audio limitation (Limitazione audio) nell'elenco delle funzionalità gestite tramite il Registro di sistema.

# Browser content redirection (Reindirizzamento del contenuto del browser)

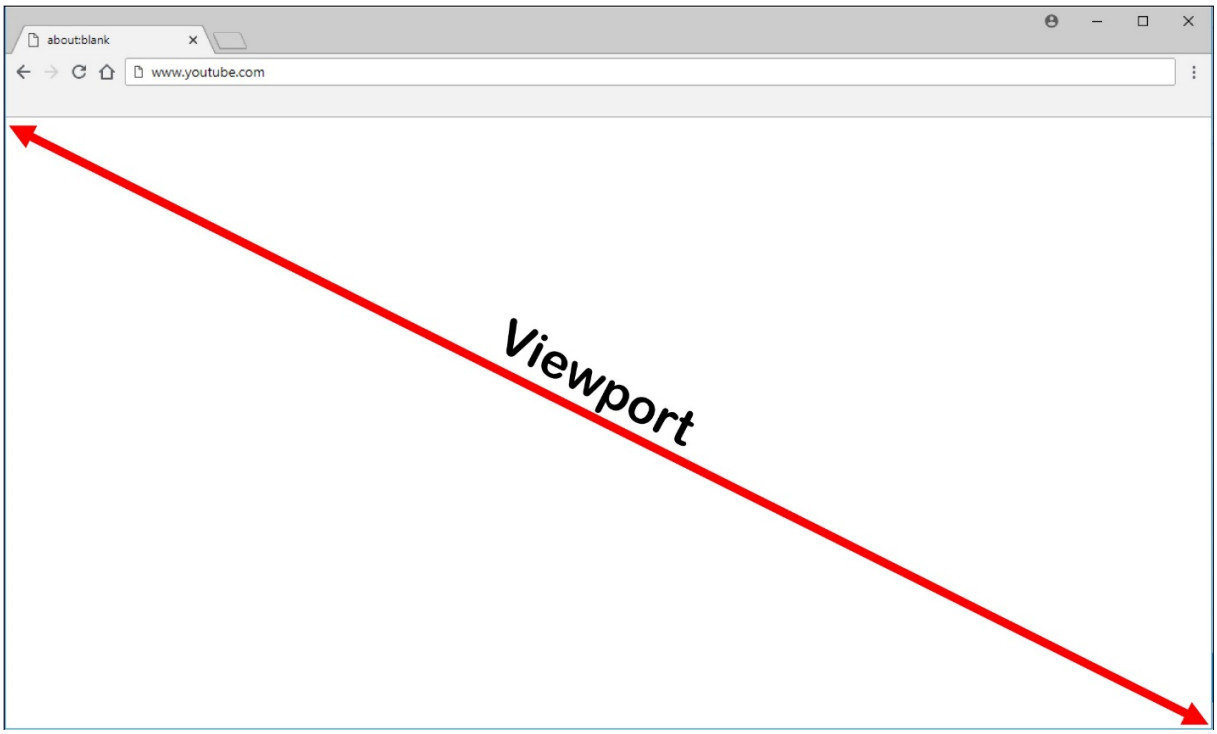
January 7, 2024

Il reindirizzamento del contenuto del browser impedisce il rendering delle pagine Web nell'elenco di elementi consentiti sul lato VDA. Questa funzionalità utilizza l'app Citrix Workspace per Windows o per Linux per creare un'istanza di un motore di rendering corrispondente sul lato client, che recupera i contenuti HTTP e HTTPS dall'URL.

> **Nota:**
>
> È possibile specificare che le pagine Web vengano reindirizzate al lato VDA (e non sul lato client) utilizzando un elenco di blocco.

Questo motore di layout Web di sovrapposizione viene eseguito sul dispositivo endpoint anziché sul VDA e utilizza la CPU, la GPU, la RAM e la rete dell'endpoint.

Viene reindirizzato solo il riquadro di visualizzazione del browser. Il riquadro di visualizzazione è l'area rettangolare del browser in cui viene visualizzato il contenuto. Il riquadro di visualizzazione non include elementi quali barra degli indirizzi, barra dei **Preferiti** e barra di stato. Tali elementi sono nell'interfaccia utente e sono ancora in esecuzione sul browser nel VDA.




1. Configurare un criterio di Studio che specifica un elenco di controllo di accesso contenente gli URL nell'elenco degli elementi consentiti per il reindirizzamento o l'elenco di blocco che dis-

abilita il reindirizzamento per percorsi URL specifici. Perché il browser sul VDA rilevi che l'URL che l'utente sta per aprire corrisponde all'elenco di elementi consentiti o non corrisponde a un elenco di blocco, un'estensione del browser esegue il confronto. L'estensione del browser per Internet Explorer 11 è inclusa nel supporto di installazione e viene installata automaticamente. Per Chrome, l'estensione del browser è disponibile nel Chrome Web Store ed è possibile distribuirla utilizzando i Criteri di gruppo e i file ADMX. Le estensioni di Chrome vengono installate per ciascun utente. Non è necessario aggiornare un'immagine golden per aggiungere o rimuovere un'estensione.

2. Se viene trovata una corrispondenza nell'elenco degli elementi consentiti (ad esempio `https://www.mycompany.com/`) e non esiste alcuna corrispondenza con un URL nell'elenco di blocco (ad esempio `https://www.mycompany.com/engineering`), un canale virtuale (CTXCSB) indica all'app Citrix Workspace che è necessario un reindirizzamento e inoltra l'URL. L'app Citrix Workspace crea un'istanza di un motore di rendering locale e visualizza il sito Web.
3. L'app Citrix Workspace riporta quindi senza problemi il sito Web nell'area del contenuto del browser del desktop virtuale.

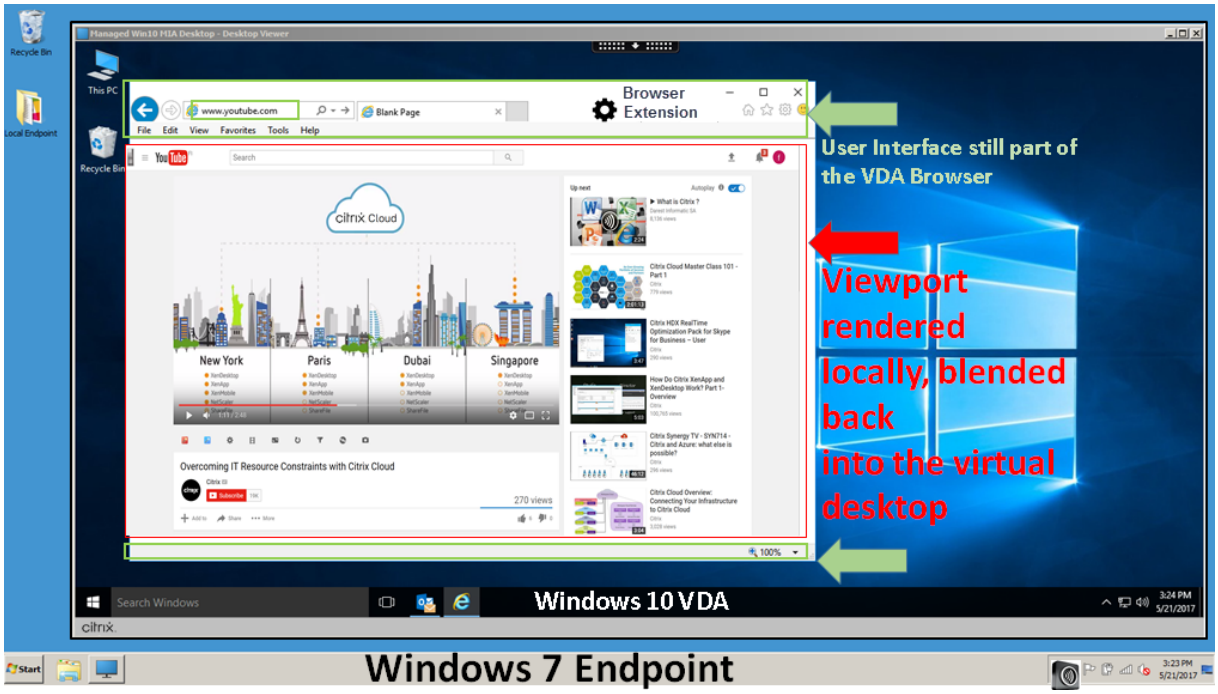
> **Nota:**
>
> Per ulteriori informazioni sulle novità e sulle soluzioni dei problemi dell'estensione di reindirizzamento del contenuto del browser, visitare il Chrome Web Store e cercare «citrix bcr» per trovare l'estensione.

Il colore del logo specifica lo stato dell'estensione Chrome. Si tratta di uno di questi tre colori:

- Verde: attivo e connesso.
- Grigio: non attivo/inattivo nella scheda corrente.
- Rosso: non funzionante.

È possibile eseguire il debug dei log utilizzando **Opzioni** nel menu delle estensioni.




Di seguito sono riportati gli scenari dei modi in cui l'app Citrix Workspace recupera il contenuto:

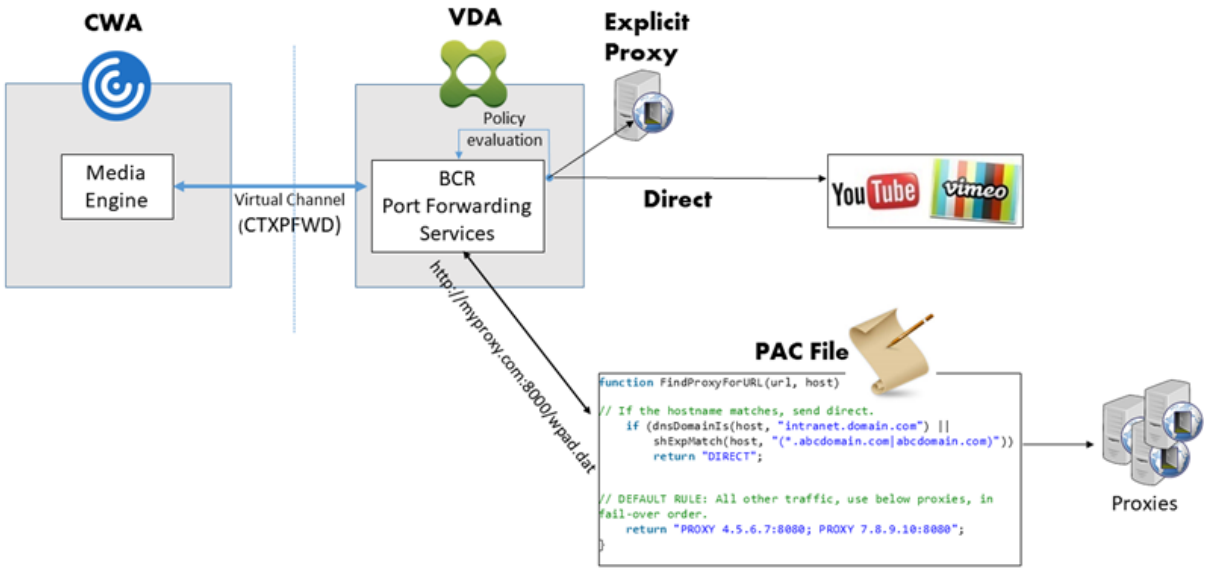
- **Recupero dal server e rendering sul server**: non vi è alcun reindirizzamento perché il sito non è stato aggiunto all'elenco degli elementi consentiti o il reindirizzamento non è riuscito. Si ritorna al rendering della pagina Web sul VDA e si utilizza Thinwire per la gestione remota della grafica. Utilizzare i criteri per controllare il comportamento di fallback. Elevato consumo di CPU, RAM e larghezza di banda sul VDA.
- **Recupero dal server e rendering sul client**: l'app Citrix Workspace contatta e recupera i contenuti dal server Web tramite il VDA utilizzando un canale virtuale (CTXPFWD). Questa opzione è utile quando il client non dispone di accesso a Internet (ad esempio, thin client). Basso consumo di CPU e RAM sul VDA, ma la larghezza di banda viene consumata sul canale virtuale ICA.

  Esistono tre modalità di funzionamento per questo scenario. Il termine proxy si riferisce a un dispositivo proxy a cui il VDA accede per ottenere l'accesso a Internet.

  Quale opzione dei criteri scegliere:

  - Explicit Proxy (Proxy esplicito): se si dispone di un singolo proxy esplicito nel centro dati.
  - Direct (Diretto) o Transparent (Trasparente) : se non si dispone di proxy o se si utilizzano proxy trasparenti.
  - PAC files (File PAC): se si fa affidamento su file PAC in modo che i browser nel VDA possano scegliere automaticamente il server proxy appropriato per il recupero di un URL specificato.

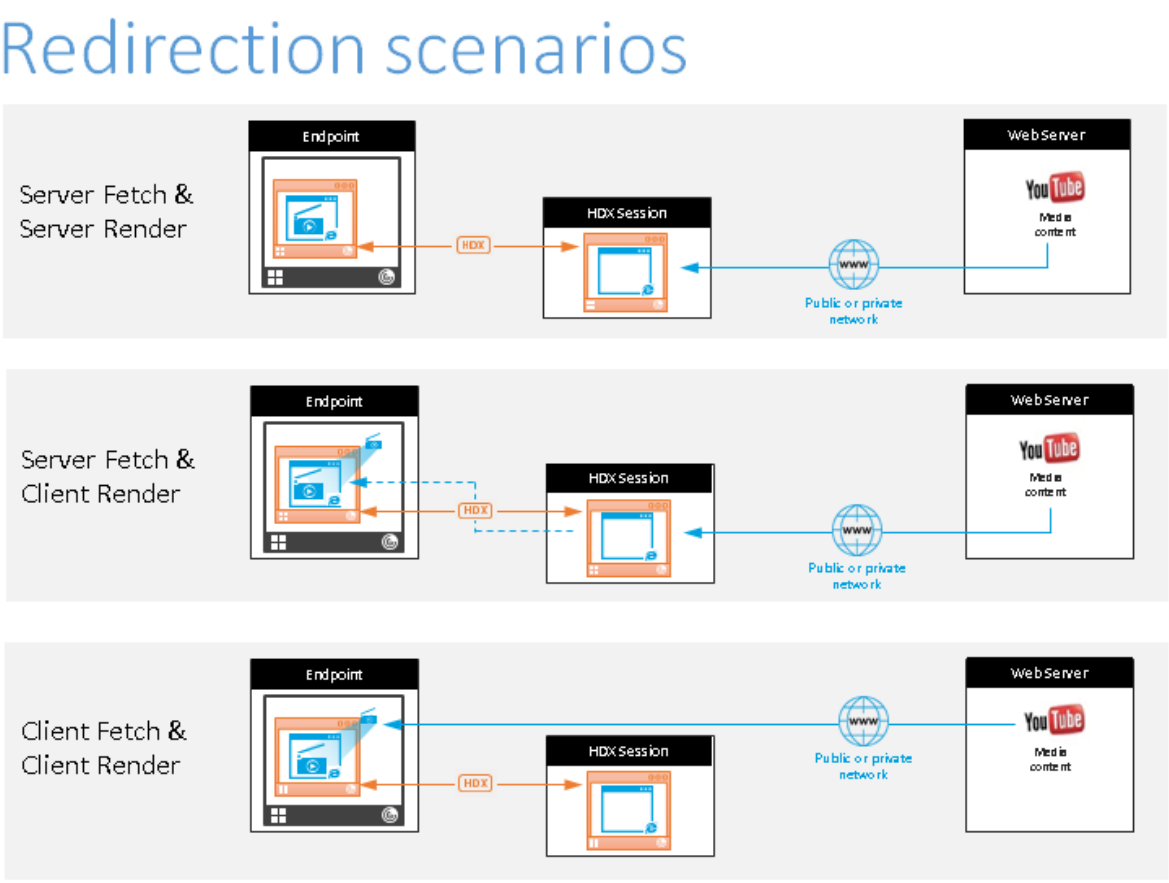



- **Recupero dal client e rendering sul client**: poiché l'app Citrix Workspace contatta direttamente il server Web, richiede l'accesso a Internet. Questo scenario consente l'offload di tutto l'utilizzo di rete, CPU e RAM dal sito XenApp e XenDesktop.

  Vantaggi:

  - Migliore esperienza utente finale (Adaptive Bit Rate [ABR])
  - Utilizzo ridotto delle risorse VDA (CPU/RAM/IO)
  - Consumo di larghezza di banda ridotto




**Meccanismo di fallback:**

In alcuni casi, il reindirizzamento del client non riesce. Ad esempio, se il computer client non dispone di accesso diretto a Internet, al VDA potrebbe essere restituita una risposta di errore. In questi casi, il browser sul VDA può quindi ricaricare la pagina sul server ed eseguirne il rendering.

È possibile impedire il rendering sul server di elementi video utilizzando i criteri di **prevenzione del fallback di Windows Media** esistenti. Impostare questo criterio su **Play all content only on client (Riproduci tutto il contenuto solo sul client)** o **Play only client-accessible content on client (Riproduci solo il contenuto accessibile dal client sul client)**. Queste impostazioni impediscono la riproduzione di elementi video sul server in caso di errori nel reindirizzamento del client. Questo criterio ha effetto solo quando si attiva il reindirizzamento del contenuto del browser e il criterio **Elenco di controllo di accesso** contiene l'URL di cui viene eseguito il fallback. L'URL non può essere incluso nel criterio dell'elenco di blocco.

**Requisiti di sistema:**

Endpoint Windows:

- Windows 10
- App Citrix Workspace 1809 per Windows o versioni successive

> **Nota:**
>
> Il reindirizzamento del contenuto del browser è supportato solo nella versione corrente dell'app Citrix Workspace per Windows, ma non nelle versioni LTSR dell'app Citrix Workspace, 1912 e 2203.1.

Endpoint Linux:

- App Citrix Workspace 1808 per Linux o versioni successive
- I terminali thin client devono includere WebKitGTK+

Citrix Virtual Apps and Desktops 7 1808 o versioni successive e XenApp e XenDesktop 7.15 CU5 o versioni successive:

- Sistema operativo VDA: Windows 10 (versione minima 1607), Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
- Browser sul VDA:
  - Google Chrome v66 o versioni successive (Chrome richiede l'app Citrix Workspace 1809 per Windows o versione successiva sull'endpoint dell'utente, VDA Citrix Virtual Apps and Desktops 7 1808 o versione successiva e l'estensione di reindirizzamento del contenuto del browser)
  - Internet Explorer 11 con le seguenti opzioni configurate:
    * Disabilitare **Modalità protetta avanzata** in: **Opzioni Internet** > **Avanzate** > **Sicurezza**
    * Selezionare **Abilita estensioni del browser di terze parti** in: **Opzioni Internet** > **Avanzate** > **Esplorazione**

### Risoluzione dei problemi

Per informazioni sulla risoluzione dei problemi, vedere l'articolo del Knowledge Center https://support.citrix.com/article/CTX230052

### Estensione Chrome per il reindirizzamento del contenuto del browser

Per utilizzare il reindirizzamento del contenuto del browser con Chrome, aggiungere l'estensione di reindirizzamento del contenuto del browser dal Chrome Web Store. Fare clic su **Add to Chrome** (Aggiungi a Chrome) nell'ambiente Citrix Virtual Apps and Desktops.

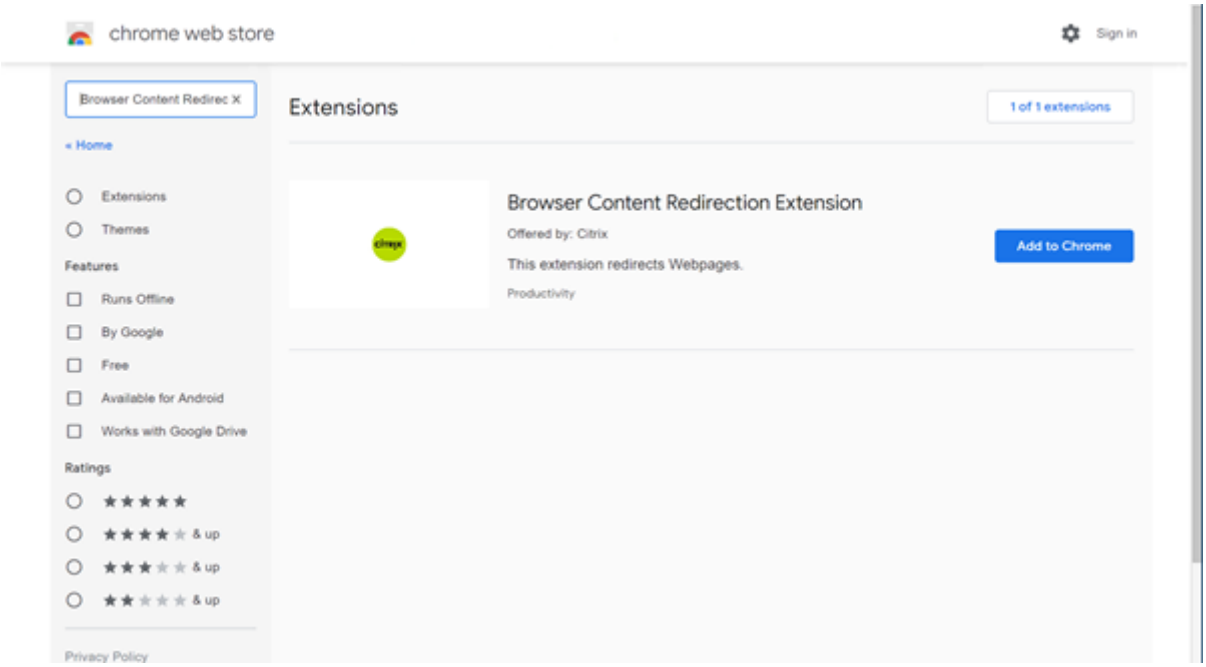
L'estensione **non** è richiesta sul computer client dell'utente, ma solo sul VDA.

### Requisiti di sistema

- Chrome v66 o versione successiva
- Estensione per il reindirizzamento del contenuto del browser
- Citrix Virtual Apps and Desktops 7 1808 o versioni successive
- App Citrix Workspace 1809 per Windows o versioni successive

> **Nota:**
>
> Il reindirizzamento del contenuto del browser è supportato solo nella versione corrente dell'app Citrix Workspace per Windows, ma non nelle versioni LTSR dell'app Citrix Workspace, 1912 e 2203.1.

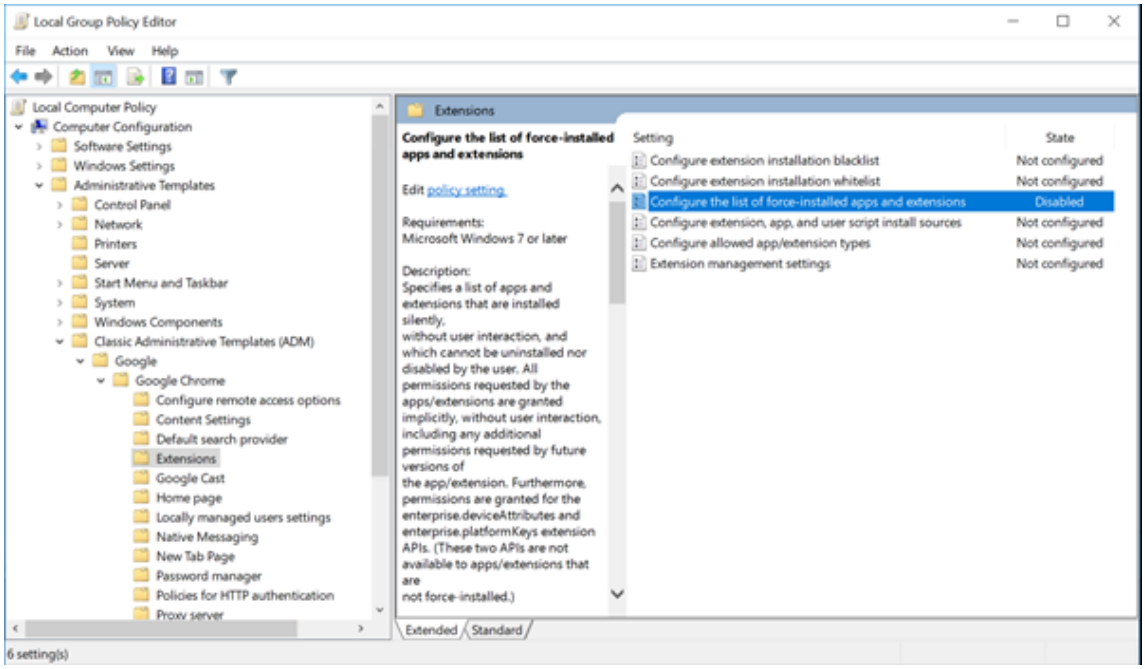



Questo metodo funziona per i singoli utenti. Per distribuire l'estensione a un grande gruppo di utenti dell'organizzazione, distribuire l'estensione utilizzando Criteri di gruppo.

### Distribuire l'estensione utilizzando Criteri di gruppo

1. Importare i file ADMX di Google Chrome nell'ambiente. Per informazioni sul download dei modelli di criteri e sull'installazione e la configurazione dei modelli nell'Editor Criteri di gruppo, vedere Impostare i criteri del browser Chrome sui PC gestiti.
2. Aprire la console Gestione Criteri di gruppo e andare a **Configurazione utente\Modelli amministrativi classici (ADM)\Google\Google Chrome\Estensioni**. Abilitare l'impostazione **Configure the list of force-installed apps and extensions (Configura l'elenco delle app e delle estensioni installate forzatamente)**.

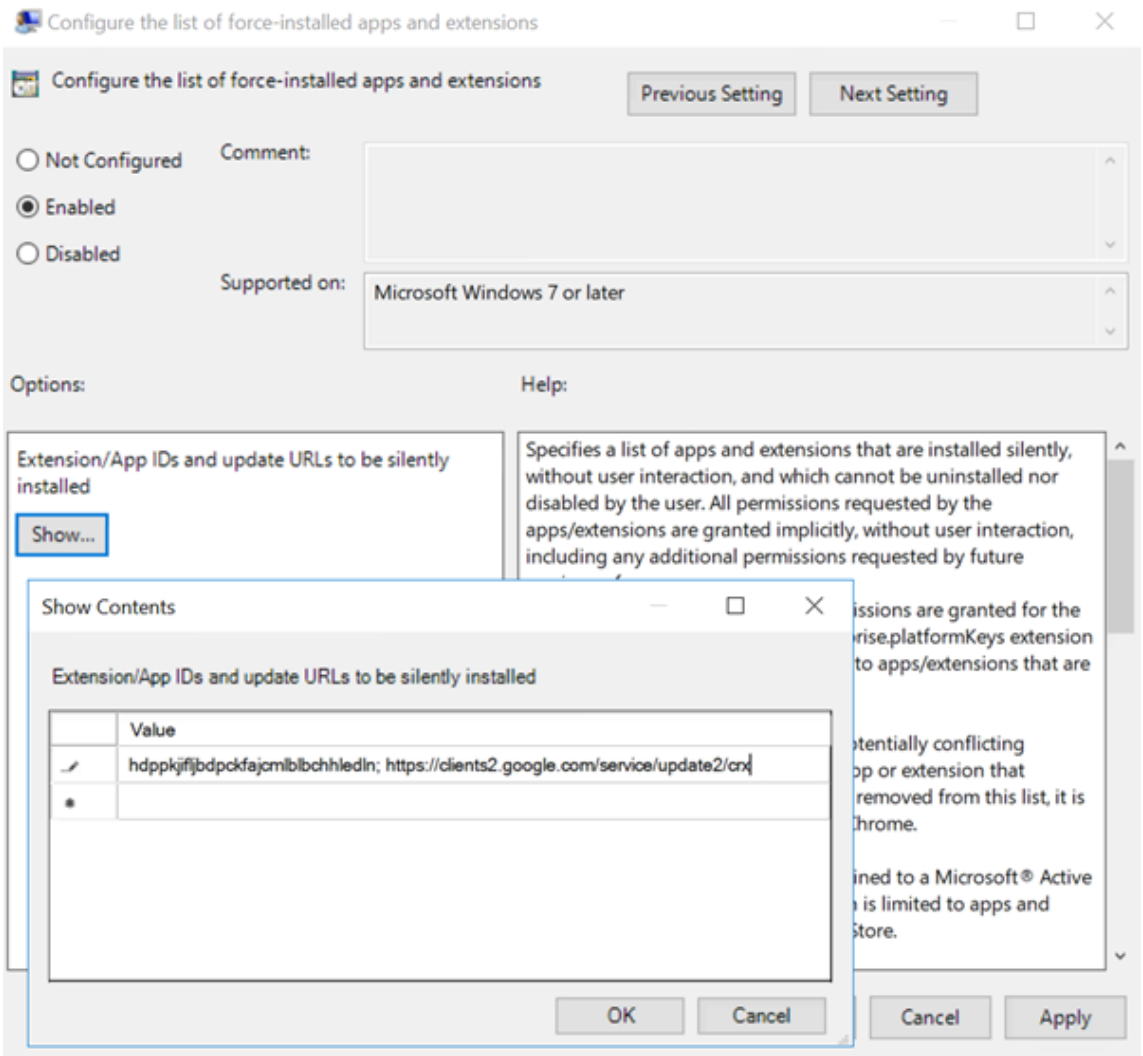
 




3. Fare clic su **Show (Mostra)** e digitare la seguente stringa, che corrisponde all'ID estensione. Aggiornare l'URL per l'estensione di reindirizzamento del contenuto del browser.

   ```
   hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
   ```




4. Applicare l'impostazione e dopo un aggiornamento di **gpupdate**, l'utente riceve automaticamente l'estensione. Se si avvia il browser Chrome nella sessione dell'utente, l'estensione è già applicata e l'utente non può rimuoverla.

   Eventuali aggiornamenti dell'estensione vengono installati automaticamente sui computer degli utenti tramite l'URL di aggiornamento specificato nell'impostazione.

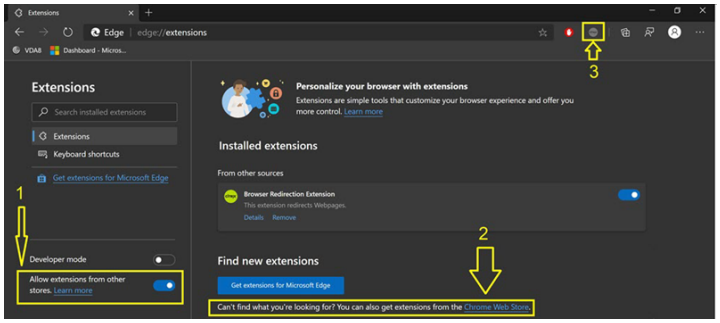
   Se l'impostazione **Configure the list of force-installed apps and extensions (Configura l'elenco delle app e delle estensioni installate forzatamente)** è impostata su **Disabled (Disabilitata)**, l'estensione viene rimossa automaticamente da Chrome per tutti gli utenti.

### Estensione Edge Chromium per il reindirizzamento del contenuto del browser

Per installare l'estensione di reindirizzamento del contenuto del browser in Edge, assicurarsi di avere installato la versione **83.0.478.37** o successiva del browser Edge.

1. Fai clic sull'opzione **Extensions** . Scegliere **Manage extension** (Gestisci estensione). Attivare **Allow extensions from other stores** (Consenti estensioni da altri negozi).
2. Fare clic sul collegamento **Chrome Web Store** e l'estensione verrà visualizzata nella barra in alto a destra.
   Per ulteriori informazioni sulle estensioni di Microsoft Edge, vedere Estensioni.




## Reindirizzamento del contenuto del browser e DPI

Quando si utilizza il reindirizzamento del contenuto del browser con DPI (ridimensionamento) impostato su un valore superiore a 100% sulla macchina dell'utente, la schermata del contenuto del browser reindirizzato viene visualizzata in modo errato. Per evitare questo problema, non impostare il DPI quando si utilizza il reindirizzamento del contenuto del browser. Un altro modo per evitare il problema è disabilitare l'accelerazione GPU per il reindirizzamento del contenuto del browser per Chrome creando la chiave del Registro di sistema sulla macchina dell'utente. Per informazioni, vedere Reindirizzamento del contenuto del browser e DPI nell'elenco delle funzionalità gestite tramite il registro.

## Single Sign-on con Autenticazione integrata di Windows

Il reindirizzamento del contenuto del browser migliora l'overlay per utilizzare lo schema Negotiate (Negozia) per l'autenticazione ai server Web configurati con l'autenticazione integrata di Windows (IWA) all'interno dello stesso dominio del VDA.

Per impostazione predefinita, il reindirizzamento del contenuto del browser utilizza uno schema di autenticazione di base che richiede agli utenti di autenticarsi con le proprie credenziali VDA ogni volta che accedono al server Web. Per il Single Sign-On, è possibile abilitare l'impostazione dei criteri **Browser content redirection Integrated Windows Authentication support** (Supporto dell'autenticazione Windows integrata per il reindirizzamento del contenuto del browser) oppure creare una chiave del Registro di sistema sul VDA.

Prima di abilitare il Single Sign-On, completare quanto segue:

- Configurare l'infrastruttura Kerberos per emettere ticket per i nomi principali di servizio (SPN) creati dal nome host. Ad esempio, `HTTP/serverhostname.com`.
- Per il recupero dal server: quando si utilizza il reindirizzamento del contenuto del browser in modalità di recupero dal server, assicurarsi che DNS sia configurato correttamente sul VDA.
- Per il recupero dal client: quando si utilizza il reindirizzamento del contenuto del browser in modalità di recupero dal client, assicurarsi che DNS sia configurato correttamente sul dispositivo client e che le connessioni TCP siano consentite dalla sovrapposizione all'indirizzo IP del server Web.

Per configurare il servizio Single Sign-On utilizzando il criterio di reindirizzamento del contenuto del browser, vedere l'impostazione Supporto dell'autenticazione Windows integrata per il reindirizzamento del contenuto del browser.

In alternativa, è possibile abilitare il Single Sign-On su un server Web aggiungendo una chiave del Registro di sistema sul VDA. Per informazioni, vedere Single Sign-on con Autenticazione integrata di Windows per il reindirizzamento del contenuto del browser nell'elenco delle funzionalità gestite tramite il registro.

### Intestazione della richiesta utente-agente

L'intestazione utente-agente aiuta a identificare le richieste HTTP inviate dal reindirizzamento del contenuto del browser. Questa impostazione può essere utile quando si configurano regole proxy e firewall. Ad esempio, se il server blocca le richieste inviate dal reindirizzamento del contenuto del browser, è possibile creare una regola che contiene l'intestazione utente-agente per ignorare determinati requisiti.

Solo i dispositivi Windows supportano l'intestazione della richiesta utente-agente.

Per impostazione predefinita, la stringa di intestazione della richiesta utente-agente è disabilitata. Per abilitare l'intestazione utente-agente per il contenuto con rendering sul client, utilizzare l'editor del Registro di sistema. Per informazioni, vedere Intestazione della richiesta utente-agente nell'elenco delle funzionalità gestite tramite il Registro di sistema.

### Compatibilità del client con il reindirizzamento del contenuto del browser

È possibile utilizzare WMI per verificare se il client è compatibile con il reindirizzamento del contenuto del browser. Utilizzare qualsiasi metodo che funzioni per accedere a WMI. Di seguito è riportato un esempio di utilizzo di PowerShell.

1. Aprire PowerShell.
2. Eseguire `Get-WmiObject -Class CTXBCRStatus`.
3. Controllare il parametro `BCR_Capable`.

- In caso di `True`, il client è compatibile con il reindirizzamento del contenuto del browser.
- In caso di `False`, il client non è compatibile con il reindirizzamento del contenuto del browser.

**Informazioni aggiuntive**

- Se `CtxBrowserSvc` non è disponibile, non viene visualizzato alcun risultato durante l'esecuzione del comando.
- Se `CtxBrowserSvc` non è mai stato eseguito, i risultati restituiscono un errore di classe non valido.

## Videoconferenze HDX e compressione video della webcam

January 7, 2024

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Le webcam possono essere utilizzate dalle applicazioni in esecuzione all'interno della sessione virtuale utilizzando la compressione video della webcam HDX o il reindirizzamento USB generico HDX plug-n-play. Utilizzare l'**app Citrix Workspace > Preferences (Preferenze) > Devices (Dispositivi)** per passare da una modalità all'altra. Citrix consiglia di utilizzare sempre la compressione video della webcam HDX, se possibile. Il reindirizzamento USB generico HDX è consigliato solo in caso di problemi di compatibilità delle applicazioni con la compressione video HDX o quando si richiedono funzionalità native avanzate della webcam. Per migliorare le prestazioni, Citrix consiglia che sul Virtual Delivery Agent siano disponibili almeno due CPU virtuali.

Per impedire agli utenti di modificare la compressione video HDX della webcam, disabilitare il reindirizzamento dei dispositivi USB utilizzando le impostazioni dei criteri in **ICA policy settings (Impostazioni criteri ICA) > USB Devices policy (Criteri dispositivi USB)**. Gli utenti dell'app Citrix Workspace possono ignorare il comportamento predefinito scegliendo l'impostazione **Non usare il microfono e la web** in Microfono e webcam in Desktop Viewer.

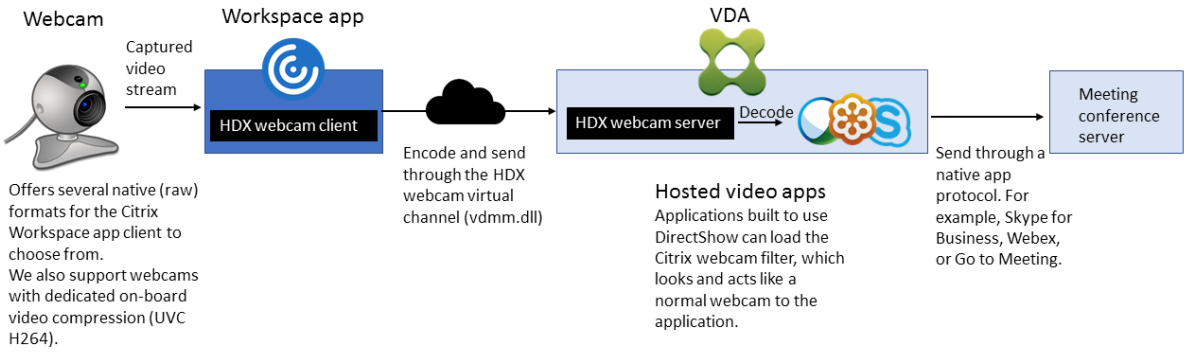
### Compressione video della webcam HDX

La compressione video della webcam HDX è anche chiamata modalità webcam **ottimizzata**. Questo tipo di compressione del video della webcam invia il video H.264 direttamente all'applicazione di videoconferenza in esecuzione nella sessione virtuale. Per ottimizzare le risorse VDA, la compressione della webcam HDX non codifica, transcodifica e decodifica i video della webcam. Questa funzionalità è abilitata per impostazione predefinita.

Per disabilitare lo streaming video diretto dal server all'app per videoconferenze, impostare la chiave del Registro di sistema su 0 nel VDA. Per informazioni, vedere Compressione video webcam nell'elenco delle funzionalità gestite tramite il registro.

Se si disabilita la funzionalità predefinita per lo streaming delle risorse video, la compressione video della webcam HDX utilizza la tecnologia del framework multimediale che fa parte del sistema operativo client per intercettare il video dai dispositivi di acquisizione, transcodificarlo e comprimerlo. I produttori di dispositivi di acquisizione forniscono i driver che si collegano all'architettura di streaming del kernel del sistema operativo.

Il client gestisce la comunicazione con la webcam. Il client invia quindi il video solo al server che può visualizzarlo correttamente. Il server non interagisce direttamente con la webcam, ma la sua integrazione offre la stessa esperienza sul desktop. L'app Workspace comprime il video per risparmiare larghezza di banda e fornire una migliore resilienza negli scenari WAN.




I criteri per le **conferenze multimediali** devono essere abilitati per la compressione video della webcam HDX. Questo criterio è abilitato per impostazione predefinita.

Se una webcam supporta la codifica hardware, la compressione video HDX utilizza la codifica hardware per impostazione predefinita. La codifica hardware potrebbe consumare più larghezza di banda rispetto alla codifica software. Per forzare la compressione del software, modificare la chiave del Registro di sistema sul client. Per informazioni, vedere Compressione del software della webcam nell'elenco delle funzionalità gestite tramite il registro.

**Requisiti di compressione video della webcam HDX**

La compressione video della webcam HDX supporta le seguenti versioni dell'app Citrix Workspace:

| Piattaforma | Processore |
|---|---|
| App Citrix Workspace per Windows | L'app Citrix Workspace per Windows supporta la compressione video della webcam per applicazioni a 32 e 64 bit su XenApp e XenDesktop 7.17 e versioni successive. Nelle versioni precedenti, l'app Citrix Workspace per Windows supporta solo app a 32 bit. |
| App Citrix Workspace per Mac | L'app Citrix Workspace per Mac 2006 o versioni successive supporta la compressione video della webcam per app a 64 bit su XenApp e XenDesktop 7.17 e versioni successive. Nelle versioni precedenti, l'app Citrix Workspace per Mac supporta solo app a 32 bit. |
| App Citrix Workspace per Linux | L'app Citrix Workspace per Linux supporta sia le app a 32 bit che quelle a 64 bit sul desktop virtuale. |
| App Citrix Workspace per Chrome | Poiché alcuni Chromebook ARM non supportano la codifica H.264, solo le app a 32 bit possono utilizzare la compressione video ottimizzata della webcam HDX. |

Le applicazioni video basate su Media Foundation supportano la compressione video della webcam HDX su Windows 8.x o versioni successive e Windows Server 2012 R2 e versioni successive. Per ulteriori informazioni, vedere l'articolo CTX132764 del Knowledge Center.

Altri requisiti del dispositivo utente:

- Hardware appropriato per riprodurre il suono.
- Webcam compatibile con DirectShow (utilizzare le impostazioni predefinite della webcam). Le webcam con funzionalità di codifica hardware riducono l'utilizzo della CPU lato client.
- Per la compressione video della webcam HDX, installare i driver della webcam sul client, ottenuti dal produttore della videocamera, se possibile. L'installazione dei driver del dispositivo non è necessaria sul server.

Webcam diverse offrono frequenze dei fotogrammi diverse e hanno livelli diversi di luminosità e contrasto. La regolazione del contrasto della webcam può ridurre significativamente il traffico a monte. Citrix utilizza le seguenti webcam per la convalida iniziale delle funzionalità:

- Modelli Microsoft LifeCam VX (2000, 3000, 5000, 7000)
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger
- Logitech C600, C920
- Webcam HP Deluxe

Per regolare la frequenza dei fotogrammi video preferita, modificare la chiave del Registro di sistema sul client. Per informazioni, vedere Frequenza dei fotogrammi di compressione video della webcam nell'elenco delle funzionalità gestite tramite il Registro di sistema.

### Streaming della webcam ad alta definizione

L'applicazione di videoconferenza sul server seleziona il formato e la risoluzione della webcam in base ai tipi di formato supportati. Quando si avvia una sessione, il client invia le informazioni della webcam al server. Scegliere una webcam dall'applicazione. Quando la webcam e l'applicazione di videoconferenza supportano il rendering ad alta definizione, l'applicazione utilizza una risoluzione ad alta definizione. Supportiamo tutte le risoluzioni delle webcam.

Questa funzionalità richiede l'app Citrix Workspace per Windows, versione minima 1808 o Citrix Receiver per Windows, versione minima 4.10.

È possibile utilizzare una chiave del Registro di sistema per disabilitare e abilitare la funzionalità. Per informazioni, vedere Streaming della webcam ad alta definizione nell'elenco delle funzionalità gestite tramite il registro.

Se la negoziazione del tipo di supporto non riesce, HDX torna alla risoluzione VGA predefinita (640 x 480 pixel). È possibile utilizzare le chiavi del Registro di sistema nel client per configurare la risoluzione predefinita. Assicurarsi che la videocamera supporti la risoluzione specificata. Per informazioni, vedere Risoluzione della webcam ad alta definizione nell'elenco delle funzionalità gestite tramite il registro.

La compressione video della webcam HDX utilizza una larghezza di banda significativamente inferiore rispetto al reindirizzamento USB generico plug-n-play e funziona bene sulle connessioni WAN. Per regolare la larghezza di banda, impostare la chiave del Registro di sistema sul client. Per informazioni, vedere Larghezza di banda della webcam ad alta definizione nell'elenco delle funzionalità gestite tramite il registro.

Immettere un valore in bit al secondo. Se non si specifica la larghezza di banda, le applicazioni di videoconferenza utilizzano 350.000 bps per impostazione predefinita.

### Reindirizzamento USB generico HDX plug-n-play

Il reindirizzamento USB generico HDX plug-n-play (isocrono) è anche chiamato modalità webcam **generica**. Il vantaggio del reindirizzamento USB generico HDX plug-n-play è che non è necessario installare driver sul thin client/endpoint. Lo stack USB è virtualizzato in modo tale che tutto ciò che si collega al client locale venga inviato alla macchina virtuale remota. Il desktop remoto agisce come se fosse collegato in modo nativo. Il desktop Windows gestisce tutte le interazioni con l'hardware ed esamina la logica plug-n-play per trovare i driver corretti. La maggior parte delle webcam funziona se i driver sono presenti sul server e possono funzionare su ICA. La modalità webcam generica utilizza una larghezza di banda significativamente maggiore (molti megabit al secondo) perché vengono inviati video non compressi sulla rete con il protocollo USB.

## Reindirizzamento multimediale HTML5

January 7, 2024

Il reindirizzamento multimediale HTML5 estende le funzionalità di reindirizzamento multimediale di HDX MediaStream per includere audio e video HTML5. A causa della crescita della distribuzione online di contenuti multimediali, in particolare ai dispositivi mobili, l'industria dei browser ha sviluppato modi più efficienti per presentare audio e video.

Flash è stato lo standard, ma richiede un plug-in, non funziona su tutti i dispositivi e richiede un maggiore utilizzo della batteria nei dispositivi mobili. Aziende come YouTube, Netflix e le versioni più recenti dei browser di Mozilla, Google e Microsoft stanno passando a HTML5, che sta diventando il nuovo standard.

I contenuti multimediali basati su HTML5 presentano molti vantaggi rispetto ai plug-in proprietari, tra cui:

- Standard indipendenti dall'azienda (W3C)
- Flusso di lavoro DRM (Digital Rights Management) semplificato
- Prestazioni migliori senza problemi di sicurezza generati dai plug-in

### Download progressivi HTTP

Il download progressivo HTTP è un metodo di pseudo-streaming basato su HTTP che supporta HTML5. In un download progressivo, il browser riproduce un singolo file (codificato con un'unica qualità) mentre viene scaricato da un server Web HTTP. Il video viene memorizzato sull'unità mentre viene ricevuto e viene riprodotto dall'unità. Se si guarda nuovamente il video, il browser può caricarlo dalla cache.

Per un esempio di download progressivo, vedere la pagina di test di reindirizzamento video HTML5. Per ispezionare gli elementi video nella pagina Web e trovare le fonti (formato contenitore mp4) nei tag video HTML5, utilizzare gli strumenti di sviluppo nel browser:

### Confronto tra HTML5 e Flash

| Funzionalità | HTML5 | Flash |
|---|---|---|
| Richiede un lettore proprietario | No | Sì |
| Funziona su dispositivi mobili | Sì | Alcuni |
| Velocità di esecuzione su piattaforme diverse | Elevata | Bassa |
| Supportato da iOS | Sì | No |
| Utilizzo delle risorse | Minore | Maggiore |
| Caricamento più rapido | Sì | No |

### Requisiti

Supportiamo solo il reindirizzamento per download progressivi in formato mp4. Non supportiamo le tecnologie di streaming della velocità in bit WebM e Adaptive come DASH/HLS.

Supportiamo quanto segue e utilizziamo i criteri per il controllo. Per ulteriori informazioni, vedere Impostazioni dei criteri multimediali.

- Rendering lato server
- Rendering sul client con recupero dal server
- Recupero e rendering lato client

Versioni minime dell'app Citrix Workspace e di Citrix Receiver:

- App Citrix Workspace 1808 per Windows
- Citrix Receiver per Windows 4.5
- App Citrix Workspace 1808 per Linux
- Citrix Receiver per Linux 13.5

| Versione minima del browser del VDA | Versione del sistema operativo/build/SP Windows |
|---|---|
| Internet Explorer 11.0 | Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows 7 x86 e x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |
| Firefox 47 Aggiungere manualmente i certificati all'archivio dei certificati di Firefox o configurare Firefox per cercare i certificati da un archivio di certificati attendibili di Windows. Per ulteriori informazioni, vedere https://wiki.mozilla.org/CA:AddRootToFirefox | Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows 7 x86 e x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |
| Chrome 51 | Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows 7 x86 e x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |

### Componenti della soluzione di reindirizzamento video HTML5

- **HdxVideo.js**: comandi video ch che intercettano gli hook JavaScript sul sito Web. HdxVideo.js comunica con WebSocketService utilizzando Secure WebSockets (SSL/TLS).
- **Certificati SSL WebSocket**
  - Per la CA (root): **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA)
    Posizione: **Certificati (Computer locale) > Autorità di certificazione radice attendibili > Certificati**.
  - Per l'entità finale (foglia): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service)
    Posizione: **Certificati (Computer locale) > Personale > Certificati**.
- **WebSocketService.exe**: viene eseguito sul sistema locale ed esegue la terminazione SSL e il mapping della sessione utente. TLS Secure WebSocket in ascolto sulla porta 127.0.0.1 9001.
- **WebSocketAgent.exe**: viene eseguito nella sessione utente ed esegue il rendering del video come indicato dai comandi WebSocketService.

### Come è possibile abilitare il reindirizzamento video HTML5?

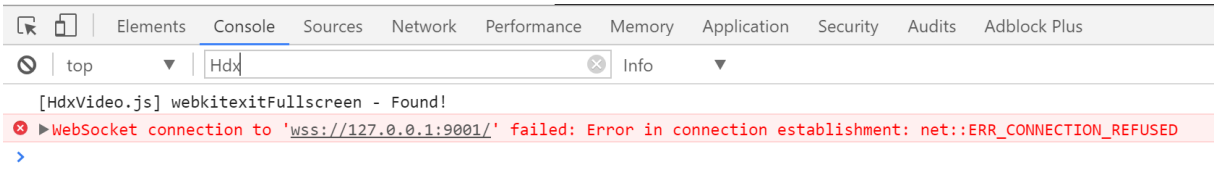
In questa versione, questa funzionalità è disponibile solo per le pagine Web controllate. Richiede l'aggiunta del JavaScript HdxVideo.js (incluso nel supporto di installazione di Citrix Virtual Apps and Desktops) alle pagine Web in cui è disponibile il contenuto multimediale HTML5. Ad esempio, i video su un sito di formazione interno.

Siti Web come youtube.com, basati su tecnologie di bitrate adattivo (ad esempio, HTTP Live Streaming [HLS] e Dynamic Adaptive Streaming over HTTP [DASH]), non sono supportati.

Per ulteriori informazioni, vedere *Impostazioni dei criteri multimediali*.

### Consigli per la risoluzione dei problemi

Possono verificarsi degli errori quando la pagina Web tenta di eseguire HdxVideo.js. Se il JavaScript non viene caricato, il meccanismo di reindirizzamento HTML5 non va a buon fine. Assicurarsi che non vi siano errori relativi a HdxVideo.js ispezionando la console nelle finestre degli strumenti di sviluppo del browser. Ad esempio:




## Ottimizzazione di Microsoft Teams

January 7, 2024

> **Nota:**
>
> Il nuovo Microsoft Teams 2.1 è attualmente testato da Microsoft in anteprima. Questa versione di Teams sarà compatibile con Citrix Teams Optimization tramite WebRTC (VDI 1.0). Ciò richiede una nuova impostazione di configurazione del registro nel VDA per consentire alla nuova versione di Teams di accedere al canale virtuale Citrix.
> Per abilitare l'ottimizzazione di Teams 2.1, configurare la seguente chiave di registro nel VDA:
>
> Posizione: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
>
> Chiave (REG_Multi_SZ): `ProcessWhitelist`

> Valore: `msedgewebview2.exe`
>
> Per ulteriori informazioni, vedere la documentazione Microsoft.

Citrix offre ottimizzazione per Microsoft Teams basato su desktop utilizzando Citrix Virtual Apps and Desktops e l'app Citrix Workspace. Per impostazione predefinita, tutti i componenti necessari vengono raggruppati nell'app Citrix Workspace e nel Virtual Delivery Agent (VDA).

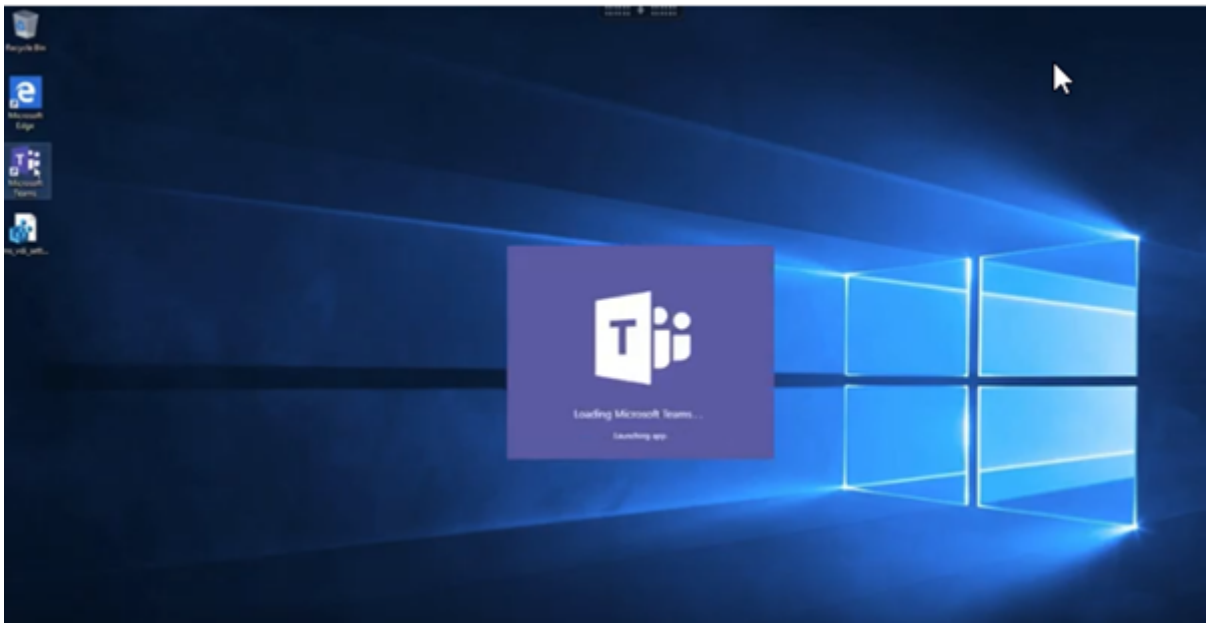
L'ottimizzazione di Citrix per Microsoft Teams include servizi HDX lato VDA e un'API per interfacciarsi con l'app ospitata Microsoft Teams per ricevere comandi. Questi componenti aprono un canale virtuale di controllo (CTXMTOP) verso il motore multimediale sul lato dell'app Citrix Workspace. L'endpoint decodifica i contenuti multimediali e ne esegue il provisioning localmente, spostando nuovamente la finestra dell'app Citrix Workspace nell'app Microsoft Teams ospitata.

L'autenticazione e la segnalazione si verificano in modo nativo nell'app ospitata Microsoft Teams, proprio come gli altri servizi Microsoft Teams (ad esempio chat o collaborazione). Il reindirizzamento audio/video non influisce.

`CTXMTOP` è un comando e un canale virtuale di controllo. Ciò significa che i contenuti multimediali non vengono scambiati tra l'app Citrix Workspace e il VDA.

È disponibile solo il recupero dal client e il rendering sul client.

Questo video dimostrativo dà un'idea di come Microsoft Teams funziona in un ambiente virtuale Citrix.



### Installazione di Microsoft Teams

Citrix e Microsoft consigliano di utilizzare l'ultima versione disponibile di Microsoft Teams e di mantenerla aggiornata.
Le versioni dell'app desktop Microsoft Teams con date di rilascio più vecchie di 90 giorni rispetto alla data di rilascio della versione corrente non sono supportate.
Le versioni dell'app desktop Microsoft Teams non supportate presentano agli utenti una pagina di blocco e richiedono di aggiornare l'app.

Per informazioni sulle ultime versioni disponibili, vedere la cronologia degli aggiornamenti per la versione dell'app Microsoft Teams (desktop e Mac).

Si consiglia di seguire le linee guida per l'installazione di Microsoft Teams a livello di macchina. Evitare di utilizzare il programma di installazione .exe che installa Microsoft Teams in `AppData`. Installare invece in `C:\Program Files (x86)\Microsoft\Teams` utilizzando il flag `ALLUSER=1` dalla riga di comando.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1
ALLUSERS=1
```

In questo esempio viene utilizzato anche il parametro `ALLUSERS=1`. Quando si imposta questo parametro, il programma di installazione di Microsoft Teams a livello di macchina viene visualizzato in **Programmi e funzionalità** nel **Pannello di controllo**. Inoltre, in **App e funzionalità** nelle Impostazioni di Windows per tutti gli utenti del computer. Tutti gli utenti possono quindi disinstallare Microsoft Teams se dispongono di credenziali di amministratore.

È importante capire la differenza tra `ALLUSERS=1` e `ALLUSER=1`. È possibile utilizzare il parametro `ALLUSERS=1` in ambienti non VDI e VDI. Utilizzare il parametro `ALLUSER=1` solo negli ambienti VDI per specificare un'installazione per ogni macchina.

In modalità `ALLUSER=1` l'applicazione Microsoft Teams non si aggiorna automaticamente ogni volta che è disponibile una nuova versione. Questa modalità è consigliata per ambienti non persistenti, come app o desktop condivisi ospitati di Windows Server o cataloghi random/in pool di Windows 10. Per ulteriori informazioni, vedere Installare Microsoft Teams utilizzando MSI (sezione Installazione VDI).

Supponiamo che si disponga di un ambiente VDI persistente Windows 10 dedicato. Si desidera che l'applicazione Microsoft Teams si aggiorni automaticamente e si preferisce che Microsoft Teams si installi per ciascun utente in `Appdata/Local`. In questo caso, utilizzare il programma di installazione di `.exe` o il file MSI senza `ALLUSER=1`.

> **Nota:**
>
> Si consiglia di installare il VDA prima di installare Microsoft Teams nell'immagine golden. Questo ordine di installazione è necessario perché il flag `ALLUSER=1` abbia effetto. Se è stato instal-

> lato Microsoft Teams sulla macchina virtuale prima di installare il VDA, disinstallare e reinstallare Microsoft Teams.

### Per l'accesso remoto al PC

Si consiglia di installare Microsoft Teams versione 1.4.00.22472 o successiva, dopo aver installato il VDA. In caso contrario, è necessario disconnettersi e accedere nuovamente in modo che Microsoft Teams rilevi il VDA come previsto. La versione 1.4.00.22472 e le successive includono la logica aumentata eseguita al momento dell'avvio di Microsoft Teams e il tempo di accesso per il rilevamento del VDA. Queste versioni includono anche l'identificazione del tipo di sessione attiva (HDX, RDP o connessione locale alla macchina client). Se si è connessi localmente, le versioni precedenti di Microsoft Teams potrebbero non riuscire a rilevare e disabilitare determinate funzionalità o elementi dell'interfaccia utente. Ad esempio, stanze per sottogruppi di lavoro, finestre a comparsa per riunioni e chat o reazioni alle riunioni.

> **Importante:**
>
> Quando si esegue il roaming da una sessione locale a una sessione HDX e Microsoft Teams viene mantenuto aperto e in esecuzione in background, è necessario uscire e riavviare Microsoft Teams per ottimizzare correttamente con HDX.
> Al contrario, se si utilizza Microsoft Teams in remoto tramite una sessione HDX ottimizzata, disconnettere la sessione HDX e riconnettersi alla stessa sessione di Windows localmente sul dispositivo. Quando si lavora dall'ufficio, è necessario riavviare Microsoft Teams in modo che possa rilevare correttamente lo stato di Remote PC Access (HDX o locale). poiché Microsoft Teams può valutare la modalità VDI solo al momento dell'avvio dell'app e non mentre è già in esecuzione in background. Senza un riavvio, Microsoft Teams potrebbe non riuscire a caricare funzionalità come finestre disancorate, stanze di lavoro o reazioni alle riunioni.

### Per App Layering

Se si utilizza Citrix App Layering per gestire le installazioni di VDA e Microsoft Teams in livelli diversi, è necessario creare una chiave del Registro di sistema sui VDA Windows prima di installare Microsoft Teams con il flag `ALLUSER=1` dalla riga di comando. Per ulteriori informazioni, vedere la sezione *Ottimizzazione per Microsoft Teams con Citrix App Layering* in Multimedia.

### Consigli per la gestione dei profili

Si consiglia di utilizzare il programma di installazione a livello di macchina per ambienti Windows Server e Windows 10 VDI in pool.

Quando il flag **ALLUSER=1** viene trasferito all'MSI dalla riga di comando (il programma di installazione a livello di macchina), l'app Microsoft Teams viene installata in `C:\Program Files (x86)` (~300 MB). L'app utilizza `AppData\Local\Microsoft\TeamsMeetingAddin` per i log e `AppData\Roaming\Microsoft\Teams` (~ 600-700 MB) per configurazioni specifiche dell'utente, memorizzazione nella cache degli elementi nell'interfaccia utente e così via.

> **Importante:**
>
> Se non si trasferisce il flag **ALLUSER=1**, il file MSI inserisce il programma di installazione Teams.exe e `setup.json` in `C:\Program Files (x86)\Teams Installer`. Una chiave del Registro di sistema (TeamsMachineInstaller) viene aggiunta in: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
>
> Un successivo accesso utente attiva invece l'installazione finale in **AppData**.

#### Programma di installazione a livello di macchina

Di seguito è riportato un esempio di cartelle, collegamenti sul desktop e chiavi del Registro di sistema creati installando un programma di installazione di Microsoft Teams a livello di macchina in una macchina virtuale Windows Server 2016 a 64 bit:

*Cartella:*

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

*Collegamento sul desktop:*

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

*Chiavi del Registro di sistema:*

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- Nome: `Teams`
- Tipo: `REG_SZ`
- Valore: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **Nota:**
>
> La posizione del Registro di sistema varia in base ai sistemi operativi sottostanti e al numero di bit.

### Consigli

- Si consiglia di disabilitare l'avvio automatico eliminando le chiavi del Registro di sistema di Microsoft Teams. Ciò impedisce che molti accessi che si verificano contemporaneamente (ad esempio, all'inizio della giornata lavorativa) sovraccarichino la CPU della VM.
- Se il desktop virtuale non dispone di una GPU/vGPU, si consiglia di impostare l'opzione **Disable GPU hardware acceleration** (Disabilita l'accelerazione hardware della GPU) nelle **impostazioni** di Microsoft Teams per migliorare le prestazioni. Questa impostazione (`"disableGpu":true`) è memorizzata in `%Appdata%\Microsoft\Teams` in `desktop-config.json`. È possibile utilizzare uno script di accesso per modificare tale file e impostare il valore su **true**.
- Se si utilizza Citrix Workspace Environment Management (WEM), abilitare **CPU Spikes Protection** (Protezione dai picchi di utilizzo della CPU) per gestire il consumo del processore per Microsoft Teams.

### Programma di installazione per ciascun utente

Quando si utilizza il programma di installazione di `.exe`, il processo di installazione è diverso. Tutti i file sono inseriti in AppData.

*Cartella:*

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

*Collegamento sul desktop:*

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"
```

*Chiavi del Registro di sistema:*

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

### Procedure consigliate

I consigli sulle procedure consigliate si basano sugli scenari di utilizzo.
L'utilizzo di Microsoft Teams con una configurazione non persistente richiede un gestore di memorizzazione nella cache dei profili per una sincronizzazione efficiente dei dati di runtime di Microsoft

Teams. Con un gestore di memorizzazione nella cache dei profili, le informazioni appropriate specifiche dell'utente vengano memorizzate nella cache durante la sessione utente. Ad esempio, le informazioni specifiche dell'utente includono dati utente, profilo e impostazioni. Sincronizzare i dati in queste due cartelle:

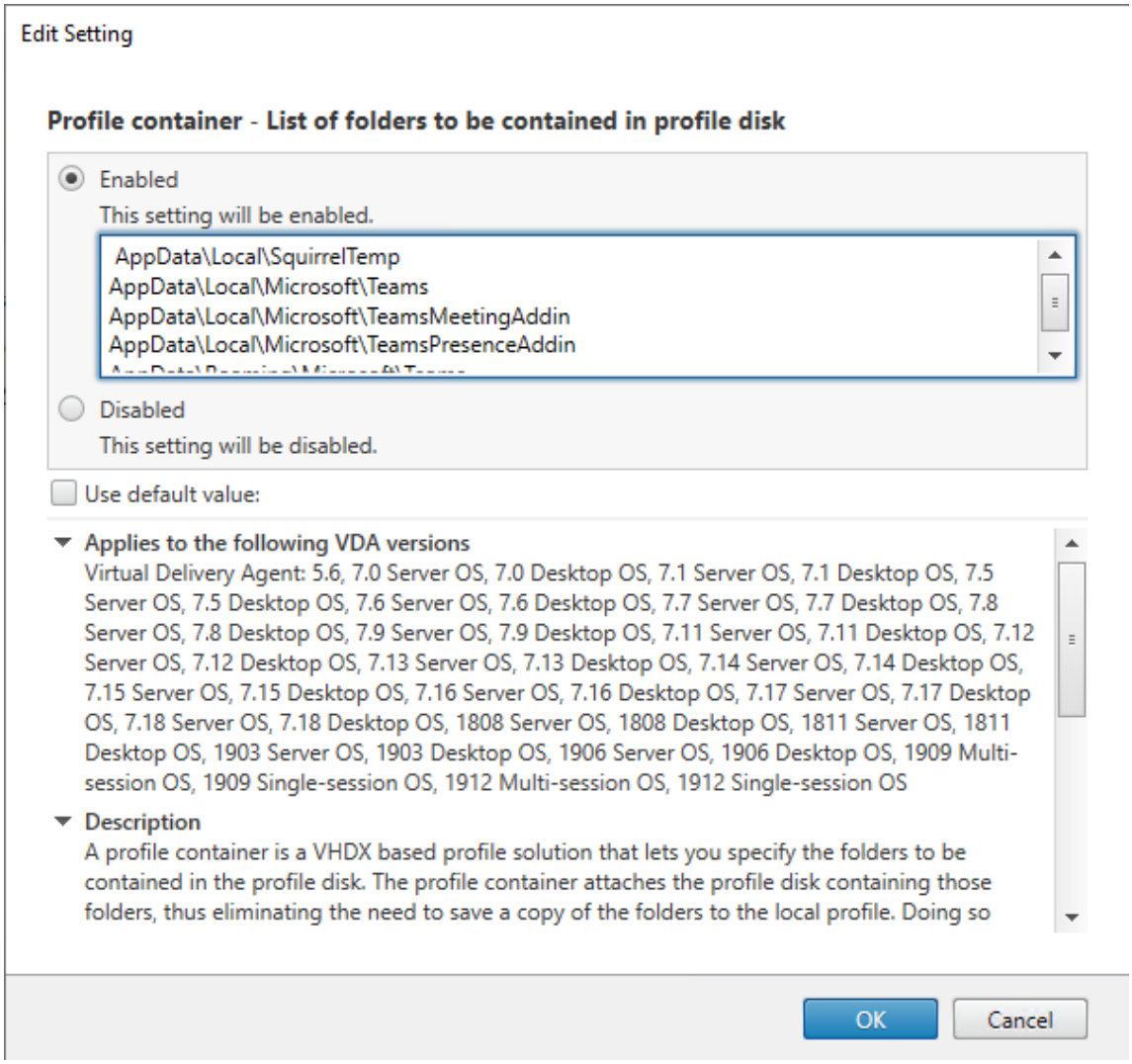
- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

**Elenco di esclusione dei contenuti di Microsoft Teams memorizzati nella cache per la configurazione non persistente** Escludere i file e le directory dalla cartella di memorizzazione nella cache di Microsoft Teams come descritto nella documentazione Microsoft. Questa azione consente di ridurre le dimensioni della memorizzazione nella cache dell'utente per ottimizzare ulteriormente la configurazione non persistente.

**Caso d'uso: scenario con sessione singola** In questo scenario, l'utente finale utilizza Microsoft Teams in una posizione alla volta. Non è necessario eseguire Microsoft Teams in due sessioni Windows contemporaneamente. In una distribuzione di desktop virtuale comune, ogni utente viene assegnato a un desktop e Microsoft Teams viene distribuito all'interno del desktop virtuale come un'unica applicazione.
Si consiglia di abilitare il contenitore Citrix Profile e di reindirizzare nel contenitore le directory per utente elencate in Per-user installer.

1. Distribuire il programma di installazione a livello di macchina di Microsoft Teams (**ALLUSER=1**) nell'immagine golden.
2. Abilitare Citrix Profile Management e configurare l'archivio dei profili utente con le autorizzazioni appropriate.
3. Abilitare la seguente impostazione dei criteri di Profile Management (Gestione profili): **File system > Synchronization (Sincronizzazione) > Profile container –List of folders to be contained in profile disk (Contenitore profilo - Elenco delle cartelle che devono essere contenute nel disco del profilo)**.




Elencare tutte le directory per ciascun utente in questa configurazione. È anche possibile configurare queste impostazioni utilizzando il servizio Citrix WEM (Workspace Environment Management).

4. Applicare le impostazioni al gruppo di consegna corretto.
5. Accedere per convalidare la distribuzione.

## Requisiti di sistema

### Versione minima consigliata - Delivery Controller (DDC) 1906.2

Se si utilizza una versione precedente, vedere Abilitare l'ottimizzazione di Microsoft Teams:

Sistemi operativi supportati:

- Windows Server 2022, 2019, 2016, 2012R2 edizioni Standard e per centri dati e con l'opzione Server Core

**Versione minima - Virtual Delivery Agent (VDA) 1906.2**

Sistemi operativi supportati:

- Windows 11.
- Windows 10 a 64 bit, versioni 1607 e successive. Le app ospitate da VM sono supportate nell'app Citrix Workspace per Windows 2109.1 e versioni successive.
- Windows Server 2022, 2019, 2016 e 2012 R2 (edizioni standard e per data center).

Requisiti:

- BCR_x64.msi: file MSI che include il codice di ottimizzazione di Microsoft Teams e viene avviato automaticamente dalla GUI. Se si utilizza l'interfaccia della riga di comando per l'installazione del VDA, non escluderlo.

**Versione consigliata: versione corrente più recente dell'app Citrix Workspace per Windows e versione minima: app Citrix Workspace 1907 per Windows**

- Windows 11.
- Windows 10 (edizioni a 32 bit e 64 bit, incluse le edizioni Embedded) (il supporto di Windows 7 è stato interrotto alla versione 2006) (il supporto di Windows 8.1 è stato interrotto alla versione 2204.1).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) e 2019 LTSC (v1809).
- Architetture di processore (CPU) supportate: x86 e x64 (ARM non è supportato).
- Requisiti endpoint: CPU dual core di circa 2,2-2,4 GHz in grado di supportare una risoluzione HD a 720p durante una chiamata in videoconferenza peer-to-peer.
- CPU dual o quad-core con velocità base più basse (~1,5 GHz) dotate di Intel Turbo Boost o AMD Turbo Core con possibile aumento fino ad almeno 2,4 GHz.
- Thin client HP verificati: t630/t640, t730/t740, mt44/mt45.
- Thin client Dell verificati: 5070, 5470 Mobile TC e AIO.
- Thin Client 10ZiG verificati: 4510 e 5810q.
- Per un elenco completo degli endpoint verificati, vedere Thin client.
- L'app Citrix Workspace richiede almeno 600 MB di spazio libero su disco e 1 GB di RAM.
- Il requisito minimo di Microsoft .NET Framework è la versione 4.8. L'app Citrix Workspace scarica e installa automaticamente .NET Framework se non è presente sul sistema.

Gli amministratori possono abilitare/disabilitare Microsoft Teams a partire dalla modalità ottimizzata modificando il criterio Optimization for Microsoft Teams. Gli utenti che iniziano in modalità ottimizzata nell'app Citrix Workspace non possono di disabilitare Microsoft Teams.

**Versione minima: app Citrix Workspace 2006 per Linux**

Per ulteriori informazioni, vedere Ottimizzazione per Microsoft Teams nella documentazione dell'app Citrix Workspace per Linux.

Software:

- GStreamer 1.0 o versione successiva o Cairo 2
- libc++-9.0 o versioni successive
- libgdk 3.22 o versione successiva
- OpenSSL 1.1.1d
- Distribuzione Linux x64

Miglioramento dell'autenticazione:

- Libreria Libsecret
- libreria libunwind-12. Per ulteriori informazioni, vedere Adding the libunwind-12 library dependency for llvm-12.

Hardware:

- CPU dual-core da almeno 1,8 GHz in grado di supportare una risoluzione HD a 720p durante una chiamata in videoconferenza peer-to-peer
- CPU dual o quad-core con una velocità base di 1,8 GHz e un'alta velocità Intel Turbo Boost di almeno 2,9 GHz

Per un elenco completo degli endpoint verificati, vedere Thin client.

Per ulteriori informazioni, vedere Prerequisiti per installare l'app Citrix Workspace.

È possibile disabilitare l'ottimizzazione di Microsoft Teams aggiornando il valore del campo **VDWEBRTC** su Off nel file `/opt/Citrix/ICAClient/config/module.ini`. Il valore predefinito è VDWEBRTC=On. Una volta completato l'aggiornamento, riavviare la sessione. (è richiesta l'autorizzazione root).

**Versione minima: app Citrix Workspace 2012 per Mac**

Sistemi operativi supportati:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 e versione successiva.
- macOS Monterey.

Funzionalità supportate:

- Audio

- Video
- Ottimizzazione della condivisione dello schermo (in entrata e in uscita)

> **Nota:**
>
> L'app Citrix Viewer richiede l'accesso alle preferenze di sicurezza e privacy di macOS perché la condivisione dello schermo possa funzionare. Gli utenti configurano questa preferenza accedendo al **menu Apple > Preferenze di sistema > Sicurezza e privacy > scheda Privacy > Registrazione dello schermo** e selezionando **Citrix Viewer**.

L'ottimizzazione di Microsoft Teams funziona per impostazione predefinita con l'app Citrix Workspace 2012 o versioni successive e macOS 10.15.

Se si desidera disabilitare l'ottimizzazione di Microsoft Teams, eseguire questo comando nel terminale e riavviare l'app Citrix Workspace:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

**Versione minima: l'ultima versione dell'app Citrix Workspace per ChromeOS in esecuzione sull'ultima versione di ChromeOS**

Hardware:

- Processori che funzionano alla pari o meglio del processore Intel i3, quad core da 2,4 GHz.

Funzionalità supportate:

- Audio
- Video
- Ottimizzazione della condivisione dello schermo (in entrata e in uscita): disabilitata per impostazione predefinita. Consultare queste impostazioni per istruzioni su come abilitarla.

## Scalabilità di un singolo server

Questa sezione fornisce consigli e indicazioni su come stimare il numero di utenti o macchine virtuali (VM) che possono essere supportati su un singolo host fisico. Questo è comunemente indicato come Scalabilità per server singolo di Citrix Virtual Apps and Desktops (SSS). Nel contesto di Citrix Virtual Apps (CVA) o della virtualizzazione delle sessioni, è anche comunemente noto come densità degli utenti. L'idea è scoprire quanti utenti o quante macchine virtuali possono essere eseguiti su un singolo componente hardware che esegue un hypervisor principale.

> **Nota:**
>
> Questa sezione include una guida per stimare l'SSS. La guida è di alto livello e potrebbe non

> essere necessariamente specifica per la propria situazione o il proprio ambiente specifico. L'unico modo per comprendere veramente l'SSS di Citrix Virtual Apps and Desktops è utilizzare uno strumento di test di scalabilità o carico come Login VSI. Citrix consiglia di utilizzare questa guida e queste semplici regole per stimare rapidamente solo l'SSS. Tuttavia, Citrix consiglia di utilizzare Login VSI o lo strumento di test di carico preferito per convalidare i risultati, soprattutto prima di acquistare hardware o prendere decisioni finanziarie.

**Hardware (sistema in prova)**

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 a 2,60 GHz (max Turbo 3,70 GHz), 12 core per socket, doppio socket con Hyperthreading abilitato
- 382 GB di RAM
- Archiviazione RAID 0 SSD locale (11 dischi) 6 TB

**Software**

Una singola macchina virtuale (40 processori logici) con Windows 2019 (TSVDA) che esegue Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7

**Terminologia**

- Carico di lavoro del lavoratore della conoscenza: include Acrobat Reader, Freemind/Java, Photo Viewer, Edge e app MS Office come Excel, Outlook, PowerPoint e Word.
- Baseline: test di scalabilità server eseguiti con il carico di lavoratore della conoscenza (senza Microsoft Teams)
- Carico di lavoro di Microsoft Teams: carico di lavoro tipico dei lavoratori della conoscenza + Microsoft Teams

**Come Microsoft Teams viene sottoposto a test di stress**

- Microsoft Teams è ottimizzato con HDX. Pertanto, tutta l'elaborazione multimediale viene scaricata sull'endpoint o sul client e non fa parte della misurazione.
- Tutti i processi di Microsoft Teams sono stati arrestati o interrotti prima dell'inizio del carico di lavoro.
- Aprire Microsoft Teams (avvio a freddo).
- Misurare il tempo impiegato da Microsoft Teams per caricare e catturare l'attenzione della finestra principale di Microsoft Teams.

- Passare alla finestra di chat usando i tasti di scelta rapida.
- Passare alla finestra del calendario usando i tasti di scelta rapida.
- Inviare il messaggio di chat a un utente specifico utilizzando le scorciatoie da tastiera.
- Passare alla finestra di Microsoft Teams utilizzando i tasti di scelta rapida.

**Risultati**

- Impatto sulla scalabilità del 40% con Microsoft Teams Workload (81 utenti) rispetto a Baseline (137 utenti).
- L'aumento della capacità del server di circa il 40% (in CPU) ripristina il numero di utenti come con il carico di lavoro Baseline.
- 20% di memoria extra richiesta con Microsoft Teams Workload, rispetto a Baseline.
- Aumento delle dimensioni di archiviazione per utente di 512-1024 MB.
- circa il 50% di incremento in scrittura IOPS, circa il 100% di incremento nelle letture IOPS. Microsoft Teams può avere un impatto significativo in un ambiente con archiviazione più lenta.

## Supporto delle funzionalità e versioni supportate

| Funzionalità | Microsoft Teams (versione minima) | VDA (versione minima) | App Citrix Workspace per Windows CR (versione minima) | App Citrix Workspace per Mac (versione minima) | App Citrix Workspace per Linux (versione minima) | App Citrix Workspace per ChromeOS (versione minima) |
|---|---|---|---|---|---|---|
| Audio/Video (P2P e conferenza) | versione attuale meno 90 giorni | 1906 | 1907 | 2009 | 2004 | 2105.5 |
| Condivisione dello schermo | Versione attuale meno 90 giorni | 1906 | 1907 | 2012 | 2006 | 2105.5 |
| i. Indicatore schermo Bordo rosso | Versione attuale meno 90 giorni | 1906 | 2002 | 2012 | 2006 | No |

| Funzionalità | Microsoft Teams (versione minima) | VDA (versione minima) | App Citrix Workspace per Windows CR (versione minima) | App Citrix Workspace per Mac (versione minima) | App Citrix Workspace per Linux (versione minima) | App Citrix Workspace per ChromeOS (versione minima) |
|---|---|---|---|---|---|---|
| ii. Limita l' acqui-sizione in Desktop Viewer | Versione attuale meno 90 giorni | 1906 | 2009.5 | 2012 | 2006 | No |
| iii. Multi-monitor | Versione attuale meno 90 giorni | 1912 CU6+ | 2106 (1) | 2106 | 2106 | No |
| DTMF | Versione attuale meno 90 giorni | N/A | 2102 | 2101 | 2101 | 2111.1 |
| Supporto dei server proxy | Versione attuale meno 90 giorni | N/A | 2012 (2) | 2104 (3) | 2101 (3) | 2305 |
| Condivisione di app | Versione attuale meno 90 giorni | 2109 | 2109.1 | 2203.1 | 2209 | No |
| Sottotitoli live | Versione attuale meno 90 giorni | N/A (4) | 2109.1 | 2109 | 2109 | 2303 |
| e911 dinamico | Versione attuale meno 90 giorni | N/A | 2112.1 | 2112 | 2112 | 2112 |

| Funzionalità | Microsoft Teams (versione minima) | VDA (versione minima) | App Citrix Workspace per Windows CR (versione minima) | App Citrix Workspace per Mac (versione minima) | App Citrix Workspace per Linux (versione minima) | App Citrix Workspace per ChromeOS (versione minima) |
|---|---|---|---|---|---|---|
| Concedere il controllo | Versione attuale meno 90 giorni | N/A | 2112.1 | 2203.1 | No | No |
| Richiedi il controllo | Versione attuale meno 90 giorni | N/A | 2112.1 | 2203.1 | 2203 | 2303 |
| Multifinestra | 1.5.00.11865 | 2112, 1912 CU6 (5) | 2112.1 | 2203.1 | 2203 | 2303 |
| Trascrizioni delle riunioni | Versione attuale meno 90 giorni | 2112.1, 1912 CU6+ | 2112 | 2203.1 | 2203 | 2303 |
| Sfocatura dello sfondo | Versione attuale meno 90 giorni | 2112, 1912 CU6+ | 2207 | 2301 | 2212 | 2303 |

1. Visualizzatore CD solo in modalità a schermo intero. MAIUSC+F2 non è supportato.
2. Negotiate/Kerberos, NTLM, Basic e Digest. Sono supportati anche i file Pac.
3. Solo anonimo.
4. Se il VDA è la versione 2112 o una versione superiore, Live Captions funzionerà solo se la versione dell'app Citrix Workspace è 2203.1 per MAC e 2203 Linux o 2112 per Windows. Questo perché Live Captions si comporta in modo diverso se Microsoft Teams è in modalità interfaccia utente a finestra singola o multifinestra.
5. La modalità multifinestra è stata introdotta nel VDA versione 2112, ma è stata trasferita alla versione VDA 1912 LTSR CU6.

> **Nota:**
>
> • Tutte le funzionalità elencate nell'**app Citrix Workspace per Windows 1912 CU6 (o ver-**

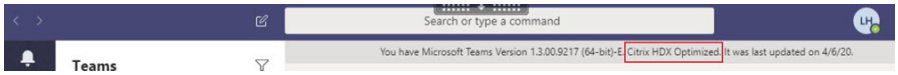
> **sione successiva)** sono applicabili all'app Citrix Workspace per Windows 2203.1 LTSR CU1.
> - Microsoft ha reso obsoleto il supporto della modalità a finestra singola in Microsoft Teams. Per garantire la conformità, è necessario aggiornare il VDA alla versione 1912 CU6+ LTSR e all'app Citrix Workspace 2303 CU2+ o superiore, che supporta la modalità multifinestra.

### Abilitare l'ottimizzazione di Microsoft Teams

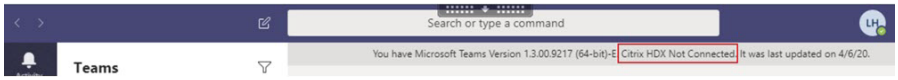
Per abilitare l'ottimizzazione per Microsoft Teams, utilizzare i criteri di gestione della console descritti nel criterio di reindirizzamento di Microsoft Teams. Questo criterio è **ON** (attivato) per impostazione predefinita. Oltre all'abilitazione di questo criterio, HDX verifica che la versione dell'app Citrix Workspace corrisponda almeno alla versione minima richiesta. Se il criterio è stato abilitato e la versione dell'app Citrix Workspace è supportata, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRe** viene impostato automaticamente su **1** sul VDA. Microsoft Teams legge la chiave per caricarsi in modalità VDI.

> **Nota:**
>
> Se si utilizzano VDA versione 1906.2 o successiva con versioni precedenti del controller (ad esempio, versione 7.15) che non dispongono del criterio disponibile in Manage console (Gestione console) (Studio), il VDA può comunque essere ottimizzato. L'ottimizzazione HDX per Microsoft Teams è abilitata per impostazione predefinita nel VDA.

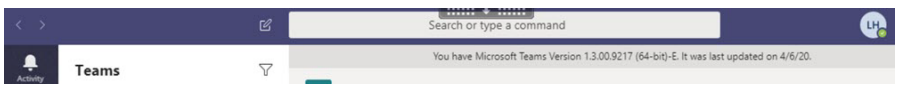
Se si fa clic su **About (Informazioni) > Version (Versione)**, viene visualizzata la legenda **Citrix HDX Optimized (Ottimizzato per Citrix HDX)**:




Se viene visualizzato il messaggio **Citrix HDX Not Connected** (Citrix HDX non connesso), l'API Citrix viene caricata in Microsoft Teams. Il caricamento dell'API è il primo passo verso il reindirizzamento. Ma c'è un errore nelle parti successive dello stack. L'errore è molto probabilmente nei servizi VDA o nell'app Citrix Workspace.




Se non viene visualizzata alcuna legenda, Microsoft Teams non è riuscito a caricare l'API Citrix. Uscire da Microsoft Teams facendo clic con il pulsante destro del mouse sull'icona dell'area di notifica e riavviare l'applicazione. Assicurarsi che il criterio Manage console (Gestisci console) non sia impostato su **Prohibited** (Non consentito) e che la versione dell'app Citrix Workspace sia supportata.



> **Importante: riconnessioni di sessione**
>
> - Potrebbe essere necessario riavviare Microsoft Teams per ottenere una sessione ottimizzata per HDX quando la connettività cambia. Ad esempio, se si sta eseguendo il roaming da un endpoint non supportato (app Workspace per iOS, Android o versioni precedenti di Windows/Linux/Mac) a uno supportato (app Workspace per Windows/Linux/Mac/ChromeOS/HTML5) o nella direzione opposta.
> - Un rilancio di Microsoft Teams è necessario anche se è stata installata l'app utilizzando il programma di installazione .exe di Microsoft Teams nel VDA. Il programma di installazione .exe è consigliato per le distribuzioni VDI persistenti. In questi casi, Microsoft Teams può aggiornarsi automaticamente mentre la sessione HDX è in stato disconnesso. Pertanto, gli utenti che si riconnettono a una sessione HDX trovano che l'esecuzione di Microsoft Teams non è ottimizzata.
> - Quando si passa da una sessione locale a una sessione HDX, si deve riavviare Microsoft Teams per l'ottimizzazione con HDX. Questa azione è necessaria in uno scenario di accesso remoto al PC.

## Requisiti di rete

Microsoft Teams si affida ai server del processore di contenuti multimediali di Microsoft 365 per riunioni o chiamate con più partecipanti. Inoltre, Microsoft Teams si basa sui relè di trasporto di Microsoft 365 per questi scenari:

- Due peer in una chiamata point-to-point non hanno connettività diretta
- Un partecipante non dispone di connettività diretta al processore multimediale.

Di conseguenza, l'integrità della rete tra il peer e il cloud di Microsoft 365 determina le prestazioni della chiamata. Per linee guida dettagliate sulla pianificazione della rete, fare riferimento all'articolo Principi di connettività di rete di Microsoft 365.

Si consiglia di valutare l'ambiente per identificare eventuali rischi e requisiti che possono influenzare la distribuzione globale di voce e video nel cloud.
Utilizzare lo strumento di valutazione della rete Skype for Business per verificare se la rete è pronta per Microsoft Teams. Per informazioni sull'assistenza, vedere Supporto.

### Riepilogo delle principali raccomandazioni di rete per il traffico RTP (Real Time Protocol)

- Connettersi alla rete di Microsoft 365 il più direttamente possibile dalla filiale.
- Pianificare e fornire una larghezza di banda sufficiente presso la filiale.
- Verificare la connettività e la qualità della rete di ogni filiale.

- Se è necessario utilizzare uno dei seguenti elementi presso la filiale, assicurarsi che il traffico RTP/UDP (gestito da HdxRtcEngine.exe nell'app Citrix Workspace) non sia ostacolato.
  - Ignorare i server proxy
  - Intercettazione SSL di rete
  - Dispositivi di ispezione profonda dei pacchetti
  - Hairpin VPN (utilizzare lo split tunneling se possibile)

> **Importante: configurazione VPN Split tunnel**
>
> Il traffico di HdxRtcEngine.exe deve essere deviato dal tunnel VPN e autorizzato a utilizzare la connessione Internet locale dell'utente per connettersi direttamente al servizio. Il modo in cui ciò viene realizzato varia a seconda del prodotto VPN e della piattaforma della macchina utilizzata, ma la maggior parte delle soluzioni VPN consente una semplice configurazione dei criteri per applicare questa logica. Per ulteriori informazioni sulla guida allo split tunnelling specifico per la piattaforma VPN, vedere questo articolo Microsoft.

Il motore multimediale WebRTC nell'app Workspace (HdxRtcEngine.exe) utilizza il protocollo SRTP (Secure Real-Time Transport Protocol) per i flussi multimediali di cui viene eseguito l'offloading nel client. SRTP assicura riservatezza e autenticazione all'RTP. Per questa funzione, vengono utilizzate le chiavi simmetriche (negoziate con DTLS) per crittografare i media e controllare i messaggi utilizzando il cifrario di crittografia AES.

Le seguenti metriche sono consigliate per un'esperienza utente positiva:

| Metrica | Endpoint a Microsoft 365 |
|---|---|
| Latenza (a senso unico) | < 50 msec |
| Latenza (RTT) | < 100 msec |
| Perdita di pacchetti | <1% durante ogni intervallo di 15 secondi |
| Jitter inter-arrivo dei pacchetti | <30 ms durante ogni intervallo di 15 secondi |

Per ulteriori informazioni, vedere Preparare la rete dell'organizzazione per Microsoft Teams.

Per quanto riguarda i requisiti di larghezza di banda, l'ottimizzazione per Microsoft Teams può utilizzare un'ampia gamma di codec per audio (OPUS/G.722/PCM G711) e video (H264).

I peer negoziano questi codec durante il processo di creazione delle chiamate utilizzando l'offerta/risposta SDP (Session Description Protocol).
Le raccomandazioni minime di Citrix per utente sono:

| Tipo | Larghezza di banda | Codec |
|---|---|---|
| Audio (tutte le direzioni) | ~ 90 kbps | G.722 |
| Audio (tutte le direzioni) | ~ 60 kbps | Opus* |
| Video (tutte le direzioni) | ~ 700 kbps | H264 360p @ 30 fps 16:9 |
| Condivisione dello schermo | ~ 300 kbps | H264 1080p @ 15 fps |

* Opus supporta la codifica dei bitrate costante e variabile da 6 kbps fino a 510 kbps.

Opus e H264 sono i codec preferiti per le chiamate peer-to-peer e in conferenza.

> **Importante:**
>
> Per quanto riguarda le prestazioni, la codifica è più costosa della decodifica per l'uso della CPU sul computer client. È possibile codificare la massima risoluzione di codifica nell'app Citrix Workspace per Linux e Windows. Vedere Stima delle prestazioni dell'encoder e Ottimizzazione per Microsoft Teams.

### Server proxy

A seconda della posizione del proxy, considerare quanto segue:

- Configurazione proxy sul VDA:

  Se si configura un server proxy esplicito nel VDA e si instradano le connessioni all'host locale tramite un proxy, il reindirizzamento non riesce. Per configurare correttamente il proxy, è necessario selezionare l'impostazione **Bypass proxy servers for local address** (Ignora i server proxy per l'indirizzo locale) in **Opzioni Internet > Connessioni > Impostazioni LAN > Server proxy** e ignorare `127.0.0.1:9002`.

  Se si utilizza un file PAC, lo script di configurazione del proxy VDA del file PAC deve restituire **DIRECT** per `wss://127.0.0.1:9002`. In caso contrario, l'ottimizzazione non riesce. Per assicurarsi che lo script restituisca **DIRECT**, utilizzare `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Configurazione proxy sull'app Citrix Workspace:

  Se la filiale è configurata per accedere a Internet tramite un proxy, queste versioni supportano i server proxy:

  - App Citrix Workspace per Windows versione 2012 (Negotiate/Kerberos, NTLM, Basic e Digest; sono supportati anche i file `Pac`)

- App Citrix Workspace per Windows versione 1912 CU5 (Negotiate/Kerberos, NTLM, Basic e Digest. Sono supportati anche i file Pac)
- App Citrix Workspace per Linux versione 2101 (autenticazione anonima)
- App Citrix Workspace per Mac versione 2104 (autenticazione anonima)

I dispositivi client con versioni precedenti dell'app Citrix Workspace non possono leggere le configurazioni proxy. Questi dispositivi inviano il traffico direttamente ai server TURN di Microsoft 365.

> **Importante:**
>
> - Verificare che il dispositivo client possa connettersi al server DNS per effettuare le risoluzioni DNS. Un dispositivo client deve essere in grado di risolvere i seguenti FQDN del server Microsoft Teams Relay:
>
>   - worldaz.relay.teams.microsoft.com
>   - inaz.relay.teams.microsoft.com
>   - uaeaz.relay.teams.microsoft.com
>   - euaz.relay.teams.microsoft.com
>   - usaz.relay.teams.microsoft.com
>   - turn.dod.teams.microsoft.us
>   - turn.gov.teams.microsoft.us
>
> Se le richieste DNS non hanno esito positivo, le chiamate P2P con utenti esterni e la creazione di supporti per le teleconferenze con la creazione di media non riescono.
>
> - La posizione del server della conferenza viene selezionata in base alla posizione del desktop virtuale (non al client) del primo partecipante.

### Percorsi per l'avvio di chiamate e il flusso di contenuti multimediali

Quando possibile, il motore multimediale HDX WebRTC nell'app Citrix Workspace (HdxRtcEngine.exe) tenta di stabilire una connessione SRTP (Secure Real-Time Transport Protocol) di rete diretta tramite UDP (User Datagram Protocol) in una chiamata peer-to-peer. Se le porte UDP alte sono bloccate, il motore multimediale torna a TCP/TLS 443.

Il motore multimediale HDX supporta ICE, STUN (Session Traversal Utilities for NAT) e TURN (Traversal Using Relays around NAT) per individuare candidati e stabilire connessioni. Questo supporto significa che l'endpoint deve essere in grado di eseguire risoluzioni DNS.

Si consideri uno scenario in cui non esiste un percorso diretto tra i due peer o tra un peer e un server di conferenza e si sta partecipando a una chiamata o a una riunione con più parti. HdxRtcEngine.exe utilizza un relé server di trasporto Microsoft Teams in Microsoft 365 per raggiungere l'altro peer o il processore multimediale, dove sono ospitate le riunioni. Il computer client deve avere accesso a tre intervalli di indirizzi IP di subnet di Microsoft 365 e quattro porte UDP (o TCP/TLS 443 come fallback se

UDP è bloccato). Per ulteriori informazioni, vedere il diagramma Architettura in Configurazione delle chiamate e URL di Office 365 e intervalli di indirizzi IP ID 11.

| ID | Categoria | Indirizzi | Porte di destinazione |
|---|---|---|---|
| 11 | Ottimizzazione richiesta | 13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14 | **UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (fallback) |

Questi intervalli includono sia i relè di trasporto che i processori multimediali, con un sistema di bilanciamento del carico di Azure come front-end.
I relè di trasporto di Microsoft Teams forniscono funzionalità STUN e TURN, ma non sono endpoint ICE. Inoltre, i relè di trasporto di Microsoft Teams non interrompono gli elementi multimediali o TLS e non eseguono alcuna transcodificazione. Possono collegare TCP (se HdxRtcEngine.exe utilizza TCP) a UDP quando inoltrano il traffico ad altri peer o processori multimediali.

Il motore multimediale WebRTC dell'app Workspace contatta il relè di trasporto di Microsoft Teams più vicino nel cloud di Microsoft 365. Il motore multimediale utilizza IP anycast e le porte UDP 3478-3481 (porte UDP diverse per carico di lavoro, anche se può verificarsi il multiplexing) o 443 TCP/TLS per i fallback. La qualità delle chiamate dipende dal protocollo di rete sottostante. Poiché UDP è sempre consigliato su TCP, si consiglia di progettare le reti in modo da supportare il traffico UDP nella filiale.

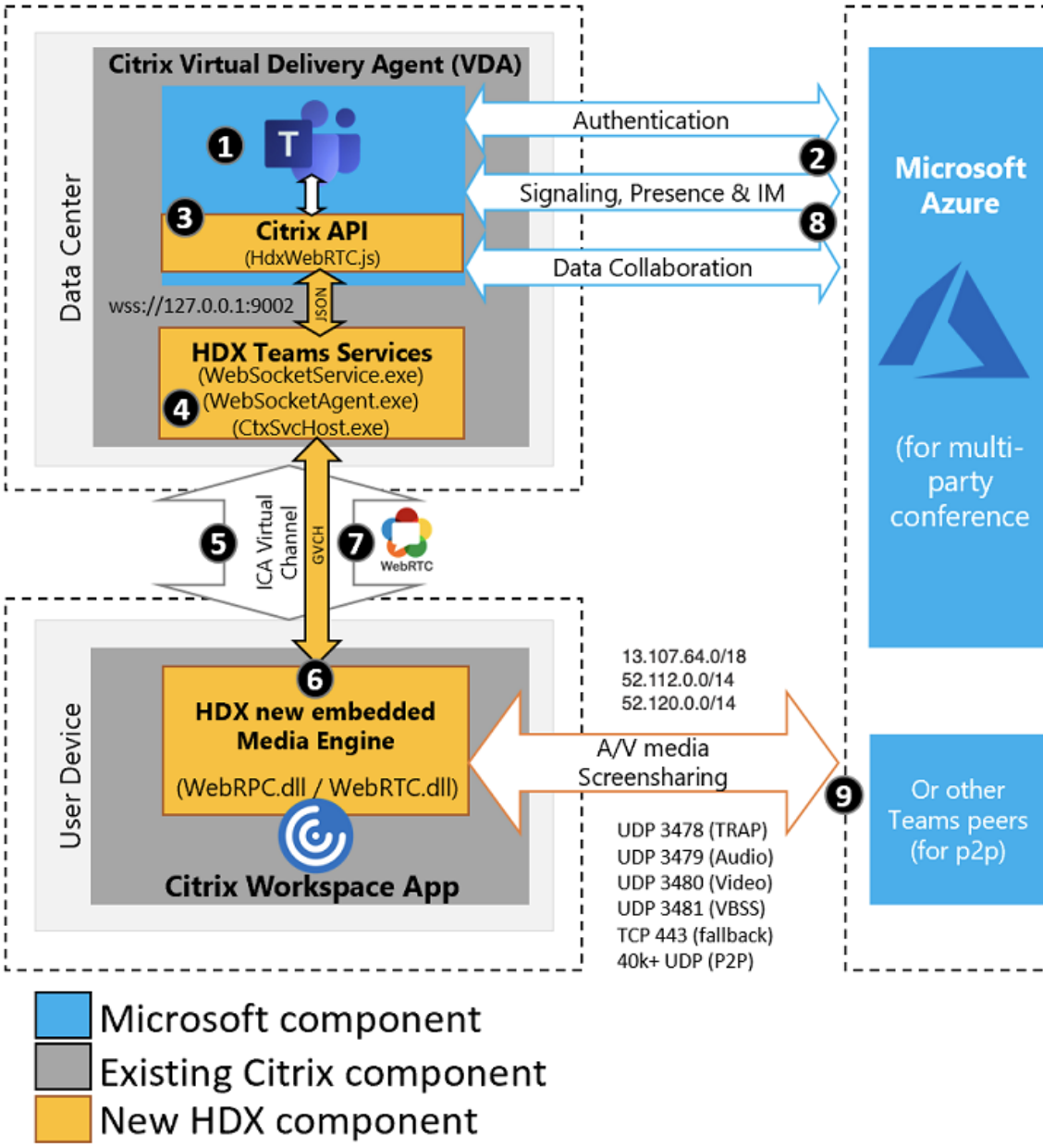
Se Microsoft Teams è stato caricato in modalità ottimizzata e HdxRtcEngine.exe è in esecuzione sull'endpoint, gli errori ICE potrebbero causare un errore di configurazione delle chiamate o audio/video monodirezionale. Quando una chiamata non può essere completata o i flussi multimediali non sono full duplex, controllare prima la **traccia Wireshark** sull'endpoint. Per ulteriori informazioni sul processo di raccolta dei candidati ICE, vedere "Raccolta dei log"nella sezione Supporto.

> **Nota:**
>
> Se gli endpoint non hanno accesso a Internet, potrebbe comunque essere possibile per gli utenti effettuare una chiamata peer-to-peer se si trovano entrambi sulla stessa LAN. Non è possibile tenere riunioni. In questo caso, c'è un timeout di 30 secondi prima dell'inizio della configurazione della chiamata.

#### Configurazione delle chiamate

Utilizzare questo diagramma di architettura come riferimento visivo per la sequenza del flusso di chiamata. I passaggi corrispondenti sono indicati nel diagramma.




**Architettura**

1. Avviare Microsoft Teams.
2. Microsoft Teams si autentica in O365. I criteri tenant vengono spostati al client Microsoft Teams e le informazioni pertinenti relative a TURN e al canale di segnalazione vengono inoltrate all'app.
3. Microsoft Teams rileva che è in esecuzione in un VDA ed effettua chiamate API all'API JavaScript Citrix.
4. Il JavaScript Citrix in Microsoft Teams apre una connessione WebSocket sicura a WebSocketService.exe in esecuzione sul VDA, che genera WebSocketAgent.exe all'interno della sessione utente.

5. WebSocketAgent.exe crea un'istanza di un canale virtuale generico chiamando il servizio di reindirizzamento di Microsoft Teams Citrix HDX (CtxSvcHost.exe).
6. wfica32.exe (motore HDX) dell'app Citrix Workspace genera un nuovo processo chiamato HdxRtcEngine.exe, che è il nuovo motore WebRTC utilizzato per l'ottimizzazione di Microsoft Teams.
7. Il motore multimediale Citrix e Teams.exe hanno un percorso di canale virtuale a 2 vie e possono iniziare a elaborare le richieste multimediali.

   ——Chiamate dell'utente——

8. Il **peer A** fa clic sul pulsante di **chiamata**. Teams.exe comunica con i servizi Microsoft Teams in Microsoft 365 stabilendo un percorso di segnalazione end-to-end con il **peer B**. Microsoft Teams chiede a HdxRtcEngine una serie di parametri di chiamata supportati (codec, risoluzioni e così via, questo è noto come offerta SDP [Session Description Protocol]). Questi parametri di chiamata vengono quindi inoltrati utilizzando il percorso di segnalazione ai servizi Microsoft Teams in Microsoft 365 e da lì all'altro peer.
9. L'offerta/risposta SDP (negoziazione a passaggio singolo) avviene attraverso il canale di segnalazione e vengono completati i controlli di connettività ICE (attraversamenti NAT e firewall utilizzando le richieste di associazione STUN). Quindi, i contenuti multimediali SRTP (Secure Real-time Transport Protocol) vanno direttamente da HdxRtcEngine.exe all'altro peer e viceversa (o i Conference Server Microsoft 365 se si tratta di una riunione).

### Microsoft Phone System

Phone System è la tecnologia Microsoft che consente il controllo delle chiamate e PBX nel cloud di Microsoft 365 con Microsoft Teams. L'ottimizzazione per Microsoft Teams supporta Phone System, utilizzando i piani di chiamata di Microsoft 365 o il routing diretto. Con il routing diretto è possibile connettere il session border controller supportato da Microsoft Phone System direttamente senza alcun software locale aggiuntivo.
Sono supportati code di chiamata, trasferimento, inoltro, messa in pausa, disattivazione dell'audio e ripresa di una chiamata.

#### DTMF

La funzione DTMF (Dual Tone Multi Frequency) è supportata con queste versioni dell'app Citrix Workspace (e versioni successive):

- App Citrix Workspace per Windows versione 2102
- App Citrix Workspace per Windows LTSR 1912 CU5 (solo sistema operativo Windows 10)
- App Citrix Workspace per Linux versione 2101
- App Citrix Workspace per Mac versione 2101

- App Citrix Workspace per ChromeOS versione 2111.1

#### Supporto di e911 dinamico

A partire dalla versione 2112, l'app Citrix Workspace supporta le chiamate di emergenza dinamiche. Se utilizzato in Microsoft Calling Plans, Operator Connect e Direct Routing, consente di eseguire le seguenti operazioni:

- Configurare e indirizzare le chiamate di emergenza.
- Informare il personale di sicurezza.

La notifica viene fornita in base alla posizione corrente dell'app Citrix Workspace in esecuzione sull'endpoint, anziché sul client Microsoft Teams in esecuzione sul VDA.

La legge di Ray Baum richiede che la posizione inviabile di chi chiama il 911 sia trasmessa al Public Safety Answering Point (PSAP) appropriato. L'ottimizzazione di Microsoft Teams con HDX è conforme alla legge di Ray Baum se utilizzata con le seguenti versioni dell'app Citrix Workspace:

- App Citrix Workspace per Windows versione 2112.1 e successiva
- App Citrix Workspace per Linux versione 2112 e successiva
- App Citrix Workspace per Mac versione 2112 e successiva
- App Citrix Workspace per ChromeOS versione 2112 e successiva

Per abilitare le chiamate di emergenza dinamiche, l'amministratore deve utilizzare l'interfaccia di amministrazione di Microsoft Teams e configurare quanto segue per creare una mappa della posizione di rete o di emergenza:

- Impostazioni di rete
- Servizio informazioni sulla posizione (LIS)

Per ulteriori informazioni sulle chiamate di emergenza dinamiche, vedere la documentazione di Microsoft.

Le informazioni sulla posizione inviabili che l'app Citrix Workspace inoltra a Microsoft Teams sono:

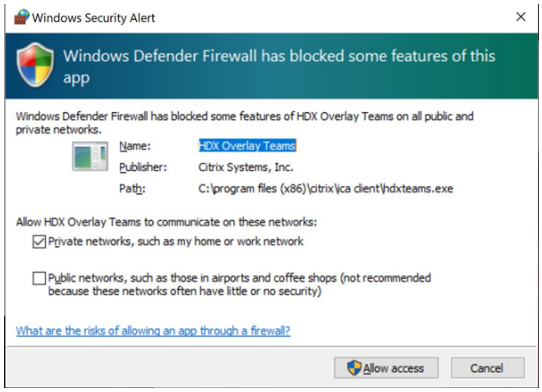
- ID chassis/ID porta utilizzando il Link Layer Discovery Protocol (LLDP) per le connessioni Ethernet/Switch. Ethernet/Switch (LLDP) è supportato su:
  - Versioni Windows 8.1 e 10
  - macOS, che richiede il software di abilitazione LLDP. Per scaricare il software di abilitazione LLDP, passare a `www.microsoft.com` e cercare il software di abilitazione LLDP.
  - Linux, che richiede che la libreria LLDP sia inclusa nella distribuzione del sistema operativo (OS) del Thin Client.

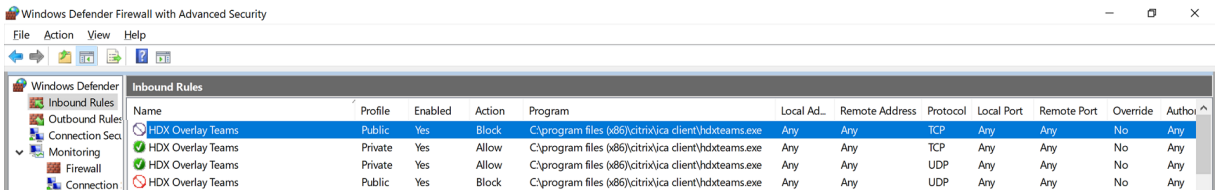
- WLAN BBSID e {IPv4-IPv6; Subnet; MAC Address} dell'endpoint in cui è installata l'app Citrix Workspace.
  - Le posizioni basate su subnet e WiFi sono supportate nell'app Workspace per Windows, Linux e Mac.
- Latitude e Longitude, se l'autorizzazione dell'utente è concessa a livello di sistema operativo in cui è installata l'app Citrix Workspace (l'autorizzazione è impostata su HDX RTC Engine)
  - Funzionalità supportata su tutte le piattaforme app Workspace. Tuttavia, in Citrix Workspace for Linux, è necessario includere la libreria `libgps` nella distribuzione del sistema operativo del Thin Client (>sudo apt-get install libgps23 gpsd lldpd).

### Considerazioni sul firewall

Quando gli utenti avviano una chiamata ottimizzata utilizzando il client Microsoft Teams per la prima volta, potrebbero notare un avviso nelle impostazioni del **firewall di Windows**. L'avviso richiede agli utenti di consentire la comunicazione per HdxTeams.exe o HdxRtcEngine.exe (HDX Overlay Microsoft Teams).




Le quattro voci seguenti vengono aggiunte in **Regole in entrata** nella console **Windows Defender Firewall > Sicurezza avanzata**. Se si desidera, è possibile applicare regole più restrittive.




### Coesistenza di Microsoft Teams e Skype for Business

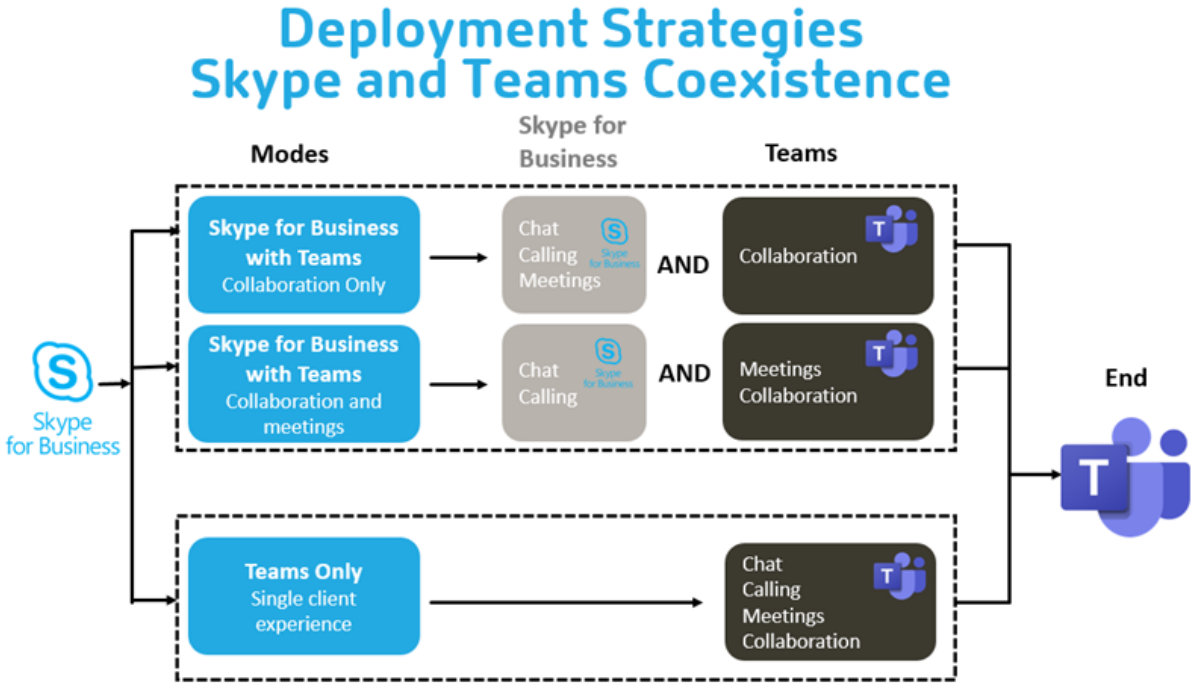
È possibile distribuire Microsoft Teams e Skype for Business fianco a fianco, come due soluzioni separate con funzionalità sovrapposte.

Per ulteriori informazioni, vedere Comprendere la coesistenza e l'interoperabilità di Microsoft Teams e Skype for Business.

Citrix RealTime Optimization Pack e l'ottimizzazione HDX per i motori multimediali di Microsoft Teams rispettano quindi la configurazione impostata nell'ambiente. Gli esempi includono le modalità isola e Skype for Business con la collaborazione in Microsoft Teams. Inoltre, Skype for Business con la collaborazione e le riunioni di Microsoft Teams.

L'accesso alle periferiche può essere concesso solo a una singola applicazione alla volta. Ad esempio, l'accesso alla webcam da parte di RealTime Media Engine durante una chiamata blocca il dispositivo di imaging durante una chiamata. Quando il dispositivo viene rilasciato, diventa disponibile per Microsoft Teams.




### Citrix SD-WAN: connettività di rete ottimizzata per Microsoft Teams

La qualità audio e video ottimale richiede una connessione di rete al cloud di Microsoft 365 con bassa latenza, basso jitter e bassa perdita di pacchetti. Il backhauling del traffico RTP audio-video di Microsoft Teams dagli utenti dell'app Citrix Workspace nelle sedi delle filiali a un centro dati prima del passaggio a Internet può aggiungere latenza eccessiva. Potrebbe anche causare congestione sui collegamenti WAN. Citrix SD-WAN ottimizza la connettività per Microsoft Teams seguendo i principi di connettività di rete di Microsoft 365. Citrix SD-WAN utilizza l'indirizzo IP e il servizio web di Microsoft 365 basati su Microsoft REST e il DNS di prossimità. Tutto questo serve a identificare, classificare e indirizzare il traffico di Microsoft Teams.

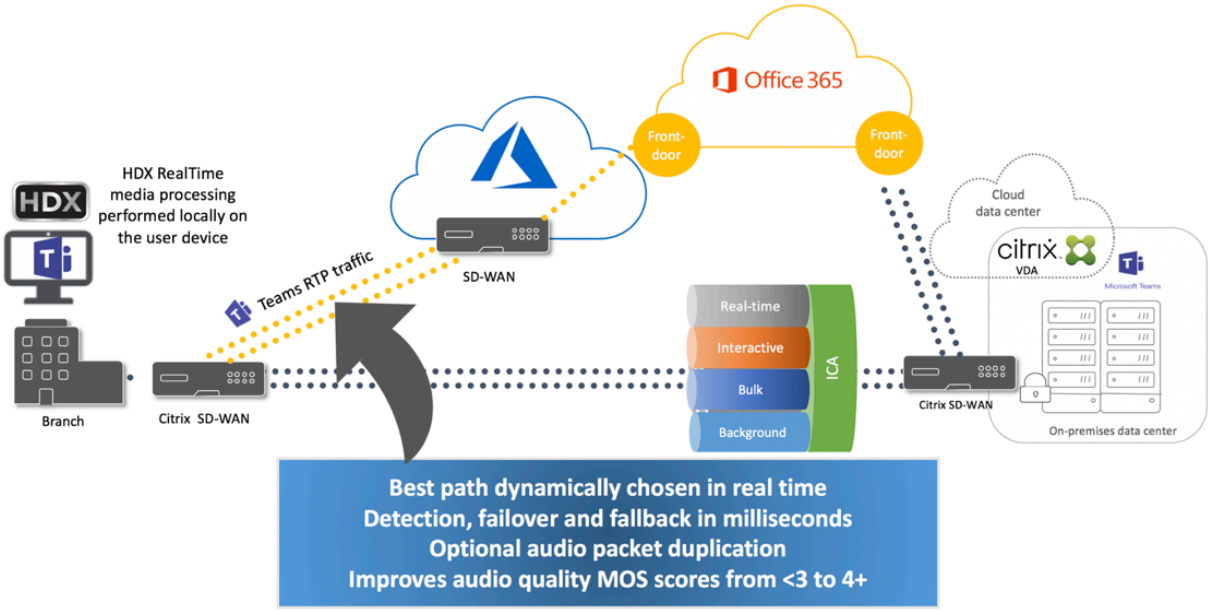
 

Le connessioni a Internet aziendali a banda larga in molte zone soffrono di perdite intermittenti di pacchetti, periodi di jitter eccessivo e interruzioni.

Citrix SD-WAN offre due soluzioni per preservare la qualità audio-video di Microsoft Teams quando lo stato della rete è variabile o degradato.

- Se si utilizza Microsoft Azure, un'appliance virtuale Citrix SD-WAN (VPX) distribuita nella rete virtuale di Azure fornisce ottimizzazioni di connettività avanzate. Queste ottimizzazioni includono il failover dei collegamenti senza soluzione di continuità e il racing dei pacchetti audio.
- I clienti Citrix SD-WAN possono connettersi a Microsoft 365 tramite il servizio Citrix Cloud Direct. Questo servizio offre una consegna affidabile e sicura per tutto il traffico collegato a Internet.

Se la qualità della connessione internet della filiale non è un problema, potrebbe essere sufficiente per ridurre al minimo la latenza. Indirizzare il traffico di Microsoft Teams direttamente dall'appliance della filiale Citrix SD-WAN alla porta principale di Microsoft 365 più vicina per ridurre al minimo la latenza. Per ulteriori informazioni, vedere Ottimizzazione di Citrix SD-WAN Office 365.




### Riunioni e chat con più finestre

È possibile utilizzare più finestre di riunione o chat per Microsoft Teams in Windows. Per informazioni dettagliate sulla funzionalità pop-out, vedere You can use multiple meetings or chat windows for Microsoft Teams in Windows sul sito di Microsoft 365.

> **Nota:**
>
> Questa funzione è supportata con l'app Citrix Workspace per Windows 2112.1, Mac 2203, Linux 2203, ChromeOS 2303. Richiede VDA 2112 o versioni successive ed è stato trasferito su 1912 CU6+

> LTSR.

### Sfocatura dello sfondo ed effetti di sfondo

L'app Citrix Workspace per Windows, Mac, Linux e ChromeOS/HTML5 supporta la sfocatura dello sfondo e gli effetti per gli effetti di sfondo presenti nell'ottimizzazione di Microsoft Teams con HDX.

È possibile sfocare lo sfondo o sostituirlo con un'immagine predefinita ed evitare distrazioni impreviste aiutando la conversazione a rimanere concentrata sulla silhouette (corpo e viso). È possibile utilizzare questa funzionalità con chiamate P2P o in conferenza.

> **Nota:**
>
> Questa funzionalità è integrata con i pulsanti dell'interfaccia utente di Microsoft Teams. Il supporto MultiWindow è un prerequisito che richiede un aggiornamento del VDA alla versione 2112 o a una versione successiva. Per ulteriori informazioni, vedere Riunioni e chat con più finestre.

I controlli dell'interfaccia utente di Microsoft Teams sulla sfocatura e gli effetti dello sfondo richiedono le seguenti versioni minime:

- App Citrix Workspace per Windows 2207
- App Citrix Workspace per Mac 2301
- App Citrix Workspace per Linux versione 2212
- App Citrix Workspace per ChromeOS 2303

**Limitazioni:**

- Il client deve essere connesso a Internet mentre si sostituisce l'immagine di sfondo con un'immagine predefinita di Microsoft Teams.
- La sostituzione dell'immagine di sfondo definita dall'amministratore e dall'utente non è supportata nell'interfaccia utente di Microsoft Teams. Le immagini di sfondo personalizzate possono essere configurate utilizzando le impostazioni del client, se anche l'immagine è memorizzata sul client.

#### Impostare un'immagine di sfondo personalizzata

Le seguenti chiavi di registro sono necessarie solo se non si prevede di utilizzare l'interfaccia utente di Microsoft Teams per controllare la funzionalità o se un amministratore desidera ignorare i comportamenti predefiniti. Ad esempio, è possibile disabilitare la sfocatura dello sfondo quando l'endpoint non è abbastanza potente.

**In Windows** Per impostare un'immagine di sfondo personalizzata, gli amministratori o gli utenti finali devono configurare la seguente chiave del Registro di sistema sul client o sull'endpoint:

Posizione:`HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nome: VideoBackgroundEffect
- Tipo: DWORD
- Valore: 0 (disabilitato), 1 (abilitato), 2 (sostituzione immagine di sfondo)

Il valore impostato su 1 sfoca lo sfondo. Questo valore può essere impostato dall'utente finale o dall'amministratore.

Il valore impostato su 2 richiede anche la presenza della chiave **VideoBackgroundImage**. Solo l'amministratore può impostare questo valore. La chiave seguente è necessaria solo se si desidera sostituire l'immagine di sfondo e non per la sfocatura:

- Nome: VideoBackgroundImage
- Tipo: REG_SZ
- Valore: my_image_name.jpeg

L'immagine di sfondo video deve essere presente nella directory `C:\Program Files (x86)\Citrix\ICA Client`.

Questa configurazione del Registro di sistema può essere utilizzata anche per abilitare la sfocatura dello sfondo o la sostituzione dell'immagine nell'app Citrix Workspace 2206 senza il selettore dell'interfaccia utente di Microsoft Teams. In altre parole, se l'ambiente o il VDA non supporta più finestre, è comunque possibile applicare la soluzione alternativa del registro HKCU con l'app Citrix Workspace 2206 o superiore per ottenere un risultato simile, sebbene l'utente non possa controllare la funzionalità durante la sessione HDX o della chiamata di Microsoft Teams.

Le modifiche delle chiavi di registro hanno effetto solo quando la sessione HDX si connette.

**Su Mac** Posizione dell'immagine scaricata dall'utente: */Users/username/Downloads/any_image.png*

Eseguire i seguenti comandi per impostare l'immagine personalizzata come immagine predefinita:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2

defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "
/Users/username/Downloads/any_image.png"
```

**Su Linux** Posizione dell'immagine scaricata dall'utente: */home/username/Downloads/any_image.jpg*

Creare il file */var/.config/citrix/hdx_rtc_engine/config.json* e aggiungere le seguenti chiavi di configurazione in formato JSON. Ad esempio,

```
{


"VideoBackgroundEffect":2,

"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"

 }
```

**Su HTML5**

1. Accedere al file **configuration.js** nella cartella **HTML5Client**.
2. Aggiungere l'attributo **backgroundEffects** e impostare l'attributo su **true**. Ad esempio,

```
'features' : {

    'msTeamsOptimization' :
    {

        'backgroundEffects' : true
     }

 }

<!--NeedCopy-->
```

3. Salvare le modifiche.

**Considerazioni sul consumo di CPU client**

Sebbene la funzionalità di sfocatura non sfrutti eccessivamente la CPU, ci si può aspettare un aumento dei consumi. Ad esempio, su un thin client con chip Intel® Pentium® Silver 4 Core da 1,5 GHz con TurboBoost fino a 2,8 GHz, la sfocatura dello sfondo aggiunge circa il 2% all'utilizzo della CPU. L'utilizzo medio della CPU è inferiore al 20%.

## Visualizzazione Raccolta e altoparlanti attivi in Microsoft Teams

Microsoft Teams supporta i layout **Gallery** (Galleria), **Large gallery** (Galleria ampia) e la **modalità Together** (Insieme).

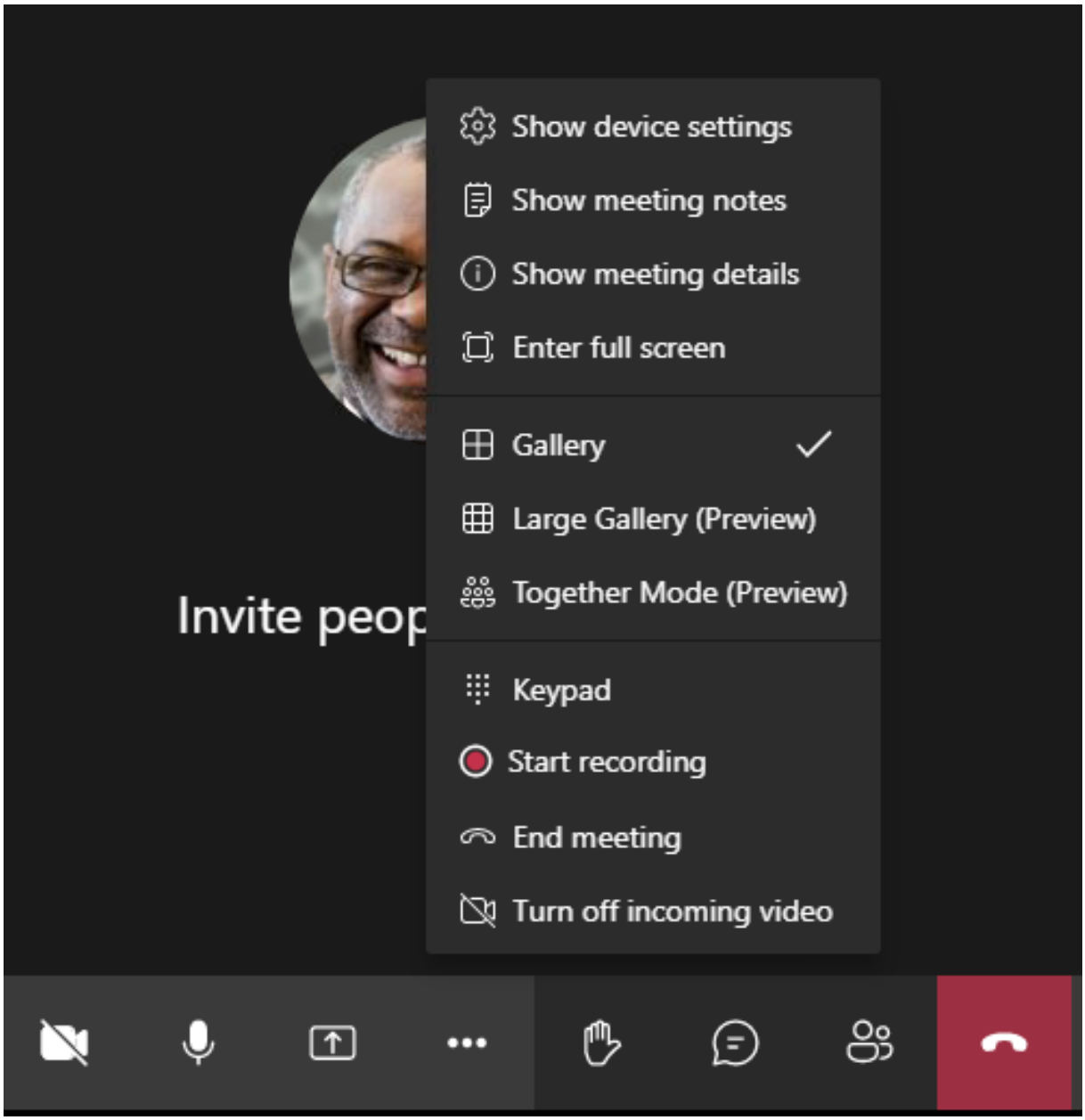
Microsoft Teams visualizza una griglia 2x2 con flussi video di quattro partecipanti (nota come **Gallery** [Galleria]). In questo caso, Microsoft Teams invia quattro flussi video al dispositivo client per la decodifica. Quando più di quattro partecipanti condividono un video, sullo schermo appaiono solo gli ultimi quattro partecipanti che hanno parlato di più.

Microsoft Teams fornisce inoltre un'ampia vista galleria con una griglia fino a 7x7. Di conseguenza, il Conference Server di Microsoft Teams combina un singolo feed video e lo invia al dispositivo client per la decodifica, con conseguente riduzione del consumo della CPU. Questo feed singolo in stile matrice potrebbe includere anche il video con anteprima automatica degli utenti.

Infine, Microsoft Teams supporta la **modalità Together** (Insieme), che fa parte della nuova esperienza di riunione. Utilizzando la tecnologia di segmentazione IA per posizionare digitalmente i partecipanti in un background condiviso, Microsoft Teams mette tutti i partecipanti nello stesso auditorium.

L'utente può controllare queste modalità durante una chiamata in conferenza selezionando i layout **Gallery** (Galleria), **Large gallery** (Galleria ampia) o la **modalità Together** (Insieme) nel menu con i tre puntini.



Supporto delle limitazioni delle proporzioni video (app Citrix Workspace per Windows 2102, app Citrix Workspace per Linux 2106, app Citrix Workspace per MAC 2106 e versioni successive):

- L'opzione **Fill to frame** (Riempi inquadratura) è disponibile nelle viste Gallery (Galleria)/Large Gallery (Galleria ampia). Questa opzione ritaglia le dimensioni del video per adattarlo alla sottofinestra. **Fit to frame** (Adatta all'inquadratura), invece, visualizza barre nere (formato 16:9) sui lati del video in modo che non ci siano ritagli.

La tabella seguente fornisce un confronto tra i layout Gallery (Galleria) e Large gallery (Galleria ampia):

| | Vista Gallery (Galleria) 2x2 (impostazione predefinita) | Vista Large Gallery (Galleria ampia) |
|---|---|---|
| Layout/Griglia | Visualizza una griglia 2x2 con flussi video di quattro partecipanti. Sullo schermo vengono visualizzati solo gli ultimi quattro altoparlanti più attivi e gli altri partecipanti non appaiono sulla griglia. | Visualizza una griglia 7x7 con flussi video di 49 partecipanti. |
| Tecnica di mixing | Un router multimediale inoltra i singoli flussi di ciascun partecipante a ogni utente. | Un server centrale per conferenze mixa e transcodifica tutto l'audio o il video per creare un layout composito su misura per ogni partecipante. Questa azione introduce una certa latenza aggiuntiva. |
| Altoparlante attivo | Il nuovo altoparlante attivo sostituisce l'altoparlante meno attivo nella griglia. | Visualizza tutti i partecipanti indipendentemente dal fatto che siano attivi o inattivi. |
| Codifica in corrispondenza dell'endpoint | Sull'endpoint potrebbero essere codificati uno o più flussi video se Simulcast è abilitato. Per ulteriori informazioni sul supporto di Simulcast, vedere Simulcast. | Sull'endpoint potrebbero essere codificati uno o più flussi video se Simulcast è abilitato. Per ulteriori informazioni sul supporto di Simulcast, vedere Simulcast. |

| | Vista Gallery (Galleria) 2x2 (impostazione predefinita) | Vista Large Gallery (Galleria ampia) |
|---|---|---|
| Decodifica in corrispondenza dell'endpoint | Ogni partecipante riceve fino a quattro flussi multimediali individuali. Ciò aumenta il consumo di CPU nell'endpoint di HdxRtcEngine.exe (per decodifica/rendering). | Ogni partecipante riceve un solo flusso per audio e video. Questa impostazione riduce il consumo di CPU nell'endpoint. |
| Risoluzione massima | 720p. Quando quattro partecipanti condividono video, la risoluzione massima è di 360p per feed video. Se meno di quattro partecipanti condividono video, la risoluzione per feed video potrebbe essere più alta. | 720p per il layout composito o il mixaggio. Non è necessario un flusso video di alta qualità per partecipante in un layout composito. A causa di questa condizione, ogni mittente riduce la risoluzione o la velocità in bit di caricamento. |
| Problema di "utente lento" | Il mittente modifica la qualità di ciascuna modalità (audio/video/condivisione dello schermo) sulla qualità di rete più bassa comune tra i partecipanti. Questo flusso multimediale viene quindi inoltrato a tutti gli altri partecipanti. Di conseguenza, un partecipante con cattive condizioni di rete influisce sulla qualità di tutti gli altri partecipanti alla chiamata. | Meno suscettibile allo scenario di qualità della rete più bassa comune. Il server per conferenze offre qualità diverse in base alle condizioni di rete dei singoli partecipanti. |
| Anteprima automatica | L'utente viene visualizzato in una piccola miniatura in tempo reale. | L'utente viene visualizzato in una miniatura e mescolato con il resto dei feed video. Di conseguenza, l'utente potrebbe vedersi incluso nel layout del video principale con un ritardo aggiuntivo. |

### Condivisione dello schermo in Microsoft Teams

Microsoft Teams si basa sulla condivisione dello schermo basata su video (VBSS), codificando essenzialmente il desktop condiviso con codec video come H264 e creando un flusso ad alta definizione. Con l'ottimizzazione HDX, la condivisione dello schermo in entrata viene considerata come un flusso video.

A partire dall'app Citrix Workspace 2109 o versione successiva per Windows, Linux, Mac e dall'app Citrix Workspace 2303 per ChromeOS, gli utenti possono condividere gli schermi e la videocamera contemporaneamente.

Con le versioni precedenti, se ci si trova nel mezzo di una videochiamata e l'altro peer inizia a condividere il desktop, il feed video della videocamera originale viene sospeso. Viene invece visualizzato il feed video per la condivisione dello schermo. Il peer deve quindi riprendere manualmente la condivisione della videocamera.

> **Nota per PowerPoint Live**
>
> Questa limitazione non esiste se si condividono contenuti da PowerPoint Live. In tal caso, gli altri colleghi possono ancora vedere la webcam e i contenuti e navigare avanti e indietro per esaminare altre diapositive. In questo scenario, le diapositive vengono renderizzate sul VDA. Per accedere a una presentazione PowerPoint Live, fare clic sul pulsante del pannello di condivisione e selezionare una delle diapositive di PowerPoint suggerite, oppure fare clic su "Sfoglia"e trovare un file PowerPoint sul proprio computer o in OneDrive.

Anche la condivisione dello schermo in uscita è ottimizzata e assegnata all'app Citrix Workspace. In questo caso, il motore multimediale acquisisce e trasmette solo la finestra Citrix Desktop Viewer (CDViewer.exe), con un bordo rosso disegnato all'intorno. Qualsiasi applicazione locale che si sovrappone a Desktop Viewer non viene acquisita.

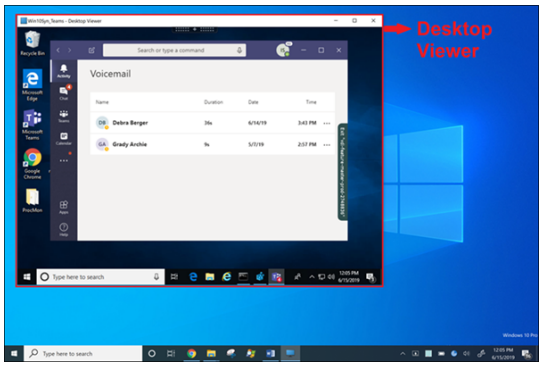
> **Nota**
>
> Impostare autorizzazioni specifiche nell'app Citrix Workspace per Mac per abilitare la condivisione dello schermo. Per ulteriori informazioni, vedere Requisiti di sistema.

**Limitazione nota:**

- Se Desktop Viewer è disabilitato o se viene utilizzato Desktop Lock, la selezione multimonitor non è disponibile nel selettore dello schermo di Microsoft Teams. Desktop Viewer potrebbe essere disabilitato modificando il modello di file `.ICA` o `StoreFront web.config`. Il tasto di scelta rapida MAIUSC+F2 non è compatibile con la condivisione dello schermo multimonitor.
- Nelle versioni dell'app Workspace precedenti alla 2106, viene condiviso solo il monitor principale. Trascinare l'applicazione nel desktop virtuale sul monitor principale in modo che l'altro peer nella chiamata la veda.

- La condivisione dello schermo multimonitor potrebbe non funzionare se si configura l'app Citrix Workspace con la funzionalità di layout del monitor virtuale (partizione logica di un singolo monitor fisico). In questo caso, tutti i monitor virtuali vengono condivisi come immagine composita.
- Le versioni precedenti dell'app Citrix Workspace per Windows (dalla 1907 alla 2008) condividono anche un'applicazione locale che viene eseguita nel computer client. Questa condivisione è possibile solo se l'app locale è stata sovrapposta a Desktop Viewer. Questo comportamento è stato rimosso nella versione 2009.6 o superiore e nella versione 1912 CU5 o superiore.
- Durante la condivisione dello schermo, se si passa dalla modalità finestra alla modalità a schermo intero, la condivisione dello schermo si interrompe. È necessario interrompere e condividere di nuovo affinché la condivisione dello schermo funzioni.
- Non è possibile aggiungere i controlli di condivisione a una posizione specifica in Microsoft Teams ottimizzato.




**Condivisione dello schermo da un'applicazione senza soluzione di continuità:**

Se si pubblica Microsoft Teams come applicazione autonoma senza soluzione di continuità, la condivisione dello schermo acquisisce il desktop locale dell'endpoint fisico. La versione minima dell'app Citrix Workspace deve essere 1909.

### Condivisione di app

A partire dall'app Citrix Workspace per Windows 2112.1 e dal VDA 2112, Microsoft Teams supporta la condivisione delle app.

A partire dall'app Citrix Workspace per Windows 2109, Mac 2203, Linux 2209 e VDA 2109, Microsoft Teams supporta la condivisione sullo schermo di app specifiche in esecuzione nella sessione virtuale. È anche possibile condividere applicazioni interne personalizzate, come Java, utilizzando Microsoft Teams ottimizzato. Per condividere un'app specifica:

1. Accedere all'app Microsoft Teams nella sessione remota.
2. Fare clic su **Condividi contenuto** nell'interfaccia utente di Microsoft Teams.

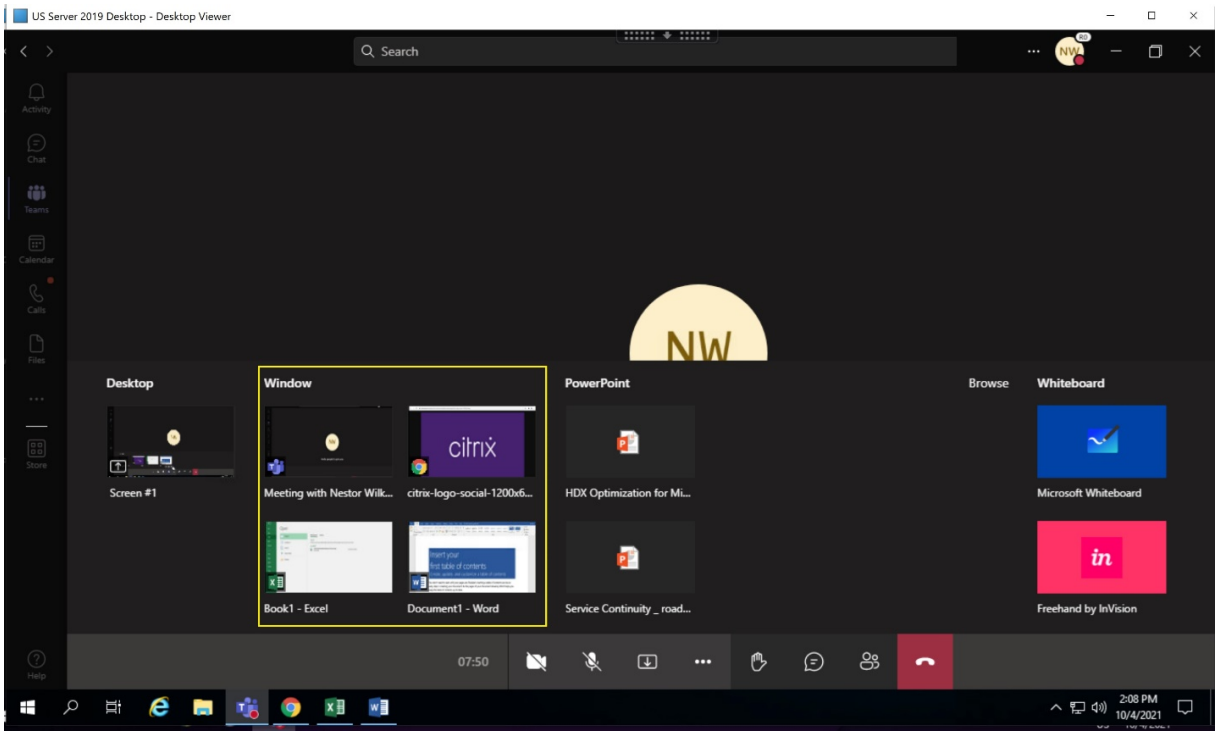
 

3. Selezionare un'app da condividere durante la riunione. Viene visualizzato un bordo rosso intorno all'app che si è selezionata e i partecipanti alla chiamata possono vedere l'app condivisa.

Per condividere un'altra app, fare nuovamente clic su **Condividi contenuto** e selezionare una nuova app.

Se si desidera disabilitare la condivisione delle app, creare la seguente chiave di registro sul VDA all'indirizzo `HKLM\SOFTWARE\Citrix\Graphics`:
Nome: `UseWsProvider`
Tipo: `DWORD`
Valore: 0

> **Nota:**
>
> - Se si riduce a icona un'app, Microsoft Teams visualizza l'ultima immagine dell'app condivisa. È possibile ingrandire la finestra per riprendere la condivisione dello schermo.
> - La condivisione dello schermo fa affidamento sull'acquisizione della finestra lato VDA. Il contenuto viene quindi inoltrato alla velocità massima all'app Citrix Workspace. La velocità massima è di 30 frame al secondo. L'app Citrix Workspace inoltra il contenuto al collega o al server della conferenza.




**Limitazioni note della condivisione dello schermo di app specifiche:**

- Il puntatore del mouse non è visibile quando si condivide un'app sullo schermo.

- Se si riduce a icona un'app quando la si condivide, nel selettore dello schermo viene visualizzata solo l'icona dell'app. La miniatura dell'app non viene visualizzata in anteprima nel selettore dello schermo. Non è possibile condividere il contenuto e non viene visualizzato il bordo rosso finché non si ingrandisce l'app.
- Nelle app LAA è visualizzato un elenco delle app che possono essere condivise con le app desktop nel Microsoft Teams ottimizzato nel VDA. Tuttavia, quando si seleziona l'app dall'elenco, il risultato potrebbe non essere quello previsto.

**Compatibilità con la protezione delle app**
La condivisione sullo schermo di un'app specifica è compatibile con la funzione di protezione delle app in Microsoft Teams ottimizzato per HDX. È possibile condividere lo schermo di un'app specifica, se l'app o il desktop è stato avviato da un gruppo di consegna per il quale è abilitata la protezione delle app.

Quando si fa clic su **Condividi contenuto** nell'interfaccia utente di Microsoft Teams, il selettore dello schermo rimuove l'opzione **Desktop**. È possibile selezionare l'opzione **Finestra** solo per condividere qualsiasi app aperta.

> **Nota:**
>
> Quando si avviano app o desktop da un gruppo di consegna con protezione app abilitata, non è possibile vedere il video in arrivo o la condivisione dello schermo se si utilizza l'app Citrix Workspace per Windows 2202 o versioni precedenti.

**Dare e richiedere il controllo in Microsoft Teams** Questa funzione è supportata nelle seguenti versioni dell'app Citrix Workspace (non vi è alcuna dipendenza dalla versione del VDA o dal sistema operativo, a sessione singola o multisessione):

- App Citrix Workspace per Windows versione 2112.1 o successiva
- App Citrix Workspace per Mac versione 2203.1 o successiva
- App Citrix Workspace per Linux versione 2203 o successiva
- App Citrix Workspace per ChromeOS versione 2303 o successiva

È possibile richiedere il controllo durante una chiamata di Microsoft Teams quando un partecipante condivide lo schermo. Una volta ottenuto il controllo, è possibile effettuare selezioni, modifiche o altre attività con tastiera e mouse sullo schermo condiviso.

Per assumere il controllo quando uno schermo viene condiviso, fare clic sul pulsante **Richiedi controllo** nell'interfaccia utente di Microsoft Teams. Il partecipante alla riunione che condivide lo schermo può accettare o rifiutare la richiesta.

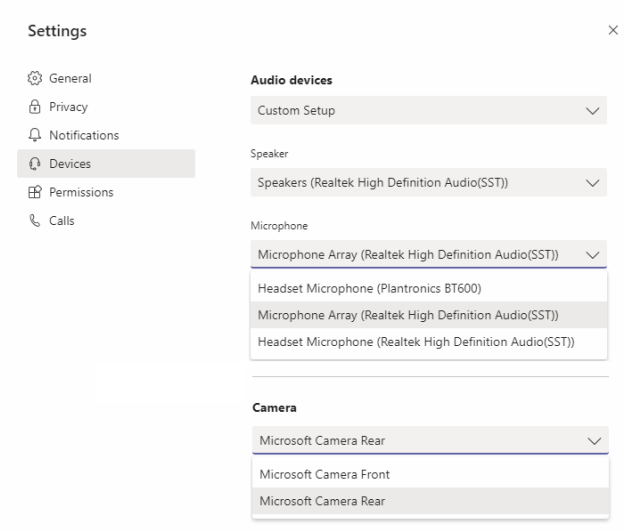
Mentre si dispone del controllo, è possibile effettuare selezioni, modifiche e altre alterazioni nello schermo condiviso. Per queste azioni, è possibile usare sia la tastiera che il mouse. Al termine fare clic su **Richiedi controllo**.

> **Limitazioni:**
>
> - I comandi Concedi controllo e Richiedi controllo non sono disponibili se l'utente sta condividendo una singola app (nota anche come condivisione app). È necessario condividere il desktop o il monitor completo.
> - La funzione per fissare la barra di controllo in una posizione specifica non è disponibile.

### Periferiche in Microsoft Teams

Quando l'ottimizzazione per Microsoft Teams è attiva, l'app Citrix Workspace accede alle periferiche (cuffie, microfono, videocamere, altoparlanti e così via). Quindi le periferiche vengono elencate correttamente nell'interfaccia utente di Microsoft Teams (**Impostazioni > Dispositivi**).




Microsoft Teams non accede direttamente ai dispositivi. Si basa invece sul motore multimediale WebRTC dell'app Workspace per l'acquisizione e l'elaborazione dei contenuti multimediali. Microsoft Teams elenca i dispositivi che l'utente può selezionare.

Le periferiche inserite mentre Microsoft Teams è attivo non sono selezionate per impostazione predefinita. È necessario selezionare manualmente le periferiche dalla schermata **Impostazioni** > **Dispositivi** dell'interfaccia utente di Microsoft Teams. Dopo che le periferiche sono state selezionate, Microsoft Teams ne memorizza le informazioni nella cache. Di conseguenza, le periferiche vengono selezionate automaticamente quando ci si riconnette a una sessione dallo stesso endpoint.

**Raccomandazioni:**

- Cuffie certificate Microsoft Teams con cancellazione dell'eco integrata. Nelle configurazioni con periferiche aggiuntive, in cui il microfono e gli altoparlanti si trovano su dispositivi separati, potrebbe essere presente un'eco. Un esempio è una webcam con un microfono incorporato

e un monitor con altoparlanti. Quando si utilizzano altoparlanti esterni, posizionarli il più lontano possibile dal microfono. Inoltre, posizionarli lontano da qualsiasi superficie che potrebbe rifrangere il suono nel microfono. Per ulteriori informazioni, passare a www.microsoft.com e cercare le cuffie certificate Microsoft Teams.

- Fotocamere certificate Microsoft Teams, sebbene le periferiche certificate Skype for Business siano compatibili con Microsoft Teams. Per ulteriori informazioni, passare a www.microsoft.com e cercare le fotocamere certificate Microsoft Teams e le periferiche certificate Skype for Business.
- Il motore multimediale dell'app Citrix Workspace non può sfruttare l'offload della CPU con webcam che eseguono la codifica H.264 on-board UVC 1.1 e 1.5.

> **Nota:**
>
> L'app Workspace 2009.6 per Windows è ora in grado di acquisire periferiche con formati audio a 24 bit o con frequenze superiori a 96 kHz.
>
> HdxTeams.exe (nell'app Citrix Workspace per Windows 2009 o versioni precedenti) supporta solo questi formati specifici dei dispositivi audio (canali, profondità di bit e frequenza di campionamento):
>
> - Dispositivi di riproduzione: fino a 2 canali, 16 bit, frequenze fino a 96.000 Hz
> - Dispositivi di registrazione: fino a 4 canali, 16 bit, frequenze fino a 96.000 Hz
>
> Anche se un solo altoparlante o microfono non corrisponde alle impostazioni previste, l'enumerazione dei dispositivi in Microsoft Teams non va a buon fine e viene visualizzato **Nessuno** in **Impostazioni > Dispositivi**.
> I log
> **Webrpc** in **HdxTeams.exe** mostrano questo tipo di informazioni:
>
> ```
> Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing ...
> ```
>
> ```
> Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!
> ```
>
> Come soluzione alternativa, disabilitare il dispositivo specifico oppure:
>
> 1. Aprire **Audio nel Pannello di controllo** (mmsys.cpl).
> 2. Selezionare il dispositivo di riproduzione o registrazione.
> 3. Andare a **Proprietà > Avanzate** e modificare le impostazioni su una modalità supportata.

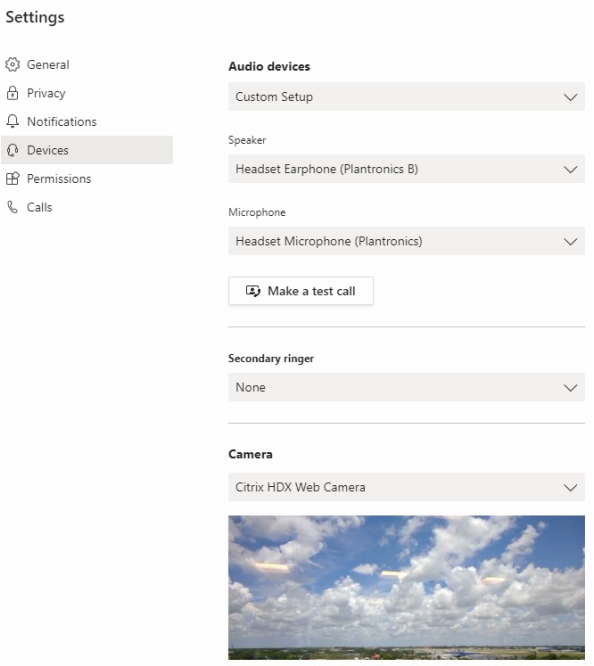
### Modalità di fallback

Se Microsoft Teams non riesce a caricarsi in modalità VDI ottimizzata ("Citrix HDX Not Connected"[Citrix HDX non connesso] in Teams/Informazioni/Versione), il VDA torna a utilizzare le tecnologie HDX legacy. Le tecnologie HDX legacy potrebbero essere il reindirizzamento della webcam e il reindirizzamento del microfono e dell'audio del client. Se si utilizza una versione dell'app Workspace/un sistema operativo della piattaforma che non supporta l'ottimizzazione di Microsoft Teams, le chiavi del Registro di sistema di fallback non si applicano.
In modalità di fallback, le periferiche sono mappate al VDA. Le periferiche vengono visualizzate nell'app Microsoft Teams come se fossero collegate localmente al desktop virtuale.

Ora è possibile controllare granularmente il meccanismo di fallback impostando le chiavi del Registro di sistema nel VDA. Per ulteriori informazioni, vedere Modalità di fallback di Microsoft Teams nell'elenco delle funzionalità gestite tramite il Registro di sistema.

Questa funzionalità richiede Microsoft Teams versione 1.3.0.13565 o successiva.

Per determinare se si è in modalità ottimizzata o non ottimizzata quando si esamina la scheda **Impostazioni > Dispositivi** nell'app Microsoft Teams, la differenza più significativa è il nome della videocamera. Se Microsoft Teams è stato caricato in modalità non ottimizzata, vengono avviate le tecnologie HDX legacy. Il nome della webcam presenta il suffisso **Citrix HDX**, come mostrato nell'immagine seguente. I nomi dell'altoparlante e del microfono potrebbero essere leggermente diversi (o troncati) rispetto alla modalità ottimizzata.




Quando vengono utilizzate tecnologie HDX legacy, Microsoft Teams non esegue l'offload dell'elaborazione di audio, video e condivisione dello schermo nel motore multimediale WebRTC dell'app Citrix Workspace dell'endpoint. Le tecnologie HDX utilizzano invece il rendering lato server. È previsto un

elevato consumo di CPU sul VDA quando viene attivato il video. Le prestazioni audio in tempo reale potrebbero non essere ottimali.

## Limitazioni note

### Limitazioni Citrix

Limitazioni sull'app Citrix Workspace:

- Pulsanti HID: risposta e fine chiamata non sono supportati. I tasti per abbassare e alzare il volume sono supportati.
- Le impostazioni QoS nell'interfaccia di amministrazione per Microsoft Teams non sono valide per gli utenti VDI.
- Gli utenti non possono acquisire schermate dei contenuti di Microsoft Teams quando utilizzano uno strumento di cattura su VDA. Tuttavia, se viene utilizzato uno strumento di cattura sul lato client, il contenuto può essere acquisito.

Limitazione sul VDA:

- Quando si configura l'impostazione High DPI (DPI elevato) dell'app Citrix Workspace su **Yes** (Sì), la finestra video reindirizzata non è nella posizione corretta. Questa limitazione si verifica quando il fattore di ridimensionamento DPI del monitor è impostato su un valore superiore al 100%

Limitazioni sull'app Citrix Workspace e sul VDA:

- È possibile controllare il volume di una chiamata ottimizzata solo utilizzando la barra del volume sul computer client, non sul VDA.

### Simulcast

Il supporto di Simulcast è abilitato per videoconferenze Microsoft Teams ottimizzate su Windows e Mac. Per Linux, rivolgersi al proprio fornitore di thin client.
Con Simulcast, la qualità e l'esperienza delle videoconferenze su diversi endpoint vengono migliorate adattandosi alla risoluzione corretta per la migliore esperienza di chiamata per tutti i chiamanti.

Con questa esperienza migliorata, ogni utente potrebbe fornire più flussi video con risoluzioni diverse (ad esempio 720p, 360p e così via) a seconda di diversi fattori, tra cui la capacità dell'endpoint, le condizioni della rete e così via. L'endpoint ricevente richiede quindi la massima risoluzione di qualità che può gestire, offrendo così a tutti gli utenti un'esperienza video ottimale.

> **Nota:**
>
> Questa funzionalità è disponibile solo dopo l'implementazione di un aggiornamento di Microsoft Teams. Per informazioni sulla data di pubblicazione, passare a https://www.microsoft.com/ e cercare la roadmap di Microsoft 365. Quando l'aggiornamento verrà implementato da Microsoft, sarà possibile leggere l'articolo CTX253754 per il relativo annuncio e l'aggiornamento della documentazione.

#### Limitazioni Microsoft

- La vista galleria 3x3 non è supportata. Dipendenza di Microsoft Teams: contattare Microsoft per sapere quando sarà disponibile la griglia 3x3.
- L'interoperabilità con Skype for Business è limitata alle chiamate audio, nessuna modalità video.
- La risoluzione massima del flusso video in entrata e in uscita è 720p.
- Il tono di suoneria delle chiamate PSTN non è supportato.
- Il bypass dei contenuti multimediali per il routing diretto non è supportato.
- I ruoli di produttore e presentatore di eventi broadcast e live non sono supportati. Il ruolo di partecipante è supportato ma non ottimizzato (viene invece eseguito il rendering sul VDA).
- La funzione zoom avanti e zoom indietro in Microsoft Teams non è supportata.
- Il routing basato sulla posizione e il bypass dei supporti non sono supportati.
- L'unione delle chiamate non è supportata (opzione non visualizzata nell'interfaccia utente).

#### Limitazioni Citrix e Microsoft

- Quando si esegue la condivisione dello schermo, l'opzione **Includi audio di sistema** non è disponibile.
- Simulcast non è supportato su ChromeOS.

### Imminente la fine del ciclo di vita di Microsoft Teams a finestra singola

Il 31 gennaio 2024, Microsoft ritirerà il supporto di Microsoft Teams per l'interfaccia utente a finestra singola quando si utilizza l'ottimizzazione VDI Microsoft Teams e supporterà solo l'esperienza multifinestra. Microsoft ha comunicato tale deprecazione l'8 settembre 2023 nell'M365s Admin Center (ID post: MC674419).
I dettagli pubblici sulla funzionalità multifinestra sono disponibili nell'articolo della Tech Community New Meeting and Calling Experience in Microsoft Teams (Nuova esperienza di riunioni e chiamate in Microsoft Teams).

È necessario aggiornare l'app VDA e Citrix Workspace alle versioni supportate per continuare a utilizzare Microsoft Teams in modalità ottimizzata per la condivisione di video e schermo. Se non si effettua l'aggiornamento dell'infrastruttura e degli endpoint per supportare il multi-finestra, è possibile effettuare solo chiamate audio. Non sarà possibile utilizzare la funzionalità ottimizzata di condivisione di video e schermo.

La tabella seguente illustra le versioni minime, LTSR e consigliate dei VDA e dell'app Citrix Workspace necessarie per continuare a utilizzare le chiamate ottimizzate in Microsoft Teams su Citrix VDI:

| Componente | Versione minima | Versione supportata dalla LTSR | Versione consigliata |
|---|---|---|---|
| Microsoft Teams | 1.5.00.11865 | Non applicabile | Più recente |
| VDA | 1912 CU6 LTSR, 2203 LTSR, 2112 CR | 1912 CU7+, 2203 CU2+ | 2308 CR+ |
| App Citrix Workspace per Windows | 2205 CR | 2203 CU2+ | 2309 CR+ |
| App Citrix Workspace per Mac | 2209 CR | Non applicabile | 2308 CR+ |
| App Citrix Workspace per Linux | 2209 CR | Non applicabile | 2308 CR+ |
| App Citrix Workspace per ChromeOS o HTML5 | 2303 CR | Non applicabile | 2309 CR+ |

## Annuncio di obsolescenza del formato SDP (Piano B) di WebRTC

Citrix prevede di eliminare l'attuale supporto del formato SDP (Piano B) di WebRTC nelle versioni future. È necessario utilizzare Unified Plan in WebRTC per supportare le funzionalità ottimizzate di Microsoft Teams.

### Prodotti interessati

In una delle versioni future dell'applicazione Citrix Workspace, le chiamate tra endpoint con la prossima versione dell'app Citrix Workspace e gli endpoint con l'app Citrix Workspace 2108 o versioni precedenti non saranno supportate. Questa incompatibilità di chiamata include i client dell'app Citrix Workspace (CWA) 1912 LTSR. Sono interessati i seguenti client CWA:

- App Citrix Workspace per Windows
- App Citrix Workspace per Linux

- App Citrix Workspace per Mac
- App Citrix Workspace per Chrome

#### Sostituto per Plan B

Se si utilizza una versione dell'app Citrix Workspace precedente alla 2109, è necessario eseguire l'aggiornamento a una versione supportata (preferibilmente l'ultima versione CR). In caso contrario, le chiamate con una versione futura o con endpoint più recenti non riusciranno a connettersi. Potrebbe inoltre non essere possibile completare le chiamate tra le versioni future e i partner di comunicazione federati se il partner federato non ha aggiornato il proprio Citrix Workspace.

La versione 2108 dell'app Citrix Workspace ha completato la data di supporto in marzo 2023 e deve essere aggiornata a una versione più recente. Per ulteriori informazioni, vedere App Workspace che illustra i dettagli sul supporto della versione dell'app Citrix Workspace.

Per ulteriori informazioni sulla deprecazione del Piano B, consulta la documentazione di WebRTC.

### Informazioni aggiuntive

- Monitorare, risolvere i problemi e supportare Microsoft Teams
- Distribuire l'app desktop Microsoft Teams nella macchina virtuale
- Installare Microsoft Teams utilizzando MSI (sezione Installazione VDI)
- Thin client
- Strumento di valutazione della rete di Skype for Business
- Comprendere la coesistenza e l'interoperabilità di Microsoft Teams e Skype for Business

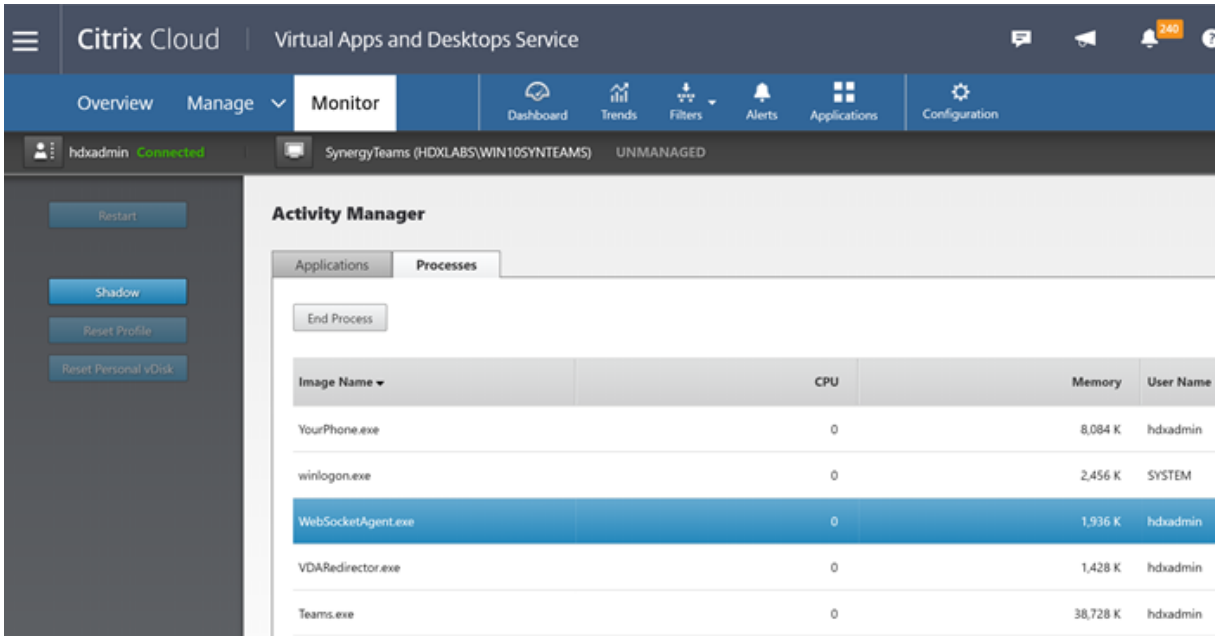
## Monitorare, risolvere i problemi e supportare Microsoft Teams

January 7, 2024

### Monitorare Teams

Questa sezione fornisce linee guida per il monitoraggio dell'ottimizzazione di Microsoft Teams con HDX.
Se si utilizza la modalità ottimizzata e `HdxRtcEngine.exe` è in esecuzione sul computer client, sul VDA è in esecuzione un processo chiamato `WebSocketAgent.exe` nella sessione. Utilizzare **Activity Manager (Gestione attività)** in Director per visualizzare l'applicazione.




Con la versione minima del VDA 1912, è possibile monitorare le chiamate di Teams attive utilizzando Citrix HDX Monitor (versione minima 3.11). L'ISO del prodotto Citrix Virtual Apps and Desktops contiene l'ultima versione di `hdxmonitor.msi` nella cartella `layout\image-full\Support\HDX Monitor`.

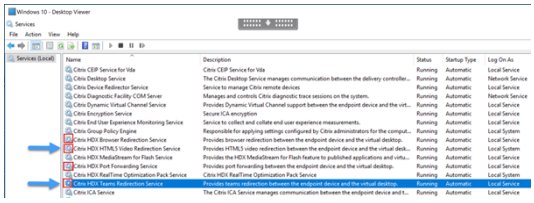
Per ulteriori informazioni, vedere *Monitoraggio* nell'articolo del Knowledge Center CTX253754.

## Risoluzione dei problemi

In questa sezione vengono forniti suggerimenti per la risoluzione dei problemi che potrebbero verificarsi quando si utilizza l'ottimizzazione per Microsoft Teams. Per ulteriori informazioni, vedere CTX253754.

### Sul Virtual Delivery Agent

Esistono quattro servizi installati da BCR_x64.msi. Solo due sono responsabili del reindirizzamento di Microsoft Teams nel VDA.



- Il **servizio di reindirizzamento di Teams di Citrix HDX** stabilisce il canale virtuale utilizzato in Microsoft Teams. Il servizio si basa su CtxSvcHost.exe.

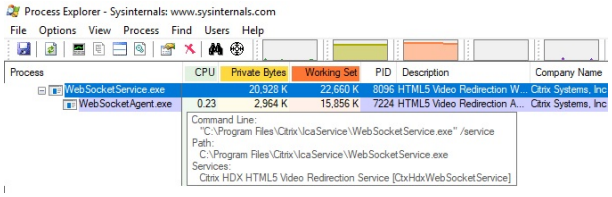
- Il **servizio di reindirizzamento video HTML5 di Citrix HDX** viene eseguito come WebSocketService.exe in ascolto su TCP 127.0.0.1:9002. WebSocketService.exe esegue due funzioni principali:

  i. La **terminazione TLS per WebSocket protetti** riceve una connessione WebSocket protetta da vdiCitrixPeerConnection.js, che è un componente all'interno dell'app Microsoft Teams. È possibile tenerne traccia con lo strumento Process Monitor. Per ulteriori informazioni sui certificati, vedere la sezione "Reindirizzamento video TLS e HTML5 e reindirizzamento del contenuto del browser"in Comunicazione tra Controller e VDA.

  Alcuni software di sicurezza antivirus e desktop interferiscono con il corretto funzionamento di `WebSocketService.exe` e dei relativi certificati. Mentre il servizio di reindirizzamento video HTML5 di Citrix HDX potrebbe essere in esecuzione nella console di `services.msc`, il socket TCP `127.0.0.1:9002` dell'host locale non è mai in modalità di ascolto come si vede in netstat. Il servizio si blocca se si cerca di riavviarlo ("Stopping…."[Arresto in corso…]). Assicurarsi di applicare le esclusioni appropriate per il processo `WebSocketService.exe`.

  ii. **Mappatura della sessione utente.** Quando viene avviata l'applicazione Microsoft Teams, WebSocketService.exe avvia il processo WebSocketAgent.exe nella sessione dell'utente nel VDA. WebSocketService.exe viene eseguito nella sessione 0 come account LocalSystem.

  È possibile utilizzare `netstat` per verificare se il servizio WebSocketService.exe è in uno stato di ascolto attivo nel VDA.

  Eseguire `netstat -anob -p tcp` da una finestra del prompt dei comandi con privilegi elevati:

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

  In caso di connessione riuscita, lo stato viene modificato in ESTABLISHED (STABILITO):

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

> **Importante:**
>
> WebSocketService.exe è in ascolto in due socket TCP, 127.0.0.1:9001 e 127.0.0.1:9002. La porta 9001 viene utilizzata per il reindirizzamento del contenuto del browser e il reindirizzamento video HTML5. La porta 9002 viene utilizzata per il reindirizzamento di Microsoft Teams. Assicurarsi di non disporre di alcuna configurazione proxy nel sistema operativo Windows del VDA che possa impedire una comunicazione diretta tra Teams.exe e WebSocketService.exe. Talvolta, quando si configura un proxy esplicito in Internet Explorer 11 (**Opzioni Internet > Connessioni > Impostazioni LAN > Server proxy**), le connessioni potrebbero passare attraverso un server proxy assegnato. Verificare che l'opzione **Ignora server proxy per indirizzi locali** sia selezionata quando si utilizza un'impostazione proxy manuale ed esplicita.

**Posizioni e descrizioni dei servizi**

| Servizio | Percorso dell'eseguibile nel sistema operativo Windows Server | Accesso come | Descrizione |
|---|---|---|---|
| Servizio di reindirizzamento video HTML5 Citrix | "C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service | Account di sistema locale | Fornisce più servizi multimediali HDX con il framework iniziale necessario per eseguire il reindirizzamento dei file multimediali tra il desktop virtuale e il dispositivo endpoint. |
| Servizio di reindirizzamento del browser Citrix HDX | "C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs | Questo account (servizio locale) | Fornisce il reindirizzamento del contenuto del browser tra il dispositivo endpoint e il desktop virtuale. |
| Servizio di port forwarding Citrix | "C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs | Questo account (servizio locale) | Fornisce il port forwarding tra il dispositivo endpoint e il desktop virtuale per il reindirizzamento del contenuto del browser. |

| Servizio | Percorso dell'eseguibile nel sistema operativo Windows Server | Accesso come | Descrizione |
|---|---|---|---|
| Servizio di reindirizzamento di Teams di Citrix HDX | "C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs | Account di sistema locale | Fornisce il reindirizzamento di Microsoft Teams tra il dispositivo endpoint e il desktop virtuale. |

**App Citrix Workspace**

Nell'endpoint dell'utente, l'app Citrix Workspace per Windows crea un'istanza di un nuovo servizio denominato HdxTeams.exe o HdxRtcEngine.exe. Lo fa quando Microsoft Teams viene avviato nel VDA e l'utente tenta di chiamare le periferiche o di accedervi in anteprima automatica. Se questo servizio non viene visualizzato, controllare quanto segue:

1. Assicurarsi di aver installato l'app Workspace (versione minima 1905) per Windows. HdxTeams.exe o HdxRtcEngine.exe e i file binari webrpc.dll sono visualizzati nel percorso di installazione dell'app Workspace?
2. Se è stato convalidato il passo 1, effettuare le seguenti operazioni per verificare se HdxTeams.exe o HdxRtcEngine.exe viene avviato.
    a) Chiudere Microsoft Teams sul VDA.
    b) Avviare services.msc sul VDA.
    c) Arrestare il servizio di reindirizzamento di Teams di Citrix HDX.
    d) Disconnettere la sessione ICA.
    e) Collegare la sessione ICA.
    f) Avviare il servizio di reindirizzamento di Teams di Citrix HDX.
    g) Riavviare il servizio di reindirizzamento video HTML5 di Citrix HDX.
    h) Avviare Microsoft Teams sul VDA.
3. Se HdxTeams.exe o HdxRtcEngine.exe non viene ancora avviato nell'endpoint client, effettuare le seguenti operazioni:
    a) Riavviare il VDA.
    b) Riavviare l'endpoint client.

## Supporto

Citrix e Microsoft supportano congiuntamente la distribuzione di Microsoft Teams da Citrix Virtual Apps and Desktops utilizzando l'ottimizzazione per Microsoft Teams. Questo supporto congiunto è il risultato di una stretta collaborazione tra le due società. Se si dispone di contratti di assistenza validi e si verifica un problema con questa soluzione, aprire un ticket di supporto con il fornitore di cui si sospetta che il codice stia causando il problema. Ossia, Microsoft per Teams o Citrix per i componenti di ottimizzazione.
Citrix o Microsoft ricevono il ticket, esaminano il problema e ne avviano la risoluzione come appropriato. Non è necessario contattare il team di supporto di ogni azienda.

In caso di problemi, si consiglia di fare clic su **Aiuto > Segnala un problema** nell'interfaccia utente di Teams. I log sul lato VDA vengono automaticamente condivisi tra Citrix e Microsoft per risolvere i problemi tecnici più rapidamente.

### Raccolta di log

I log del motore multimediale HDX si trovano sul computer dell'utente (non sul VDA). In caso di problemi, assicurarsi di allegare i log al caso di supporto.

**Log di Windows:**

I log di Windows sono disponibili in %TEMP% all'interno della cartella **HDXTeams** (AppData/Local/Temp/HDXTeams o AppData/Local/Temp/HdxRtcEngine). Cercare un file .txt denominato webrpc_Day_Month_timestamp_Year.txt. Se si utilizzano versioni più recenti dell'app Citrix Workspace, ad esempio l'app Citrix Workspace 2009.5 o versioni successive, archiviare i log in AppData\Local\Temp\HdxRtcEngine.

Ogni sessione crea una cartella separata per i log.

**Log Mac:**

1. Log VDWEBRTC: registra l'esecuzione del canale virtuale.

   Posizione:/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt

2. Log HdxRtcEngine: registra l'esecuzione dei processi su HdxRtcEngine.

   Posizione:$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log

   Il log HdxRtcEngine è abilitato per impostazione predefinita.

3. Webrpc logs - sono i log più importanti che registrano l'esecuzione del wrap-up della libreria webrtc.

   Posizione:/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log

**Log Linux:**

È possibile individuare i log di Linux nelle cartelle /tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/.
Log Webrtc: /tmp/webrpc/<current date>/webrtc.log
log del kernel: /var/log/syslog

**Log ICE/STUN/TURN/ :**

Quando si avvia una chiamata, sono necessarie queste quattro fasi ICE:

- Raccolta dei candidati
- Scambio dei candidati
- Controlli di connettività (richieste di binding STUN)
- Promozione dei candidati

Nei log HdxRtcEngine.exe, le voci seguenti sono le voci ICE (Interactive Connectivity Establishment) pertinenti. Queste voci devono essere presenti per consentire alla configurazione di una chiamata di avere esito positivo. Vedere il seguente frammento di esempio per la fase di raccolta:

```
RPCStubs Info: -> device id = \\?\display#int3470#4&1835d135&0&uid13424
    #{
 65e8773d-8f56-11d0-a3b9-00a0c9223196 }
 {
 bf89b5a5-61f7-4127-a279-e187013d7caf }
  label = Microsoft Camera Front groupId =

webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
webrtcapi.RTCPeerConnection Info: setLocalDescription.
>>> begin:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveLocalOffer

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Gathering

[...]
>>> begin:sdp
candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
    generation 0 ufrag oVk6 network-id 1
<<< end:sdp
[...]
>>> begin:sdp
candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay
    raddr 73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1
    network-cost 10
<<< end:sdp
[...]
>>> begin:sdp
```

```
26 candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx
      raddr 10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id
      1
27 <<< end:sdp
28 [...]
29
30 webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
      Complete webrtcapi.RTCPeerConnection Info: setRemoteDescription.
31 >>> begin:sdp
32 [...]
33
34 webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
      HaveRemotelOffer
35
36 <!--NeedCopy-->
```

Se ci sono più candidati ICE, l'ordine di preferenza è:

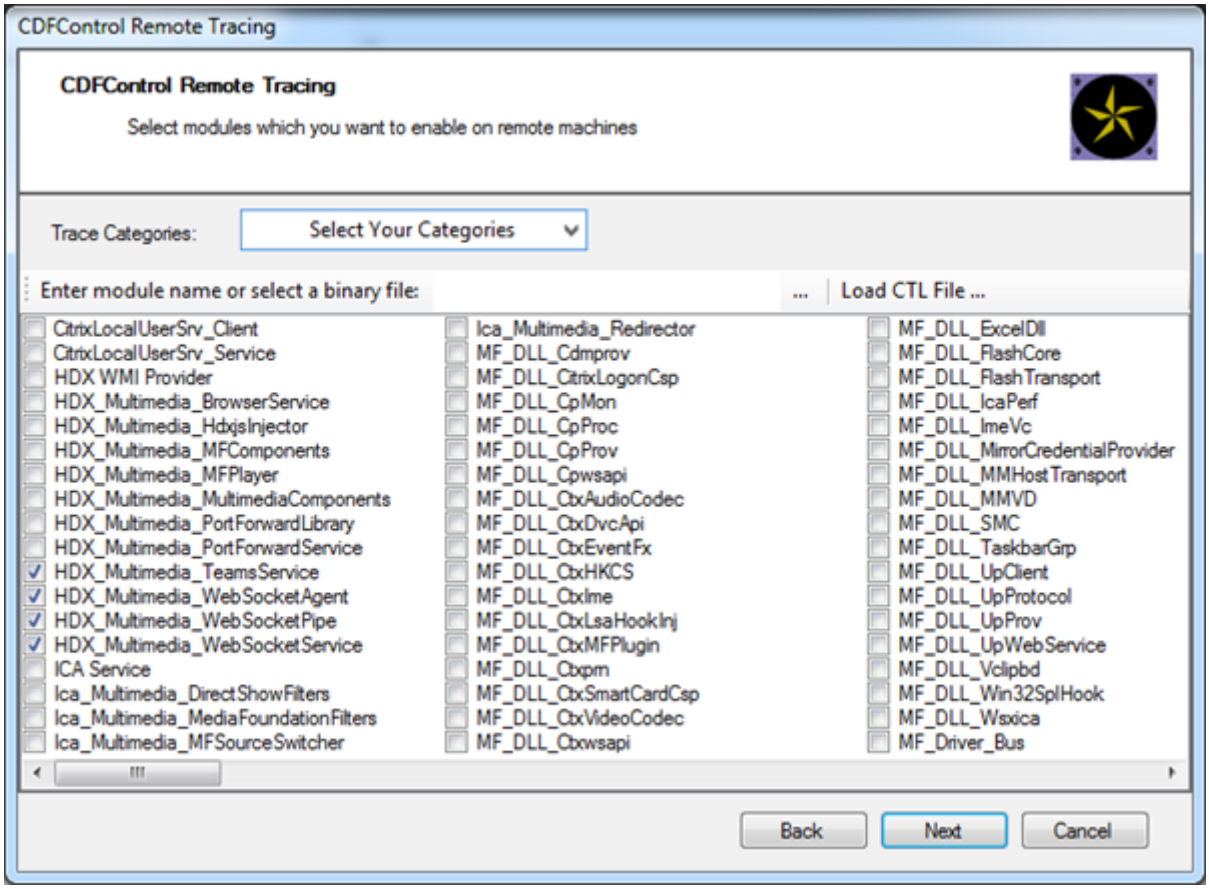
1. host
2. peer riflessivo
3. server riflessivo
4. relè di trasporto

Se si riscontra un problema e si riesce a riprodurlo in modo coerente, si consiglia di fare clic su**Aiuto > Segnala un problema** in Teams. I log vengono condivisi tra Citrix e Microsoft per risolvere problemi tecnici se è stato aperto un caso con Microsoft.
Anche l'acquisizione di tracce CDF prima di contattare il supporto Citrix è utile. Per ulteriori informazioni, vedere l'articolo del Knowledge Center CDFcontrol.

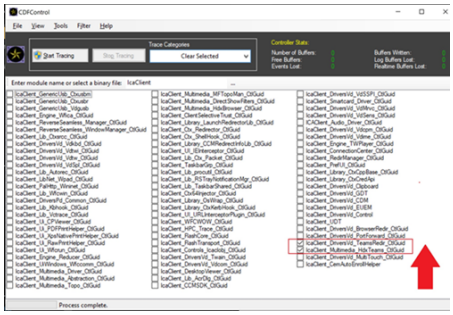
Per consigli sulla raccolta delle tracce CDF, vedere l'articolo del Knowledge Center Raccomandazioni per la raccolta di tracce CDF.

**Tracce CDF lato VDA: abilitare i seguenti provider di traccia CDF:**




**Tracce CDF lato app Workspace - Abilitare i seguenti provider di traccia CDF:**



- IcaClient_DriversVd_TeamsRedir (opzionale)
- IcaClient_Multimedia_HdxTeams (richiede l'app Citrix Workspace 2012 o versione successiva)

## Reindirizzamento di Windows Media

January 7, 2024

Il reindirizzamento di Windows Media controlla e ottimizza il modo in cui i server forniscono audio

e video in streaming agli utenti. Riproducendo i file multimediali di runtime sul dispositivo client anziché sul server, il reindirizzamento di Windows Media riduce i requisiti di larghezza di banda per la riproduzione di file multimediali. Il reindirizzamento di Windows Media migliora le prestazioni di Windows Media Player e dei lettori compatibili in esecuzione su desktop Windows virtuali.

Se i requisiti per il recupero dei contenuti sul lato client di Windows Media non vengono soddisfatti, la distribuzione dei contenuti multimediali utilizza automaticamente il recupero lato server. Questo metodo è trasparente per gli utenti. È possibile utilizzare Citrix Scout per eseguire una traccia Citrix Diagnosis Facility (CDF) da HostMMTransport.dll per determinare il metodo utilizzato. Per ulteriori informazioni, vedere Citrix Scout.

Il reindirizzamento di Windows Media intercetta la pipeline dei contenuti multimediali nel server host, acquisisce i dati multimediali nel formato compresso nativo e reindirizza i contenuti al dispositivo client. Il dispositivo client ricrea quindi la pipeline dei contenuti multimediali per decomprimere i dati multimediali ricevuti dal server host ed eseguirne il rendering. Il reindirizzamento di Windows Media funziona bene sui dispositivi client con sistema operativo Windows. Questi dispositivi dispongono del framework multimediale necessario per ricostruire la pipeline dei contenuti multimediali così come era presente sul server host. I client Linux utilizzano framework multimediali open source simili per ricostruire la pipeline dei contenuti multimediali.

L'impostazione del criterio **Windows Media Redirection (Reindirizzamento di Windows Media)** controlla questa funzionalità e il valore predefinito è **Allowed (Consentito)**. In genere, questa impostazione aumenta la qualità audio e video di cui il server esegue il rendering a un livello paragonabile ai contenuti riprodotti localmente su un dispositivo client. In rari casi, la riproduzione di file multimediali utilizzando il reindirizzamento di Windows Media risulta peggiore rispetto ai contenuti multimediali sottoposti a rendering utilizzando la compressione ICA di base e l'audio normale. È possibile disabilitare questa funzionalità aggiungendo l'impostazione **Windows Media Redirection (Reindirizzamento di Windows Media)** a un criterio e impostandone il valore su **Prohibited (Vietato)**.

Per ulteriori informazioni sulle impostazioni dei criteri, vedere Impostazioni dei criteri multimediali.

**Limitazione:**

Quando si utilizza Windows Media Player e RAVE (Remote Audio & Video Extensions) abilitati all'interno di una sessione, potrebbe essere visualizzata una schermata nera. Questa schermata nera potrebbe essere visualizzata facendo clic con il pulsante destro del mouse sul contenuto video e selezionando **Mostra sempre In esecuzione in primo piano**.

## Reindirizzamento generale del contenuto

January 7, 2024

Il reindirizzamento dei contenuti consente di controllare se gli utenti accedono alle informazioni utilizzando applicazioni pubblicate sui server o utilizzando applicazioni in esecuzione localmente sui dispositivi utente.

### Reindirizzamento delle cartelle client

Il reindirizzamento delle cartelle client modifica il modo in cui i file lato client sono accessibili nella sessione lato host.

- Quando si abilita solo il mapping delle unità client sul server, i volumi completi lato client vengono automaticamente mappati alle sessioni come collegamenti UNC (Universal Naming Convention).
- Quando si abilita il reindirizzamento delle cartelle client sul server e l'utente lo configura sul dispositivo desktop Windows, la parte del volume locale specificata dall'utente viene reindirizzata.

### Reindirizzamento da host a client

Prendere in considerazione l'utilizzo del reindirizzamento da host a client per specifici casi di utilizzo non comuni. Normalmente, altre forme di reindirizzamento dei contenuti potrebbero essere migliori. Supportiamo questo tipo di reindirizzamento solo sui VDA del sistema operativo multisessione e non sui VDA del sistema operativo a sessione singola.

### Accesso alle app locali e reindirizzamento URL

L'accesso alle app locali integra perfettamente le applicazioni Windows installate localmente in un ambiente desktop ospitato. Lo fa senza passare da un computer all'altro.

La tecnologia HDX fornisce un **reindirizzamento USB generico** per dispositivi speciali che non dispongono di alcun supporto ottimizzato o dove questo non è adatto.

## Reindirizzamento delle cartelle client

January 7, 2024

Il reindirizzamento delle cartelle client modifica il modo in cui i file lato client sono accessibili nella sessione lato host. Se si abilita solo il mapping delle unità client sul server, i volumi completi lato client vengono automaticamente mappati come collegamenti UNC (Universal Naming Convention) alle sessioni. Quando si abilita il reindirizzamento delle cartelle client sul server e l'utente lo configura sul dispositivo utente, la parte del volume locale specificata dall'utente viene reindirizzata.

Solo le cartelle specificate dall'utente vengono visualizzate come collegamenti UNC all'interno delle sessioni. Ossia invece del file system completo sul dispositivo utente. Se si disattivano i collegamenti

UNC tramite il Registro di sistema, le cartelle client vengono visualizzate come unità mappate all'interno della sessione.

Il reindirizzamento delle cartelle client è supportato solo sui computer con sistema operativo Windows a sessione singola.

Il reindirizzamento delle cartelle client per un'unità USB esterna non viene salvato durante lo scollegamento e il collegamento del dispositivo.

Abilitare il reindirizzamento della cartella client sul server. Quindi, sul dispositivo client, specificare quali cartelle reindirizzare. L'applicazione utilizzata per specificare le opzioni delle cartelle client è inclusa nell'app Citrix Workspace fornita con questa versione.

**Requisiti:**

Per i server:

- Windows Server 2022
- Windows Server 2019 edizioni Standard e Datacenter
- Windows Server 2016, edizioni standard e Datacenter
- Windows Server 2012 R2, edizioni standard e Datacenter

Per i client:

- Windows 10, edizioni a 32 bit e a 64 bit (versione minima 1607)
- Windows 8.1, edizioni a 32 bit e 64 bit (inclusa l'edizione Embedded)
- Windows 7, edizioni a 32 bit e 64 bit (inclusa l'edizione Embedded)

Per abilitare il reindirizzamento delle cartelle client sul server, vedere Reindirizzamento delle cartelle clientnell'elenco delle funzionalità gestite tramite il Registro di sistema.

Sul dispositivo utente, specificare quali cartelle reindirizzare:

1. Assicurarsi che sia installata la versione più recente dell'app Citrix Workspace.
2. Dalla directory di installazione dell'app Citrix Workspace, avviare CtxCFRUI.exe.
3. Scegliere il pulsante di opzione **Custom (Personalizza)** e aggiungere, modificare o rimuovere cartelle.
4. Disconnettere e riconnettere le sessioni in modo che l'impostazione venga applicata.

## Reindirizzamento da host a client

January 10, 2024

Il reindirizzamento da host a client consente l'apertura degli URL, incorporati come collegamenti ipertestuali nelle applicazioni in esecuzione su una sessione Citrix, utilizzando l'applicazione corrispondente sul dispositivo endpoint dell'utente. Alcuni casi d'uso comuni per il reindirizzamento da host a client includono:

- Reindirizzamento di siti Web nei casi in cui il server Citrix non dispone di accesso a Internet o di rete all'origine.
- Non si desidera utilizzare il reindirizzamento dei siti Web quando si esegue un browser Web all'interno della sessione Citrix per motivi di sicurezza, prestazioni, compatibilità o scalabilità.
- Reindirizzamento di tipi di URL specifici nei casi in cui le applicazioni richieste per aprire l'URL non sono installate sul server Citrix.

Il reindirizzamento da host a client non è destinato agli URL a cui si accede su una pagina Web o che si digitano nella barra degli indirizzi del browser Web in esecuzione nella sessione Citrix. Per il reindirizzamento degli URL nei browser Web, vedere Reindirizzamento URL bidirezionale o Reindirizzamento del contenuto del browser.

### Requisiti di sistema

- VDA con sistema operativo multisessione
- Client supportati:
  - App Citrix Workspace per Windows
  - App Citrix Workspace per Mac
  - App Citrix Workspace per Linux
  - App Citrix Workspace per HTML5
  - App Citrix Workspace per Chrome

Il dispositivo client deve avere un'applicazione installata e configurata per gestire il reindirizzamento dei tipi di URL.

### Configurazione

Utilizzare il criterio Citrix Host to client redirection (reindirizzamento da host a client) per abilitare questa funzionalità. Il **reindirizzamento da host a client** è disabilitato per impostazione predefinita. Dopo aver abilitato il criterio di reindirizzamento da host a client, l'applicazione Citrix Launcher si registra con il server Windows per assicurarsi che possa intercettare gli URL e inviarli al dispositivo client.

Successivamente è necessario configurare i criteri di gruppo di Windows per utilizzare Citrix Launcher come applicazione predefinita per i tipi di URL richiesti. Sul VDA del server Citrix, creare il file ServerFTAdefaultPolicy.xml e inserire il seguente codice XML.

```
<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />

<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
    "ServerFTA" />

</DefaultAssociations>
<!--NeedCopy-->
```

Dalla Console Gestione Criteri di gruppo, andare a **Configurazione computer > Modelli amministrativi > Componenti di Windows > Esplora file > Imposta file di configurazione delle associazioni predefinite** e salvare il file ServerFTAdefaultPolicy.xml.

> **Nota:**
>
> Se un server Citrix non dispone delle impostazioni Criteri di gruppo, Windows richiede agli utenti di selezionare un'applicazione per l'apertura degli URL.

Per impostazione predefinita, supportiamo il reindirizzamento dei seguenti tipi di URL:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

Per includere altri tipi di URL standard o personalizzati nell'elenco per il reindirizzamento, creare una nuova riga **Association Identifier** (Identificatore di associazione) nel file ServerFTAdefaultPolicy.xml citato in precedenza. Ad esempio:

```
<Association Identifier="ftp"ProgId="ServerFTAHTML"ApplicationName="
ServerFTA"/>

<Association Identifier="mailto"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>

<Association Identifier="customtype1"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>

<Association Identifier="customtype2"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

L'aggiunta di tipi di URL all'elenco richiede anche la configurazione del client. Creare la chiave del Registro di sistema e i valori seguenti sul client Windows.

> **Nota:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Nome del valore: ExtraURLProtocols
- Tipo di valore: REG_SZ
- Dati valore: specificare i tipi di URL richiesti separati da punto e virgola. Includere tutto prima della parte dell'URL relativa all'autorità. Ad esempio:
  `ftp://;mailto:;customtype1://;custometype2://`

È possibile aggiungere tipi di URL solo per i client Windows. I client che non hanno le impostazioni del Registro di sistema sopra indicate rifiutano il reindirizzamento alla sessione Citrix. Il client deve avere un'applicazione installata e configurata per gestire i tipi di URL specificati.

Per rimuovere i tipi di URL dall'elenco di reindirizzamento predefinito, creare la chiave del Registro di sistema e i valori seguenti sul server VDA.

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome valore: DisableServerFTA
- Tipo di valore: DWORD
- Dati del valore: 1
- Nome valore: NoRedirectClasses
- Tipo di valore: REG_MULTI_SZ
- Dati del valore: specificare qualsiasi combinazione di valori: `http`,`https`, `rtsp`, `rtspu`, `pnm` o `mms`. Digitare più valori su righe separate. Ad esempio:

```
http
https
rtsp
```

Per abilitare il reindirizzamento da host a client per un insieme specifico di siti Web, creare una chiave del Registro di sistema e i valori sul server VDA.

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA

- Nome del valore: ValidSites
- Tipo di valore: REG_MULTI_SZ
- Dati del valore: specificare qualsiasi combinazione di nomi di dominio completi (FQDN). Digitare più FQDN su righe separate. Includere solo il nome di dominio completo, senza protocolli (`http://` o `https://`). Un nome di dominio completo può includere un asterisco (*) come carattere jolly solo nella posizione più a sinistra. Questo carattere jolly corrisponde a un singolo livello di dominio, che è coerente con le regole in RFC 6125. Ad esempio:

`www.exmaple.com`

`*.example.com`

> **Nota:**
>
> Non è possibile utilizzare il tasto **ValidSites** in combinazione con le chiavi **DisableServerFTA** e **NoRedirectClasses**.

### Configurazione predefinita del browser del server VDA

L'abilitazione del reindirizzamento da host al client come indicato in questa sezione sostituisce qualsiasi precedente configurazione predefinita del browser sul server VDA. Se un URL Web non viene reindirizzato, Citrix Launcher trasferisce l'URL al browser configurato nella chiave del Registro di sistema`command_backup`. La chiave punta a Internet Explorer per impostazione predefinita, ma è possibile modificarla per includere il percorso a un browser diverso. Per ulteriori informazioni, vedere Configurazione predefinita del browser del server VDA nell'elenco delle funzionalità gestite tramite il Registro di sistema.

## Reindirizzamento del contenuto bidirezionale

January 7, 2024

Il reindirizzamento bidirezionale dei contenuti consente di trasmettere gli URL HTTP o HTTPS presenti nei browser Web o incorporati nelle applicazioni fra la sessione Citrix VDA e l'endpoint client in entrambe le direzioni. Un URL inserito in un browser in esecuzione nella sessione Citrix può essere aperto utilizzando il browser predefinito del client. Al contrario, un URL inserito in un browser in esecuzione sul client può essere aperto in una sessione Citrix, con un'applicazione pubblicata o un desktop. Alcuni casi d'uso comuni per il reindirizzamento bidirezionale dei contenuti includono:

- Reindirizzamento degli URL Web nei casi in cui il browser di partenza non abbia accesso alla rete alla fonte.
- Reindirizzamento degli URL Web per motivi di compatibilità e sicurezza del browser.

- Il reindirizzamento degli URL Web incorporati nelle applicazioni quando si esegue un browser Web nella sessione Citrix o sul client non è richiesto.

### Requisiti di sistema

- VDA con sistema operativo a sessione singola o multisessione
- App Citrix Workspace per Windows

Browser:

- Internet Explorer 11
- Google Chrome con estensione per il reindirizzamento del browser Citrix (disponibile sul Google Chrome Web Store)
- Microsoft Edge (Chromium) con Citrix Browser Redirection Extension (disponibile sul Google Chrome Web Store)

### Configurazione

Il reindirizzamento bidirezionale dei contenuti deve essere abilitato utilizzando la politica Citrix sia sul VDA che sul client affinché il reindirizzamento funzioni. Il reindirizzamento bidirezionale dei contenuti è disabilitato per impostazione predefinita.

Per la configurazione del VDA, vedere Reindirizzamento bidirezionale del contenuto nelle impostazioni dei criteri ICA.

Per la configurazione del client, vedere Reindirizzamento bidirezionale del contenuto nella documentazione dell'app Citrix Workspace per Windows.

Le estensioni del browser devono essere registrate utilizzando i comandi descritti. Eseguire i comandi secondo necessità sul VDA e sul client in base al browser in uso.

Per registrare le estensioni del browser su VDA, aprire un prompt dei comandi. Quindi, eseguire `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` con l'opzione del browser richiesta come negli esempi illustrati:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge
```

Per registrare l'estensione su tutti i browser disponibili eseguire:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall
```

Per annullare la registrazione di un'estensione del browser utilizzare l'opzione `/unreg<browser>` come nell'esempio:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

Per registrare le estensioni del browser sul client, aprire un prompt dei comandi ed eseguire `%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe` con le stesse opzioni degli esempi.

> **Nota:**
>
> Il comando register fa sì che i browser Chrome ed Edge chiedano agli utenti di abilitare l'estensione di reindirizzamento del browser Citrix durante il primo avvio. L'estensione del browser può essere installata anche manualmente dal Google Chrome Web Store.

### Reindirizzamento con caratteri jolly da Citrix VDA al client

Il reindirizzamento bidirezionale dei contenuti supporta l'uso di caratteri jolly quando si definiscono gli URL da reindirizzare. Per configurare il reindirizzamento bidirezionale dei contenuti, vedere le istruzioni di configurazione.

In Web Studio, impostare l'URL con caratteri jolly in **Allowed URLs to be redirected to Client** (URL consentiti da reindirizzare al client). L'asterisco (*) è il carattere jolly.

> **NOTA:**
>
> - Non impostare **Allowed URLs to be redirected to VDA** (URL con reindirizzamento a VDA consentito) nei criteri del client. Assicurarsi che i siti impostino **Allowed URLs to be redirected to VDA** (URL con reindirizzamento a VDA consentito) per evitare cicli di reindirizzamento infiniti.
> - I domini di primo livello non sono supportati. Ad esempio, `https://www.citrix.*` oppure `http://www.citrix.co*` non viene reindirizzato.

### Reindirizzamento del protocollo personalizzato dal VDA al client

Il reindirizzamento bidirezionale dei contenuti supporta il reindirizzamento di protocolli personalizzati da Citrix VDA al client. Sono supportati protocolli diversi da HTTP o HTTPS. Per configurare il reindirizzamento bidirezionale dei contenuti, vedere le istruzioni di configurazione.

In Web Studio, impostare il protocollo personalizzato in **Allowed URLs to be redirected to Client** (URL con reindirizzamento al client consentito).

> **NOTA:**
>
> - Il client deve avere un'applicazione registrata per gestire il protocollo. In caso contrario, l'URL reindirizza al client e l'avvio non riesce.
> - Gli URL di protocollo personalizzati immessi o avviati nei browser Chrome ed Edge non sono

> supportati e non sono reindirizzati.
> - I seguenti protocolli non sono supportati: `rtsp://`, `rtspu://`, `pnm://`, `mms://`.

### Altre considerazioni

- I requisiti e le configurazioni del browser sono applicabili solo al browser che avvia il reindirizzamento. Il browser di destinazione, in cui l'URL si apre dopo che il reindirizzamento è riuscito, non è considerato per il supporto. Quando si reindirizzano gli URL dal VDA a un client, una configurazione del browser supportata è richiesta solo sul VDA. Invece, quando si reindirizzano gli URL dal client a un VDA, una configurazione del browser supportata è richiesta solo sul client. Gli URL reindirizzati vengono trasferiti al browser predefinito configurato sulla macchina di destinazione, il client o il VDA, a seconda della direzione. L'utilizzo dello stesso tipo di browser sul VDA e il client NON è richiesto.
- Verificare che le regole di reindirizzamento non determinino una configurazione ciclica. Ad esempio, una politica VDA è impostata per reindirizzare `https://www.citrix.com` e il criterio del client è impostato per reindirizzare lo stesso URL, con conseguente loop infinito.
- Sono supportati solo gli URL con protocollo HTTP/HTTPS. Gli abbreviatori di URL non sono supportati.
- Il reindirizzamento da client a VDA richiede che il client Windows sia installato con diritti di amministratore.
- Se il browser di destinazione è già aperto, l'URL reindirizzato si apre in una nuova scheda. Altrimenti l'URL si apre in una nuova finestra del browser.
- Il reindirizzamento bidirezionale dei contenuti non funziona quando Local App Access (LAA) è abilitato.

## Accesso alle app locali e reindirizzamento URL

January 7, 2024

### Introduzione

L'accesso alle app locali integra perfettamente le applicazioni Windows installate localmente in un ambiente desktop ospitato senza passare da un desktop all'altro. Con l'accesso alle app locali, è possibile:

- Accedere alle applicazioni installate localmente su un laptop, PC o altro dispositivo fisico direttamente dal desktop virtuale.

- Fornire una soluzione flessibile per la distribuzione delle applicazioni. Se gli utenti dispongono di applicazioni locali che non è possibile virtualizzare o che l'IT non gestisce, tali applicazioni si comportano comunque come se fossero installate su un desktop virtuale.
- Eliminare la latenza a doppio hop quando le applicazioni sono ospitate separatamente dal desktop virtuale. È possibile farlo inserendo un collegamento all'applicazione pubblicata sul dispositivo Windows dell'utente.
- Utilizzare applicazioni quali:
  - Software per videoconferenze come GoToMeeting.
  - Applicazioni speciali o di nicchia che non sono ancora virtualizzate.
  - Applicazioni e periferiche che altrimenti trasferirebbero grandi quantità di dati da un dispositivo utente a un server e da un server al dispositivo utente. Ad esempio, masterizzatori DVD e sintonizzatori TV.

In Citrix Virtual Apps and Desktops, le sessioni desktop ospitate utilizzano il reindirizzamento URL per avviare le applicazioni della funzionalità di accesso alle app locali. Il reindirizzamento URL rende l'applicazione disponibile in più di un indirizzo URL. Avvia un browser locale (basato sull'elenco di blocco URL del browser) selezionando i collegamenti incorporati all'interno di un browser in una sessione desktop. Se si passa a un URL non presente nell'elenco di blocco, l'URL viene riaperto nella sessione desktop.

Il reindirizzamento URL funziona solo per le sessioni desktop, non per le sessioni di applicazioni. L'unica funzionalità di reindirizzamento che è possibile utilizzare per le sessioni di applicazione è il reindirizzamento del contenuto da host a client, ovvero un tipo di reindirizzamento FTA (File Type Association) del server. Questa FTA reindirizza determinati protocolli al client, ad esempio HTTP, HTTPS, RTSP o MMS. Ad esempio, se si aprono solo collegamenti incorporati con HTTP, i collegamenti vengono aperti direttamente con l'applicazione client. Gli elenchi di blocco o le liste consentite di URL non sono supportati.

Quando l'accesso alle app locali è abilitato, gli URL che per gli utenti vengono visualizzati come collegamenti da applicazioni eseguite localmente, da applicazioni ospitate dagli utenti o come collegamenti sul desktop vengono reindirizzati in uno dei modi seguenti:

- Dal computer dell'utente al desktop ospitato
- Dal server Citrix Virtual Apps and Desktops al computer dell'utente
- Ne viene eseguito il rendering nell'ambiente in cui vengono avviati (non reindirizzati)

Per specificare il percorso di reindirizzamento del contenuto di siti Web specifici, configurare l'elenco di blocco e la lista consentita di URL nel Virtual Delivery Agent. Tali elenchi contengono chiavi del Registro di sistema a più stringhe che specificano le impostazioni dei criteri di reindirizzamento URL. Per ulteriori informazioni, vedere Impostazioni dei criteri di accesso alle app locali.

Può essere eseguito il rendering degli URL sul VDA, con le seguenti eccezioni:

- Informazioni locali/geografiche: siti Web che richiedono informazioni sulle impostazioni internazionali, come msn.com o news.google.com (apre una pagina specifica per il paese in base all'area geografica). Ad esempio, se viene eseguito il provisioning del VDA da un centro dati nel Regno Unito e il client si connette dall'India, l'utente si aspetta di vedere in.msn.com. Invece, l'utente vede uk.msn.com.
- Contenuti multimediali: i siti Web con contenuti multimediali, quando ne viene eseguito il rendering sul dispositivo client, offrono agli utenti finali un'esperienza nativa e consentono inoltre di risparmiare larghezza di banda anche in reti ad alta latenza. Questa funzionalità reindirizza i siti con altri tipi di supporti, ad esempio Silverlight. Questo processo avviene in un ambiente sicuro. Ossia gli URL approvati dall'amministratore vengono eseguiti sul client, mentre gli altri URL vengono reindirizzati al VDA.

Oltre al reindirizzamento URL, è possibile utilizzare il reindirizzamento FTA. FTA avvia le applicazioni locali quando viene rilevato un file nella sessione. Se l'app locale viene avviata, deve avere accesso al file per aprirlo. Di conseguenza, è possibile aprire solo i file che risiedono in condivisioni di rete o su unità client (utilizzando il mapping delle unità client) tramite applicazioni locali. Ad esempio, quando si apre un file PDF, se un lettore PDF è un'app locale, il file si apre utilizzando quel lettore PDF. Poiché l'app locale può accedere direttamente al file, non vi è alcun trasferimento di rete del file tramite ICA per aprirlo.

### Requisiti, considerazioni e limitazioni

Supportiamo l'accesso alle app locali sui sistemi operativi validi per i VDA per i sistemi operativi Windows multisessione e per i VDA per i sistemi operativi Windows a sessione singola. L'accesso alle app locali richiede l'app Citrix Workspace per Windows (versione minima 4.1). Sono supportati i seguenti browser:

- Edge, ultima versione
- Firefox, ultima versione e rilascio del supporto esteso
- Chrome, ultima versione

Tenere presenti le considerazioni e le limitazioni seguenti quando si utilizza l'accesso alle app locali e il reindirizzamento URL.

- L'accesso alle app locali è progettato per desktop virtuali a schermo intero che occupano l'intero monitor:
  - L'esperienza utente può risultare confusa se si utilizza l'accesso alle app locali con un desktop virtuale che viene eseguito in modalità finestra o non copre tutti i monitor.
  - Più monitor: quando un monitor viene ingrandito, diventa il desktop predefinito per tutte le applicazioni avviate in quella sessione. Questa impostazione predefinita si verifica anche se le applicazioni successive si avviano in genere su un altro monitor.

  - La funzionalità supporta un VDA. Non vi è alcuna integrazione con più VDA simultanei.

- Alcune applicazioni possono comportarsi in modo imprevisto, con conseguenze per gli utenti:
  - Le lettere di unità potrebbero confondere gli utenti, ad esempio la C: del computer locale anziché l'unità C: del desktop virtuale.
  - Le stampanti disponibili nel desktop virtuale non sono disponibili per le applicazioni locali.
  - Le applicazioni che richiedono autorizzazioni elevate non possono essere avviate come applicazioni ospitate dal client.
  - Non esiste una gestione speciale per le applicazioni a istanza singola (ad esempio Windows Media Player).
  - Le applicazioni locali vengono visualizzate con il tema Windows del computer locale.
  - Le applicazioni a schermo intero non sono supportate. Queste applicazioni includono applicazioni che si aprono a schermo intero, come presentazioni di PowerPoint o visualizzatori di foto che occupano l'intero desktop.
  - L'accesso alle app locali copia le proprietà dell'applicazione locale (ad esempio i collegamenti sul desktop del client e il menu Start) sul VDA. Tuttavia, non copia altre proprietà, come i tasti di scelta rapida e gli attributi di sola lettura.
  - Le applicazioni che personalizzano la modalità di gestione dell'ordine delle finestre sovrapposte possono avere risultati imprevedibili. Ad esempio, alcune finestre potrebbero essere nascoste.
  - I collegamenti non sono supportati, tra cui Risorse del computer, Cestino, Pannello di controllo, collegamenti alle unità di rete e collegamenti alle cartelle.
  - I tipi di file e i file seguenti non sono supportati: tipi di file personalizzati, file senza programmi associati, file zip e file nascosti.
  - Il raggruppamento della barra delle applicazioni non è supportato per le applicazioni ospitate su client a 32 e 64 bit o le applicazioni VDA miste. Ossia, il raggruppamento di applicazioni locali a 32 bit con applicazioni VDA a 64 bit.
  - Le applicazioni non possono essere avviate utilizzando COM. Ad esempio, se si fa clic su un documento di Office incorporato da un'applicazione Office, l'avvio del processo non può essere rilevato e l'integrazione dell'applicazione locale ha esito negativo.

- Gli scenari a doppio hop, in cui un utente avvia un desktop virtuale da un'altra sessione di desktop virtuale, non sono supportati.
- Il reindirizzamento URL supporta solo URL espliciti (ovvero URL visualizzati nella barra degli indirizzi del browser o trovati utilizzando la navigazione nel browser, a seconda del browser).
- Il reindirizzamento URL funziona solo con le sessioni desktop, non con le sessioni delle applicazioni.
- La cartella desktop locale in una sessione VDA non consente agli utenti di creare file.
- Più istanze di un'applicazione in esecuzione localmente si comportano in base alle im-

postazioni della barra delle applicazioni impostate per il desktop virtuale. Tuttavia, i collegamenti alle applicazioni eseguite localmente non vengono raggruppati con istanze in esecuzione di tali applicazioni. Inoltre, non sono raggruppati con istanze in esecuzione di applicazioni ospitate o collegamenti alle applicazioni ospitate aggiunti. Gli utenti possono chiudere solo le finestre delle applicazioni in esecuzione localmente dalla barra delle applicazioni. Sebbene gli utenti possano aggiungere le finestre delle applicazioni locali alla barra delle applicazioni del desktop e al menu Start, le applicazioni potrebbero non essere avviate in modo coerente quando si utilizzano questi collegamenti.

- Se l'impostazione del criterio **Allow Local App Access (Consenti accesso alle app locali)** è **Abilitata**, il reindirizzamento del contenuto del browser non è supportato. Per impostazione predefinita, l'accesso alle app locali è vietato.

### Interazione con Windows

L'interazione dell'accesso alle app locali con Windows include i seguenti comportamenti.

- Comportamento dei collegamenti di Windows 8 e Windows Server 2012
  - Le applicazioni di Windows Store installate nel client non vengono enumerate come parte dei collegamenti dell'accesso alle app locali.
  - I file di immagine e video vengono aperti per impostazione predefinita utilizzando le applicazioni di Windows Store. Tuttavia, l'accesso alle app locali enumera le applicazioni di Windows Store e apre i collegamenti con le applicazioni desktop.
- Programmi locali
  - Per Windows 7, la cartella è disponibile nel menu Start.
  - Per Windows 8, Programmi locali è disponibile solo quando l'utente sceglie **Tutte le app** come categoria dalla schermata Start. Non tutte le sottocartelle vengono visualizzate in Programmi locali.
- Funzionalità grafiche di Windows 8 per le applicazioni
  - Le applicazioni desktop sono limitate all'area desktop e sono coperte dalla schermata Start e dalle applicazioni in stile Windows 8.
  - Le applicazioni dell'accesso alle app locali non si comportano come le applicazioni desktop in modalità multi-monitor. In modalità multi-monitor, la schermata Start e il desktop vengono visualizzati su monitor diversi.
- Reindirizzamento URL dell'accesso alle app locali e di Windows 8
  - Poiché Internet Explorer di Windows 8 non dispone di componenti aggiuntivi abilitati, utilizzare Internet Explorer desktop per abilitare il reindirizzamento degli URL.

- In Windows Server 2012, Internet Explorer disabilita i componenti aggiuntivi per impostazione predefinita. Per implementare il reindirizzamento URL, disabilitare la configurazione avanzata di Internet Explorer. Quindi reimpostare le opzioni di Internet Explorer ed eseguire il riavvio per assicurarsi che i componenti aggiuntivi siano abilitati per gli utenti standard.

## Configurare l'accesso alle app locali e il reindirizzamento URL

Per utilizzare l'accesso alle app locali e il reindirizzamento URL con l'app Citrix Workspace:

- Installare l'app Citrix Workspace sul computer client locale. È possibile abilitare entrambe le funzionalità durante l'installazione dell'app Citrix Workspace oppure abilitare il modello di accesso alle app locali utilizzando l'Editor Criteri di gruppo.
- Configurare l'impostazione dei criteri **Allow local app access** (Consenti accesso alle app locali) su **Enabled (Abilitato)**. È inoltre possibile configurare le impostazioni dei criteri degli elenchi di blocco e delle liste consentite di URL per il reindirizzamento degli URL. Per ulteriori informazioni, vedere Impostazioni dei criteri di accesso alle app locali.

### Abilitare l'accesso alle app locali e il reindirizzamento URL

Per abilitare l'accesso alle app locali per tutte le applicazioni locali, attenersi alla seguente procedura:

1. Accedere a Web Studio e fare clic su **Policies** nel riquadro a sinistra.
2. Nella barra delle azioni, fare clic su **Create Policy** (Crea criterio).
3. Nella finestra Create Policy (Crea criterio) digitare "Allow Local App Access"(Consenti accesso alle app locali) nella casella di ricerca, quindi fare clic su **Select** (Seleziona).
4. Nella finestra Edit Setting (Modifica impostazione), selezionare **Allowed (Consentita)**. Per impostazione predefinita, il criterio **Allow local app access (Consenti accesso alle app locali)** è vietato. Una volta consentita questa impostazione, il VDA consente all'utente finale di decidere se le applicazioni pubblicate e i collegamenti dell'accesso alle app locali sono ablitati nella sessione. Se questa impostazione è vietata, sia le applicazioni pubblicate che i collegamenti dell'accesso alle app locali non funzionano per il VDA. Questa impostazione del criterio si applica all'intero computer e al criterio di reindirizzamento URL.
5. Nella finestra Crea criterio digitare "URL redirection allow list"(Elenco consentito per il reindirizzamento URL) nella casella di ricerca, quindi fare clic su **Select** (Seleziona). L'elenco consentito per il reindirizzamento URL specifica gli URL da aprire nel browser predefinito della sessione remota.
6. Nella finestra Edit Setting (Modifica impostazione) fare clic su **Add (Aggiungi)** per aggiungere gli URL, quindi fare clic su **OK**.

7. Nella finestra Create Policy (Crea criterio), digitare "URL redirection block list"(Elenco di blocco per il reindirizzamento URL) nella casella di ricerca, quindi fare clic su **Select** (Seleziona). L'elenco di blocco per il reindirizzamento URL specifica gli URL reindirizzati al browser predefinito in esecuzione sull'endpoint.
8. Nella finestra Edit Setting (Modifica impostazione) fare clic su **Add (Aggiungi)** per aggiungere gli URL, quindi fare clic su **OK**.
9. Nella pagina Settings (Impostazioni) fare clic su **Next (Avanti)**.
10. Nella pagina Users and Machines (Utenti e computer) assegnare il criterio ai gruppi di consegna applicabili, quindi fare clic su **Next (Avanti)**.
11. Nella pagina Summary (Riepilogo) esaminare le impostazioni e fare clic su **Finish (Fine)**.

Per abilitare il reindirizzamento URL per tutte le applicazioni locali durante l'installazione dell'app Citrix Workspace, attenersi alla seguente procedura:

1. Abilitare il reindirizzamento URL quando si installa l'app Citrix Workspace per tutti gli utenti su un computer. In questo modo vengono registrati anche i componenti aggiuntivi del browser necessari per il reindirizzamento URL.
2. Dal prompt dei comandi eseguire il comando appropriato per installare l'app Citrix Workspace utilizzando una delle seguenti opzioni:
   - Per CitrixReceiver.exe, utilizzare `/ALLOW_CLIENTHOSTEDAPPSURL=1`.
   - Per CitrixReceiverWeb.exe, utilizzare `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

#### Attivare il modello dell'accesso alle app locali utilizzando l'Editor Criteri di gruppo

> **Nota:**
>
> - Prima di abilitare il modello dell'accesso alle app locali utilizzando l'Editor Criteri di gruppo, aggiungere i file del modello receiver.admx/adml all'oggetto Criteri di gruppo locale.
> - I file del modello dell'app Citrix Workspace per Windows sono disponibili nell'oggetto Criteri di gruppo locale nella cartella **Modelli amministrativi > Citrix Components (Componenti Citrix) > Citrix Workspace** solo quando si aggiunge CitrixBase.admx/CitrixBase.adml alla cartella %systemroot%\policyDefinitions.

Per abilitare il modello dell'accesso alle app locali utilizzando l'editor Criteri di gruppo, attenersi alla seguente procedura:

1. Eseguire **gpedit.msc**.
2. Andare a **Configurazione computer > Modelli amministrativi > Modelli amministrativi classici (ADM) > Citrix Components (Componenti Citrix) > Citrix Workspace > User Experience (Esperienza utente)**.
3. Fare clic su **Local App Access settings (Impostazioni di accesso alle app locali)**.

4. Selezionare **Enabled (Abilitate)**, quindi **Allow URL Redirection (Consenti reindirizzamento URL)**. Per il reindirizzamento URL, registrare i componenti aggiuntivi del browser utilizzando la riga di comando descritta nella sezione *Registrare i componenti aggiuntivi del browser* più oltre in questo articolo.

#### Fornire l'accesso solo alle applicazioni pubblicate

È possibile fornire l'accesso alle applicazioni pubblicate utilizzando l'Editor del Registro di sistema o l'SDK PowerShell.

Nell'Editor del Registro di sistema, vedere Accesso alle app locali per le applicazioni pubblicate nell'elenco delle funzionalità gestite tramite il Registro di sistema.

Per utilizzare l'SDK PowerShell:

1. Aprire PowerShell sul computer su cui è in esecuzione il Delivery Controller.
2. Immettere il seguente comando: `set-configsitemetadata -name "studio_clientHostedAp` `"-value "true"`.

Per avere accesso a **Add Local App Access Application (Aggiungi applicazione di accesso alle app locali)** in una distribuzione con servizio cloud, utilizzare Remote PowerShell SDK di Citrix DaaS. Per ulteriori informazioni, vedere Remote PowerShell SDK per Citrix DaaS.

1. Scaricare il programma di installazione:

   https://download.apps.cloud.com/CitrixPoshSdk.exe

2. Eseguire questi comandi:

   a) `asnp citrix.*`
   b) `Get-XdAuthentication`

3. Immettere il seguente comando: `set-configsitemetadata -name "studio_clientHostedAp` `"-value "true"`.

Dopo aver completato i passaggi precedenti applicabili, attenersi alla seguente procedura per continuare.

1. Accedere a Web Studio e selezionare **Applications** nel riquadro a sinistra.
2. Nel riquadro centrale superiore, fare clic con il pulsante destro del mouse sull'area vuota e selezionare **Add Local App Access Application (Aggiungi applicazione di accesso alle app locali)** dal menu di scelta rapida. È inoltre possibile fare clic su **Add Local App Access Application (Aggiungi applicazione di accesso alle app locali)** nella barra delle azioni. Per visualizzare l'opzione Add Local App Access Application (Aggiungi applicazione di accesso alle app locali) nella barra delle azioni, fare clic su **Refresh** (Aggiorna).

3. Pubblicare l'applicazione di accesso alle app locali.

    - Viene avviata la procedura guidata dell'accesso alle applicazioni locali con una pagina introduttiva, che è possibile rimuovere dai futuri avvii della procedura guidata.
    - La procedura guidata guida l'utente attraverso le pagine Groups (Gruppi), Location (Posizione), Identification (Identificazione), Delivery (Consegna) e Summary (Riepilogo) descritte di seguito. Al termine di ogni pagina, fare clic su **Next** (Avanti) fino a raggiungere la pagina Summary (Riepilogo).
    - Nella pagina Groups (Gruppi) selezionare uno o più gruppi di consegna in cui verranno aggiunte le nuove applicazioni, quindi fare clic su **Next** (Avanti).
    - Nella pagina Location (Posizione) digitare il percorso eseguibile completo dell'applicazione sul computer locale dell'utente e digitare il percorso della cartella in cui si trova l'applicazione. Citrix consiglia di utilizzare il percorso della variabile di ambiente di sistema, ad esempio %ProgramFiles(x86)%\Internet Explorer\iexplore.exe.
    - Nella pagina Identification (Identificazione) accettare i valori predefiniti o digitare le informazioni desiderate, quindi fare clic su **Next (Avanti)**.
    - Nella pagina Delivery (Consegna) configurare il modo in cui l'applicazione viene consegnata agli utenti, quindi fare clic su **Next (Avanti)**. È possibile specificare l'icona per l'applicazione selezionata. È inoltre possibile specificare se il collegamento all'applicazione locale sul desktop virtuale è visibile nel menu Start, sul desktop o in entrambi.
    - Nella pagina Summary (Riepilogo) esaminare le impostazioni, quindi fare clic su **Finish (Fine)** per uscire dalla procedura guidata dell'accesso alle applicazioni locali.

#### Registrare i componenti aggiuntivi del browser

> **Nota:**
>
> I componenti aggiuntivi del browser necessari per il reindirizzamento degli URL vengono registrati automaticamente quando si installa l'app Citrix Workspace dalla riga di comando utilizzando l'opzione /ALLOW_CLIENTHOSTEDAPPSURL=1.

È possibile utilizzare i seguenti comandi per registrare uno o tutti i componenti aggiuntivi e annullarne la registrazione:

- Per registrare componenti aggiuntivi su un dispositivo client: <*client-installation-folder*>\redirector.exe /reg<*browser*>
- Per annullare la registrazione dei componenti aggiuntivi su un dispositivo client: <*client-installation-folder*>\redirector.exe /unreg<*browser*>
- Per registrare componenti aggiuntivi in un VDA: <*VDAinstallation-folder*>\VDARedirector.exe /reg<*browser*>

- Per annullare la registrazione di componenti aggiuntivi in un VDA: <*VDAinstallation-folder*>\VDARedirector.exe /unreg<*browser*>

In cui <*browser*> è Internet Explorer, Firefox, Chrome o Tutti.

Ad esempio, il comando seguente registra i componenti aggiuntivi di Internet Explorer su un dispositivo con l'app Citrix Workspace in esecuzione.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

Il comando seguente registra tutti i componenti aggiuntivi in un VDA con sistema operativo Windows multisessione.

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

#### Intercettazione URL tra browser

- Per impostazione predefinita, Internet Explorer reindirizza l'URL specificato. Se l'URL non è incluso nell'elenco di blocco ma il browser o il sito Web lo reindirizza a un altro URL, l'URL finale non viene reindirizzato. Non viene reindirizzato anche se è incluso nell'elenco di blocco.

Perché il reindirizzamento URL funzioni correttamente, abilitare il componente aggiuntivo quando viene richiesto dal browser. Se i componenti aggiuntivi che utilizzano le opzioni Internet o i componenti aggiuntivi nel prompt sono disabilitati, il reindirizzamento URL non funziona correttamente.

- I componenti aggiuntivi di Firefox reindirizzano sempre gli URL.

Quando viene installato un componente aggiuntivo, Firefox chiede di consentire o impedire l'installazione del componente aggiuntivo in una nuova scheda. Consentire il componente aggiuntivo per garantire il corretto funzionamento della funzionalità.

- Il componente aggiuntivo di Chrome reindirizza sempre l'URL finale a cui si accede e non gli URL inseriti.

Le estensioni sono state installate esternamente. Quando si disabilita l'estensione, la funzionalità di reindirizzamento URL non funziona in Chrome. Se il reindirizzamento URL è richiesto in modalità di navigazione in incognito, consentire l'esecuzione dell'estensione in tale modalità nelle impostazioni del browser.

#### Configurare il comportamento dell'applicazione locale allo scollegamento e alla disconnessione

> **Nota:**
>
> Se non si esegue questa procedura per configurare le impostazioni, per impostazione predefinita le applicazioni locali continuano a essere eseguite quando un utente si scollega o si disconnette

> dal desktop virtuale. Dopo la riconnessione, le applicazioni locali vengono reintegrate se sono disponibili sul desktop virtuale.

Per configurare il comportamento dell'applicazione locale in caso di scollegamento e disconnessione, vedere Comportamento dell'applicazione locale allo scollegamento e alla disconnessione nell'elenco delle funzionalità gestite tramite il Registro di sistema.

## Considerazioni generiche sul reindirizzamento USB e sulle unità client

January 7, 2024

La tecnologia HDX offre **supporto ottimizzato** per i dispositivi USB più diffusi. Il supporto ottimizzato offre una migliore esperienza utente con migliori prestazioni ed efficienza della larghezza di banda su una WAN. Il supporto ottimizzato è solitamente l'opzione migliore, soprattutto in ambienti con latenza elevata o sensibili alla sicurezza.

La tecnologia HDX fornisce un **reindirizzamento USB generico** per dispositivi speciali che non dispongono di alcun supporto ottimizzato o dove questo non è adatto, ad esempio:

- Il dispositivo USB dispone di funzioni più avanzate che non fanno parte del supporto ottimizzato, come un mouse o una webcam con più pulsanti.
- Gli utenti hanno bisogno di funzioni che non fanno parte del supporto ottimizzato.
- Il dispositivo USB è un dispositivo specializzato, come apparecchiature di test e misurazione o un controller industriale.
- Un'applicazione richiede l'accesso diretto al dispositivo come dispositivo USB.
- La periferica USB ha solo un driver Windows disponibile. Ad esempio, un lettore di smart card potrebbe non avere un driver disponibile per l'app Citrix Workspace per Android.
- La versione dell'app Citrix Workspace non fornisce alcun supporto ottimizzato per questo tipo di dispositivo USB.

Con il reindirizzamento USB generico:

- Gli utenti non devono installare driver del dispositivo sul dispositivo utente.
- I driver del client USB sono installati sul computer VDA.

> **Importante:**
>
> - Il reindirizzamento USB generico può essere usato insieme al supporto ottimizzato. Se si abilita il reindirizzamento USB generico, configurare le impostazioni dei criteri dei dispositivi USB Citrix sia per il reindirizzamento USB generico che per il supporto ottimizzato.
> - L'impostazione dei criteri Citrix nelle regole di ottimizzazione dei dispositivi USB client è un'

> impostazione specifica per il reindirizzamento USB generico, per un particolare dispositivo USB. Non si applica al supporto ottimizzato come descritto qui.

### Considerazioni sulle prestazioni per i dispositivi USB

La latenza e la larghezza di banda della rete possono influire sull'esperienza utente e sul funzionamento dei dispositivi USB quando si utilizza il reindirizzamento USB generico per alcuni tipi di dispositivi USB. Ad esempio, i dispositivi sensibili all'orario potrebbero non funzionare correttamente su collegamenti a bassa larghezza di banda e a latenza elevata. Utilizzare invece il supporto ottimizzato, dove possibile.

Alcuni dispositivi USB richiedono un'elevata larghezza di banda per poter essere utilizzati, ad esempio un mouse 3D (utilizzato con app 3D che in genere richiedono un'elevata larghezza di banda). Se la larghezza di banda non può essere aumentata, potrebbe esssere possibile mitigare il problema ottimizzando l'utilizzo della larghezza di banda di altri componenti tramite le impostazioni dei criteri di larghezza di banda. Per ulteriori informazioni, vedere Impostazioni dei criteri di larghezza di banda per il reindirizzamento del dispositivo USB client e Impostazioni dei criteri delle connessioni multiflusso.

### Considerazioni sulla sicurezza per i dispositivi USB

Alcuni dispositivi USB sono sensibili alla sicurezza per natura, ad esempio i lettori di smart card, i lettori di impronte digitali e i signature pad. Altri dispositivi USB, come i dispositivi di archiviazione USB, possono essere utilizzati per trasmettere dati potenzialmente sensibili.

I dispositivi USB vengono spesso utilizzati per distribuire malware. La configurazione dell'app Citrix Workspace e di Citrix Virtual Apps and Desktops può ridurre, ma non eliminare, i rischi derivanti da questi dispositivi USB. Questa situazione è valida sia che venga utilizzato il reindirizzamento USB generico sia che venga utilizzato il supporto ottimizzato.

> **Importante:**
>
> Per i dispositivi e i dati sensibili alla sicurezza, proteggere sempre la connessione HDX utilizzando TLS o IPsec.
>
> Abilitare il supporto solo per i dispositivi USB necessari. Configurare sia il reindirizzamento USB generico che il supporto ottimizzato per soddisfare questa esigenza.
>
> Fornire indicazioni agli utenti per l'uso sicuro dei dispositivi USB:
>
> - Utilizzare solo dispositivi USB che sono stati ottenuti da una fonte affidabile.
> - Non lasciare i dispositivi USB incustoditi in ambienti aperti, ad esempio un'unità flash in un Internet café.

> • Spiegare i rischi derivanti dall'utilizzo di un dispositivo USB su più di un computer.

### Compatibilità con il reindirizzamento USB generico

Il reindirizzamento USB generico è supportato per i dispositivi USB 2.0 e precedenti. Il reindirizzamento USB generico è supportato anche per i dispositivi USB 3.0 collegati a una porta USB 2.0 o USB 3.0. Il reindirizzamento USB generico non supporta le funzionalità USB introdotte in USB 3.0, ad esempio la super velocità.

Queste app Citrix Workspace supportano il reindirizzamento USB generico:

- App Citrix Workspace per Windows, vedere Configurazione della distribuzione delle applicazioni.
- App Citrix Workspace per Mac, vedere App Citrix Workspace per Mac.
- App Citrix Workspace per Linux, vedere Ottimizzare.
- App Citrix Workspace per Chrome OS, vedere App Citrix Workspace per Chrome.

Per le versioni dell'app Citrix Workspace, vedere la matrice delle funzionalità dell'app Citrix Workspace.

Se si utilizzano versioni precedenti dell'app Citrix Workspace, vedere la documentazione dell'app Citrix Workspace per verificare che il reindirizzamento USB generico sia supportato. Per eventuali restrizioni sui tipi di dispositivi USB supportati, consultare la documentazione dell'app Citrix Workspace.

Il reindirizzamento USB generico è supportato per le sessioni desktop da VDA per sistema operativo a sessione singola versione 7.6 fino alla versione corrente.

Il reindirizzamento USB generico è supportato per le sessioni desktop da VDA per sistema operativo multisessione dalla versione 7.6 fino alla versione corrente, con le seguenti restrizioni:

- Il VDA deve eseguire Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 o Windows Server 2022.
- I driver dei dispositivi USB devono essere completamente compatibili con l'host sessione Desktop remoto (RDSH) per il sistema operativo del VDA (Windows 2012 R2), incluso il supporto completo della virtualizzazione.

Alcuni tipi di dispositivi USB non sono supportati per il reindirizzamento USB generico perché non sarebbe utile reindirizzarli:

- Modem USB.
- Schede di rete USB.
- Hub USB. I dispositivi USB collegati agli hub USB vengono gestiti singolarmente.

- Porte COM virtuali USB. Utilizzare il reindirizzamento della porta COM anziché il reindirizzamento USB generico.

Per informazioni sui dispositivi USB testati con il reindirizzamento USB generico, vedere Citrix Ready Marketplace. Alcuni dispositivi USB non funzionano correttamente con il reindirizzamento USB generico.

### Configurare il reindirizzamento USB generico

È possibile controllare e configurare separatamente quali tipi di dispositivi USB utilizzano il reindirizzamento USB generico:

- Sul VDA, utilizzando le impostazioni dei criteri Citrix. Per ulteriori informazioni, vedere Reindirizzamento delle unità client e dei dispositivi utente e Impostazioni dei criteri dei dispositivi USB nella sezione Riferimenti per le impostazioni dei criteri.
- Nell'app Citrix Workspace, utilizzando meccanismi dipendenti dall'app Citrix Workspace. Ad esempio, un modello amministrativo controlla le impostazioni del Registro di sistema che configurano l'app Citrix Workspace per Windows. Per impostazione predefinita, il reindirizzamento USB è consentito per determinate classi di dispositivi USB e negato per altri. Per ulteriori informazioni, vedere Configurare nella documentazione dell'app Citrix Workspace per Windows.

Questa configurazione separata offre flessibilità. Ad esempio:

- Se due diverse organizzazioni o reparti sono responsabili dell'app Citrix Workspace e del VDA, possono applicare il controllo separatamente. Questa configurazione si applica quando un utente di un'organizzazione accede a un'applicazione in un'altra organizzazione.
- Le impostazioni dei criteri Citrix possono controllare i dispositivi USB consentiti solo per determinati utenti o per gli utenti che si connettono solo tramite una LAN (anziché tramite Citrix Gateway).

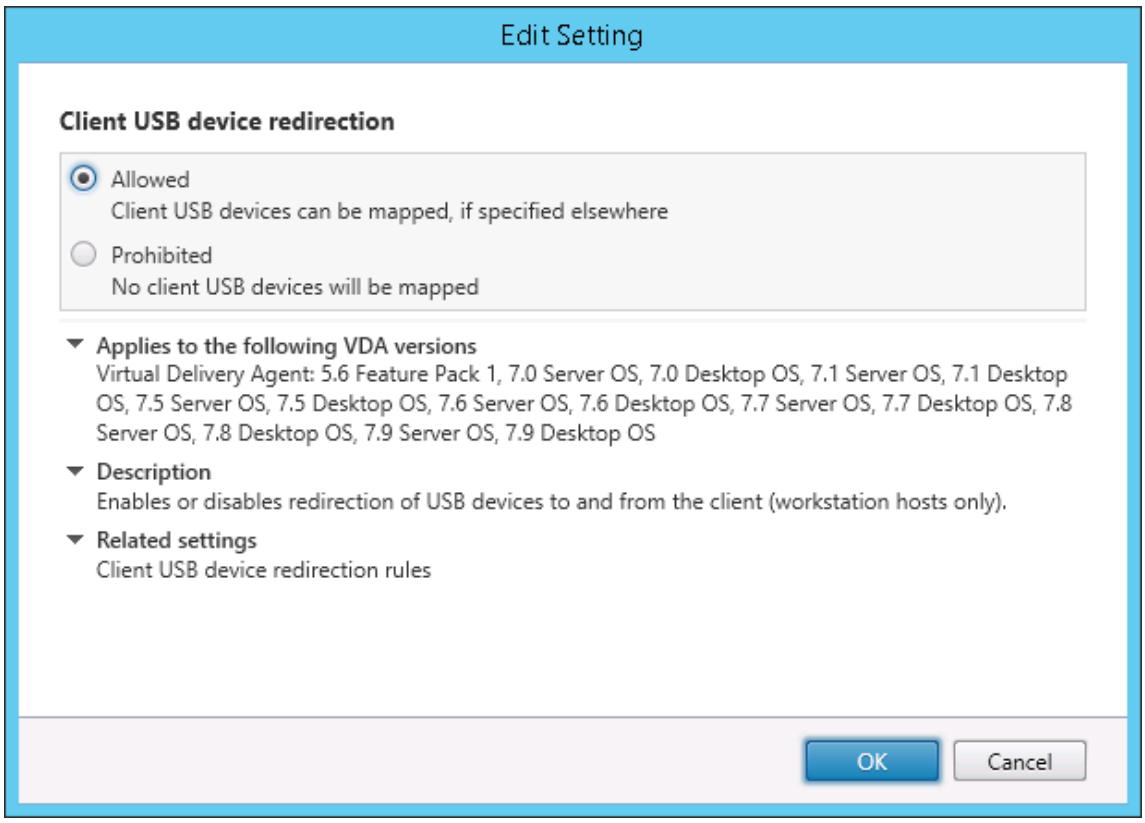
### Abilitare il reindirizzamento USB generico

Per abilitare il reindirizzamento USB generico e non richiedere il reindirizzamento manuale da parte dell'utente, configurare sia le impostazioni dei criteri Citrix che le preferenze di connessione dell'app Citrix Workspace.

Nelle impostazioni dei criteri Citrix:

1. Aggiungere il reindirizzamento del dispositivo USB client a un criterio e impostarne il valore su **Consentito**.

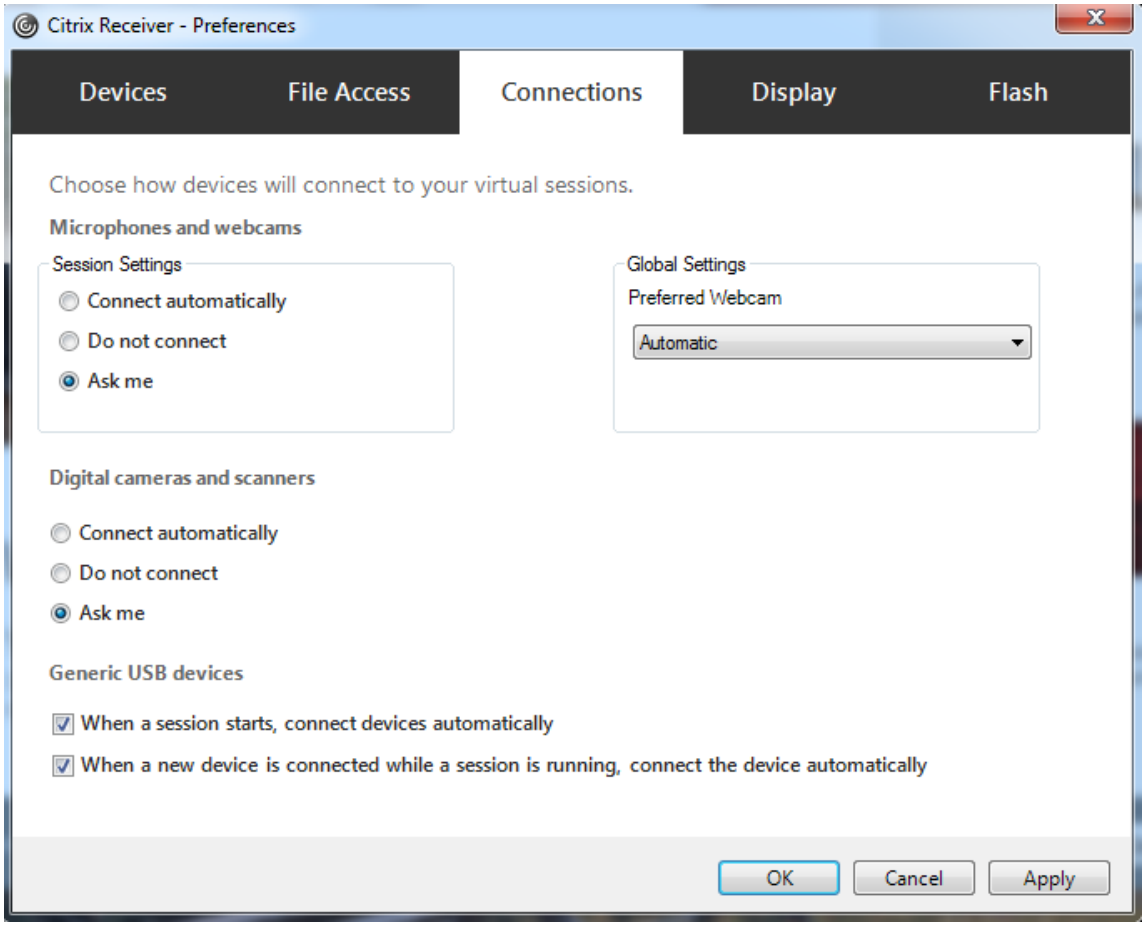



2. (Facoltativo) Per aggiornare l'elenco dei dispositivi USB disponibili per il reindirizzamento, aggiungere l'impostazione Client USB device redirection rules (Reole di reindirizzamenot dispositivo USB client) a un criterio e specificare le regole dei criteri USB.

   Una volta completate le impostazioni dei criteri, nell'app Citrix Workspace:

3. Specificare che i dispositivi siano collegati automaticamente senza reindirizzamento manuale. È possibile eseguire questa operazione utilizzando un modello amministrativo o nell'app Citrix Workspace per **Windows > Preferenze > Connessioni**.




Se nel passaggio precedente sono state specificate le regole dei criteri USB per il VDA, specificare le stesse regole dei criteri per l'app Citrix Workspace.

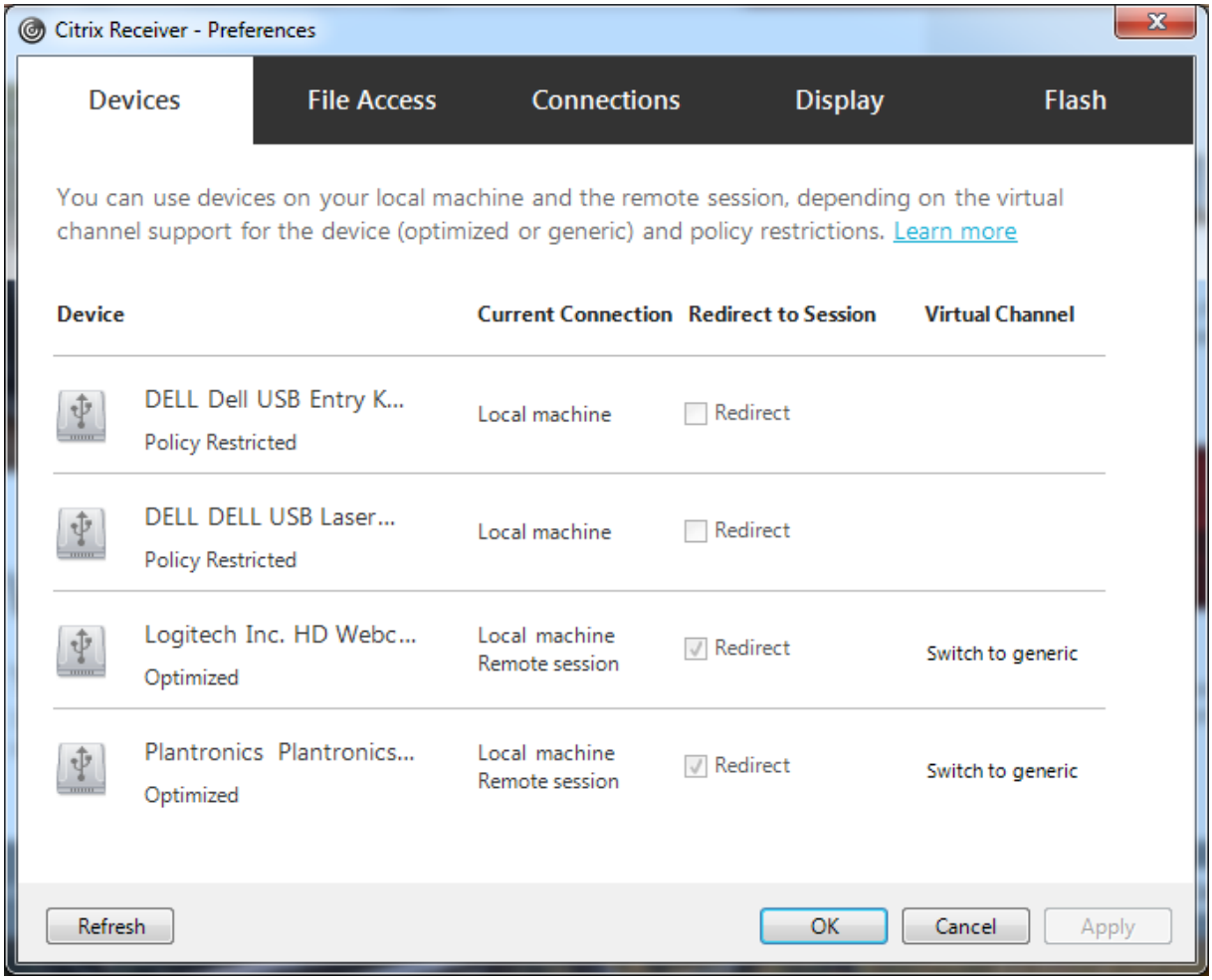
Per i thin client, consultare il produttore per informazioni dettagliate sul supporto USB e per eventuali configurazioni richieste.

### Configurazione dei tipi di dispositivi USB disponibili per il reindirizzamento USB generico

I dispositivi USB vengono reindirizzati automaticamente quando il supporto USB è abilitato e le impostazioni delle preferenze utente USB sono impostate per collegare automaticamente i dispositivi USB. Anche i dispositivi USB vengono reindirizzati automaticamente quando la barra di connessione non è presente.

Gli utenti possono reindirizzare esplicitamente i dispositivi che non vengono reindirizzati automaticamente selezionando i dispositivi dall'elenco dei dispositivi USB. Per ulteriori informazioni, l'articolo della guida per l'utente dell'app Citrix Workspace per Windows, Visualizzare i dispositivi in Desktop Viewer.




Per utilizzare il reindirizzamento USB generico anziché il supporto ottimizzato, è possibile:

- Nell'app Citrix Workspace, selezionare manualmente il dispositivo USB per utilizzare il reindirizzamento USB generico e scegliere **Switch to generic (Passa a generico)** dalla scheda Devices (Dispositivi) della finestra di dialogo Preferences (Preferenze).
- Selezionare automaticamente il dispositivo USB per utilizzare il reindirizzamento USB generico, configurando il reindirizzamento automatico per il tipo di dispositivo USB (ad esempio, AutoRedirectStorage=1) e impostare le impostazioni delle preferenze utente USB per collegare automaticamente i dispositivi USB. Per ulteriori informazioni, vedere Configurare il reindirizzamento automatico dei dispositivi USB.

> **Nota:**
>
> Configurare il reindirizzamento USB generico per l'utilizzo con una webcam solo se la webcam risulta incompatibile con il reindirizzamento multimediale HDX.

Per evitare che i dispositivi USB vengano elencati o reindirizzati, è possibile specificare le regole dei dispositivi per l'app Citrix Workspace e il VDA.

Per il reindirizzamento USB generico, è necessario conoscere almeno la classe e la sottoclasse del dispositivo USB. Non tutti i dispositivi USB utilizzano la relativa classe e sottoclasse ovvie di dispositivi USB. Ad esempio:

- Le penne utilizzano la classe del mouse.
- I lettori di smart card possono utilizzare la classe di dispositivo HID o definita dal fornitore.

Per un controllo più preciso, è necessario conoscere l'ID fornitore, l'ID prodotto e l'ID versione. È possibile ottenere queste informazioni dal fornitore del dispositivo.

> **Importante:**
>
> I dispositivi USB dannosi potrebbero presentare caratteristiche dei dispositivi USB che non corrispondono all'utilizzo previsto. Le regole del dispositivo non hanno lo scopo di impedire questo comportamento.

È possibile controllare i dispositivi USB disponibili per il reindirizzamento USB generico specificando le regole di reindirizzamento dei dispositivi USB, per ignorare le regole dei criteri USB predefinite.

Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops):

- Nella maggior parte dei casi, scaricare la Citrix Group Policy Management Console MSI (`CitrixGroupPolicyManagement_x64.msi`) e installarla nel sistema Active Directory, quindi gestire i criteri di gruppo AD. Non installare MSI su un VDA.
- Per l'app Citrix Workspace per Windows, modificare il registro del dispositivo utente. Nel supporto di installazione è incluso un modello amministrativo (file ADM) che consente di modificare il dispositivo utente tramite Criteri di gruppo di Active Directory: dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

Citrix Virtual Apps and Desktops locale:

- Per il VDA, modificare le regole di override dell'amministratore per i computer con sistema operativo multisessione tramite le regole dei criteri di gruppo. La Console Gestione Criteri di gruppo è inclusa nel supporto di installazione:
  - x64: dvd root `\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86: dvd root `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`
- Per l'app Citrix Workspace per Windows, modificare il registro del dispositivo utente. Nel supporto di installazione è incluso un modello amministrativo (file ADM) che consente di modificare il dispositivo utente tramite Criteri di gruppo di Active Directory: dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Le regole predefinite del prodotto sono memorizzate in HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Client\GenericUSB. Non modificare queste regole predefinite del prodotto. Utilizzarle invece come guida per la creazione di regole di override dell'amministratore, come illustrato più avanti in questo articolo. Le regole di override dell'Oggetto Criteri di gruppo vengono valutate prima delle regole predefinite del prodotto.

Le regole di override dell'amministratore sono memorizzate in HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\
Le regole dei criteri Criteri di gruppo hanno il formato **{Allow:|Deny:}** seguito da un insieme di espressioni *tag=value* separate da uno spazio bianco.

Sono supportati i seguenti tag:

| Tag | Descrizione |
|---|---|
| VID | ID fornitore del descrittore del dispositivo |
| PID | ID prodotto del descrittore del dispositivo |
| REL | ID versione del descrittore del dispositivo |
| Class | Classe del descrittore del dispositivo o di un descrittore di interfaccia; vedere il sito Web USB alla pagina http://www.usb.org/ per i codici di classe USB disponibili |
| SubClass | Sottoclasse del descrittore del dispositivo o di un descrittore di interfaccia |
| Prot | Protocollo del descrittore del dispositivo o di un descrittore di interfaccia |

Durante la creazione di regole dei criteri, tenere presente quanto segue:

- Le regole non fanno distinzione tra maiuscole e minuscole.
- Le regole possono avere un commento facoltativo alla fine, introdotto da #. Non è necessario un delimitatore e il commento viene ignorato per scopi di corrispondenza.
- Le righe di commento vuote e pure vengono ignorate.

- Lo spazio bianco viene utilizzato come separatore, ma non può essere visualizzato al centro di un numero o di un identificatore. Ad esempio, Deny: Class = 08 SubClass=05 è una regola valida, ma non Deny: Class=0 Sub Class=05.
- I tag devono utilizzare l'operatore corrispondente =. Ad esempio, VID=1230.
- Ogni regola deve iniziare su una nuova riga o far parte di un elenco separato da punto e virgola.

> **Nota:**
>
> - A partire dalla versione 2212 di Citrix Virtual Apps and Desktops, alcuni dispositivi USB non possono utilizzare la funzione di reindirizzamento USB generico. È necessario aggiungere questi dispositivi utilizzando esplicitamente i rispettivi Vendor ID (VID) e Product ID (PID).
> - Se si utilizza il file del modello ADM, è necessario creare regole su un'unica riga, come elenco separato da punto e virgola.

Esempi:

- Nell'esempio seguente viene illustrata una regola dei criteri USB definita dall'amministratore per gli identificatori di fornitore e prodotto:

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
 Deny: VID=046D # Deny all Logitech products
```

- Nell'esempio seguente viene illustrata una regola dei criteri USB definita dall'amministratore per una classe, una sottoclasse e un protocollo definiti:

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF
# Allow all USB-Miscellaneous devices
```

### Utilizzare e rimuovere dispositivi USB

Gli utenti possono collegare un dispositivo USB prima o dopo l'avvio di una sessione virtuale.

Quando si utilizza l'app Citrix Workspace per Windows, si applicano le seguenti condizioni:

- I dispositivi collegati dopo l'inizio di una sessione vengono visualizzati immediatamente nel menu USB di Desktop Viewer.
- Se un dispositivo USB non viene reindirizzato correttamente, è possibile provare a risolvere il problema aspettando di connettere il dispositivo fino all'avvio della sessione virtuale.
- Per evitare la perdita di dati, utilizzare l'icona "Rimozione sicura dell'hardware"di Windows prima di rimuovere il dispositivo USB.

### Controlli di sicurezza per dispositivi di archiviazione di massa USB

Il supporto ottimizzato è fornito per i dispositivi di archiviazione di massa USB. Questo supporto fa parte della mappatura delle unità client di Citrix Virtual Apps and Desktops. Le unità sul dispositivo utente vengono mappate automaticamente alle lettere di unità sul desktop virtuale quando gli utenti accedono. Le unità vengono visualizzate come cartelle condivise con lettere di unità mappate. Per configurare il mapping delle unità client, utilizzare l'impostazione **Client removable drives (Unità client rimovibili)**. Questa impostazione si trova nella sezione Impostazioni dei criteri di reindirizzamento file delle impostazioni dei criteri ICA.

Con i dispositivi di archiviazione di massa USB, è possibile utilizzare la mappatura delle unità client oppure il reindirizzamento USB generico oppure entrambi. È possibile controllarli utilizzando i criteri Citrix. Le principali differenze sono:

| Funzionalità | Mappatura unità client | Reindirizzamento USB generico |
|---|---|---|
| Attivato per impostazione predefinita | Sì | No |
| Accesso in sola lettura configurabile | Sì | No |
| Accesso ai dispositivi crittografati | Sì, se la crittografia viene sbloccata prima dell'accesso al dispositivo | Sì |
| Dispositivi BitLocker To Go | No | No |
| Eliminazione sicura del dispositivo durante una sessione | No | Sì, a condizione che gli utenti seguano le raccomandazioni del sistema operativo per la rimozione sicura |

Se sia il reindirizzamento USB generico che i criteri di mappatura delle unità client sono abilitati e viene inserito un dispositivo di archiviazione di massa prima o dopo l'avvio di una sessione, questo viene reindirizzato utilizzando la mappatura delle unità client. Se sia il reindirizzamento USB generico che i criteri di mappatura delle unità client sono abilitati e un dispositivo è configurato per il reindirizzamento automatico e viene inserito un dispositivo di archiviazione di massa prima o dopo l'avvio di una sessione, viene reindirizzato utilizzando il reindirizzamento USB generico. Per ulteriori informazioni, vedere l'articolo CTX123015 del Knowledge Center.

> **Nota:**

> Il reindirizzamento USB è supportato su connessioni a larghezza di banda inferiore, ad esempio 50 Kbps. Tuttavia, la copia di file di grandi dimensioni non funziona.

# Stampa

January 7, 2024

La gestione delle stampanti nell'ambiente è un processo multistadio:

1. Acquisire familiarità con i concetti di stampa, se non la si ha già.
2. Pianificare l'architettura di stampa. Ciò include l'analisi delle esigenze aziendali, dell'infrastruttura di stampa esistente, del modo in cui gli utenti e le applicazioni interagiscono con la stampa oggi e di quale modello di gestione della stampa si applica meglio all'ambiente in uso.
3. Configurare l'ambiente di stampa selezionando un metodo di provisioning della stampante e quindi creando criteri per la distribuzione del progetto di stampa. Aggiornare i criteri quando vengono aggiunti nuovi dipendenti o server.
4. Verificare una configurazione di stampa pilota prima di distribuirla agli utenti.
5. Effettuare la manutenzione dell'ambiente di stampa Citrix gestendo i driver della stampante e ottimizzando le prestazioni di stampa.
6. Risolvere i problemi che potrebbero sorgere.

## Nozioni relative alla stampa

Prima di iniziare a pianificare la distribuzione, assicurarsi di comprendere questi concetti fondamentali per la stampa:

- I tipi di provisioning delle stampanti disponibili
- Come vengono instradati i processi di stampa
- Le nozioni di base della gestione dei driver della stampante

I concetti di stampa si basano sui concetti di stampa di Windows. Per configurare e gestire correttamente la stampa nel proprio ambiente, è necessario comprendere come funziona la stampa di rete e client Windows e come questo si traduce in un comportamento di stampa in questo ambiente.

## Processo di stampa

In questo ambiente, tutta la stampa viene avviata (dall'utente) su macchine che ospitano applicazioni. I processi di stampa vengono reindirizzati al dispositivo di stampa tramite il server di stampa di rete o il dispositivo dell'utente.

Non esiste un'area di lavoro permanente per gli utenti di desktop e applicazioni virtuali. Al termine di una sessione, l'area di lavoro dell'utente viene eliminata, pertanto tutte le impostazioni devono essere ricostruite all'inizio di ogni sessione. Di conseguenza, ogni volta che un utente avvia una nuova sessione, il sistema deve ricostruire l'area di lavoro dell'utente.

Quando un utente stampa:

- Determina quali stampanti fornire all'utente. Questo è noto come provisioning della stampante.
- Ripristina le preferenze di stampa dell'utente.
- Determina quale stampante è quella predefinita per la sessione.

È possibile personalizzare la modalità di esecuzione di queste attività configurando le opzioni per il provisioning della stampante, il routing dei processi di stampa, la conservazione delle proprietà della stampante e la gestione dei driver. Assicurarsi di valutare in che modo le varie impostazioni delle opzioni possono modificare le prestazioni della stampa nel proprio ambiente e l'esperienza utente.

### Provisioning della stampante

Il processo che rende disponibili le stampanti in una sessione è noto come provisioning. Il provisioning della stampante viene in genere gestito dinamicamente. Ossia, le stampanti visualizzate in una sessione non sono predeterminate e memorizzate. Le stampanti vengono invece assemblate, in base ai criteri, poiché la sessione viene creata durante l'accesso e la riconnessione. Di conseguenza, le stampanti possono cambiare in base ai criteri, alla posizione dell'utente e ai cambiamenti della rete, a condizione che si riflettano in criteri. Pertanto, gli utenti che si trasferiscono in una posizione diversa potrebbero osservare cambiamenti dell'area di lavoro.

Il sistema monitora inoltre le stampanti lato client e regola dinamicamente le stampanti create automaticamente durante la sessione in base alle aggiunte, alle eliminazioni e alle modifiche apportate alle stampanti lato client. Questo rilevamento dinamico delle stampanti è utile per gli utenti mobili quando si connettono da vari dispositivi.

I metodi più comuni di provisioning delle stampanti sono:

- **Universal Print Server**: Citrix Universal Print Server fornisce supporto di stampa universale per le stampanti di rete. Universal Print Server utilizza il driver di stampa universale. Questa soluzione consente di utilizzare un singolo driver su un sistema operativo multisessione per consentire la stampa in rete da qualsiasi dispositivo.

Citrix consiglia Citrix Universal Print Server per gli scenari di server di stampa remoti. Universal Print Server trasferisce il lavoro di stampa sulla rete in un formato ottimizzato e compresso, riducendo al minimo l'utilizzo della rete e migliorando l'esperienza utente.

La funzionalità Universal Print Server comprende:

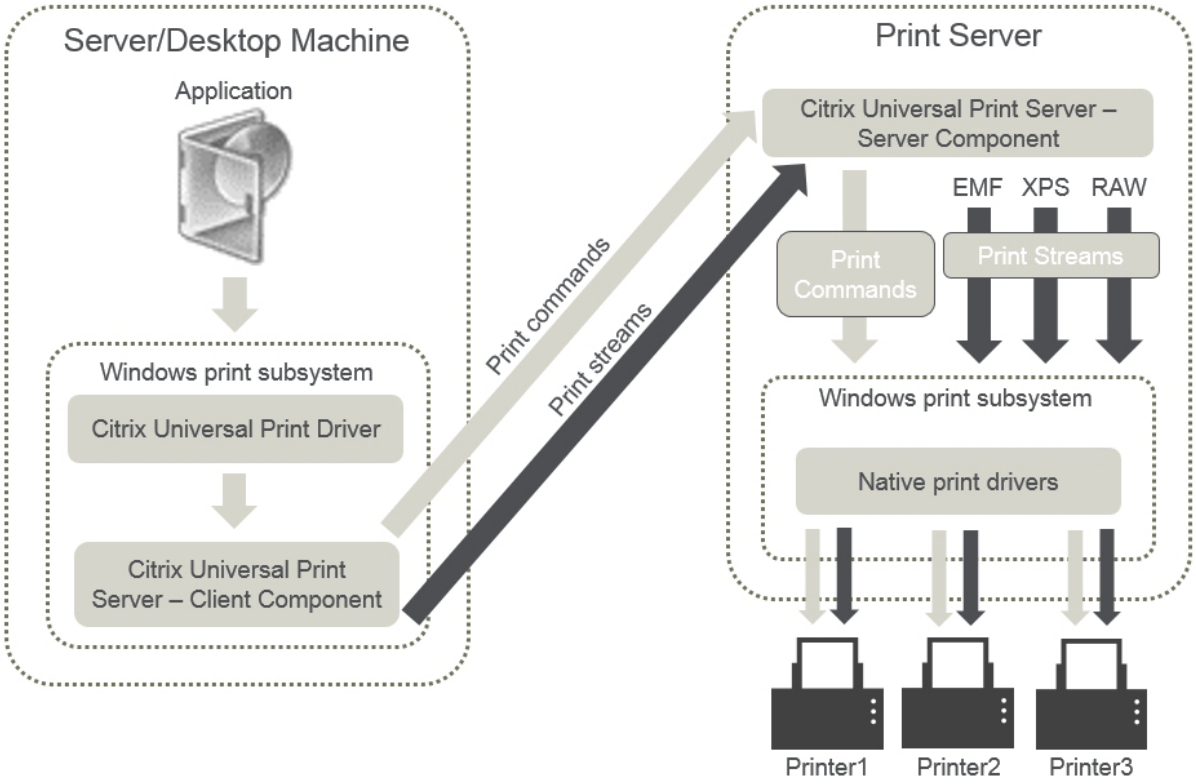
 

Un componente client, **UPClient**: Abilita UPClient su ogni computer del sistema operativo multisessione che esegue il provisioning di stampanti di rete di sessione e utilizza il driver di stampa Universal.

Un componente server, **UPServer**: Installa UPServer su ogni server di stampa che esegue il provisioning delle stampanti di rete di sessione e utilizza il driver di stampa Universal per le stampanti di sessione (indipendentemente dal fatto che le stampanti di sessione siano dotate o meno di provisioning centralizzato).

Per i requisiti e i dettagli di configurazione di Universal Print Server, fare riferimento ai requisiti di sistema e agli articoli sull'installazione.

Nella figura seguente viene illustrato il flusso di lavoro tipico di una stampante di rete in un ambiente che utilizza Universal Print Server.




Quando si attiva Citrix Universal Print Server, tutte le stampanti di rete collegate lo utilizzano automaticamente tramite il rilevamento automatico.

- **Creazione automatica**: *Creazione automatica* si riferisce alle stampanti create automaticamente all'inizio di ogni sessione. È possibile creare automaticamente sia stampanti di rete remote che stampanti client collegate localmente. Prendere in considerazione la possibilità di creare automaticamente solo la stampante client predefinita per ambienti con un numero elevato di stampanti per utente. La creazione automatica di un numero minore di stampanti dà meno sovraccarico (memoria e CPU) sulle macchine del sistema operativo multisessione.

Ridurre al minimo le stampanti create automaticamente può anche ridurre i tempi di accesso degli utenti.

Le stampanti create automaticamente si basano su:

- Le stampanti installate sul dispositivo dell'utente.
- Eventuali criteri applicabili alla sessione.

  Le impostazioni dei criteri di creazione automatica consentono di limitare il numero o il tipo di stampanti create automaticamente. Per impostazione predefinita, le stampanti sono disponibili nelle sessioni quando si configurano automaticamente tutte le stampanti sul dispositivo utente, incluse le stampanti collegate localmente e quelle di rete.

Dopo che l'utente termina la sessione, le stampanti di quella sessione vengono eliminate.

La creazione automatica di client e stampanti di rete comporta manutenzione. Ad esempio, per aggiungere una stampante è necessario:

- Aggiornare l'impostazione del criterio Stampanti sessione.
- Aggiungere il driver a tutte le macchine del sistema operativo multisessione mediante l'impostazione del mapping dei driver della stampante e dei criteri di compatibilità.

## Instradamento del processo di stampa

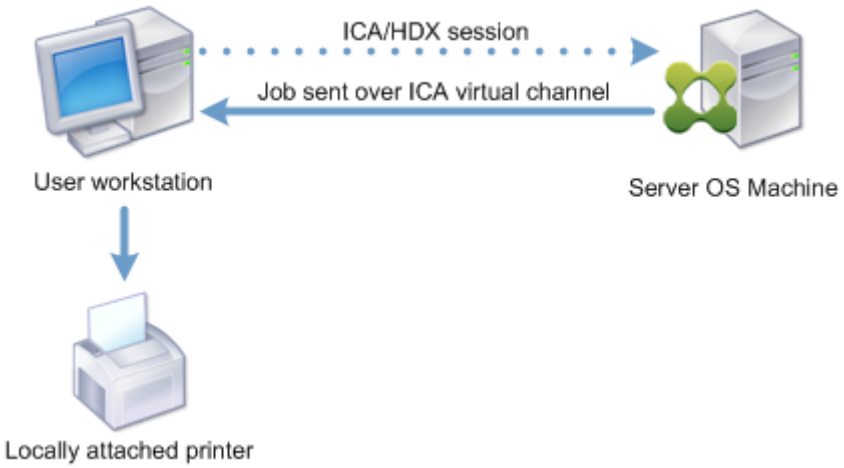
Il termine percorso di stampa comprende sia il percorso in base al quale vengono instradati i processi di stampa sia la posizione in cui viene effettuato lo spooling dei processi di stampa. Entrambi gli aspetti di questo concetto sono importanti. L'instradamento influisce sul traffico di rete. Lo spooling influisce sull'utilizzo delle risorse locali sul dispositivo che elabora il processo.

In questo ambiente, i processi di stampa possono seguire due percorsi per raggiungere un dispositivo di stampa: tramite il client o tramite un server di stampa di rete. Tali percorsi vengono denominati percorso di stampa client e percorso di stampa in rete. Il percorso scelto per impostazione predefinita dipende dal tipo di stampante utilizzata.

### Stampanti collegate localmente

Il sistema instrada i processi alle stampanti collegate localmente dal computer del sistema operativo multisessione, attraverso il client e quindi al dispositivo di stampa. Il protocollo ICA ottimizza e comprime il traffico dei processi di stampa. Quando un dispositivo di stampa è collegato localmente al dispositivo dell'utente, i processi di stampa vengono instradati sul canale virtuale ICA.




**Stampanti di rete**

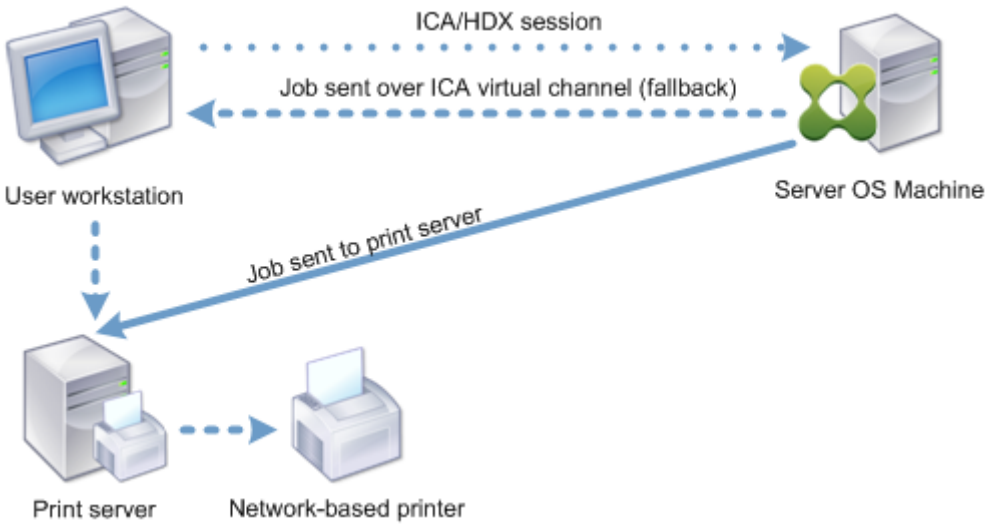
Per impostazione predefinita, tutti i processi di stampa destinati alle stampanti di rete vengono instradati dal computer del sistema operativo multisessione, attraverso la rete e direttamente al server di stampa. Tuttavia, i processi di stampa vengono instradati automaticamente tramite la connessione ICA nelle seguenti situazioni:

- Se il desktop virtuale o l'applicazione non è in grado di contattare il server di stampa.
- Se il driver della stampante nativa non è disponibile sul computer del sistema operativo multisessione.

Se Universal Print Server non è abilitato, la configurazione del percorso di stampa client per la stampa in rete è utile per le connessioni a larghezza di banda ridotta, ad esempio le reti ad area larga, che possono trarre vantaggio dall'ottimizzazione e dalla compressione del traffico derivante dall'invio di processi tramite la connessione ICA.

Il percorso di stampa client consente inoltre di limitare il traffico o di limitare la larghezza di banda allocata per i processi di stampa. Se non è possibile instradare i processi attraverso il dispositivo utente, ad esempio nel caso dei thin client privi di funzionalità di stampa, la qualità del servizio deve essere configurata in modo da dare priorità al traffico ICA/HDX e garantire una buona esperienza utente durante la sessione.




## Gestione dei driver di stampa

Il driver di stampa Citrix Universal Printer Driver (UPD) è un driver di stampa indipendente dal dispositivo, compatibile con la maggior parte delle stampanti. Il Citrix UPD è composto da due componenti:

**Componente server**. L'UPD Citrix viene installato nell'ambito dell'installazione del VDA di Citrix Virtual Apps and Desktops. Il VDA installa i seguenti driver con Citrix UPD: "Citrix Universal Printer"(driver EMF) e "Citrix XPS Universal Printer"(driver XPS).

| Name | Processor | Type |
|---|---|---|
| Citrix Universal Printer | x64 | Type 3 - User Mode |
| Citrix XPS Universal Printer | x64 | Type 3 - User Mode |

I programmi di installazione VDA non offrono più opzioni per controllare l'installazione del driver della stampante PDF di Universal Print Server. Il driver della stampante PDF ora viene sempre installato automaticamente. Quando si esegue l'aggiornamento alla versione 7.17 VDA (o una versione supportata successiva), qualsiasi driver della stampante Citrix PDF installato in precedenza viene automaticamente rimosso e sostituito con la versione più recente.

Quando viene avviato un processo di stampa, il driver registra l'output dell'applicazione e lo invia, senza alcuna modifica del dispositivo endpoint.

**Componente client**. L'UPD Citrix viene installato nell'ambito dell'installazione dell'app Citrix Workspace. Recupera il flusso di stampa in ingresso per la sessione di Citrix Virtual Apps and Desktops. Inoltra quindi il flusso di stampa al sottosistema di stampa locale in cui viene eseguito il rendering del lavoro di stampa utilizzando i driver della stampante specifici del dispositivo.

L'UPD Citrix supporta i seguenti formati di stampa:

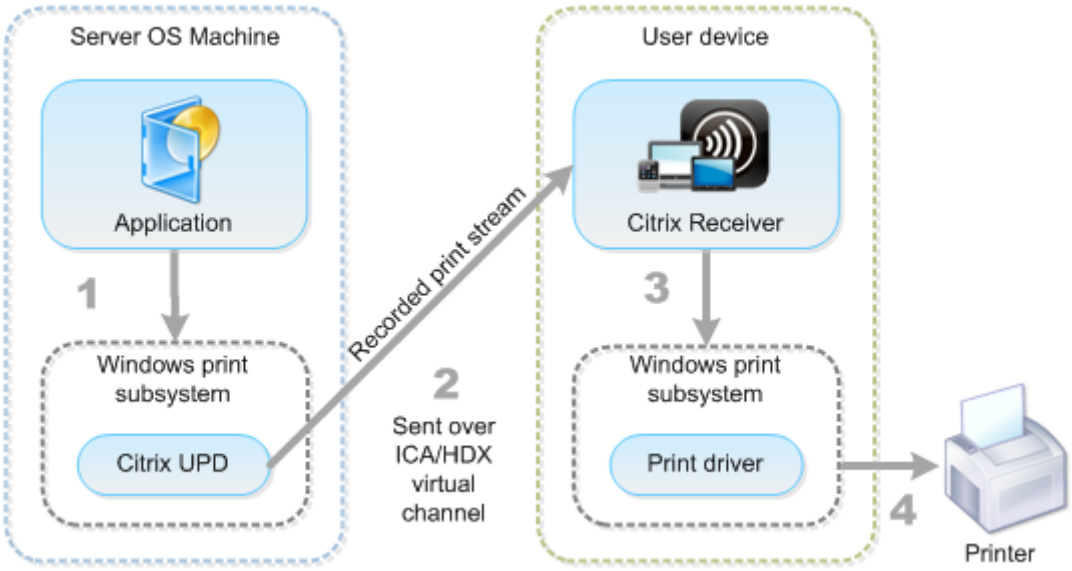
 

- Formato metafile avanzato (**EMF**), impostazione predefinita. EMF è la versione a 32 bit del formato Windows Metafile (WMF). Il driver EMF può essere utilizzato solo dai client basati su Windows.
- XML Paper Specification (**XPS**). Il driver XPS utilizza XML per creare una "carta elettronica" indipendente dalla piattaforma, simile al formato Adobe PDF.
- Linguaggio di comando della stampante (**PCL5c** e **PCL4**). PCL è un protocollo di stampa sviluppato originariamente da Hewlett-Packard per stampanti a getto d'inchiostro. Viene utilizzato per la stampa di testo e grafica di base ed è ampiamente supportato su HP LaserJet e periferiche multifunzione.
- PostScript (**PS**). PostScript è un linguaggio informatico che può essere utilizzato per la stampa di testo e grafica vettoriale. Il driver è ampiamente utilizzato nelle stampanti a basso costo e nelle periferiche multifunzione.

I driver PCL e PS sono più adatti all'uso con dispositivi non basati su Windows come un client Mac o UNIX. L'ordine in cui Citrix UPD tenta di utilizzare i driver può essere modificato utilizzando l'impostazione dei criteri Universal driver preference (Preferenza driver universale).

Citrix UPD (driver EMF e XPS) supporta funzioni di stampa avanzate come la pinzatura e la selezione delle fonti di carta. Queste funzionalità sono disponibili se il driver nativo le rende disponibili utilizzando la tecnologia Microsoft Print Capability. Il driver nativo deve utilizzare le parole chiave standard dello schema di stampa nel formato XML delle funzionalità di stampa. Se si utilizzano parole chiave non standard, le funzioni di stampa avanzate non sono disponibili utilizzando il driver di stampa Citrix Universal.

Nella figura seguente vengono illustrati i componenti del driver di stampa Universal e un flusso di lavoro tipico per una stampante collegata localmente a una periferica.



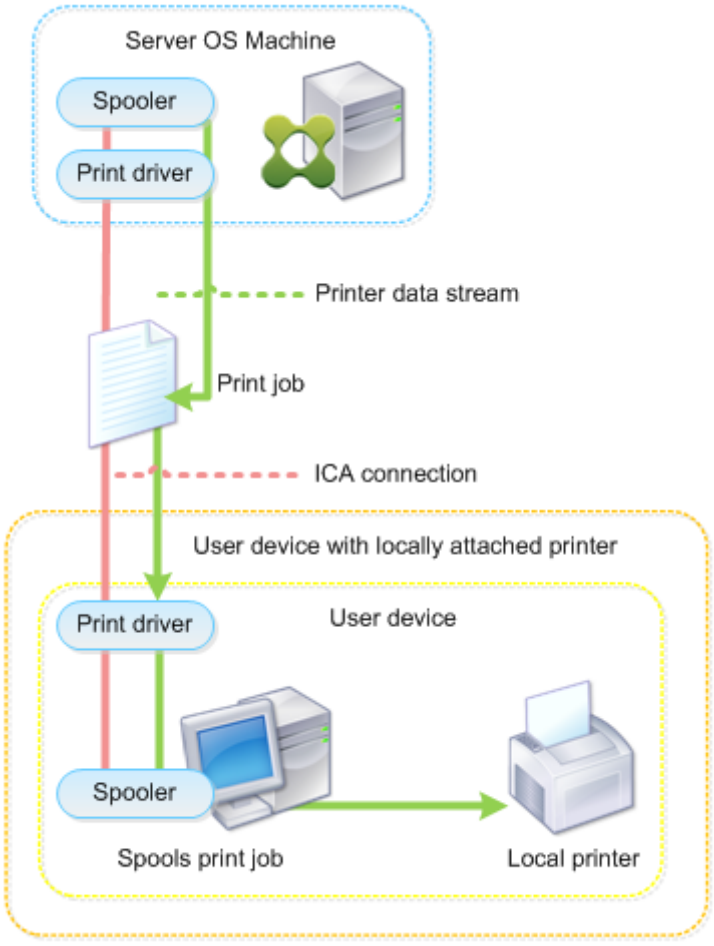

Quando si pianifica la strategia di gestione dei driver, determinare quali driver di stampa si support-

eranno: il driver di stampa Universal, i driver specifici del dispositivo o entrambi. Se si supportano i driver standard, è necessario determinare:

Durante la creazione automatica della stampante il sistema, se rileva una nuova stampante locale collegata a un dispositivo utente, controlla il driver della stampante richiesto nel computer del sistema operativo multisessione. Per impostazione predefinita, se non è disponibile un driver nativo di Windows, il sistema utilizza il driver di stampa Universal.

Il driver della stampante presente sul computer con il sistema operativo multisessione e il driver presente sul dispositivo utente devono corrispondere affinché la stampa abbia esito positivo. Nella figura seguente viene illustrato come un driver della stampante viene utilizzato in due posizioni per la stampa client.




- I tipi di driver da supportare.
- Indica se installare automaticamente i driver della stampante quando mancano dai computer con sistema operativo multisessione.
- Indica se creare elenchi di compatibilità dei driver.

### Contenuti correlati

- Esempio di configurazione di stampa
- Procedure consigliate, considerazioni sulla sicurezza e operazioni predefinite
- Criteri di stampa e preferenze
- Provisioning delle stampanti
- Mantenere l'ambiente di stampa

## Esempio di configurazione di stampa

January 7, 2024

La scelta delle opzioni di configurazione di stampa più appropriate per le proprie esigenze e il proprio ambiente può semplificare l'amministrazione. Sebbene la configurazione di stampa predefinita consenta agli utenti di stampare nella maggior parte degli ambienti, i valori predefiniti potrebbero non fornire l'esperienza utente prevista o l'utilizzo della rete e il sovraccarico di gestione ottimali per l'ambiente.

La configurazione di stampa dipende dai seguenti fattori:

- Le esigenze aziendali e l'infrastruttura di stampa esistente.

  Progettare la configurazione di stampa in base alle esigenze dell'organizzazione. L'implementazione di stampa esistente (se gli utenti possono aggiungere stampanti, quali utenti hanno accesso a quali stampanti e così via) potrebbe essere una guida utile per definire la configurazione di stampa.

- Se l'organizzazione dispone di criteri di sicurezza che riservano stampanti per determinati utenti (ad esempio stampanti per il team che si occupa delle risorse umane o delle buste paga).
- Se gli utenti devono stampare quando sono lontani dal luogo di lavoro principale, ad esempio i lavoratori che si spostano tra più workstation o che viaggiano per lavoro.

Quando si progetta la configurazione di stampa, provare a offrire agli utenti in una sessione un'esperienza equivalente a quella della stampa dai dispositivi utente locali.

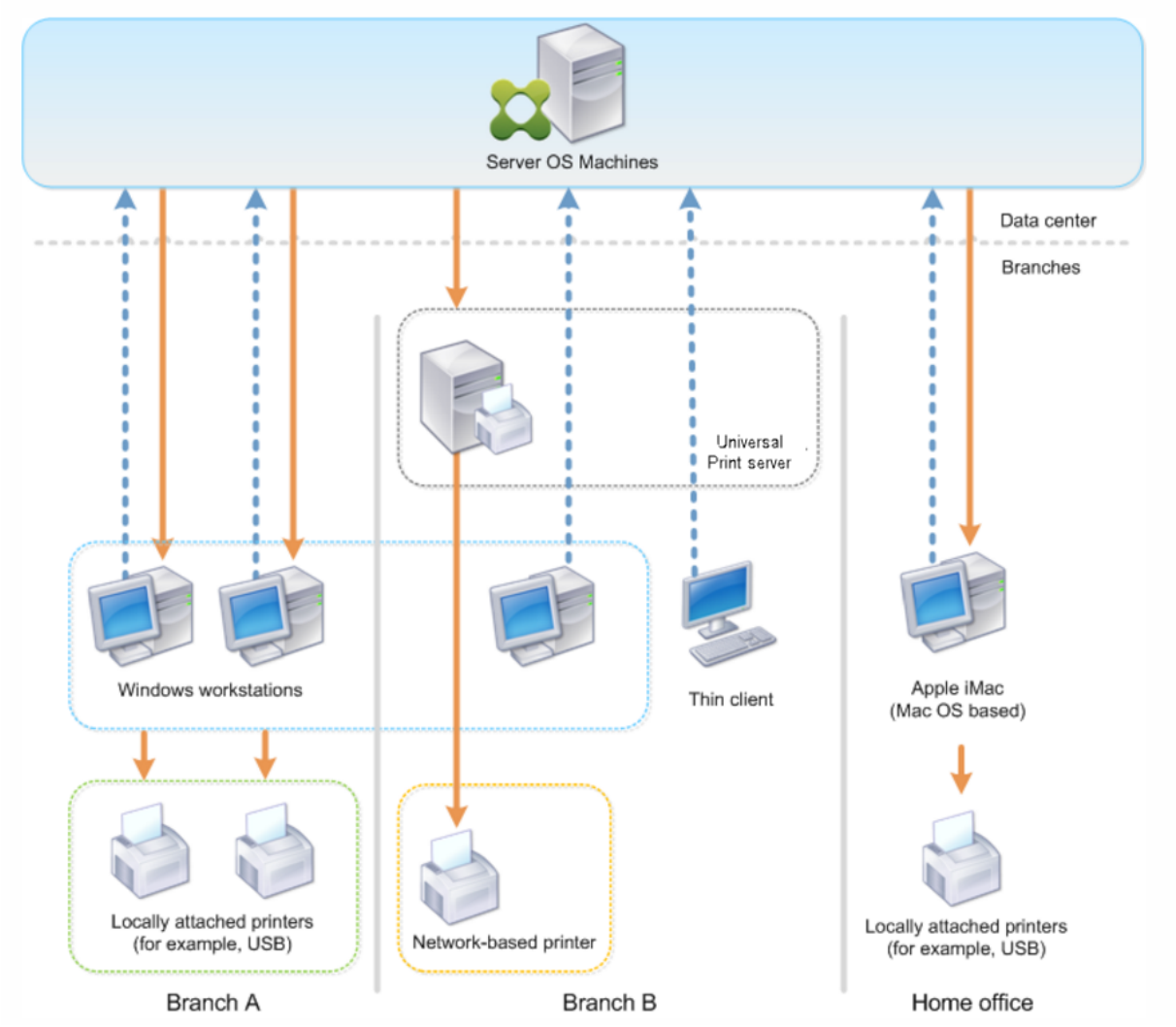
### Esempio di distribuzione di stampa

Nella figura seguente viene illustrata la distribuzione di stampa per questi casi d'uso:

- **Filiale A**: una piccola filiale all'estero con alcune workstation Windows. Ogni workstation utente dispone di una stampante privata collegata localmente.

- **Filiale B**: una grande filiale con thin client e workstation basate su Windows. Per una maggiore efficienza, gli utenti di questa filiale condividono le stampanti basate sulla rete (una per piano). I server di stampa basati su Windows situati all'interno della filiale gestiscono le code di stampa.
- **Ufficio domestico**: un ufficio domestico con un dispositivo utente basato su Mac OS che accede all'infrastruttura Citrix dell'azienda. Il dispositivo utente dispone di una stampante collegata localmente.




Le sezioni seguenti descrivono le configurazioni che riducono al minimo la complessità dell'ambiente e ne semplificano la gestione.

### Stampanti client create automaticamente e driver per stampante universale Citrix

Nella filiale A, tutti gli utenti lavorano su workstation basate su Windows, pertanto vengono utilizzate stampanti client create automaticamente e il driver della stampante universale. Tali tecnologie offrono questi vantaggi:

- Prestazioni: i processi di stampa vengono distribuiti sul canale di stampa ICA, quindi i dati di stampa possono essere compressi per risparmiare larghezza di banda.

  Per garantire che un singolo utente che stampa un documento di grandi dimensioni comprometta le prestazioni delle sessioni di altri utenti, è configurato un criterio Citrix per specificare la larghezza di banda massima di stampa.

  Una soluzione alternativa consiste nello sfruttare una connessione ICA multiflusso, in cui il traffico di stampa viene trasferito all'interno di una connessione TCP separata a bassa priorità. ICA multiflusso è un'opzione disponibile quando Quality of Service (QoS) non è implementato sulla connessione WAN.

- Flessibilità: l'utilizzo del driver della stampante universale Citrix garantisce che tutte le stampanti connesse a un client possano essere utilizzate anche da una sessione di applicazione o desktop virtuale, senza integrare un nuovo driver di stampa nel data center.

### Citrix Universal Print Server

Nella filiale B, tutte le stampanti sono basate sulla rete e le loro code sono gestite su un server di stampa Windows, pertanto Citrix Universal Print Server è la configurazione più efficiente.

Tutti i driver di stampa richiesti vengono installati e gestiti sul server di stampa dagli amministratori locali. La mappatura delle stampanti nelle sessioni di applicazione o desktop virtuale funziona come segue:

- Per workstation basate su Windows: il team IT locale aiuta gli utenti a connettere la stampante appropriata basata sulla rete alle workstation Windows. Ciò consente agli utenti di stampare da applicazioni installate localmente.

  Durante una sessione di applicazione o desktop virtuale, le stampanti configurate localmente vengono enumerate tramite creazione automatica. L'applicazione o il desktop virtuale si connette quindi al server di stampa come connessione diretta di rete, se possibile.

  I componenti di Citrix Universal Print Server sono installati e abilitati, pertanto non sono necessari driver di stampa nativi. Se un driver viene aggiornato o viene modificata una coda della stampante, non è richiesta alcuna configurazione aggiuntiva nel data center.

- Per i thin client: per gli utenti di thin client, le stampanti devono essere collegate all'interno della sessione dell'applicazione o desktop virtuale. Per offrire agli utenti l'esperienza di stampa più semplice, gli amministratori configurano un singolo criterio Citrix Session Printer (Stampante di sessione Citrix) per piano per collegare la stampante di un piano come stampante predefinita.

  Per garantire che la stampante corretta sia collegata anche se gli utenti si alternano tra i piani, i criteri vengono filtrati in base alla subnet o al nome del thin client. Tale configurazione, denomi-

nata stampa di prossimità, consente la manutenzione locale del driver della stampante (in base al modello di amministrazione delegato).

Se è necessario modificare o aggiungere una coda della stampante, gli amministratori Citrix devono modificare il rispettivo criterio Session printer (Sessione stampante) all'interno dell'ambiente.

Poiché il traffico di stampa di rete verrà inviato al di fuori del canale virtuale ICA, viene implementato QoS. Il traffico di rete in entrata e in uscita sulle porte utilizzate dal traffico ICA/HDX è prioritario rispetto a tutto l'altro traffico di rete. Tale configurazione garantisce che le sessioni utente non siano influenzate da processi di stampa di grandi dimensioni.

### Stampanti client create automaticamente e driver per stampante universale Citrix

Per gli uffici domestici in cui gli utenti lavorano su workstation non standard e utilizzano dispositivi di stampa non gestiti, l'approccio più semplice consiste nell'utilizzare stampanti client create automaticamente e il driver della stampante universale.

### Riepilogo della distribuzione

In sintesi, la distribuzione di esempio è configurata come segue:

- Nessun driver di stampa è installato su macchine con sistema operativo multisessione. Viene utilizzato solo il driver della stampante universale Citrix. Il fallback alla stampa nativa e l'installazione automatica dei driver della stampante sono disabilitati.
- È configurato un criterio per creare automaticamente tutte le stampanti client per tutti gli utenti. Le macchine del sistema operativo multisessione si connetteranno direttamente ai server di stampa per impostazione predefinita. L'unica configurazione necessaria è l'abilitazione dei componenti di Universal Print Server.
- Un criterio Session printer (Stampante di sessione) è configurato per ogni piano della filiale B e applicato a tutti i thin client del rispettivo piano.
- QoS è implementato per la filiale B per garantire un'esperienza utente eccellente.

## Procedure consigliate, considerazioni sulla sicurezza e operazioni predefinite

January 7, 2024

### Procedure consigliate

Molti fattori determinano la migliore soluzione di stampa per un determinato ambiente. Alcune di queste procedure consigliate potrebbero non essere applicabili al sito in uso.

- Utilizzare Citrix Universal Print Server.
- Utilizzare il driver della stampante universale o i driver nativi di Windows.
- Ridurre al minimo il numero di driver delle stampanti installati su macchine con sistema operativo multisessione.
- Usare la mappatura dei driver sui driver nativi.
- Non installare mai driver di stampa non testati in un sito di produzione.
- Evitare di aggiornare un driver. Tentare sempre di disinstallare un driver, riavviare il server di stampa e quindi installare il driver sostitutivo.
- Disinstallare i driver non utilizzati o utilizzare il criterio Printer driver mapping and compatibility (Mappatura e compatibilità del driver della stampante) per impedire che vengano create stampanti con il driver.
- Cercare di evitare di utilizzare i driver in modalità kernel versione 2.
- Per determinare se un modello di stampante è supportato, contattare il produttore o vedere la guida ai prodotti Citrix Ready all'indirizzo www.citrix.com/ready.

  In generale, tutti i driver di stampa forniti da Microsoft sono testati con Servizi terminal e garantiscono il funzionamento con Citrix. Tuttavia, prima di utilizzare un driver di stampa di terze parti, vedere il fornitore del driver di stampa per verificare che il driver sia certificato per Servizi terminal dal programma WHQL (Windows Hardware Quality Labs). Citrix non certifica i driver delle stampanti.

### Considerazioni sulla sicurezza

Le soluzioni di stampa Citrix sono progettate per essere sicure.

- Il servizio Citrix Print Manager monitora e risponde costantemente a eventi di sessione come accesso e scollegamento, disconnessione, riconnessione e terminazione della sessione. Gestisce le richieste di servizio rappresentando l'utente effettivo della sessione.
- La stampa Citrix assegna a ciascuna stampante uno spazio dei nomi univoco in una sessione.
- La stampa Citrix imposta il descrittore di sicurezza predefinito per le stampanti create automaticamente per garantire che le stampanti client create automaticamente in una sessione non siano accessibili agli utenti che eseguono altre sessioni. Per impostazione predefinita, gli utenti

amministrativi non possono stampare accidentalmente sulla stampante client di un'altra sessione, anche se possono visualizzare e regolare manualmente le autorizzazioni per qualsiasi stampante client.

### Operazioni di stampa predefinite

Per impostazione predefinita, se non si configurano regole dei criteri, il comportamento di stampa è il seguente:

- Universal Print Server è disabilitato.
- Tutte le stampanti configurate sul dispositivo utente vengono create automaticamente all'inizio di ogni sessione.

  Questo comportamento equivale alla configurazione dell'impostazione dei criteri Citrix Auto-create client printers (Crea automaticamente stampanti client) con l'opzione Auto-create all client printers (Crea automaticamente tutte le stampanti client).
- Il sistema instrada tutti i processi di stampa in coda alle stampanti collegate localmente ai dispositivi utente come processi di stampa client (ovvero attraverso il canale ICA e il dispositivo utente).
- Il sistema instrada tutti i processi di stampa in coda alle stampanti di rete direttamente dalle macchine del sistema operativo multisessione. Se il sistema non è in grado di instradare i processi sulla rete, li instraderà attraverso il dispositivo utente come processo di stampa client reindirizzato.

  Questo comportamento equivale a disabilitare l'impostazione dei criteri Citrix Direct connection to print servers (Connessione diretta ai server di stampa).
- Il sistema tenta di memorizzare le proprietà di stampa, una combinazione delle preferenze di stampa dell'utente e delle impostazioni specifiche del dispositivo di stampa, sul dispositivo utente. Se il client non supporta questa operazione, il sistema memorizza le proprietà di stampa nei profili utente sulla macchina con sistema operativo multisessione.

  Questo comportamento equivale alla configurazione dell'impostazione dei criteri Citrix Printer properties retention (Conservazione delle proprietà della stampante) con l'opzione Held in profile only if not saved on client (Conservate nel profilo solo se non salvate sul client).
- Nei VDA versione 7.16 e successive, l'impostazione del criterio Citrix Automatic installation of inbox printer drivers (Installazione automatica dei driver della stampante inclusi) non ha alcun effetto su Windows 8 e sulle versioni dei sistemi operativi Windows successive, poiché i driver della stampante V3 inclusi non sono inclusi nel sistema operativo.
- Nelle versioni di VDA precedenti alla 7.16, il sistema utilizza la versione di Windows del driver della stampante, se è disponibile sulla macchina con sistema operativo multisessione. Se il

driver della stampante non è disponibile, il sistema tenta di installare il driver dal sistema operativo Windows. Se il driver non è disponibile in Windows, utilizza un driver di stampa universale Citrix.

Questo comportamento equivale all'abilitazione dell'impostazione dei criteri Citrix Automatic installation of in-box printer drivers (Installazione automatica dei driver di stampa inclusi) e alla configurazione dell'impostazione Universal printing (Stampa universale) con l'opzione Use universal printing only if requested driver is unavailable (Utilizza la stampa universale solo se il driver richiesto non è disponibile).

L'abilitazione dell'opzione Automatic installation of in-box printer drivers (Installazione automatica dei driver di stampa inclusi) potrebbe comportare l'installazione di un numero elevato di driver di stampa nativi.

> **Nota:**
>
> Se non si è sicuri di quali siano le impostazioni predefinite di spedizione per la stampa, visualizzale creando un nuovo criterio e impostando tutte le regole dei criteri di stampa su Enabled (Abilitato). L'opzione visualizzata è quella predefinita.

### Always-On logging (Registrazione sempre attiva)

È disponibile una funzionalità Always-On logging (Registrazione sempre attiva) per il server di stampa e il sottosistema di stampa sul VDA.

Per raccogliere i log come ZIP per l'invio tramite e-mail o per caricare automaticamente i log su Citrix Insight Services, utilizzare il cmdlet PowerShell **Start-TelemetryUpload**.

## Criteri di stampa e preferenze

January 7, 2024

Quando gli utenti accedono alle stampanti da applicazioni pubblicate, è possibile configurare i criteri Citrix per specificare:

- Come viene eseguito il provisioning delle stampanti (o come vengono aggiunte alle sessioni)
- Come vengono instradati i processi di stampa
- Come vengono gestiti i driver delle stampanti

È possibile avere configurazioni di stampa diverse per diversi dispositivi utente, utenti o qualsiasi altro oggetto su cui vengono filtrati i criteri.

La maggior parte delle funzioni di stampa sono configurate tramite le impostazioni dei criteri di stampa Citrix. Le impostazioni di stampa seguono il comportamento standard dei criteri Citrix.

Il sistema può scrivere le impostazioni della stampante sull'oggetto stampante al termine di una sessione o su un dispositivo di stampa client, a condizione che l'account di rete dell'utente disponga di autorizzazioni sufficienti. Per impostazione predefinita, l'app Citrix Workspace utilizza le impostazioni memorizzate nell'oggetto stampante nella sessione, prima di cercare le impostazioni e le preferenze in altre posizioni.

Per impostazione predefinita, il sistema memorizza o mantiene le proprietà della stampante sul dispositivo utente (se supportato dal dispositivo) o nel profilo utente sulla macchina con sistema operativo multisessione. Quando un utente modifica le proprietà della stampante durante una sessione, tali modifiche vengono aggiornate nel profilo utente sulla macchina. Al successivo accesso o riconnessione dell'utente, il dispositivo utente eredita le impostazioni mantenute. Ossia, le modifiche alle proprietà della stampante sul dispositivo utente non influiscono sulla sessione corrente fino a quando l'utente non si disconnette e accede nuovamente.

### Posizioni delle preferenze di stampa

Negli ambienti di stampa Windows, le modifiche apportate alle preferenze di stampa possono essere memorizzate sul computer locale o in un documento. In questo ambiente, quando gli utenti modificano le impostazioni di stampa, le impostazioni vengono memorizzate nelle seguenti posizioni:

- **Sul dispositivo utente stesso**: gli utenti Windows possono modificare le impostazioni del dispositivo sul dispositivo utente facendo clic con il pulsante destro del mouse sulla stampante nel Pannello di controllo e selezionando Preferenze di stampa. Ad esempio, se Orizzontale è selezionato come orientamento pagina, tale orientamento viene salvato come preferenza di orientamento pagina predefinita per quella stampante.
- **All'interno di un documento**: nei programmi di elaborazione testi e desktop publishing, le impostazioni dei documenti, come l'orientamento della pagina, vengono spesso memorizzate all'interno dei documenti. Ad esempio, quando si mette in coda un documento da stampare, in genere Microsoft Word memorizza le preferenze di stampa specificate, ad esempio l'orientamento della pagina e il nome della stampante, all'interno del documento. Queste impostazioni vengono visualizzate per impostazione predefinita la volta successiva in cui il documento viene stampato.
- **Dalle modifiche apportate da un utente durante una sessione**: il sistema conserva solo le modifiche alle impostazioni di stampa di una stampante creata automaticamente se la modifica è stata apportata nel Pannello di controllo nella sessione, ovvero sulla macchina con sistema operativo multisessione.
- **Sulla macchina con sistema operativo multisessione**: queste sono le impostazioni predefinite associate a un determinato driver della stampante sulla macchina.

Le impostazioni conservate in qualsiasi ambiente basato su Windows variano a seconda di dove l'utente ha apportato le modifiche. Ciò significa anche che le impostazioni di stampa che appaiono in un'unica posizione, ad esempio in un programma di fogli di calcolo, possono essere diverse da quelle di altri programmi, come i documenti. Di conseguenza, le impostazioni di stampa applicate a una stampante specifica possono cambiare durante una sessione.

### Gerarchia delle preferenze di stampa dell'utente

Poiché le preferenze di stampa possono essere memorizzate in più posizioni, il sistema le elabora in base a una priorità specifica. Inoltre, è importante notare che le impostazioni dei dispositivi sono trattate in modo distinto e di solito hanno la precedenza sulle impostazioni dei documenti.

Per impostazione predefinita, il sistema applica sempre tutte le impostazioni di stampa modificate dall'utente durante una sessione (ovvero le impostazioni mantenute) prima di prendere in considerazione altre impostazioni. Quando l'utente stampa, il sistema unisce e applica le impostazioni di stampa predefinite memorizzate sulla macchina con sistema operativo multisessione con qualsiasi impostazione della stampante conservata o client.

### Salvare le preferenze di stampa degli utenti

Citrix consiglia di non modificare la posizione in cui sono memorizzate le proprietà della stampante. L'impostazione predefinita, che salva le proprietà della stampante sul dispositivo utente, è il modo più semplice per garantire proprietà di stampa uniformi. Se il sistema non è in grado di salvare le proprietà sul dispositivo utente, torna automaticamente al profilo utente sulla macchina con sistema operativo multisessione.

Controllare l'impostazione del criterio di conservazione delle proprietà della stampante se si applicano questi scenari:

- Se si utilizzano plug-in legacy che non consentono agli utenti di memorizzare le proprietà della stampante su un dispositivo utente.
- Se si utilizzano profili obbligatori sulla rete Windows e si desidera mantenere le proprietà della stampante dell'utente.

## Provisioning delle stampanti

April 3, 2024

### Citrix Universal Print Server

Quando si determina la migliore soluzione di stampa per il proprio ambiente, prendere in considerazione quanto segue:

- Universal Print Server offre funzionalità non disponibili per il provider di stampa Windows: memorizzazione nella cache di immagini e font, compressione avanzata, ottimizzazione e supporto QoS.
- Il driver di stampa universale supporta le impostazioni pubbliche indipendenti dal dispositivo definite da Microsoft. Se gli utenti hanno bisogno di accedere alle impostazioni del dispositivo specifiche di un produttore di driver di stampa, Universal Print Server associato a un driver nativo di Windows potrebbe essere la soluzione migliore. Con questa configurazione si mantengono i vantaggi di Universal Print Server, fornendo agli utenti l'accesso a funzionalità di stampa specializzate. Un aspetto da considerare è che i driver nativi di Windows richiedono manutenzione.
- Citrix Universal Print Server fornisce supporto di stampa universale per le stampanti di rete. Universal Print Server utilizza il driver di stampa universale, un singolo driver sulla macchina con sistema operativo multisessione che consente la stampa locale o di rete da qualsiasi dispositivo, inclusi thin client e tablet.

Per utilizzare Universal Print Server con un driver nativo di Windows, abilitare Universal Print Server. Per impostazione predefinita viene utilizzato il driver nativo di Windows, se disponibile. In caso contrario, viene utilizzato il driver di stampa universale. Per specificare le modifiche a tale comportamento, ad esempio per utilizzare solo il driver nativo di Windows o solo il driver di stampa universale, aggiornare l'impostazione del criterio di utilizzo del driver di stampa universale.

#### Installare Universal Print Server

Per utilizzare Universal Print Server, installare il componente UpsServer sui server di stampa, come descritto nei documenti di installazione, e configurarlo. Per ulteriori informazioni, vedere Installare i componenti principali e Installare utilizzando la riga di comando.

Per gli ambienti in cui si desidera distribuire separatamente il componente UPClient, ad esempio con **XenApp 6.5**:

1. Scaricare il pacchetto standalone Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA) per sistema operativo Windows a sessione singola o sistema operativo Windows multisessione.
2. Estrarre il VDA utilizzando le istruzioni della riga di comando descritte in Installare utilizzando la riga di comando.
3. Installare i prerequisiti da \Image-Full\Support\VcRedist_2013_RTM
    - Vcredist_x64 / vcredist_x86

  - Eseguire x86 solo per le distribuzioni a 32 bit ed entrambi per le distribuzioni a 64 bit

4. Installare il prerequisito cdf da \Image-Full\x64\Virtual Desktop Components o \Image-Full\x86\Virtual Desktop Components.
   - Cdf_x64 / Cdf_x86
     - x86 per 32 bit, x64 per 64 bit
5. Individuare il componente UPClient in \Image-Full\x64\Virtual Desktop Components o \Image-Full\x86\Virtual Desktop Components.
6. Installare il componente UPClient estraendo e quindi avviando il file MSI del componente.
7. È necessario un riavvio dopo l'installazione del componente UPClient.

#### Annullare la registrazione al programma CEIP per Universal Print Server

Quando si installa Universal Print Server, l'utente viene automaticamente registrato al programma CEIP (Citrix Customer Experience Improvement Program). Il primo caricamento dei dati avviene dopo sette giorni dalla data e dall'ora dell'installazione.

Per annullare la registrazione al programma CEIP, modificare la chiave del Registro di sistema **HKLM\Software\Citrix\Universal Print Server\CEIPEnabled** e impostare il valore **DWORD** su **0**.

Per effettuare nuovamente la registrazione, impostare il valore DWORD su 1.

**Attenzione**: la modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Per ulteriori informazioni, vedere Citrix Insight Services.

#### Configurare Universal Print Server

Utilizzare le seguenti impostazioni dei criteri Citrix per configurare Universal Print Server. Per ulteriori informazioni, vedere la guida a schermo sulle impostazioni dei criteri.

- **Universal Print Server enable (Abilitazione di Universal Print Server)**. Universal Print Server è disabilitato per impostazione predefinita. Quando si abilita Universal Print Server, è possibile scegliere se utilizzare il provider di stampa Windows se Universal Print Server non è disponibile. Dopo aver abilitato Universal Print Server, un utente può aggiungere ed enumerare le stampanti di rete tramite le interfacce dei provider di stampa Windows e Citrix.

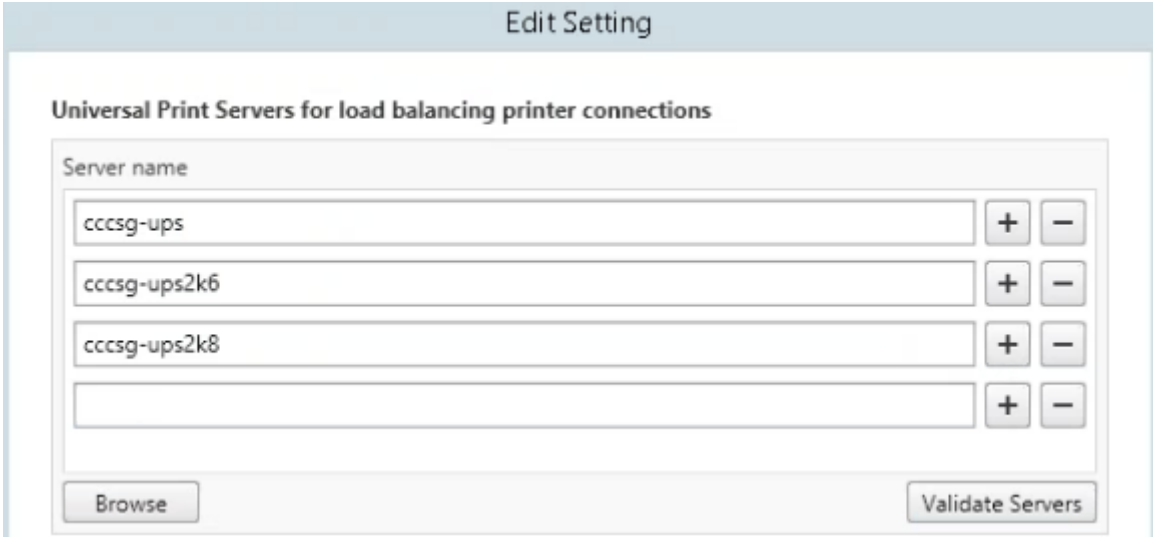
- **Universal Print Server print data stream (CGP) port (Porta del flusso di dati di stampa di Universal Print Server [CGP])**. Specifica il numero di porta TCP utilizzato dal listener CGP (Common Gateway Protocol) del flusso di dati di stampa di Universal Print Server. Il valore predefinito è **7229**.
- **Universal Print Server web service (HTTP/SOAP) port (Porta del servizio Web di Universal Print Server [HTTP/SOAP])**. Specifica il numero di porta TCP utilizzato dal listener Universal Print Server per le richieste HTTP/SOAP in arrivo. Il valore predefinito è **8080**.

Per modificare la porta predefinita HTTP 8080 per la comunicazione tra Universal Print Server e i VDA Citrix Virtual Apps and Desktops, è necessario creare anche la seguente chiave del Registro di sistema e modificare il valore del numero di porta sui computer Universal Print Server:

HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Citrix\\PrintingPolicies
“UpsHttpPort”=DWORD:<portnumber>

Questo numero di porta deve corrispondere alla porta del servizio Web HDX Policy, Universal Print Server (HTTP/SOAP) in Studio.

- **Universal Print Server print stream input bandwidth limit (kpbs) (Limite della larghezza di banda di input del flusso di stampa di Universal Print Server [kpbs])**. Specifica il limite superiore (in kilobit al secondo) per la velocità di trasferimento dei dati di stampa inviati da ciascun processo di stampa a Universal Print Server utilizzando CGP. Il valore predefinito è 0 (illimitato).
- **Universal Print Servers for load balancing (Universal Print Server per il bilanciamento del carico)**. Questa impostazione elenca gli Universal Print Server da utilizzare per bilanciare il carico delle connessioni della stampante stabilite all’avvio della sessione, dopo aver valutato altre impostazioni dei criteri di stampa Citrix. Per ottimizzare i tempi di creazione della stampante, Citrix consiglia che tutti i server di stampa abbiano lo stesso set di stampanti condivise.



- **Universal Print Servers out-of-service threshold (Soglia fuori servizio di Universal Print Server)**. Specifica per quanto tempo il bilanciatore del carico deve attendere il ripristino di un server di stampa non disponibile prima di determinare che il server è permanentemente offline e prima di ridistribuire il carico ad altri server di stampa disponibili. Il valore predefinito è 180 (secondi).

Una volta modificati i criteri di stampa sul Delivery Controller, potrebbero essere necessari alcuni minuti prima che le modifiche del criterio vengano applicate ai VDA.

**Interazioni con altre impostazioni dei criteri**: Universal Print Server rispetta le altre impostazioni dei criteri di stampa Citrix e interagisce con esse come indicato nella tabella seguente. Le informazioni fornite presuppongono che l'impostazione dei criteri Universal Print Server sia abilitata, che i componenti di Universal Print Server siano installati e che vengano applicate le impostazioni dei criteri.

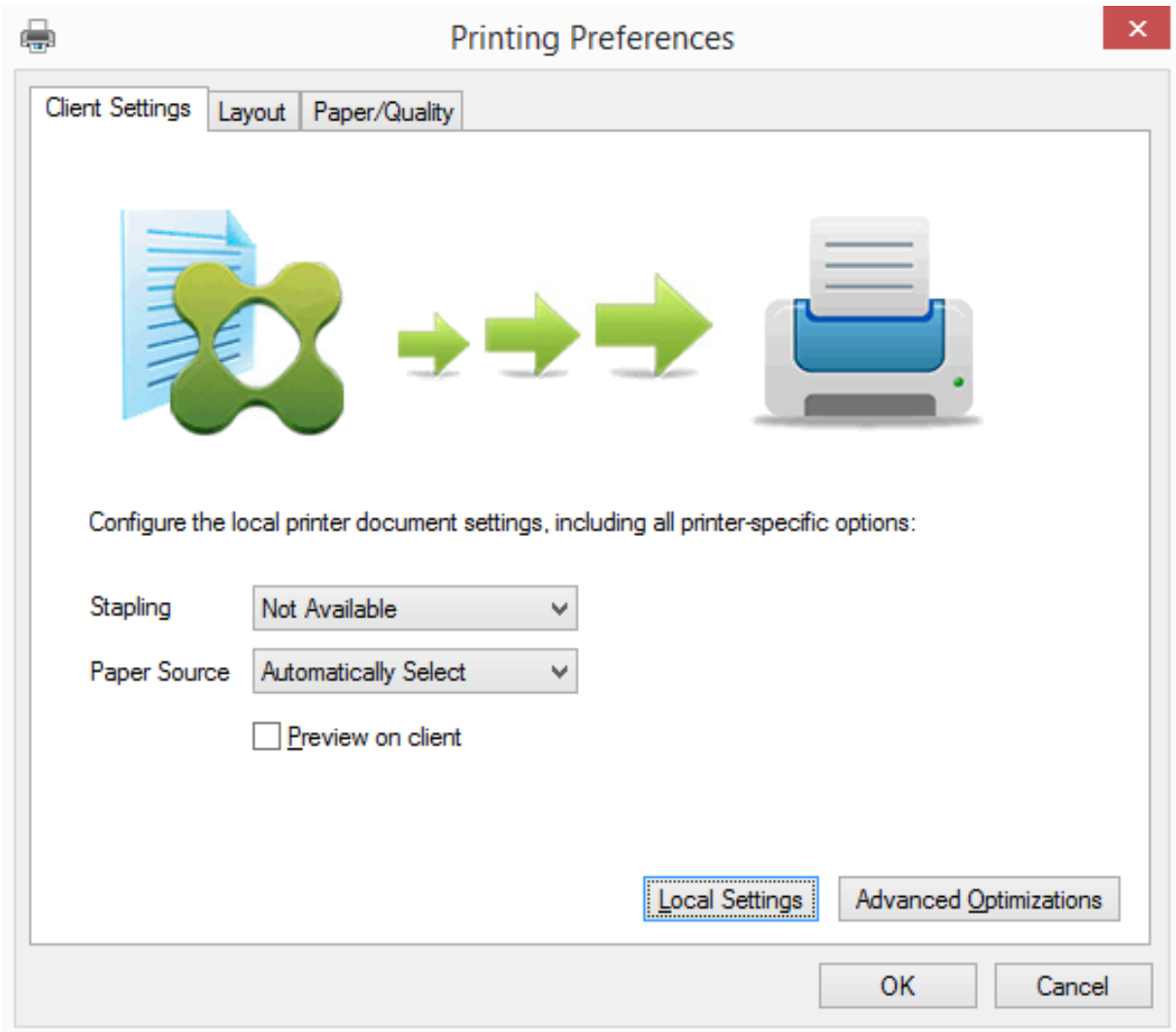
| Impostazione dei criteri | Interazione |
| --- | --- |
| Client printer redirection (Reindirizzamento stampanti client), Auto-create client printers (Crea automaticamente stampanti client) | Dopo aver abilitato Universal Print Server, le stampanti di rete client vengono create utilizzando il driver di stampa universale anziché i driver nativi. Gli utenti vedono lo stesso nome della stampante di prima. |
| Session printers (Stampanti di sessione) | Quando si utilizza la soluzione Citrix Universal Print Server, le impostazioni dei criteri del driver di stampa universale vengono rispettate. |
| Direct connections to print servers (Connessioni dirette al server di stampa) | Quando Universal Print Server è abilitato e l'impostazione dei criteri Universal print driver usage (Utilizzo del driver di stampa universale) è configurata per utilizzare solo la stampa universale, è possibile creare una connessione diretta della stampante di rete al server di stampa utilizzando il driver di stampa universale. |
| UPD preference (Preferenza UPD) | Supporta driver EMF e XPS. |

**Effetti sulle interfacce utente**: il driver di stampa universale Citrix utilizzato da Universal Print Server disabilita i seguenti controlli dell'interfaccia utente:

- Nella finestra di dialogo Printer Properties (Proprietà stampante), il pulsante Local Printer Settings (Impostazioni stampante locale)
- Nella finestra di dialogo Document Properties (Proprietà documento), i pulsanti Local Printer Settings (Impostazioni stampante locale) e Preview on client (Anteprima sul client)

Il driver di stampa universale Citrix (driver EMF e XPS) supporta funzionalità di stampa avanzate come la graffatura e l'origine carta. L'utente può selezionare le opzioni Stapling (Graffatura) o Paper Source (Origine carta) dalla finestra di dialogo di stampa UPD personalizzata se le stampanti client o di rete che sono mappate sull'UPD nella sessione supportano queste funzionalità.




Per configurare impostazioni di stampa non standard come la graffatura e la protezione con PIN, selezionare **Local settings** (Impostazioni locali) nella finestra di dialogo di stampa UPD del cliente per qualsiasi stampante mappata client che utilizza i driver EMF o XPS UPD Citrix. La finestra di dialogo **Printing Preferences** (Preferenze stampa) della stampante mappata viene visualizzata all'esterno della sessione sul client, consentendo all'utente di modificare qualsiasi opzione della stampante e le impostazioni della stampante modificate vengono utilizzate nella sessione attiva durante la stampa del documento.

Queste funzionalità sono disponibili se il driver nativo le rende disponibili utilizzando la tecnologia Microsoft Print Capability. Il driver nativo deve utilizzare le parole chiave standard dello schema di stampa nel formato XML delle funzionalità di stampa. Se si utilizzano parole chiave non standard,

le funzionalità di stampa avanzate non sono disponibili se si utilizza il driver di stampa universale Citrix.

Quando si utilizza Universal Print Server, la procedura guidata di aggiunta di una stampante per Citrix Print Provider è la stessa del provider di stampa Windows, con le seguenti eccezioni:

- Quando si aggiunge una stampante in base al nome o all'indirizzo, è possibile fornire un numero di porta HTTP/SOAP per il server di stampa. Il numero di porta diventa parte del nome della stampante e viene visualizzato nei display.
- Se l'impostazione dei criteri Citrix Universal print driver usage (Utilizzo del driver di stampa universale Citrix) specifica che è necessario utilizzare la stampa universale, viene visualizzato il nome del driver di stampa universale quando si seleziona una stampante. Il provider di stampa Windows non può utilizzare il driver di stampa universale.

Il provider di stampa Citrix non supporta il rendering lato client.

Per ulteriori informazioni su Universal Print Server, vedere CTX200328.

### Stampanti client create automaticamente

Queste soluzioni di stampa universali sono fornite per le stampanti client:

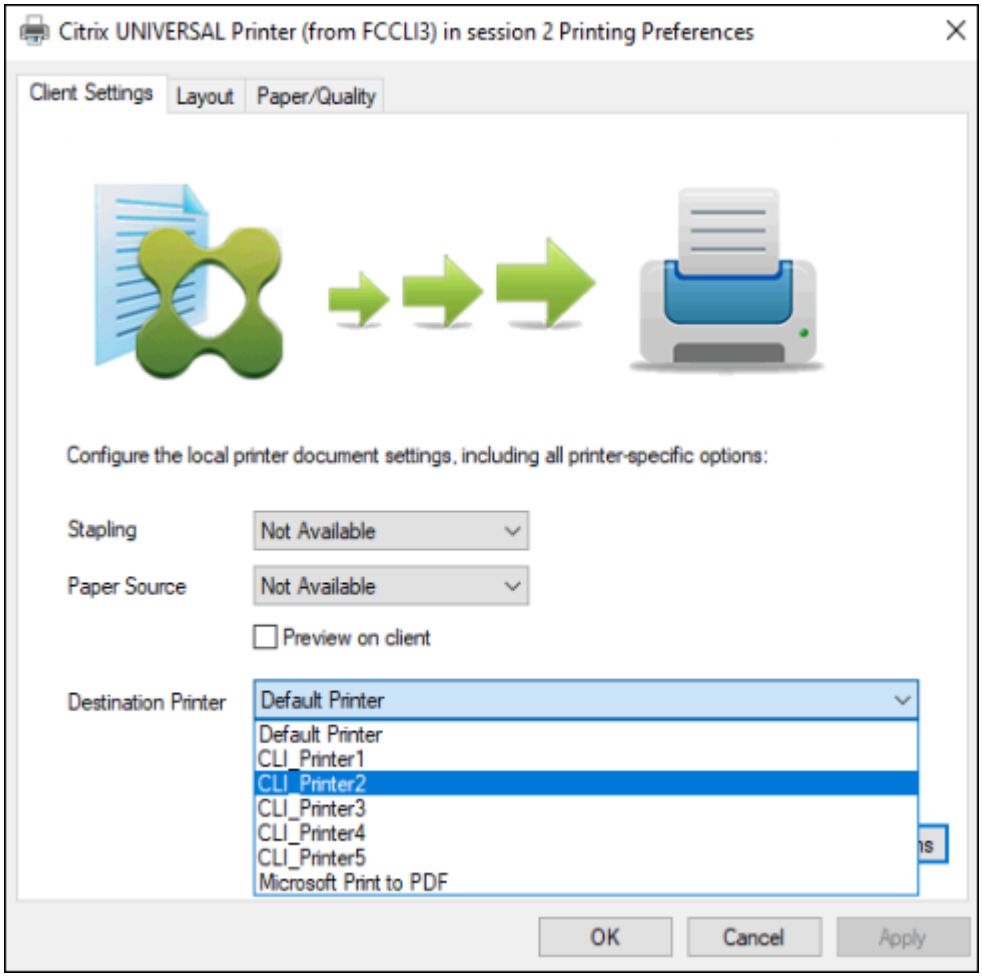
- **Stampante universale Citrix**: stampante generica creata all'inizio delle sessioni, che non è legata a un dispositivo di stampa. Quando si crea automaticamente e si utilizza solo la stampante universale Citrix, è possibile che si verifichi una riduzione dell'utilizzo delle risorse e dei tempi di accesso degli utenti. La stampante universale è in grado di stampare su qualsiasi dispositivo di stampa lato client.

  La stampante universale Citrix potrebbe non funzionare per tutti i dispositivi utente o le app Citrix Workspace nell'ambiente. La stampante universale Citrix richiede un ambiente Windows e non supporta il plug-in Citrix Offline o le applicazioni di cui viene eseguito lo streaming al client. Per tali ambienti, prendere in considerazione l'utilizzo di stampanti client create automaticamente e il driver di stampa universale.

  Per utilizzare una soluzione di stampa universale per app Citrix Workspace non Windows, utilizzare uno degli altri driver di stampa universale basati su Postscript/PCL.

  La stampante universale Citrix consente di selezionare la stampante predefinita del client o una stampante client specifica come destinazione di stampa. Per scegliere una stampante specifica per un lavoro di stampa, aprire la finestra di dialogo **Preferenze stampa**. Selezionare il menu a discesa **Destination Printer** (Stampante di destinazione). L'opzione **Stampante predefinita** invia i lavori di stampa alla stampante predefinita del client. Sono elencate anche tutte le stampanti reindirizzate dal client collegate all'endpoint che esegue la sessione. La stampante selezionata viene salvata come stampante di destinazione per eventuali lavori di stampa futuri.




- **Driver di stampa universale Citrix**: un driver di stampa indipendente dal dispositivo. Se si configura un driver di stampa universale Citrix, il sistema utilizza il driver di stampa universale basato su EMF per impostazione predefinita.

  Il driver di stampa universale Citrix potrebbe creare processi di stampa più piccoli rispetto ai driver di stampa meno recenti o meno avanzati. Tuttavia, potrebbe essere necessario un driver specifico del dispositivo per ottimizzare i processi di stampa per una stampante specializzata.

**Configurare la stampa universale**: utilizzare le seguenti impostazioni dei criteri Citrix per configurare la stampa universale. Per ulteriori informazioni, vedere la guida a schermo sulle impostazioni dei criteri.

- Universal print driver usage (Utilizzo del driver di stampa universale): specifica quando utilizzare la stampa universale.
- Auto-create generic universal printer (Crea automaticamente la stampante universale generica): abilita o disabilita la creazione automatica dell'oggetto generico Citrix Universal Printer per le sessioni in cui è in uso un dispositivo utente compatibile con la stampa universale. Per impostazione predefinita, l'oggetto Universal Printer generico non viene creato automatica-

mente.

- Universal driver preference (Preferenza driver universale): specifica l'ordine in cui vengono utilizzati i driver della stampante universale, a partire dalla prima voce dell'elenco. È possibile aggiungere, modificare o rimuovere driver e modificare l'ordine dei driver nell'elenco.
- Universal printing preview preference (Preferenza anteprima di stampa universale): specifica se utilizzare o meno la funzione di anteprima di stampa per stampanti universali create automaticamente o generiche.
- Universal printing EMF processing mode (Modalità di elaborazione EMF della stampa universale): controlla il metodo di elaborazione del file di spooling EMF sul dispositivo utente Windows. Per impostazione predefinita, lo spooling dei record EMF viene eseguito direttamente sulla stampante. Lo spooling direttamente sulla stampante consente allo spooler di elaborare i dati più velocemente e di utilizzare meno risorse della CPU.

Per ulteriori criteri, vedere Ottimizzare le prestazioni di stampa. Per modificare le impostazioni predefinite per impostazioni quali il formato carta, la qualità di stampa, il colore, il fronte/retro e il numero di copie, vedere CTX113148.

**Auto-create printers from the user device** (Crea automaticamente stampanti dal dispositivo utente): all'inizio di una sessione, il sistema crea automaticamente tutte le stampanti sul dispositivo utente per impostazione predefinita. È possibile controllare quali tipi di stampanti vengono assegnati agli utenti e impedire la creazione automatica.

Utilizzare l'impostazione dei criteri Citrix
Auto-create client printers to control autocreation (Crea automaticamente stampanti client per controllare la creazione automatica). È possibile specificare quanto segue:

- Tutte le stampanti visibili al dispositivo utente, incluse le stampanti di rete e collegate localmente, vengono create automaticamente all'inizio di ogni sessione (impostazione predefinita)
- Tutte le stampanti locali fisicamente collegate al dispositivo utente vengono create automaticamente
- Viene creata automaticamente solo la stampante predefinita per il dispositivo utente
- La creazione automatica è disabilitata per tutte le stampanti client

L'impostazione Auto-create client printers (Crea automaticamente stampanti client) richiede che l'impostazione Client printer redirection (Reindirizzamento stampante client) sia impostata su Allowed (Consentito - impostazione predefinita).

### Assegnare stampanti di rete agli utenti

Per impostazione predefinita, le stampanti di rete sul dispositivo utente vengono create automaticamente all'inizio delle sessioni. Il sistema consente di ridurre il numero di stampanti di rete enumerate

e mappate specificando le stampanti di rete da creare all'interno di ogni sessione. Tali stampanti sono denominate "stampanti di sessione".

È possibile filtrare i criteri delle stampanti di sessione per indirizzo IP per fornire la stampa di prossimità. La stampa di prossimità consente agli utenti all'interno di un intervallo di indirizzi IP specificato di accedere automaticamente ai dispositivi di stampa di rete esistenti nello stesso intervallo. La stampa di prossimità è fornita da Citrix Universal Print Server e non richiede la configurazione descritta in questa sezione.

La stampa di prossimità potrebbe comportare il seguente scenario:

- La rete aziendale interna funziona con un server DHCP che designa automaticamente gli indirizzi IP agli utenti.
- Tutti i reparti all'interno dell'azienda hanno intervalli di indirizzi IP designati univoci.
- Sono presenti stampanti di rete all'interno dell'intervallo di indirizzi IP di ciascun reparto.

Quando la stampa di prossimità è configurata e un dipendente si sposta da un reparto all'altro, non è richiesta alcuna configurazione aggiuntiva del dispositivo di stampa. Una volta riconosciuto, il dispositivo utente nell'intervallo di indirizzi IP del nuovo reparto avrà accesso a tutte le stampanti di rete all'interno di tale intervallo.

**Configurare stampanti specifiche da reindirizzare nelle sessioni**: per creare stampanti assegnate dall'amministratore, configurare l'impostazione dei criteri Citrix Session printers (Stampanti di sessione). Aggiungere una stampante di rete a tale criterio utilizzando uno dei seguenti metodi:

- Immettere il percorso UNC della stampante utilizzando il formato \\nomeserver\nomestampante.
- Selezionare una posizione della stampante sulla rete.
- Cercare stampanti su un server specifico. Immettere il nome del server utilizzando il formato \\nomeserver e fare clic su Browse (Sfoglia).

Importante: il server unisce tutte le impostazioni della stampante di sessione abilitate per tutti i criteri applicati, a partire dalle priorità più alte a quelle più basse. Quando una stampante è configurata in più oggetti dei criteri, le impostazioni predefinite personalizzate vengono prese solo dall'oggetto del criterio con priorità più alta in cui è configurata la stampante.

Le stampanti di rete create con l'impostazione Session printers (Stampanti di sessione) possono variare a seconda del punto in cui è stata avviata la sessione filtrando oggetti come le subnet.

**Specificare una stampante di rete predefinita per una sessione**: per impostazione predefinita, la stampante principale dell'utente viene utilizzata come stampante predefinita per la sessione. Utilizzare l'impostazione dei criteri Citrix Default printer (Stampante predefinita) per modificare il modo in cui viene stabilita la stampante predefinita sul dispositivo utente in una sessione.

1. Nella pagina Default printer settings (Impostazioni della stampante predefinita), selezionare un'impostazione per Choose client's default printer (Scegli stampante predefinita del client):

- Network printer name (Nome stampante di rete): le stampanti aggiunte con l'impostazione dei criteri Session printers (Stampanti di sessione) vengono visualizzate in questo menu. Selezionare la stampante di rete da utilizzare come predefinita per questo criterio.
- Do not adjust the user's default printer (Non regolare la stampante predefinita dell'utente): viene utilizzata l'impostazione corrente del profilo utente di Servizi terminal o di Windows per la stampante predefinita. Per ulteriori informazioni, vedere la guida a schermo sulle impostazioni dei criteri.

2. Applicare il criterio al gruppo di utenti (o altri oggetti filtrati) su cui si vuole che abbia effetto.

**Configure proximity printing** (Configura la stampa di prossimità): la stampa di prossimità è fornita anche da Citrix Universal Print Server, che non richiede la configurazione descritta qui.

1. Creare un criterio separato per ogni subnet (o in modo che corrisponda alla posizione della stampante).
2. In ogni criterio, aggiungere le stampanti nella posizione geografica della subnet all'impostazione Session printers (Stampanti di sessione).
3. Configurare l'impostazione Default printer (Stampante predefinita) su Do not adjust the user's default printer (Non regolare la stampante predefinita dell'utente).
4. Filtrare i criteri in base all'indirizzo IP del client. Assicurarsi di aggiornare questi criteri per riflettere le modifiche apportate agli intervalli di indirizzi IP DHCP.

## Mantenere l'ambiente di stampa

January 7, 2024

La manutenzione dell'ambiente di stampa include:

- Gestione dei driver della stampante
- Ottimizzazione delle prestazioni di stampa
- Visualizzazione della stampante e gestione delle code di stampa

### Gestione dei driver della stampante

Per ridurre al minimo il carico amministrativo e i potenziali problemi dei driver di stampa, Citrix consiglia di utilizzare il driver di stampa universale Citrix.

Se la creazione automatica non riesce, per impostazione predefinita il sistema installa un driver di stampa nativo di Windows fornito con Windows. Se un driver non è disponibile, il sistema torna al

driver di stampa universale. Per ulteriori informazioni sui valori predefiniti del driver della stampante, fare riferimento a Procedure consigliate, considerazioni sulla sicurezza e operazioni predefinite.

Se il driver di stampa universale Citrix non è un'opzione per tutti gli scenari, mappare i driver della stampante per ridurre al minimo la quantità di driver installati sulle macchine del sistema operativo multisessione. Inoltre, la mappatura dei driver delle stampanti consente di:

- Consentire alle stampanti specificate di utilizzare solo il driver di stampa universale Citrix
- Consentire o impedire la creazione di stampanti con un driver specificato
- Sostituire i driver obsoleti o corrotti con driver della stampante funzionanti
- Sostituire un driver disponibile sul server Windows con il nome di un driver client

**Impedire l'installazione automatica dei driver della stampante**: l'installazione automatica dei driver di stampa deve essere disabilitata per garantire la coerenza tra le macchine con sistema operativo multisessione. Ciò può essere ottenuto tramite i criteri Citrix, i criteri Microsoft o entrambi. Per impedire l'installazione automatica dei driver delle stampanti nativi di Windows, disabilitare l'impostazione dei criteri Citrix Automatic installation of in-box printer drivers (Installazione automatica dei driver inclusi della stampante).

**Mappare i driver della stampante client**: ogni client fornisce informazioni sulle stampanti lato client durante l'accesso, incluso il nome del driver della stampante. Durante la creazione automatica delle stampanti client, vengono selezionati i nomi dei driver della stampante del server Windows che corrispondono ai nomi dei modelli di stampante forniti dal client. Il processo di creazione automatica utilizza quindi i driver di stampa identificati e disponibili per creare code di stampa client reindirizzate.

Ecco il processo generale per la definizione delle regole di sostituzione dei driver e la modifica delle impostazioni di stampa per i driver della stampante client mappati:

1. Per specificare le regole di sostituzione dei driver per le stampanti client create automaticamente, configurare l'impostazione dei criteri Citrix Printer driver mapping and compatibility (Mappatura e compatibilità del driver della stampante) aggiungendo il nome del driver della stampante client e selezionando il driver del server con il quale si desidera sostituire il driver della stampante client dal menu Find printer driver (Trova driver stampante). È possibile utilizzare caratteri jolly in questa impostazione. Ad esempio, per forzare tutte le stampanti HP a utilizzare un driver specifico, specificare HP* nell'impostazione dei criteri.
2. Per vietare un driver di stampa, selezionare il nome del driver e scegliere l'impostazione Do not create (Non creare).
3. In base alle esigenze, modificare una mappatura esistente, rimuovere una mappatura o modificare l'ordine delle voci dei driver nell'elenco.
4. Per modificare le impostazioni di stampa per i driver della stampante client mappati, selezionare il driver della stampante, fare clic su Settings (Impostazioni) e specificare impostazioni quali qualità di stampa, orientamento e colore. Se si specifica un'opzione di

stampa che il driver della stampante non supporta, tale opzione non ha alcun effetto. Questa impostazione sostituisce le impostazioni della stampante configurate dall'utente durante una sessione precedente.

5. Citrix consiglia di testare in dettaglio il comportamento delle stampanti dopo la mappatura dei driver, poiché alcune funzionalità delle stampanti possono essere disponibili solo con un driver specifico.

Quando gli utenti accedono, il sistema controlla l'elenco di compatibilità dei driver della stampante client prima di configurare le stampanti client.

### Ottimizzare le prestazioni di stampa

Per ottimizzare le prestazioni di stampa, utilizzare Universal Print Server e il driver di stampa universale. I seguenti criteri controllano l'ottimizzazione e la compressione della stampa:

- Universal printing optimization defaults (Impostazioni predefinite per l'ottimizzazione della stampa universale): specifica le impostazioni predefinite per la stampante universale quando viene creata per una sessione.
  - La qualità dell'immagine desiderata specifica il limite di compressione delle immagini predefinito applicato alla stampa universale. Per impostazione predefinita, la qualità standard è abilitata, il che significa che gli utenti possono stampare le immagini solo utilizzando una compressione standard o di qualità ridotta.
  - L'opzione Enable heavyweight compression (Abilita la compressione heavyweight) abilita o disabilita la riduzione della larghezza di banda oltre il livello di compressione impostato dall'opzione Desired image quality (Qualità immagine desiderata), senza perdere la qualità dell'immagine. Per impostazione predefinita, la compressione heavyweight è disabilitata.
  - Le impostazioni di memorizzazione nella cache di immagini e caratteri specificano se memorizzare o meno nella cache immagini e caratteri visualizzati più volte nel flusso di stampa, assicurando che ogni immagine o carattere univoco venga inviato alla stampante una sola volta. Per impostazione predefinita, le immagini e i caratteri incorporati vengono memorizzati nella cache.
  - L'impostazione Allow non-administrators to modify these settings (Consenti a utenti non amministratori di modificare queste impostazioni) specifica se gli utenti possono modificare o meno le impostazioni di ottimizzazione di stampa predefinite all'interno di una sessione. Per impostazione predefinita, gli utenti non sono autorizzati a modificare le impostazioni di ottimizzazione di stampa predefinite.
- Universal printing image compression limit (Limite di compressione delle immagini per la stampa universale): specifica la qualità massima e il livello minimo di compressione disponibile

per le immagini stampate con il driver di stampa universale Citrix. Per impostazione predefinita, il limite di compressione delle immagini è impostato su Best quality (lossless compression) (Migliore qualità [compressione senza perdita di dati]).
- Universal printing print quality limit (Limite della qualità di stampa per la stampa universale): specifica il numero massimo di punti per pollice (dpi) disponibili per la generazione di output stampato in una sessione. Per impostazione predefinita, non viene specificato alcun limite.

Per impostazione predefinita, tutti i processi di stampa destinati alle stampanti di rete vengono instradati dal computer del sistema operativo multisessione, attraverso la rete e direttamente al server di stampa. Si consiglia di instradare i processi di stampa tramite la connessione ICA se la rete ha una latenza sostanziale o una larghezza di banda limitata. A tale scopo, disabilitare l'impostazione dei criteri Citrix Direct connections to print servers (Connessioni dirette ai server di stampa). I dati inviati tramite la connessione ICA sono compressi, quindi si consuma meno larghezza di banda mentre i dati viaggiano attraverso la WAN.

**Migliorare le prestazioni della sessione limitando la larghezza di banda di stampa**: durante la stampa di file da macchine con sistema operativo multisessione alle stampanti utente, altri canali virtuali (ad es. video) potrebbero subire una riduzione delle prestazioni a causa della concorrenza per la larghezza di banda, soprattutto se gli utenti accedono ai server tramite reti più lente. Per evitare tale degradazione, è possibile limitare la larghezza di banda utilizzata dalla stampa degli utenti. Limitando la velocità di trasmissione dei dati per la stampa, è possibile rendere disponibile una maggiore larghezza di banda nel flusso di dati HDX per la trasmissione di dati relativi a video, pressioni dei tasti e mouse.

> **Importante:**
>
> Il limite di larghezza di banda della stampante viene sempre applicato, anche quando non sono in uso altri canali.

Utilizzare le seguenti impostazioni della stampante per la larghezza di banda dei criteri Citrix per configurare i limiti di sessione della larghezza di banda di stampa. Per impostare i limiti per il sito, eseguire questa operazione utilizzando Studio. Per impostare i limiti per i singoli server, eseguire questa operazione utilizzando la Console Gestione Criteri di gruppo in Windows localmente su ogni macchina con sistema operativo multisessione.

- L'impostazione Printer redirection bandwidth limit (Limite della larghezza di banda per il reindirizzamento della stampante) specifica la larghezza di banda disponibile per la stampa in kilobit al secondo (kbps).
- L'impostazione Printer redirection bandwidth limit percent (Percentuale del limite della larghezza di banda per il reindirizzamento della stampante) limita la larghezza di banda disponibile per la stampa a una percentuale della larghezza di banda complessiva disponibile.

  Nota: per specificare la larghezza di banda come percentuale utilizzando l'impostazione Printer

redirection bandwidth limit percent (Percentuale del limite della larghezza di banda per il reindirizzamento della stampante), abilitare anche l'impostazione Overall session bandwidth limit (Limite della larghezza di banda complessiva della sessione).

Se si immettono valori per entrambe le impostazioni, viene applicata l'impostazione più restrittiva (il valore inferiore).

Per ottenere informazioni in tempo reale sulla larghezza di banda di stampa, utilizzare Citrix Director.

### Bilanciare il carico degli Universal Print Server

La soluzione Universal Print Server può essere scalata aggiungendo più server di stampa alla soluzione di bilanciamento del carico. Non esiste un singolo punto di errore, poiché ogni VDA dispone di un proprio bilanciatore del carico per distribuire il carico di stampa a tutti i server di stampa.

Utilizzare le impostazioni dei criteri Universal Print Servers for load balancing (Universal Print Server per il bilanciamento del carico) e Universal Print Server out-of-service threshold (Soglia fuori servizio del server di stampa universale) per distribuire il carico di stampa su tutti i server di stampa nella soluzione di bilanciamento del carico.

In caso di errore imprevisto di un server di stampa, il meccanismo di failover del bilanciatore del carico in ciascun VDA ridistribuisce automaticamente le connessioni della stampante allocate sui server di stampa che presentano problemi agli altri server di stampa disponibili, in modo che tutte le sessioni esistenti e in entrata funzionino normalmente senza ripercussioni sull'esperienza utente e senza richiedere l'intervento immediato dell'amministratore.

Gli amministratori possono monitorare l'attività dei server di stampa con bilanciamento del carico utilizzando un set di contatori delle prestazioni per monitorare quanto segue sul VDA:

- Elenco dei server di stampa con bilanciamento del carico sul VDA e relativo stato (disponibile, non disponibile)
- Numero di connessioni stampante accettate da ciascun server di stampa
- Numero di connessioni stampante non riuscite su ciascun server di stampa
- Numero di connessioni stampante attive su ciascun server di stampa
- Numero di connessioni stampante in sospeso su ciascun server di stampa

### Visualizzare e gestire le code di stampa

La tabella seguente riepiloga dove è possibile visualizzare le stampanti e gestire le code di stampa nel proprio ambiente.

| | | Percorso di stampa |
|---|---|---|
| Stampanti client (stampanti collegate al dispositivo utente) | Percorso di stampa client | Opzione UAC Enabled (UAC abilitato) abilitata: snap-in Gestione stampa disponibile in Microsoft Management Console; opzione UAC Enabled (UAC abilitato) disabilitata: pre-Windows 8: Pannello di controllo, Windows 8: snap-in Gestione stampa |
| Stampanti di rete (stampanti su un server di stampa di rete) | Percorso di stampa di rete | Opzione UAC Enabled (UAC abilitato) abilitata: Server di stampa > snap-in Gestione stampa disponibile in Microsoft Management Console; opzione UAC Enabled (UAC abilitato) disabilitata: Server di stampa > Pannello di controllo |
| Stampanti di rete (stampanti su un server di stampa di rete) | Percorso di stampa client | Opzione UAC Enabled (UAC abilitato) abilitata: Server di stampa > snap-in Gestione stampa disponibile in Microsoft Management Console; opzione UAC Enabled (UAC abilitato) disabilitata: pre-Windows 8: Pannello di controllo, Windows 8: snap-in Gestione stampa |
| Stampanti del server di rete locale (stampanti di un server di stampa di rete aggiunte a una macchina con sistema operativo multisessione) | Percorso di stampa di rete | Opzione UAC Enabled (UAC abilitato) abilitata: Server di stampa > Pannello di controllo; opzione UAC Enabled (UAC abilitato) disabilitata: Server di stampa > Pannello di controllo |

> **Nota:**
>
> Le code di stampa per le stampanti di rete che utilizzano il percorso di stampa di rete sono private e non possono essere gestite tramite il sistema.

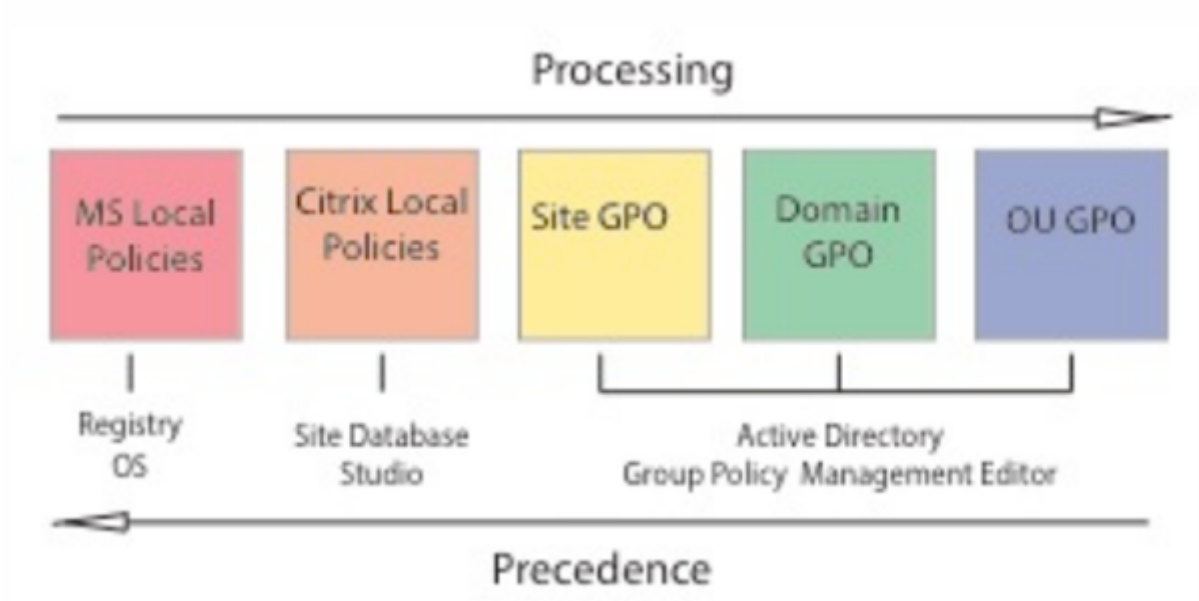
 

# Criteri

January 7, 2024

I criteri sono una raccolta di impostazioni che definiscono la modalità di gestione delle sessioni, della larghezza di banda e della sicurezza per un gruppo di utenti, di dispositivi o di tipi di connessione.

È possibile applicare le impostazioni dei criteri a macchine fisiche e virtuali o agli utenti. È possibile applicare le impostazioni a singoli utenti a livello locale o nei gruppi di protezione in un'Active Directory. Le configurazioni definiscono criteri e regole specifici. Se i criteri non vengono assegnati in modo specifico, le impostazioni vengono applicate a tutte le connessioni.




È possibile applicare criteri a diversi livelli della rete. Le impostazioni dei criteri posizionate a livello di oggetto Criteri di gruppo unità organizzativa hanno la precedenza più alta sulla rete. I criteri a livello di oggetto Criteri di gruppo di dominio sostituiscono i criteri a livello di oggetto Criteri di gruppo del sito. I criteri a livello di oggetto Criteri di gruppo del sito ignorano eventuali criteri in conflitto a livello di Criteri locali di Microsoft e Citrix.

Tutti i criteri locali Citrix vengono creati e gestiti nella console Web Studio e memorizzati nel database del sito. I criteri di gruppo vengono creati e gestiti tramite la Console Gestione Criteri di gruppo Microsoft (GPMC) e archiviati nell'Active Directory. I criteri locali Microsoft vengono creati nel sistema operativo Windows e vengono memorizzati nel Registro di sistema.

Studio utilizza una Modellazione guidata per aiutare gli amministratori a confrontare le impostazioni di configurazione all'interno di modelli e criteri per aiutare a eliminare le impostazioni in conflitto e ridondanti. Gli amministratori possono impostare gli oggetti Criteri di gruppo utilizzando GPMC per

configurare le impostazioni. Possono inoltre applicarli a un gruppo target di utenti a diversi livelli della rete.

Questi oggetti Criteri di gruppo vengono salvati nell'Active Directory. L'accesso alla gestione di queste impostazioni è limitato per la maggior parte del personale IT per motivi di sicurezza.

Le impostazioni vengono unite in base alla priorità e alla loro condizione. Qualsiasi impostazione disabilitata sostituisce un'impostazione abilitata a livello inferiore. Le impostazioni dei criteri non configurati vengono ignorate e non sostituiscono le impostazioni di livello inferiore.

I criteri locali possono inoltre avere conflitti con i criteri di gruppo in Active Directory e potrebbero sovrascriversi reciprocamente a seconda della situazione.

Tutti i criteri vengono elaborati nel seguente ordine:

1. L'utente finale accede a un computer utilizzando le credenziali di dominio.
2. Le credenziali vengono inviate al controller di dominio.
3. Active Directory applica tutti i criteri (utente finale, endpoint, unità organizzativa e dominio).
4. L'utente finale accede all'app Citrix Workspace e accede a un'applicazione o a un desktop.
5. I criteri Citrix e Microsoft vengono elaborati per l'utente finale e la macchina che ospita la risorsa.
6. Active Directory determina la precedenza per le impostazioni dei criteri. Quindi le applica ai registri del dispositivo endpoint e alla macchina che ospita la risorsa.
7. L'utente finale si scollega dalla risorsa. I criteri Citrix per l'utente finale e il dispositivo endpoint non sono più attivi.
8. L'utente finale scollega il dispositivo utente, che rilascia i criteri utente GPO.
9. L'utente finale spegne il dispositivo, che rilascia i criteri della macchina GPO.

Quando si creano criteri per gruppi di utenti, dispositivi e macchine, alcuni membri potrebbero avere requisiti diversi e richiedere eccezioni ad alcune impostazioni dei criteri. Le eccezioni vengono effettuate tramite filtri in Studio e GPMC che determinano chi o cosa viene influenzato dal criterio.

> **Nota:**
>
> Non è supportata la combinazione di criteri Windows e Citrix nello stesso oggetto Criteri di gruppo.

## Lavorare con i criteri

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Configurare i criteri Citrix per controllare l'accesso degli utenti e gli ambienti delle sessioni. I criteri Citrix sono il metodo più efficiente per controllare le impostazioni relative a connessione, sicurezza e larghezza di banda. È possibile creare criteri per gruppi specifici di utenti, dispositivi o tipi di connessione. Ogni criterio può contenere più impostazioni.

## Strumenti per lavorare con i criteri Citrix

È possibile utilizzare i seguenti strumenti con i criteri Citrix.

- **Web Studio.** Se si è amministratori Citrix senza l'autorizzazione per gestire i criteri di gruppo, utilizzare Web Studio per creare criteri per il sito. I criteri creati con Web Studio vengono archiviati nel database del sito e gli aggiornamenti vengono inviati al VDA quando tale VDA effettua la registrazione con il broker o quando un utente si connette a tale VDA.
- **Editor Criteri di gruppo locali** (snap-in della console di gestione Microsoft). Se l'ambiente di rete utilizza Active Directory e si dispone dell'autorizzazione per gestire i criteri di gruppo, è possibile utilizzare l'Editor Criteri di gruppo locali per creare criteri per il sito. Le impostazioni configurate influiscono sugli oggetti Criteri di gruppo specificati nella Console Gestione Criteri di gruppo.

> **Importante:**
>
> Si consiglia di utilizzare l'Editor Criteri di gruppo locale per configurare alcune impostazioni dei criteri. Gli esempi includono le impostazioni relative alla registrazione dei VDA con un controller e le impostazioni relative ai server Microsoft App-V.

## Ordine di elaborazione e precedenza dei criteri

Le impostazioni dei criteri di gruppo vengono elaborate nell'ordine seguente:

1. Oggetto Criteri di gruppo locale
2. Oggetti Criteri di gruppo del sito Virtual Apps and Desktops (archiviati nel database del sito)
3. Oggetti Criteri di gruppo a livello di sito
4. Oggetti Criteri di gruppo a livello di dominio
5. Unità organizzative

Tuttavia, se si verifica un conflitto, le impostazioni dei criteri elaborate per ultime sovrascrivono le impostazioni elaborate in precedenza. L'ordine di precedenza per le impostazioni dei criteri è il seguente:

1. Unità organizzative
2. Oggetti Criteri di gruppo a livello di dominio
3. Oggetti Criteri di gruppo a livello di sito
4. Oggetti Criteri di gruppo del sito Virtual Apps and Desktops (archiviati nel database del sito)
5. Oggetto Criteri di gruppo locale

Ad esempio, un amministratore Citrix utilizza Web Studio per creare un criterio (Criterio A) che abilita il reindirizzamento dei file client per i dipendenti del team di vendita dell'azienda. Nel frattempo, un altro amministratore utilizza l'Editor Criteri di gruppo per creare un criterio (Criterio B) che disabilita il reindirizzamento dei file client per i dipendenti del team di vendita. Quando gli addetti alle vendite accedono ai desktop virtuali, viene applicato il criterio B e viene ignorato il criterio A. Il motivo è che il criterio B è stato elaborato a livello di dominio e il criterio A è stato elaborato a livello di oggetto Criteri di gruppo Virtual Apps and Desktops Site.

Tuttavia, quando un utente avvia una sessione ICA o RDP (Remote Desktop Protocol), le impostazioni della sessione Citrix sostituiscono le stesse impostazioni configurate in un criterio di Active Directory o utilizzando Configurazione host sessione Desktop remoto. Questa impostazione include le impostazioni relative alle impostazioni di connessione client RDP tipiche. Gli esempi per le impostazioni di connessione del client RDP sono lo sfondo del desktop, l'animazione del menu e il contenuto della finestra di visualizzazione durante il trascinamento.

Quando si utilizzano più criteri, è possibile assegnare priorità ai criteri che contengono impostazioni in conflitto. Per ulteriori informazioni, vedere Confrontare i criteri, assegnarvi priorità, modellarli e risolverne i problemi.

### Flusso di lavoro per i criteri Citrix

Il processo di configurazione dei criteri è il seguente:

1. Creare il criterio.
2. Configurare le impostazioni dei criteri.
3. Assegnare il criterio agli oggetti macchina e utente.
4. Assegnare una priorità al criterio.
5. Verificare il criterio effettivo eseguendo la Modellazione guidata Criteri di gruppo Citrix.

> **Nota:**
>
> Per aprire la Modellazione guidata Criteri di gruppo Citrix, andare alla scheda **Policies > Modeling** (Criteri > Modellazione) e quindi fare clic su **Launch Modeling Wizard** (Avvia Modellazione guidata) nella barra delle azioni. La scheda **Modeling** è disponibile in Web Studio su richiesta del cliente.

### Esplorare i criteri e le impostazioni Citrix

Nell'Editor Criteri di gruppo locali, i criteri e le impostazioni vengono visualizzati in due categorie: Configurazione computer e Configurazione utente. Ogni categoria ha un nodo Citrix Policies (Criteri Citrix). Per informazioni dettagliate sull'esplorazione e sull'utilizzo di questo snap-in, vedere la documentazione di Microsoft.

In Web Studio, le impostazioni dei criteri vengono ordinate in categorie in base alla funzione o alla funzionalità a cui si riferiscono. Ad esempio, la sezione **Profile Management** include le impostazioni dei criteri per la gestione dei profili.

- Le impostazioni del computer (impostazioni dei criteri applicabili alle macchine) definiscono il comportamento dei desktop virtuali e vengono applicate all'avvio di un desktop virtuale. Queste impostazioni si applicano anche quando non sono presenti sessioni utente attive sul desktop virtuale. Le impostazioni utente definiscono l'esperienza utente durante la connessione utilizzando ICA. I criteri utente vengono applicati quando un utente si connette o si riconnette utilizzando ICA. I criteri utente non vengono applicati se un utente si connette tramite RDP o accede direttamente alla console.

  Per accedere ai criteri, alle impostazioni o ai modelli, selezionare **Policies** (Criteri) nel riquadro a sinistra di Web Studio.

  - Nella scheda **Policies** (Criteri) sono elencati tutti i criteri. Quando si seleziona un criterio, le schede in basso visualizzano:
    - Overview (Panoramica): elenca nome, priorità, stato attivato/disattivato e descrizione
    - Settings (Impostazioni): elenca tutte le impostazioni configurate
    - Assigned To (Assegnato a): elenca gli oggetti utente e macchina a cui è assegnato il criterio.
      Per ulteriori informazioni, vedere Creare criteri.
  - Nella scheda **Templates** (Modelli) sono elencati i modelli forniti da Citrix e quelli personalizzati che sono stati creati. Quando si seleziona un modello, le schede in basso visualizzano:
    - Descrizione (perché potrebbe essere utile usare il modello);

    - Impostazioni (elenco delle impostazioni configurate). Per ulteriori informazioni, vedere Modelli di criteri.
  - La scheda **Comparison** (Confronto) consente di confrontare le impostazioni di un criterio o di un modello con quelle di altri criteri o modelli. Ad esempio, si potrebbe voler verificare i valori delle impostazioni per garantire la conformità alle procedure consigliate. Per ulteriori informazioni, vedere Confrontare i criteri, assegnarvi priorità, modellarli e risolverne i problemi.

Per cercare un'impostazione in un criterio o in un modello:

1. Selezionare il criterio o il modello.
2. Selezionare **Edit policy** (Modifica criterio) o **Edit Template** (Modifica modello) nella barra delle azioni.
3. Nella pagina **Settings** (Impostazioni) digitare il nome dell'impostazione nel campo **di ricerca**:

   È possibile restringere l'ambito di ricerca selezionando:

   - Una versione specifica del prodotto
   - Una categoria (ad esempio la larghezza di banda)
   - Parole chiave nel nome dell'impostazione
   - La casella di controllo **View selected only** (Visualizza solo selezionati)
   - Per cercare solo le impostazioni che sono state aggiunte al criterio selezionato.

Per eseguire una ricerca non filtrata, selezionare **All Settings** (Tutte le impostazioni).

- Per cercare un'impostazione all'interno di un criterio:

  1. Selezionare il criterio.
  2. Selezionare la scheda **Settings** (Impostazioni) e digitare il nome dell'impostazione.

È possibile perfezionare la ricerca selezionando una versione specifica del prodotto o selezionando una categoria. Per eseguire una ricerca non filtrata, selezionare **All Settings** (Tutte le impostazioni).

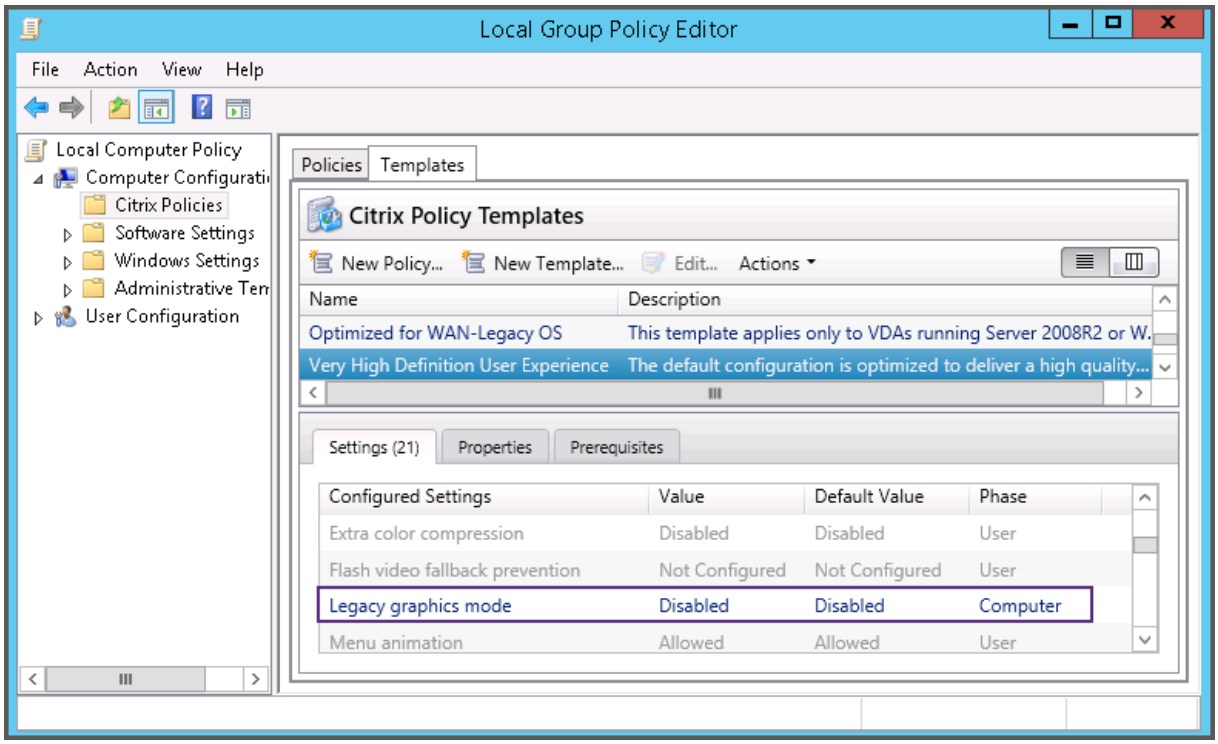
Una volta creato, un criterio è indipendente dal modello utilizzato. È possibile utilizzare il campo **Description** (Descrizione) di un nuovo criterio per tenere traccia del modello di origine utilizzato.

Nell'Editor Criteri di gruppo, le impostazioni computer e utente devono essere applicate separatamente, anche se create da un modello che include entrambi i tipi di impostazioni. In questo esempio si sceglie di utilizzare Very High Definition User Experience (Esperienza utente ad altissima definizione) in Computer Configuration (Configurazione computer):

- La modalità grafica legacy è un'impostazione del computer che viene utilizzata in un criterio creato da questo modello.

- Le impostazioni utente (disabilitate) non vengono utilizzate in un criterio creato da questo modello.




## Modelli di criterio

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

I modelli sono un'origine per la creazione di criteri da un punto di partenza predefinito. I modelli Citrix integrati, ottimizzati per ambienti specifici o condizioni di rete, possono essere utilizzati come:

- Fonte per la creazione di criteri e modelli personalizzati da condividere tra siti.
- Un riferimento per un confronto più semplice dei risultati tra le distribuzioni, in quanto si è in grado di citare i risultati, ad esempio, "…quando si utilizza il modello Citrix x o y…".
- Un metodo per comunicare i criteri al supporto Citrix o a terze parti attendibili mediante l'importazione o l'esportazione di modelli.

I modelli di criteri possono essere importati ed esportati.

### Modelli Citrix incorporati

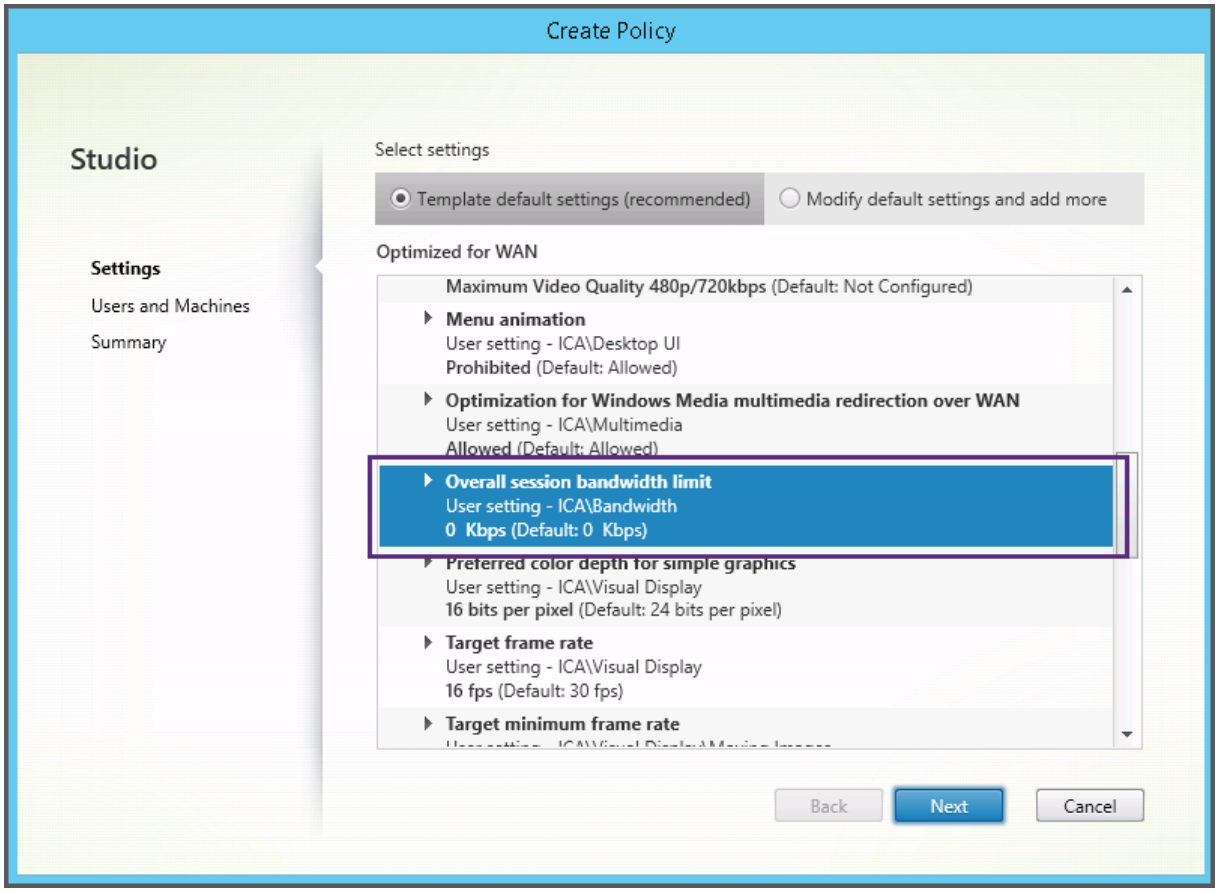
Sono disponibili i seguenti modelli di criteri:

- **Very High Definition User Experience** (Esperienza utente ad altissima definizione). Questo modello applica le impostazioni predefinite che ottimizzano l'esperienza utente. Utilizzare questo modello in scenari in cui più criteri vengono elaborati in ordine di precedenza.
- **High Server Scalability** (Elevata scalabilità server). Applicare questo modello per risparmiare risorse del server. Questo modello consente di bilanciare l'esperienza utente e la scalabilità del server. Offre una buona esperienza utente aumentando al contempo il numero di utenti che è possibile ospitare su un singolo server. Questo modello non utilizza un codec video per la compressione della grafica e impedisce il rendering multimediale sul lato server.
- **High Server Scalability-Legacy OS** (Sistema operativo legacy ad alta scalabilità server). Questo modello di scalabilità server elevata si applica solo ai VDA che eseguono Windows Server 2008 R2 o Windows 7 e versioni precedenti. Questo modello si basa sulla modalità grafica legacy, che è più efficiente per tali sistemi operativi.
- **Optimized for NetScaler SD-WAN** (Ottimizzato per NetScaler SD-WAN). Applicare questo modello per gli utenti che lavorano nelle filiali con NetScaler SD-WAN per ottimizzare la distribuzione di Citrix Virtual Desktops (NetScaler SD-WAN è il nuovo nome di CloudBridge).
- **Optimized for WAN** (Ottimizzato per WAN). Questo modello è destinato ai lavoratori delle filiali che utilizzano una connessione WAN condivisa o postazioni remote con connessioni a bassa larghezza di banda che accedono alle applicazioni con interfacce utente dalla grafica semplice e contenuti multimediali ridotti. Questo modello ottimizza l'efficienza della larghezza di banda a scapito dell'esperienza di riproduzione video e di una parte della scalabilità dei server.
- **Optimized for WAN-Legacy OS** (Ottimizzato per WAN-sistema operativo legacy). Questo modello *Optimized for WAN* (Ottimizzato per WAN) si applica solo ai VDA che eseguono Windows Server 2008 R2 o Windows 7 e versioni precedenti. Questo modello si basa sulla modalità grafica legacy, che è più efficiente per tali sistemi operativi.
- **Security and Control** (Sicurezza e controllo). Utilizzare questo modello in ambienti con bassa tolleranza al rischio, per ridurre al minimo le funzionalità abilitate per impostazione predefinita in Citrix Virtual Apps and Desktops. Questo modello include impostazioni che disabilitano l'accesso alla stampa, agli Appunti, alle periferiche, alla mappatura delle unità, al reindirizzamento delle porte e all'accelerazione Flash sui dispositivi utente. L'applicazione di questo modello potrebbe utilizzare più larghezza di banda e ridurre la densità utente per server.

Sebbene sia consigliato utilizzare i modelli Citrix incorporati con le relative impostazioni predefinite, esistono impostazioni che non hanno un valore specifico consigliato. Ad esempio, **Overall session bandwidth limit** (Limite di larghezza di banda generale della sessione), opzione inclusa nei modelli

Optimized for WAN (Ottimizzato per WAN). In questo caso, il modello mette in evidenza l'impostazione in modo che l'amministratore capisca che è probabile che questa impostazione si applichi allo scenario.




Se si utilizza una distribuzione (gestione dei criteri e VDA) precedente a XenApp e XenDesktop 7.6 FP3 e si richiedono modelli High Server Scalability (Elevata scalabilità server) e Optimized for WAN (Ottimizzato per WAN), utilizzare le versioni del sistema operativo legacy di questi modelli quando sono applicabili.

> **Nota:**
>
> Citrix crea e aggiorna i modelli incorporati. Non è possibile modificare o eliminare questi modelli.

### Creare e gestire i modelli utilizzando Web Studio

Per creare un modello basato su un modello:

1. Accedere a Web Studio e selezionare **Policies** nel riquadro a sinistra.
2. Selezionare la scheda **Templates** (Modelli), quindi selezionare il modello da cui si desidera creare il modello.
3. Selezionare **Create Template** (Crea modello) nella barra delle azioni.

4. Selezionare e configurare le impostazioni dei criteri da includere nel modello. Rimuovere le impostazioni esistenti non appropriate.
5. Immettere un nome per il modello, quindi fare clic su **Finish** (Fine). Il nuovo modello viene visualizzato nella scheda **Templates** (Modelli).

Per creare un modello basato su un criterio:

1. Accedere a Web Studio e selezionare **Policies** nel riquadro a sinistra.
2. Selezionare la scheda **Policies** (Criteri), quindi selezionare il criterio da cui si desidera creare il modello.
3. Selezionare **Save as Template** (Salva come modello) nella barra delle azioni.
4. Selezionare e configurare le nuove impostazioni dei criteri da includere nel modello. Rimuovere le impostazioni esistenti non appropriate.
5. Immettere un nome e una descrizione per il modello, quindi fare clic su **Finish** (Fine).

Per importare un modello:

1. Accedere a Web Studio e selezionare **Policies** nel riquadro a sinistra.
2. Selezionare la scheda **Templates** (Modelli), quindi selezionare **Import Template** (Importa modello).
3. Selezionare il file del modello da importare, quindi fare clic su **Open** (Apri). Se si importa un modello con lo stesso nome di un modello esistente, è possibile scegliere di sovrascrivere il modello esistente o salvare il modello con un nome diverso generato automaticamente.

Per esportare un modello:

1. Accedere a Web Studio e selezionare **Policies** nel riquadro a sinistra.
2. Selezionare la scheda **Templates** (Modelli), quindi **Export Template** (Esporta modello).
3. Selezionare il percorso in cui si desidera salvare il modello, quindi fare clic su **Save** (Salva).

Viene creato un file `.gpt` nella posizione specificata.

### Creare e gestire modelli utilizzando l'Editor Criteri di gruppo

Dall'Editor Criteri di gruppo espandere Computer Configuration or User Configuration (Configurazione computer o Configurazione utente). Espandere il nodo **Criteri** e quindi selezionare **Citrix Policies** (Criteri Citrix). Scegliere l'azione appropriata.

| Attività | Istruzione |
| --- | --- |
| Creare un modello da un criterio esistente | Nella scheda **Policies** (Criteri) selezionare il criterio, quindi selezionare **Actions > Save as Template** (Azioni > Salva come modello). |
| Creare un criterio da un modello esistente | Nella scheda **Templates** (Modelli), selezionare il modello e quindi fare clic su **New Policy** (Nuovo criterio). |
| Creare un modello da un modello esistente | Nella scheda **Templates** (Modelli), selezionare il modello e quindi fare clic su **New Template** (Nuovo modello). |
| Importare un modello | Nella scheda **Templates** (Modelli), selezionare **Actions > Import** (Azioni > Importa). |
| Esportare un modello | Nella scheda **Templates** (Modelli), selezionare **Actions > Export** (Azioni > Esporta). |
| Visualizzare le impostazioni del modello | Nella scheda **Templates** (Modelli), selezionare il modello e quindi fare clic sulla scheda **Settings** (Impostazioni). |
| Visualizzare un riepilogo delle proprietà del modello | Nella scheda **Templates** (Modelli), selezionare il modello e quindi fare clic sulla scheda **Properties** (Proprietà). |
| Visualizzare i prerequisiti dei modelli | Nella scheda **Templates** (Modelli), selezionare il modello e quindi fare clic sulla scheda **Prerequisites** (Prerequisiti). |

### Modelli e amministrazione delegata

I modelli dei criteri vengono memorizzati sulla macchina in cui è stato installato il pacchetto di gestione dei criteri. Questa macchina è la macchina Delivery Controller o la macchina di gestione degli oggetti Criteri di gruppo, non il database del sito di Citrix Virtual Apps and Desktops. Ciò significa che le autorizzazioni amministrative di Windows controllano i file dei modelli di criteri anziché i ruoli e gli ambiti di amministrazione delegata del sito.

Di conseguenza, un amministratore con autorizzazione di sola lettura nel sito può, ad esempio, creare modelli. Tuttavia, poiché i modelli sono file locali, non vengono apportate modifiche all'ambiente.

I modelli personalizzati sono visibili solo all'account utente che li crea e vengono archiviati nel profilo Windows dell'utente. Per esporre ulteriormente un modello personalizzato, creare un criterio da tale modello o esportarlo in una posizione condivisa.

# Creare criteri

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Prima di creare un criterio, decidere su quale gruppo di utenti o dispositivi può influire. Potrebbe essere utile creare un criterio basato sulla funzione del processo utente, sul tipo di connessione, sul dispositivo utente o sulla posizione geografica. È anche possibile utilizzare gli stessi criteri utilizzati per i Criteri di gruppo di Windows Active Directory.

Se è già stato creato un criterio applicabile a un gruppo, è consigliabile modificarlo anziché creare un altro criterio. Dopo aver modificato il criterio, configurare le impostazioni appropriate. Evitare di creare un criterio esclusivamente per abilitare un'impostazione specifica o per impedire che il criterio venga applicato a determinati utenti.

Quando si crea un criterio, è possibile basarlo sulle impostazioni di un modello di criterio e personalizzare le impostazioni in base alle esigenze. È anche possibile crearlo senza utilizzare un modello e aggiungere tutte le impostazioni necessarie.

In Web Studio, i nuovi criteri creati vengono impostati su Disabled (Disabilitato), a meno che la casella di controllo **Enable policy** (Abilita criterio) non sia esplicitamente selezionata.

## Impostazioni dei criteri

Le impostazioni dei criteri possono essere abilitate, disabilitate o non configurate. Per impostazione predefinita, le impostazioni dei criteri non sono configurate, il che significa che non vengono aggiunte a un criterio. Le impostazioni vengono applicate solo quando vengono aggiunte a un criterio.

Alcune impostazioni dei criteri possono essere in uno dei seguenti stati:

- Allowed (Consentito) o Prohibited (Non consentito) consente o impedisce l'azione controllata dall'impostazione. A volte agli utenti è consentito o impedito di gestire l'azione dell'impostazione in una sessione. Ad esempio, se l'impostazione relativa all'animazione del menu è impostata su Allowed (Consentita), gli utenti possono controllare le animazioni dei menu nell'ambiente client.

- Le opzioni Enabled (Abilitato) o Disabled (Disabilitato) abilitano o disabilitano l'impostazione. Se si disabilita un'impostazione, questa non viene abilitata nei criteri con classificazione inferiore.

Inoltre, alcune impostazioni controllano l'efficacia delle impostazioni dipendenti. Ad esempio, il reindirizzamento delle unità client controlla se gli utenti possono accedere alle unità sui propri dispositivi. Sia questa impostazione che l'impostazione **Client network drives** (Unità di rete client) devono essere aggiunte al criterio per consentire agli utenti di accedere alle unità di rete. Se l'impostazione **Client drive redirection** (Reindirizzamento unità client) è disabilitata, gli utenti non possono accedere alle unità di rete, anche se l'impostazione **Client network drives** (Unità di rete client) è abilitata.

In generale, le modifiche delle impostazioni dei criteri che influiscono sulle macchine entrano in vigore al riavvio del desktop virtuale o all'accesso di un utente. Le modifiche delle impostazioni dei criteri che influiscono sugli utenti entrano in vigore al successivo accesso degli utenti. Se si utilizza Active Directory, le impostazioni dei criteri vengono aggiornate quando Active Directory rivaluta i criteri a intervalli di 90 minuti. Inoltre, le impostazioni dei criteri vengono applicate al riavvio del desktop virtuale o all'accesso di un utente.

Per alcune impostazioni dei criteri, è possibile immettere o selezionare un valore quando si aggiunge l'impostazione a un criterio. È possibile limitare la configurazione dell'impostazione selezionando Use default value (Usa valore predefinito). Questa selezione disabilita la configurazione dell'impostazione e consente di utilizzare solo il valore predefinito dell'impostazione quando viene applicato il criterio. Questa selezione è a prescindere dal valore immesso prima di selezionare Use default value (Usa valore predefinito).

Come best practice:

- Assegnare criteri ai gruppi anziché ai singoli utenti. Se si assegnano criteri ai gruppi, le assegnazioni vengono aggiornate automaticamente quando si aggiungono o rimuovono utenti dal gruppo.
- Non abilitare impostazioni in conflitto o in sovrapposizione in Configurazione host sessione Desktop remoto. A volte la Configurazione host sessione Desktop remoto fornisce funzionalità simili alle impostazioni dei criteri Citrix. Quando possibile, mantenere coerenti tutte le impostazioni (abilitate o disabilitate) per facilitare la risoluzione dei problemi.
- Disabilitare i criteri inutilizzati. I criteri senza impostazioni aggiunte generano un'elaborazione non necessaria.

### Assegnazioni dei criteri

Quando si crea un criterio, viene assegnato a determinati utenti e oggetti macchina. Tale criterio viene applicato alle connessioni in base a criteri o regole specifici. In generale, è possibile aggiungere tutte le assegnazioni desiderate a un criterio, in base a una combinazione di criteri.

Se non si specifica alcuna assegnazione o si specificano assegnazioni ma le si disattiva, il criterio viene applicato a **tutte** le connessioni.

> **Nota:**
>
> Le assegnazioni dei criteri sono note anche come filtri dei criteri. Per ulteriori informazioni, vedere i seguenti argomenti:
>
> - Creare, modificare o eliminare un filtro per un criterio
> - Come vengono applicati i filtri?

Nella tabella seguente sono elencate le assegnazioni disponibili:

| Nome assegnazione | Applica un criterio basato su |
|---|---|
| Controllo degli accessi | Condizioni di controllo degli accessi attraverso le quali un client si connette. *Connection type* (Tipo di connessione): indica se applicare il criterio alle connessioni effettuate con o senza NetScaler Gateway. *NetScaler Gateway farm name* (Nome farm NetScaler Gateway): nome del server virtuale NetScaler Gateway. *Access condition* (Condizione di accesso): nome del criterio di analisi degli endpoint o del criterio di sessione da utilizzare. |
| NetScaler SD-WAN | Indica se una sessione utente viene avviata tramite NetScaler SD-WAN. **Nota:** è possibile aggiungere una sola assegnazione NetScaler SD-WAN a un criterio. |
| Indirizzo IP client | Indirizzo IP del dispositivo utente utilizzato per connettersi alla sessione: esempi IPv4: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; esempi IPv6: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54 |
| Nome client | Nome del dispositivo utente. Corrispondenza esatta: NomeABCClient. Utilizzo del carattere jolly: Nome*Client. |
| Gruppo di consegna | Appartenenza al gruppo di consegna. |

| Nome assegnazione | Applica un criterio basato su |
| --- | --- |
| Tipo di gruppo di consegna | Tipo di desktop o applicazione: desktop privato, desktop condiviso, applicazione privata o applicazione condivisa. **Nota:** le opzioni di filtro per desktop privato e desktop condiviso sono disponibili solo per Citrix Virtual Apps and Desktops 7.x. Per ulteriori informazioni, vedere CTX219153. |
| Unità organizzativa (OU) | Unità organizzativa. |
| Tag | Tag. **Nota:** applicare questo criterio a tutte le macchine con tag. I tag delle applicazioni non sono inclusi. |
| Utente o gruppo | Nome utente o gruppo. |

Quando un utente accede, vengono identificati tutti i criteri corrispondenti alle assegnazioni per la connessione. Tali criteri vengono ordinati in ordine di priorità e vengono confrontate più istanze di tutte le impostazioni. Ogni impostazione viene applicata in base alla classificazione di priorità del criterio. Qualsiasi impostazione dei criteri disabilitata ha la precedenza su un'impostazione di livello inferiore abilitata. Le impostazioni dei criteri non configurate vengono ignorate.

> **Importante:**
>
> Quando si configurano i criteri Active Directory e Citrix utilizzando la Console Gestione Criteri di gruppo, le assegnazioni e le impostazioni potrebbero non essere applicate come previsto. Per ulteriori informazioni, vedere CTX127461.

Per impostazione predefinita viene fornito un criterio denominato "Unfiltered"(Non filtrato).

- Se si utilizza Web Studio per gestire i criteri Citrix, le impostazioni aggiunte al criterio Unfiltered (Non filtrato) vengono applicate a tutti i server, i desktop e le connessioni di un sito.
- Se si utilizza l'Editor Criteri di gruppo locali per gestire i criteri Citrix, le impostazioni aggiunte al criterio Unfiltered (Non filtrato) vengono applicate a tutti i siti e le connessioni. I siti e le connessioni devono rientrare nell'ambito degli oggetti Criteri di gruppo (GPO) che includono il criterio. Ad esempio, l'unità organizzativa Vendite include un oggetto Criteri di gruppo denominato Vendite-Stati Uniti che include tutti i membri del team di vendita degli Stati Uniti. L'oggetto Criteri di gruppo Vendite-Stati Uniti è configurato con un criterio Unfiltered (Non filtrato) che include diverse impostazioni dei criteri utente. Quando il responsabile delle vendite degli Stati Uniti accede al sito, le impostazioni del criterio Unfiltered (Non filtrato) vengono applicate automaticamente alla sessione. Questa configurazione è dovuta al fatto che l'utente è un membro dell'oggetto Criteri di gruppo Vendite USA.

La modalità di assegnazione determina se il criterio viene applicato solo alle connessioni che corrispondono a tutti i criteri di assegnazione. Se la modalità è impostata su Allowed (Consenti, impostazione predefinita), il criterio viene applicato solo alle connessioni che corrispondono ai criteri di assegnazione. Se la modalità è impostata su Deny (Nega), il criterio viene applicato se la connessione non corrisponde ai criteri di assegnazione. Gli esempi seguenti illustrano come le modalità di assegnazione influiscono sui criteri Citrix quando sono presenti più assegnazioni.

- **Esempio: assegnazioni di tipo simile con modalità diverse** - Nei criteri con due assegnazioni dello stesso tipo, una impostata su Allow (Consenti) e una impostata su Deny (Nega), l'assegnazione impostata su Deny (Nega) ha la precedenza, a condizione che la connessione soddisfi entrambe le assegnazioni. Ad esempio:

  Il criterio 1 include le seguenti assegnazioni:

  - L'Assegnazione A specifica il gruppo Vendite. La modalità è impostata su Allow (Consenti).
  - L'Assegnazione B specifica l'account del responsabile delle vendite. La modalità è impostata su Deny (Nega).

  Poiché la modalità per l'Assegnazione B è impostata su Deny (Nega), il criterio non viene applicato quando il responsabile delle vendite accede al sito, anche se l'utente è membro del gruppo Vendite.

- **Esempio: assegnazioni di tipo diverso con modalità simili** - Nei criteri con due o più assegnazioni di tipi diversi, impostate su Allow (Consenti), la connessione deve soddisfare almeno un'assegnazione di ogni tipo per applicare il criterio. Ad esempio:

  Il criterio 2 include le seguenti assegnazioni:

  - L'Assegnazione C è un'assegnazione utente che specifica il gruppo Vendite. La modalità è impostata su Allow (Consenti).
  - L'Assegnazione D è un'assegnazione relatiiva all'indirizzo IP client che specifica 10.8.169.* (la rete aziendale). La modalità è impostata su Allow (Consenti).

  Quando il responsabile delle vendite accede al sito dall'ufficio, il criterio viene applicato perché la connessione soddisfa entrambe le assegnazioni.

  Il criterio 3 include le seguenti assegnazioni:

  - L'Assegnazione E è un'assegnazione utente che specifica il gruppo Vendite. La modalità è impostata su Allow (Consenti).
  - L'Assegnazione F è un'assegnazione di controllo degli accessi che specifica le condizioni di connessione di NetScaler Gateway. La modalità è impostata su Allow (Consenti).

  Quando il responsabile delle vendite accede al sito dall'ufficio, il criterio non viene applicato perché la connessione non soddisfa l'Assegnazione F.

### Creare un criterio basato su un modello, utilizzando Web Studio

1. Accedere a Web Studio e selezionare **Policies** nel riquadro a sinistra.
2. Selezionare la scheda **Templates**(Modelli) e selezionare un modello.
3. Selezionare **Create Policy from Template** (Crea criterio da modello) nella barra delle azioni.
4. Per impostazione predefinita, il nuovo criterio utilizza tutte le impostazioni predefinite del modello. In questo caso, è selezionata l'opzione **Template default settings (recommended)** (Impostazioni predefinite modello [consigliate]). Se si desidera modificare le impostazioni, selezionare **Modify defaults settings and add more** (Modifica impostazioni predefinite e aggiungine altre), quindi aggiungere o rimuovere delle impostazioni.
5. Specificare la modalità di applicazione del criterio selezionando una delle seguenti opzioni:
   - **Oggetti utente e macchina selezionati**. Per applicare il criterio a oggetti utente e macchina selezionati, quindi fare clic su **Assign** per selezionare gli oggetti utente e macchina a cui applicare il criterio.
   - **Tutti gli oggetti del sito**. Per applicare il criterio a tutti gli oggetti utente e macchina del sito.
6. Immettere un nome per il criterio. Valutare la possibilità di assegnare al criterio un nome in base alle persone o agli elementi a cui si riferisce, ad esempio Reparto contabilità o Utenti remoti. Se si desidera, aggiungere una descrizione.

   Il criterio è disabilitato per impostazione predefinita; è possibile abilitarlo. L'abilitazione del criterio consente di applicarlo immediatamente agli utenti che accedono. La disabilitazione impedisce l'applicazione del criterio. Se è necessario assegnare priorità al criterio o aggiungere impostazioni in un secondo momento, è consigliabile disabilitare il criterio fino a quando non si è pronti ad applicarlo.

### Creare un criterio utilizzando Web Studio

1. Accedere a Web Studio e selezionare **Policies** nel riquadro a sinistra.
2. Selezionare la scheda **Policies** (Criteri).
3. Selezionare **Create Policy** (Crea criterio) nella barra delle azioni.
4. Aggiungere e configurare le impostazioni dei criteri.
5. Specificare la modalità di applicazione del criterio scegliendo una delle seguenti opzioni:
   - Assign to selected user and machine objects (Assegna a oggetti utente e macchina selezionati), quindi selezionare gli oggetti utente e macchina a cui dovrà essere applicato il criterio.

- Assign to all objects in a site (Assegna a tutti gli oggetti di un sito) per applicare il criterio a tutti gli oggetti utente e macchina nel sito.

6. Immettere un nome per il criterio o accettare l'impostazione predefinita. Valutare la possibilità di assegnare al criterio un nome in base alle persone o agli elementi a cui si riferisce, ad esempio Reparto contabilità o Utenti remoti. Se si desidera, aggiungere una descrizione.

   Il criterio è abilitato per impostazione predefinita, è possibile disabilitarlo. L'abilitazione del criterio consente di applicarlo immediatamente agli utenti che accedono. La disabilitazione impedisce l'applicazione del criterio. Se è necessario assegnare priorità al criterio o aggiungere impostazioni in un secondo momento, è consigliabile disabilitare il criterio fino a quando non si è pronti ad applicarlo.

### Creare e gestire criteri utilizzando l'Editor Criteri di gruppo

Dall'Editor Criteri di gruppo espandere **Computer Configuration or User Configuration** (Configurazione computer o Configurazione utente). Espandere il nodo **Criteri** e quindi selezionare **Citrix Policies** (Criteri Citrix). Scegliere l'azione appropriata:

| Attività | Istruzione |
|---|---|
| Creare un criterio | Nella scheda **Policies** (Criteri), fare clic su **New** (Nuovo). |
| Modificare un criterio esistente | Nella scheda **Policies** (Criteri), selezionare il criterio e quindi fare clic su **Edit** (Modifica). |
| Modificare la priorità di un criterio esistente | Nella scheda **Policies** (Criteri), selezionare il criterio e quindi fare clic su **Higher** (Superiore) o **Lower** (Inferiore). |
| Visualizzare informazioni di riepilogo su un criterio | Nella scheda **Policies** (Criteri), selezionare il criterio e quindi fare clic sulla scheda **Summary** (Riepilogo). |
| Visualizzare e modificare le impostazioni dei criteri | Nella scheda **Policies** (Criteri), selezionare il criterio e quindi fare clic sulla scheda **Settings** (Impostazioni). |
| Visualizzare e modificare i filtri dei criteri | Nella scheda **Policies** (Criteri), selezionare il criterio e quindi fare clic sulla scheda **Filters** (Filtri). Quando si aggiungono più filtri a un criterio, è necessario che vengano soddisfatte tutte le condizioni di filtro perché il criterio venga applicato. |

| Attività | Istruzione |
| --- | --- |
| Abilitare o disabilitare un criterio | Nella scheda **Policies** (Criteri), selezionare il criterio e quindi selezionare **Actions > Enable** (Azioni > Abilita) o **Actions > Disable** (Azioni > Disabilita). |
| Creare un criterio da un modello esistente | Nella scheda **Templates** (Modelli), selezionare il modello e quindi fare clic su **New Policy** (Nuovo criterio). |

## Confrontare i criteri, assegnarvi priorità e risolverne i problemi

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

È possibile utilizzare più criteri per personalizzare l'ambiente allo scopo di soddisfare le esigenze degli utenti in base al loro ruolo, all'ubicazione geografica o ai tipi di connessione. Ad esempio, per una maggiore sicurezza, applicare restrizioni ai gruppi di utenti che interagiscono regolarmente con dati sensibili.

È inoltre possibile creare un criterio che impedisca agli utenti di salvare file sensibili sulle unità client locali. Tuttavia, se alcuni utenti del gruppo di utenti hanno bisogno di accedere alle unità locali, è possibile creare un altro criterio solo per tali utenti. È quindi possibile classificare i due criteri o assegnarvi priorità per controllare quale ha la precedenza. Quando si utilizzano più criteri, è necessario determinare:

- Come stabilire le priorità dei criteri
- Come creare eccezioni
- Come visualizzare il criterio efficace quando i criteri sono in conflitto.

In generale, i criteri sostituiscono impostazioni simili configurate per l'intero sito, per Delivery Controller specifici o sul dispositivo dell'utente. L'eccezione a questo principio è la sicurezza. L'impostazione di crittografia più elevata dell'ambiente sostituisce sempre altre impostazioni e criteri.

L'impostazione di crittografia più elevata include il sistema operativo e le impostazioni di shadowing più restrittive.

I criteri Citrix interagiscono con i criteri impostati nel sistema operativo. In un ambiente Citrix, le impostazioni Citrix sostituiscono le stesse impostazioni configurate in un criterio di Active Directory o utilizzando Configurazione host sessione Desktop remoto. Questa impostazione include le impostazioni relative alle impostazioni di connessione client RDP (Remote Desktop Protocol) tipiche. Le impostazioni tipiche di RDP includono impostazioni come lo sfondo del desktop, l'animazione del menu e il contenuto della finestra di visualizzazione durante il trascinamento.

Alcune impostazioni dei criteri, ad esempio Secure ICA (ICA sicura), devono corrispondere alle impostazioni del sistema operativo. Se altrove è impostato un livello di crittografia con priorità più alta, è possibile ignorare le impostazioni **Secure ICA policy** (Criterio ICA sicuro) specificate nel criterio o quando si distribuiscono applicazioni e desktop.

Ad esempio, le impostazioni di crittografia specificate durante la creazione dei gruppi di consegna devono essere allo stesso livello delle impostazioni di crittografia specificate in tutto l'ambiente.

> **Nota:**
>
> Nel secondo hop di scenari a doppio hop, tenere presente che un sistema operativo VDA a sessione singola si connette a un VDA con sistema operativo multisessione. In questo caso, i criteri Citrix agiscono sulla VDA del sistema operativo a sessione singola come se fosse il dispositivo dell'utente. Ad esempio, considerare che sono impostati criteri per memorizzare nella cache le immagini sul dispositivo utente. In questo esempio le immagini memorizzate nella cache per il secondo hop in uno scenario a doppio hop vengono memorizzate nella cache sulla macchina VDA con sistema operativo a sessione singola.

## Utilizzare la procedura guidata per la modellazione dei criteri

La modellazione dei criteri consente di simulare i criteri abilitati con filtri per scopi di pianificazione e test. Vengono modellati solo i criteri abilitati con filtri. I criteri disabilitati non vengono mai applicati e i criteri abilitati senza filtri vengono sempre applicati.

Eseguire i seguenti passaggi per aprire la procedura guidata **Policy Modeling**:

1. Selezionare **Policies** nella barra di navigazione a sinistra.
2. Selezionare la scheda **Modeling** (Modellazione).
3. Selezionare **Policy Modeling** nella barra delle azioni.
4. Leggere la pagina **Introduction** e fare clic su **Next**.
5. Selezionare utenti o computer. È possibile sfogliare per trovare contenitori oppure utenti o computer specifici. Fare clic su **Next** (Avanti).

6. Scegliere le prove da filtrare. Facoltativamente, è possibile ottenere una simulazione più dettagliata inserendo dettagli aggiuntivi, quali **gruppo di consegna**, **tag**, **indirizzo IP del client**e così via. Fare clic su **Next** (Avanti).
7. Rivedere il riepilogo delle selezioni e fai clic su **Run** (Esegui).

Dopo aver fatto clic su **Run**, la procedura guidata genera un report dei risultati della modellazione. Durante la visualizzazione di questo report, è possibile:

- Selezionare se visualizzare **All settings** (Tutte le impostazioni), **Computer settings**(Impostazioni del computer) o **User settings** (Impostazioni utente) nel menu a discesa.
- Utilizzare la barra di ricerca per cercare impostazioni specifiche.
- Fare clic su un'impostazione specifica per visualizzarne i dettagli. Ad esempio, se a un criterio specifico non sono state applicate tutte le impostazioni utente, il riquadro **Dettagli** mostra il motivo per cui le impostazioni non sono state applicate.
- Fare clic su **Export** (Esporta) per esportare i risultati della modellazione in formato JSON, in formato HTML o in entrambi.

Dopo che è stata eseguita la modellazione dei criteri, saranno disponibili più opzioni. È possibile effettuare le seguenti operazioni:

- **View Modeling Report** (Visualizza report di modellazione): questo apre lo stesso report di modellazione di cui sopra in modo da poterlo visualizzare nuovamente o esportarlo.
- **Rerun Policy Modeling** (Rieseguire la modellazione dei criteri): consente di rieseguire la modellazione dei criteri con lo stesso insieme di criteri selezionati in precedenza e generare nuovi risultati di modellazione. Questo è utile se alcuni criteri sono stati modificati e si desidera vedere come le modifiche influiscono sul modello attuale.
- **Delete Modeling Report** (Elimina report di modellazione): questo elimina il report di modellazione corrente.

### Confrontare criteri e modelli

È possibile confrontare le impostazioni di un criterio o di un modello con le impostazioni degli altri criteri o modelli. Ad esempio, potrebbe essere necessario verificare i valori delle impostazioni per mantenere la conformità alle procedure consigliate. Oppure potrebbe essere necessario confrontare le impostazioni in un criterio o un modello con le impostazioni predefinite che vengono fornite da Citrix.

1. Accedere a Web Studio e selezionare **Policies** nel riquadro a sinistra.
2. Fare clic sulla scheda **Comparison** (Confronto) e quindi su **Select** (Seleziona).
3. Scegliere i criteri o i modelli da confrontare. Per includere i valori predefiniti nel confronto, selezionare la casella di controllo **Compare to default settings** (Confronta con le impostazioni predefinite).

4. Dopo che si è fatto clic su **Compare** (Confronta), le impostazioni configurate vengono visualizzate in colonne.
5. Per visualizzare tutte le impostazioni, selezionare **Show All Settings** (Mostra tutte le impostazioni). Per tornare alla visualizzazione predefinita, selezionare **Show Common Settings** (Mostra impostazioni comuni).

### Assegnare priorità ai criteri

L'assegnazione di priorità ai criteri consente di definire la priorità dei criteri quando contengono impostazioni in conflitto. Quando un utente accede, vengono identificati tutti i criteri corrispondenti alle assegnazioni per la connessione. Tali criteri vengono ordinati in ordine di priorità e vengono confrontate più istanze di tutte le impostazioni. Ogni impostazione viene applicata in base alla classificazione di priorità del criterio.

È possibile assegnare priorità ai criteri dando loro numeri di priorità diversi. Per impostazione predefinita, ai nuovi criteri viene assegnata la priorità più bassa. Se le impostazioni dei criteri sono in conflitto, un criterio con una priorità più alta (il numero di priorità 1 è il più alto) sostituisce un criterio con una priorità inferiore. Le impostazioni vengono unite in base alla priorità e alla loro condizione. Ad esempio, se l'impostazione è disabilitata o abilitata. Qualsiasi impostazione disabilitata sostituisce un'impostazione abilitata di livello inferiore. Le impostazioni dei criteri non configurate vengono ignorate e non sostituiscono le configurazioni delle impostazioni di livello inferiore.

1. Accedere a Web Studio, selezionare **Policies** nel riquadro a sinistra, quindi fare clic sulla scheda **Policies**.
2. Selezionare un criterio.
3. Selezionare **Change Policy Priorities** (Modifica le priorità del criterio) nella barra delle azioni.
4. In **Change Policy Priorities**, modificare le priorità dei criteri utilizzando le icone corrispondenti.
5. Fare clic su **Save** per salvare le modifiche e uscire.

### Eccezioni

Quando si creano criteri per gruppi di utenti, dispositivi utente o macchine, alcuni membri del gruppo potrebbero richiedere eccezioni ad alcune impostazioni dei criteri. È possibile creare eccezioni nei modi seguenti:

- Creando un criterio solo per i membri del gruppo che necessitano delle eccezioni e quindi assegnando al criterio una classificazione più elevata rispetto al criterio per l'intero gruppo
- Utilizzare la modalità Deny (Nega) per un'assegnazione aggiunta al criterio

Un'assegnazione con la modalità impostata su Deny (Nega) applica un criterio solo alle connessioni che non corrispondono ai criteri di assegnazione. Ad esempio, un criterio include le seguenti assegnazioni:

- L'assegnazione A è un'assegnazione di un indirizzo IP client che specifica l'intervallo 208.77.88.*. La modalità è impostata su Allow (Consenti).
- Assignment B è un'assegnazione utente che specifica un determinato account utente. La modalità è impostata su Deny (Nega).

Il criterio viene applicato a tutti gli utenti che accedono al sito con indirizzi IP nell'intervallo specificato nell'Assegnazione A. Tuttavia, il criterio non viene applicato all'utente che accede al sito con l'account utente specificato nell'Assegnazione B.

### Determinare quali criteri si applicano a una connessione

Una connessione potrebbe non rispondere come previsto perché si applicano più criteri. Se a una connessione viene applicato un criterio di priorità più alto, è possibile ignorare le impostazioni configurate nel criterio originale. È possibile calcolare il gruppo di criteri risultante e determinare la modalità di unione delle impostazioni dei criteri finali per una connessione.

È possibile calcolare il valore di Resultant Set of Policy (Gruppo di criteri risultante) nei modi seguenti:

- Utilizzare la procedura guidata **Citrix Group Policy Modeling** (Modellazione Criteri di gruppo Citrix) per simulare uno scenario di connessione e individuare come potrebbero essere applicati i criteri Citrix. È possibile specificare le condizioni per uno scenario di connessione, ad esempio:
  - Controller di dominio
  - Utenti
  - Valori delle prove di assegnazione dei criteri Citrix
  - Impostazioni dell'ambiente simulate come connessione di rete lenta

    Il report prodotto dalla procedura guidata elenca i criteri di Citrix che vengono applicati nello scenario. Poiché ci si connette al controller come utente di dominio, la procedura guidata calcola i risultati utilizzando sia le impostazioni dei criteri del sito che gli oggetti Criteri di gruppo di Active Directory.
- Utilizzare **Group Policy Results** (Risultati dei criteri di gruppo) per generare un report che descrive i criteri Citrix in vigore per un determinato utente e controller. Lo strumento Group Policy Results (Risultati Criteri di gruppo) consente di valutare lo stato attuale degli oggetti Criteri di gruppo nel proprio ambiente e di generare un report. Il report generato descrive come questi oggetti, inclusi i criteri Citrix, vengono attualmente applicati a un determinato utente e controller.

È possibile avviare la modellazione guidata Criteri di gruppo Citrix in Web Studio. In alternativa, è possibile avviare lo strumento Group Policy Results tramite la console di gestione delle politiche di gruppo in Windows.

Le impostazioni dei criteri del sito create utilizzando Web Studio non sono incluse nel set di criteri risultante nei seguenti casi:

- Se si esegue Citrix Group Policy Modeling Wizard da Group Policy Management Console
- Se si esegue lo strumento Group Policy Results dalla console di gestione dei criteri di gruppo

Per verificare di aver ottenuto il set di criteri risultante più completo, Citrix consiglia di avviare la procedura guidata Modellazione Criteri di gruppo Citrix da Web Studio, a meno che non si creino criteri utilizzando solo la Console Gestione Criteri di gruppo.

### Risolvere i problemi relativi ai criteri

Gli utenti, gli indirizzi IP e altri oggetti assegnati possono avere più criteri che si applicano contemporaneamente. Questo scenario può causare conflitti e un criterio potrebbe non comportarsi come previsto. Quando si esegue la Modellazione guidata Criteri di gruppo Citrix o lo strumento Rapporti Criteri di gruppo, si potrebbe scoprire che non vengono applicati criteri alle connessioni utente. In uno scenario di questo tipo, le impostazioni dei criteri non vengono applicate agli utenti che si connettono alle loro applicazioni e ai loro desktop in condizioni che corrispondono ai criteri di valutazione dei criteri. Questa situazione si verifica quando:

- Nessun criterio dispone di assegnazioni che corrispondono ai criteri di valutazione dei criteri.
- I criteri che corrispondono all'assegnazione non hanno impostazioni configurate.
- I criteri che corrispondono all'assegnazione sono disabilitati.

Se si desidera applicare le impostazioni dei criteri alle connessioni che soddisfano i criteri specificati, assicurarsi che:

- I criteri che si desidera applicare a tali connessioni siano abilitati.
- I criteri che si desidera applicare dispongano delle impostazioni appropriate configurate.

## Impostazioni dei criteri predefinite

January 7, 2024

Nelle tabelle seguenti sono elencate le impostazioni dei criteri, le relative impostazioni predefinite e le versioni di VDA (Virtual Delivery Agent) a cui si applicano.

### ICA

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Trasporto adattivo | Off. Utilizzarlo quando si preferisce | VDA 7.13-7.15; da VDA 7.16 alla versione corrente |
| Client clipboard redirection (Reindirizzamento degli Appunti client) | Consentito | Tutte le versioni di VDA |
| Client clipboard write allowed formats (Formati consentiti per la scrittura degli Appunti client) | Nessun formato specificato | Da VDA 7.6 alla versione corrente |
| Desktop launches (Avvii del desktop) | Non consentito | Da VDA per OS multisessione 7 alla versione corrente |
| ICA listener port number (Numero porta listener ICA) | 1494 | Tutte le versioni di VDA |
| Launching of non-published programs during client connection (Avvio di programmi non pubblicati durante la connessione client) | Non consentito | Da VDA per OS multisessione 7 alla versione corrente |
| Limit clipboard client to session transfer size (Limita il client degli Appunti alle dimensioni del trasferimento della sessione) | Disabilitato | VDA 2009 |
| Limit clipboard session to client transfer size (Limita la sessione degli Appunti alle dimensioni del trasferimento del client) | Disabilitato | VDA 2009 |
| Loss tolerant mode (Modalità tollerante alle perdite) | Consentito | VDA 2003. Nota: la modalità di tolleranza alle perdite non è ancora disponibile. Questa versione del VDA la supporta quando è disponibile. |
| Loss tolerant thresholds (Soglie tolleranti alle perdite) | Quando è disponibile la modalità tollerante alle perdite: Perdita di pacchetti: 5%, Latenza: 300 ms (RTT) | Da VDA 2003 alla versione corrente |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Rendezvous protocol (Protocollo Rendezvous) | Disabilitato | Si applica solo alle sessioni HDX stabilite tramite Citrix Cloud. |
| Restrict client clipboard write (Limita scrittura degli Appunti client) | Non consentito | Da VDA 7.6 alla versione corrente |
| Restrict session clipboard write (Limita scrittura degli Appunti di sessione) | Non consentito | Da VDA 7.6 alla versione corrente |
| Session clipboard write allowed formats (Formati consentiti di scrittura degli Appunti di sessione) | Nessun formato specificato | Da VDA 7.6 alla versione corrente |
| Tablet mode toggle (Abilita/disabilita modalità tablet) | Abilitato | Da VDA 7.16 alla versione corrente; per VDA 7.14 e 7.15 LTSR, configurare questa impostazione utilizzando il Registro di sistema. |
| Virtual channel allow list (Elenco degli elementi consentiti dei canali virtuali) | Abilitato | VDA 2109 |

### ICA/distribuzione di Adobe Flash/reindirizzamento Flash

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Flash video fallback prevention (Prevenzione del fallback video Flash) | Non configurato | Da VDA 7.6 FP3 alla versione corrente |
| Flash video fallback prevention error *.swf (Errore di prevenzione del fallback video Flash *.swf) | | Da VDA 7.6 FP3 alla versione corrente |

### ICA/Audio

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Audio adattivo | Abilitato | Si applica sia alle sessioni del sistema operativo a sessione singola che alle sessioni del sistema operativo multisessione di VDA che utilizzano Citrix Virtual Apps and Desktops 2109 o versioni successive. |
| Audio over UDP real-time transport (Audio con trasporto UDP in tempo reale) | Consentito | Tutte le versioni di VDA |
| Audio Plug N Play | Consentito | Da VDA per OS multisessione 7 alla versione corrente |
| Audio quality (Qualità audio) | Alta: audio ad alta definizione | Tutte le versioni di VDA |
| Client audio redirection (Reindirizzamento audio client) | Consentito | Tutte le versioni di VDA |
| Client microphone redirection (Reindirizzamento microfono client) | Consentito | Tutte le versioni di VDA |

### ICA/riconnessione automatica del client

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Auto client reconnect (Riconnessione automatica client) | Consentito | Tutte le versioni di VDA |
| Auto client reconnect authentication (Autenticazione della riconnessione automatica client) | Do not require authentication (Non richiedere l' autenticazione) | Tutte le versioni di VDA |
| Auto client reconnect logging (Registrazione della riconnessione automatica client) | Do not log auto-reconnect events (Non registrare eventi di riconnessione automatica) | Tutte le versioni di VDA |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Auto client reconnect timeout (Timeout di riconnessione automatica client) | 120 secondi | Da VDA 7.13 alla versione corrente |
| Reconnect UI transparency level (Riconnetti livello di trasparenza dell'interfaccia utente) | 80% | Da VDA 7.13 alla versione corrente |

### ICA/larghezza di banda

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Audio redirection bandwidth limit (Limite della larghezza di banda di reindirizzamento audio) | 0 Kbps | Tutte le versioni di VDA |
| Audio redirection bandwidth limit percent (Percentuale del limite della larghezza di banda di reindirizzamento audio) | 0 | Tutte le versioni di VDA |
| Client USB device redirection bandwidth limit (Limite della larghezza di banda di reindirizzamento del dispositivo USB client) | 0 Kbps | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Client USB device redirection bandwidth limit percent (Percentuale del limite della larghezza di banda di reindirizzamento del dispositivo USB client) | 0 | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Clipboard redirection bandwidth limit (Limite della larghezza di banda per il reindirizzamento degli appunti) | 0 Kbps | Tutte le versioni di VDA |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Clipboard redirection bandwidth limit percent (Limite della larghezza di banda per il reindirizzamento degli appunti) | 0 | Tutte le versioni di VDA |
| COM port redirection bandwidth limit (Limite della larghezza di banda di reindirizzamento della porta COM) | 0 Kbps | Tutte le versioni di VDA; per VDA da 7.0 a 7.8, configurare questa impostazione utilizzando il Registro di sistema |
| COM port redirection bandwidth limit percent (Percentuale del limite della larghezza di banda di reindirizzamento della porta COM) | 0 | Tutte le versioni di VDA; per VDA da 7.0 a 7.8, configurare questa impostazione utilizzando il Registro di sistema |
| File redirection bandwidth limit (Limite della larghezza di banda di reindirizzamento file) | 0 Kbps | Tutte le versioni di VDA |
| File redirection bandwidth limit percent (Percentuale del limite della larghezza di banda per il reindirizzamento file) | 0 | Tutte le versioni di VDA |
| HDX MediaStream Multimedia Acceleration bandwidth limit (Limite della larghezza di banda HDX MediaStream Multimedia Acceleration) | 0 Kbps | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 e VDA per OS a sessione singola 7 fino a VDA corrente per sistema operativo multisessione e VDA per sistema operativo a sessione singola |
| HDX MediaStream Multimedia Acceleration bandwidth limit percent (Percentuale del limite della larghezza di banda HDX MediaStream Multimedia Acceleration) | 0 | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| LPT port redirection bandwidth limit (Limite della larghezza di banda per il reindirizzamento della porta LPT) | 0 Kbps | Tutte le versioni di VDA; per VDA da 7.0 a 7.8, configurare questa impostazione utilizzando il Registro di sistema |
| LPT port redirection bandwidth limit percent (Percentuale del limite della larghezza di banda per il reindirizzamento della porta LPT) | 0 | Tutte le versioni di VDA; per VDA da 7.0 a 7.8, configurare questa impostazione utilizzando il Registro di sistema |
| Overall session bandwidth limit (Limite della larghezza di banda complessiva della sessione) | 0 Kbps | Tutte le versioni di VDA |
| Printer redirection bandwidth limit (Limite della larghezza di banda per il reindirizzamento della stampante) | 0 Kbps | Tutte le versioni di VDA |
| Printer redirection bandwidth limit percent (Percentuale del limite della larghezza di banda per il reindirizzamento della stampante) | 0 | Tutte le versioni di VDA |
| TWAIN device redirection bandwidth limit (Limite della larghezza di banda per il reindirizzamento dei dispositivi TWAIN) | 0 Kbps | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| TWAIN device redirection bandwidth limit percent (Percentuale del limite della larghezza di banda per il reindirizzamento dei dispositivi TWAIN) | 0 | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |

### ICA/reindirizzamento bidirezionale del contenuto

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Allow bidirectional content redirection (Consenti reindirizzamento bidirezionale del contenuto) | Non consentito | Da VDA 7.13 alla versione corrente |
| Allowed URLs to be redirected to client (URL consentiti da reindirizzare al client) | vuoto | Da VDA 7.13 alla versione corrente |
| Allowed URLs to be redirected to VDA (URL consentiti da reindirizzare al VDA) | vuoto | Da VDA 7.13 alla versione corrente |
| Client to host (VDA) and client to client bidirectional content redirection (Reindirizzamento del contenuto bidirezionale da client a host (VDA) e da client a client) | | Utilizzare il modello amministrativo di Oggetto Criteri di gruppo dell'app Citrix Workspace |

### ICA/reindirizzamento del contenuto del browser

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Browser content redirection (Reindirizzamento del contenuto del browser) | Consentito | Da VDA 7.16 alla versione corrente |
| Browser content redirection ACL configuration (Configurazione ACL di reindirizzamento del contenuto del browser) | `https://www.youtube.com/*` | Da VDA 7.16 alla versione corrente |
| Browser content redirection Integrated Windows Authentication support (Supporto dell'autenticazione Windows integrata per il reindirizzamento del contenuto del browser) | Non consentito | Da VDA 2106 alla versione corrente |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Browser content redirection proxy configuration (Configurazione proxy per il reindirizzamento del contenuto del browser) | vuoto | Da VDA 7.16 alla versione corrente |
| Browser content redirection server fetch web proxy authentication (Autenticazione del proxy Web per il recupero dal server del reindirizzamento del contenuto del browser) | Non consentito | Da VDA 2012 alla versione corrente |

### ICA/sensori client

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Consentire alle applicazioni di utilizzare la posizione fisica del dispositivo client | Non consentito | VDA 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |

### ICA/interfaccia utente desktop

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Desktop Composition Redirection (Reindirizzamento composizione desktop) | Disabilitato (da 7,6 FP3 fino alla versione corrente); abilitato (da 5,6 a 7,6 FP2) | VDA 5.6, VDA per sistema operativo a sessione singola da 7 fino alla versione 7.15 |
| Desktop Composition Redirection graphics quality (Qualità grafica di reindirizzamento composizione desktop) | Medio | VDA 5.6, VDA per sistema operativo a sessione singola da 7 fino alla versione 7.15 |
| Desktop wallpaper (Sfondo del desktop) | Consentito | Tutte le versioni di VDA |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Menu animation (Animazione menu) | Consentito | Tutte le versioni di VDA |
| View window contents while dragging (Visualizza contenuto della finestra durante il trascinamento) | Consentito | Tutte le versioni di VDA |

### ICA/monitoraggio utente finale

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| ICA round trip calculation (Calcolo del round trip ICA) | Abilitato | Tutte le versioni di VDA |
| ICA round trip calculation interval (Intervallo di calcolo del round trip ICA) | 15 secondi | Tutte le versioni di VDA |
| ICA round trip calculations for idle connections (Calcoli del round trip ICA per le connessioni inattive) | Disabilitato | Tutte le versioni di VDA |

### ICA/esperienza desktop migliorata

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Enhanced Desktop Experience (Esperienza desktop migliorata) | Consentito | Da VDA per OS multisessione 7 alla versione corrente |

### ICA/reindirizzamento file

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Auto connect client drives (Connetti automaticamente le unità client) | Consentito | Tutte le versioni di VDA |
| Client drive redirection (Reindirizzamento delle unità client) | Consentito | Tutte le versioni di VDA |
| Client fixed drives (Unità fisse client) | Consentito | Tutte le versioni di VDA |
| Client floppy drives (Unità floppy client) | Consentito | Tutte le versioni di VDA |
| Client network drives (Unità di rete client) | Consentito | Tutte le versioni di VDA |
| Client optical drives (Unità ottiche client) | Consentito | Tutte le versioni di VDA |
| Client removable drives (Unità rimovibili client) | Consentito | Tutte le versioni di VDA |
| Reindirizzamento da host a client | Disabilitato | Da VDA per OS multisessione 7 alla versione corrente |
| Preserve client drive letters (Mantieni lettere di unità client) | Disabilitato | VDA 5, 5.5, 5.6 FP1, VDA per sistema operativo a sessione singola 7 fino alla versione corrente |
| Read-only client drive access (Accesso alle unità client in sola lettura) | Disabilitato | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Special folder redirection (Reindirizzamento cartelle speciali) | Consentito | Solo distribuzioni dell' interfaccia Web; VDA per OS multisessione 7 fino alla versione corrente |
| Use asynchronous writes (Usa scritture asincrone) | Disabilitato | Tutte le versioni di VDA |

### ICA/grafica

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Allow visually lossless compression (Consenti compressione senza perdita di dati dal punto di vista visivo) | Disabilitato | Da VDA 7.6 alla versione corrente |
| Display memory limit (Visualizza limite di memoria) | 65.536 Kb | VDA 5, 5.5, 5.6 FP1, VDA per sistema operativo a sessione singola 7 fino alla versione corrente |
| Display mode degrade preference (Preferenza per il peggioramento della modalità di visualizzazione) | Degrade color depth first (Degrada prima la profondità del colore) | Tutte le versioni di VDA |
| Dynamic windows preview (Anteprima finestre dinamiche) | Abilitato | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Graphics status indicator | Disabilitato | Da VDA 7.16 alla versione corrente |
| Caching delle immagini | Abilitato | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Legacy graphics mode (Modalità grafica legacy) | Disabilitato | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Maximum allowed color depth (Profondità colore massima consentita) | 32 bit per pixel | Tutte le versioni di VDA |
| Notify user when display mode is degraded (Avvisa l'utente quando la modalità di visualizzazione peggiora) | Disabilitato | Da VDA per OS multisessione 7 alla versione corrente |
| Ottimizzazione per carichi di lavoro grafici 3D | Disabilitato | Da VDA 7.17 alla versione corrente |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Queuing and tossing (Metti in coda e ignora) | Abilitato | Tutte le versioni di VDA |
| Condivisione dello schermo | Disabilitato | VDA 2112 |
| Use video codec for compression (Usa codec video per la compressione) | Use video codec when preferred (Usa codec video quando preferito) | Da VDA 7.6 FP3 alla versione corrente |
| Use hardware encoding for video codec (Usa codifica hardware per codec video) | Abilitato | Da VDA 7.11 alla versione corrente |

### ICA/grafica/memorizzazione nella cache

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Persistent cache threshold (Soglia cache persistente) | 3.000.000 bps | Da VDA per OS multisessione 7 alla versione corrente |

### ICA/grafica/Framehawk

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Framehawk display channel (Canale di visualizzazione Framehawk) | Disabilitato | Da VDA 7.6 FP2 alla versione corrente |
| Framehawk display channel port range (Gamma di porte del canale di visualizzazione Framehawk) | 3224,3324 | Da VDA 7.6 FP2 alla versione corrente |

### ICA/Keep alive

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| ICA keep-alive timeout (Timeout ICA keep-alive) | 60 secondi | Tutte le versioni di VDA |
| ICA keep alives (ICA keep-alive) | Do not send ICA keep alive messages (Non inviare messaggi ICA keep-alive) | Tutte le versioni di VDA |

### ICA/tastiera e IME

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Client keyboard layout synchronization and IME improvement (Sincronizzazione del layout della tastiera client e miglioramento IME) | Disabilitato | Si applica solo al 1912 LTSR CU2 e versioni successive. |
| Abilitare o disabilitare il mapping del layout di tastiera Unicode | Non consentito | Si applica solo al 1912 LTSR CU2 e versioni successive. |
| Show keyboard layout switch pop-up message box (Mostra messaggio a comparsa dell' interruttore di layout della tastiera) | Non consentito | Si applica solo al 1912 LTSR CU2 e versioni successive. |

### ICA/accesso alle app locali

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Allow Local App Access (Consenti accesso alle app locali) | Non consentito | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| URL redirection block list (Elenco di elementi non consentiti per il reindirizzamento URL) | No sites are specified (Nessun sito specificato) | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| URL redirection allow list (Elenco di elementi consentiti per il reindirizzamento URL) | No sites are specified (Nessun sito specificato) | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |

### ICA/esperienza mobile

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Automatic keyboard display (Visualizzazione automatica della tastiera) | Non consentito | VDA 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Launch touch-optimized desktop (Avvia desktop ottimizzato per il tocco) | Consentito | VDA 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente. Questa impostazione è disabilitata e non è disponibile per le macchine Windows 10 e Windows Server 2016. |
| Remote the combo box (Esegui in remoto la casella combinata) | Non consentito | VDA 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |

### ICA/elementi multimediali

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| HTML5 video redirection (Reindirizzamento video HTML5) | Non consentito | Da VDA 7.12 alla versione corrente |
| Limit video quality (Limita la qualità video) | Non configurato | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Microsoft Teams redirection (Reindirizzamento di Microsoft Teams) | Consentito | VDA per OS multisessione 1906 fino alla versione corrente, VDA per sistema operativo a sessione singola 1906 fino alla versione corrente. |
| Multimedia conferencing (Conferenze multimediali) | Consentito | Tutte le versioni di VDA |
| Optimization for Windows Media multimedia redirection over WAN (Ottimizzazione per il reindirizzamento multimediale Windows Media su WAN) | Consentito | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Use GPU for optimizing Windows Media multimedia redirection over WAN (Utilizza la GPU per ottimizzare il reindirizzamento multimediale di Windows Media su WAN) | Non consentito | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Windows Media fallback prevention (Prevenzione del fallback di Windows Media) | Non configurato | Da VDA 7.6 FP3 alla versione corrente |
| Windows Media client-side content fetching (Recupero del contenuto sul lato client di Windows Media) | Consentito | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Reindirizzamento di Windows Media | Consentito | Tutte le versioni di VDA |
| Windows Media Redirection buffer size (Dimensione del buffer di reindirizzamento di Windows Media) | 5 secondi | Da VDA 5, 5.5, 5,6 FP1 alla versione corrente |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Windows Media Redirection buffer size use (Utilizzo delle dimensioni del buffer di reindirizzamento di Windows Media) | Disabilitato | Da VDA 5, 5.5, 5,6 FP1 alla versione corrente |

### ICA/connessioni multi-stream

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Audio over UDP (Audio su UDP) | Consentito | Da VDA per OS multisessione 7 alla versione corrente |
| Audio UDP port range (Intervallo di porte UDP audio) | 16500, 16509 | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Multi-Port policy (Criterio multi-porta) | La porta principale (2598) ha priorità elevata | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Impostazione Multi-Stream computer (Computer multi-flusso) | Disabilitato | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Impostazione Multi-Stream user (Utente multi-flusso) | Disabilitato | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Impostazione Multi-Stream virtual channel stream assignment (Assegnazione del flusso del canale virtuale multi-flusso) | Vedere Impostazione dell'assegnazione del canale virtuale multi-flusso per le assegnazioni di flusso predefinite | VDA 2003 |

### ICA/reindirizzamento porte

| Nome | Impostazione predefinita | VDA |
|---|---|---|
| Auto connect client COM ports (Collegamento automatico delle porte COM client) | Disabilitato | Tutte le versioni di VDA; per VDA da 7.0 a 7.8, configurare questa impostazione utilizzando il Registro di sistema |
| Auto connect client LPT ports (Collegamento automatico delle porte LPT client) | Disabilitato | Tutte le versioni di VDA; per VDA da 7.0 a 7.8, configurare questa impostazione utilizzando il Registro di sistema |
| Client COM port redirection (Reindirizzamento porta COM client) | Non consentito | Tutte le versioni di VDA; per VDA da 7.0 a 7.8, configurare questa impostazione utilizzando il Registro di sistema |
| Client LPT port redirection (Reindirizzamento porta LPT client) | Non consentito | Tutte le versioni di VDA; per VDA da 7.0 a 7.8, configurare questa impostazione utilizzando il Registro di sistema |

### ICA/stampa

| Nome | Impostazione predefinita | VDA |
|---|---|---|
| Client printer redirection (Reindirizzamento stampanti client) | Consentito | Tutte le versioni di VDA |
| Default printer (Stampante predefinita) | Set default printer to the client's main printer (Imposta la stampante principale del client come stampante predefinita) | Tutte le versioni di VDA |
| Printer assignments (Assegnazioni stampante) | La stampante attuale dell'utente viene utilizzata come stampante predefinita per la sessione | Tutte le versioni di VDA |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Printer auto-creation event log preference (Preferenza registro eventi per la creazione automatica della stampante) | Errori e avvisi dei log | Tutte le versioni di VDA |
| Session printers (Stampanti di sessione) | Nessuna stampante specificata | Tutte le versioni di VDA |
| Wait for printers to be created (desktop) (Attendi la creazione delle stampanti [desktop]) | Disabilitato | Tutte le versioni di VDA |

### ICA/stampa/stampanti client

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Auto-create client printers (Creazione automatica delle stampanti client) | Auto-create client printers (Crea automaticamente le stampanti client) | Tutte le versioni di VDA |
| Auto-create generic universal printer (Crea automaticamente la stampante universale generica) | Disabilitato | Tutte le versioni di VDA |
| Nomi delle stampanti client | Nomi delle stampanti standard | VDA 5.6 |
| Direct connections to print servers (Connessioni dirette ai server di stampa) | Abilitato | Tutte le versioni di VDA |
| Printer driver mapping and compatibility (Mappatura e compatibilità dei driver della stampante) | Nessuna regola specificata | Tutte le versioni di VDA |
| Printer properties retention (Conservazione delle proprietà della stampante) | Held in profile only if not saved on client (Conservate nel profilo solo se non salvate sul client) | Tutte le versioni di VDA |
| Retained and restored client printers (Stampanti client conservate e ripristinate) | Consentito | VDA 5, 5.5, 5.6 FP1 |

### ICA/stampa/driver

| Nome | Impostazione predefinita | VDA |
|---|---|---|
| Automatic installation of in-box printer drivers (Installazione automatica dei driver inclusi della stampante) | Abilitato | Tutte le versioni di VDA |
| Universal driver preference (Preferenza driver universale) | EMF, XPS, PCL5c, PCL4, PS | Tutte le versioni di VDA |
| Universal print driver usage (Utilizzo del driver della stampante universale) | Utilizzare la stampa universale solo se il driver richiesto non è disponibile | Tutte le versioni di VDA |

### ICA/stampa/server di stampa universale

| Nome | Impostazione predefinita | VDA |
|---|---|---|
| Universal Print Server enable (Abilitazione server di stampa universale) | Disabilitato | Tutte le versioni di VDA |
| Universal Print Server print data stream (CGP) port (Porta del flusso di dati di stampa (CGP) del server di stampa universale) | 7229 | Tutte le versioni di VDA |
| Universal Print Server print stream input bandwidth limit (kpbs) (Limite della larghezza di banda di input del flusso di stampa del server di stampa universale [kpbs]) | 0 | Tutte le versioni di VDA |
| Universal Print Server web service (HTTP/SOAP) port (Porta del servizio Web del server di stampa universale [HTTP/SOAP]) | 8080 | Tutte le versioni di VDA |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Universal Print Servers for load balancing (Universal Print Server per il bilanciamento del carico) | | Da VDA versione 7.9 alla versione corrente |
| Universal Print Server out-of-service threshold (Soglia fuori servizio del server di stampa universale) | 180 (secondi) | Da VDA versione 7.9 alla versione corrente |

### ICA/stampa/stampa universale

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Universal printing EMF processing mode (Modalità di elaborazione EMF della stampa universale) | Spool directly to printer (Esegui lo spooling direttamente sulla stampante) | Tutte le versioni di VDA |
| Universal printing image compression limit (Limite di compressione delle immagini per la stampa universale) | Best quality (lossless compression) (Migliore qualità [compressione senza perdita di dati]) | Tutte le versioni di VDA |
| Universal printing optimization defaults (Impostazioni predefinite per l'ottimizzazione della stampa universale) | Compressione immagine: Qualità immagine desiderata = Qualità standard, Abilita compressione heavyweight = False; Memorizzazione nella cache di immagini e tipi di carattere: Consenti memorizzazione nella cache delle immagini incorporate = True; Consenti a utenti non amministratori di modificare queste impostazioni = False | Tutte le versioni di VDA |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Universal printing preview preference (Preferenza anteprima di stampa universale) | Do not use print preview for auto-created or generic universal printers (Non utilizzare l'anteprima di stampa per stampanti universali create automaticamente o generiche) | Tutte le versioni di VDA |
| Universal printing print quality limit (Limite della qualità di stampa per la stampa universale) | Nessun limite | Tutte le versioni di VDA |

### ICA/sicurezza

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| SecureICA minimum encryption level (Livello minimo di crittografia SecureICA) | Livello base | Da VDA per OS multisessione 7 alla versione corrente |

### ICA/limiti server

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Server idle timer interval (Intervallo del timer inattivo del server) | 0 millisecondi | Da VDA per OS multisessione 7 alla versione corrente |

### ICA/limiti sessione

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Disconnected session timer (Timer di sessione disconnesso) | Disabilitato | VDA 5, 5.5, 5.6 FP1, VDA per sistema operativo a sessione singola 7 fino alla versione corrente |
| Remote PC Access disconnected session timer (Timer di sessione disconnesso per accesso PC remoto) | Disabilitato | Da VDA per OS a sessione singola 7 fino alla versione corrente |
| Disconnected session timer interval (Intervallo del timer di sessione disconnesso) | 1.440 minuti | VDA 5, 5.5, 5.6 FP1, VDA per sistema operativo a sessione singola 7 fino alla versione corrente |
| Session connection timer (Timer di connessione sessione) | Disabilitato | VDA 5, 5.5, 5.6 FP1, VDA per sistema operativo a sessione singola 7 fino alla versione corrente |
| Session connection timer interval (Intervallo timer di connessione sessione) | 1.440 minuti | VDA 5, 5.5, 5.6 FP1, VDA per sistema operativo a sessione singola 7 fino alla versione corrente |
| Session idle timer (Timer di inattività sessione) | Abilitato | VDA 5, 5.5, 5.6 FP1, VDA per sistema operativo a sessione singola 7 fino alla versione corrente |
| Session idle timer interval (Intervallo del timer di inattività sessione) | 1.440 minuti | VDA 5, 5.5, 5.6 FP1, VDA per sistema operativo a sessione singola 7 fino alla versione corrente |

### ICA/affidabilità sessione

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Session reliability connections (Connessioni di affidabilità delle sessioni) | Consentito | Tutte le versioni di VDA |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Session reliability port number (Numero di porta dell'affidabilità della sessione) | 2598 | Tutte le versioni di VDA |
| Session reliability timeout (Timeout affidabilità sessione) | 180 secondi | Tutte le versioni di VDA |

### ICA/controllo fuso orario

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Estimate local time for legacy clients (Stima l'ora locale per i client legacy) | Abilitato | Da VDA per OS multisessione 7 alla versione corrente |
| Restore Single-session OS time zone on session disconnect or logoff (Ripristina fuso orario del sistema operativo a sessione singola alla disconnessione della sessione o allo scollegamento) | Abilitato | Versione VDA attuale |
| Use local time of client (Usa ora locale del client) | Use server time zone (Usa fuso orario del server) | Tutte le versioni di VDA |

### ICA/dispositivi TWAIN

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Client TWAIN device redirection (Reindirizzamento del dispositivo TWAIN client) | Consentito | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| TWAIN compression level (Livello di compressione TWAIN) | Medio | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |

### ICA/dispositivi USB

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Regole di ottimizzazione dei dispositivi USB client | Abilitato (da VDA 7.6 FP3 fino alla versione corrente); Disabilitato (da VDA 7.11 fino alla versione corrente); per impostazione predefinita, non vengono specificate regole | Da VDA 7.6 FP3 alla versione corrente |
| Client USB device redirection (Reindirizzamento dei dispositivi USB client) | Non consentito | Tutte le versioni di VDA |
| Client USB device redirection rules (Regole di reindirizzamento dei dispositivi USB client) | Nessuna regola specificata | Tutte le versioni di VDA |
| Client USB plug and play device redirection (Reindirizzamento del dispositivo plug and play USB client) | Consentito | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |

### ICA/visualizzazione

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Profondità di colore preferita per grafiche semplici | 24 bit per pixel | Da VDA 7.6 FP3 alla versione corrente |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Target frame rate (Frequenza fotogrammi target) | 30 fps | Tutte le versioni di VDA |
| Qualità visiva | Medio | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |

### ICA/visualizzazione/immagini in movimento

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Minimum image quality (Qualità minima dell' immagine) | Normale | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Moving image compression (Compressione delle immagini in movimento) | Abilitato | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Progressive compression level (Livello di compressione progressivo) | Nessuna | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Progressive compression threshold value (Valore della soglia di compressione progressiva) | 2.147.483.647 Kbps | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Target minimum frame rate (Frequenza fotogrammi target minima) | 10 fps | VDA 5.5, 5.6 FP1, VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |

### ICA/visualizzazione/immagini fisse

| Nome | Impostazione predefinita | VDA |
|---|---|---|
| Extra color compression (Compressione extra dei colori) | Disabilitato | Tutte le versioni di VDA |
| Extra color compression threshold (Soglia della compressione extra dei colori) | 8.192 Kbps | Tutte le versioni di VDA |
| Heavyweight compression (Compressione heavyweight) | Disabilitato | Tutte le versioni di VDA |
| Lossy compression level (Livello di compressione con perdita di dati) | Medio | Tutte le versioni di VDA |
| Lossy compression threshold value (Valore della soglia di compressione con perdita di dati) | 2.147.483.647 Kbps | Tutte le versioni di VDA |

### ICA/WebSocket

| Nome | Impostazione predefinita | VDA |
|---|---|---|
| WebSockets connections (Connessioni WebSocket) | Non consentito | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| WebSockets port number (Numero di porta WebSocket) | 8008 | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| WebSockets trusted origin server list (Elenco dei server di origine attendibili WebSocket) | Il carattere jolly, *, viene utilizzato per considerare attendibili tutti gli URL Receiver per Web | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |

### Gestione del carico

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Concurrent logon tolerance (Tolleranza agli accessi simultanei) | 2 | Da VDA per OS multisessione 7 alla versione corrente |
| CPU usage (Utilizzo della CPU) | Disabilitato | Da VDA per OS multisessione 7 alla versione corrente |
| CPU usage excluded process priority (Priorità dei processi escluso l'utilizzo della CPU) | Below Normal (Inferiore al normale) o Low (Basso) | Da VDA per OS multisessione 7 alla versione corrente |
| Disk usage (Utilizzo del disco) | Disabilitato | Da VDA per OS multisessione 7 alla versione corrente |
| Maximum number of sessions (Numero massimo di sessioni) | 250 | Da VDA per OS multisessione 7 alla versione corrente |
| Memory usage (Utilizzo della memoria) | Disabilitato | Da VDA per OS multisessione 7 alla versione corrente |
| Memory usage base load (Carico base dell'utilizzo della memoria) | Carico zero: 768 MB | Da VDA per OS multisessione 7 alla versione corrente |

### Profile Management/impostazioni avanzate

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Disable automatic configuration (Disabilita configurazione automatica) | Disabilitato | Tutte le versioni di VDA |
| Log off user if a problem is encountered (Scollega l'utente se si verifica un problema) | Disabilitato | Tutte le versioni di VDA |
| Number of retries when accessing locked files (Numero di tentativi durante l'accesso ai file bloccati) | 5 | Tutte le versioni di VDA |
| Process Internet cookie files on logoff (Elabora file dei cookie Internet allo scollegamento) | Disabilitato | Tutte le versioni di VDA |

### Profile Management/impostazioni di base

| Nome | Impostazione predefinita | VDA |
|---|---|---|
| Active write back (Scrittura attiva) | Disabilitato | Tutte le versioni di VDA |
| Enable Profile Management (Abilita Gestione profili) | Disabilitato | Tutte le versioni di VDA |
| Excluded groups (Gruppi esclusi) | Disabled. Vengono elaborati i membri di tutti i gruppi di utenti. | Tutte le versioni di VDA |
| Offline profile support (Supporto profilo offline) | Disabilitato | Tutte le versioni di VDA |
| Path to user store (Percorso dello store utente) | Windows | Tutte le versioni di VDA |
| Process logons of local administrators (Elabora accessi degli amministratori locali) | Disabilitato | Tutte le versioni di VDA |
| Processed groups (Gruppi elaborati) | Disabilitato. Vengono elaborati i membri di tutti i gruppi di utenti. | Tutte le versioni di VDA |

### Profile Management/impostazioni multipiattaforma

| Nome | Impostazione predefinita | VDA |
|---|---|---|
| Cross-platform settings user groups (Gruppi di utenti per le impostazioni multipiattaforma) | Disabilitato. Vengono elaborati tutti i gruppi di utenti specificati in Processed groups (Gruppi elaborati) | Tutte le versioni di VDA |
| Enable cross-platform settings (Abilita impostazioni multipiattaforma) | Disabilitato | Tutte le versioni di VDA |
| Path to cross-platform definitions (Percorso delle definizioni multipiattaforma) | Disabilitato. Non è specificato alcun percorso. | Tutte le versioni di VDA |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Path to cross-platform settings store (Percorso dello store delle impostazioni multipiattaforma) | Disabilitato. Viene utilizzato Windows\PM_CM. | Tutte le versioni di VDA |
| Source for creating cross-platform settings (Origine per la creazione di impostazioni multipiattaforma) | Disabilitato | Tutte le versioni di VDA |

### Profile Management/file system/esclusioni

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Exclusion list - directories (Elenco di esclusione - directory) | Disabilitato. Vengono sincronizzate tutte le cartelle nel profilo utente. | Tutte le versioni di VDA |
| Exclusion list - files (Elenco di esclusione - file) | Disabilitato. Vengono sincronizzati tutti i file nel profilo utente. | Tutte le versioni di VDA |

### Profile Management/file system/sincronizzazione

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Directories to synchronize (Directory da sincronizzare) | Disabilitato. Solo le cartelle non escluse sono sincronizzate. | Tutte le versioni di VDA |
| Files to synchronize (File da sincronizzare) | Disabilitato. Sono sincronizzati solo i file non esclusi. | Tutte le versioni di VDA |
| Folders to mirror (Cartelle di cui eseguire il mirroring) | Disabilitato. Non viene eseguito il mirroring di nessuna cartella. | Tutte le versioni di VDA |

### Profile Management/reindirizzamento cartelle

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Grant administrator access (Concedi accesso all' amministratore) | Disabilitato | Tutte le versioni di VDA |
| Include domain name (Includi nome di dominio) | Disabilitato | Tutte le versioni di VDA |

### Profile Management/reindirizzamento cartelle/AppData(roaming)

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Percorso AppData(Roaming) | Disabilitato. Non è specificata alcuna posizione. | Tutte le versioni di VDA |
| Impostazioni di reindirizzamento per AppData(Roaming) | I contenuti vengono reindirizzati al percorso UNC specificato nelle impostazioni dei criteri del percorso AppData(Roaming) | Tutte le versioni di VDA |

### Profile Management/reindirizzamento cartelle/contatti

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Contacts path (Percorso contatti) | Disabilitato. Non è specificata alcuna posizione. | Tutte le versioni di VDA |
| Impostazioni di reindirizzamento per Contatti | I contenuti vengono reindirizzati al percorso UNC specificato nelle impostazioni dei **criteri del percorso Contatti** | Tutte le versioni di VDA |

### Profile Management/reindirizzamento cartelle/desktop

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Desktop path (Percorso Desktop) | Disabilitato. Non è specificata alcuna posizione. | Tutte le versioni di VDA |
| Impostazioni di reindirizzamento per Desktop | I contenuti vengono reindirizzati al percorso UNC specificato nelle impostazioni dei **criteri del percorso Desktop** | Tutte le versioni di VDA |

### Profile Management/reindirizzamento cartelle/Documenti

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Documents path (Percorso Documenti) | Disabilitato. Non è specificata alcuna posizione. | Tutte le versioni di VDA |
| Impostazioni di reindirizzamento per Documenti | Il contenuto viene reindirizzato al percorso UNC specificato nelle impostazioni dei **criteri del percorso Documenti** | Tutte le versioni di VDA |

### Profile Management/reindirizzamento cartelle/Download

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Downloads path (Percorso Download) | Disabilitato. Non è specificata alcuna posizione. | Tutte le versioni di VDA |
| Impostazioni di reindirizzamento per Download | I contenuti vengono reindirizzati al percorso UNC specificato nelle impostazioni dei **criteri del percorso Download** | Tutte le versioni di VDA |

### Profile Management/reindirizzamento cartelle/Preferiti

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Favorites path (Percorso Preferiti) | Disabilitato. Non è specificata alcuna posizione. | Tutte le versioni di VDA |
| Impostazioni di reindirizzamento per Preferiti | I contenuti vengono reindirizzati al percorso UNC specificato nelle impostazioni dei **criteri del percorso Preferiti** | Tutte le versioni di VDA |

### Profile Management/reindirizzamento cartelle/Collegamenti

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Links path (Percorso Collegamenti) | Disabilitato. Non è specificata alcuna posizione. | Tutte le versioni di VDA |
| Impostazioni di reindirizzamento per Collegamenti | I contenuti vengono reindirizzati al percorso UNC specificato nelle impostazioni dei **criteri del percorso Collegamenti** | Tutte le versioni di VDA |

### Profile Management/reindirizzamento cartelle/Musica

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Music path (Percorso Musica) | Disabilitato. Non è specificata alcuna posizione. | Tutte le versioni di VDA |
| Impostazioni di reindirizzamento per Musica | I contenuti vengono reindirizzati al percorso UNC specificato nelle impostazioni dei **criteri del percorso Musica** | Tutte le versioni di VDA |

### Profile Management/reindirizzamento cartelle/Immagini

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Pictures path (Percorso Immagini) | Disabilitato. Non è specificata alcuna posizione. | Tutte le versioni di VDA |
| Impostazioni di reindirizzamento per Immagini | I contenuti vengono reindirizzati al percorso UNC specificato nelle impostazioni dei **criteri del percorso Immagini** | Tutte le versioni di VDA |

### Profile Management/reindirizzamento cartelle/Giochi salvati

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Saved Games path (Percorso Giochi salvati) | Disabilitato. Non è specificata alcuna posizione. | Tutte le versioni di VDA |
| Impostazioni di reindirizzamento per Giochi salvati | I contenuti vengono reindirizzati al percorso UNC specificato nelle impostazioni dei **criteri del percorso Giochi salvati** | Tutte le versioni di VDA |

### Profile Management/reindirizzamento cartelle/Ricerche

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Searches path (Percorso Ricerche) | Disabilitato. Non è specificata alcuna posizione. | Tutte le versioni di VDA |
| Impostazioni di reindirizzamento per Ricerche | I contenuti vengono reindirizzati al percorso UNC specificato nelle impostazioni dei **criteri del percorso Ricerche** | Tutte le versioni di VDA |

### Profile Management/reindirizzamento cartelle/Menu Start

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Start Menu path (Percorso Menu Start) | Disabilitato. Non è specificata alcuna posizione. | Tutte le versioni di VDA |
| Impostazioni di reindirizzamento per Menu Start | Il contenuto viene reindirizzato al percorso UNC specificato nelle impostazioni dei criteri del percorso Menu Start | Tutte le versioni di VDA |

### Gestione profilo/reindirizzamento cartelle/Video

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Video path (Percorso Video) | Disabled. Non è specificata alcuna posizione. | Tutte le versioni di VDA |
| Impostazioni di reindirizzamento per Video | I contenuti vengono reindirizzati al percorso UNC specificato nelle impostazioni dei **criteri del percorso Video** | Tutte le versioni di VDA |

### Profile Management/impostazioni dei log

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Active Directory actions (Azioni di Active Directory) | Disabilitato | Tutte le versioni di VDA |
| Common information (Informazioni comuni) | Disabilitato | Tutte le versioni di VDA |
| Common warnings (Avvisi comuni) | Disabilitato | Tutte le versioni di VDA |
| Enable logging (Abilita registrazione) | Disabilitato | Tutte le versioni di VDA |
| File system actions (Azioni del file system) | Disabilitato | Tutte le versioni di VDA |
| File system notifications (Notifiche del file system) | Disabilitato | Tutte le versioni di VDA |
| Logoff (Scollega) | Disabilitato | Tutte le versioni di VDA |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Logon (Accedi) | Disabilitato | Tutte le versioni di VDA |
| Maximum size of the log file (Dimensioni massime del file di log) | 1048576 | Tutte le versioni di VDA |
| Path to log file (Percorso del file di log) | Disabled. I file di log vengono salvati nella posizione predefinita, %System-Root%\System32\Logfiles\UserProfileManager. | Tutte le versioni di VDA |
| Personalized user information (Informazioni utente personalizzate) | Disabilitato | Tutte le versioni di VDA |
| Policy values at logon and logoff (Valori dei criteri all' accesso e allo scollegamento) | Disabilitato | Tutte le versioni di VDA |
| Registry actions (Azioni del Registro di sistema) | Disabilitato | Tutte le versioni di VDA |
| Registry differences at logoff (Differenze del Registro di sistema allo scollegamento) | Disabilitato | Tutte le versioni di VDA |

### Profile Management/gestione del profilo

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Delay before deleting cached profiles (Attendi prima di eliminare i profili memorizzati nella cache) | 0 | Tutte le versioni di VDA |
| Delete locally cached profiles on logoff (Elimina i profili memorizzati nella cache locale allo scollegamento) | Disabilitato | Tutte le versioni di VDA |
| Local profile conflict handling (Gestione dei conflitti di profilo locali) | Use local profile (Utilizza profilo locale) | Tutte le versioni di VDA |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Migration of existing profiles (Migrazione dei profili esistenti) | Local and roaming (Locali e mobili) | Tutte le versioni di VDA |
| Path to the template profile (Percorso del profilo del modello) | Disabled. I nuovi profili utente vengono creati dal profilo utente predefinito sul dispositivo a cui un utente accede per la prima volta. | Tutte le versioni di VDA |
| Template profile overrides local profile (Il profilo del modello sostituisce il profilo locale) | Disabilitato | Tutte le versioni di VDA |
| Template profile overrides roaming profile (Il profilo del modello sostituisce il profilo mobile) | Disabilitato | Tutte le versioni di VDA |
| Template profile used as a Citrix mandatory profile for all logons (Profilo del modello utilizzato come profilo Citrix obbligatorio per tutti gli accessi) | Disabilitato | Tutte le versioni di VDA |

### Profile Management/Registro di sistema

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Elenco di esclusione | Disabled. Tutte le chiavi del Registro di sistema nell'hive HKCU vengono elaborate quando un utente si disconnette. | Tutte le versioni di VDA |
| Inclusion list (Elenco di inclusione) | Disabled. Tutte le chiavi del Registro di sistema nell'hive HKCU vengono elaborate quando un utente si disconnette. | Tutte le versioni di VDA |

### Profile Management/profili utente in streaming

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Always cache (Memorizza sempre nella cache) | Disabilitato | Tutte le versioni di VDA |
| Always cache size (Memorizza sempre nella cache in base alle dimensioni) | 0 MB | Tutte le versioni di VDA |
| Profile streaming (Streaming del profilo) | Disabilitato | Tutte le versioni di VDA |
| Streamed user profile groups (Gruppi di profili utente in streaming) | Disabled. Tutti i profili utente all'interno di un'unità organizzativa vengono elaborati normalmente. | Tutte le versioni di VDA |
| Timeout for pending area lock files (days) (Timeout per i file bloccati nell'area in sospeso [giorni]) | 1 giorno | Tutte le versioni di VDA |

### Receiver

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| StoreFront accounts list (Elenco account StoreFront) | Non sono specificati negozi | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |

### Livello di personalizzazione utente

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| User Layer Repository Path (Percorso del repository del livello utente) | Disabled. Nessun percorso specificato. | VDA 19.12 e versioni successive |

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Dimensione livello utente in GB | 10 GB. Un livello utente è un disco con thin provisioning che si espande fino alle dimensioni impostate. Le dimensioni dei livelli utente non diminuiscono mai. | VDA 19.12 o versioni successive |

### Virtual Delivery Agent

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Controller registration IPv6 netmask (Netmask IPv6 di registrazione controller) | Nessuna maschera di rete specificata | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Controller registration port (Porta di registrazione del controller) | 80 | Tutte le versioni di VDA |
| Controller SIDs (SID controller) | Nessun SID specificato | Tutte le versioni di VDA |
| Controllers (Controller) | Nessun controller specificato | Tutte le versioni di VDA |
| Enable auto update of controllers (Abilita aggiornamento automatico dei controller) | Abilitato | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Only use IPv6 controller registration (Utilizza solo la registrazione del controller IPv6) | Disabilitato | VDA per OS multisessione 7 fino alla versione corrente, VDA per OS a sessione singola 7 fino alla versione corrente |
| Sute GUID (GUID sito) | Nessun GUID specificato | Tutte le versioni di VDA |

### Virtual Delivery Agent/HDX 3D Pro

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Enable lossless (Abilita senza perdita di dati) | Abilitato | VDA 5.5, 5.6 FP1 |
| HDX 3D Pro quality settings (Impostazioni di qualità HDX 3D Pro) | | VDA 5.5, 5.6 FP1 |

### Virtual Delivery Agent/monitoraggio

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Enable process monitoring (Abilita il monitoraggio dei processi) | Disabilitato | Da VDA 7.11 alla versione corrente |
| Enable resource monitoring (Abilita il monitoraggio delle risorse) | Abilitato | Da VDA 7.11 alla versione corrente |

### IP virtuale

| Nome | Impostazione predefinita | VDA |
| --- | --- | --- |
| Virtual IP loopback support (Supporto per loopback dell'IP virtuale) | Disabilitato | Da VDA 7.6 alla versione corrente |
| Virtual IP virtual loopback programs list (Elenco dei programmi di loopback virtuale dell'IP virtuale) | Nessuna | Da VDA 7.6 alla versione corrente |

## Riferimento alle impostazioni dei criteri

January 7, 2024

I criteri includono impostazioni che vengono applicate quando il criterio viene abilitato. Le descrizioni contenute in questa sezione indicano anche se sono necessarie altre impostazioni per abilitare una funzionalità o se sono simili a un'impostazione.

### Riferimenti rapidi

Nelle tabelle seguenti sono elencate le impostazioni che è possibile configurare all'interno di un criterio. Individuare l'attività che si desidera completare nella colonna di sinistra, quindi individuare l'impostazione corrispondente nella colonna di destra.

Un elenco completo di tutte le impostazioni dei criteri è disponibile in formato .CHM (Compiled HTML) e in formato .CSV. Questi file sono disponibili nella cartella `\program files\citrix\grouppolicy` sul server in cui è installato il broker (Delivery Controller). È inoltre possibile scaricare la versione più recente delle impostazioni dei criteri facendo clic qui.

### Audio

| Per questa attività | Utilizzare questa impostazione |
|---|---|
| Controllare se consentire l'uso di più dispositivi audio | Audio Plug N Play |
| Controllare se consentire l'ingresso audio dai microfoni sul dispositivo utente | Client microphone redirection (Reindirizzamento microfono client) |
| Controllare la qualità audio sul dispositivo utente | Audio quality (Qualità audio) |
| Controllare la mappatura audio per gli altoparlanti sul dispositivo utente | Client audio redirection (Reindirizzamento audio client) |

### Larghezza di banda per i dispositivi utente

| Per limitare la larghezza di banda utilizzata per | Utilizzare questa impostazione |
|---|---|
| Mappatura audio client | Audio redirection bandwidth limit (Limite di larghezza di banda di reindirizzamento audio) o Audio redirection bandwidth limit percent (Percentuale del limite di larghezza di banda di reindirizzamento audio) |
| Tagliare e incollare utilizzando gli Appunti locali | Clipboard redirection bandwidth limit (Limite di larghezza di banda per il reindirizzamento degli Appunti) o Clipboard redirection bandwidth limit percent (Percentuale del limite della larghezza di banda per il reindirizzamento degli Appunti) |

| Per limitare la larghezza di banda utilizzata per | Utilizzare questa impostazione |
| --- | --- |
| Accesso in una sessione alle unità client locali | File redirection bandwidth limit (Limite di larghezza di banda di reindirizzamento file) o File redirection bandwidth limit percent (Percentuale del limite della larghezza di banda di reindirizzamento file) |
| Accelerazione multimediale HDX MediaStream | HDX MediaStream Multimedia Acceleration bandwidth limit (Limite di larghezza di banda dell'accelerazione multimediale HDX MediaStream) o HDX MediaStream Multimedia Acceleration bandwidth limit percent (Percentuale del limite di larghezza di banda dell'accelerazione multimediale HDX MediaStream) |
| Sessione client | Overall session bandwidth limit (Limite della larghezza di banda complessiva della sessione) |
| Stampa | Printer redirection bandwidth limit (Limite di larghezza di banda del reindirizzamento della stampante) o Printer redirection bandwidth limit percent (Percentuale del limite della larghezza di banda di reindirizzamento della stampante) |
| Dispositivi TWAIN (come una fotocamera o uno scanner) | TWAIN device redirection bandwidth limit (Limite di larghezza di banda di reindirizzamento dei dispositivi TWAIN) o TWAIN device redirection bandwidth limit percent (Percentuale del limite di larghezza di banda per il reindirizzamento dei dispositivi TWAIN) |
| Dispositivi USB | Client USB device redirection bandwidth limit (Limite di larghezza di banda di reindirizzamento dei dispositivi USB client) o Client USB device redirection bandwidth limit percent (Percentuale del limite di larghezza di banda di reindirizzamento dei dispositivi USB client) |

### Reindirizzamento delle unità client e dei dispositivi utente

| Per questa attività | Utilizzare questa impostazione |
| --- | --- |
| Controllare se le unità sul dispositivo utente sono connesse o meno quando gli utenti accedono al server | Auto connect client drives (Connetti automaticamente le unità client) |
| Controllare il trasferimento dei dati delle operazioni di copia e incolla tra il server e gli Appunti locali | Client clipboard redirection (Reindirizzamento degli Appunti client) |
| Controllare il modo in cui le unità vengono mappate dal dispositivo utente | Client drive redirection (Reindirizzamento delle unità client) |
| Controllare se i dischi rigidi locali degli utenti sono disponibili in una sessione | Client fixed drives (Unità fisse client) e Client drive redirection (Reindirizzamento delle unità client) |
| Controllare se le unità floppy locali degli utenti sono disponibili in una sessione | Client floppy drives (Unità floppy client) e Client drive redirection (Reindirizzamento delle unità client) |
| Controllare se le unità di rete degli utenti sono disponibili in una sessione | Client network drives (Unità di rete client) e Client drive redirection (Reindirizzamento delle unità client) |
| Controllare se le unità CD, DVD o Blu-ray locali degli utenti sono disponibili in una sessione | Unità ottiche client e reindirizzamento delle unità client |
| Controllare se le unità rimovibili locali degli utenti sono disponibili in una sessione | Client removable drives (Unità rimovibili client) e Client drive redirection (Reindirizzamento delle unità client) |
| Controllare se i dispositivi TWAIN degli utenti, come scanner e fotocamere, sono disponibili in una sessione e controllare la compressione dei trasferimenti di dati delle immagini | Client TWAIN device redirection (Reindirizzamento dei dispositivi TWAIN client); TWAIN compression redirection (Reindirizzamento della compressione TWAIN) |
| Controllare se i dispositivi USB sono disponibili in una sessione | Client USB device redirection (Reindirizzamento dei dispositivi USB client) e Client USB device redirection rules (Regole di reindirizzamento dei dispositivi USB client) |
| Migliorare la velocità di scrittura e copia di file su un disco client su una rete WAN | Use asynchronous writes (Usa scritture asincrone) |

### Reindirizzamento del contenuto

| Per questa attività | Utilizzare questa impostazione |
| --- | --- |
| Controllare se utilizzare il reindirizzamento del contenuti dal server al dispositivo utente | Reindirizzamento da host a client |

### Interfaccia utente desktop

| Per questa attività | Utilizzare questa impostazione |
| --- | --- |
| Controllare se lo sfondo del desktop viene utilizzato o meno nelle sessioni degli utenti | Desktop wallpaper (Sfondo del desktop) |
| Visualizzare il contenuto della finestra mentre viene trascinata | View window contents while dragging (Visualizza contenuto della finestra durante il trascinamento) |

### Elementi grafici e multimediali

> **Importante:**
>
> Il criterio Flash rimane solo per consentire ai clienti con VDA meno recenti di utilizzare controller più recenti (ad esempio, i controller versione 1912) e utilizzare ancora Flash. Questa versione di VDA non supporta Flash.

| Per questa attività | Utilizzare questa impostazione |
| --- | --- |
| Controllare il numero massimo di fotogrammi al secondo inviati ai dispositivi utente dai desktop virtuali | Target frame rate (Frequenza fotogrammi target) |
| Controllare la qualità visiva delle immagini visualizzate sul dispositivo utente | Qualità visiva |

| Per questa attività | Utilizzare questa impostazione |
| --- | --- |
| Controllare se i siti web possono visualizzare contenuti Flash quando si accede a tali contenuti nelle sessioni | Flash server-side content fetching URL list (Elenco di URL di recupero contenuti sul lato server Flash); Flash URL compatibility list (Elenco di compatibilità URL Flash); Flash video fallback prevention policy setting (Impostazione dei criteri di prevenzione del fallback video Flash); Flash video fallback prevention error *.swf (Errore di prevenzione del fallback video Flash *.swf) |
| Controllare la compressione dei video di cui viene eseguito il rendering sul server | Use video codec for compression (Utilizza codec video per la compressione); Use hardware encoding for video codec (Utilizza la codifica hardware per codec video) |
| Controllare la distribuzione di contenuti web multimediali HTML5 agli utenti | HTML5 video redirection (Reindirizzamento video HTML5) |

### Assegnare priorità al traffico di rete multi-flusso

| Per questa attività | Utilizzare questa impostazione |
| --- | --- |
| Specificare le porte per il traffico ICA tra più connessioni e stabilire le priorità di rete | Multi-Port policy (Criterio multi-porta) |
| Abilitare il supporto per connessioni multi-flusso tra server e dispositivi utente | Multi-Stream (computer and user settings) (Multi-flusso [impostazioni del computer e dell'utente]) |

### Stampa

| Per questa attività | Utilizzare questa impostazione |
| --- | --- |
| Controllare la creazione di stampanti client sul dispositivo utente | Auto-create client printers (Crea automaticamente stampanti client) e Client printer redirection (Reindirizzamento stampanti client) |

| Per questa attività | Utilizzare questa impostazione |
| --- | --- |
| Controllare la posizione in cui sono memorizzate le proprietà della stampante | Printer properties retention (Conservazione delle proprietà della stampante) |
| Controllare se il client o il server elabora le richieste di stampa | Direct connections to print servers (Connessioni dirette ai server di stampa) |
| Controllare se gli utenti possono accedere alle stampanti collegate ai propri dispositivi utente | Client printer redirection (Reindirizzamento stampanti client) |
| Controllare l'installazione di driver Windows nativi durante la creazione automatica di stampanti client e di rete | Automatic installation of in-box printer drivers (Installazione automatica dei driver inclusi della stampante) |
| Controllare quando utilizzare il driver della stampante universale | Universal print driver usage (Utilizzo del driver della stampante universale) |
| Scegliere una stampante in base alle informazioni di una sessione utente mobile | Default printer (Stampante predefinita) |
| Bilanciare il carico e impostare la soglia di failover per server di stampa universali | Universal Print Servers for load balancing (Server di stampa universali per il bilanciamento del carico); Universal Print Servers out-of-service threshold (Soglia fuori servizio dei server di stampa universali) |

> **Nota:**
>
> I criteri non possono essere utilizzati per abilitare uno screen saver in una sessione desktop o applicazione. Per gli utenti che richiedono screen saver, lo screen saver può essere implementato sul dispositivo utente.

## Impostazioni dei criteri ICA

April 3, 2024

> **Nota:**
>
> Questa pagina fornisce descrizioni e valori di configurazione supportati per le impostazioni dei criteri ICA. Per ulteriori informazioni su come lavorare con i criteri, vedere la sezione Lavorare con i criteri.

### Trasporto adattivo

Questa impostazione consente o impedisce il trasporto dei dati tramite EDT come opzione principale e tramite TCP come fallback.

Per impostazione predefinita, il trasporto adattivo è abilitato (**Preferred** [Preferito]) e quando è possibile viene utilizzato EDT, con TCP come fallback. È possibile modificarne l'impostazione in base alle esigenze:

- **Preferred** (Preferito). Il trasporto adattivo su EDT viene utilizzato quando è possibile, con fallback a TCP.
- **Diagnostic mode** (Modalità diagnostica). EDT viene abilitato in modo forzato e TCP viene disabilitato come fallback. Si consiglia questa impostazione solo per la risoluzione dei problemi.
- **Off**. TCP viene abilitato in modo forzato ed EDT è disabilitato.

Per ulteriori informazioni, vedere Adaptive transport (Trasporto adattivo).

### Impostazione del trascinamento della selezione

Questa impostazione consente o impedisce il trascinamento di file tra il client e le applicazioni o i desktop virtuali. Per impostazione predefinita, il criterio di trascinamento della selezione è disabilitato. Se necessario, è possibele abilitare questo criterio.

### Application launch wait timeout (Timeout di attesa di avvio dell'applicazione)

Questa impostazione specifica il valore di timeout di attesa in millisecondi per l'avvio della prima applicazione in una sessione. Se l'avvio dell'applicazione supera questo periodo di tempo, la sessione termina.

È possibile scegliere il periodo di tempo predefinito (10.000 millisecondi) o specificare un numero in millisecondi.

### Client clipboard redirection (Reindirizzamento degli Appunti client)

Questa impostazione consente o impedisce che gli Appunti sul dispositivo utente vengano mappati negli Appunti sul server.

Per impostazione predefinita, il reindirizzamento degli Appunti è consentito.

Per impedire il trasferimento di dati tramite copia e incolla tra una sessione e gli Appunti locali, selezionare **Prohibit** (Vieta). Gli utenti possono comunque copiare e incollare i dati tra le applicazioni in esecuzione nelle sessioni.

Dopo aver abilitato questa impostazione, configurare la larghezza di banda massima consentita che gli Appunti possono consumare in una connessione client. Utilizzare le impostazioni **Clipboard redirection bandwidth limit** (Limite di larghezza di banda per il reindirizzamento degli Appunti) o **Clipboard redirection bandwidth limit percent** (Percentuale del limite della larghezza di banda per il reindirizzamento degli Appunti).

#### Client clipboard write allowed formats (Formati consentiti per la scrittura degli Appunti client)

Quando l'impostazione **Restrict client clipboard write** (Limita scrittura degli Appunti client) è impostata su **Enabled** (Abilitata), i dati degli Appunti host non possono essere condivisi con l'endpoint client. È possibile utilizzare questa impostazione per consentire la condivisione di formati di dati specifici con gli Appunti dell'endpoint client. Per utilizzare questa impostazione, abilitarla e aggiungere i formati specifici da consentire.

I seguenti formati degli Appunti sono definiti dal sistema:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

I seguenti formati personalizzati sono predefiniti in XenApp e XenDesktop e Citrix Virtual Apps and

Desktops:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

Il formato HTML è disabilitato per impostazione predefinita. Per abilitare questa funzionalità:

- Verificare che l'opzione **Client clipboard redirection** (Reindirizzamento degli Appunti client) sia impostata su **Allowed** (Consentito).
- Verificare che l'opzione **Restrict client clipboard write** (Limita scrittura degli Appunti client) sia impostata su **Allowed** (Consentita).
- Aggiungere una voce per **CF_HTML** (e qualsiasi altro formato che si desidera supportare) in **Client clipboard write allowed formats** (Formati consentiti per la scrittura degli Appunti client).

È possibile aggiungere altri formati personalizzati. Il nome del formato personalizzato deve corrispondere ai formati da registrare con il sistema. I nomi dei formati fanno distinzione tra maiuscole e minuscole.

Questa impostazione non si applica se il criterio di **reindirizzamento degli appunti client** è impostato su **Proibito** o se il criterio di **limitazione scrittura degli appunti client** è impostato su **Disabilitato.**

> **Nota:**
>
> L'abilitazione del supporto per la copia degli Appunti in formato HTML (CF_HTML) copia gli script dall'origine del contenuto copiato alla destinazione. Verificare che l'origine sia attendibile prima di procedere alla copia. Se si copia contenuto contenente script, questi sono attivi solo se si salva il file di destinazione come file HTML e lo si esegue.

### Limit clipboard client to session transfer size (Limita il client degli Appunti alle dimensioni del trasferimento della sessione)

Questa impostazione specifica la dimensione massima dei dati degli Appunti che un utente può trasferire da un endpoint client a una sessione virtuale durante una singola operazione di copia e incolla.

Per limitare le dimensioni del trasferimento degli Appunti, abilitare l'impostazione **Limit clipboard client to session transfer size** (Limita il client degli Appunti alle dimensioni del trasferimento della sessione). Quindi, nel campo **Size Limit** (Limite dimensioni), immettere un valore in kilobyte per definire la dimensione del trasferimento dei dati tra gli Appunti locali e una sessione.

Per impostazione predefinita, questa impostazione è disabilitata e non ci sono limiti ai trasferimenti dal client alla sessione.

#### Limit clipboard session to client transfer size (Limita la sessione degli Appunti alle dimensioni del trasferimento del client)

Questa impostazione specifica la dimensione massima dei dati degli Appunti che un utente può trasferire da una sessione virtuale a un endpoint client durante una singola operazione di copia e incolla.

Per limitare le dimensioni del trasferimento degli Appunti, abilitare l'impostazione **Limit clipboard session to client transfer size** (Limita la sessione degli Appunti alle dimensioni del trasferimento del client). Quindi, nel campo **Size Limit** (Limite dimensioni), immettere un valore in kilobyte per definire la dimensione del trasferimento dei dati tra una sessione e gli Appunti locali.

Per impostazione predefinita, questa impostazione è disabilitata e non ci sono limiti ai trasferimenti dalla sessione al client.

#### Restrict client clipboard write (Limita scrittura degli Appunti client)

Se questa impostazione è impostata su **Enabled** (Disabilitata), i dati degli Appunti dell'host non possono essere condivisi con l'endpoint client. È possibile consentire formati specifici abilitando l'impostazione **Client clipboard write allowed formats** (Formati consentiti per la scrittura degli Appunti client).

Per impostazione predefinita, questa impostazione è **disabilitata**.

#### Restrict session clipboard write (Limita scrittura degli Appunti di sessione)

Quando questa impostazione è impostata su **Enabled** (Abilitata), i dati degli Appunti del client non possono essere condivisi all'interno della sessione utente. È possibile consentire formati specifici abilitando l'impostazione **Session clipboard write allowed formats** (Formati consentiti di scrittura degli Appunti di sessione).

Per impostazione predefinita, questa impostazione è **disabilitata**.

#### Session clipboard write allowed formats (Formati consentiti di scrittura degli Appunti di sessione)

Quando l'impostazione **Restrict session clipboard write** (Limita scrittura degli Appunti di sessione) è impostata su **Enabled** (Abilitata), i dati degli Appunti client non possono essere condivisi con le

applicazioni di sessione. È possibile utilizzare questa impostazione per consentire la condivisione di formati di dati specifici con gli Appunti della sessione.

I seguenti formati degli Appunti sono definiti dal sistema:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

I seguenti formati personalizzati sono predefiniti in XenApp e XenDesktop e Citrix Virtual Apps and Desktops:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

Il formato HTML è disabilitato per impostazione predefinita. Per abilitare questa funzionalità:

- Verificare che l'opzione **Client clipboard redirection** (Reindirizzamento degli Appunti client) sia impostata su **Allowed** (Consentito).
- Verificare che l'opzione **Restrict session clipboard write** (Limita scrittura degli Appunti di sessione) sia impostata su **Enabled** (Abilitata).

- Aggiungere una voce per **CF_HTML** (e qualsiasi altro formato che si desidera supportare) in **Session clipboard write allowed formats** (Formati consentiti di scrittura degli Appunti di sessione).

È possibile aggiungere altri formati personalizzati. Il nome del formato personalizzato deve corrispondere ai formati da registrare con il sistema. I nomi dei formati fanno distinzione tra maiuscole e minuscole.

Questa impostazione non si applica se il criterio di **reindirizzamento degli appunti client** è impostato su **Proibito** o se il criterio di **limitazione scrittura degli appunti sessione** è impostato su **Disabilitato.**

> **Nota:**
>
> L'abilitazione del supporto per la copia degli Appunti in formato HTML (CF_HTML) copia gli script dall'origine del contenuto copiato alla destinazione. Verificare che l'origine sia attendibile prima di procedere alla copia. Se si copia contenuto contenente script, questi sono attivi solo se si salva il file di destinazione come file HTML e lo si esegue.

### Desktop starts (Avvii del desktop)

Questa impostazione consente o impedisce le connessioni a una sessione sul VDA utilizzando una connessione ICA da parte di utenti non amministrativi in un gruppo VDA Direct Access Users.

Per impostazione predefinita, gli utenti non amministrativi non possono connettersi a queste sessioni.

Questa impostazione non influisce sugli utenti non amministrativi di un gruppo VDA Direct Access Users che utilizzano una connessione RDP. Questi utenti possono connettersi al VDA quando questa impostazione è abilitata o disabilitata. Questa impostazione non influisce sugli utenti non amministrativi che non fanno parte di un gruppo VDA Direct Access Users. Questi utenti possono connettersi al VDA quando questa impostazione è abilitata o disabilitata.

### FIDO2 redirection (Reindirizzamento FIDO2)

Questa impostazione abilita o disabilita il reindirizzamento FIDO2. Il reindirizzamento FIDO2 consente agli utenti di sfruttare i componenti FIDO2 dell'endpoint locale in una macchina virtuale. Gli utenti possono autenticare la sessione virtuale mediante chiavi di sicurezza FIDO2 o biometria integrata su dispositivi dotati di TPM 2.0 e Windows Hello.

Quando questa impostazione è impostata su **Allowed** (Consentita), gli utenti possono eseguire l'autenticazione FIDO2 utilizzando le funzionalità dell'endpoint locale. L'impostazione predefinita è **Allowed**.

### ICA listener connection timeout (Timeout di connessione del listener ICA)

Questa impostazione specifica il tempo di attesa massimo per il completamento di una connessione che utilizza il protocollo ICA.

Per impostazione predefinita, il tempo di attesa massimo è 120.000 millisecondi o due minuti.

### ICA listener port number (Numero porta listener ICA)

Questa impostazione specifica il numero di porta TCP/IP utilizzato dal protocollo ICA sul server.

Per impostazione predefinita, il numero di porta è impostato su 1494.

I numeri di porta validi devono essere compresi nell'intervallo 0-65535 e non devono essere in conflitto con altri numeri di porta noti. Se si modifica il numero di porta, riavviare il server perché il nuovo valore abbia effetto. Se si modifica il numero di porta sul server, è necessario modificarlo anche su ogni app o plug-in Citrix Workspace che si connette al server.

### Keyboard and Input Method Editor (IME) (Tastiera e Input Method Editor [IME])

Questa impostazione abilita o disabilita quanto segue:

- Sincronizzazione dinamica del layout della tastiera
- IME (Input Method Editor)
- Mappatura del layout di tastiera Unicode
- Nasconde o mostra il messaggio di notifica dell'interruttore del layout della tastiera

1. In Web Studio, selezionare **Keyboard and IME** (Tastiera e IME).
2. Selezionare **Client keyboard layout synchronization and IME improvement** (Sincronizzazione del layout della tastiera client e miglioramento IME) per controllare la sincronizzazione dinamica del layout della tastiera e le funzionalità IME (Input Method Editor) generiche del client nel VDA. Le opzioni disponibili sono:

   **Disabled** (Disabilitato): sincronizzazione dinamica del layout della tastiera e IME (Input Method Editor) generico del client.

   **Support dynamic client keyboard layout synchronization** (Supporta sincronizzazione dinamica del layout della tastiera client): consente la sincronizzazione dinamica del layout della tastiera.

   **Support dynamic client keyboard layout synchronization and IME improvement** (Supporta miglioramento di IME e della sincronizzazione dinamica del layout della tastiera client): consente sia la sincronizzazione dinamica del layout della tastiera che l'IME (Input Method Editor) generico del client.

3. Selezionare **Enable Unicode keyboard layout mapping** (Abilita mappatura del layout della tastiera Unicode) per abilitare o disabilitare la mappatura della tastiera Unicode.
4. Selezionare **Hide keyboard layout switch pop-up message box** (Nascondi messaggio a comparsa sull'interruttore del layout della tastiera) per controllare se viene visualizzato o meno un messaggio che indica che il layout della tastiera si sta sincronizzando quando l'utente modifica il layout della tastiera client. Se si impedisce la visualizzazione del messaggio, gli utenti devono attendere qualche istante prima di digitare, per evitare l'inserimento di caratteri errati.

Impostazioni predefinite:

- **Client keyboard layout synchronization and IME improvement** (Sincronizzazione del layout della tastiera client e miglioramento IME)
  - Disabilitato in Windows Server 2016 e Windows Server 2019.
  - Supporta la sincronizzazione dinamica del layout della tastiera client e il miglioramento IME in Windows Server 2012 e Windows 2010.
- **Disable Unicode keyboard layout mapping** (Disabilita la mappatura del layout della tastiera Unicode)
- **Show keyboard layout switch pop-up message box** (Mostra messaggio a comparsa dell'interruttore di layout della tastiera)

Questo criterio sostituisce le impostazioni del Registro di sistema elencate nella sezione **Description** (Descrizione) delle impostazioni dei criteri.

### Logoff checker startup delay (Ritardo di avvio del controllo disconnessione)

Questa impostazione specifica la durata del ritardo dell'avvio del controllo disconnessione. Utilizzare questo criterio per impostare il tempo (in secondi) di attesa di una sessione client prima di disconnettere la sessione.

Questa impostazione aumenta anche il tempo necessario per disconnettersi dal server.

### Loss tolerant mode (Modalità tollerante alle perdite)

> **Importante:**
>
> - La funzionalità richiede al minimo l'app Citrix Workspace 2002 per Windows. Questa versione del VDA la supporta quando è disponibile.
> - La modalità tollerante alle perdite non è supportata su Citrix Gateway o Citrix Gateway Service. Questa modalità è disponibile solo con le connessioni dirette.

Questa impostazione abilita o disabilita la modalità tollerante alle perdite.

Per impostazione predefinita, la modalità tollerante alle perdite è impostata su **Allowed** (Consentita).

Quando è consentita, la modalità viene abilitata quando la perdita di pacchetti e la latenza sono superiori a una determinata soglia. È possibile impostare le soglie utilizzando il criterio delle soglie tolleranti alle perdite.

Per ulteriori informazioni, vedere Modalità tollerante alle perdite.

### Loss tolerant thresholds (Soglie tolleranti alle perdite)

Quando la modalità tollerante alle perdite è disponibile, questa impostazione specifica le soglie delle metriche di rete raggiunte le quali la sessione passa alla modalità tollerante alle perdite.

Le soglie predefinite sono:

- Perdita pacchetto: 5%
- Latenza: 300 ms (RTT)

Per ulteriori informazioni, vedere Modalità tollerante alle perdite.

### Rendezvous protocol (Protocollo Rendezvous)

Questa impostazione modifica il modo in cui viene eseguito il proxy delle sessioni HDX quando si utilizza il servizio Citrix Gateway. Quando è abilitata, il traffico HDX non passa più attraverso Citrix Cloud Connector. Il VDA stabilisce invece una connessione in uscita direttamente con il servizio Citrix Gateway (migliorando la scalabilità di Cloud Connector).

> **Importante:**
>
> Una funzione di commutazione in Citrix Cloud e un'impostazione dei criteri HDX controllano questa funzionalità. L'interruttore della funzionalità Citrix Cloud è abilitato per impostazione predefinita, mentre l'impostazione HDX è disabilitata per impostazione predefinita. L'impostazione HDX ha effetto solo sulle sessioni HDX stabilite tramite Citrix Gateway Service. Questa impostazione non influisce sulle sessioni stabilite direttamente tra client e VDA o tramite Citrix Gateway on-premise.

Per informazioni, vedere Protocollo Rendezvous.

### Rendezvous proxy configuration (Configurazione del proxy Rendezvous)

Questa impostazione consente di configurare un proxy esplicito da utilizzare con il protocollo Rendezvous. Se si utilizza un proxy trasparente, non è necessario abilitare questa impostazione.

Per impostazione predefinita, questa impostazione è disabilitata.

Quando è disabilitata, il VDA non instrada il traffico in uscita attraverso proxy non trasparenti quando si tenta di stabilire una connessione Rendezvous con il servizio gateway.

Quando è abilitata, il VDA tenta di stabilire una connessione Rendezvous con il servizio gateway tramite il proxy definito in questa impostazione.

Il VDA supporta l'utilizzo di proxy HTTP e SOCKS5 per le connessioni Rendezvous. Per configurare il VDA per l'utilizzo di un proxy per la connessione Rendezvous, è necessario abilitare questa impostazione. Specificare inoltre l'indirizzo del proxy o il percorso del file PAC. Ad esempio:

- Indirizzo proxy: `http://<URL or IP>:<port>` o `socks5://<URL or IP>:<port>`
- File PAC: `http://<URL or IP>/<path>/<filename>.pac`

  VDA versione 2103 è la versione minima supportata per la configurazione proxy con un file PAC. Per ulteriori informazioni sullo schema di file PAC per i proxy SOCKS5, vedere Configurazione proxy.

> **Nota:**
>
> Solo i proxy SOCKS5 supportano il trasporto dei dati tramite EDT. Per un proxy HTTP, utilizzare TCP come protocollo di trasporto per ICA.

Per ulteriori informazioni, vedere Protocollo Rendezvous.

### Avvio di programmi non pubblicati durante la connessione client

Questa impostazione specifica se consentire l'avvio delle applicazioni iniziali tramite RDP sul server.

Per impostazione predefinita, l'avvio delle applicazioni iniziali tramite RDP sul server non è consentito.

### Impostazioni dei criteri di abilitazione/disabilitazione della modalità tablet

La modalità tablet consente di ottimizzare l'aspetto e il comportamento delle app Store, delle app Win32 e della shell di Windows sul VDA. Questo avviene passando automaticamente dalla modalità desktop virtuale alla modalità Tablet quando ci si connette da dispositivi con fattore di forma ridotto come telefoni e tablet o qualsiasi dispositivo touch.

Se questo criterio è disabilitato, il VDA è nella modalità in cui l'utente lo imposta e mantiene sempre la stessa modalità, a prescindere dal tipo di client.

## Impostazioni dei criteri di riconnessione automatica client

January 7, 2024

La sezione **Auto client reconnect** (Riconnessione automatica client) contiene le impostazioni dei criteri per il controllo della riconnessione automatica delle sessioni.

### Auto client reconnect (Riconnessione automatica client)

Questa impostazione consente o impedisce la riconnessione automatica da parte dello stesso client dopo l'interruzione di una connessione.

Per Citrix Receiver per Windows 4.7 e versioni successive e per l'app Citrix Workspace 1808 e versioni successive, la riconnessione automatica client utilizza solo le impostazioni dei criteri di Citrix Studio. Gli aggiornamenti di questi criteri in Studio sincronizzano la riconnessione automatica del client dal server al client. Con le versioni precedenti di Citrix Receiver per Windows, per configurare la riconnessione automatica del client utilizzare un criterio di Studio e modificare il Registro di sistema o il file default.ica.

Se consentita, la riconnessione automatica del client consente agli utenti di riprendere a lavorare dove si erano fermati quando una connessione è stata interrotta. La riconnessione automatica rileva le connessioni interrotte e quindi riconnette gli utenti alle loro sessioni.

Se il cookie dell'app Citrix Workspace contenente la chiave per l'ID di sessione e le credenziali non viene utilizzato, la riconnessione automatica potrebbe causare l'avvio di una nuova sessione invece di riconnettersi a una sessione esistente. Il cookie non viene utilizzato se è scaduto. Ad esempio, il cookie potrebbe scadere a causa di un ritardo nella riconnessione o se è necessario reinserire le credenziali. Se gli utenti si disconnettono intenzionalmente, la riconnessione automatica del client non viene attivata.

Una finestra di sessione è disattivata quando è in corso una riconnessione. Un timer di conto alla rovescia visualizza il tempo rimanente prima della riconnessione della sessione. Quando una sessione scade, viene disconnessa.

Per le sessioni delle applicazioni, quando è consentita la riconnessione automatica, nell'area di notifica viene visualizzato un timer di conto alla rovescia. Questo timer specifica il tempo rimanente prima che la sessione venga ricollegata. L'app Citrix Workspace tenta di riconnettersi alla sessione finché la connessione non viene ristabilita o fino a quando l'utente annulla i tentativi di riconnessione.

Per le sessioni utente, quando è consentita la riconnessione automatica, l'app Citrix Workspace tenta di riconnettersi alla sessione per un periodo di tempo specificato, a meno che la connessione non venga ristabilita o l'utente annulli i tentativi di riconnessione. Per impostazione predefinita, questo periodo è di due minuti. Per modificare questo periodo, modificare il criterio.

Per impostazione predefinita, la riconnessione automatica del client è consentita. Può essere disattivata impostando il criterio su **Prohibited** (Proibito).

### Auto client reconnect authentication (Autenticazione della riconnessione automatica client)

Questa impostazione specifica se è necessaria l'autenticazione per le riconnessioni automatiche dei client.

Quando un utente accede inizialmente, le credenziali vengono crittografate e archiviate nella memoria e viene creato un cookie contenente la chiave di crittografia. Il cookie viene inviato all'app Citrix Workspace. Quando questa impostazione è configurata, i cookie non vengono utilizzati. Viene invece visualizzata una finestra di dialogo per gli utenti che richiedono le credenziali quando l'app Citrix Workspace tenta di riconnettersi automaticamente.

Per impostazione predefinita, l'autenticazione non è richiesta.

### Auto client reconnect logging (Registrazione della riconnessione automatica client)

Questa impostazione abilita o disabilita la registrazione delle riconnessioni automatiche del client nel registro eventi.

Quando la registrazione è abilitata, il registro di sistema del server acquisisce informazioni sugli eventi di riconnessione automatica riusciti e non riusciti. Un sito non fornisce un registro combinato degli eventi di riconnessione per tutti i server.

Per impostazione predefinita, la registrazione è disabilitata.

### Auto client reconnect timeout (Timeout di riconnessione automatica client)

Per impostazione predefinita, il timeout di riconnessione automatica client è impostato su 120 secondi, il valore massimo configurabile per un timeout di riconnessione automatica client è 300 secondi. Utilizzare questo criterio per impostare il valore di timeout.

### Reconnect UI transparency level (Riconnetti livello di trasparenza dell'interfaccia utente)

Questa impostazione consente di specificare il livello di opacità applicato alla finestra di sessione di XenApp o XenDesktop durante il tempo di riconnessione dell'affidabilità della sessione.

Per impostazione predefinita, l'opzione Reconnect UI transparency level (Riconnetti livello di trasparenza dell'interfaccia utente) è impostata su 80%.

## Impostazioni dei criteri audio

January 7, 2024

La sezione **Audio** include le impostazioni dei criteri che consentono ai dispositivi utente di inviare e ricevere audio nelle sessioni senza ridurre le prestazioni.

### Audio adattivo

Questa impostazione abilita o disabilita l'audio adattivo. Quando si abilita questo criterio, le impostazioni della qualità audio vengono regolate dinamicamente per offrire la migliore esperienza utente. Questa impostazione si applica sia alle sessioni del sistema operativo a sessione singola che alle sessioni del sistema operativo multisessione di VDA che utilizzano Citrix Virtual Apps and Desktops 2109 o versioni successive.

Quando questa impostazione non è consentita, viene applicato il criterio della qualità audio. Per ulteriori informazioni, vedere Qualità audio.

Per impostazione predefinita, il criterio dell'audio adattivo è abilitato.

### Audio over UDP real-time transport (Audio con trasporto UDP in tempo reale)

Questa impostazione consente o impedisce la trasmissione e la ricezione dell'audio tra il VDA e il dispositivo utente tramite RTP utilizzando UDP (User Datagram Protocol). Quando questa impostazione è disabilitata, l'audio viene inviato e ricevuto tramite TCP.

Per impostazione predefinita, l'audio tramite UDP è consentito.

### Audio Plug N Play

Questa impostazione consente o impedisce l'uso di più dispositivi audio per registrare e riprodurre suoni.

Per impostazione predefinita, l'uso di più dispositivi audio è consentito.

Questa impostazione si applica solo alle macchine con sistema operativo Windows multisessione.

### Audio quality (Qualità audio)

Questa impostazione specifica il livello di qualità del suono ricevuto nelle sessioni utente.

Per impostazione predefinita, la qualità del suono è impostata su High - high definition audio (Elevata - Audio ad alta definizione).

Per controllare la qualità del suono, scegliere una delle seguenti opzioni:

- Selezionare Low - for low speed connections (Bassa - per connessioni a bassa velocità) per le connessioni a larghezza di banda ridotta. I suoni inviati al dispositivo utente vengono compressi fino a 16 Kbps. Questa compressione si traduce in una significativa riduzione della qualità del suono. Ma consente anche prestazioni ragionevoli per una connessione a larghezza di banda ridotta.
- Selezionare Medium: ottimizzato per la voce per fornire applicazioni Voice over Internet Protocol. Questa impostazione consegna applicazioni multimediali in connessioni di rete impegnative con linee inferiori a 512 Kbps, o con una notevole congestione e perdita di pacchetti. Questo codec offre tempi di codifica rapidi, quindi è ideale per l'utilizzo con softphone e applicazioni Unified Communications quando si richiede l'elaborazione di elementi multimediali sul lato server.

  L'audio inviato al dispositivo utente viene compresso fino a 64 Kbps. Questa compressione si traduce in una moderata riduzione della qualità dell'audio riprodotto sul dispositivo utente, fornendo allo stesso tempo una bassa latenza e un consumo ridotto di larghezza di banda. Se la qualità del protocollo Voice over Internet non è soddisfacente, assicurarsi che l'impostazione dei criteri Audio over UDP Real-time Transport (Audio con trasporto UDP in tempo reale) sia impostata su Allowed (Consentito).

  Al momento il trasporto UDP in tempo reale (RTP) è supportato solo quando è selezionata questa qualità audio. Utilizzare questa qualità audio anche per fornire applicazioni multimediali per connessioni di rete problematiche come linee a bassa velocità (meno di 512 Kbps). Utilizzarla anche quando c'è congestione e perdita di pacchetti nella rete.
- Selezionare High - high definition audio (Alta - Audio ad alta definizione) per connessioni con elevata larghezza di banda e in cui la qualità del suono è importante. I client possono riprodurre il suono alla velocità nativa. I suoni vengono compressi a un livello di qualità elevata mantenendo una qualità simile ai CD e utilizzando fino a 112 Kbps di larghezza di banda. La trasmissione di questa quantità di dati può comportare un aumento dell'utilizzo della CPU e una maggiore congestione della rete.

La larghezza di banda viene consumata solo durante la registrazione o la riproduzione dell'audio. Se entrambi questi eventi si verificano contemporaneamente, il consumo di larghezza di banda raddoppia.

Per specificare la quantità massima di larghezza di banda, configurare le impostazioni **Audio redirection bandwidth limit** (Limite della larghezza di banda di reindirizzamento audio) o **Audio redirection bandwidth limit percent** (Percentuale del limite della larghezza di banda di reindirizzamento audio).

### Client audio redirection (Reindirizzamento audio client)

Questa impostazione specifica se le applicazioni ospitate sul server possono riprodurre suoni tramite un dispositivo audio installato sul dispositivo utente. Questa impostazione specifica anche se gli utenti possono registrare l'ingresso audio.

Per impostazione predefinita, il reindirizzamento audio è consentito.

Dopo aver consentito questa impostazione, è possibile limitare la larghezza di banda utilizzata durante la riproduzione o la registrazione dell'audio. Limitare la quantità di larghezza di banda consumata dall'audio può migliorare le prestazioni delle applicazioni, ma potrebbe anche compromettere la qualità audio. La larghezza di banda viene consumata solo durante la registrazione o la riproduzione dell'audio. Se entrambi questi eventi si verificano contemporaneamente, il consumo di larghezza di banda raddoppia. Per specificare la quantità massima di larghezza di banda, configurare le impostazioni **Audio redirection bandwidth limit** (Limite della larghezza di banda di reindirizzamento audio) o **Audio redirection bandwidth limit percent** (Percentuale del limite della larghezza di banda di reindirizzamento audio).

Nelle macchine con sistema operativo Windows multisessione, assicurarsi che l'impostazione **Audio Plug N Play** sia abilitata per supportare più dispositivi audio.

Importante: se il reindirizzamento audio client non è consentito, vengono disabilitate tutte le funzionalità audio HDX.

### Client microphone redirection (Reindirizzamento microfono client)

Questa impostazione abilita o disabilita il reindirizzamento del microfono client. Se abilitata, gli utenti possono utilizzare i microfoni per registrare l'ingresso audio in una sessione.

Per impostazione predefinita, il reindirizzamento del microfono è consentito.

Per motivi di sicurezza, gli utenti vengono avvisati quando i server che non sono considerati attendibili dai propri dispositivi tentano di accedere ai microfoni. Gli utenti possono scegliere di accettare o non accettare l'accesso. Gli utenti possono disabilitare l'avviso sull'app Citrix Workspace.

Nelle macchine con sistema operativo Windows multisessione, assicurarsi che l'impostazione Audio Plug N Play sia abilitata per supportare più dispositivi audio.

Se l'impostazione **Client microphone redirection** (Reindirizzamento audio client) è disabilitata sul dispositivo utente, questa regola non ha effetto.

## Impostazioni dei criteri della larghezza di banda

January 7, 2024

La sezione **Bandwidth** (Larghezza di banda) include le impostazioni dei criteri per evitare problemi di prestazioni correlati all'utilizzo della larghezza di banda della sessione client.

Importante: l'utilizzo di queste impostazioni dei criteri con le impostazioni **Multi-Stream policy** (Criteri multi-flusso) potrebbe produrre risultati imprevisti. Se si utilizzano le impostazioni multi-flusso in un criterio, assicurarsi che queste impostazioni dei criteri del limite della larghezza di banda non siano incluse.

### Audio redirection bandwidth limit (Limite della larghezza di banda di reindirizzamento audio)

Questa impostazione specifica la larghezza di banda massima consentita per la riproduzione o la registrazione di audio in una sessione utente. La larghezza di banda massima consentita è specificata in kilobit al secondo.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **Audio redirection bandwidth limit percent** (Percentuale del limite della larghezza di banda di reindirizzamento audio), viene applicata l'impostazione più restrittiva (valore inferiore).

### Audio redirection bandwidth limit percent (Percentuale del limite della larghezza di banda di reindirizzamento audio)

Questa impostazione specifica il limite massimo consentito di larghezza di banda per la riproduzione o la registrazione audio come percentuale della larghezza di banda totale della sessione.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **Audio redirection bandwidth limit** (Limite della larghezza di banda di reindirizzamento audio), viene applicata l'impostazione più restrittiva (il valore inferiore).

Se si configura questa impostazione, è necessario configurare anche l'impostazione **Overall session bandwidth limit** (Limite della larghezza di banda generale della sessione), che specifica la quantità totale di larghezza di banda disponibile per le sessioni client.

### Client USB device redirection bandwidth limit (Limite della larghezza di banda di reindirizzamento del dispositivo USB client)

Questa impostazione specifica la larghezza di banda massima consentita per il reindirizzamento dei dispositivi USB da e verso il client. La larghezza di banda massima consentita è specificata in kilobit al secondo.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **Client USB device redirection bandwidth limit percent** (Percentuale del limite della larghezza di banda di reindirizzamento del dispositivo USB client), viene applicata l'impostazione più restrittiva (il valore inferiore).

### Client USB device redirection bandwidth limit percent (Percentuale del limite della larghezza di banda di reindirizzamento del dispositivo USB client)

Questa impostazione specifica la larghezza di banda massima consentita per il reindirizzamento dei dispositivi USB da e verso il client come percentuale della larghezza di banda totale della sessione.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **Client USB device redirection bandwidth limit** (Limite della larghezza di banda di reindirizzamento del dispositivo USB client), viene applicata l'impostazione più restrittiva (il valore inferiore).

Se si configura questa impostazione, è necessario configurare anche l'impostazione **Overall session bandwidth limit** (Limite della larghezza di banda generale della sessione), che specifica la quantità totale di larghezza di banda disponibile per le sessioni client.

### Clipboard redirection bandwidth limit (Limite della larghezza di banda per il reindirizzamento degli appunti)

Questa impostazione specifica la larghezza di banda massima consentita per il trasferimento dei dati tra una sessione e gli appunti locali. La larghezza di banda massima consentita è specificata in kilobit al secondo.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **Clipboard redirection bandwidth limit percent** (Limite della larghezza di banda per il reindirizzamento degli appunti), viene applicata l'impostazione più restrittiva (il valore inferiore).

### Clipboard redirection bandwidth limit percent (Limite della larghezza di banda per il reindirizzamento degli appunti)

Questa impostazione specifica la larghezza di banda massima consentita per il trasferimento dei dati tra una sessione e gli appunti locali come percentuale della larghezza di banda totale della sessione.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **Clipboard redirection bandwidth limit** (Limite della larghezza di banda per il reindirizzamento degli appunti), viene applicata l'impostazione più restrittiva (il valore inferiore).

Se si configura questa impostazione, è necessario configurare anche l'impostazione **Overall session bandwidth limit** (Limite della larghezza di banda generale della sessione), che specifica la quantità totale di larghezza di banda disponibile per le sessioni client.

### COM port redirection bandwidth limit (Limite della larghezza di banda di reindirizzamento della porta COM)

Nota: per Virtual Delivery Agent da 7.0 a 7.8, configurare questa impostazione utilizzando il Registro di sistema. Vedere Configurare le impostazioni di reindirizzamento delle porte COM e LPT utilizzando il Registro di sistema.

Questa impostazione specifica la larghezza di banda massima consentita in kilobit al secondo per accedere a una porta COM in una connessione client. Se si immette un valore per questa impostazione e un valore per l'impostazione **COM port redirection bandwidth limit percent** (Percentuale del limite della larghezza di banda di reindirizzamento della porta COM), viene applicata l'impostazione più restrittiva (il valore inferiore).

### COM port redirection bandwidth limit percent (Percentuale del limite della larghezza di banda di reindirizzamento della porta COM)

Nota: per Virtual Delivery Agent da 7.0 a 7.8, configurare questa impostazione utilizzando il Registro di sistema. Vedere Configurare le impostazioni di reindirizzamento delle porte COM e LPT utilizzando il Registro di sistema.

Questa impostazione specifica la larghezza di banda massima consentita per l'accesso alle porte COM in una connessione client come percentuale della larghezza di banda totale della sessione.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **COM port redirection bandwidth limit** (Limite della larghezza di banda di reindirizzamento della porta COM), viene applicata l'impostazione più restrittiva (il valore inferiore).

Se si configura questa impostazione, è necessario configurare anche l'impostazione **Overall session bandwidth limit** (Limite della larghezza di banda generale della sessione), che specifica la quantità totale di larghezza di banda disponibile per le sessioni client.

### File redirection bandwidth limit (Limite della larghezza di banda di reindirizzamento file)

Questa impostazione specifica la larghezza di banda massima consentita per accedere a un'unità client in una sessione utente. La larghezza di banda massima consentita è specificata in kilobit al secondo.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **File redirection bandwidth limit percent** (Percentuale del limite della larghezza di banda per il reindirizzamento file), verrà applicata l'impostazione più restrittiva (il valore inferiore).

### File redirection bandwidth limit percent (Percentuale del limite della larghezza di banda per il reindirizzamento file)

Questa impostazione specifica il limite massimo di larghezza di banda consentito per l'accesso alle unità client come percentuale della larghezza di banda totale della sessione.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **File redirection bandwidth limit** (Limite della larghezza di banda per il reindirizzamento file), viene applicata l'impostazione più restrittiva (il valore inferiore).

Se si configura questa impostazione, è necessario configurare anche l'impostazione **Overall session bandwidth limit** (Limite della larghezza di banda generale della sessione), che specifica la quantità totale di larghezza di banda disponibile per le sessioni client.

### HDX MediaStream Multimedia Acceleration bandwidth limit (Limite della larghezza di banda HDX MediaStream Multimedia Acceleration)

Questa impostazione specifica il limite massimo consentito di larghezza di banda per la trasmissione di audio e video in streaming utilizzando HDX MediaStream Multimedia Acceleration. La larghezza di

banda massima consentita è specificata in kilobit al secondo.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **HDX MediaStream Multimedia Acceleration bandwidth limit percent** (Percentuale del limite della larghezza di banda HDX MediaStream Multimedia Acceleration), verrà applicata l'impostazione più restrittiva (il valore inferiore).

### HDX MediaStream Multimedia Acceleration bandwidth limit percent (Percentuale del limite della larghezza di banda HDX MediaStream Multimedia Acceleration)

Questa impostazione specifica la larghezza di banda massima consentita per la trasmissione di audio e video in streaming utilizzando HDX MediaStream Multimedia Acceleration come percentuale della larghezza di banda totale della sessione.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **HDX MediaStream Multimedia Acceleration bandwidth limit** (Limite della larghezza di banda HDX MediaStream Multimedia Acceleration), verrà applicata l'impostazione più restrittiva (il valore inferiore).

Se si configura questa impostazione, è necessario configurare anche l'impostazione **Overall session bandwidth limit** (Limite della larghezza di banda generale della sessione), che specifica la quantità totale di larghezza di banda disponibile per le sessioni client.

### LPT port redirection bandwidth limit (Limite della larghezza di banda per il reindirizzamento della porta LPT)

Nota: per Virtual Delivery Agent da 7.0 a 7.8, configurare questa impostazione utilizzando il Registro di sistema. Vedere Configurare le impostazioni di reindirizzamento delle porte COM e LPT utilizzando il Registro di sistema.

Questa impostazione specifica la larghezza di banda massima consentita per i processi di stampa che utilizzano una porta LPT in una singola sessione utente. La larghezza di banda massima consentita è specificata in kilobit al secondo.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **LPT port redirection bandwidth limit percent** (Percentuale del limite della larghezza di banda per il reindirizzamento della porta LPT), viene applicata l'impostazione più restrittiva (il valore inferiore).

### LPT port redirection bandwidth limit percent (Percentuale del limite della larghezza di banda per il reindirizzamento della porta LPT)

Nota: per Virtual Delivery Agent da 7.0 a 7.8, configurare questa impostazione utilizzando il Registro di sistema. Vedere Configurare le impostazioni di reindirizzamento delle porte COM e LPT utilizzando il Registro di sistema.

Questa impostazione specifica il limite di larghezza di banda per i processi di stampa che utilizzano una porta LPT in una singola sessione client come percentuale della larghezza di banda totale della sessione.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **LPT port redirection bandwidth limit** (Limite della larghezza di banda per il reindirizzamento della porta LPT), viene applicata l'impostazione più restrittiva (il valore inferiore).

Se si configura questa impostazione, è necessario configurare anche l'impostazione **Overall session bandwidth limit** (Limite della larghezza di banda generale della sessione), che specifica la quantità totale di larghezza di banda disponibile per le sessioni client.

### Overall session bandwidth limit (Limite della larghezza di banda complessiva della sessione)

Questa impostazione specifica la quantità totale di larghezza di banda disponibile, in kilobit al secondo, per le sessioni utente.

Il limite massimo della larghezza di banda applicabile è di 20 Mbps (20.000 Kbps). Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Limitare la quantità di larghezza di banda utilizzata da una connessione client può migliorare le prestazioni quando altre applicazioni esterne alla connessione client si contendono una larghezza di banda limitata.

### Printer redirection bandwidth limit (Limite della larghezza di banda per il reindirizzamento della stampante)

Questa impostazione specifica la larghezza di banda massima consentita per accedere alle stampanti client in una sessione utente. La larghezza di banda massima consentita è specificata in kilobit al secondo.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **Printer redirection bandwidth limit percent** (Percentuale del limite della larghezza di banda per il reindirizzamento della stampante), viene applicata l'impostazione più restrittiva (il valore inferiore).

### Printer redirection bandwidth limit percent (Percentuale del limite della larghezza di banda per il reindirizzamento della stampante)

Questa impostazione specifica la larghezza di banda massima consentita per l'accesso alle stampanti client come percentuale della larghezza di banda totale della sessione.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **Printer redirection bandwidth limit** (Limite della larghezza di banda per il reindirizzamento della stampante), viene applicata l'impostazione più restrittiva (con il valore inferiore).

Se si configura questa impostazione, è necessario configurare anche l'impostazione **Overall session bandwidth limit** (Limite della larghezza di banda generale della sessione), che specifica la quantità totale di larghezza di banda disponibile per le sessioni client.

### TWAIN device redirection bandwidth limit (Limite della larghezza di banda per il reindirizzamento dei dispositivi TWAIN)

Questa impostazione specifica la larghezza di banda massima consentita per controllare i dispositivi di imaging TWAIN delle applicazioni pubblicate. La larghezza di banda massima consentita è specificata in kilobit al secondo.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **TWAIN device redirection bandwidth limit percent** (Percentuale del limite della larghezza di banda per il reindirizzamento dei dispositivi TWAIN), viene applicata l'impostazione più restrittiva (il valore inferiore).

### TWAIN device redirection bandwidth limit percent (Percentuale del limite della larghezza di banda per il reindirizzamento dei dispositivi TWAIN)

Questa impostazione specifica la larghezza di banda massima consentita per il controllo dei dispositivi di imaging TWAIN delle applicazioni pubblicate come percentuale della larghezza di banda totale della sessione.

Per impostazione predefinita, non viene specificato alcun valore massimo (zero).

Se si immette un valore per questa impostazione e un valore per l'impostazione **TWAIN device redirection bandwidth limit** (Limite della larghezza di banda per il reindirizzamento dei dispositivi TWAIN), viene applicata l'impostazione più restrittiva (con il valore inferiore).

Se si configura questa impostazione, è necessario configurare anche l'impostazione **Overall session bandwidth limit** (Limite della larghezza di banda generale della sessione), che specifica la quantità totale di larghezza di banda disponibile per le sessioni client.

## Impostazioni dei criteri di reindirizzamento bidirezionale del contenuto

January 7, 2024

La sezione **Bidirectional content redirection** (Reindirizzamento bidirezionale del contenuto) contiene le impostazioni dei criteri per abilitare o disabilitare il reindirizzamento degli URL dal client all'host e dall'host al client.

I criteri del server sono impostati in Web Studio. I criteri del client vengono impostati dal modello di amministrazione degli oggetti Criteri di gruppo dell'app Citrix Workspace.

Citrix offre il reindirizzamento da host a client e Local App Access per il reindirizzamento da client a URL. Tuttavia, si consiglia di utilizzare il reindirizzamento bidirezionale del contenuto per i client Windows aggiunti al dominio.

### Allow bidirectional content redirection (Consenti reindirizzamento bidirezionale del contenuto)

Impostare questo criterio su **Consentito** per abilitare il reindirizzamento tra server (VDA) e client. È impostato su **Prohibited** per impostazione predefinita.

Utilizzare il criterio **Allowed URLs to be redirected to client** (URL consentiti da reindirizzare al client) per configurare l'elenco di URL per il reindirizzamento da VDA a client.

> **Nota:**
>
> Questo criterio deve essere impostato con il criterio **Bidirectional Content Redirection** sul client affinché il reindirizzamento sia consentito.

### Allowed URLs to be redirected to client (URL consentiti da reindirizzare al client)

Specifica l'elenco di URL da aprire sul client quando è consentito il reindirizzamento bidirezionale del contenuto.

Il delimitatore è un punto e virgola (;). Come carattere jolly, è possibile usare un asterisco (*). Ad esempio:

```
*.xyz.com;https://www.example.com
```

## Impostazioni dei criteri di reindirizzamento del contenuto del browser

January 7, 2024

La sezione Browser content redirection (Reindirizzamento del contenuto del browser) include le impostazioni dei criteri per configurare questa funzionalità.

Il reindirizzamento del contenuto del browser controlla e ottimizza il modo in cui Citrix Virtual Apps and Desktops distribuisce tutti i contenuti del browser Web (ad esempio, HTML5) agli utenti. Viene reindirizzata solo l'area visibile del browser in cui viene visualizzato il contenuto.

Il reindirizzamento video HTML5 e il reindirizzamento del contenuto del browser sono funzionalità indipendenti. I criteri di reindirizzamento video HTML5 non sono necessari per il funzionamento di questa funzione. Tuttavia, il servizio di reindirizzamento video HTML5 Citrix HDX viene utilizzato per il reindirizzamento dei contenuti del browser. Per ulteriori informazioni, vedere Reindirizzamento del contenuto del browser.

> **Nota:**
>
> Le impostazioni dei criteri disponibili in Web Studio possono essere sovrascritte con le chiavi del Registro di sistema sul VDA, ma le chiavi del Registro di sistema sono facoltative.

### TLS e reindirizzamento del contenuto del browser

È possibile utilizzare il reindirizzamento del contenuto del browser per reindirizzare i siti Web HTTPS. Il JavaScript inserito in tali siti Web deve stabilire una connessione TLS al servizio di reindirizzamento video HTML5 Citrix HDX (WebSocketService.exe) in esecuzione sul VDA. Per ottenere questo reindirizzamento e mantenere l'integrità TLS della pagina Web, il servizio di reindirizzamento video HTML5 Citrix HDX genera due certificati personalizzati nell'archivio certificati sul VDA.

HdxVideo.js utilizza socket Secure Web per comunicare con WebSocketService.exe in esecuzione sul VDA. Questo processo viene eseguito sul sistema locale ed esegue la terminazione SSL e la mappatura della sessione utente.

WebSocketService.exe è in ascolto sulla porta 127.0.0.1 9001.

### Browser content redirection (Reindirizzamento del contenuto del browser)

Per impostazione predefinita, l'app Citrix Workspace tenta il recupero dal client e il rendering dal client. Il rendering lato server viene tentato in caso di mancata riuscita del recupero del client e del rendering del client. Se si abilita anche il criterio di configurazione del proxy di reindirizzamento del contenuto del browser, l'app Citrix Workspace tenta solo il recupero dal server e il rendering dal client.

L'impostazione predefinita è Allowed.

### Impostazione Browser content redirection Integrated Windows Authentication support (Supporto dell'Autenticazione integrata di Windows per il reindirizzamento del contenuto del browser)

Il reindirizzamento del contenuto del browser abilita la sovrapposizione che utilizza lo schema Negotiate (Negozia) per l'autenticazione. Questo miglioramento fornisce il Single Sign-on a un server Web configurato con l'Autenticazione integrata di Windows (IWA) all'interno dello stesso dominio del VDA.

Se è impostata su **Allowed** (Consentita), la sovrapposizione di reindirizzamento del contenuto del browser ottiene un ticket Negotiate (Negozia) utilizzando le credenziali VDA dell'utente. L'utente si autentica quindi sul server Web con il Single Sign-on.

Se è impostata su **Prohibited** (Non consentita), l'overlay di reindirizzamento del contenuto del browser non richiede un ticket Negotiate (Negozia) dal VDA. L'utente esegue l'autenticazione su un server Web utilizzando un metodo di autenticazione di base. Questo metodo di autenticazione di base richiede agli utenti di immettere le proprie credenziali VDA ogni volta che accedono al server Web.

L'impostazione predefinita è Prohibited (Non consentito).

### Impostazione Browser content redirection server fetch web proxy authentication (Autenticazione del proxy Web per il recupero dal server del reindirizzamento del contenuto del browser)

Questa impostazione indirizza il traffico HTTP proveniente da una sovrapposizione tramite un proxy Web downstream. Il proxy Web downstream autorizza e autentica il traffico HTTP utilizzando le credenziali di dominio dell'utente VDA tramite lo schema di autenticazione Negotiate (Negozia).

È necessario configurare il reindirizzamento del contenuto del browser per la modalità di recupero dal server nel file PAC utilizzando il criterio di configurazione Browser content redirection proxy (Proxy di reindirizzamento del contenuto del browser). Nello script PAC, fornire istruzioni per instradare il traffico di sovrapposizione attraverso un proxy Web downstream. Quindi, configurare il proxy Web downstream per autenticare gli utenti VDA tramite lo schema di autenticazione Negotiate.

Se è impostato su **Allowed** (Consentito), il proxy Web risponde con un problema 407 Negotiate, contenente un'intestazione **Proxy-Authenticate: Negotiate**. Il reindirizzamento del contenuto del browser ottiene quindi un ticket di assistenza Kerberos utilizzando le credenziali di dominio dell'utente VDA. Includere inoltre il ticket di servizio nelle richieste successive al proxy web.

Se è impostato su **Prohibited** (Non consentito), il reindirizzamento del contenuto del browser invia tramite proxy tutto il traffico TCP tra la sovrapposizione e il proxy Web senza interferire. La sovrapposizione utilizza le credenziali di autenticazione di base o qualsiasi altra credenziale disponibile per eseguire l'autenticazione nel proxy Web.

L'impostazione predefinita è Prohibited (Non consentito).

### Impostazioni dei criteri Browser content redirection Access Control List (ACL) (Elenco di controllo di accesso per il reindirizzamento del contenuto del browser)

Utilizzare questa impostazione per configurare un elenco di controllo di accesso (ACL, Access Control List) di URL che possono utilizzare il reindirizzamento del contenuto del browser o a cui è negato l'accesso al reindirizzamento del contenuto del browser.

Gli URL autorizzati sono gli URL nell'elenco di elementi consentiti il cui contenuto viene reindirizzato al client.

Il carattere jolly * è consentito, ma non lo è all'interno del protocollo o della parte dell'indirizzo di dominio dell'URL. Tuttavia, a partire da Citrix Virtual Apps and Desktops 7 2206, i caratteri jolly * sono consentiti all'interno della parte dell'indirizzo del sottodominio dell'URL.

Consentiti: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`, `http://*.xyz.com/`

Non consentiti: `http://*.*.com/`

È possibile ottenere una migliore granularità specificando percorsi nell'URL. Ad esempio, se si specifica `https://www.xyz.com/sports/index.html`, viene reindirizzata solo la pagina index.html.

Per impostazione predefinita, questa opzione è impostata su `https://www.youtube.com/*`

Per ulteriori informazioni, vedere l'articolo del Knowledge Center CTX238236.

### Browser content redirection authentication sites (Siti di autenticazione per il reindirizzamento del contenuto del browser)

Utilizzare questa impostazione per configurare un elenco di URL. I siti reindirizzati utilizzando il reindirizzamento del contenuto del browser utilizzano l'elenco per autenticare un utente. L'impostazione

specifica gli URL per i quali il reindirizzamento del contenuto del browser rimane attivo (reindirizzato) quando si esce da un URL nell'elenco di elementi consentiti.

Uno scenario classico è un sito Web che si basa su un provider di identità (IdP) per l'autenticazione. Ad esempio, un sito Web `www.xyz.com` deve essere reindirizzato all'endpoint, ma un IDP di terze parti, come Okta (`www.xyz.okta.com`), gestisce la porzione di autenticazione. L'amministratore utilizza il criterio di configurazione ACL di reindirizzamento del contenuto del browser per aggiungere `www.xyz.com` all'elenco di elementi consentiti. Quindi utilizza i siti di autenticazione del reindirizzamento del contenuto del browser per aggiungere `www.xyz.okta.com` all'elenco di autorizzazioni.

Per ulteriori informazioni, vedere l'articolo del Knowledge Center CTX238236.

### Impostazione Browser content redirection block list (Elenco di elementi non consentiti per il reindirizzamento del contenuto del browser)

Questa impostazione funziona insieme all'impostazione di configurazione ACL per il reindirizzamento del contenuto del browser. Considerare che gli URL sono presenti nell'impostazione di configurazione ACL di reindirizzamento del contenuto del browser e nell'impostazione di configurazione dell'elenco di blocco. In questo caso, la configurazione dell'elenco di blocco ha la precedenza e il contenuto del browser dell'URL non viene reindirizzato.

**Unauthorized URLs (URL non autorizzati):** specifica gli URL nell'elenco di elementi non consentiti per i quali il contenuto del browser non viene reindirizzato al client, ma ne viene eseguito il rendering sul server.

Il carattere jolly * è consentito, ma non è consentito all'interno del protocollo o della parte dell'indirizzo di dominio dell'URL.

Consentiti: `http://www.xyz.com/index.html`,`https://www.xyz.com/*`,`http://www.xyz.com/*videos*`

Non consentiti: `http://*.xyz.com/`

È possibile ottenere una migliore granularità specificando percorsi nell'URL. Ad esempio, se si specifica `https://www.xyz.com/sports/index.html`, solo index.html è presente nell'elenco di elementi non consentiti.

### Impostazione Browser content redirection proxy (Proxy di reindirizzamento del contenuto del browser)

Questa impostazione fornisce opzioni di configurazione per le impostazioni proxy sul VDA per il reindirizzamento del contenuto del browser. Se è abilitata con un indirizzo proxy e un numero di porta validi,

un URL PAC/WPAD o l'impostazione Direct/Transparent (Diretto/Trasparente), l'app Citrix Workspace tenta solo il recupero dal server e il rendering sul client.

Se è disabilitata o non configurata e utilizza un valore predefinito, l'app Citrix Workspace tenta il recupero dal client e il rendering sul client.

L'impostazione predefinita è Prohibited (Non consentito).

**Criterio consentito per un proxy esplicito:**

```
http://\<hostname/ip address\>:\<port\>
```

**Esempio:**

```
http://proxy.example.citrix.com:80
http://10.10.10.10:8080
```

**Criteri consentiti per i file PAC/WPAD:**

```
http://<hostname/ip address>:<port>/<path>/<Proxy.pac>
```

**Esempio:** `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

```
https://<hostname/ip address>:<port>/<path>/<wpad.dat>
```

**Esempio:** `http://10.10.10.10/configuration/pac/wpad.dat`

**Criteri consentiti per proxy diretti o trasparenti:**

Digitare la parola **DIRECT** nella casella di testo dei criteri.

## Sostituzioni della chiave del Registro di sistema per il reindirizzamento del contenuto del browser

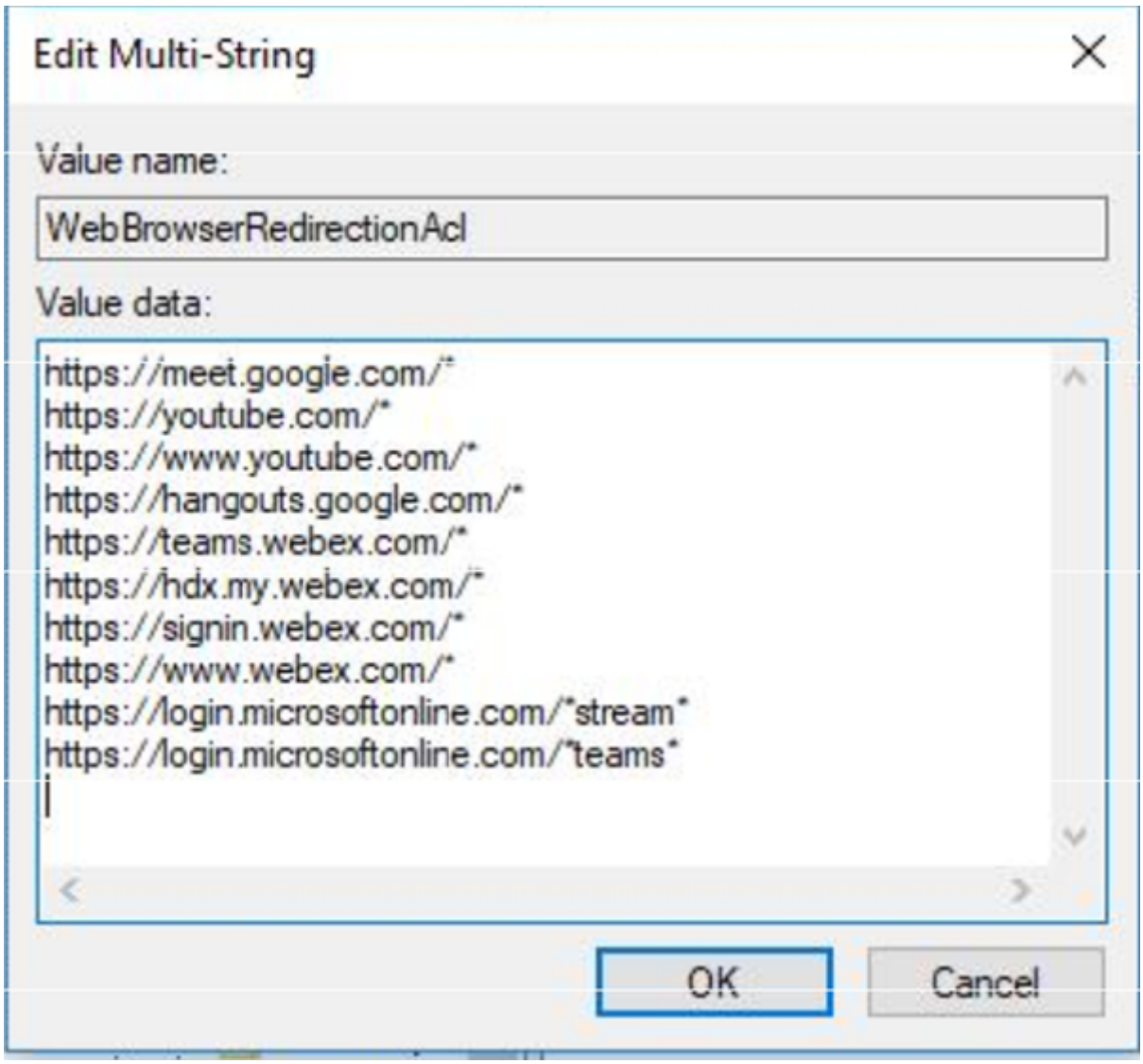
> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.
>
> Opzioni di sostituzione delle chiavi del Registro di sistema per le impostazioni dei criteri:

`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

| Nome | Tipo | Valore |
|---|---|---|
| WebBrowserRedirection | DWORD | 1=Consentito, 0=Vietato |

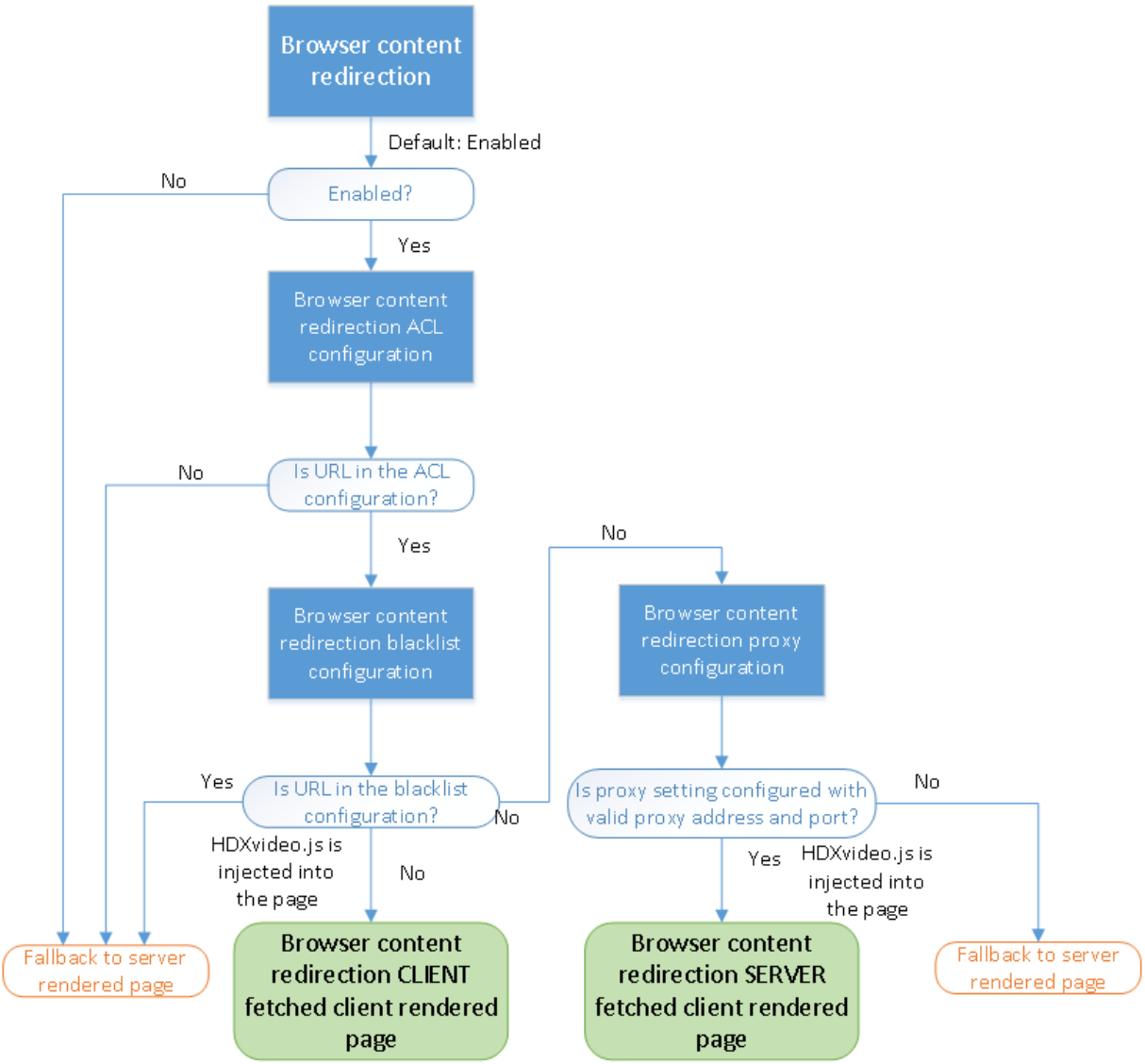
 

| Nome | Tipo | Valore |
| --- | --- | --- |
| WebBrowserRedirectionAcl | REG_MULTI_SZ | |
| WebBrowserRedirectionAuthenticationWhitelist | REG_MULTI_SZ | |
| WebBrowserRedirectionProxyAddress | REG_SZ | `http://myproxy.citrix.com:8080` o `http://10.10.10.10:8888` |
| WebBrowserRedirectionBlacklist | REG_MULTI_SZ | |



### Inserimento di HDXVideo.js per il reindirizzamento del contenuto del browser




HdxVideo.js viene inserito nella pagina Web utilizzando l'estensione Chrome di reindirizzamento del contenuto del browser o Internet Explorer Browser Helper Object (BHO). BHO è un modello di plug-in per Internet Explorer. Fornisce hook per le API del browser e consente al plug-in di accedere al DOM (Document Object Model) della pagina per controllare la navigazione.

Il BHO decide se inserire HdxVideo.js in una determinata pagina. La decisione si basa sui criteri amministrativi indicati nel diagramma di flusso precedente.

Dopo aver deciso di inserire JavaScript e reindirizzare il contenuto del browser al client, la pagina Web sul browser Internet Explorer nel VDA è vuota. L'impostazione di **document.body.innerHTML** su "vuoto"rimuove l'intero corpo della pagina Web sul VDA. La pagina è pronta per essere inviata al client in modo da essere visualizzata nel browser di sovrapposizione (Hdxbrowser.exe) sul client.

# Impostazioni dei criteri dei sensori client

January 7, 2024

La sezione **Client Sensors** (Sensori client) include le impostazioni dei criteri per controllare il modo in cui le informazioni sui sensori dei dispositivi mobili vengono gestite in una sessione utente.

## Consentire alle applicazioni di utilizzare la posizione fisica del dispositivo client

Questa impostazione determina se le applicazioni in esecuzione in una sessione su un dispositivo mobile possono utilizzare la posizione fisica del dispositivo utente.

Per impostazione predefinita, l'uso delle informazioni sulla posizione è vietato

Quando questa impostazione non è consentita, i tentativi da parte di un'applicazione di recuperare le informazioni sulla posizione restituiscono un valore "autorizzazione negata".

Quando questa impostazione è consentita, un utente può vietare l'utilizzo delle informazioni sulla posizione negando a una richiesta dell'app Citrix Workspace di accedere alla posizione. I dispositivi Android e iOS mostrano un avviso alla prima richiesta di informazioni sulla posizione in ogni sessione.

Quando si sviluppano applicazioni ospitate che utilizzano l'impostazione Allow applications to use the physical location of the client device (Consenti alle applicazioni di utilizzare la posizione fisica del dispositivo client), considerare quanto segue:

- Assicurarsi che un'applicazione abilitata alla posizione non si basi sulla disponibilità delle informazioni sulla posizione, in quanto:
  - Un utente potrebbe non consentire l'accesso alle informazioni sulla posizione.
  - La posizione potrebbe non essere disponibile o potrebbe cambiare durante l'esecuzione dell'applicazione.
  - Un utente potrebbe connettersi alla sessione dell'applicazione da un dispositivo diverso che non supporta le informazioni sulla posizione.
- Un'applicazione abilitata alla posizione deve:
  - Avere la funzionalità relativa alla posizione disabilitata per impostazione predefinita.
  - Fornire all'utente un'opzione per consentire o non consentire la funzionalità durante l'esecuzione dell'applicazione.
  - Fornire all'utente un'opzione per cancellare i dati sulla posizione che l'applicazione memorizza nella cache (l'app Citrix Workspace non memorizza nella cache i dati sulla posizione).

- Un'applicazione abilitata alla posizione deve gestire la granularità delle informazioni sulla posizione. Questa gestione garantisce che i dati acquisiti siano adatti allo scopo dell'applicazione. Inoltre, è conforme alle normative di tutte le giurisdizioni pertinenti.
- Utilizzare una connessione sicura (ad esempio, tramite TLS o VPN) quando si utilizzano i servizi di posizione. Connettere l'app Citrix Workspace ai server attendibili.
- Prendere in considerazione la possibilità di ottenere consulenza legale in merito all'utilizzo dei servizi di posizione.

## Impostazioni dei criteri dell'interfaccia utente desktop

January 7, 2024

La sezione **Desktop UI** (Interfaccia utente desktop) include le impostazioni dei criteri che controllano gli effetti visivi quali sfondo del desktop, animazioni dei menu e immagini di trascinamento. Queste impostazioni dei criteri aiutano a gestire la larghezza di banda utilizzata nelle connessioni client. È possibile migliorare le prestazioni delle applicazioni su una WAN limitando l'utilizzo della larghezza di banda.

> **Importante:**
>
> In questa versione non sono supportate la modalità grafica legacy e DCR (Desktop Composition Redirection). Questo criterio è incluso solo per la compatibilità con le versioni precedenti quando si utilizzano:
>
> - XenApp 7.15 LTSR
> - XenDesktop 7.15 LTSR
> - Versioni precedenti di VDA con Windows 7 e Windows 2008 R2.

### Desktop Composition Redirection (Reindirizzamento composizione desktop)

Ai fini di offrire agli utenti un'esperienza desktop Windows più fluida, questa impostazione specifica se utilizzare le funzionalità di elaborazione per il rendering della grafica DirectX locale di quanto segue:

- Unità di elaborazione grafica (GPU) sul dispositivo dell'utente
- Oppure
- Processore grafico integrato (IGP) sul dispositivo dell'utente

Se abilitata, l'opzione **Desktop Composition Redirection** (Reindirizzamento composizione desktop) offre un'esperienza Windows altamente reattiva mantenendo al contempo un'elevata scalabilità sul server.

Per impostazione predefinita, l'opzione **Desktop Composition Redirection** (Reindirizzamento composizione desktop) è disabilitata.

Per deselezionare **Desktop Composition Redirection** (Reindirizzamento composizione desktop) e ridurre la larghezza di banda richiesta nelle sessioni utente, selezionare **Disabled** (Disabilitato) quando si aggiunge questa impostazione a un criterio.

### Desktop Composition Redirection graphics quality (Qualità grafica di reindirizzamento composizione desktop)

Questa impostazione specifica la qualità della grafica utilizzata per Desktop Composition Redirection (Reindirizzamento composizione desktop).

L'impostazione predefinita è High (Alta).

Scegli tra High (Alta), Medium (Media), Low (Bassa) o Lossless (Senza perdita di dati).

### Desktop wallpaper (Sfondo del desktop)

Questa impostazione consente o impedisce la visualizzazione dello sfondo nelle sessioni utente.

Per impostazione predefinita, le sessioni utente possono mostrare lo sfondo.

Per deselezionare lo sfondo del desktop e ridurre la larghezza di banda richiesta nelle sessioni utente, selezionare **Prohibited** (Non consentito) quando si aggiunge questa impostazione a un criterio.

### Menu animation (Animazione menu)

Questa impostazione consente o impedisce l'animazione del menu nelle sessioni utente.

Per impostazione predefinita, l'animazione del menu è consentita.

L'animazione del menu è un'impostazione delle preferenze personali di Microsoft per facilitare l'accesso. Se abilitata, viene visualizzato un menu dopo un breve ritardo, mediante scorrimento o dissolvenza in entrata. Nella parte inferiore del menu viene visualizzata un'icona a forma di freccia. Il menu viene visualizzato quando si punta su tale freccia.

L'animazione del menu è abilitata su un desktop se questa impostazione dei criteri è impostata su **Allowed** (Consentita) e l'impostazione delle preferenze personali di Microsoft per l'animazione del menu è abilitata.

> **Nota:**
>
> Le modifiche apportate all'impostazione delle preferenze personali di Microsoft per l'animazione del menu influiscono sul desktop. Considerare la possibilità di impostare il desktop

> per annullare le modifiche al termine della sessione. In questo caso, un utente che ha abilitato le animazioni del menu potrebbe non avere a disposizione l'animazione del menu nelle sessioni successive. Per gli utenti che richiedono l'animazione del menu, abilitare l'impostazione Microsoft nell'immagine principale per il desktop o assicurarsi che il desktop mantenga le modifiche dell'utente.

### View window contents while dragging (Visualizza contenuto della finestra durante il trascinamento)

Questa impostazione consente o impedisce la visualizzazione del contenuto della finestra quando si trascina una finestra sullo schermo.

Per impostazione predefinita, la visualizzazione del contenuto della finestra è consentita.

Se questa opzione è impostata su **Allowed** (Consentita), l'intera finestra viene spostata quando viene trascinata. Se è impostata su **Prohibited** (Non consentita), viene visualizzato solo il contorno della finestra finché non viene rilasciata.

## Impostazioni dei criteri di monitoraggio dell'utente finale

January 7, 2024

La sezione **End User Monitoring** (Monitoraggio dell'utente finale) include le impostazioni dei criteri per la misurazione del traffico delle sessioni.

### ICA round trip calculation (Calcolo del round trip ICA)

Questa impostazione determina se vengono eseguiti i calcoli di round trip ICA per le connessioni attive.

Per impostazione predefinita, i calcoli per le connessioni attive sono abilitati.

Per impostazione predefinita, ogni avvio della misurazione di andata e ritorno ICA è ritardato. Questo ritardo è fino a quando viene rilevato traffico che indica un'interazione dell'utente. Questo ritardo può essere di lunghezza indefinita e ha lo scopo di evitare che la misurazione del round trip ICA sia l'unica ragione del traffico ICA.

### ICA round trip calculation interval (Intervallo di calcolo del round trip ICA)

Questa impostazione specifica la frequenza, espressa in secondi, con la quale vengono eseguiti i calcoli del round trip ICA.

Per impostazione predefinita, il round trip ICA viene calcolato ogni 15 secondi.

### ICA round trip calculations for idle connections (Calcoli del round trip ICA per le connessioni inattive)

Questa impostazione determina se vengono eseguiti i calcoli di round trip ICA per le connessioni inattive.

Per impostazione predefinita, i calcoli non vengono eseguiti per le connessioni inattive.

Per impostazione predefinita, ogni avvio della misurazione di andata e ritorno ICA è ritardato. Questo ritardo è fino a quando viene rilevato traffico che indica un'interazione dell'utente. Questo ritardo può essere di lunghezza indefinita e ha lo scopo di evitare che la misurazione del round trip ICA sia l'unica ragione del traffico ICA.

## Impostazione dei criteri Esperienza desktop migliorata

January 7, 2024

L'impostazione dei criteri Enhanced desktop experience (Esperienza desktop migliorata) esegue sessioni su sistemi operativi server che assomigliano a desktop Windows 7 locali.

Per impostazione predefinita, questa impostazione è consentita.

Se sul desktop virtuale esiste un profilo utente con il tema Windows classico, questo criterio non fornisce un'esperienza desktop migliorata per tale utente. Considerare che un utente con un profilo utente a tema di Windows 7 accede a un desktop virtuale che esegue Windows Server 2012. Inoltre, questo criterio è non configurato o disabilitato. In questo caso, quell'utente visualizza un messaggio di errore che indica la mancata applicazione del tema.

In entrambi i casi, la reimpostazione del profilo utente risolve il problema.

Se si disabilita il criterio su un desktop virtuale con sessioni utente attive, l'interfaccia di tali sessioni diventa incoerente sui desktop Windows 7 e Windows classico. Per evitare questa incoerenza, assicurarsi di riavviare il desktop virtuale dopo aver modificato questa impostazione dei criteri. Eliminare quindi tutti i profili di roaming sul desktop virtuale. Citrix consiglia inoltre di eliminare qualsiasi altro profilo utente sul desktop virtuale per evitare incongruenze tra i profili.

Considerare che si stanno utilizzando profili utente mobili nel proprio ambiente. In questo caso, verificare che la funzionalità Enhanced Desktop Feature (Esperienza desktop migliorata) sia abilitata o disabilitata per tutti i desktop virtuali che condividono un profilo.

Citrix sconsiglia di condividere profili di roaming tra desktop virtuali che eseguono sistemi operativi server e sistemi operativi client. I profili per i sistemi operativi client e server differiscono. La condivisione di profili di roaming tra entrambi i tipi può causare incongruenze nelle proprietà del profilo quando un utente si sposta tra i due.

## Impostazioni dei criteri di reindirizzamento file

January 7, 2024

La sezione **File Redirection** (Reindirizzamento file) include le impostazioni dei criteri relativi alla mappatura e all'ottimizzazione delle unità client.

### Auto connect client drives (Connetti automaticamente le unità client)

Questa impostazione consente o impedisce la connessione automatica delle unità client quando gli utenti accedono.

Per impostazione predefinita, la connessione automatica è consentita.

Quando si aggiunge questa impostazione a un criterio, assicurarsi di abilitare le impostazioni per i tipi di unità che si desidera connettere automaticamente. Ad esempio, per consentire il collegamento automatico delle unità CD-ROM degli utenti, configurare questa impostazione e l'impostazione **Client optical drives** (Unità ottiche client).

Le seguenti impostazioni dei criteri sono correlate:

- **Client drive redirection (Reindirizzamento delle unità client)**
- **Client floppy drives (Unità floppy client)**
- **Client optical drives (Unità ottiche client)**
- **Client fixed drives (Unità fisse client)**
- **Client network drives (Unità di rete client)**
- **Client removable drives (Unità rimovibili client)**

### Client drive redirection (Reindirizzamento delle unità client)

Questa impostazione abilita o disabilita il reindirizzamento dei file da e verso le unità sul dispositivo utente.

Per impostazione predefinita, il reindirizzamento dei file è abilitato.

> **Nota:**
>
> Le impostazioni dei criteri di reindirizzamento delle unità client non si applicano alle unità mappate a sessioni che utilizzano il reindirizzamento USB generico.

Se abilitate, gli utenti possono salvare i file in tutte le unità client. Quando sono disattivate, ogni operazione di reindirizzamento file viene impedita. Questa configurazione è applicabile indipendentemente dallo stato delle singole impostazioni di reindirizzamento file. Le singole impostazioni di reindirizzamento file includono le unità floppy client e le unità di rete client.

Le seguenti impostazioni dei criteri sono correlate:

- **Client floppy drives (Unità floppy client)**
- **Client optical drives (Unità ottiche client)**
- **Client fixed drives (Unità fisse client)**
- **Client network drives (Unità di rete client)**
- **Client removable drives (Unità rimovibili client)**

### Client fixed drives (Unità fisse client)

Questa impostazione consente o impedisce agli utenti di accedere o salvare file su unità fisse sul dispositivo utente.

Per impostazione predefinita, è consentito accedere alle unità fisse client.

Quando si aggiunge questa impostazione a un criterio, assicurarsi che l'impostazione **Client drive redirection** (Reindirizzamento unità client) sia presente e impostata su Allowed (Consentito). Se queste impostazioni sono disabilitate, le unità fisse client non vengono mappate e gli utenti non possono accedere manualmente a queste unità, indipendentemente dallo stato dell'impostazione **Client fixed drives** (Unità fisse client).

Configurare l'impostazione Auto **connect client drives** (Connetti automaticamente unità client) per garantire che le unità fisse vengano collegate automaticamente quando gli utenti eseguono l' accesso.

### Client floppy drives (Unità floppy client)

Questa impostazione consente o impedisce agli utenti di accedere o salvare file su unità floppy sul dispositivo utente.

Per impostazione predefinita, l'accesso alle unità floppy client è consentito.

Quando si aggiunge questa impostazione a un criterio, assicurarsi che l'impostazione **Client drive redirection** (Reindirizzamento unità client) sia presente e impostata su Allowed (Consentito). Se

queste impostazioni sono disabilitate, le unità floppy client non vengono mappate e gli utenti non possono accedere manualmente a queste unità, indipendentemente dallo stato dell'impostazione **Client floppy drives** (Unità floppy client).

Per garantire che le unità floppy siano connesse automaticamente quando gli utenti accedono, configurare l'impostazione **Auto connect client drives** (Connetti automaticamente unità client).

### Client network drives (Unità di rete client)

Questa impostazione consente o impedisce agli utenti di accedere e salvare file su unità di rete (remote) tramite il dispositivo utente.

Per impostazione predefinita, l'accesso alle unità di rete client è consentito.

Quando si aggiunge questa impostazione a un criterio, assicurarsi che l'impostazione **Client drive redirection** (Reindirizzamento unità client) sia presente e impostata su Allowed (Consentito). Se queste impostazioni sono disabilitate, le unità di rete client non vengono mappate e gli utenti non possono accedere manualmente a queste unità. Questa configurazione è applicabile a prescindere dallo stato dell'impostazione **Client network drives** (Unità di rete client).

Per garantire che le unità di rete vengano connesse automaticamente quando gli utenti accedono, configurare l'impostazione **Auto connect client drives** (Connetti automaticamente unità client).

### Client optical drives (Unità ottiche client)

Questa impostazione consente o impedisce agli utenti di accedere o salvare i file nei seguenti supporti:

- CD-ROM sul dispositivo dell'utente
- DVD-ROM sul dispositivo dell'utente
- Unità BD-ROM sul dispositivo dell'utente.

Per impostazione predefinita, l'accesso alle unità ottiche client è consentito.

Quando si aggiunge questa impostazione a un criterio, assicurarsi che l'impostazione **Client drive redirection** (Reindirizzamento unità client) sia presente e impostata su **Allowed** (Consentito). Se queste impostazioni sono disabilitate, le unità ottiche client non vengono mappate e gli utenti non possono accedere manualmente a queste unità. Questa configurazione è applicabile a prescindere dallo stato dell'impostazione **Client optical drives** (Unità ottiche client).

Per garantire che le unità ottiche siano connesse automaticamente quando gli utenti accedono, configurare l'impostazione **Auto connect client drives** (Connetti automaticamente unità client).

### Client removable drives (Unità rimovibili client)

Questa impostazione consente o impedisce agli utenti di accedere ai file o salvarli su unità USB sul dispositivo utente.

Per impostazione predefinita, l'accesso alle unità rimovibili client è consentito.

Quando si aggiunge questa impostazione a un criterio, verificare che l'impostazione **Client drive redirection**(Reindirizzamento unità client) sia presente e sia impostata su Allowed (Consentito). Se queste impostazioni sono disabilitate, le unità rimuovibili dal client non vengono mappate e gli utenti non possono accedere manualmente a queste unità. Questa configurazione è applicabile a prescindere dallo stato dell'impostazione **Client removable drives** (Unità rimuovibili client).

Configurare l'impostazione **Auto connect client drives** (Connetti automaticamente unità client) per garantire che le unità rimuovibili vengano collegate automaticamente quando gli utenti eseguono l'accesso.

### Reindirizzamento da host a client

Questa impostazione abilita o disabilita le associazioni dei tipi di file per gli URL e alcuni contenuti multimediali da aprire sul dispositivo utente. Se è disabilitata, il contenuto si apre sul server.

Per impostazione predefinita, l'associazione dei tipi di file è disabilitata.

Questi tipi di URL vengono aperti localmente quando si abilita questa impostazione:

- HTTP
- HTTPS
- RTSP (Real Player e QuickTime)
- RTSPU (Real Player e QuickTime)
- PNM (Legacy Real Player)
- Microsoft Media Server (MMS)

### Preserve client drive letters (Mantieni lettere di unità client)

Questa impostazione abilita o disabilita la mappatura delle unità client alla stessa lettera di unità nella sessione.

Per impostazione predefinita, le lettere di unità client non vengono conservate.

Quando si aggiunge questa impostazione a un criterio, assicurarsi che l'impostazione **Client drive redirection** (Reindirizzamento unità client) sia presente e impostata su Allowed (Consentito).

### Read-only client drive access (Accesso alle unità client in sola lettura)

Questa impostazione consente o impedisce agli utenti e alle applicazioni di:

- Creare file su unità client mappate
- Modificare file su unità client mappate
- Modificare le cartelle su unità client mappate

Per impostazione predefinita, i file e le cartelle sulle unità client mappate possono essere modificati.

Se è impostata su Enabled (Abilitata), i file e le cartelle sono accessibili con autorizzazioni di sola lettura.

Quando si aggiunge questa impostazione a un criterio, assicurarsi che l'impostazione **Client drive redirection** (Reindirizzamento unità client) sia presente e impostata su Allowed (Consentito).

### Special folder redirection (Reindirizzamento cartelle speciali)

Questa impostazione consente o impedisce agli utenti dell'app Citrix Workspace e dell'interfaccia Web di visualizzare le cartelle speciali Documenti e Desktop locali da una sessione.

Per impostazione predefinita, il reindirizzamento delle cartelle speciali è consentito.

Questa impostazione impedisce che il reindirizzamento delle cartelle speciali venga applicato a eventuali oggetti filtrati tramite un criterio, indipendentemente dalle impostazioni configurate altrove. Quando questa impostazione non è consentita, tutte le impostazioni correlate specificate per StoreFront, per l'interfaccia Web o per l'app Citrix Workspace vengono ignorate.

Per definire a quali utenti è applicabile il reindirizzamento delle cartelle speciali, selezionare **Allowed** (Consentito) e includere questa impostazione in un criterio a cui è applicato un filtro relativo agli utenti per i quali si desidera rendere disponibile questa funzionalità. Questa impostazione sostituisce tutte le altre impostazioni di reindirizzamento delle cartelle speciali.

Le impostazioni dei criteri che impediscono agli utenti di accedere ai file o salvarli sui dischi rigidi locali impediscono anche il funzionamento del reindirizzamento delle cartelle speciali. Questa situazione si verifica perché il reindirizzamento delle cartelle speciali deve interagire con il dispositivo dell'utente.

Quando si aggiunge questa impostazione a un criterio, assicurarsi che l'impostazione **Client fixed drives** (Unità fisse client) sia presente e sia impostata su Allowed (Consentito).

### Criteri di trasferimento file

Per impostazione predefinita, il trasferimento dei file è abilitato. Utilizzare Web Studio per modificare questi criteri, che si trovano in **User Setting < ICA\File Redirection** (Impostazioni utente < ICA\Reindirizzamento file). Quando si utilizzano i criteri di trasferimento file, tenere presenti gli elementi seguenti:

- **File transfer for Citrix Workspace app for Chrome OS/HTML5** (Trasferimento di file per l'app Citrix Workspace per Chrome OS/HTML5): consente o impedisce agli utenti di trasferire file tra una sessione di Citrix Virtual Apps and Desktops e i loro dispositivi.
- **Upload file for Citrix Workspace app for Chrome OS/HTML5** (Carica file per l'app Citrix Workspace per Chrome OS/HTML5): consente o impedisce agli utenti di caricare file dal proprio dispositivo a una sessione di Citrix Virtual Apps and Desktops.
- **Download file for Citrix Workspace app for Chrome OS/HTML5** (Scarica il file per l'app Citrix Workspace per Chrome OS/HTML5): consente o impedisce agli utenti di scaricare file da una sessione di Citrix Virtual Apps and Desktops sul proprio dispositivo.

> **Nota:**
>
> I criteri di trasferimento dei file si applicano solo all'app Citrix Workspace per HTML5 e all'app Citrix Workspace per Chrome OS.

### Use asynchronous writes (Usa scritture asincrone)

Questa impostazione abilita o disabilita le scritture su disco asincrone.

Per impostazione predefinita, le scritture asincrone sono disabilitate.

Le scritture su disco asincrone possono migliorare la velocità di trasferimento e scrittura di file su dischi client per le WAN, solitamente caratterizzate da larghezza di banda relativamente elevata e latenza elevata. Tuttavia, se si verifica un errore di connessione o disco, il file client o i file in fase di scrittura potrebbero passare a uno stato non definito. In tal caso, una finestra popup informa l'utente dei file interessati. L'utente può quindi eseguire azioni correttive, ad esempio il riavvio di un trasferimento di file interrotto al momento della riconnessione o quando l'errore del disco viene corretto.

Citrix consiglia di abilitare le scritture asincrone su disco solo per gli utenti che necessitano di connettività remota con una buona velocità di accesso ai file. E per coloro che possono facilmente recuperare file o dati persi in caso di connessione o guasto del disco.

Quando si aggiunge questa impostazione a un criterio, verificare che l'impostazione **Client drive redirection**(Reindirizzamento unità client) sia presente e sia impostata su Allowed (Consentito). Se questa impostazione è disabilitata, le scritture asincrone non vengono eseguite.

# Impostazioni dei criteri di grafica

April 3, 2024

La sezione **Graphics** include le impostazioni dei criteri per controllare la modalità di gestione delle immagini nelle sessioni utente.

## Allow visually lossless compression (Consenti compressione senza perdita di dati dal punto di vista visivo)

Questa impostazione consente di utilizzare la compressione senza perdita di dati dal punto di vista visivo anziché la vera compressione senza perdita di dati per la grafica. La prima opzione, rispetto alla seconda, migliora le prestazioni, ma comporta una perdita di piccola entità non visibile a occhio. Questa impostazione modifica il modo in cui vengono utilizzati i valori dell'impostazione Visual quality (Qualità visiva).

Per impostazione predefinita, questa impostazione è disabilitata.

## Graphics status indicator

Questa impostazione configura l'indicatore di stato della grafica per l'esecuzione nella sessione utente. Questo strumento consente all'utente di visualizzare informazioni sulla modalità grafica attiva. Le informazioni includono dettagli di codec video, codifica hardware, qualità dell'immagine e monitor in uso per la sessione. Con l'indicatore di stato grafico, l'utente può anche abilitare o disabilitare la modalità pixel perfect.

La versione 2103 di Citrix Virtual Apps and Desktops e le versioni successive includono un dispositivo di scorrimento della qualità dell'immagine per aiutare l'utente a trovare il giusto equilibrio tra qualità dell'immagine e interattività.

La versione 2109 di Citrix Virtual Apps and Desktops e le versioni successive includono funzionalità per configurare un layout di visualizzazione virtuale tramite un'interfaccia utente avviata utilizzando l'indicatore di stato grafico.

L'indicatore di stato grafico sostituisce lo strumento indicatore senza perdita di dati delle versioni precedenti. Questa politica abilita l'indicatore lossless per Citrix Virtual Apps and Desktops versioni da 7.16 a 1809.

### Condivisione dello schermo

Questa impostazione consente agli utenti di condividere le proprie sessioni, inclusi i contenuti dello schermo, tastiere e mouse, con altri utenti.

Per impostazione predefinita, questa impostazione è disabilitata.

Il VDA tenta di utilizzare le porte dell'intervallo di porte TCP per lo scambio di dati, iniziando dalla porta più bassa e incrementando ogni connessione successiva. La porta gestisce il traffico sia in entrata che in uscita.

Per impostazione predefinita, l'intervallo di porte TCP è impostato su 52525-52625.

La porta utilizzata per la condivisione dello schermo deve essere aggiunta all'elenco delle eccezioni del firewall. Questa opzione viene visualizzata come casella di controllo durante l'installazione del VDA. Per impostazione predefinita, questa opzione non è selezionata.

### Display memory limit (Visualizza limite di memoria)

Questa impostazione specifica la dimensione massima del buffer video in kilobyte per la sessione.

Per impostazione predefinita, il limite di memoria di visualizzazione è 65.536 kilobyte.

Specifica la dimensione massima del buffer video in kilobyte per la sessione. Specificare una quantità in kilobyte da 128 a 4.194.303. Il valore massimo di 4.194.303 non limita la memoria di visualizzazione. Per impostazione predefinita, la memoria di visualizzazione è 65.536 kilobyte. L'utilizzo di una maggiore profondità di colore e di una risoluzione più elevata per le connessioni richiede più memoria. In modalità grafica legacy, se viene raggiunto il limite di memoria, la qualità della visualizzazione diminuisce in base all'impostazione Display mode degrade preference (Preferenza per il peggioramento della modalità di visualizzazione).

Per le connessioni che richiedono una maggiore profondità di colore e una risoluzione più elevata, aumentare il limite. Calcolare la memoria massima richiesta utilizzando l'equazione:

Profondità della memoria in byte = (profondità del colore in bit per pixel)/8) x (risoluzione verticale in pixel) x (risoluzione orizzontale in pixel).

Ad esempio, si consideri uno scenario con una profondità di colore di 32, una risoluzione verticale di 600 e una risoluzione orizzontale di 800. In questo caso, la memoria massima richiesta è (32/8) x (600) x (800) = 1920000 byte, il che produce un limite di memoria di visualizzazione di 1920 KB.

Le profondità di colore diverse da 32 bit sono disponibili solo se è abilitata l'impostazione dei criteri Legacy graphics mode (Modalità grafica legacy).

HDX alloca solo la quantità di memoria di visualizzazione necessaria per ogni sessione. Pertanto, se solo alcuni utenti richiedono un valore superiore a quello predefinito, non vi è alcun impatto negativo sulla scalabilità se si aumenta il limite di memoria di visualizzazione.

### Display mode degrade preference (Preferenza per il peggioramento della modalità di visualizzazione)

> **Nota:**
>
> Per Virtual Delivery Agent 7.x, questa impostazione dei criteri si applica solo quando è abilitata l'impostazione dei criteri Legacy graphics mode (Modalità grafica legacy).

Quando viene raggiunto il limite di memoria di visualizzazione della sessione, questa impostazione specifica se peggiorerà prima la profondità del colore o la risoluzione.

Per impostazione predefinita, la profondità del colore peggiorerà per prima.

Quando viene raggiunto il limite di memoria della sessione, è possibile ridurre la qualità delle immagini visualizzate. È possibile ridurre questa qualità scegliendo se peggiora per prima la profondità o la risoluzione del colore. Quando la profondità del colore peggiora per prima, le immagini visualizzate utilizzano meno colori. Quando la risoluzione peggiora per prima, le immagini visualizzate utilizzano meno pixel per pollice.

Per avvertire gli utenti del peggioramento della profondità del colore o della risoluzione, configurare l'impostazione Notify user when display mode is degraded (Avvisa l'utente quando la modalità di visualizzazione peggiora).

### Dynamic windows preview (Anteprima finestre dinamiche)

Questa impostazione abilita o disabilita la visualizzazione di finestre senza soluzione di continuità in:

- Capovolgimento
- Scorrimento finestre 3D
- Anteprima della barra delle applicazioni
- Anteprima di Windows

| Opzione di anteprima di Windows Aero | Descrizione |
|---|---|
| Anteprima della barra delle applicazioni | Quando l'utente passa il mouse sull'icona della barra delle applicazioni di una finestra, viene visualizzata un'immagine di tale finestra sopra la barra delle applicazioni. |
| Anteprima di Windows | Quando l'utente passa il mouse su un'immagine di anteprima della barra delle applicazioni, sullo schermo viene visualizzata un'immagine di dimensioni standard della finestra. |

| Opzione di anteprima di Windows Aero | Descrizione |
| --- | --- |
| Capovolgimento | Quando l'utente preme ALT+TAB, vengono visualizzate piccole icone di anteprima per ogni finestra aperta. |
| Scorrimento finestre 3D | Quando l'utente preme il tasto TAB+logo Windows, vengono sovrapposte sullo schermo immagini di grandi dimensioni delle finestre aperte. |

Per impostazione predefinita, questa impostazione è abilitata.

### Caching delle immagini

> **Nota:**
>
> Per Virtual Delivery Agent 7.x, questa impostazione dei criteri si applica solo quando è abilitata l'impostazione dei criteri Legacy graphics mode (Modalità grafica legacy).

Questa impostazione abilita o disabilita la memorizzazione nella cache e il recupero di sezioni di immagini nelle sessioni. La memorizzazione nella cache delle immagini nelle sezioni e il recupero di queste sezioni quando necessario dà origine a quanto segue:

- Scorrimento più fluido sul dispositivo dell'utente
- Minore quantità di dati trasmessi in rete sul dispositivo dell'utente
- Minore elaborazione richiesta sul dispositivo dell'utente

Per impostazione predefinita, l'impostazione di memorizzazione nella cache delle immagini è abilitata.

> **Nota:**
>
> L'impostazione di memorizzazione nella cache delle immagini controlla il modo in cui le immagini vengono memorizzate nella cache e recuperate. L'impostazione non controlla se le immagini sono memorizzate nella cache. Le immagini vengono memorizzate nella cache se l'impostazione Legacy graphics mode (Modalità grafica legacy) è abilitata.

### Legacy graphics mode (Modalità grafica legacy) - non supportata. Solo per compatibilità con le versioni precedenti

> **Importante:**
>
> In questa versione non sono supportate la modalità grafica legacy e DCR (Desktop Composition Redirection). Questo criterio è incluso solo per la compatibilità con le versioni precedenti quando si utilizza XenApp 7.15 LTSR, XenDesktop 7.15 LTSR e le versioni di VDA precedenti con Windows 7 e Windows 2008 R2.

Questa impostazione disabilita l'esperienza grafica avanzata. Utilizzare questa impostazione per ripristinare l'esperienza grafica legacy, riducendo il consumo di larghezza di banda su una connessione WAN o mobile. Le riduzioni della larghezza di banda introdotte in XenApp e XenDesktop 7.13 rendono questa modalità obsoleta.

Per impostazione predefinita, questa impostazione è disabilitata e gli utenti usufruiscono di un'esperienza grafica avanzata.

La modalità grafica legacy è supportata nei seguenti sistemi:

- Windows 7
- VDA per Windows Server 2008 R2.

La modalità grafica legacy non è supportata nei seguenti sistemi:

- Windows 8.x e 10
- Windows Server 2012, 2012 R2 e 2016.

Per ulteriori informazioni sull'ottimizzazione delle modalità grafiche e dei criteri in XenApp e XenDesktop 7.6 FP3 o versioni successive, vedere CTX202687.

### Maximum allowed color depth (Profondità colore massima consentita)

> **Nota:**
>
> Per Virtual Delivery Agent 7.x, questa impostazione dei criteri si applica solo quando è abilitata l'impostazione dei criteri Legacy graphics mode (Modalità grafica legacy).

Questa impostazione specifica la profondità di colore massima consentita per una sessione.

Per impostazione predefinita, la profondità di colore massima consentita è di 32 bit per pixel.

Questa impostazione si applica solo ai driver e alle connessioni Thinwire. Non si applica ai VDA che hanno un driver non ThinWire come driver video principale. Questi VDA sono VDA che utilizzano un driver WDDM (Windows Display Driver Model) come driver video principale. Per i VDA con sistema operativo a sessione singola che utilizzano un driver WDDM come driver di visualizzazione principale, ad esempio Windows 8, questa impostazione non ha effetto. Per i VDA con sistema operativo Windows multisessione che utilizzano un driver WDDM, ad esempio Windows Server 2012 R2, questa impostazione potrebbe impedire agli utenti di connettersi al VDA.

L'impostazione di una profondità di colore elevata richiede più memoria. Per ridurre la profondità del colore quando viene raggiunto il limite di memoria, configurare l'impostazione **Display mode degrade preference** (Preferenza per il peggioramento della modalità di visualizzazione). Quando la profondità del colore peggiora, le immagini visualizzate utilizzano meno colori.

### Notify user when display mode is degraded (Avvisa l'utente quando la modalità di visualizzazione peggiora)

> **Nota:**
>
> Per Virtual Delivery Agent 7.x, questa impostazione dei criteri si applica solo quando è abilitata l'impostazione dei criteri Legacy graphics mode (Modalità grafica legacy).

Questa impostazione visualizza una breve spiegazione all'utente quando la profondità o la risoluzione del colore peggiorano.

Per impostazione predefinita, l'invio di una notifica agli utenti è disabilitata.

### Ottimizzazione per carichi di lavoro grafici 3D

Questa impostazione configura le impostazioni predefinite appropriate che meglio si adattano ai carichi di lavoro ad elevato consumo di grafica. Abilitare questa impostazione per gli utenti il cui carico di lavoro viene eseguito su applicazioni ad elevato uso di grafica. Applicare questo criterio solo nei casi in cui una GPU è disponibile per la sessione. Qualsiasi altra impostazione che sovrascrive esplicitamente le impostazioni predefinite impostate da questo criterio ha la precedenza.

Per impostazione predefinita, l'ottimizzazione per il carico di lavoro della grafica 3D è disabilitata.

### Queuing and tossing (Metti in coda e ignora)

> **Nota:**
>
> Per Virtual Delivery Agent 7.x, questa impostazione dei criteri si applica solo quando è abilitata l'impostazione dei criteri Legacy graphics mode (Modalità grafica legacy).

Questa impostazione elimina le immagini in coda sostituite da un'altra immagine.

Per impostazione predefinita, questa impostazione è abilitata.

Questa impostazione migliora la risposta quando la grafica viene inviata al dispositivo utente. Configurando questa impostazione, le animazioni diventano mosse a causa di fotogrammi non elaborati.

### Use video codec for compression (Usa codec video per la compressione)

Consente di utilizzare un codec video per comprimere la grafica quando la decodifica video è disponibile nell'endpoint. Quando si sceglie **For the entire screen** (Per l'intero schermo), il codec video viene applicato come codec predefinito per tutti. Quando si seleziona **For actively changing regions** (Per zone che cambiano attivamente), il codec video viene utilizzato per le zone in cui è presente un cambiamento costante sullo schermo, gli altri dati utilizzano la compressione delle immagini fisse e la memorizzazione nella chat delle bitmap. Quando la decodifica video non è disponibile nell'endpoint o quando si specifica **Do not use video codec** (Non utilizzare il codec video), viene utilizzata una combinazione di compressione delle immagini fisse e memorizzazione nella cache delle bitmap. Quando si seleziona **Use when preferred** (Usa in base alla preferenza), il sistema sceglie in base a vari fattori. I risultati possono variare tra le versioni man mano che il metodo di selezione viene migliorato.

Selezionare **Use when preferred** (Usa in base alla preferenza) per consentire al sistema di scegliere le impostazioni appropriate per lo scenario corrente.

Selezionare **For the entire screen** (Per l'intero schermo) per migliorare l'esperienza utente e la larghezza di banda, soprattutto nei casi con un uso intensivo di video e grafica 3D con rendering sul server.

Selezionare **For actively changing regions** (Per zone che cambiano attivamente) per ottimizzare le prestazioni video, in particolare con larghezza di banda ridotta, mantenendo al contempo la scalabilità per contenuti statici e che cambiano lentamente. Questa impostazione è supportata nelle distribuzioni con più monitor.

Selezionare **Do not use video codec** (Non utilizzare codec video) per ottimizzare il carico della CPU del server e per i casi in cui non sono presenti numerosi video con rendering sul server o altre applicazioni ad uso intensivo di grafica.

L'impostazione predefinita è **Use when preferred** (Usa in base alla preferenza).

### Use hardware encoding for video (Utilizza codifica hardware per i video)

Questa impostazione consente l'utilizzo di hardware grafico, se disponibile, per comprimere gli elementi dello schermo con il codec video. Se tale hardware non è disponibile, il VDA torna alla codifica basata su CPU utilizzando il codec video software.

L'opzione predefinita per questa impostazione dei criteri è **Enabled** (Abilitata).

Sono supportati più monitor.

Qualsiasi app Citrix Workspace che supporta la decodifica video può essere utilizzata con la codifica hardware.

#### NVIDIA

Per le GPU NVIDIA GRID, la codifica hardware è supportata con VDA per sistema operativo multisessione e sistema operativo a sessione singola.

Le GPU NVIDIA devono supportare la codifica hardware NVENC. Vedere SDK del codec video NVIDIA per un elenco delle GPU supportate.

NVIDIA GRID richiede un driver versione 3.1 o successiva. NVIDIA Quadro richiede un driver versione 362.56 o successiva. Citrix consiglia i driver del tipo NVIDIA R361 Release.

Il testo senza perdita di dati non è compatibile con la codifica hardware NVENC. Se il testo senza perdita di dati è abilitato, ha la priorità sulla codifica hardware NVENC.

L'uso selettivo del codec hardware H.264 per zone in continua evoluzione è supportato.

La compressione senza perdita di dati dal punto di vista visivo (YUV 4:4:4) è supportata. Senza perdita di dati dal punto di vista visivo (impostazione dei criteri grafici Allow visually lossless compression [Consenti compressione senza perdita di dati dal punto di vista visivo]) richiede l'app Citrix Workspace 1808 o versioni successive o Citrix Receiver per Windows 4.5 o versioni successive.

#### Intel

Per i processori grafici Intel Iris Pro, la codifica hardware è supportata con VDA per sistema operativo a sessione singola e sistema operativo multisessione.

Sono supportati i processori grafici Intel Iris Pro della famiglia di processori Intel Broadwell e versioni successive. È richiesto l'SDK Intel Remote Displays versione 1.0, che può essere scaricato dal sito Web Intel: SDK Remote Displays.

Il testo senza perdita di dati è supportato solo quando il criterio Video codec (Codec video) è impostato per l'intero schermo e il criterio **Optimize for 3D graphics workload** (Ottimizza per il carico di lavoro della grafica 3D) è disabilitato.

L'opzione Visually losssless (YUV 4:4:4) (Senza perdita di dati dal punto di vista visivo) non è supportata.

Il codificatore Intel offre una buona esperienza utente per un massimo di otto sessioni di codifica (ad esempio un utente che utilizza otto monitor o otto utenti che utilizzano un monitor ciascuno). Se sono necessarie più di otto sessioni di codifica, verificare con quanti monitor si connette la macchina virtuale. L'amministratore decide di configurare questa impostazione dei criteri per utente o per macchina per mantenere una buona esperienza utente.

#### AMD

Per AMD, la codifica hardware è supportata con VDA per sistema operativo a sessione singola.

Le GPU AMD devono supportare RapidFire SDK. Ad esempio, le GPU AMD Radeon Pro o FirePro.

Perché la codifica funzioni correttamente, installare i driver AMD più recenti. È possibile scaricare questi driver da https://www.amd.com/en/support.

Il testo senza perdita di dati non è compatibile con la codifica hardware AMD. Se il testo senza perdita di dati è abilitato, ha la priorità sulla codifica hardware AMD.

L'uso selettivo del codec hardware H.264 per zone in continua evoluzione è supportato.

## Impostazioni dei criteri di memorizzazione nella cache

January 7, 2024

Questa sezione include le impostazioni dei criteri che consentono la memorizzazione nella cache dei dati delle immagini sui dispositivi utente quando le connessioni client dispongono di una larghezza di banda limitata.

### Persistent cache threshold (Soglia cache persistente)

**Nota**: Per Virtual Delivery Agent 7.x, questa impostazione dei criteri si applica solo quando è abilitata l'impostazione dei criteri **Legacy graphics mode** (Modalità grafica legacy).

Questa impostazione memorizza nella cache le bitmap sul disco rigido del dispositivo utente e quindi consente il riutilizzo di immagini di grandi dimensioni utilizzate frequentemente nelle sessioni precedenti.

Per impostazione predefinita, la soglia è 3.000.000 bit al secondo.

Il valore di soglia rappresenta il punto al di sotto del quale la funzionalità Persistent Cache (Cache persistente) ha effetto. Ad esempio, utilizzando il valore predefinito, le bitmap vengono memorizzate nella cache sul disco rigido del dispositivo utente quando la larghezza di banda scende al di sotto di 3.000.000 bps.

## Impostazioni dei criteri Framehawk

January 7, 2024

> **Importante:**
>
> A partire da Citrix Virtual Apps and Desktops 7 1903, Framehawk non è più supportato. Utilizzare

> invece Thinwire con il trasporto adattivo abilitato.

La sezione **Framehawk** include le impostazioni dei criteri che abilitano e configurano il canale di visualizzazione Framehawk sul server.

### Framehawk display channel (Canale di visualizzazione Framehawk)

Se l'opzione è abilitata, il server tenta di utilizzare il canale di visualizzazione Framehawk per la grafica dell'utente e la comunicazione remota di input. Questo canale di visualizzazione utilizza UDP per offrire una migliore esperienza utente sulle reti caratterizzate da perdita e latenza elevate. Tuttavia, può anche utilizzare più risorse server e larghezza di banda rispetto ad altre modalità grafiche.

Per impostazione predefinita, il canale di visualizzazione Framehawk è disabilitato.

### Framehawk display channel port range (Gamma di porte del canale di visualizzazione Framehawk)

Questa impostazione dei criteri specifica l'intervallo di numeri di porta UDP utilizzato da VDA per scambiare i dati del canale di visualizzazione Framehawk con il dispositivo utente. I numeri di porta sono nel formato *numero di porta più basso o numero di porta più alto*. Il VDA tenta di utilizzare ciascuna porta, partendo dal numero di porta più basso e incrementandolo ad ogni tentativo successivo. La porta gestisce il traffico in entrata e in uscita.

Per impostazione predefinita, l'intervallo di porte è 3224.3324.

## Impostazioni dei criteri keep-alive

January 7, 2024

La sezione **Keep Alive** contiene le impostazioni dei criteri per la gestione dei messaggi ICA keep-alive.

### ICA keep-alive timeout (Timeout ICA keep-alive)

Questa impostazione specifica il numero di secondi tra i messaggi ICA keep-alive consecutivi.

Per impostazione predefinita, l'intervallo tra i messaggi keep-alive è di 60 secondi.

Specificare un intervallo compreso tra 1 e 3600 secondi in cui inviare i messaggi ICA keep-alive. Non configurare questa impostazione se il software di monitoraggio della rete è responsabile della chiusura delle connessioni inattive.

### ICA keep-alive messages (Messaggi ICA keep-alive)

Questa impostazione abilita o disabilita l'invio periodico di messaggi ICA keep-alive.

Per impostazione predefinita, i messaggi keep-alive non vengono inviati.

L'abilitazione di questa impostazione impedisce la disconnessione delle connessioni interrotte. Se il server non rileva alcuna attività, questa impostazione impedisce a Servizi Desktop remoto di disconnettere la sessione. Il server invia messaggi keep-alive ogni pochi secondi per rilevare se la sessione è attiva. Se la sessione non è più attiva, il server contrassegna la sessione come disconnessa.

ICA keep-alive non funziona se si utilizza l'affidabilità della sessione. Configurare ICA keep-alive solo per le connessioni che non utilizzano l'affidabilità della sessione.

Impostazioni dei criteri correlate: connessioni di affidabilità della sessione.

## Impostazioni dei criteri di accesso alle app locali

January 7, 2024

La sezione **Local App Access** (Accesso alle app locali) include le impostazioni dei criteri che gestiscono le applicazioni degli utenti installate localmente con le applicazioni in hosting. Queste impostazioni dei criteri gestiscono l'integrazione in un ambiente desktop ospitato.

### Allow Local App Access (Consenti accesso alle app locali)

Questa impostazione consente o impedisce l'integrazione delle applicazioni degli utenti installate localmente con le applicazioni in hosting. Queste impostazioni dei criteri gestiscono l'integrazione in un ambiente desktop ospitato.

Quando un utente avvia un'applicazione installata localmente, tale applicazione sembra essere eseguita all'interno del proprio desktop virtuale, anche se in realtà è in esecuzione localmente.

Se si imposta l'opzione **Allow local app access** (Consenti accesso alle app locali) su **Enabled** (Abilitata), il reindirizzamento del contenuto del browser non è supportato e lo stato della batteria dell' area di notifica lato client non viene visualizzato nelle sessioni desktop.

Per impostazione predefinita, il criterio **Allow local app access** (Consenti accesso alle app locali) è vietato.

### URL redirection block list (Elenco di elementi non consentiti per il reindirizzamento URL)

Questa impostazione specifica i siti Web reindirizzati e avviati nel browser Web locale. Questi siti Web potrebbero includere:

- Siti Web che richiedono informazioni sulle impostazioni locali, come msn.com o news-google.com
- Siti Web che contengono contenuti multimediali che vengono resi meglio sul dispositivo dell'utente.

Per impostazione predefinita, non viene specificato alcun sito.

### URL redirection allow list (Elenco di elementi consentiti per il reindirizzamento URL)

Questa impostazione specifica i siti Web di cui viene eseguito il rendering nell'ambiente in cui vengono avviati.

Per impostazione predefinita, non viene specificato alcun sito.

## Impostazioni dei criteri per l'esperienza mobile

January 7, 2024

La sezione **Mobile Experience** (Esperienza mobile) include le impostazioni dei criteri per la gestione di Citrix Mobility Pack.

### Automatic keyboard display (Visualizzazione automatica della tastiera)

Questa impostazione abilita o disabilita la visualizzazione automatica della tastiera sugli schermi dei dispositivi mobili.

Per impostazione predefinita, la visualizzazione automatica della tastiera è disabilitata.

### Launch touch-optimized desktop (Avvia desktop ottimizzato per il tocco)

Questa impostazione è disabilitata e non disponibile per le macchine Windows 10 o Windows Server 2016.

Questa impostazione determina il comportamento complessivo dell'interfaccia dell'app Citrix Workspace. Questa impostazione consente o vieta un'interfaccia abilitata per il tocco ottimizzata per i dispositivi tablet.

Per impostazione predefinita, viene utilizzata un'interfaccia abilitata per il tocco.

Per utilizzare solo l'interfaccia di Windows, impostare questa impostazione dei criteri su Prohibited (Non consentita).

### Remote the combo box (Esegui in remoto la casella combinata)

Questa impostazione determina i tipi di caselle combinate che è possibile visualizzare nelle sessioni sui dispositivi mobili. Impostare questa impostazione dei criteri su Allowed (Consentita) per visualizzare il controllo relativo alla casella combinata nativa per il dispositivo. Quando questa impostazione è consentita, un utente può modificare un'impostazione di sessione dell'app Citrix Workspace per iOS per utilizzare la casella combinata di Windows.

Per impostazione predefinita, la funzione **Remote the combo box** (Esegui in remoto la casella combinata) non è consentita.

## Impostazioni dei criteri multimediali

January 7, 2024

La sezione **Multimedia** (Contenuti multimediali) include le impostazioni dei criteri per la gestione dello streaming audio e video HTML5 e Windows nelle sessioni utente.

> **Avviso**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

### Criteri multimediali

Per impostazione predefinita, tutti i criteri multimediali impostati sul Delivery Controller sono archiviati in queste chiavi del Registro di sistema:

Criteri macchina:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

Criteri utente:

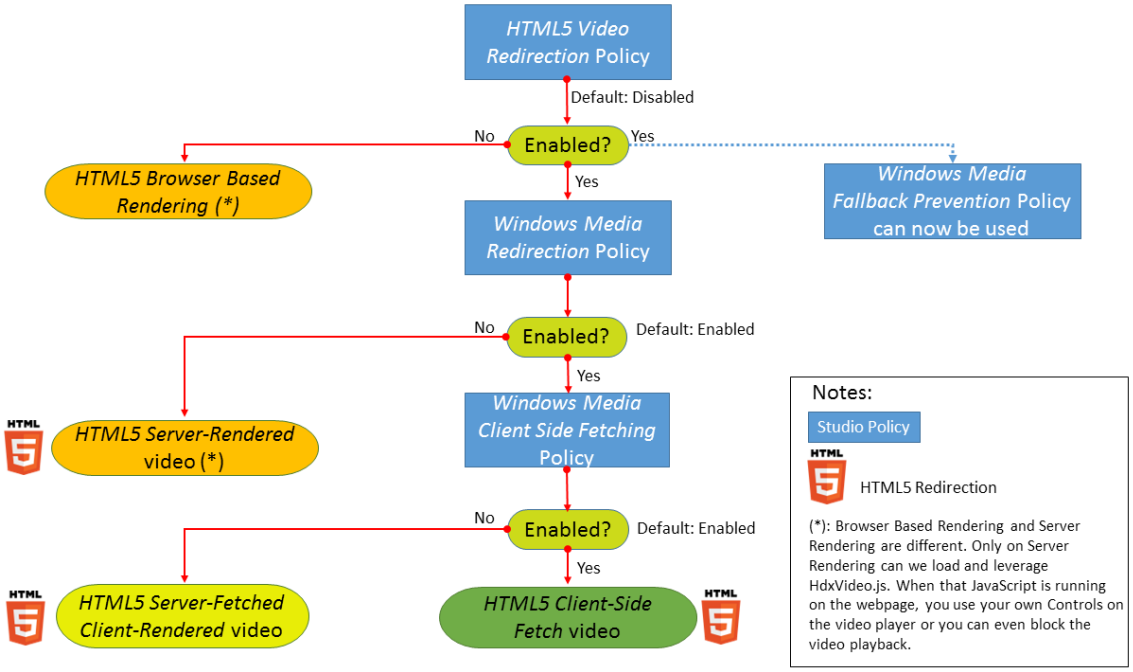
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{User Session ID}\User\MultimediaPolicies

Per individuare l'ID sessione utente corrente, eseguire il comando **qwinsta** nella riga di comando di Windows.

### HTML5 video redirection (Reindirizzamento video HTML5)

Controlla e ottimizza il modo in cui i server Citrix Virtual Apps and Desktops forniscono contenuti Web multimediali HTML5 agli utenti.

Per impostazione predefinita, questa impostazione è disabilitata.




In questa versione, questa funzionalità è disponibile solo per le pagine Web controllate. Richiede l'aggiunta di JavaScript alle pagine Web in cui è disponibile il contenuto multimediale HTML5, ad esempio video su un sito di formazione interno.

Per configurare il reindirizzamento video HTML5:

1. Copiare il file **HdxVideo.js** da %Program Files%/Citrix/ICA Service/HTML5 Video Redirection nell'installazione VDA nella posizione della pagina Web interna.
2. Inserire questa riga nella pagina Web (se la pagina Web ha altri script, includere **HdxVideo.js** prima di tali script):
   ```
   <script src="HdxVideo.js"type="text/javascript"\></script>
   ```

**Nota**: se HdxVideo.js non si trova nella stessa posizione della pagina Web, utilizzare l'attributo **src** per specificare il percorso completo.

Tenere presente che JavaScript non viene aggiunto alle pagine Web controllate e che l'utente riproduce un video HTML5. In questo caso, Citrix Virtual Apps and Desktops utilizza per impostazione predefinita il rendering lato server.

Perché il reindirizzamento dei video HTML5 funzioni, consentire il ***reindirizzamento di Windows Media***. Questo criterio è obbligatorio per Server Fetch Client Render e necessario per il recupero lato client. Il recupero lato client, a sua volta, richiede anche che *Windows Media client-side content fetching* (Recupero del contenuto lato client di Windows Media) sia impostato su Allowed.

Microsoft Edge non supporta questa funzionalità.

HdxVideo.js sostituisce i controlli del browser HTML5 Player con i propri. Per verificare che il criterio di reindirizzamento video HTML5 sia in vigore su un determinato sito Web, confrontare i controlli del lettore con uno scenario in cui il criterio di **reindirizzamento video HTML5** non è consentito:

(Controlli Citrix personalizzati quando il criterio è consentito)

(Controlli della pagina Web nativa quando il criterio non è consentito o non è configurato)


Sono supportati i seguenti controlli video:

- riproduci
- metti in pausa
- cerca
- ripeti
- audio
- schermo intero

È possibile visualizzare una pagina di test di reindirizzamento video HTML5 all'indirizzo https://www.citrix.com/virtualization/hdx/html5-redirect.html.

#### TLS, reindirizzamento video HTML5 e reindirizzamento del contenuto del browser

È possibile utilizzare il reindirizzamento video HTML5 per:

- Reindirizzare video da siti Web HTTPS
- oppure

- Reindirizzare i contenuti del browser per reindirizzare l'intero sito

Il JavaScript inserito in tali siti Web deve stabilire una connessione TLS al servizio di reindirizzamento video HTML5 Citrix HDX (WebSocketService.exe) in esecuzione sul VDA. Citrix HDX HTML5 Video Redirection Service che si trova nell'archivio certificati sul VDA genera due certificati personalizzati per:

- Ottenere il reindirizzamento video
- Mantenere l'integrità TLS della pagina Web

HdxVideo.js utilizza Secure WebSockets per comunicare con WebSocketService.exe in esecuzione sul VDA. Questo processo viene eseguito come account di sistema locale ed esegue la terminazione SSL e la mappatura delle sessioni utente.

WebSocketService.exe è in ascolto sulla porta 127.0.0.1 9001.

### Limit video quality (Limita la qualità video)

Questa impostazione si applica solo a Windows Media e non a HTML5. È necessario abilitare **l'ottimizzazione per il reindirizzamento multimediale Windows Media su WAN**.

Questa impostazione specifica il livello di qualità video massimo consentito per una connessione HDX. Una volta configurata, la qualità video massima è limitata al valore specificato, garantendo che la qualità del servizio (QoS) multimediale sia mantenuta all'interno di un ambiente.

Per impostazione predefinita, questa impostazione non è configurata.

Per limitare il livello massimo di qualità video consentito, scegliere una delle seguenti opzioni:

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

La riproduzione simultanea di più video sullo stesso server consuma grandi quantità di risorse e può influire sulla scalabilità del server.

### Microsoft Teams redirection (Reindirizzamento di Microsoft Teams)

Questa impostazione consente l'ottimizzazione di Microsoft Teams, in base alla tecnologia HDX.

Se questo criterio è abilitato e si utilizza una versione supportata dell'app Citrix Workspace, questa chiave del Registro di sistema è impostata su **1** sul VDA. L'applicazione Microsoft Teams legge la chiave da caricare in modalità VDI.
Tenere presente che non è necessario impostare manualmente la chiave del Registro di sistema.

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

Nome: MSTeamsRedirSupport

Valore: DWORD (1 - abilitato, 0 - disabilitato)

> **Nota:**
>
> Si consideri che si sta utilizzando la versione 1906.2 VDA o successiva con versioni precedenti del Controller, che non hanno il criterio disponibile in Web Studio. Un esempio di versione precedente del controller è la versione 7.15. In questo caso, l'ottimizzazione HDX è abilitata per impostazione predefinita sul VDA. Se la versione dell'app Workspace è 1907 o successiva, Microsoft Teams viene avviato in modalità ottimizzata. Per informazioni sugli aspetti negativi dell'utilizzo in contemporanea di controller LTSR 7.15 e VDA CR, vedere l'articolo del Knowledge Center CTX205549.
>
> In questo caso, per disabilitare la funzione per utenti specifici, è possibile ignorare l'impostazione del Registro di sistema. Ignorare le impostazioni del Registro di sistema utilizzando un criterio di gruppo per applicare uno script di accesso all'unità organizzativa dell'utente.

Per impostazione predefinita, il reindirizzamento di Microsoft Teams è abilitato.

### Multimedia conferencing (Conferenze multimediali)

Questa impostazione consente o impedisce l'uso di una tecnologia di reindirizzamento della webcam ottimizzata da parte delle applicazioni di videoconferenza.

Per impostazione predefinita, il supporto per le videoconferenze è abilitato.

Quando si aggiunge questa impostazione a un criterio, verificare che l'impostazione **Windows Media redirection**(Reindirizzamento di Windows Media) sia presente e impostata su **Allowed** (l'impostazione predefinita).

Quando si conducono **conferenze multimediali**, verificare che siano soddisfatte le seguenti condizioni:

- I driver forniti dal produttore per la webcam utilizzata per le conferenze multimediali sono installati sul client.
- Collegare la webcam al dispositivo utente prima di avviare una sessione di videoconferenza. Il server utilizza una sola webcam installata alla volta. Se sul dispositivo utente sono installate più webcam, il server tenta di utilizzare ogni webcam in successione. Questo tentativo continua fino a quando non viene creata correttamente una sessione di videoconferenza.

Questo criterio non è necessario per il reindirizzamento della webcam utilizzando il reindirizzamento USB generico. In tal caso, installare i driver della webcam sul VDA.

### Optimization for Windows Media multimedia redirection over WAN (Ottimizzazione per il reindirizzamento multimediale Windows Media su WAN)

Questa impostazione si applica solo a Windows Media e non a HTML5. L'impostazione consente quanto segue:

- Transcodifica multimediale in tempo reale
- Streaming di contenuti multimediali audio e video su dispositivi mobili su reti degradate
- Migliore esperienza utente grazie al miglioramento del modo in cui i contenuti Windows Media vengono distribuiti su una WAN.

Per impostazione predefinita, la distribuzione di contenuti Windows Media tramite WAN è ottimizzata.

Quando si aggiunge questa impostazione a un criterio, assicurarsi che l'impostazione **Windows Media Redirection** (Reindirizzamento Windows Media) sia presente e impostata su **Allowed** (Consentito).

Quando questa impostazione è abilitata, la transcodifica multimediale in tempo reale viene implementata automaticamente come necessario per abilitare lo streaming multimediale. Inoltre, fornisce un'esperienza utente senza interruzioni anche in condizioni di rete estreme.

### Use GPU for optimizing Windows Media multimedia redirection over WAN (Utilizza la GPU per ottimizzare il reindirizzamento multimediale di Windows Media su WAN)

Questa impostazione si applica solo a Windows Media e consente la transcodificazione multimediale in tempo reale nell'unità di elaborazione grafica (GPU) sul Virtual Delivery Agent (VDA). Migliora la scalabilità del server. La transcodificazione GPU è disponibile solo se il VDA ha una GPU supportata per l'accelerazione hardware. In caso contrario, la transcodificazione torna alla CPU.

**Nota:** la transcodificazione GPU è supportata solo su GPU NVIDIA.

Per impostazione predefinita, non è consentito utilizzare la GPU sul VDA per ottimizzare la distribuzione di contenuti Windows Media sulla WAN.

Quando si aggiunge questa impostazione a un criterio, assicurarsi che le seguenti impostazioni siano presenti e impostate su Allowed:

- **Reindirizzamento di Windows Media**
- **Optimization for Windows Media multimedia redirection over WAN (Ottimizzazione per il reindirizzamento multimediale Windows Media su WAN)**

### Windows Media fallback prevention (Prevenzione del fallback di Windows Media)

Questa impostazione si applica al reindirizzamento del contenuto del browser, HTML5 e Windows Media. Per supportare HTML5, impostare il criterio **HTML5 video redirection** (Reindirizzamento video HTML5) su **Allowed** (Consentito).

Gli amministratori possono utilizzare l'impostazione **Windows Media fallback prevention** (Prevenzione del fallback di Windows Media) per specificare i metodi che si tentano di utilizzare per distribuire contenuto in streaming agli utenti.

Per impostazione predefinita, questa impostazione non è configurata. Quando l'impostazione è impostata su Not Configured (Non configurata), il comportamento è lo stesso di **Play all content** (Riproduci tutto il contenuto).

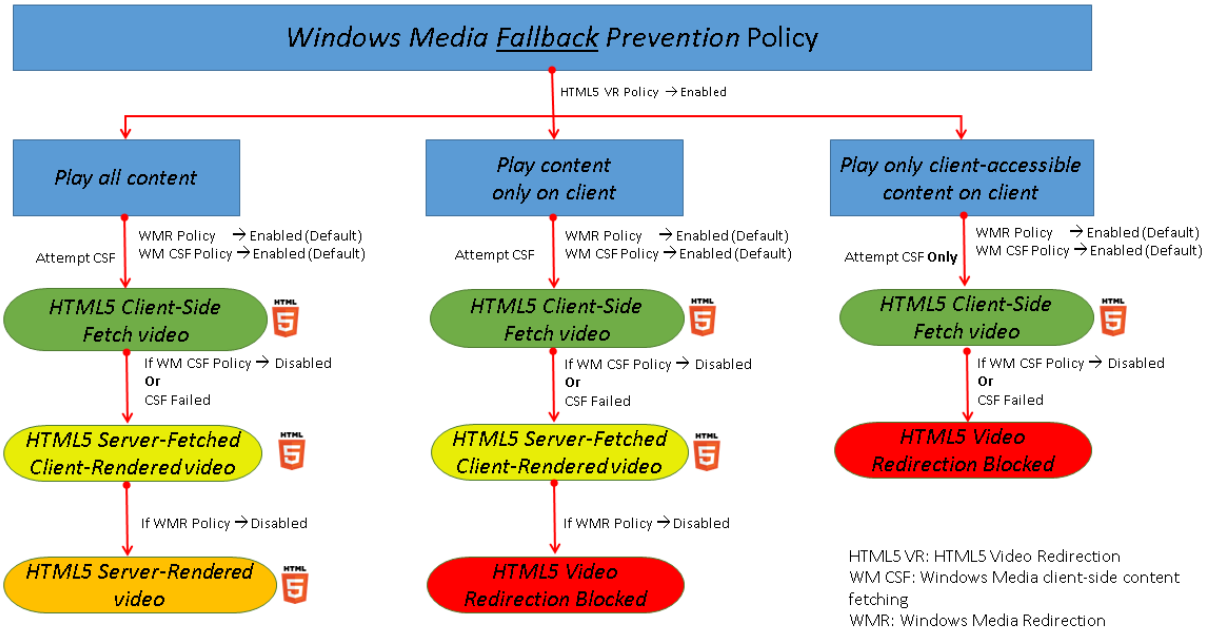
Per configurare questa impostazione, scegliere una delle seguenti opzioni:

- **Play all content** (Riproduci tutto il contenuto). Tentare il recupero del contenuto sul lato client, seguito dal reindirizzamento di Windows Media. Se l'operazione non va a buon fine, riprodurre il contenuto sul server.
- **Play all content only on client** (Riproduci tutto il contenuto solo sul client). Tentare il recupero sul lato client, seguito dal reindirizzamento di Windows Media. Se l'operazione non va a buon fine, il contenuto non viene riprodotto.
- **Play only client-accessible content on client** (Riproduci solo contenuti accessibili dal client sul client). Tentare il recupero solo sul lato client. Se l'operazione non va a buon fine, il contenuto non viene riprodotto.

Quando il contenuto non viene riprodotto, viene visualizzato il seguente messaggio di errore nella finestra del lettore (per una durata predefinita di 5 secondi):

```
"Company has blocked video because of lack of resources"
```




La durata di questo messaggio di errore può essere personalizzata con la seguente chiave del Registro di sistema sul VDA. Se la voce del Registro di sistema non esiste, la durata predefinita è 5 secondi.

Il percorso del Registro di sistema varia a seconda dell'architettura del VDA:

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

oppure

\HKLM\SOFTWARE\Citrix\HdxMediastream

Chiave di registro:

Nome: VideoLoadManagementErrDuration

Tipo: DWORD

Intervallo: 1 - fino al limite DWORD (impostazione predefinita = 5)

Unità: secondi

### Windows Media client-side content fetching (Recupero del contenuto sul lato client di Windows Media)

Questa impostazione si applica sia ad HTML5 che a Windows Media. Questa impostazione consente a un dispositivo utente di trasmettere in streaming file multimediali direttamente dal provider di origine su Internet o intranet, anziché tramite il server host XenApp o XenDesktop.

L'impostazione predefinita è **Allowed**. Consentire questa impostazione migliora l'utilizzo della rete e la scalabilità del server. Questo miglioramento si ottiene spostando qualsiasi elaborazione che

avviene sul supporto dal server host al dispositivo dell'utente. Elimina inoltre il requisito che un framework multimediale avanzato come Microsoft DirectShow o Media Foundation sia installato sul dispositivo utente. The user device requires only the ability to play a file from a URL (Il dispositivo utente richiede solo la possibilità di riprodurre un file da un URL)

Quando si aggiunge questa impostazione a un criterio, assicurarsi che l'impostazione **Windows Media Redirection** (Reindirizzamento Windows Media) sia presente e impostata su **Allowed** (Consentito). Se il criterio **Windows Media Redirection** (Reindirizzamento di Windows Media) è disabilitato, viene disabilitato anche lo streaming di file multimediali al dispositivo utente direttamente dal provider di origine.

### Reindirizzamento di Windows Media

Questa impostazione si applica sia a HTML5 che a Windows Media e controlla e ottimizza il modo in cui i server distribuiscono audio e video in streaming agli utenti.

L'impostazione predefinita è **Allowed**. Per HTML5, questa impostazione non ha effetto se il criterio **HTML5 video redirection** (Reindirizzamento video HTML5) è impostato su **Prohibited** (Non consentito).

Quando questa impostazione aumenta la qualità dell'audio e del video provenienti dal server a un livello comparabile con l'audio e il video riprodotti localmente su un dispositivo utente. Il server trasmette contenuti multimediali al client nella forma originale compressa e consente al dispositivo utente di decomprimerli ed eseguirne il rendering.

Il reindirizzamento di Windows Media ottimizza i file multimediali codificati con codec conformi agli standard Microsoft DirectShow, DirectX Media Objects (DMO) e Media Foundation. Per riprodurre un determinato file multimediale, sul dispositivo dell'utente deve essere presente un codec compatibile con il formato di codifica del file multimediale.

Per impostazione predefinita, l'audio è disabilitato nell'app Citrix Workspace. Per consentire agli utenti di eseguire applicazioni multimediali nelle sessioni ICA, attivare l'audio o concedere agli utenti l'autorizzazione ad attivare l'audio nell'interfaccia dell'app Citrix Workspace.

Selezionare **Prohibited** (Non consentito) solo se la riproduzione di contenuti multimediali utilizzando il reindirizzamento di Windows Media risulta peggiore rispetto a quando viene eseguito il rendering utilizzando la compressione ICA di base e l'audio normale. Questa situazione è rara, ma può verificarsi in condizioni di larghezza di banda ridotta, ad esempio con contenuti multimediali con una bassa frequenza di fotogrammi chiave.

### Windows Media Redirection buffer size (Dimensione del buffer di reindirizzamento di Windows Media)

Questa impostazione è legacy e non si applica ad HTML5.

Questa impostazione specifica una dimensione del buffer da 1 a 10 secondi per l'accelerazione multimediale.

Per impostazione predefinita, la dimensione del buffer è di 5 secondi.

### Windows Media Redirection buffer size use (Utilizzo delle dimensioni del buffer di reindirizzamento di Windows Media)

Questa impostazione è legacy e non si applica ad HTML5.

Questa impostazione esegue l'abilitazione o la disabilitazione utilizzando la dimensione del buffer specificata nell'impostazione **Windows Media Redirection buffer size** (Dimensione buffer di reindirizzamento di Windows Media).

Per impostazione predefinita, la dimensione del buffer specificata non viene utilizzata.

Se questa impostazione è disabilitata o se l'impostazione **Windows Media Redirection buffer size** (Dimensione del buffer di reindirizzamento di Windows Media) non è configurata, il server utilizza il valore predefinito della dimensione del buffer (cinque secondi).

## Impostazioni dei criteri delle connessioni multi-flusso

January 7, 2024

La sezione **Multi-Stream connections** (Connessioni multi-flusso) include le impostazioni dei criteri per la gestione delle priorità della qualità del servizio per più connessioni ICA in una sessione.

> **Nota:**
>
> Il rilevamento MTU non è supportato se il criterio per le connessioni multi-flusso è abilitato.

### Audio over UDP (Audio su UDP)

Questa impostazione consente o impedisce l'audio su UDP sul server.

Per impostazione predefinita, l'audio su UDP è consentito sul server.

Se abilitata, questa impostazione apre una porta UDP sul server per supportare tutte le connessioni configurate per l'utilizzo del trasporto in tempo reale dell'audio su UDP.

### Audio UDP port range (Intervallo di porte UDP audio)

Questa impostazione specifica l'intervallo di numeri di porta (numero di porta più basso, numero di porta più alto) utilizzato da Virtual Delivery Agent (VDA). In questo modo aiuta a scambiare dati di pacchetti audio con il dispositivo dell'utente. Il VDA tenta di utilizzare ogni coppia di porte UDP per scambiare dati con il dispositivo utente, iniziando dal più basso e incrementando di due per ogni tentativo successivo. Ogni porta gestisce sia il traffico in entrata che in uscita.

Per impostazione predefinita, questo intervallo è impostato su 16500,16509.

### Multi-Port policy (Criterio multi-porta)

Questa impostazione specifica le porte TCP da utilizzare per il traffico ICA e stabilisce la priorità di rete per ciascuna porta.

Per impostazione predefinita, la porta primaria (2598) ha una priorità alta.

Quando si configurano le porte, è possibile assegnare le seguenti priorità:

- **Very High** (Molto alta): per attività in tempo reale, come le conferenze con webcam
- **High** (Alta): per elementi interattivi, come schermo, tastiera e mouse
- **Medium** (Media): per le procedure in blocco, ad esempio la mappatura delle unità client
- **Low** (Bassa): per attività in background, come la stampa

Ogni porta deve avere una priorità univoca. Ad esempio, non è possibile assegnare una priorità molto alta sia alla porta CGP 1 che alla porta CGP 3.

Per rimuovere una porta dall'elenco di priorità, impostare il numero di porta su 0. Non è possibile rimuovere la porta primaria e modificarne il livello di priorità.

Quando si configura questa impostazione, riavviare il server. Questa impostazione ha effetto solo quando è abilitata l'impostazione dei criteri **Multi-Stream computer** (Computer multi-stream).

### Impostazione Multi-Stream computer (Computer multi-flusso)

Questa impostazione abilita o disabilita il multi-flusso sul server.

Per impostazione predefinita, il multi-flusso è disabilitato. Configurare l'impostazione dei criteri Multi-Stream computer (Computer multi-flusso) se si utilizzano Citrix SD-WAN o router di terze parti per ottenere la qualità del servizio desiderata.

Se il multi-flusso è abilitato, il rilevamento MTU, una funzionalità del trasporto adattivo, non è supportato.

Quando si configura questa impostazione, riavviare il server per assicurarsi che le modifiche abbiano effetto.

> **Importante:**
>
> l'utilizzo di questa impostazione dei criteri con impostazioni dei criteri relative al limite della larghezza di banda, ad esempio Overall session bandwidth limit (Limite complessivo della larghezza di banda), potrebbe generare risultati imprevisti. Quando si include questa impostazione in un criterio, assicurarsi che le impostazioni del limite di larghezza di banda non siano incluse.

### Impostazione Multi-Stream user (Utente multi-flusso)

Questa impostazione abilita o disabilita il multi-flusso sul dispositivo utente.

Per impostazione predefinita, il multi-flusso è disabilitato per tutti gli utenti. Configurare l'impostazione Multi-Stream user (Utente multi-flusso) se si utilizzano Citrix SD-WAN o router di terze parti per ottenere la qualità del servizio desiderata.

Questa impostazione ha effetto solo sugli host in cui è abilitata l'impostazione dei criteri **Multi-Stream computer** (Computer multi-flusso).

> **Importante:**
>
> l'utilizzo di questa impostazione dei criteri con impostazioni dei criteri relative al limite della larghezza di banda, ad esempio Overall session bandwidth limit (Limite complessivo della larghezza di banda), potrebbe generare risultati imprevisti. Quando si include questa impostazione in un criterio, assicurarsi che le impostazioni del limite di larghezza di banda non siano incluse.

### Impostazioni Multi-Stream virtual channel assignment (Assegnazione del canale virtuale multi-flusso)

Questa impostazione specifica il flusso ICA a cui vengono assegnati i canali virtuali quando viene utilizzato il multi-flusso.

Se non si configurano queste impostazioni, i canali virtuali vengono mantenuti nel loro flusso predefinito. Per assegnare un canale virtuale a un flusso ICA, selezionare il numero di flusso desiderato (0, 1, 2, 3) dall'elenco **Stream number** (Numero flusso) accanto al nome del canale virtuale.

Se nell'ambiente è presente un canale virtuale personalizzato, fare clic su **Add** (Aggiungi), specificare il nome del canale virtuale nella casella di testo in **Virtual Channels** (Canali virtuali) e selezionare il numero di flusso desiderato dall'elenco **Stream Number** (Numero flusso) a fianco. Il nome specificato deve essere il nome effettivo del canale virtuale e non un nome descrittivo. Ad esempio, CTXSBR invece di Citrix Browser Acceleration.

Queste impostazioni hanno effetto solo quando è stata abilitata l'impostazione Multi-Stream computer (Computer multi-flusso).

Per impostazione predefinita, i canali virtuali e le relative assegnazioni di flusso sono:

- AppFlow: 2
- Audio: 0
- Reindirizzamento del contenuto del browser: 2
- Mappatura porta COM client: 3
- Mappatura unità client: 2
- Mappatura stampante client: 3
- Appunti: 2
- CTXDND: 1 (**Nota:** questo supporta il trascinamento e il rilascio di file tra una sessione Citrix e un endpoint locale)
- Plug-in DVC (nome VC statico generato automaticamente dal nome descrittivo del plug-in DVC o assegnato dall'amministratore): 2
- Monitoraggio dell'esperienza utente finale: 1
- Trasferimento file (ricevitore HTML5): 2
- Trasferimento dati generico: 2
- Controllo ICA: 1
- Editor dei metodi di input: 1
- Mappatura stampante client legacy (COM1): 1, 3
- Mappatura stampante client legacy (COM2): 2, 3
- Mappatura stampante client legacy (LPT1): 1, 3
- Mappatura stampante client legacy (LPT2): 2, 3
- Gestione delle licenze: 1
- Reindirizzamento di Microsoft Teams/WebRTC: 1
- Ricevitore mobile: 1
- MultiTouch: 1
- Inoltro porta: 2
- Estensioni audio e video remote (RAVE): 2
- Senza soluzione di continuità (integrazione con finestra trasparente): 1
- Sensore e posizione: 1
- Smart Card: 1
- Scheda grafica Thinwire: 1
- Integrazione interfaccia utente trasparente/stato di accesso: 2
- Reindirizzamento TWAIN: 2
- USB: 2
- Carattere e tastiera a latenza zero: 2
- Canale dati a latenza zero: 2

Per ulteriori informazioni sulle assegnazioni e sulle priorità dei canali virtuali, vedere l'articolo del Knowledge Center CTX131001.

## Impostazioni dei criteri di reindirizzamento delle porte

January 7, 2024

La sezione **Port Redirection** (Reindirizzamento porta) contiene le impostazioni dei criteri per la mappatura delle porte LPT e COM client.

Per le versioni di Virtual Delivery Agent **precedenti alla 7.0**, utilizzare le seguenti impostazioni dei criteri per configurare il reindirizzamento delle porte. Per le versioni di VDA da **7.0 a 7.8**, configurare queste impostazioni utilizzando il Registro di sistema; vedere Configurare le impostazioni di reindirizzamento delle porte COM e LPT utilizzando il Registro di sistema. Per i VDA versione **7.9**, utilizzare le impostazioni dei criteri seguenti.

### Auto connect client COM ports (Collegamento automatico delle porte COM client)

Questa impostazione abilita o disabilita la connessione automatica delle porte COM sui dispositivi utente quando gli utenti accedono a un sito.

Per impostazione predefinita, le porte COM client non sono collegate automaticamente.

### Auto connect client LPT ports (Collegamento automatico delle porte LPT client)

Questa impostazione abilita o disabilita la connessione automatica delle porte LPT sui dispositivi utente quando gli utenti accedono a un sito.

Per impostazione predefinita, le porte LPT client non vengono collegate automaticamente.

### Client COM port redirection (Reindirizzamento porta COM client)

Questa impostazione consente o impedisce l'accesso alle porte COM sul dispositivo utente.

Per impostazione predefinita, il reindirizzamento delle porte COM non è consentito.

Le seguenti impostazioni dei criteri sono correlate:

- COM port redirection bandwidth limit (Limite della larghezza di banda di reindirizzamento della porta COM)
- COM port redirection bandwidth limit percent (Percentuale del limite della larghezza di banda di reindirizzamento della porta COM)

### Client LPT port redirection (Reindirizzamento porta LPT client)

Questa impostazione consente o impedisce l'accesso alle porte LPT sul dispositivo utente.

Per impostazione predefinita, il reindirizzamento delle porte LPT non è consentito.

Le porte LPT vengono utilizzate solo da applicazioni legacy che inviano processi di stampa alle porte LPT. Queste porte non sono utilizzate da applicazioni legacy che inviano lavori di stampa agli oggetti di stampa sul dispositivo dell'utente. La maggior parte delle applicazioni oggi può inviare processi di stampa agli oggetti della stampante. Questa impostazione dei criteri è necessaria solo per i server che ospitano applicazioni legacy che stampano su porte LPT.

Tenere presente che, sebbene il reindirizzamento della porta COM client sia bidirezionale, il reindirizzamento della porta LPT è solo output ed è limitato a \\client\LPT1 e \\client\LPT2 all'interno di una sessione ICA.

Le seguenti impostazioni dei criteri sono correlate:

- LPT port redirection bandwidth limit (Limite della larghezza di banda per il reindirizzamento della porta LPT)
- LPT port redirection bandwidth limit percent (Percentuale del limite della larghezza di banda per il reindirizzamento della porta LPT)

## Impostazioni dei criteri di stampa

January 7, 2024

La sezione Printing (Stampa) contiene le impostazioni dei criteri per la gestione della stampa client.

### Client printer redirection (Reindirizzamento stampanti client)

Questa impostazione controlla se le stampanti client vengono mappate a un server quando un utente accede a una sessione.

Per impostazione predefinita, la mappautra delle stampanti client è consentita. Se questa impostazione è disabilitata, la stampante PDF per la sessione non viene creata automaticamente.

Impostazioni dei criteri correlati: creazione automatica delle stampanti client

### Default printer (Stampante predefinita)

Questa impostazione specifica il modo in cui la stampante predefinita sul dispositivo utente viene stabilita in una sessione.

Per impostazione predefinita, la stampante corrente dell'utente viene utilizzata come stampante predefinita per la sessione.

Per utilizzare l'impostazione corrente di Servizi Desktop remoto o del profilo utente di Windows per la stampante predefinita, selezionare Do not adjust the user's default printer (Non regolare la stampante predefinita dell'utente). Se si sceglie questa opzione, la stampante predefinita non viene salvata nel profilo e non cambia in base ad altre proprietà della sessione o del client. La stampante predefinita in una sessione è la prima stampante creata automaticamente nella sessione, ovvero:

- La prima stampante aggiunta localmente al server Windows in **Pannello di controllo > Dispositivi** e **stampanti**.
- La prima stampante creata automaticamente, se non sono presenti stampanti aggiunte localmente al server.

È possibile utilizzare questa opzione per presentare agli utenti la stampante più vicina tramite le impostazioni del profilo (questa procedura è detta "stampa di prossimità").

### Printer assignments (Assegnazioni stampante)

Questa impostazione fornisce un'alternativa alle impostazioni Default printer (Stampante predefinita) e Session printers (Stampanti di sessione). Utilizzare le singole impostazioni Default printer (Stampante predefinita) e Session printers (Stampanti di sessione) per configurare i comportamenti per un sito, un gruppo di grandi dimensioni o un'unità organizzativa. Utilizzare l'impostazione **Printer assignments** (Assegnazioni stampante) per assegnare un grande gruppo di stampanti a più utenti.

Questa impostazione specifica il modo in cui la stampante predefinita sui dispositivi utente elencati viene stabilita in una sessione.

Per impostazione predefinita, la stampante corrente dell'utente viene utilizzata come stampante predefinita per la sessione.

Specifica inoltre le stampanti di rete da creare automaticamente in una sessione per ogni dispositivo utente. Per impostazione predefinita, non viene specificata alcuna stampante.

- Quando si imposta il valore predefinito della stampante:

  Per utilizzare la stampante predefinita corrente per il dispositivo utente, selezionare Do not adjust (Non regolare).

  Per utilizzare l'impostazione corrente di Servizi Desktop remoto o del profilo utente di Windows per la stampante predefinita, selezionare Do not adjust (Non regolare). Se si sceglie questa opzione, la stampante predefinita non viene salvata nel profilo e non cambia in base ad altre proprietà della sessione o del client. La stampante predefinita in una sessione è la prima stampante creata automaticamente nella sessione, ovvero:

  - La prima stampante aggiunta localmente al server Windows in **Pannello di controllo > Dispositivi** e stampanti.
  - La prima stampante creata automaticamente, se non sono presenti stampanti aggiunte localmente al server.

- Quando si imposta il valore delle stampanti di sessione: per aggiungere stampanti, digitare il percorso UNC della stampante che si desidera creare automaticamente. Dopo aver aggiunto la stampante, è possibile applicare impostazioni personalizzate per la sessione corrente a ogni accesso.

### Printer auto-creation event log preference (Preferenza registro eventi per la creazione automatica della stampante)

Questa impostazione specifica gli eventi registrati durante il processo di creazione automatica della stampante. È possibile scegliere di non registrare errori o avvisi, solo errori o errori e avvisi.

Per impostazione predefinita, vengono registrati errori e avvisi.

Un esempio di avviso è un evento in cui non è possibile installare il driver nativo di una stampante e viene installato il driver di stampa universale. Per utilizzare il driver di stampa universale in questo scenario, configurare l'impostazione Universal print driver usage (Utilizzo driver di stampa universale) su Use universal printing only (Utilizza solo stampa universale) o Use universal printing only if the requested driver is unavailable (Usa stampa universale solo se il driver richiesto non è disponibile).

### Session printers (Stampanti di sessione)

Questa impostazione specifica le stampanti di rete da creare automaticamente in una sessione. All'interno della sessione ICA/HDX, il servizio Citrix Print Manager (CpSvc.exe) crea una connessione alla stampante di rete durante l'accesso alla sessione per ogni stampante di rete specificata nell'impostazione dei criteri **Session Printer** (Stampante di sessione). Elimina le stampanti durante lo scollegamento della sessione. Per impostazione predefinita, non viene specificata alcuna stampante.

Nell'impostazione dei criteri **Session Printer** (Stampante di sessione), le stampanti di rete possono risiedere in un server di stampa Windows o un server di stampa universale Citrix.

- **Server di stampa Windows:** condivide una o più stampanti di rete. Dispone inoltre dei driver della stampante nativi necessari per utilizzare le stampanti di rete.
- **Server di stampa universale:** un server di stampa Windows in cui è stato installato il software Citrix Universal Print Server.

Quando si utilizza un server di stampa Windows, il servizio Citrix Print Manager crea le connessioni della stampante di rete utilizzando i driver della stampante nativi. Sul server Citrix Virtual Apps devono essere installati i driver della stampante nativi.

Quando si utilizza un server di stampa universale Citrix, il servizio Citrix Print Manager crea le connessioni della stampante di rete utilizzando driver di stampante nativi, il driver della stampante universale Citrix o il driver della stampante XPS universale Citrix. Il driver utilizzato è controllato dall'impostazione dei criteri di utilizzo del driver di stampa universale.

Tutti i driver della stampante Windows sono attualmente inclusi nella versione del driver v3 o v4. Per ulteriori informazioni, vedere Supporto per le architetture del driver della stampante Microsoft V3 e V4.

Per aggiungere stampanti di sessione e verificare se vengono visualizzate nelle sessioni, attenersi alla procedura seguente:

1. Accedere a Web Studio, selezionare **Policies** nel riquadro a sinistra, quindi fare clic sulla scheda **Policies**.
2. Abilita il criterio **Session printers** (Stampanti di sessione).
3. Nel criterio, aggiungere la stampante di sessione. Per aggiungere stampanti, digitare il percorso UNC della stampante che si desidera creare automaticamente. Dopo aver aggiunto la stampante, è possibile applicare impostazioni personalizzate per la sessione corrente a ogni accesso. La stampante di sessione deve essere visualizzata nell'elenco.
4. Dopo aver impostato il criterio, l'applicazione pubblicata potrebbe non visualizzare le stampanti di sessione. Questo problema può verificarsi perché il driver della stampante è mancante nel server Citrix Virtual Apps o il criterio è stato creato ma non abilitato.

   > **Nota:**
   >
   > Se una stampante di sessione necessita di un driver della stampante nativo e il driver della stampante nativo non è installato sul VDA, è possibile che la stampante di sessione non venga creata nella sessione.

5. Avviare il desktop pubblicato e aggiungere manualmente la stampante di sessione in **Pannello di controllo > Dispositivi e stampanti**.
6. In caso contrario, esaminare la comunicazione tra il server Citrix Virtual Apps e il server di stampa. Prendere in considerazione l'esecuzione di un test con RDP.

### Wait for printers to be created (Attendi la creazione di stampanti)

Utilizzare il criterio sul Delivery Controller per abilitare la funzionalità in Citrix Virtual Desktops.

**Wait for printers to be created (Server Desktop):** (Attendi la creazione delle stampanti (Server Desktop))

Questa impostazione consente un ritardo nella connessione a una sessione in modo che le stampanti reindirizzate dal client possano essere create automaticamente.

Per impostazione predefinita, non si verifica un ritardo di connessione.

**Wait for printers to be created (Citrix Virtual Apps):** (Attendi la creazione delle stampanti (Citrix Virtual Apps))

L'esecuzione del seguente cmdlet PowerShell consente un ritardo nella connessione alle app virtuali in esecuzione su host multisessione in modo che le stampanti reindirizzate dal client possano essere create automaticamente prima dell'apertura dell'applicazione.

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation
$true
```

Per impostazione predefinita, non si verifica un ritardo di connessione.

## Impostazioni dei criteri delle stampanti client

January 10, 2024

La sezione **Client Printers** (Stampanti client) include le impostazioni dei criteri per le stampanti client, incluse le impostazioni per la creazione automatica delle stampanti client, la conservazione delle proprietà della stampante e la connessione ai server di stampa.

### Auto-create client printers (Creazione automatica delle stampanti client)

Questa impostazione specifica le stampanti client create automaticamente. Questa impostazione sostituisce le impostazioni predefinite per la creazione automatica delle stampanti client.

Per impostazione predefinita, tutte le stampanti client vengono create automaticamente.

Questa impostazione ha effetto solo se l'impostazione **Client printer redirection** (Reindirizzamento della stampante client) è presente ed è impostata su **Allowed** (Consentito).

Quando si aggiunge questa impostazione a un criterio, selezionare un'opzione:

- L'opzione **Auto-create all client printers** (Crea automaticamente tutte le stampanti client) crea automaticamente tutte le stampanti su un dispositivo utente.
- L'opzione **Auto-create the client's default printer only** (Crea automaticamente solo la stampante predefinita del client) crea solo la stampante selezionata come stampante predefinita sul dispositivo dell'utente.

- L'opzione **Auto-create local (non-network) client printers only** (Crea automaticamente solo le stampanti clienti (non di rete)) crea solo le stampanti collegate direttamente al dispositivo utente tramite una porta LPT, COM, USB, TCP/IP o un'altra porta locale.
- L'opzione **Do non auto-create client printers** (Non creare automaticamente stampanti client) disabilita la creazione automatica per tutte le stampanti client quando gli utenti accedono. Se si sceglie questa opzione, le impostazioni di Servizi Desktop remoto (RDS) per la creazione automatica delle stampanti client sostituiscono questa impostazione nei criteri con priorità inferiore.

### Auto-create generic universal printer (Crea automaticamente la stampante universale generica)

Questa impostazione abilita o disabilita la creazione automatica dell'oggetto generico Citrix Universal Printer per le sessioni. Queste sessioni includono solo le sessioni in cui è in uso un dispositivo utente compatibile con Universal Printing.

Per impostazione predefinita, l'oggetto Universal Printer generico non viene creato automaticamente.

Le seguenti impostazioni dei criteri sono correlate:

- Universal print driver usage (Utilizzo del driver della stampante universale)
- Universal driver preference (Preferenza driver universale)

### Auto-create PDF universal printer (Creazione automatica della stampante universale PDF)

Questa impostazione abilita o disabilita la creazione automatica della stampante Citrix PDF per le sessioni che utilizzano:

- App Citrix Workspace per Windows (a partire da VDA 7.19)
- App Citrix Workspace per HTML5
- App Citrix Workspace per Chrome

Per impostazione predefinita, la stampante PDF Citrix non viene creata automaticamente.

### Nomi delle stampanti client

Questa impostazione seleziona la convenzione di denominazione per le stampanti client create automaticamente.

Per impostazione predefinita, vengono utilizzati nomi di stampanti standard.

Selezionare **Standard printer names** (Nomi stampanti standard) per utilizzare nomi delle stampanti come "HPLaserJet 4 dal nome del client nella sessione 3".

Selezionare **Legacy printer names** (Nomi stampanti legacy) per utilizzare i nomi delle stampanti client vecchio stile e per mantenere la compatibilità con le versioni precedenti con i nomi delle stampanti legacy presenti nelle versioni XenApp e XenDesktop del prodotto. È possibile utilizzare questa opzione con le attuali versioni Citrix Virtual Apps and Desktops del prodotto. Un esempio di nome stampante legacy è "Client/nomeclient#/HPLaserJet 4". Questa opzione è meno sicura.

Quando si utilizza la stampante PDF Citrix in una sessione avviata dall'app Citrix Workspace per HTML5, impostare **Clienti printer names** (Nomi stampanti client) come opzione predefinita o selezionare **Standard printer names** (Nomi stampanti standard). Se si seleziona **Legacy printer names** (Nomi stampanti legacy), l'app Citrix Workspace per HTML5 non supporta l'opzione Citrix PDF Printer (Stampante PDF Citrix).

### Direct connections to print servers (Connessioni dirette ai server di stampa)

Questa impostazione abilita o disabilita le connessioni dirette dalle applicazioni che ospitano desktop virtuali o server a un server di stampa per stampanti client. Qui, le stampanti client sono ospitate su una condivisione di rete accessibile.

Per impostazione predefinita, le connessioni dirette sono abilitate.

Abilitare le connessioni dirette se il server di stampa di rete non si trova su una rete WAN dalle applicazioni che ospitano desktop virtuali o server. La comunicazione diretta comporta una stampa più rapida se il server di stampa di rete e le applicazioni che ospitano desktop virtuali o server si trovano sulla stessa LAN.

Disabilitare le connessioni dirette se la rete si trova su una WAN o ha una latenza sostanziale o una larghezza di banda limitata. I processi di stampa vengono instradati attraverso il dispositivo utente in cui vengono reindirizzati al server di stampa di rete. I dati inviati al dispositivo utente vengono compressi, quindi viene consumata meno larghezza di banda quando i dati viaggiano attraverso la WAN.

Se due stampanti di rete hanno lo stesso nome, viene utilizzata la stampante sulla stessa rete del dispositivo utente.

### Printer driver mapping and compatibility (Mappatura e compatibilità dei driver della stampante)

Questa impostazione specifica le regole di sostituzione dei driver per le stampanti client create automaticamente.

Questa impostazione è configurata per escludere Microsoft OneNote e XPS Document Writer dall'elenco delle stampanti client create automaticamente.

Quando si definiscono le regole di sostituzione dei driver, è possibile consentire o impedire la creazione di stampanti con il driver specificato. Inoltre, è possibile consentire alle stampanti create di utilizzare solo driver di stampa universali. La sostituzione dei driver sostituisce o mappa i nomi dei driver della stampante forniti dal dispositivo utente, sostituendo un driver equivalente sul server. Queste regole offrono alle applicazioni server l'accesso alle stampanti client con gli stessi driver del server, ma nomi di driver diversi.

È possibile procedere come segue:

- Aggiungere una mappatura dei driver
- Modificare una mappatura esistente
- Sostituire le impostazioni personalizzate di una mappatura
- Rimuovere una mappatura
- Modificare l'ordine delle voci dei driver nell'elenco

Quando si aggiunge una mappatura, immettere il nome del driver della stampante client e quindi selezionare il driver del server che si desidera sostituire.

### Printer properties retention (Conservazione delle proprietà della stampante)

Questa impostazione specifica se memorizzare le proprietà della stampante e dove memorizzarle.

Per impostazione predefinita, il sistema determina se le proprietà della stampante sono memorizzate sul dispositivo utente, se disponibile, o nel profilo utente.

Quando si aggiunge questa impostazione a un criterio, selezionare un'opzione:

- L'opzione Saved on the client device only (Salvate solo sul dispositivo client) si applica ai dispositivi utente che dispongono di un profilo obbligatorio o di roaming che non viene salvato. Scegliere questa opzione solo se tutti i server del proprio ambiente eseguono XenApp 5 e versioni successive. Inoltre, gli utenti utilizzano il plug-in online Citrix versioni da 9 a 12.x o Citrix Receiver 3.x.
- L'opzione Retained in user profile only (Conservate solo nel profilo utente) è per i dispositivi utente limitati dalla larghezza di banda (questa opzione riduce il traffico di rete) e dalla velocità di accesso o per gli utenti con plug-in legacy. Questa opzione memorizza le proprietà della stampante nel profilo utente sul server e impedisce lo scambio di proprietà con il dispositivo utente. Utilizzare questa opzione con MetaFrame Presentation Server 3.0 o versioni precedenti e MetaFrame Presentation Server Client 8.x o versioni precedenti. Questa opzione è applicabile solo se viene utilizzato un profilo di roaming di Servizi Desktop remoto (RDS).

- L'opzione Held in profile only if not saved on the client (Conservate nel profilo solo se non salvate sul client) consente al sistema di determinare dove sono memorizzate le proprietà della stampante. Le proprietà della stampante vengono memorizzate sul dispositivo utente, se disponibile, o nel profilo utente. Sebbene questa opzione sia la più flessibile, può anche rallentare il tempo di accesso e utilizzare ulteriore larghezza di banda per il controllo del sistema.
- L'opzione Do not retain printer properties (Non conservare le proprietà della stampante) impedisce la memorizzazione delle proprietà della stampante.

### Retained and restored client printers (Stampanti client conservate e ripristinate)

Questa impostazione abilita o disabilita la conservazione e la nuova creazione delle stampanti sul dispositivo utente. Per impostazione predefinita, le stampanti client vengono conservate automaticamente e ripristinate automaticamente.

Le stampanti conservate sono stampanti create dall'utente che vengono create nuovamente o ricordate all'inizio della sessione successiva. Quando Citrix Virtual Apps ricrea una stampante conservata, considera tutte le impostazioni dei criteri tranne l'impostazione **Auto-create client printers** (Crea automaticamente stampanti client).

Le stampanti ripristinate sono stampanti completamente personalizzate da un amministratore, con uno stato salvato collegato in modo permanente a una porta client.

### Driver stampante universale PDF Citrix

Il driver stampante universale PDF Citrix consente agli utenti di stampare documenti aperti con applicazioni ospitate o applicazioni che sono in esecuzione su desktop virtuali forniti da Citrix Virtual Apps and Desktops. Quando un utente seleziona l'opzione **Citrix PDF Printer** (Stampante PDF Citrix), il driver converte il file in PDF e trasferisce il PDF al dispositivo locale. Il PDF viene quindi aperto per la visualizzazione e la stampa da una stampante collegata localmente. PDF è uno dei formati supportati da Citrix Universal Printing (oltre a EMF e XPS).
La stampante PDF può essere abilitata, configurata e impostata come predefinita utilizzando un criterio Citrix. L'opzione **Citrix PDF Printer** (Stampante PDF Citrix) è disponibile per gli utenti dell'app Citrix Workspace per Windows, Chrome e HTML5.

> **Nota:**
>
> Per gli endpoint di Windows è necessario un visualizzatore PDF. Il client deve disporre di un'applicazione con un'associazione di tipi di file registrata su Windows per aprire i file PDF.

# Impostazioni dei criteri dei driver

January 7, 2024

La sezione **Drivers** contiene le impostazioni dei criteri relativi ai driver della stampante.

## Automatic installation of in-box printer drivers (Installazione automatica dei driver inclusi della stampante)

> **Nota**
>
> Questo criterio non supporta i VDA in questa versione.

Questa impostazione abilita o disabilita l'installazione automatica dei driver delle stampanti tra i seguenti:

- Set di driver Windows in dotazione
- Pacchetti di driver approntati sull'host utilizzando `pnputil.exe /a`

Per impostazione predefinita, questi driver vengono installati in base alle esigenze.

## Universal driver preference (Preferenza driver universale)

Questa impostazione specifica l'ordine in cui vengono utilizzati i driver della stampante universale, a partire dalla prima voce dell'elenco.

Per impostazione predefinita, l'ordine di preferenza è:

- EMF
- XPS
- PCL5c
- PCL4
- PS

È possibile aggiungere, modificare o rimuovere driver e modificare l'ordine dei driver nell'elenco.

## Universal print driver usage (Utilizzo del driver della stampante universale)

Questa impostazione specifica quando utilizzare la stampa universale.

Per impostazione predefinita, la stampa universale viene utilizzata solo se il driver richiesto non è disponibile.

La stampa universale utilizza driver delle stampanti generici anziché driver specifici per modelli standard, semplificando potenzialmente l'onere della gestione dei driver sui computer host. La disponibilità dei driver di stampa universali dipende dalle funzionalità del dispositivo utente, dell'host e del software del server di stampa. In alcune configurazioni, la stampa universale potrebbe non essere disponibile.

Quando si aggiunge questa impostazione a un criterio, selezionare un'opzione dalla tabella seguente:

| Opzione | Descrizione |
| --- | --- |
| **Utilizzare solo driver specifici del modello di stampante** | Specifica che la stampante client utilizza solo i driver standard specifici del modello creati automaticamente durante l'accesso. Se il driver richiesto non è disponibile, la stampante client non può essere creata automaticamente. |
| **Use universal printing only (Usa solo la stampa universale)** | Specifica che non vengono utilizzati driver standard specifici del modello. Per creare stampanti vengono utilizzati solo driver di stampa universali. |
| **Utilizzare la stampa universale solo se il driver richiesto non è disponibile** | Utilizza driver specifici del modello standard per la creazione della stampante, se disponibili. Se il driver non è disponibile sul server, la stampante client viene creata automaticamente con il driver universale appropriato. |
| **Use printer model specific drivers only if universal printing is unavailable (Utilizza driver specifici del modello di stampante solo se la stampa universale non è disponibile)** | Utilizza il driver di stampa universale, se disponibile. Se il driver non è disponibile sul server, la stampante client viene creata automaticamente con il driver della stampante appropriato specifico del modello. |

## Impostazioni dei criteri di Universal Print Server

January 7, 2024

La sezione **Universal Print Server** (Server di stampa universale) include le impostazioni dei criteri per la gestione del server di stampa universale.

### SSL cipher suite (Suite di cifratura SSL)

Questa impostazione specifica l'insieme di suite di cifratura SSL/TLS utilizzato nel client di stampa universale per le connessioni del flusso di dati di stampa (GCP).

Per controllare il pacchetto di crittografia utilizzato dal client di stampa universale per le connessioni del servizio Web di stampa crittografato (HTTPS/SOAP), vedere [SCHANNEL].

Valore predefinito: ALL

Questa impostazione ha i seguenti valori: ALL, COM o GOV.

Le suite di cifratura corrispondenti a ciascun valore sono le seguenti:

**ALL:**

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

**COM:**

TLS_ECDHE_RSA_AES128_CBC_SHA

**GOV:**

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

### SSL compliance mode (Modalità di conformità SSL)

Questa impostazione specifica il livello di conformità al documento NIST Special Publication 800-52 utilizzato dal client di stampa universale per le connessioni del flusso di dati di stampa (CGP) crittografate.

Valore predefinito: None (Nessuno).

Questa impostazione ha i seguenti valori:

**None (Nessuno).**

Le connessioni del flusso dei dati di stampa (CGP) crittografate utilizzano la modalità di conformità predefinita.

**SP800-52.**

Le connessioni del flusso dei dati di stampa (CGP) crittografate utilizzano la modalità di conformità al documento NIST Special Publication 800-52.

### SSL enabled (SSL abilitato)

Questa impostazione specifica se SSL/TLS viene utilizzato da Universal Print Client per quanto segue:

- Connessioni CGP (Print Data Stream)
- Connessioni al servizio Web (HTTP/SOAP)

Quando si imposta l'opzione **Universal Print Server enable** (Abilitazione server di stampa universale) su **Enabled with fallback to Windows'native remote printing** (Abilitato con fallback per la stampa remota nativa di Windows), le connessioni di fallback vengono stabilite dal provider di stampa di rete di Microsoft Windows. Questa impostazione non influisce su queste connessioni di fallback.

Valore predefinito: Disabled (Disabilitato)

Questa impostazione ha i seguenti valori:

**Enabled.**

Il client di stampa universale utilizza SSL/TLS per connettersi al server di stampa universale.

**Disabled.**

Il client di stampa universale utilizza SSL/TLS per connettersi al server di stampa universale.

### SSL FIPS mode (Modalità FIPS SSL)

Questa impostazione specifica se il modulo crittografico SSL/TLS utilizzato dal client di stampa universale per le connessioni del flusso di dati di stampa (CGP) viene eseguito in modalità FIPS.

Valore predefinito: Disabled (Disabilitato)

Questa impostazione ha i seguenti valori:

**Enabled.**

La modalità FIPS è abilitata.

**Disabled.**

La modalità FIPS è disabilitata.

### SSL protocol version (Versione del protocollo SSL)

Questa impostazione specifica la versione del protocollo SSL/TLS utilizzata dal client di stampa universale.

Valore predefinito: ALL

Questa impostazione ha i seguenti valori:

**ALL** (TUTTI).

Utilizzare TLS versioni 1.0, 1.1 o 1.2.

**TLSv1.**

Utilizzare TLS versione 1.0.

**TLSv1.1.**

Utilizzare TLS versione 1.1.

**TLSv1.2.**

Utilizzare TLS versione 1.2.

### SSL Universal Print Server encrypted print data stream (CGP) port (Porta del flusso di dati di stampa (CGP) crittografata del server di stampa universale SSL)

Questa impostazione specifica il numero di porta TCP della porta del flusso di dati di stampa (CGP) crittografata del server di stampa universale. Questa porta riceve i dati per i processi di stampa.

Valore predefinito: 443

### SSL Universal Print Server encrypted web service (HTTPS/SOAP) port (Porta del servizio Web crittografato (HTTPS/SOAP) del server di stampa universale SSL)

Questa impostazione specifica il numero di porta TCP della porta del servizio Web crittografato (HTTPS/SOAP) del server di stampa universale. Questa porta riceve i dati per i comandi di stampa.

Valore predefinito: 8443

### Universal Print Server enable (Abilitazione server di stampa universale)

Questo criterio abilita o disabilita l'uso di Citrix Universal Print Server (UPS). Applicare questa impostazione dei criteri alle unità organizzative (OU) che includono il desktop virtuale o le applicazioni di hosting del server. Queste impostazioni dei criteri includono opzioni di fallback per consentire le connessioni ai server di stampa utilizzando il servizio di stampa remota nativo di Windows nel caso in cui il componente Citrix UPS non fosse installato o non fosse disponibile sul server di stampa richiesto. Le modifiche apportate a questa politica sono applicabili solo dopo il riavvio del VDA.

Per impostazione predefinita, l'impostazione Universal Print Server (Server di stampa universale) è disabilitata.

Quando si aggiunge questa impostazione a un criterio, selezionare una delle seguenti opzioni:

- **Enabled with fallback to Windows native remote printing** (Abilitato con il fallback alla stampa remota nativa di Windows): Universal Print Server serve le connessioni della stampante di rete, se possibile. Se il server di stampa universale non è disponibile, viene utilizzato il provider di stampa di Windows. Il provider di stampa di Windows continua a gestire tutte le stampanti create in precedenza con il provider di stampa di Windows.
- **Enabled with no fallback to Windows native remote printing** (Abilitato senza alcun fallback alla stampa remota nativa di Windows): Universal Print Server serve esclusivamente le connessioni delle stampanti di rete. Se il server di stampa universale non è disponibile, la connessione della stampante di rete non riesce. Sostanzialmente, questa impostazione disabilita la stampa di rete tramite il provider di stampa di Windows. Le stampanti create in precedenza con il provider di stampa di Windows non vengono create quando è attivo un criterio contenente questa impostazione.
- **Disabled**: la funzionalità Universal Print Server (Server di stampa universale) è disabilitata. Non viene effettuato alcun tentativo di connessione con il server di stampa universale durante la connessione a una stampante di rete con un nome UNC. Le connessioni alle stampanti remote continuano a utilizzare la funzione di stampa remota nativa di Windows.

### Universal Print Server print data stream (CGP) port (Porta del flusso di dati di stampa (CGP) del server di stampa universale)

Questa impostazione specifica il numero di porta TCP utilizzato dal listener CGP (Common Gateway Protocol) del flusso di dati di stampa del server di stampa universale. Applicare questa impostazione dei criteri solo alle unità organizzative in cui si trova il server di stampa.

Per impostazione predefinita, il numero di porta è impostato su 7229.

I numeri di porta validi devono essere compresi tra 1 e 65.535.

### Universal Print Server print stream input bandwidth limit (Kbps) (Limite della larghezza di banda di input del flusso di stampa del server di stampa universale [Kbps])

Questa impostazione specifica il limite superiore (in kilobit al secondo) della velocità di trasferimento dei dati di stampa. La velocità di trasferimento viene calcolata per i dati di stampa che vengono consegnati da ciascun lavoro di stampa a Universal Print Server utilizzando CGP. Applicare questa impostazione dei criteri alle unità organizzative in cui si trovano le applicazioni che ospitano desktop virtuali o server.

Per impostazione predefinita, il valore è 0, che non specifica alcun limite superiore.

### Universal Print Server web service (HTTP/SOAP) port (Porta del servizio Web del server di stampa universale [HTTP/SOAP])

Questa impostazione specifica il numero di porta TCP utilizzato dal listener del servizio Web (HTTP/-SOAP) del server di stampa universale. Il server di stampa universale è un componente opzionale che consente l'utilizzo dei driver di stampa universali Citrix per scenari di stampa in rete.

Quando si utilizza il server di stampa universale, i comandi di stampa vengono inviati dagli host di Citrix Virtual Apps and Desktops al server di stampa universale tramite SOAP su HTTP. Questa impostazione modifica la porta TCP predefinita su cui il server di stampa universale è in ascolto per le richieste HTTP/SOAP in entrata.

È necessario configurare la porta HTTP dell'host e del server di stampa in modo identico. Se non si configurano le porte in modo identico, il software host non si connetterà al server di stampa universale. Questa impostazione modifica il VDA su Citrix Virtual Apps and Desktops. Inoltre, è necessario modificare la porta predefinita sul server di stampa universale.

Per impostazione predefinita, il numero di porta è impostato su 8080.

I numeri di porta validi devono essere compresi tra 0 e 65535.

### Universal Print Servers for load balancing (Universal Print Server per il bilanciamento del carico)

Questa impostazione elenca gli Universal Print Server da utilizzare per bilanciare il carico delle connessioni della stampante stabilite all'avvio della sessione, dopo aver valutato altre impostazioni dei criteri di stampa Citrix. Per ottimizzare i tempi di creazione della stampante, Citrix consiglia che tutti i server di stampa abbiano lo stesso set di stampanti condivise. Non esiste un limite superiore al numero di server di stampa che possono essere aggiunti per il bilanciamento del carico.

Questa impostazione implementa inoltre il rilevamento del failover del server di stampa e il ripristino delle connessioni della stampante. I server di stampa vengono controllati periodicamente per verificare la disponibilità. Se viene rilevato un errore del server, tale server viene rimosso dallo schema di bilanciamento del carico. Inoltre, le connessioni delle stampanti a quel server vengono ridistribuite tra gli altri server di stampa disponibili. Quando il server di stampa non funzionante viene ripristinato, viene restituito allo schema di bilanciamento del carico.

Fare clic su **Convalida server** per verificare che ogni server sia un server di stampa, che l'elenco dei server non includa nomi di server duplicati e che tutti i server dispongano di un set identico di stampanti condivise installato. Questa operazione potrebbe richiedere del tempo.

### Universal Print Servers out-of-service threshold (Soglia fuori servizio degli Universal Print Server)

Questa impostazione specifica per quanto tempo il bilanciatore del carico deve attendere il ripristino di un server di stampa non disponibile prima di determinare che il server è permanentemente offline e prima di ridistribuire il carico ad altri server di stampa disponibili.

Per impostazione predefinita, il valore di soglia è impostato su 180 (secondi).

### Timeout di connessione al servizio Web Universal Print Server (HTTP/SOAP)

Questa impostazione specifica il numero di secondi che Universal Print Client deve attendere fino al timeout dell'operazione connect() del servizio Web Universal Print Server. Questa impostazione ha i valori seguenti. Tutti questi valori sono numerici e le unità (di tempo) sono i secondi.

- Il valore minimo è 0.
- Il valore massimo è 60.
- Il valore predefinito è 10.

Quando il timeout è compreso tra 1 e 60 (inclusi), Universal Print Client attende il tempo specificato per il completamento dell'operazione. Questa è un'operazione di connessione con socket TCP. I socket sono una funzionalità del sistema operativo Windows che consente la comunicazione tra processi su reti TCP/IP.

Quando il timeout è 0, Universal Print Client utilizza il timeout predefinito stabilito dal sistema operativo. Questa configurazione era quella disponibile nelle versioni precedenti di Universal Print Client prima di questa modifica.

Universal Print Client è il componente del Virtual Delivery Agent (VDA) che comunica con Universal Print Server.

> **Nota:**
>
> questa impostazione dei criteri è applicabile nelle versioni VDA 7.35 e successive.

### Timeout di ricezione del servizio Web Universal Print Server (HTTP/SOAP)

Questa impostazione specifica il numero di secondi che Universal Print Client deve attendere fino al timeout dell'operazione recv() del servizio Web di Universal Print Server. Questa impostazione ha i seguenti valori, che sono tutti numerici e le unità (di tempo) sono i secondi.

- Il valore minimo è 0.
- Il valore massimo è 60.
- Il valore predefinito è 10.

Quando il timeout è compreso tra 1 e 60 (inclusi), Universal Print Client attende il tempo specificato per il completamento dell'operazione. Questa è un'operazione di ricezione con socket TCP. I socket sono una funzionalità del sistema operativo Windows che consente la comunicazione tra processi su reti TCP/IP.

Quando il timeout è 0, Universal Print Client utilizza il timeout predefinito stabilito dal sistema operativo. Questa configurazione era quella disponibile nelle versioni precedenti di Universal Print Client prima di questa modifica.

Universal Print Client è il componente del Virtual Delivery Agent (VDA) che comunica con Universal Print Server.

> **Nota:**
>
> questa impostazione dei criteri è applicabile nelle versioni VDA 7.35 e successive.

### Timeout di invio del servizio Web Universal Print Server (HTTP/SOAP)

Questa impostazione specifica il numero di secondi che Universal Print Client deve attendere fino al timeout dell'operazione send() del servizio Web di Universal Print Server. Questa impostazione ha i valori seguenti. Tutti questi valori sono numerici e le unità (di tempo) sono i secondi.

- Il valore minimo è 0.
- Il valore massimo è 60.
- Il valore predefinito è 10.

Quando il timeout è compreso tra 1 e 60 (inclusi), Universal Print Client attende il tempo specificato per il completamento dell'operazione. Questa è un'operazione di invio socket TCP. I socket sono una funzionalità del sistema operativo Windows che consente la comunicazione tra processi su reti TCP/IP.

Quando il timeout è 0, Universal Print Client utilizza il timeout predefinito stabilito dal sistema operativo. Questa configurazione era quella disponibile nelle versioni precedenti di Universal Print Client prima di questa modifica.

Universal Print Client è il componente del VDA che comunica con Universal Print Server.

> **Nota:**
>
> questa impostazione dei criteri è applicabile nelle versioni VDA 7.35 e successive.

## Impostazioni dei criteri di stampa universale

January 7, 2024

La sezione **Universal Printing** (Stampa universale) contiene le impostazioni dei criteri per la gestione della stampa universale.

### Universal printing EMF processing mode (Modalità di elaborazione EMF della stampa universale)

Questa impostazione controlla il metodo di elaborazione del file di spool EMF sul dispositivo utente Windows.

Per impostazione predefinita, lo spooling dei record EMF viene eseguito direttamente sulla stampante.

Quando si aggiunge questa impostazione a un criterio, selezionare un'opzione:

- La rielaborazione di EMF per la stampante impone la rielaborazione del file di spooling EMF, che verrà inviato attraverso il sottosistema GDI sul dispositivo utente. È possibile utilizzare questa impostazione per i driver che richiedono la rielaborazione EMF ma che potrebbero non essere selezionati automaticamente in una sessione.
- Lo spooling diretto sulla stampante, se utilizzato con il driver di stampa universale Citrix, assicura che venga eseguito lo spooling dei record EMF e che vengano consegnati al dispositivo utente per l'elaborazione. In genere, questi file di spooling EMF vengono inseriti direttamente nella coda di spooling del client. Per stampanti e driver compatibili con il formato EMF, questo è il metodo di stampa più veloce.

### Universal printing image compression limit (Limite di compressione delle immagini per la stampa universale)

Questa impostazione specifica quanto segue:

- Massima qualità disponibile per le immagini stampate con il driver di stampa Citrix Universal
- Livello di compressione minimo disponibile per le immagini stampate con il driver di stampa Citrix Universal

Per impostazione predefinita, il limite di compressione delle immagini è impostato su Best quality (lossless compression) (Migliore qualità (compressione senza perdita di dati)).

Se viene selezionata l'opzione No compression (Nessuna compressione), la compressione è disabilitata solo per la stampa EMF.

Quando si aggiunge questa impostazione a un criterio, selezionare un'opzione:

- No compression (Nessuna compressione)
- Best quality (lossless compression) (Migliore qualità [compressione senza perdita di dati])

- High quality (Alta qualità)
- Standard quality (Qualità standard)
- Reduced quality (maximum compression) (Qualità ridotta (compressione massima))

Quando si aggiunge questa impostazione a un criterio che include l'impostazione **Universal printing optimization defaults** (Impostazioni predefinite dell'ottimizzazione della stampa universale), tenere presente quanto segue:

- Considerare che il livello di compressione nell'impostazione **Universal printing image compression limit** (Limite di compressione delle immagini per la stampa universale) è inferiore al livello definito nell'impostazione **Universal printing optimization defaults** (Impostazioni predefinite per l'ottimizzazione della stampa universale). In questo caso, le immagini vengono compresse al livello definito nell'impostazione Universal printing image compression limits (Limiti di compressione delle immagini per la stampa universale).
- Se la compressione è disabilitata, le opzioni Desired image quality (Qualità immagine desiderata) e Enable heavyweight compression (Abilita compressione heavyweight) delll'impostazione Universal printing optimization defaults (Impostazioni predefinite per l'ottimizzazione della stampa universale) non hanno alcun effetto nel criterio.

### Universal printing optimization defaults (Impostazioni predefinite per l'ottimizzazione della stampa universale)

Questa impostazione specifica i valori predefiniti per l'ottimizzazione della stampa quando viene creato il driver di stampa universale per una sessione.

- La qualità dell'immagine desiderata specifica il limite di compressione delle immagini predefinito applicato alla stampa universale. Per impostazione predefinita, la qualità standard è abilitata, il che significa che gli utenti possono stampare le immagini solo utilizzando una compressione standard o di qualità ridotta.
- L'opzione Enable heavyweight compression (Abilita la compressione heavyweight) abilita o disabilita la riduzione della larghezza di banda oltre il livello di compressione impostato dall'opzione Desired image quality (Qualità immagine desiderata), senza perdere la qualità dell'immagine. Per impostazione predefinita, la compressione heavyweight è disabilitata.
- Le impostazioni di memorizzazione nella cache di immagini e caratteri specificano se memorizzare nella cache immagini e caratteri visualizzati più volte nel flusso di stampa o meno. Questa impostazione garantisce che ogni immagine o carattere univoco venga inviato alla stampante una sola volta. Per impostazione predefinita, le immagini e i caratteri incorporati vengono memorizzati nella cache. Queste impostazioni si applicano solo se il dispositivo utente supporta questo comportamento.
- L'impostazione Allow non-administrators to modify these settings (Consenti a utenti non amministratori di modificare queste impostazioni) specifica se gli utenti possono modificare le im-

postazioni di ottimizzazione di stampa predefinite all'interno di una sessione o meno. Per impostazione predefinita, gli utenti non sono autorizzati a modificare le impostazioni di ottimizzazione di stampa predefinite.

Nota: tutte queste opzioni sono supportate per la stampa EMF. Per la stampa XPS è supportata solo l'opzione Desired image quality (Qualità dell'immagine desiderata).

Quando si aggiunge questa impostazione a un criterio che include l'impostazione **Universal printing image compression limit** (Limite di compressione delle immagini per la stampa universale), tenere presente quanto segue:

- Considerare che il livello di compressione nell'impostazione **Universal printing image compression limit** (Limite di compressione delle immagini per la stampa universale) è inferiore al livello definito nell'impostazione **Universal printing optimization defaults** (Impostazioni predefinite per l'ottimizzazione della stampa universale). In questo caso, le immagini vengono compresse al livello definito nell'impostazione Universal printing image compression limits (Limiti di compressione delle immagini per la stampa universale).
- Se la compressione è disabilitata, le opzioni Desired image quality (Qualità immagine desiderata) e Enable heavyweight compression (Abilita compressione heavyweight) delll'impostazione Universal printing optimization defaults (Impostazioni predefinite per l'ottimizzazione della stampa universale) non hanno alcun effetto nel criterio.

### Universal printing preview preference (Preferenza anteprima di stampa universale)

Questa impostazione specifica se utilizzare la funzione di anteprima di stampa per stampanti universali create automaticamente o generiche.

Per impostazione predefinita, l'anteprima di stampa non viene utilizzata per stampanti universali create automaticamente o generiche.

Quando si aggiunge questa impostazione a un criterio, selezionare un'opzione:

- Do not use print preview for auto-created or generic universal printers (Non utilizzare l'anteprima di stampa per stampanti universali create automaticamente o generiche)
- Use print preview for auto-created printers only (Utilizza l'anteprima di stampa solo per stampanti create automaticamente)
- Use print preview for generic universal printers only (Utilizza l'anteprima di stampa solo per stampanti universali generiche)
- Use print preview for both auto-created and generic universal printers (Utilizza l'anteprima di stampa per stampanti universali create automaticamente e generiche)

### Universal printing print quality limit (Limite della qualità di stampa per la stampa universale)

Questa impostazione specifica il numero massimo di punti per pollice (dpi) disponibili per la generazione di output stampato in una sessione.

Per impostazione predefinita, l'opzione No Limit (Nessun limite) è abilitata, il che significa che gli utenti possono selezionare la massima qualità di stampa consentita dalla stampante a cui si connettono.

Questa impostazione, se configurata, limita la massima qualità di stampa disponibile per gli utenti in termini di risoluzione di output. Sia la qualità di stampa stessa che le funzionalità relative alla qualità di stampa della stampante a cui l'utente si connette sono limitate all'impostazione configurata.

Ad esempio, se è configurata la Medium Resolution (600 DPI), gli utenti possono stampare l'output con una qualità massima di soli 600 DPI. Inoltre, l'impostazione **Print Quality** (Qualità di stampa) nella scheda **Advanced** (Avanzate) della finestra di dialogo **Universal Printer** (Stampante universale) visualizza le impostazioni di risoluzione solo fino a Medium Quality (600 DPI) inclusa.

Quando si aggiunge questa impostazione a un criterio, selezionare un'opzione:

- Draft (150 DPI) (Bozza (150 DPI))
- Low Resolution (300 DPI) (Bassa risoluzione (300 DPI))
- Medium Resolution (600 DPI) (Media risoluzione (600 DPI))
- High Resolution (1200 DPI) (Alta risoluzione (1200 DPI))
- No Limit (Nessun limite)

## Impostazioni dei criteri di sicurezza

January 7, 2024

La sezione **Security** (Sicurezza) include l'impostazione dei criteri per la configurazione della crittografia della sessione e della crittografia dei dati di accesso.

### SecureICA minimum encryption level (Livello minimo di crittografia SecureICA)

Questa impostazione specifica il livello minimo al quale crittografare i dati di sessione inviati tra il server e un dispositivo utente.

**Importante:** per Virtual Delivery Agent 7.x, questa impostazione dei criteri può essere utilizzata solo per abilitare la crittografia dei dati di accesso con crittografia RC5 a 128 bit. Altre impostazioni sono

disponibili solo per la retrocompatibilità con le versioni precedenti di Citrix Virtual Apps and Desktops.

Per VDA 7.x, la crittografia dei dati di sessione viene impostata utilizzando le impostazioni di base del gruppo di consegna di VDA. Se per il gruppo di consegna è selezionata l'opzione Enable Secure ICA (Abilita ICA sicura), i dati della sessione vengono crittografati utilizzando la crittografia RC5 (128 bit). Se l'opzione Enable Secure ICA (Abilita ICA sicura) non è selezionata per il gruppo di consegna, i dati della sessione vengono crittografati con crittografia di base.

Quando si aggiunge questa impostazione a un criterio, selezionare un'opzione:

- L'opzione Basic (Di base) crittografa la connessione client utilizzando un algoritmo diverso da RC5. Protegge il flusso di dati dalla lettura diretta, ma può essere decrittografato. Per impostazione predefinita, il server utilizza la crittografia di base per il traffico client-server.
- L'opzione RC5 (128 bit) logon (Accesso RC5 (128 bit)) crittografa solo i dati di accesso utilizzando la crittografia RC5 a 128 bit e la connessione client utilizzando la crittografia di base.
- L'opzione RC5 (40 bit) crittografa la connessione client utilizzando la crittografia RC5 a 40 bit.
- L'opzione RC5 (56 bit) crittografa la connessione client utilizzando la crittografia RC5 a 56 bit.
- L'opzione RC5 (128 bit) crittografa la connessione client utilizzando la crittografia RC5 a 128 bit.

Le impostazioni specificate per la crittografia client-server possono interagire con qualsiasi altra impostazione di crittografia nell'ambiente e nel sistema operativo Windows. Considerare che un livello di crittografia con priorità più alta è impostato su un server o su un dispositivo utente. In questo caso, le impostazioni specificate per le risorse pubblicate possono essere sostituite.

È possibile aumentare i livelli di crittografia per proteggere ulteriormente le comunicazioni e l'integrità dei messaggi per determinati utenti. Se un criterio richiede un livello di crittografia più elevato, ai ricevitori Citrix che utilizzano un livello di crittografia inferiore viene negata la connessione.

SecureICA non esegue l'autenticazione e non verifica l'integrità dei dati. Per fornire la crittografia end-to-end per il sito, utilizzare SecureICA con crittografia TLS.

SecureICA non utilizza algoritmi compatibili con FIPS. Se questa impostazione è un problema, configurare il server e i ricevitori Citrix per evitare l'utilizzo di SecureICA.

SecureICA utilizza la crittografia a blocchi RC5 come descritto in RFC 2040 per la riservatezza. La dimensione del blocco è di 64 bit (un multiplo di unità di parole a 32 bit). La lunghezza della chiave è 128 bit. Il numero di giri è 12.

Le chiavi per la crittografia a blocchi RC5 vengono negoziate quando viene creata una sessione. La negoziazione viene eseguita utilizzando l'algoritmo Diffie-Hellman. Questa negoziazione utilizza parametri pubblici Diffie-Hellman. Questi parametri vengono memorizzati nel Registro di sistema di Windows quando è installato Virtual Delivery Agent. I parametri pubblici non sono segreti. Il risultato della negoziazione Diffie-Hellman è una chiave segreta, da cui derivano le chiavi di sessione per la crittografia a blocchi RC5. Vengono utilizzate chiavi di sessione separate per l'accesso dell'utente e

per il trasferimento dei dati. Inoltre, vengono utilizzate chiavi di sessione separate per il traffico da e verso il Virtual Delivery Agent. Pertanto, ci sono quattro chiavi di sessione per ogni sessione. Le chiavi segrete e le chiavi di sessione non sono memorizzate. Anche i vettori di inizializzazione per la crittografia a blocchi RC5 derivano dalla chiave segreta.

## Impostazioni dei criteri dei limiti del server

January 7, 2024

La sezione **Server Limits** (Limiti server) include l'impostazione dei criteri per il controllo delle connessioni inattive.

### Server idle timer interval (Intervallo del timer inattivo del server)

Questa impostazione determina per quanto tempo una sessione utente ininterrotta viene mantenuta in assenza di input da parte dell'utente. I dati vengono calcolati in millisecondi.

Per impostazione predefinita, le connessioni inattive non vengono disconnesse (intervallo timer inattivo del server = 0). Citrix consiglia di impostare questo valore su un minimo di 60.000 millisecondi (60 secondi).

Per visualizzare il criterio, selezionare **Multiple Versions** (Più versioni), deselezionare le versioni del sistema operativo a sessione singola e quindi selezionare **Server Limits** (Limiti server).

> **Nota**
>
> Quando si utilizza questa impostazione dei criteri, gli utenti potrebbero visualizzare una finestra di dialogo "Idle timer expired"(Timer inattivo scaduto) quando la sessione è rimasta inattiva per il tempo specificato. Le impostazioni dei criteri Citrix non controllano questa finestra di dialogo Microsoft. Per ulteriori informazioni, vedere http://support.citrix.com/article/CTX118618.

## Impostazioni dei criteri per i limiti di sessione

January 7, 2024

La sezione **Session Limits** (Limiti sessione) include impostazioni dei criteri che controllano per quanto tempo le sessioni rimangono connesse prima che vengano costrette a disconnettersi.

### Disconnected session timer (Timer di sessione disconnesso)

Questa impostazione abilita o disabilita un timer che specifica per quanto tempo un desktop bloccato e disconnesso rimane bloccato prima che la sessione venga terminata.

Se questo timer è abilitato, la sessione disconnessa viene terminata alla scadenza del timer.

Per impostazione predefinita, le sessioni disconnesse non vengono scollegate.

### Remote PC Access disconnected session timer (Timer di sessione disconnesso per accesso PC remoto)

Questa impostazione abilita o disabilita un timer che scollega una sessione utente disconnessa dopo la scadenza del timer. Se si abilita questa impostazione, utilizzare l'impostazione **Disconnected session timer interval** (Intervallo timer sessione disconnessa) per specificare per quanti minuti un desktop disconnesso rimane bloccato prima che la sessione utente venga disconnessa.

Per impostazione predefinita, questa impostazione è disabilitata.

### Disconnected session timer interval (Intervallo del timer di sessione disconnesso)

Questa impostazione specifica per quanti minuti un desktop bloccato e disconnesso può rimanere bloccato prima che la sessione venga scollegata.

Per impostazione predefinita, il periodo di tempo è 1.440 minuti (24 ore).

### Disconnected session timer –Multi-session (Timer sessione disconnesso - Multisessione)

Questa impostazione abilita o disabilita un timer per determinare per quanto tempo una sessione RDS disconnessa può persistere prima che la sessione si scolleghi. Per impostazione predefinita, questo timer è disabilitato e le sessioni disconnesse non vengono scollegate.

### Disconnected session timer interval –Multi-session (Intervallo timer sessione disconnessa —Multisessione)

Questa impostazione determina per quanti minuti una sessione RDS disconnessa può persistere prima che la sessione venga scollegata. Per impostazione predefinita, il periodo di tempo è 1.440 minuti (24 ore).

### Session connection timer (Timer di connessione sessione)

Questa impostazione abilita o disabilita un timer che specifica la durata massima di una connessione ininterrotta tra un dispositivo utente e un desktop. Se questo timer è abilitato, la sessione viene disconnessa o terminata alla scadenza del timer. L'impostazione di Microsoft **Termina la sessione quando si raggiungono i limiti di tempo** determina lo stato successivo per la sessione.

Per impostazione predefinita, questo timer è disabilitato.

### Session connection timer interval (Intervallo timer di connessione sessione)

Questa impostazione specifica il numero massimo di minuti per una connessione ininterrotta tra un dispositivo utente e un desktop.

Per impostazione predefinita, la durata massima è 1.440 minuti (24 ore).

### Session connection timer –Multi-session (Timer di connessione alla sessione — Multisessione)

Questa impostazione abilita o disabilita un timer che specifica la durata massima di una connessione ininterrotta tra un dispositivo utente e un server terminal. Per impostazione predefinita, questo timer è disabilitato.

### Session connection timer interval –Multi-session (Intervallo timer di connessione alla sessione —Multisessione)

Questa impostazione specifica il numero massimo di minuti per una connessione ininterrotta tra un dispositivo utente e una sessione RDS. Per impostazione predefinita, la durata massima è 1.440 minuti (24 ore).

### Session idle timer (Timer di inattività sessione)

Quando un utente non fornisce alcun input, questa impostazione viene utilizzata per abilitare o disabilitare:

- Un timer che specifica per quanto tempo viene mantenuta una connessione ininterrotta dal dispositivo utente a un desktop.

Quando questo timer scade, la sessione viene posizionata nello stato disconnesso e si applica il **timer di sessione disconnessa**. Se l'opzione **Disconnected session timer** (Timer di sessione disconnessa) è disabilitata, la sessione non viene disconnessa.

Per impostazione predefinita, questo timer è abilitato.

### Session idle timer interval (Intervallo del timer di inattività sessione)

Quando non ci sono input da parte dell'utente, questa impostazione viene utilizzata per specificare:

- Il numero di minuti per i quali viene mantenuta una connessione ininterrotta dal dispositivo utente a un desktop.

Per impostazione predefinita, le connessioni inattive vengono mantenute per 1.440 minuti (24 ore).

### Session idle timer –Multi-session (Timer di inattività sessione —Multisessione)

Questa impostazione abilita o disabilita un timer per determinare la durata massima di una connessione inattiva tra un dispositivo utente e un server terminal. Per impostazione predefinita, questo timer è disabilitato.

### Session idle timer interval–Multi-session (Intervallo timer di inattività sessione - Multisessione)

Questa impostazione specifica dopo quanti minuti viene considerata inattiva una connessione tra un dispositivo utente e una sessione RDS. Per impostazione predefinita, la durata massima è 1.440 minuti (24 ore).

> **Nota:**
>
> Si prevede che le impostazioni del timer per le macchine multisessione configurate utilizzando i criteri Citrix sovrascrivano le impostazioni del timer configurate tramite Criteri di gruppo Microsoft. Per evitare comportamenti imprevisti, si consiglia di configurare le impostazioni del timer utilizzando uno dei due metodi.

## Impostazioni dei criteri di affidabilità della sessione

January 7, 2024

La sezione relativa all'**affidabilità della sessione** include le impostazioni dei criteri per la gestione delle connessioni di affidabilità delle sessioni.

### Session reliability connections (Connessioni di affidabilità delle sessioni)

Questa impostazione consente o impedisce che le sessioni siano mantenute aperte durante la perdita della connettività di rete. L'affidabilità delle sessioni, insieme alla riconnessione automatica del client, consente agli utenti di riconnettersi automaticamente alle sessioni dell'app Citrix Workspace dopo il ripristino da interruzioni della rete. Per impostazione predefinita, l'affidabilità della sessione è impostata su Allowed (Consentita).

Le impostazioni di Web Studio vengono applicate al client per quanto segue:

- App Citrix Workspace 1808 e versioni successive
- Citrix Receiver per Windows 4.7 e versioni successive.

I criteri di Web Studio sostituiscono l'oggetto Criteri di gruppo di Citrix Receiver Group sui client. Gli aggiornamenti di questi criteri in Web Studio sincronizzano l'affidabilità della sessione da server a client.

> **Nota:**
>
> - Citrix Receiver per Windows 4.7 e versioni successive e app Citrix Workspace per Windows: impostare il criterio in Web Studio.
> - Versioni di Citrix Receiver per Windows precedenti alla 4.7 - Impostare le politiche in Web Studio. Impostare anche il modello dell'oggetto Criteri di gruppo di Citrix Receiver sul client per un comportamento coerente.

L'affidabilità delle sessioni mantiene attive le sessioni e le mantiene sullo schermo dell'utente quando la connettività di rete viene interrotta. Gli utenti continuano a visualizzare l'applicazione che stanno utilizzando fino al ripristino della connettività di rete.

Utilizzare l'affidabilità della sessione per mantenere attiva sul server la sessione. Per indicare che la connettività è stata interrotta, il display dell'utente diventa opaco. L'utente potrebbe vedere una sessione bloccata durante l'interruzione. L'utente può riprendere l'interazione con l'applicazione quando viene ripristinata la connessione di rete. La funzione di affidabilità della sessione riconnette gli utenti senza richieste di riautenticazione.

Se si utilizza sia l'affidabilità della sessione che la riconnessione automatica del client, le due funzionalità funzionano in sequenza. L'affidabilità della sessione chiude (o disconnette) la sessione utente dopo il tempo specificato nell'impostazione del timeout dell'affidabilità della sessione. Dopodiché avranno effetto le impostazioni di riconnessione automatica del client, che tentano di riconnettere l'utente alla sessione disconnessa.

Per impostazione predefinita, l'affidabilità della sessione è impostata su Allowed (Consentita).

> **Nota:**
>
> Quando Citrix ADC è in uso, è necessario selezionare **Enable session reliability** in the Citrix StoreFront > **Manage Citrix Gateways** / **Secure Ticket Authority** per eseguire il proxy delle connessioni ICA.

### Session reliability port number (Numero di porta dell'affidabilità della sessione)

Questa impostazione specifica il numero di porta TCP per le connessioni di affidabilità della sessione in ingresso.

Per impostazione predefinita, il numero di porta è impostato su 2598.

### Session reliability timeout (Timeout affidabilità sessione)

Questa impostazione specifica la durata di tempo, in secondi. Questo è il tempo durante il quale il proxy di affidabilità della sessione attende la riconnessione di un utente prima di consentire la disconnessione della sessione.

Sebbene sia possibile estendere il periodo di tempo in cui una sessione viene mantenuta aperta, questa funzionalità è comoda e non richiede all'utente di eseguire nuovamente l'autenticazione. Più a lungo rimane aperta una sessione, più aumentano le probabilità che un utente possa lasciare il dispositivo incustodito e potenzialmente accessibile a utenti non autorizzati.

Per impostazione predefinita, il timeout è impostato su 180 secondi o tre minuti.

## Impostazioni dei criteri per la filigrana di sessione

January 7, 2024

La sezione della **filigrana di sessione** contiene le impostazioni dei criteri per configurare questa funzionalità.
L'abilitazione di questa funzionalità comporta un aumento significativo della larghezza di banda di rete e dell'utilizzo della CPU da parte della macchina VDA. Si consiglia di configurare la filigrana di sessione per i computer VDA selezionati in base alle risorse hardware disponibili.

> **Importante**
>
> Abilitare la filigrana di sessione per rendere effettive le altre impostazioni dei criteri della filigrana. Per un'esperienza utente migliore, non abilitare più di due elementi di testo della filigrana.

### Enable session watermark (Abilita filigrana di sessione)

Quando si abilita questa impostazione, la visualizzazione della sessione ha una filigrana testuale opaca che visualizza informazioni specifiche della sessione. Le altre impostazioni della filigrana dipendono dall'abilitazione di questa impostazione.

Per impostazione predefinita, la filigrana di sessione è disabilitata.

### Include client IP address (Includi indirizzo IP client)

Quando si abilita questa impostazione, la sessione visualizza l'indirizzo IP del client corrente come filigrana.

Per impostazione predefinita, l'opzione Include client IP address (Includi indirizzo IP client) è disabilitata.

### Include connection time (Includi ora di connessione)

Quando si abilita questa impostazione, la filigrana di sessione visualizza un'ora di connessione. Il formato è mm/gg/aaaa hh:mm. L'ora visualizzata si basa sull'orologio di sistema e sul fuso orario.

Per impostazione predefinita, l'opzione Include connection time (Includi ora di connessione) è disabilitata.

### Include logon user name (Includi nome utente di accesso)

Quando si abilita questa impostazione, la sessione visualizza il nome utente di accesso corrente come filigrana. Il formato di visualizzazione è NOMEUTENTE@NOMEDOMINIO. È consigliabile che il nome utente non superi i 20 caratteri. Quando un nome utente è superiore a 20 caratteri, potrebbero verificarsi troncamenti o i caratteri potrebbero apparire eccessivamente piccoli e ridurre l'efficacia della filigrana.

Per impostazione predefinita, l'opzione Include logon user name (Includi nome utente di accesso) è abilitato.

### Include VDA host name (Includi nome host VDA)

Quando si abilita questa impostazione, la sessione visualizza il nome host VDA della sessione ICA corrente come filigrana.

Per impostazione predefinita, l'impostazione Include VDA host name (Includi nome host VDA) è abilitata.

### Include VDA IP address (Includi indirizzo IP VDA)

Quando si abilita questa impostazione, la sessione visualizza l'indirizzo IP VDA della sessione ICA corrente come filigrana.

Per impostazione predefinita, l'indirizzo IP VDA è disabilitato.

### Session watermark style (Stile filigrana sessione)

Questa impostazione controlla se si visualizza una singola etichetta di testo della filigrana o più etichette. Scegliere **Multiple** (Multiple) o **Single** (Singola) dal menu a discesa **Value** (Valore).

**Multiple** (Multiple) visualizza cinque etichette di filigrana nella sessione, una al centro e quattro negli angoli.

**Single** (Singola) visualizza una singola etichetta di filigrana al centro della sessione.

Per impostazione predefinita, lo stile della filigrana di sessione è Multiple.

### Watermark custom text (Testo personalizzato della filigrana)

Questa impostazione consente di applicare testo personalizzato (ad esempio, il nome dell'azienda) da visualizzare nella filigrana della sessione. Quando si configura una stringa non vuota, viene visualizzato il testo in una nuova riga che aggiunge altre informazioni abilitate nella filigrana. Il testo personalizzato della filigrana è limitato a 25 caratteri Unicode. Se si configura una stringa più lunga, viene troncata a 25 caratteri.

Non è presente testo predefinito.

A partire da Citrix Virtual Apps and Desktops 7 2206, è possibile aggiungere ulteriori personalizzazioni utilizzando tag personalizzati nel testo. Di conseguenza, il numero massimo di caratteri del testo personalizzato viene aumentato a 1024.

I tag disponibili per le impostazioni della filigrana sono descritti nella tabella seguente:

| Tag | Descrizione | Esempio |
|---|---|---|
| `<font=value>` | Consente di modificare il tipo di carattere del testo della filigrana. Il valore è il nome di un tipo di carattere disponibile sul VDA. | `<font=Courier New>` |

| Tag | Descrizione | Esempio |
|---|---|---|
| <fontzoom=value> | Consente di impostare la percentuale del fattore di ingrandimento del carattere. Il valore è 200 per l'ingrandimento del 200% sul testo della filigrana. | <fontzoom=200> |
| <position=value> | Consente di modificare la posizione del testo della filigrana. I valori sono center, topleft, topright, bottomleft e bottomright. Questo tag è applicabile solo con lo stile singolo. | <position=topright> |
| <rotation=value> | Consente di ruotare il testo della filigrana. Il valore è specificato in gradi e l'intervallo è compreso tra -360 e 360. | <rotation=45> |
| <style=value> | Consente di modificare lo stile di visualizzazione. Questo tag sostituisce il criterio di stile della filigrana di sessione. | <style=single> |

Sono disponibili i seguenti stili di filigrana:

- Single style (Stile singolo): al centro della sessione viene visualizzata un'etichetta di testo con filigrana singola. È possibile utilizzare il tag di posizione per modificare la posizione.
- xstyle o multiple: nella sessione vengono visualizzate cinque etichette di filigrana, una al centro e una in ogni angolo.
- Tile (Affianca): nella sessione vengono visualizzate più etichette. Il testo della filigrana viene posizionato in modo uniforme su tutto lo schermo.

I tag disponibili per modificare il testo della filigrana sono descritti nella seguente tabella:

| Tag | Descrizione |
|---|---|
| <clientip> | Indirizzo IP dell'endpoint. |

| Tag | Descrizione |
| --- | --- |
| <date> | Data in cui è stata stabilita la sessione. |
| <domain> | Nome di dominio dell'account utente connesso. |
| <hostname> | Nome della macchina del VDA. |
| <newline> | Crea una linea aggiuntiva. |
| <serverip> | Indirizzo IP del VDA. |
| <time> | Ora in cui è stata stabilita la sessione. |
| <username> | Nome dell'utente. |

> **Nota:**
>
> - Il criterio **Watermark custom text** (Testo filigrana personalizzato) ha effetto solo quando è abilitato il criterio **Enable session watermark** (Abilita filigrana di sessione). Il suo valore predefinito è *Disabled*.
> - Se si utilizzano i tag per modificare il testo della filigrana, tutti gli altri criteri della filigrana di sessione, a eccezione di **Enable session watermark**, vengono ignorati. Se si utilizzano i tag per le impostazioni del testo della filigrana, è possibile utilizzare tutti gli altri criteri di filigrana.

### Watermark transparency (Trasparenza filigrana)

È possibile specificare l'opacità della filigrana da 0 a 100. Maggiore è il valore specificato, più opaca è la filigrana.

Per impostazione predefinita, il valore è 17.

## Impostazioni dei criteri di controllo del fuso orario

January 7, 2024

La sezione **Time Zone Control** (Controllo fuso orario) include le impostazioni dei criteri relative all'utilizzo dell'ora locale nelle sessioni.

### Estimate local time for legacy clients (Stima l'ora locale per i client legacy)

Questa impostazione abilita o disabilita la stima del fuso orario locale da parte dei dispositivi utente. Questi dispositivi includono i dispositivi utente che inviano informazioni errate sul fuso orario al server.

Per impostazione predefinita, il server stima il fuso orario locale quando necessario.

Questa impostazione è destinata all'utilizzo con Citrix Receiver legacy o client ICA che non inviano informazioni dettagliate sul fuso orario al server. Si consideri che questa impostazione viene utilizzata con i Citrix Receiver che inviano informazioni dettagliate sul fuso orario al server. Ad esempio, le versioni supportate di Citrix Receiver per Windows. In questo caso, questa impostazione non ha alcun effetto.

### Restore desktop OS time zone on session disconnect or logoff (Ripristina fuso orario del sistema operativo desktop alla disconnessione della sessione o all'uscita dal sistema)

Si consideri che l'utente disconnetta o scolleghi una sessione. In questo caso, questa impostazione determina se l'impostazione del fuso orario per un VDA per sistema operativo a sessione singola viene riportata al fuso orario originale della macchina. Se si abilita questa impostazione, il VDA ripristina il fuso orario della macchina all'impostazione originale quando l'utente si disconnette o esce dal sistema. Per rendere effettiva questa impostazione, impostare **Use local time of client** (Usa ora locale del client) su **Use client time zone** (Usa fuso orario client).

Per impostazione predefinita, questa impostazione è abilitata.

### Use local time of client (Usa ora locale del client)

Questa impostazione determina l'impostazione del fuso orario della sessione utente. Le scelte sono il fuso orario della sessione utente (fuso orario del server) o il fuso orario del dispositivo utente (fuso orario del client).

Per impostazione predefinita, viene utilizzato il fuso orario della sessione utente.

Per rendere effettiva questa impostazione, abilitare l'impostazione **Allow time zone redirection** (Consenti reindirizzamento fuso orario) nell'Editor Criteri di gruppo. L'impostazione è in **Criteri del computer locale** > **Configurazione computer** > **Modelli amministrativi** > **Componenti di Windows** > **Servizi Desktop remoto** > **Host sessione Desktop remoto** > **Reindirizzamento dispositivi e risorse**.

Se si utilizza un VDA a sessione singola (precedentemente noto come Workstation VDA) su macchine che eseguono un sistema operativo server, configurare il diritto utente locale **Change the time zone**

(Modifica fuso orario) su **Everyone** (Tutti). Questo diritto utente è disponibile in **Criteri computer locale** > **Configurazione computer** > **Impostazioni Windows** > **Impostazioni sicurezza** > **Criteri locali** > **Assegnazione diritti utente**.

> **Nota:**
>
> In un sistema operativo a sessione singola, gli **utenti** sono inclusi in Assegnazione diritti utente **Modifica il fuso orario**, ma non in un sistema operativo multisessione. In un sistema operativo multisessione, il fuso orario viene sincronizzato utilizzando i seguenti criteri di gruppo: Configurazione computer\Modelli amministrativi\Componenti di Windows\Servizi Desktop remoto\Host sessione Desktop remoto\Reindirizzamento dispositivi e risorse\Consenti reindirizzamento fuso orario. Questo criterio non si applica quando il server non è un host di sessione Desktop remoto nel VDA per sistema operativo multisessione (installato con il comando `/ServerVDI`). In un sistema operativo multisessione, per impostazione predefinita e per progettazione, gli utenti non hanno il diritto locale di modificare il fuso orario.

## Impostazioni dei criteri dei dispositivi TWAIN

January 7, 2024

La sezione **Dispositivi TWAIN** include le impostazioni dei criteri relative a quanto segue:

- Mappatura dei dispositivi TWAIN client, come fotocamere digitali o scanner
- Ottimizzazione dei trasferimenti di immagini dal server al client

> **Nota:**
>
> TWAIN 2.0 è supportato con Citrix Receiver per Windows 4.5.

### Client TWAIN device redirection (Reindirizzamento del dispositivo TWAIN client)

I dispositivi TWAIN comunicano con le applicazioni di elaborazione delle immagini ospitate dal server utilizzando il protocollo TWAIN.

Questa impostazione consente o impedisce agli utenti di accedere ai dispositivi TWAIN sul dispositivo utente. Per impostazione predefinita, il reindirizzamento della periferica TWAIN è consentito.

Le seguenti impostazioni dei criteri sono correlate:

- TWAIN compression level (Livello di compressione TWAIN)
- TWAIN device redirection bandwidth limit (Limite della larghezza di banda per il reindirizzamento dei dispositivi TWAIN)

- TWAIN device redirection bandwidth limit percent (Percentuale del limite della larghezza di banda per il reindirizzamento dei dispositivi TWAIN)

### TWAIN compression level (Livello di compressione TWAIN)

Questa impostazione specifica il livello di compressione dei trasferimenti di immagini da client a server. Utilizzare Low (Bassa) per una migliore qualità delle immagini, Medium (Media) per una buona qualità delle immagini o High (Alta) per una bassa qualità delle immagini. Per impostazione predefinita, viene applicata la compressione media.

## Impostazioni dei criteri dei dispositivi USB

January 7, 2024

La sezione **USB devices** (Dispositivi USB) include le impostazioni dei criteri per la gestione del reindirizzamento dei file per i dispositivi USB.

### Regole di ottimizzazione dei dispositivi USB client

Le regole di ottimizzazione dei dispositivi USB client possono essere applicate ai dispositivi per disabilitare l'ottimizzazione o per modificare la modalità di ottimizzazione.

Quando un utente collega un dispositivo di input USB, l'host controlla se le impostazioni dei **criteri USB** consentono il dispositivo. Se il dispositivo è consentito, l'host controlla quindi le **regole di ottimizzazione del dispositivo USB Client** per il dispositivo. Se non viene specificata alcuna regola, il dispositivo non viene ottimizzato. La modalità di acquisizione (04) è la modalità consigliata per i dispositivi di firma. Per altri dispositivi le cui prestazioni sono peggiori con una latenza superiore, gli amministratori possono abilitare la modalità interattiva (02). Vedere le descrizioni delle modalità disponibili nella tabella in questo articolo.

### Considerazioni importanti

- Per l'utilizzo dei signature pad e dei tablet Wacom, si consiglia di disabilitare lo screen saver. I passaggi su come disabilitare lo screen saver sono alla fine di questa sezione.
- Il supporto per l'ottimizzazione dei signature pad e dei tablet Wacom STU è stato preconfigurato nell'installazione dei criteri di Citrix Virtual Apps and Desktops.
- I dispositivi di firma funzionano su Citrix Virtual Apps and Desktops e non richiedono l'utilizzo di un driver come dispositivo di firma. Wacom offre altro software che può essere installato per personalizzare ulteriormente il dispositivo. Vedere http://www.wacom.com/.

- Tablet da disegno. Alcuni dispositivi di input da disegno potrebbero essere presenti come dispositivo HID sui bus PCI/ACPI e non sono supportati. Collegare questi dispositivi su un controller host USB sul client per reindirizzarli all'interno di una sessione Citrix Virtual Desktops.

Le regole dei criteri hanno il formato delle espressioni tag=valore separate da spazi bianchi. Sono supportati i seguenti tag:

| Nome tag | Descrizione |
|---|---|
| Modalità | La modalità di ottimizzazione è supportata per i dispositivi di input per classe =**03**. Le modalità supportate sono: No optimization - value **01** (Nessuna ottimizzazione - valore 01). Interactive mode - value **02** (Modalità interattiva - valore 02). Consigliata per dispositivi come tablet con penna e mouse 3D Pro. Capture mode - value **04** (Modalità di acquisizione - valore 04). Indicata per dispositivi come i signature pad. |
| VID | ID fornitore presente nel descrittore del dispositivo, sotto forma di numero esadecimale di quattro cifre. |
| PID | ID prodotto presente nel descrittore del dispositivo, sotto forma di numero esadecimale di quattro cifre. |
| REV | ID revisione presente nel descrittore del dispositivo, sotto forma di numero esadecimale di quattro cifre. |
| Class | Classe presente nel descrittore del dispositivo o nel descrittore dell'interfaccia. |
| SubClass | Sottoclasse presente nel descrittore del dispositivo o nel descrittore dell'interfaccia. |
| Prot | Protocollo presente nel descrittore del dispositivo o nel descrittore dell'interfaccia. |

### Esempi

Mode=00000004 VID=067B PID=1230 class=03 #Input device operating in capture mode (Il dispositivo di input opera in modalità di acquisizione)

Mode=00000002 VID=067B PID=1230 class=03 #Input device operating in interactive mode (default) (Il dispositivo di input opera in modalità interattiva - impostazione predefinita)

Mode=00000001 VID=067B PID=1230 class=03 #Input device operating without any optimization (Il dispositivo di input opera senza nessuna ottimizzazione)

Mode=00000100 VID=067B PID=1230 # Device setup optimization disabled (default) (Ottimizzazione della configurazione del dispositivo disabilitata - impostazione predefinita)

Mode=00000200 VID=067B PID=1230 # Device setup optimization enabled (Ottimizzazione della configurazione del dispositivo abilitata)

### Disabilitazione dello screen saver per i dispositivi signature pad Wacom

Per l'utilizzo dei signature pad e dei tablet Wacom, Citrix consiglia di disabilitare lo screen saver come segue:

1. Installare il driver **Wacom-STU-Driver** dopo il reindirizzamento del dispositivo.
2. Installare **Wacom-STU-Display MSI** per accedere al pannello di controllo del signature pad.
3. Andare a **Pannello di controllo > Wacom STU Display (Display Wacom STU) > STU430** o **STU530** e selezionare la scheda per il modello in uso.
4. Scegliere **Change** (Cambia), quindi selezionare **Yes** (Sì) quando viene visualizzata la finestra di sicurezza UAC.
5. Selezionare **Disable slideshow** (Disabilita presentazione), quindi **Apply** (Applica).

Dopo aver configurato l'impostazione per un modello di signature pad, questa viene applicata a tutti i modelli.

### Client USB device redirection (Reindirizzamento dei dispositivi USB client)

Questa impostazione consente o impedisce il reindirizzamento dei dispositivi USB da e verso il dispositivo utente.

Per impostazione predefinita, i dispositivi USB non vengono reindirizzati.

### Client USB device redirection rules (Regole di reindirizzamento dei dispositivi USB client)

Questa impostazione specifica le regole di reindirizzamento per i dispositivi USB.

Per impostazione predefinita, non viene specificata alcuna regola.

Quando un utente collega un dispositivo USB, il dispositivo host lo controlla a sua volta in base a ciascuna regola dei criteri fino a quando non viene trovata una corrispondenza. La prima corrispondenza per qualsiasi dispositivo è considerata definitiva. Se la prima corrispondenza è una regola Allow (Consenti), il dispositivo viene trasportato in remoto sul desktop virtuale. Se la prima corrispondenza è

una regola Deny (Vieta), il dispositivo è disponibile solo per il desktop locale. Se non viene trovata alcuna corrispondenza, vengono utilizzate regole predefinite.

Le regole dei criteri hanno il formato {Allow: | Deny:} seguito da un insieme di espressioni tag=value separate da uno spazio bianco. Sono supportati i seguenti tag:

| Nome tag | Descrizione |
|---|---|
| VID | ID fornitore del descrittore del dispositivo |
| PID | ID prodotto del descrittore del dispositivo |
| REL | ID versione del descrittore del dispositivo |
| Class | Classe presente nel descrittore del dispositivo o nel descrittore dell'interfaccia |
| SubClass | Sottoclasse del descrittore del dispositivo o di un descrittore di interfaccia |
| Prot | Protocollo del descrittore del dispositivo o di un descrittore di interfaccia |

Durante la creazione di regole dei criteri, ricordare:

- Le regole non fanno distinzione tra maiuscole e minuscole.
- Le regole possono avere un commento facoltativo alla fine, introdotto da #.
- Le righe di commento vuote e pure vengono ignorate.
- I tag devono utilizzare l'operatore corrispondente = (ad esempio, VID=067B).
- Ogni regola deve iniziare su una nuova riga o far parte di un elenco separato da punto e virgola.
- Vedere i codici delle classi USB disponibili sul sito Web USB Implementers Forum, Inc.

Esempi di regole dei criteri USB definite dall'amministratore:

- Allow: VID=067B PID=0007 # Another Industries, Another Flash Drive
- Deny: Class=08 subclass=05 # Mass Storage
- Per creare una regola che vieta tutti i dispositivi USB, utilizzare "DENY:"senza altri tag.

### Client USB plug and play device redirection (Reindirizzamento del dispositivo plug and play USB client)

Questa impostazione consente o impedisce l'utilizzo di dispositivi plug-and-play come fotocamere o dispositivi POS (Point-of-Sale) in una sessione client.

Per impostazione predefinita, il reindirizzamento del dispositivo plug-and-play è consentito. Se l'opzione è impostata su Allowed (Consentito), tutti i dispositivi plug-and-play per un utente o gruppo

specifico vengono reindirizzati. Se è impostata su Prohibited (Non consentito), non viene reindirizzato nessun dispositivo.

### Configurare il reindirizzamento automatico dei dispositivi USB

I dispositivi USB vengono reindirizzati automaticamente quando è abilitato il supporto USB. Inoltre, le impostazioni delle preferenze utente USB sono impostate per connettere automaticamente i dispositivi USB.

> **Nota:**
>
> In Receiver per Windows 4.2, anche i dispositivi USB vengono reindirizzati automaticamente quando operano in modalità Desktop Appliance. Inoltre, la barra di connessione non è presente. Nelle versioni precedenti di Citrix Receiver per Windows, anche i dispositivi USB vengono reindirizzati automaticamente quando operano nei seguenti modi:
>
> - Modalità appliance desktop
> - Applicazioni ospitate su macchine virtuali (VM)

Reindirizzare tutti i dispositivi USB non è sempre la scelta migliore. Gli utenti possono reindirizzare esplicitamente i dispositivi dell'elenco dei dispositivi USB che non vengono reindirizzati automaticamente. Per evitare che i dispositivi USB vengano elencati o reindirizzati, utilizzare DeviceRules sull'endpoint client o nel criterio DDC. Per ulteriori dettagli, vedere le Guide all'amministrazione.

> **Attenzione:**
>
> l'utilizzo non corretto dell'Editor del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

#### Impostazioni delle preferenze utente per il reindirizzamento automatico dei dispositivi USB

Criterio:

1. Aprire **Editor Criteri di gruppo locali** e andare a **Modelli amministrativi > Componenti Citrix > Citrix Receiver > Uso remoto dei dispositivi client > Uso remoto USB generico**.
2. Aprire **New USB Devices** (Nuovi dispositivi USB), selezionare **Enabled** (Abilitati) e fare clic su **OK**.
3. Aprire **Existing USB Devices** (Dispositivi USB esistenti), selezionare **Enabled** (Abilitati) e fare clic su **OK**.

Citrix Receiver:

1. Andare a **Citrix Receiver Preferences > Connections** (Preferenze Citrix Receiver > Connessioni).
2. Assicurarsi che siano selezionate le seguenti opzioni:
    - When a session starts, connect devices automatically (All'avvio di una sessione, collegare automaticamente i dispositivi)
    - When a new device is connected while a session is running, connect the device automatically (Quando un nuovo dispositivo viene collegato mentre una sessione è in esecuzione, collegarlo automaticamente)
3. Fare clic su **OK**.

Tutte le chiavi del Registro di sistema e le modifiche dei criteri vengono applicate al dispositivo client Windows.

#### Reindirizzamento delle normali stampanti USB

La soluzione migliore per le normali stampanti USB consiste nell'utilizzare il driver della stampante universale dedicato e il canale virtuale per eseguire la stampa. Per impostazione predefinita, le normali stampanti USB non vengono reindirizzate automaticamente.

Le stampanti semplici vengono rilevate utilizzando l'euristica. Inoltre si prevede che le stampanti avanzate con funzioni di scansione, ad esempio, debbano essere reindirizzate utilizzando il supporto USB per un corretto funzionamento.

Utilizzare questa chiave del Registro di sistema per stabilire se le stampanti normali vengono reindirizzate automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectPrinters

Tipo: DWORD

Dati: 00000000

Il valore predefinito è 0 (le stampanti non vengono reindirizzate automaticamente). La modifica del valore su qualsiasi numero maggiore di zero consente al supporto USB di reindirizzare le normali stampanti USB.

È inoltre possibile distribuire i criteri di Active Directory in questa chiave del Registro di sistema e ignorare il valore diverso dai criteri se entrambi sono presenti:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectAudio

Tipo: DWORD

Dati: 00000000

**Reindirizzamento delle normali periferiche audio**

Come per le stampanti normali, la migliore esperienza utente si ottiene utilizzando il canale audio virtuale dedicato di ICA per inviare dati audio da normali dispositivi audio. Tuttavia, potrebbe essere necessario reindirizzare alcuni dispositivi speciali utilizzando il supporto USB. Viene utilizzata l'euristica per determinare quali dispositivi sono dispositivi audio normali.

Utilizzare questa chiave del Registro di sistema per stabilire se i dispositivi audio normali debbano essere reindirizzati automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectAudio

Tipo: DWORD

Dati: 00000000

Il valore predefinito è impostato su 0 (i dispositivi non vengono reindirizzati automaticamente). Modificando il valore su un valore diverso da zero, i normali dispositivi audio USB vengono reindirizzati con supporto USB.

È possibile utilizzare i criteri di Active Directory per distribuire questo valore alla chiave del Registro di sistema e ignorare il valore diverso dai criteri se entrambi sono presenti:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectVideo

Tipo: DWORD

Dati: 00000000

**Reindirizzamento di normali dispositivi di archiviazione (dispositivo di archiviazione di massa)**

Per i normali dispositivi di archiviazione, è possibile ottenere la migliore esperienza utente utilizzando il canale virtuale dedicato, ad esempio la mappatura delle unità client che esegue anche l'ottimizzazione. Oltre alla semplice lettura o scrittura di file, per eseguire determinate attività speciali come la masterizzazione di un CD/DVD o l'accesso a dispositivi di file system crittografati, potrebbe comunque essere necessario reindirizzare il dispositivo utilizzando il supporto USB generico.

Viene utilizzata l'euristica per determinare quali dispositivi sono dispositivi di archiviazione normali. Utilizzare questa chiave del Registro di sistema per stabilire se i dispositivi di archiviazione normali vengono reindirizzati automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectStorage

Tipo: DWORD

Dati: 00000000

Il valore predefinito è impostato su 0 (i dispositivi non vengono reindirizzati automaticamente). Modificando il valore su un valore diverso da zero, i dispositivi di archiviazione USB normali vengono reindirizzati utilizzando il supporto USB generico.

È inoltre possibile utilizzare i criteri di Active Directory per distribuire questo valore alla seguente chiave del Registro di sistema e ignorare il valore diverso dai criteri se entrambi sono presenti:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectStorage

Tipo: DWORD

Dati: 00000000

> **Nota:**
>
> L'accesso in sola lettura al dispositivo di archiviazione normale non è configurabile se si utilizza il supporto USB generico, mentre è configurabile se si utilizza CDM.

#### Unità flash USB con reindirizzamento della crittografia hardware

Le unità flash USB con crittografia hardware solitamente sono composte da una partizione di archiviazione crittografata e una seconda partizione di *utilità* che contiene un'utilità per sbloccare la partizione crittografata. Per i dispositivi USB Flash Drive, è possibile ottenere la migliore esperienza utente utilizzando il canale virtuale HDX dedicato per la mappatura delle unità client/mappatura di thumb drive dinamici, che esegue anche l'ottimizzazione.

Il reindirizzamento USB generico è necessario per quanto segue:

- Client non Windows (ad esempio, client Linux)
- Client in cui il cliente ha limitato (bloccato) l'accesso dell'utente alle funzioni locali del client

Il reindirizzamento USB generico può reindirizzare qualsiasi dispositivo di archiviazione USB senza crittografia hardware in sessioni di sistema operativo a sessione singola e VDA del sistema operativo multisessione.

Prima di Citrix Virtual Apps and Desktops 7 1808, le unità flash USB con crittografia hardware non potevano essere reindirizzate in alcun modo utile in sessioni del sistema operativo a sessione singola o sessioni VDA del sistema operativo multisessione. Un nuovo miglioramento delle funzionalità introdotte in Citrix Virtual Apps and Desktops 7 1808 supporta il reindirizzamento generico USB di unità

flash USB con crittografia hardware in sessioni VDA con sistema operativo a sessione singola e con sistema operativo multisessione.
Dopo il reindirizzamento del dispositivo, nessuna delle relative unità viene visualizzata nel client locale. Quindi, se è necessario sbloccare l'unità, eseguire questa operazione nella sessione. Questa funzionalità richiede l'aggiornamento di Windows KB4074590.

#### Dispositivi normali per immagini fisse (scanner e fotocamere digitali)

Per i dispositivi normali per immagini fisse, è possibile ottenere la migliore esperienza utente utilizzando il canale virtuale dedicato (come il canale virtuale TWAIN), che esegue anche l'ottimizzazione. Questi dispositivi devono rispettare gli standard di settore. Considerare che un dispositivo non è conforme o non viene utilizzato secondo le intenzioni originali. In questo caso, il reindirizzamento USB generico potrebbe essere l'unico modo per utilizzare il dispositivo. Viene utilizzata l'euristica per determinare quali dispositivi sono dispositivi normali per immagini fisse.

Utilizzare questa chiave del Registro di sistema per stabilire se i dispositivi normali per immagini fisse vengono reindirizzati automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectImage

Tipo: DWORD

Dati: 00000000

Il valore predefinito è impostato su 0 (i dispositivi non vengono reindirizzati automaticamente). Modificando il valore su un valore diverso da zero, i dispositivi USB normali per immagini fisse vengono reindirizzati tramite USB generico.

È inoltre possibile utilizzare i criteri di Active Directory per distribuire questo valore in questa chiave del Registro di sistema e ignorare il valore diverso dai criteri se entrambi sono presenti:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectImage

Tipo: DWORD

Dati: 00000000

#### Impostazioni specifiche del dispositivo

Le euristiche utilizzate per selezionare i dispositivi ottimizzabili Citrix non sempre corrispondono a ciò che si desidera. Gli esempi di dispositivi ottimizzabili Citrix sono stampanti, audio, video, dispositivi di archiviazione e immagini fisse. Si potrebbe voler controllare il reindirizzamento automatico

di dispositivi che non sono elencati sopra. È possibile controllare il reindirizzamento automatico in modo specifico per ciascun dispositivo.

Ad esempio, il lettore di codici a barre DemoTech 2.000 non ha bisogno di essere reindirizzato utilizzando il supporto USB. Ha un identificativo fornitore 12AB e un identificativo prodotto 5678. Questi numeri esadecimali sono reperibili in Gestione dispositivi.

Per evitare che il dispositivo venga reindirizzato automaticamente, creare questa chiave del Registro di sistema specifica per il dispositivo:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Nome: AutoRedirect

Tipo: DWORD

Dati: 00000000

Il valore 0 impedisce che il dispositivo venga reindirizzato automaticamente. Un valore diverso da zero indica che il dispositivo deve essere preso in considerazione per il reindirizzamento automatico (in base alle preferenze dell'utente). È presente un singolo spazio tra l'identificatore del fornitore e l'identificatore del prodotto.

È inoltre possibile distribuire questo valore utilizzando i criteri di Active Directory in questa chiave del Registro di sistema. La chiave sostituisce il valore diverso dal criterio se entrambi sono presenti:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Nome: AutoRedirect

Tipo: DWORD

Dati: 00000000

Le impostazioni di AutoRedirect specifiche del dispositivo hanno la precedenza sui valori più generali di AutoRedirectXXX descritti sopra. L'euristica predefinita per i dispositivi ottimizzati Citrix potrebbe interpretare erroneamente un dispositivo come generico. Pertanto, impostare il valore AutoRedirect specifico del dispositivo su 1 per reindirizzarlo automaticamente.

### Allow existing USB devices to be automatically connected (Consenti la connessione automatica dei dispositivi USB esistenti)

Questa impostazione consente o impedisce ai dispositivi USB esistenti collegati all'endpoint all'inizio di una sessione di connettersi alla sessione remota.

Quando si aggiunge questa impostazione a un criterio, selezionare una delle seguenti opzioni:

- Ask before redirecting available USB devices (Chiedi prima di reindirizzare i dispositivi USB disponibili).
- Do not automatically redirect available USB devices (Non reindirizzare automaticamente i dispositivi USB disponibili).
- Automatically redirect available USB devices (Reindirizza automaticamente i dispositivi USB disponibili).

Per impostazione predefinita, è selezionata l'opzione **Ask before redirecting available USB devices** (Chiedi prima di reindirizzare i dispositivi USB disponibili). A seconda del criterio selezionato, l'opzione selezionata nella sezione **Preferences** > **Devices** del client può essere ignorata o meno.

> **Nota:**
>
> Attualmente, il criterio **Allow existing USB devices to be automatically connected**(Consenti la connessione automatica dei dispositivi USB esistenti) è applicabile solo all'app Citrix Workspace per Windows.

### Allow newly arrived USB devices to be automatically connected (Consenti ai dispositivi USB appena arrivati di connettersi automaticamente)

Questa impostazione consente o impedisce ai dispositivi USB che vengono inseriti nell'endpoint durante una sessione di venire automaticamente connessi alla sessione remota.

Quando si aggiunge questa impostazione a un criterio, selezionare una delle seguenti opzioni:

- Ask before redirecting available USB devices (Chiedi prima di reindirizzare i dispositivi USB disponibili).
- Do not automatically redirect available USB devices (Non reindirizzare automaticamente i dispositivi USB disponibili).
- Automatically redirect available USB devices (Reindirizza automaticamente i dispositivi USB disponibili).

Per impostazione predefinita, è selezionata l'opzione **Ask before redirecting available USB devices** (Chiedi prima di reindirizzare i dispositivi USB disponibili). A seconda del criterio selezionato, l'opzione selezionata nella sezione **Preferences** > **Devices** del client può essere ignorata o meno.

> **Nota:**
>
> Attualmente, il criterio **Allow newly arrived USB devices to be automatically connected**(Consenti la connessione automatica dei dispositivi USB appena arrivati) è applicabile solo all'app Citrix Workspace per Windows.

### Client USB device redirection rules (Version 2) [Regole di reindirizzamento dei dispositivi USB client (versione 2)]

Questa impostazione specifica le regole per filtrare, dividere e connettere automaticamente i dispositivi USB a una sessione remota.

Quando questa impostazione è selezionata, l'host ignora l'impostazione delle *regole di reindirizzamento del dispositivo USB client* adottando le regole del dispositivo configurate in questa impostazione.

Per ulteriori informazioni, vedere Configurare il reindirizzamento dei dispositivi USB compositi.

## Impostazioni dei criteri Elenco di elementi consentiti del canale virtuale

January 7, 2024

L'impostazione dei criteri **Virtual channel allow list** (Elenco di elementi consentiti del canale virtuale) consente di utilizzare un elenco di elementi consentiti che specifica quali canali virtuali possono essere aperti in una sessione ICA.

Se l'opzione è disabilitata, sono consentiti tutti i canali virtuali.

Se è abilitata, sono consentiti solo i canali virtuali Citrix.

Per utilizzare canali virtuali personalizzati o di terze parti, aggiungere i canali virtuali all'elenco. Per aggiungere un canale virtuale all'elenco:

1. Immettere il nome del canale virtuale seguito da una virgola.
2. Immettere il percorso del processo che accede al canale virtuale.

È possibile elencare più percorsi eseguibili e i percorsi sono separati da virgole.

Ad esempio,

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

A partire da Citrix Virtual Apps and Desktops 7 2109, gli elenchi dei canali virtuali consentiti sono abilitati per impostazione predefinita. Per ulteriori informazioni sull'aggiunta di canali virtuali all'elenco dei consentiti, vedere Aggiungere canali virtuali all'elenco dei consentiti

Se si utilizza HDX RealTime Optimization Pack per Skype for Business, aggiungere il canale virtuale all'elenco degli elementi consentiti. Per ulteriori informazioni, vedere la documentazione di HDX RealTime Optimization Pack.

> **Importante:**
>
> Perché l'impostazione abbia effetto, le macchine VDA devono essere riavviate.

Per ulteriori informazioni sui canali virtuali, vedere Canali virtuali ICA.

## Impostazioni dei criteri Visualizzazione

January 7, 2024

La sezione **Visual Display** (Visualizzazione virtuale) include le impostazioni dei criteri per il controllo della qualità delle immagini che vengono inviate dai desktop virtuali al dispositivo utente.

### Profondità di colore preferita per grafiche semplici

Questa impostazione dei criteri è disponibile nei VDA versione 7.6 FP3 e successive. L'opzione a 8 bit è disponibile nei VDA versione 7.12 e successive.

Questa impostazione consente di ridurre la profondità del colore con cui la grafica semplice viene inviata attraverso la rete. L'abbassamento a 8 bit o 16 bit per pixel migliora potenzialmente la reattività nelle connessioni a larghezza di banda ridotta. Tuttavia, questa azione potrebbe determinare un leggero degrado della qualità dell'immagine. La profondità del colore a 8 bit non è supportata quando l'impostazione dei criteri Use video codec for compression (Usa codec video per la compressione) è impostata su **For the entire screen** (Per l'intero schermo).

La profondità di colore preferita predefinita è 24 bit per pixel.

Se l'impostazione a 8 bit viene applicata alla versione 7.11 e precedenti, i VDA ritornano alla profondità di colore a 24 bit (predefinita).

### Target frame rate (Frequenza fotogrammi target)

Questa impostazione specifica il numero massimo di fotogrammi al secondo inviati dal desktop virtuale al dispositivo utente.

Per impostazione predefinita, il valore massimo è 30 fotogrammi al secondo.

L'impostazione di un numero elevato di fotogrammi al secondo (ad esempio, 30) migliora l'esperienza utente, ma richiede una maggiore larghezza di banda. La riduzione del numero di frame al secondo (ad esempio, 10) massimizza la scalabilità del server a scapito dell'esperienza utente. Per i dispositivi utente con CPU più lente, specificare un valore inferiore per migliorare l'esperienza utente.

La massima frequenza di fotogrammi supportata al secondo è 60.

### Qualità visiva

Questa impostazione specifica la qualità visiva desiderata per le immagini visualizzate sul dispositivo utente.

Per impostazione predefinita, questa impostazione è Medium (Media).

Per specificare la qualità delle immagini, scegliere una delle seguenti opzioni:

- **Low** (Bassa): consigliata per reti con larghezza di banda limitata in cui la qualità visiva può essere sacrificata a vantaggio dell'interattività
- **Medium** (Media): offre le migliori prestazioni e la migliore efficienza in termini di larghezza di banda nella maggior parte dei casi d'uso
- **High** (Alta): consigliata se è richiesta una qualità dell'immagine senza perdita di dati dal punto di vista visivo
- **Build to lossless** (Compila per senza perdite): invia immagini con perdita di dati al dispositivo utente durante i periodi di elevata attività di rete e immagini senza perdita di dati dopo la riduzione dell'attività di rete. Questa impostazione migliora le prestazioni rispetto alle connessioni di rete vincolate dalla larghezza di banda
- **Always lossless** (Sempre senza perdita di dati): quando la conservazione dei dati delle immagini è fondamentale, selezionare **Always lossless** (Sempre senza perdita di dati) per assicurarsi che non vengano mai inviati dati senza perdite al dispositivo utente. Ad esempio, quando si visualizzano immagini di raggi X in cui la perdita di qualità non è accettabile.

## Impostazioni dei criteri Immagini in movimento

January 7, 2024

La sezione **Moving images** (Immagini in movimento) contiene impostazioni che consentono di rimuovere o modificare la compressione per le immagini dinamiche.

### Minimum image quality (Qualità minima dell'immagine)

Nota: Per Virtual Delivery Agent 7.x, questa impostazione dei criteri si applica solo quando è abilitata l'impostazione dei criteri Legacy graphics mode (Modalità grafica legacy).

Questa impostazione specifica la qualità minima accettabile dell'immagine per Adaptive Display (Schermo adattivo). Minore è la compressione utilizzata, migliore è la qualità delle immagini visualizzate. Scegliere tra compressione ultra alta, molto alta, alta, normale o bassa.

Per impostazione predefinita, l'opzione è impostata su Normal (Normale).

### Moving image compression (Compressione delle immagini in movimento)

Questa impostazione specifica se Adaptive Display (Schermo adattivo) è abilitato o meno. Adaptive Display (Schermo adattivo) regola automaticamente la qualità dell'immagine dei video e delle diapositive di transizione nelle presentazioni in base alla larghezza di banda disponibile. Con Adaptive Display (Schermo adattivo) abilitato, gli utenti dovrebbero vedere presentazioni fluide senza riduzione della qualità.

Per impostazione predefinita, l'opzione Adaptive Display (Schermo adattivo) è abilitata.

Per le versioni VDA da 7.0 a 7.6, questa impostazione si applica solo quando è abilitata la modalità grafica legacy. Per VDA versione 7.6 FP1 e successive, questa impostazione si applica quando è abilitata la modalità grafica legacy o quando la modalità grafica legacy è disabilitata e non viene utilizzato un codec video per comprimere la grafica.

Quando la modalità grafica legacy è abilitata, la sessione deve essere riavviata prima che le modifiche dei criteri abbiano effetto. Adaptive Display (Schermo adattivo) e Progressive Display (Schermo progressivo) si escludono a vicenda: l'abilitazione di Adaptive Display (Schermo adattivo) disabilita Progressive Display (Schermo progressivo) e viceversa. Tuttavia, sia Progressive Display (Schermo progressivo) che Adaptive Display (Schermo adattivo) possono essere disabilitati contemporaneamente. Progressive Display (Schermo progressivo), essendo una funzionalità legacy, non è consigliato per XenApp o XenDesktop. L'impostazione Progressive threshold Level (Livello soglia progressiva) disabiliterà l'opzione Adaptive Display (Schermo adattivo).

### Progressive compression level (Livello di compressione progressivo)

Nota: Per Virtual Delivery Agent 7.x, questa impostazione dei criteri si applica solo quando è abilitata l'impostazione dei criteri Legacy graphics mode (Modalità grafica legacy).

Questa impostazione fornisce una visualizzazione iniziale meno dettagliata ma più veloce delle immagini.

Per impostazione predefinita, non viene applicata alcuna compressione progressiva.

L'immagine più dettagliata, definita dalla normale impostazione di compressione con perdita di dati, viene visualizzata quando diventa disponibile. Utilizzare la compressione Very High (Molto alta) o Ultra High (Ultra alta) per una migliore visualizzazione della grafica a uso intensivo di larghezza di banda, come le fotografie.

Perché la compressione progressiva sia efficace, il livello di compressione deve essere superiore all'impostazione Lossy compression level (Livello di compressione con perdita di dati).

Nota: l'aumento del livello di compressione associato alla compressione progressiva migliora anche l'interattività delle immagini dinamiche sulle connessioni client. La qualità di un'immagine dinamica, ad esempio un modello tridimensionale rotante, viene temporaneamente ridotta fino a quando l'

immagine smette di muoversi, momento in cui viene applicata la normale impostazione di compressione con perdita di dati.

Le seguenti impostazioni dei criteri sono correlate:

- Progressive compression threshold value (Valore della soglia di compressione progressiva)
- Progressive heavyweight compression (Compressione heavyweight progressiva)

### Progressive compression threshold value (Valore della soglia di compressione progressiva)

Nota: Per Virtual Delivery Agent 7.x, questa impostazione dei criteri si applica solo quando è abilitata l'impostazione dei criteri Legacy graphics mode (Modalità grafica legacy).

Questa impostazione rappresenta la larghezza di banda massima in kilobit al secondo per una connessione a cui viene applicata la compressione progressiva. Viene applicata solo alle connessioni client con larghezza di banda inferiore a questa.

Per impostazione predefinita, il valore di soglia è 2.147.483.647 kilobit al secondo.

Le seguenti impostazioni dei criteri sono correlate:

- Progressive compression threshold value (Valore della soglia di compressione progressiva)
- Progressive heavyweight compression (Compressione heavyweight progressiva)

### Target minimum frame rate (Frequenza fotogrammi target minima)

Questa impostazione specifica la frequenza di fotogrammi minima al secondo che il sistema tenta di mantenere, per le immagini dinamiche, in condizioni di larghezza di banda ridotta.

Per impostazione predefinita, questo valore è impostato su 10fps.

Per le versioni VDA da 7.0 a 7.6, questa impostazione si applica solo quando è abilitata la modalità grafica legacy. Per VDA versione 7.6 FP1 e successive, questa impostazione si applica quando la modalità grafica legacy è disabilitata o abilitata.

## Impostazioni dei criteri per le immagini fisse

January 7, 2024

La sezione **Still Images** (Immagini fisse) contiene impostazioni che consentono di rimuovere o modificare la compressione per le immagini statiche.

### Extra color compression (Compressione extra dei colori)

Questa impostazione abilita o disabilita l'uso della compressione extra dei colori sulle immagini fornite tramite connessioni client limitate nella larghezza di banda, migliorando la reattività tramite la riduzione della qualità delle immagini visualizzate.

Per impostazione predefinita, la compressione extra dei colori è disabilitata.

Se è abilitata, la compressione extra dei colori viene applicata solo quando la larghezza di banda della connessione client è inferiore al valore della soglia di compressione extra dei colori. Quando la larghezza di banda della connessione client è superiore al valore di soglia o quando si seleziona Disabled (Disabilitata), la compressione extra dei colori non viene applicata.

### Extra color compression threshold (Soglia della compressione extra dei colori)

Nota: Per Virtual Delivery Agent 7.x, questa impostazione dei criteri si applica solo quando è abilitata l'impostazione dei criteri Legacy graphics mode (Modalità grafica legacy).

Questa impostazione rappresenta la larghezza di banda massima in kilobit al secondo per una connessione al di sotto della quale viene applicata una compressione extra dei colori. Se la larghezza di banda della connessione client scende al di sotto del valore impostato, viene applicata una compressione extra dei colori, se abilitata.

Per impostazione predefinita, il valore di soglia è 8.192 kilobit al secondo.

### Heavyweight compression (Compressione heavyweight)

Nota: Per Virtual Delivery Agent 7.x, questa impostazione dei criteri si applica solo quando è abilitata l'impostazione dei criteri Legacy graphics mode (Modalità grafica legacy).

Questa impostazione abilita o disabilita la riduzione della larghezza di banda oltre la compressione progressiva senza perdere la qualità dell'immagine utilizzando un algoritmo grafico più avanzato, ma a uso più intensivo della CPU.

Per impostazione predefinita, la compressione heavyweight è disabilitata.

Se abilitata, la compressione heavyweight si applica a tutte le impostazioni di compressione con perdita di dati. È supportata dall'app Citrix Workspace ma non ha alcun effetto su altri plug-in.

Le seguenti impostazioni dei criteri sono correlate:

- Progressive compression level (Livello di compressione progressivo)
- Progressive compression threshold value (Valore della soglia di compressione progressiva)

### Lossy compression level (Livello di compressione con perdita di dati)

Nota: Per Virtual Delivery Agent 7.x, questa impostazione dei criteri si applica solo quando è abilitata l'impostazione dei criteri Legacy graphics mode (Modalità grafica legacy).

Questa impostazione controlla il grado di compressione con perdita di dati utilizzato nelle immagini distribuite tramite connessioni client limitate in termini di larghezza di banda. In questi casi, la visualizzazione di immagini senza compressione può essere lenta.

Per impostazione predefinita, viene selezionata la compressione media.

Per una migliore reattività con immagini a uso intensivo di larghezza di banda, utilizzare una compressione elevata. Nei casi in cui la conservazione dei dati delle immagini è fondamentale, ad esempio quando si visualizzano immagini di raggi X in cui non è accettabile alcuna perdita di qualità, si consiglia di non utilizzare la compressione con perdita di dati.

Impostazione dei criteri correlata: Lossy compression threshold value (Valore della soglia di compressione con perdita di dati)

### Lossy compression threshold value (Valore della soglia di compressione con perdita di dati)

Nota: Per Virtual Delivery Agent 7.x, questa impostazione dei criteri si applica solo quando è abilitata l'impostazione dei criteri Legacy graphics mode (Modalità grafica legacy).

Questa impostazione rappresenta la larghezza di banda massima in kilobit al secondo per una connessione a cui viene applicata la compressione con perdita di dati.

Per impostazione predefinita, il valore di soglia è 2.147.483.647 kilobit al secondo.

L'aggiunta dell'impostazione Lossy compression level (Livello di compressione con perdita di dati) a un criterio e la mancata inclusione di una soglia può migliorare la velocità di visualizzazione di bitmap molto dettagliate, ad esempio le fotografie, su una LAN.

Impostazione dei criteri correlata: Lossy compression level (Livello di compressione con perdita di dati)

## Impostazioni dei criteri WebSockets

January 10, 2024

La sezione **WebSockets** include le impostazioni dei criteri per l'accesso ai desktop virtuali e alle applicazioni ospitate utilizzando l'app Citrix Workspace per HTML5. La funzionalità WebSockets aumenta

la sicurezza e riduce il sovraccarico grazie alla comunicazione bidirezionale tra applicazioni e server basati su browser. La funzionalità esegue questa operazione senza aprire più connessioni HTTP.

### WebSockets connections (Connessioni WebSocket)

Questa impostazione consente o proibisce le connessioni WebSocket.

Per impostazione predefinita, le connessioni WebSocket non sono consentite.

### WebSockets port number (Numero di porta WebSocket)

Questa impostazione identificherà la porta per le connessioni WebSocket in ingresso.

Per impostazione predefinita, il valore è 8008.

### WebSockets trusted origin server list (Elenco dei server di origine attendibili WebSocket)

Questa impostazione fornisce un elenco separato da virgole di server di origine attendibili, in genere l'app Citrix Workspace per il Web, espressi come URL. Il server accetta solo connessioni WebSocket provenienti da uno di questi indirizzi.

Per impostazione predefinita, il carattere jolly * viene utilizzato per considerare attendibili tutti gli URL dell'app Citrix Workspace per il Web.

Se si sceglie di digitare un indirizzo nell'elenco, utilizzare la sintassi seguente:

<protocol>://<Nome di dominio completo dell'host>:[port]

Il protocollo deve essere HTTP o HTTPS. Se la porta non è specificata, viene utilizzata la porta 80 per HTTP e la porta 443 per HTTPS.

Il carattere jolly `*` può essere utilizzato all'interno dell'URL, tranne come parte di un indirizzo IP (`10.105.*.*`).

## Impostazioni dei criteri dei dispositivi WIA

January 7, 2024

La sezione **WIA devices** (Dispositivi WIA) include le impostazioni dei criteri per la gestione del reindirizzamento dello scanner utilizzando Acquisizione di immagini di Windows (WIA).

### Reindirizzamento WIA

I dispositivi WIA, come fotocamere digitali e scanner, comunicano con le applicazioni di elaborazione delle immagini ospitate dal server utilizzando il framework WIA. Questa impostazione consente o impedisce agli utenti di accedere ai dispositivi WIA sul dispositivo utente. Per impostazione predefinita, il reindirizzamento WIA non è consentito.

Per informazioni sui dispositivi compatibili con WIA, vedere dispositivi WIA.

## Funzionalità HDX gestite tramite il Registro di sistema

January 10, 2024

> **Nota:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Per aprire l'Editor del Registro di sistema, eseguire `regedit.exe` sul server. Quindi passare alla chiave del Registro di sistema per aggiungere o modificare le impostazioni.

### Dispositivi

#### Tastiere Bloomberg

Citrix Virtual Apps and Desktops supporta la tastiera Starboard Bloomberg modello 4 e modello 3. Per impostazione predefinita, il supporto della tastiera Bloomberg migliorata è disabilitato.

Per abilitare il supporto della tastiera Bloomberg, impostare il seguente valore del Registro di sistema sulla macchina client prima di avviare una connessione:

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB
- Nome valore: EnableBloombergHID
- Tipo di valore: DWORD
- Dati del valore: 0 = disabilita, 1 = abilita

Per ulteriori informazioni, vedere Tastiera Bloomberg.

### Unità client mappate

Come precauzione di sicurezza, quando un utente accede a Citrix Virtual Apps and Desktops, per impostazione predefinita, il server esegue il mapping delle unità client senza l'autorizzazione di esecuzione dell'utente. Per consentire agli utenti di eseguire i file eseguibili che risiedono sulle unità client mappate, ignorare questa impostazione predefinita modificando il Registro di sistema sul server.

Per consentire l'accesso, modificare il seguente valore del Registro di sistema (creare **CDMSettings** se non esiste):

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings
- Nome del valore: ExecuteFromMappedDrive
- Tipo di valore: DWORD
- Dati del valore: 1 = consenti autorizzazione, 0 = nega autorizzazione sulle unità mappate

Questa modifica ha effetto per le sessioni connesse dopo averla apportata nel Registro di sistema.

Citrix Virtual Apps and Desktops 7 2006 è la prima versione a contenere questa posizione del Registro di sistema. Le versioni precedenti di Citrix Virtual Apps and Desktops utilizzavano una posizione del Registro di sistema diversa.

Per ulteriori informazioni, vedere Client Drive Mapping (Mappatura unità client).

### Penne Microsoft Surface Pro e Surface Book

Citrix Virtual Apps and Desktops supporta la funzionalità penna standard con applicazioni basate su Windows Ink. Per impostazione predefinita, questa funzionalità è abilitata.

Per disabilitare o abilitare questa funzionalità, impostare la seguente chiave del Registro di sistema:

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi
- Nome del valore: DisablePen
- Tipo di valore: DWORD
- Dati del valore: 1 = disabilita, 0 = abilita

Per ulteriori informazioni, vedere Penne Microsoft Surface Pro e Surface Book.

### Windows Image Acquisition application allow list (Elenco di elementi consentiti dell'applicazione Acquisizione di immagini di Windows)

Questa impostazione consente di controllare quali applicazioni sul VDA possono accedere al reindirizzamento dello scanner di Acquisizione di immagini di Windows.

Per impostazione predefinita, nessuna applicazione ha accesso ad Acquisizione di immagini di Windows.

Per regolare Acquisizione di immagini di Windows per le applicazioni sul VDA, creare la seguente impostazione del Registro di sistema:

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix
- Nome del valore: WIAAllowedProcesses

  Selezionare e fare clic con il pulsante destro del mouse su **WIAAllowedProcesses**. Scegliere **New > Multi-String Value** (Nuovo > Valore multistringa) e rinominare il nuovo valore in **AllowProcesses**.
- Dati del valore: immettere il percorso completo e il nome del processo per ogni applicazione che può accedere ad Acquisizione di immagini di Windows. Indicare ogni applicazione su una nuova riga.

Eventuali modifiche a questa impostazione hanno effetto al successivo avvio di una sessione sul VDA.

## Aspetti generali

### Configurare l'accesso automatico al VDA

Questa impostazione consente di abilitare o disabilitare l'impostazione dei criteri Microsoft **Richiedi sempre password** sui VDA con sistema operativo Windows 10 a sessione singola e con sistema operativo multisessione.

Se l'opzione **Richiedi sempre password** è abilitata, gli utenti devono immettere le credenziali sul VDA all'avvio di una sessione remota. Se questa impostazione è disabilitata, gli utenti si connettono automaticamente alla sessione remota senza fornire credenziali sul VDA.

Per impostazione predefinita, l'impostazione dei criteri Microsoft è disabilitata. Per abilitare o disabilitare l'impostazione **Richiedi sempre password**, impostare il seguente valore del Registro di sistema sul VDA:

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica
- Nome del valore: AutoLogon
- Tipo di valore: DWORD
- Dati del valore:
  - 1: disabilita l'impostazione dei criteri Microsoft e consente agli utenti di accedere automaticamente a una sessione remota.
  - 0: abilita l'impostazione dei criteri Microsoft e richiede agli utenti di fornire le credenziali all'avvio di una sessione remota.

### Disable timeout warning (Disabilita avviso di timeout)

Per impostazione predefinita, gli utenti con sessioni inattive o in pausa ricevono un messaggio di avviso due minuti prima della disconnessione automatica della sessione.

Questa impostazione disabilita e rimuove il messaggio di avviso per gli utenti che raggiungono il limite di timeout della sessione inattiva per quanto segue:

- Windows Server 2004
- Sistema operativo multisessione Windows 10 2004 o multisessione successivo

Per rimuovere l'avviso, impostare il seguente valore del Registro di sistema sul VDA:

- Chiave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP
- Nome del valore: fEnableTimeoutWarning
- Tipo di valore: DWORD
- Dati del valore: 1 = disabilita il messaggio di avviso, 0 = abilita il messaggio di avviso

Per visualizzare il messaggio di avviso, eliminare il valore del Registro di sistema o impostarlo su 0.

### EDT MTU Discovery (Rilevamento MTU EDT)

MTU Discovery (Rilevamento MTU) consente a EDT di determinare automaticamente l'unità di trasmissione massima (MTU) quando si stabilisce una sessione. In questo modo si evita la frammentazione dei pacchetti EDT che potrebbe comportare un deterioramento delle prestazioni o l'impossibilità di stabilire una sessione.

Questa impostazione è abilitata per impostazione predefinita. Per disabilitare EDT MTU Discovery, configurare il seguente valore del Registro di sistema e riavviare il VDA.

- Chiave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
- Nome valore: MtuDiscovery
- Tipo di valore: DWORD
- Dati del valore: 0

Questa impostazione è a livello di macchina e influisce su tutte le sessioni che si connettono da un client supportato.

### Abilitare EDT Lossy

È possibile accedere all'audio adattivo utilizzando il protocollo di trasporto con perdita di dati EDT per il servizio audio bidirezionale per CWA per Windows, VDA multiutente e VDA desktop. Questa im-

postazione è disabilitata per impostazione predefinita. Per abilitare EDT Lossy, a seconda del computer in uso, configurare il seguente valore di registro e riavviare il rispettivo computer.

Per l'app Citrix Workspace per il client Windows,

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanc
- Nome del valore: EdtUnreliableAllowed
- Tipo di valore: REG_SZ
- Dati del valore: 1

Per TS VDA,

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio
- Nome del valore: EdtUnreliableAllowed
- Tipo di valore: DWORD
- Dati del valore: 1

Per WS VDA,

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio
- Nome del valore: EdtUnreliableAllowed
- Tipo di valore: DWORD
- Dati del valore: 1

## Reindirizzamento generale del contenuto

### Aggiungere tipi di URL per il reindirizzamento da host a client

Per impostazione predefinita, supportiamo il reindirizzamento dei seguenti tipi di URL: HTTP, HTTPS, RTSP, RTSPU, PNM e MMS. È possibile aggiungere tipi di URL all'elenco creando la chiave del Registro di sistema e i valori seguenti sul client Windows.

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Nome del valore: ExtraURLProtocols
- Tipo di valore: REG_SZ
- Dati valore: specificare i tipi di URL richiesti separati da punto e virgola. Includere tutto prima della parte dell'URL relativa all'autorità. Ad esempio:
  `ftp://;mailto:;customtype1://;custometype2://`

È possibile aggiungere tipi di URL solo per i client Windows. I client che non hanno questa impostazione del Registro di sistema rifiutano il reindirizzamento alla sessione Citrix. Il client deve avere un'applicazione installata e configurata per gestire i tipi di URL specificati.

Per ulteriori informazioni, vedere Reindirizzamento da host a client.

#### Reindirizzamento delle cartelle client

Il reindirizzamento delle cartelle client modifica il modo in cui i file lato client sono accessibili nella sessione lato host. Si consideri che si abilita il reindirizzamento delle cartelle client sul server e l'utente lo configura sul dispositivo utente. In questo caso, la parte del volume locale specificata dall'utente viene reindirizzata.

Per abilitare il reindirizzamento delle cartelle client sul server, impostare il seguente valore del Registro di sistema:

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection
- Nome del valore: CFROnlyModeAvailable
- Tipo di valore: DWORD
- Dati del valore: 1

Per ulteriori informazioni, vedere Reindirizzamento delle cartelle client.

#### Reindirizzamento da host a client per un gruppo specifico di siti Web

Per abilitare il reindirizzamento da host a client per un gruppo specifico di siti Web, impostare il seguente valore del Registro di sistema sul VDA del server.

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome del valore: ValidSites
- Tipo di valore: REG_MULTI_SZ
- Dati del valore: specificare qualsiasi combinazione di nomi di dominio completi (FQDN). Digitare più FQDN su righe separate. Includere solo il nome di dominio completo, senza protocolli (`http://` o `https://`). Un nome di dominio completo può includere un asterisco (*) come carattere jolly solo nella posizione più a sinistra. Questo carattere jolly corrisponde a un singolo livello di dominio, che è coerente con le regole in RFC 6125. Ad esempio:

`www.example.com`

`*.example.com`

Per ulteriori informazioni, vedere Reindirizzamento da host a client.

#### Comportamento dell'applicazione locale allo scollegamento e alla disconnessione

Per impostazione predefinita, le applicazioni locali continuano a funzionare quando un utente si scollega o si disconnette dal desktop virtuale. Dopo la riconnessione, le applicazioni locali vengono reintegrate se sono disponibili sul desktop virtuale. Per configurare il comportamento delle applicazioni locali in caso di scollegamento e disconnessione, impostare il seguente valore del Registro di sistema nel desktop ospitato:

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies
- Nome del valore: Session State (Stato sessione)
- Tipo di valore: DWORD
- Dati del valore:
  - 1: le applicazioni locali continuano a funzionare quando un utente si scollega o si disconnette dal desktop virtuale. Al momento della riconnessione, le applicazioni locali vengono reintegrate se sono disponibili nel desktop virtuale.
  - 3: le applicazioni locali si chiudono quando un utente si scollega o si disconnette dal desktop virtuale.

Per ulteriori informazioni, vedere Accesso alle app locali e reindirizzamento URL.

#### Rimuovere i tipi di URL dall'elenco predefinito per il reindirizzamento da host a client

Per rimuovere i tipi di URL dall'elenco di reindirizzamento predefinito, creare la chiave del Registro di sistema e i valori seguenti sul server VDA.

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome valore: DisableServerFTA
- Tipo di valore: DWORD
- Dati del valore: 1
- Nome valore: NoRedirectClasses
- Tipo di valore: REG_MULTI_SZ
- Dati del valore: specificare qualsiasi combinazione di valori: `http`,`https`, `rtsp`, `rtspu`, `pnm` o `mms`. Digitare più valori su righe separate. Ad esempio:

```
http
https
rtsp
```

Per ulteriori informazioni, vedere Reindirizzamento da host a client.

#### Configurazione predefinita del browser del server VDA

È possibile abilitare il reindirizzamento da host a client per sostituire qualsiasi configurazione predefinita del browser sul server VDA. Se un URL Web non viene reindirizzato, Citrix Launcher trasferisce l'URL al browser configurato nella chiave del Registro di sistema `command_backup`. La chiave punta a Internet Explorer per impostazione predefinita, ma è possibile modificarla per includere il percorso a un browser diverso.

- Internet Explorer (impostazione predefinita)
  - Chiave: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - Nome valore: predefinito
  - Tipo di valore: REG_SZ
  - Dati del valore: `"c:\program files\internet explorer\iexplore.exe""%1"`
  - Chiave: HKEY_CLASSES_ROOT\https\shell\open\command_backup‘
  - Nome valore: predefinito
  - Tipo di valore: REG_SZ
  - Dati del valore: `"c:\program files\internet explorer\iexplore.exe""%1"`
- Google Chrome
  - Chiave: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - Nome valore: predefinito
  - Tipo di valore: REG_SZ
  - Dati del valore: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe""%1"`
  - Chiave: HKEY_CLASSES_ROOT\https\shell\open\command_backup
  - Nome valore: predefinito
  - Tipo di valore: REG_SZ
  - Dati del valore: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe""%1"`
- Microsoft Edge
  - Chiave: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - Nome valore: predefinito
  - Tipo di valore: REG_SZ
  - Dati del valore: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe""%1"`
  - Chiave: HKEY_CLASSES_ROOT\https\shell\open\command_backup
  - Nome valore: predefinito

- Tipo di valore: REG_SZ
- Dati del valore: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe""%1"`

#### Accesso alle app locali per le applicazioni pubblicate

L'accesso alle app locali integra perfettamente le applicazioni Windows installate localmente in un ambiente desktop ospitato senza passare da un desktop all'altro. Per fornire l'accesso alle applicazioni pubblicate, impostare il seguente valore del Registro di sistema sul server:

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio
- Nome del valore: ClientHostedAppsEnabled
- Tipo di valore: DWORD
- Dati del valore: 1 = abilita, 0 = disabilita

Per ulteriori informazioni, vedere Accesso alle app locali e reindirizzamento URL.

### Grafica

#### Accelerazione GPU per applicazioni CUDA o OpenCL

L'accelerazione GPU delle applicazioni CUDA e OpenCL in esecuzione in una sessione utente è disabilitata per impostazione predefinita.

Per utilizzare le funzionalità POC dell'accelerazione CUDA, abilitare la seguente impostazione del Registro di sistema:

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper
- Nome del valore: CUDA
- Tipo di valore: DWORD
- Dati del valore: 00000001

Per utilizzare le funzionalità POC di accelerazione OpenCL, abilitare la seguente impostazione del Registro di sistema:

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper
- Nome del valore: OpenCL
- Tipo di valore: DWORD
- Dati del valore: 00000001

Per ulteriori informazioni, vedere Accelerazione GPU per sistema operativo multisessione Windows

#### Progressive mode (Modalità progressiva)

La modalità progressiva è disabilitata per impostazione predefinita. È possibile modificare lo stato della modalità progressiva con il seguente valore del Registro di sistema:

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Tipo di valore: REG_DWORD
- Nome del valore: ProgressiveDisplay
- Dati del valore:
  - 0 = sempre disabilitato (disabilita la modalità progressiva; questo è il valore predefinito)
  - 1 = automatico (abilitato/disabilitato in base alle condizioni della rete)
  - 2 = sempre abilitato

Per ulteriori informazioni, vedere Modalità progressiva.

#### Rendering Windows Presentation Foundation (WPF)

HDX 3D Pro consente di eseguire il rendering di applicazioni ad utilizzo intensivo di grafica in esecuzione in sessioni di sistema operativo multisessione Windows sulla GPU (unità di elaborazione grafica) del server. Spostando il rendering WPF (Windows Presentation Foundation) sulla GPU del server, il rendering grafico non rallenta la CPU del server.

Per abilitare il rendering delle applicazioni WPF utilizzando la GPU del server, creare la seguente impostazione nel Registro di sistema del server che esegue un sistema operativo Windows multisessione:

1. Aprire l'editor del Registro di sistema sul VDA e accedere alla seguente chiave:

   ```
   HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper
   ```

2. Creare o modificare i seguenti valori di registro:

   - [REG_DWORD] AdapterHandle = 0x00000001
   - [REG_DWORD] DevicePath = 0x00000001
   - [REG_DWORD] Flag = 0x00000412
   - [REG_DWORD] WPF = 0x00000001

3. Creare una sottochiave con il nome dell'eseguibile dell'app WPF. Ad esempio, se l'app si chiama "mywpfapp.exe", creare la seguente chiave:

   ```
   HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp
   .exe
   ```

4. Riavviare il server per rendere effettive le impostazioni.

Per ulteriori informazioni, vedere Accelerazione GPU per il sistema operativo Windows multisessione e il blog su Getting the best out of WPF apps on Windows multi-session OS (Ottenere il meglio dalle app WPF sul sistema operativo multisessione Windows).

## Contenuti multimediali

### Evitare l'eco durante le conferenze multimediali

Citrix Virtual Apps and Desktops offre un'opzione di cancellazione dell'eco che riduce al minimo qualsiasi eco. Questa funzionalità è abilitata per impostazione predefinita. Per disabilitare la cancellazione dell'eco, è possibile modificare una delle seguenti impostazioni del Registro di sistema:

- Chiave:
  - 32 bit: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules
  - 64 bit: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Adv
- Nome del valore: EchoCancellation
- Tipo di valore: DWORD
- Dati del valore: False

Per ulteriori informazioni, vedere Funzionalità audio.

### Limitazione audio

Dopo aver installato un dispositivo audio sul client, abilitare il reindirizzamento audio e avviare una sessione RDS, i file audio potrebbero non riprodurre l'audio. Come soluzione alternativa, aggiungere la seguente chiave del Registro di sistema sul computer RDS, quindi riavviare la macchina:

- Chiave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig
- Nome del valore: EnableSvchostMitigationPolicy
- Tipo di valore: DWORD
- Dati del valore: 0

Per ulteriori informazioni, vedere Funzionalità audio.

### Reindirizzamento del contenuto del browser e DPI

Quando si utilizza il reindirizzamento del contenuto del browser con DPI (ridimensionamento) impostato su un valore superiore a 100% sulla macchina dell'utente, la schermata del contenuto del

browser reindirizzato viene visualizzata in modo errato. Per evitare il problema, disabilitare l'accelerazione della GPU per il reindirizzamento del contenuto del browser per Chrome creando il seguente valore del Registro di sistema sulla macchina dell'utente:

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- Nome del valore: GPU
- Tipo di valore: DWORD
- Dati del valore: 0

Per ulteriori informazioni, vedere Reindirizzamento del contenuto del browser e DPI.

#### Streaming della webcam ad alta definizione

L'applicazione di videoconferenza sul server seleziona il formato e la risoluzione della webcam in base ai tipi di formato supportati. Citrix Virtual Apps and Desktops supporta risoluzioni della webcam fino a 1920x1080. Per disabilitare e abilitare lo streaming della webcam ad alta definizione, aggiungere il seguente valore del Registro di sistema:

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXRealTime
- Nome del valore: Enable_HighDefWebcam
- Tipo di valore: DWORD
- Dati del valore:
  - 0 = disabilita lo streaming della webcam ad alta definizione
  - 1 = abilita lo streaming della webcam ad alta definizione

#### Risoluzione della webcam ad alta definizione

Se la negoziazione del tipo di contenuti multimediali non riesce, HDX torna alla risoluzione predefinita di 352x288 CIF. È possibile utilizzare le chiavi del Registro di sistema nel client per configurare la risoluzione predefinita. Prima di impostare le seguenti chiavi del Registro di sistema, assicurarsi che la fotocamera supporti la risoluzione specificata.

- Chiave: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- Larghezza
  - Nome del valore: DefaultWidth
  - Tipo di valore: DWORD
  - Dati del valore: larghezza desiderata espressa in numeri decimali (ad esempio 1280)
- Altezza
  - Nome del valore: DefaultHeight

  - Tipo di valore: DWORD
  - Dati del valore: altezza desiderata espressa in numeri decimali (ad esempio 720)

#### Larghezza di banda della webcam ad alta definizione

La compressione video della webcam HDX utilizza una larghezza di banda significativamente inferiore rispetto al reindirizzamento USB generico plug-n-play e funziona bene sulle connessioni WAN. Per regolare la larghezza di banda, impostare il seguente valore del Registro di sistema sul client:

- Chiave: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- Nome del valore: TargetBitrate
- Tipo di valore: DWORD
- Dati del valore: 350.000

Immettere un valore in bit al secondo. Se non si specifica la larghezza di banda, le applicazioni di videoconferenza utilizzano 350.000 bps per impostazione predefinita.

Per ulteriori informazioni, vedere Compressione del video della webcam HDX.

#### Modalità di fallback di Microsoft Teams

Se Microsoft Teams non riesce a caricarsi in modalità VDI ottimizzata ("Citrix HDX Not Connected"[Citrix HDX non connesso] in Teams/Informazioni/Versione), il VDA torna a utilizzare le tecnologie HDX legacy come il reindirizzamento della webcam e il reindirizzamento del microfono e dell'audio del client. Se si utilizza una versione dell'app Workspace/un sistema operativo della piattaforma che non supporta l'ottimizzazione di Microsoft Teams, le chiavi del Registro di sistema di fallback non si applicano.

Per controllare il meccanismo di fallback, impostare uno dei seguenti valori del Registro di sistema sul VDA:

- Chiave (solo una necessaria):
  - **Impostazione del computer:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams
  - **Impostazione utente:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams
- Nome del valore: DisableFallback
- Tipo di valore: DWORD
- Dati del valore: 1 = disabilita la modalità di fallback, 2 = abilita solo l'audio

Se il valore non è presente o è impostato su 0, la modalità di fallback è abilitata. Questa funzionalità richiede Microsoft Teams versione 1.3.0.13565 o successiva. Per ulteriori informazioni, vedere Ottimizzazione per Microsoft Teams.

### Ottimizzazione per Microsoft Teams con Citrix App Layering

Se si utilizza Citrix App Layering per gestire le installazioni di VDA e Microsoft Teams in livelli diversi, creare una chiave di registro vuota denominata **PortICA** su Windows prima di installare Microsoft Teams con il flag `ALLUSER=1` dalla riga di comando. Lasciare il nome, il tipo e i dati del valore predefinito.

- Chiave per la versione a 32 bit dell'Editor del Registro di sistema: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6
- Chiave per la versione a 64 bit dell'Editor del Registro di sistema: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\

Per ulteriori informazioni, vedere Ottimizzazione per Microsoft Teams.

### Single Sign-on con Autenticazione integrata di Windows per il reindirizzamento del contenuto del browser

Questa impostazione fornisce il Single Sign-on a un server Web configurato con Autenticazione integrata di Windows (IWA) all'interno dello stesso dominio del VDA. Per abilitare il Single Sign-on, impostare il seguente valore del Registro di sistema su 1:

- Chiave:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream

  o
  - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\HdxMediastream
- Nome del valore: WebBrowserRedirectionIwaSupport
- Tipo di valore: DWORD
- Dati del valore: 1

Per ulteriori informazioni, vedere Single Sign-on con autenticazione integrata di Windows.

### Intestazione della richiesta utente-agente

L'intestazione utente-agente aiuta a identificare le richieste HTTP inviate dal reindirizzamento del contenuto del browser. Questa impostazione può essere utile quando si configurano le regole proxy e firewall. Ad esempio, se il server blocca le richieste inviate dal reindirizzamento del contenuto del browser, è possibile creare una regola che contiene l'intestazione utente-agente per ignorare determinati requisiti. Solo i dispositivi Windows supportano l'intestazione della richiesta utente-agente.

Per impostazione predefinita, la stringa di intestazione della richiesta utente-agente è disabilitata. Per abilitare l'intestazione utente-agente per il contenuto con rendering sul client, utilizzare l'editor del Registro di sistema.

Su ogni app Citrix Workspace per client Windows, configurare una delle seguenti impostazioni del Registro di sistema:

- Chiave:
  - 32 bit: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStream
  - 64 bit: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- Nome del valore: EnableCefUserAgentString
- Tipo di valore: DWORD
- Dati del valore: 1

Dopo aver aggiunto il valore del Registro di sistema, l'intestazione utente-agente contiene il testo CitrixBCR/2102.1, dove 2102.1 è l'app Citrix Workspace per Windows.

#### Compressione del software della webcam

Se una webcam supporta la codifica hardware, la compressione video HDX utilizza la codifica hardware per impostazione predefinita. La codifica hardware potrebbe consumare più larghezza di banda rispetto alla codifica software. Per forzare la compressione software, aggiungere il seguente valore sul client:

- Chiave: HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime
- Nome del valore: DeepCompress_ForceSWEncode
- Tipo di valore: DWORD
- Dati del valore: 1

Per ulteriori informazioni, vedere Compressione del video della webcam HDX.

#### Compressione video della webcam

La compressione del video della webcam HDX invia il video H.264 direttamente all'applicazione di videoconferenza in esecuzione nella sessione virtuale. Per ottimizzare le risorse VDA, la compressione della webcam HDX non codifica, transcodifica e decodifica i video della webcam. Questa funzionalità è abilitata per impostazione predefinita.

Per disabilitare lo streaming video diretto dal server all'app per videoconferenze, impostare il seguente valore del Registro di sistema nel VDA.

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime
- Nome del valore: OfferH264ToApp
- Tipo di valore: DWORD
- Dati del valore: 0

Per ulteriori informazioni, vedere Compressione del video della webcam HDX.

#### Frequenza dei fotogrammi di compressione video della webcam

Per regolare la frequenza dei fotogrammi video preferita, modificare il seguente valore del Registro di sistema sul client:

- Chiave: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- Nome del valore: FramesPerSecond
- Tipo di valore: DWORD
- Dati del valore: 15

Se la webcam non supporta la frequenza dei fotogrammi specificata, l'applicazione utilizza 15 FPS per impostazione predefinita.

Per ulteriori informazioni, vedere Compressione del video della webcam HDX.

## Impostazioni dei criteri di gestione del carico

January 7, 2024

La sezione **Load Management** (Gestione del carico) include le impostazioni dei criteri per l'abilitazione e la configurazione della gestione del carico tra i server che distribuiscono macchine con sistema operativo Windows multisessione.

Per informazioni sul calcolo dell'indice di valutazione del carico, vedere CTX202150.

### Concurrent logon tolerance (Tolleranza agli accessi simultanei)

Questa impostazione specifica il numero massimo di accessi simultanei accettabili da un server.

Per impostazione predefinita, tale valore è impostato su 2.

Quando questa impostazione è abilitata, il bilanciamento del carico cerca di evitare di avere un numero di accessi attivi superiore al numero specificato su un VDA server contemporaneamente. Tuttavia, il limite non è rigorosamente applicato. Per applicare il limite (e impedire che gli accessi simultanei che superano il numero specificato vadano a buon fine), creare la seguente chiave del Registro di sistema:

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit
> Tipo: DWORD
> Valore: 1

### CPU usage (Utilizzo della CPU)

Questa impostazione specifica il livello di utilizzo della CPU, in percentuale, al quale il server segnala un carico completo. Quando è abilitata, il valore predefinito con cui il server segnala un carico completo è del 90%.

Per impostazione predefinita, questa impostazione è disabilitata e l'utilizzo della CPU è escluso dai calcoli del carico.

### CPU usage excluded process priority (Priorità dei processi escluso l'utilizzo della CPU)

> **Nota:**
>
> Negli scenari in cui Workspace Environment Management gestisce le macchine, l'utilizzo di questa impostazione insieme alle impostazioni CPU Priority (Priorità della CPU) può avere risultati inattesi. Si consiglia di disabilitare questa impostazione se si sceglie di utilizzare le impostazioni CPU Priority (Priorità CPU).

Questa impostazione specifica il livello di priorità al quale l'utilizzo della CPU di un processo è escluso dall'indice di carico di utilizzo della CPU.

Per impostazione predefinita, questo valore è impostato su **Below Normal** (Sotto il normale) o su **Low** (Bassa).

### Disk usage (Utilizzo del disco)

Questa impostazione specifica la lunghezza della coda del disco alla quale il server segnala un carico completo al 75%. Se è abilitata, il valore predefinito per la lunghezza della coda del disco è 8.

Per impostazione predefinita, questa impostazione è disabilitata e l'utilizzo del disco è escluso dai calcoli del carico.

### Maximum number of sessions (Numero massimo di sessioni)

Questa impostazione specifica il numero massimo di sessioni che un server può ospitare. Se è abilitata, l'impostazione predefinita per il numero massimo di sessioni che un server può ospitare è 250.

Per impostazione predefinita, questa impostazione è abilitata.

### Memory usage (Utilizzo della memoria)

Questa impostazione specifica il livello di utilizzo della memoria, in percentuale, al quale il server segnala un carico completo. Quando è abilitata, il valore predefinito con cui il server segnala un carico completo è del 90%.

Per impostazione predefinita, questa impostazione è disabilitata e l'utilizzo della memoria è escluso dai calcoli del carico.

### Memory usage base load (Carico base dell'utilizzo della memoria)

Questa impostazione specifica un'approssimazione dell'utilizzo della memoria del sistema operativo di base. Inoltre definisce, in MB, l'utilizzo della memoria al di sotto del quale un server è considerato con carico zero.

Per impostazione predefinita, questo valore è impostato su 768 MB.

## Impostazioni dei criteri di Profile Management

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per abilitare e configurare Profile Management.

Per altre informazioni, ad esempio le seguenti, vedere Criteri di Profile Management:

- Nomi dell'impostazione equivalente del file .ini
- Quale versione di Profile Management è richiesta per l'impostazione di un criterio

## Impostazioni avanzate dei criteri

January 7, 2024

### Number of retries when accessing locked files (Numero di tentativi durante l'accesso ai file bloccati)

Imposta il numero di tentativi durante l'accesso ai file bloccati.

Se questo criterio è disabilitato, viene utilizzato il valore predefinito di cinque tentativi. Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, viene utilizzato il valore predefinito.

### Process Internet cookie files on logoff (Elabora file dei cookie Internet allo scollegamento)

Alcune distribuzioni lasciano cookie Internet aggiuntivi a cui `Index.dat` non fa riferimento. I cookie extra lasciati nel file system dopo la navigazione prolungata possono portare a un sovraccarico del profilo. Questo criterio consente di abilitare Profile Management per forzare l'elaborazione di Index.dat e rimuovere i cookie aggiuntivi. Il criterio aumenta i tempi di scollegamento, quindi abilitarlo solo dopo che si è verificato questo problema.

Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato né qui né nel file .ini, non viene eseguita alcuna elaborazione di Index.dat.

### Disable automatic configuration (Disabilita configurazione automatica)

Profile Management esamina qualsiasi ambiente Citrix Virtual Desktops, ad esempio la presenza di Personal vDisk, e configura i Criteri di gruppo di conseguenza. Vengono modificati solo i criteri di Profile Management nello stato Not Configured (Non configurato), in modo che le personalizzazioni eseguite vengano mantenute.

Questo criterio consente di velocizzare la distribuzione e semplificare l'ottimizzazione. Non è necessario configurare questo criterio. Tuttavia, è possibile disabilitare la configurazione automatica quando si effettua una delle seguenti operazioni:

- Aggiornare per mantenere le impostazioni delle versioni precedenti
- Risoluzione dei problemi

È possibile considerare la configurazione automatica come un controllo della configurazione dinamico che configura automaticamente le impostazioni predefinite dei criteri in base agli ambienti al runtime. Elimina la necessità di configurare manualmente le impostazioni. Gli ambienti di runtime includono:

- Sistema operativo Windows
- Versioni del sistema operativo Windows
- Presenza di Citrix Virtual Desktops
- Presenza di Personal vDisk

La configurazione automatica potrebbe modificare i criteri seguenti se l'ambiente cambia:

- Write-back attivo
- Always cache (Memorizza sempre nella cache)
- Delete locally cached profiles on logoff (Elimina i profili memorizzati nella cache locale allo scollegamento)

- Delay before deleting cached profiles (Attendi prima di eliminare i profili memorizzati nella cache)
- Profile streaming (Streaming del profilo)

Vedere la tabella seguente per lo stato predefinito dei criteri sui diversi sistemi operativi:

| | Sistema operativo multisessione | Sistema operativo a sessione singola |
|---|---|---|
| Active write back (Scrittura attiva) | Abilitato | *Disabilitato* se si utilizza Personal vDisk, altrimenti è abilitato. |
| Always cache (Memorizza sempre nella cache) | Disabilitato | *Disabilitato* se si utilizza Personal vDisk, altrimenti è abilitato. |
| Delete locally cached profiles on logoff (Elimina i profili memorizzati nella cache locale allo scollegamento) | Abilitato | *Disabled* se si verifica una delle seguenti situazioni: Personal vDisk è in uso, Citrix Virtual Desktops è assegnato o Citrix Virtual Desktops non è installato; altrimenti, abilitato. |
| Delay before deleting cached profiles (Attendi prima di eliminare i profili memorizzati nella cache) | 0 secondi | 60 secondi se le modifiche dell'utente non sono persistenti, altrimenti 0 secondi. |
| Profile streaming (Streaming del profilo) | Abilitato | *Disabilitato* se si utilizza Personal vDisk, altrimenti è abilitato. |

Tuttavia, con la configurazione automatica disabilitata, tutti i criteri di cui sopra sono impostati su **Disabled** (Disabilitato).

> **Importante:**
>
> Personal vDisk è stato deprecato. Per ulteriori informazioni, vedere Rimuovere PVD, AppDisk e host non supportati.

A partire da Profile Management 1909, è possibile ottenere un'esperienza migliorata con il menu Start di Windows 10 (versione 1607 e successive) e Windows Server 2016 e versioni successive. Questo miglioramento si ottiene attraverso la configurazione automatica dei seguenti criteri:

- Aggiungere `Appdata\Local\Microsoft\Windows\Caches` e `Appdata\Local\Packages` alle **Folders to Mirror** (Cartelle di cui eseguire il mirroring).
- Aggiungere `Appdata\Local\Microsoft\Windows\UsrClass.Dat*`ai **Files to synchronize** (File da sincronizzare).

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata né qui né nel file .ini, la configurazione automatica è attivata. In questo caso, le impostazioni di Profile Management potrebbero cambiare se l'ambiente cambia.

### Log off user if a problem is encountered (Scollega l'utente se si verifica un problema)

Consente di specificare se Profile Management deve disconnettere gli utenti in caso di problemi.

Se questo criterio è disabilitato o non configurato, Profile Management assegna un profilo temporaneo agli utenti in caso di problemi. Ad esempio, se lo store utenti non è disponibile.

Se è abilitato, viene visualizzato un messaggio di errore e gli utenti vengono disconnessi. Questa configurazione può semplificare la risoluzione del problema.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata né qui né nel file .ini, viene fornito un profilo temporaneo.

### Programma di miglioramento dell'esperienza cliente

Per impostazione predefinita, il Programma di miglioramento dell'esperienza cliente consente di migliorare la qualità e le prestazioni dei prodotti Citrix raccogliendo statistiche anonime e dati sull'utilizzo.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

### Enable search index roaming for Outlook (Abilita il roaming dell'indice di ricerca per Outlook)

Consentire l'esperienza di ricerca di Outlook basata sull'utente tramite il roaming automatico dei dati di ricerca di Outlook insieme al profilo utente. Questa funzione richiede spazio aggiuntivo nello store dell'utente per archiviare gli indici di ricerca per Outlook.

Perché questo criterio abbia effetto, scollegarsi e quindi eseguire nuovamente l'accesso.

## Outlook search index database –backup and restore (Database degli indici di ricerca di Outlook: backup e ripristino)

Consente di specificare come si deve comportare Profile Management durante l'accesso quando l'opzione Enable search index roaming for Outlook (Abilita il roaming dell'indice di ricerca per Outlook) è abilitata.

Se questo criterio è abilitato, Profile Management crea un backup del database dell'indice di ricerca ogni volta che il database viene caricato correttamente all'accesso. Profile Management considera il backup come copia valida del database dell'indice di ricerca. Quando un tentativo di caricare il database dell'indice di ricerca ha esito negativo perché il database è danneggiato, Profile Management ripristina automaticamente il database dell'indice di ricerca all'ultima copia valida nota.

> Nota:
>
> Profile Management elimina il backup salvato in precedenza dopo che un nuovo backup è stato salvato correttamente. Il backup consuma lo spazio di archiviazione VHDX disponibile.

### Abilita il supporto di sessioni concorrenti per il roaming dei dati di ricerca di Outlook

Consente a Profile Management di fornire un'esperienza di ricerca nativa di Outlook in sessioni simultanee dello stesso utente. Utilizzare questi criteri con i criteri di ricerca in roaming per Outlook.

Con questi criteri abilitati, ogni sessione concorrente utilizza un file OST di Outlook separato.

Per impostazione predefinita, è possibile utilizzare solo due dischi VHDX per archiviare i file OST di Outlook (un file per disco). Se l'utente avvia più sessioni, i suoi file OST di Outlook vengono memorizzati nel profilo utente locale. È possibile specificare il numero massimo di dischi VHDX per la memorizzazione dei file OST di Outlook.

### Abilitare il contenitore OneDrive

Consente alle cartelle di OneDrive di spostarsi con gli utenti.

Il contenitore OneDrive è una soluzione di roaming delle cartelle basata su VHDX. Profile Management crea un file VHDX per utente su una condivisione di file e memorizza le cartelle OneDrive degli utenti nei file VHDX. I file VHDX vengono allegati quando gli utenti eseguono l'accesso e separati quando gli utenti si scollegano.

## Roaming delle app UWP

Consente di abilitare le app UWP (Universal Windows Platform) per il roaming con gli utenti. Di conseguenza, gli utenti possono accedere alle stesse app UWP da dispositivi diversi.

Con questo criterio abilitato, Profile Management consente alle app UWP di spostarsi con gli utenti conservandole su dischi VHDX separati. Questi dischi vengono collegati durante l'accesso degli utenti e scollegati durante lo scollegamento degli utenti.

Precedenza di configurazione:

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.
Se questa impostazione non è configurata qui o nel file .ini, è disabilitata.

#### Abilitare l'elaborazione asincrona per i Criteri di gruppo dell'utente all'accesso

Windows offre due modalità di elaborazione per i Criteri di gruppo dell'utente: sincrona e asincrona. Windows utilizza un valore del Registro di sistema per determinare la modalità di elaborazione per il successivo accesso dell'utente. Se non esiste un valore del Registro di sistema, viene applicata la modalità sincrona. Il valore del Registro di sistema è un'impostazione a livello di macchina e non si sposta con gli utenti. Pertanto, la modalità asincrona non verrà applicata come previsto se gli utenti:

- Accedono a macchine diverse.
- Accedere alla stessa macchina in cui è abilitato il criterio Delete locally cached profiles on logoff (Elimina profili memorizzati nella cache locale allo scollegamento).

Quando questo criterio è abilitato, il valore del Registro di sistema si sposta con gli utenti. Di conseguenza, la modalità di elaborazione viene applicata ogni volta che gli utenti effettuano l'accesso.

#### Rapporto di spazio libero per attivare la compattazione del disco VHD

Applicabile quando l'opzione Enable VHD disk compaction (Abilita la compattazione del disco VHD) è abilitata. Consente di specificare il rapporto di spazio libero per attivare la compattazione del disco VHD. Quando il rapporto di spazio libero supera il valore specificato allo scollegamento dell'utente, viene attivata la compattazione del disco.

Rapporto spazio libero= (dimensione attuale del file VHD - dimensione minima del file VHD richiesta*) ÷ dimensione attuale del file VHD

*Ottenuto utilizzando il metodo GetSupportedSize della classe `MSFT_Partition` dal sistema operativo Microsoft Windows.

#### Numero di scollegamenti per attivare la compattazione del disco VHD

Applicabile quando l'opzione Enable VHD disk compaction (Abilita la compattazione del disco VHD) è abilitata. Consente di specificare il numero di scollegamenti degli utenti che attiva la compattazione del disco VHD.

Quando il numero di scollegamenti dall'ultima compattazione raggiunge il valore specificato, la compattazione del disco viene nuovamente attivata.

#### Disable defragmentation for VHD disk compaction (Disabilita la deframmentazione per la compattazione del disco VHD)

Applicabile quando l'opzione Enable VHD disk compaction (Abilita la compattazione del disco VHD) è abilitata. Consente di specificare se disabilitare la deframmentazione dei file per la compattazione del disco VHD.

Quando la compattazione del disco VHD è abilitata, il file del disco VHD viene prima deframmentato automaticamente utilizzando lo strumento `defrag` integrato di Windows e quindi compattato. La deframmentazione del disco VHD produce risultati di compattazione migliori, mentre la disattivazione può far risparmiare risorse di sistema.

### Enable multi-session write-back for profile containers (Abilita il write-back multisessione per i contenitori dei profili)

Abilita il write-back per i contenitori dei profili in scenari multisessione. Se è abilitata, viene eseguito il write-back delle modifiche in tutte le sessioni nei contenitori dei profili. In caso contrario, vengono salvate solo le modifiche nella prima sessione, perché solo la prima sessione è in modalità di lettura/scrittura nei contenitori dei profili. I contenitori dei profili di Citrix Profile Management sono supportati a partire da Citrix Profile Management 2103. FSLogix Profile Container è supportato a partire da Citrix Profile Management 2003.

Per utilizzare questo criterio per FSLogix Profile Container, assicurarsi che siano soddisfatti i seguenti prerequisiti:

- La funzionalità FSLogix Profile Container è installata e abilitata.
- Il tipo di profilo è impostato su **Try for read-write profile and fallback to read-only** (Prova con profilo lettura-scrittura e sola lettura come fallback) in FSLogix.

### Replicate user stores (Replica gli store utente)

Consente di replicare lo store remoto dei profili utente su più percorsi a ogni accesso e scollegamento. In questo modo, Profile Management fornisce la ridondanza dei profili per gli accessi degli utenti.

L'abilitazione del criterio fa aumentare l'I/O del sistema e potrebbe prolungare gli scollegamenti.

> **Nota:**
>
> - Questa funzionalità è disponibile sia per lo store utenti che per il contenitore del profilo

> completo.
> - I contenitori di profili replicati forniscono la ridondanza dei profili per gli accessi degli utenti ma non per il failover in sessione.

### Enable credential-based access to user stores (Abilita l'accesso agli store utente basato sulle credenziali)

Per impostazione predefinita, Citrix Profile Management rappresenta l'utente corrente per accedere allo store dell'utente. Abilitare questa funzione se non si desidera che Profile Management rappresenti l'utente corrente quando si accede allo store dell'utente. È possibile inserire gli store utente nei repository di archiviazione (ad esempio, File di Azure) a cui l'utente corrente non dispone dell'autorizzazione per accedere.

Per garantire che Profile Management possa accedere agli store utente, salvare le credenziali del server di archiviazione profili in Workspace Environment Management (WEM) o in Gestione credenziali di Windows. Si consiglia di utilizzare Workspace Environment Management per eliminare la necessità di configurare le stesse credenziali per ogni macchina in cui viene eseguito Profile Management. Se si utilizza Gestione credenziali di Windows, utilizzare l'account di sistema locale per salvare in modo sicuro le credenziali.

> **Nota:**
>
> Questo criterio è disponibile per gli store utente basati sia su file che su VHDX. Per le versioni di Profile Management precedenti alla 2212, questo criterio è disponibile solo per gli store utente basati su VHDX.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini. Se questa impostazione non è configurata qui o nel file .ini, è disabilitata per impostazione predefinita.

### Personalizzare il percorso di archiviazione per i file VHDX

Profile Management fornisce i seguenti criteri basati su VHDX: Profile container (Contenitore profilo), Search index roaming for Outlook (Roaming degli indici di ricerca per Outlook) e Accelerate folder mirroring (Accelerare il mirroring delle cartelle). Per impostazione predefinita, i file VHDX vengono archiviati nello store dell'utente. Questo criterio consente di specificare un percorso separato per archiviarli.

### Capacità predefinita dei contenitori VHD

Consente di specificare la capacità di archiviazione predefinita (in GB) dei contenitori VHD.

Precedenza di configurazione:

1. Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini.
2. Se questo criterio non è configurato qui o nel file.ini, l'impostazione predefinita è 50 (GB).

### Ricollegare automaticamente i dischi VHDX nelle sessioni

Con questo criterio abilitat, Profile Management garantisce un alto livello di stabilità dei criteri basati su VHDX. Per impostazione predefinita, questo criterio è abilitato.

Quando questi criteri sono abilitati, Profile Management effettua il monitoraggio dei dischi VHDX utilizzati dai criteri basati su VHDX. Se uno dei dischi è scollegato, Profile Management lo ricollega automaticamente.

### Soglia di espansione automatica del contenitore del profilo

Consente di specificare la percentuale di utilizzo della capacità di archiviazione alla quale i contenitori di profilo attivano l'espansione automatica.

Precedenza di configurazione:

- Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini.
- Se questo criterio non è configurato qui o nel file.ini, l'impostazione predefinita è 90 (%) della capacità di archiviazione.

### Incremento dell'espansione automatica del contenitore di profili

Consente di specificare di quanto si espande automaticamente la capacità di archiviazione (in GB) dei contenitori di profili quando viene attivata l'espansione automatica.

Precedenza di configurazione:

- Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini.
- Se questo criterio non è configurato qui o nel file .ini, l'impostazione predefinita è 10 (GB).

### Limite di espansione automatica del contenitore di profili

Consente di specificare la capacità di archiviazione massima (in GB) a cui i contenitori di profili possono espandersi automaticamente quando viene attivata l'espansione automatica.

Precedenza di configurazione:

- Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini.
- Se questo criterio non è configurato qui o nel file .ini, l'impostazione predefinita è 80 (GB).

### Abilitare le impostazioni dei criteri a livello utente

Con questo criterio abilitato, le impostazioni dei criteri a livello di macchina possono funzionare a livello di utente e le impostazioni a livello di utente hanno la precedenza sulle impostazioni a livello di macchina.

Precedenza di configurazione:

1. Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini.
2. Se questo criterio non è configurato né qui né nel file .ini, è disabilitato.

### Impostare l'ordine di priorità per i gruppi di utenti

Specificare l'ordine di priorità per i gruppi di utenti. L'ordine determina quale gruppo ha la precedenza quando un utente appartiene a più gruppi con impostazioni di criteri diverse.

Quando un utente appartiene a più gruppi con impostazioni dei criteri in conflitto, considerare quanto segue:

- Se l'utente appartiene a uno o più gruppi definiti in questo criterio, il gruppo con la priorità più alta ha la precedenza.
- Se l'utente non appartiene a nessuno dei gruppi definiti in questo criterio, il gruppo con il SID elencato per primo in ordine alfabetico ha la precedenza.

## Impostazioni dei criteri di base

January 7, 2024

Questa sezione contiene le impostazioni dei criteri relative alla configurazione di base di Profile Management.

### Enable Profile Management (Abilita Gestione profili)

Per impostazione predefinita, per facilitare la distribuzione Profile Management non elabora gli accessi o gli scollegamenti. Abilitare Profile Management solo dopo aver eseguito tutte le altre attività di configurazione e aver testato le prestazioni dei profili utente Citrix nell'ambiente.

Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, Profile Management non elabora in alcun modo i profili utente di Windows.

### Processed groups (Gruppi elaborati)

È possibile utilizzare sia gruppi locali di computer che gruppi di dominio (locali, globali e universali). I gruppi di dominio devono essere specificati nel formato: NOME DOMINIO\NOME GRUPPO.

Se questo criterio è configurato qui, Profile Management elabora solo i membri di questi gruppi di utenti. Se questo criterio è disabilitato, Profile Management elabora tutti gli utenti. Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, vengono elaborati i membri di tutti i gruppi di utenti.

### Excluded groups (Gruppi esclusi)

È possibile utilizzare gruppi locali di computer e gruppi di dominio (locali, globali e universali) per impedire l'elaborazione di particolari profili utente. Specificare i gruppi di dominio nel formato NOME DOMINIO\NOME GRUPPO.

Se questa impostazione è configurata qui, Profile Management esclude i membri di questi gruppi di utenti. Se questa impostazione è disabilitata, Profile Management non esclude alcun utente. Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini. Se questa impostazione non è configurata qui o nel file .ini, non viene escluso alcun membro di alcun gruppo.

### Process logons of local administrators (Elabora accessi degli amministratori locali)

Specifica se gli accessi dei membri del gruppo BUILTIN\Administrators vengono elaborati. Si consideri che questo criterio è disabilitato o non configurato sui sistemi operativi multisessione, come gli ambienti Citrix Virtual Apps. In questo caso, Profile Management presuppone che debbano essere elaborati gli accessi degli utenti del dominio, ma non degli amministratori locali. Sui sistemi operativi a sessione singola (ad esempio gli ambienti Citrix Virtual Desktops), gli accessi degli amministratori locali vengono elaborati. Questi criteri consentono agli utenti del dominio con diritti di amministratore locale, in genere gli utenti di Citrix Virtual Desktops con desktop virtuali assegnati, di effettuare le seguenti operazioni:

- Ignorare qualsiasi elaborazione
- Effettuare l'accesso
- Risolvere i problemi relativi al desktop con Profile Management

Nota: gli accessi degli utenti del dominio potrebbero essere soggetti a restrizioni imposte dall'appartenenza al gruppo, in genere per garantire il rispetto delle licenze prodotto.
Se questo criterio è disabilitato, Profile Management non elabora gli accessi degli amministratori locali. Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, gli amministratori non vengono elaborati.

### Path to user store (Percorso dello store utente)

Imposta il percorso della directory (lo store utente) in cui vengono salvate le impostazioni utente (modifiche del Registro di sistema e file sincronizzati).

Il percorso può essere:

- Un percorso relativo. Deve essere rispetto alla directory principale (che in genere è configurata come attributo #homeDirectory# per un utente in Active Directory).
- Un percorso UNC. In genere specifica una condivisione server o uno spazio dei nomi DFS.
- Disabilitato o non configurato. In questo caso, si presume che il valore sia #homeDirectory#\Windows.

Per questo criterio è possibile utilizzare i seguenti tipi di variabili:

- Variabili di ambiente di sistema racchiuse tra segni di percentuale (ad esempio, %ProfVer%). Le variabili di ambiente di sistema in genere richiedono una configurazione aggiuntiva.
- Attributi dell'oggetto utente di Active Directory racchiuso tra hash (ad esempio, #sAMAccountName#).
- Variabili di Profile Management. Per ulteriori informazioni, vedere il documento relativo alle variabili di Profile Management.

Le variabili di ambiente dell'utente non possono essere utilizzate, ad eccezione di `%username%` e `%userdomain%`. È inoltre possibile creare attributi personalizzati per definire completamente variabili organizzative quali la posizione o gli utenti. Gli attributi fanno distinzione tra maiuscole e minuscole.

Esempi:

- \server\share#sAMAccountName# memorizza le impostazioni utente nel percorso UNC \server\share\JohnSmith (se #sAMAccountName# si risolve in JohnSmith per l'utente corrente)
- \server\profiles$%USERNAME%.%USERDOMAIN%!CTX_OSNAME!!CTX_OSBITNESS! potrebbe espandersi in \server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64

Importante: indipendentemente dagli attributi o dalle variabili utilizzate, verificare che questo criterio si espanda nella cartella di un livello superiore alla cartella contenente NTUSER.DAT. Ad esempio, se questo file è contenuto in \server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile, impostare il percorso dello store utente come \server\profiles$\JohnSmith.Finance\Win8x64 (non la sottocartella \UPM_Profile).

Per ulteriori informazioni sull'utilizzo delle variabili quando si specifica il percorso dello store utente, vedere i seguenti argomenti:

- Condividere i profili utente Citrix su più file server

- Gestire i profili all'interno e tra le unità organizzative
- Elevata disponibilità e ripristino di emergenza con Profile Management

Se l'opzione Path to user store (Percorso dello store utente) è disabilitata, le impostazioni utente vengono salvate nella sottodirectory Windows della Home directory.

Se questo criterio è disabilitato, le impostazioni utente vengono salvate nella sottodirectory Windows della Home directory. Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, viene utilizzata la directory Windows nell'unità home.

### Migrate user store (Esegui la migrazione dello store utente)

Specifica il percorso della cartella in cui sono state salvate in precedenza le impostazioni utente (modifiche del Registro di sistema e file sincronizzati) (il percorso dello store utente utilizzato in precedenza).

Se questa impostazione è configurata, le impostazioni utente memorizzate nello store utente precedente vengono migrate nello store utente corrente specificato nel criterio "Path to user store"(Percorso dello store utente).

Il percorso può essere un percorso UNC assoluto o un percorso relativo alla Home directory.

In entrambi i casi, è possibile utilizzare i seguenti tipi di variabili:

- Variabili di ambiente di sistema racchiuse tra segni di percentuale
- Attributi dell'oggetto utente di Active Directory racchiusi tra segni di cancelletto

Esempi:

- La cartella `Windows\\%ProfileVer%` memorizza le impostazioni utente in una sottocartella denominata `Windows\W2K3` dello store utente (se %ProfileVer% è una variabile di ambiente di sistema che si risolve in W2K3).
- `\\server\share\\#SAMAccountName#` memorizza le impostazioni utente nel percorso UNC `\\server\share\<JohnSmith>` (se `#SAMAccountName#` si risolve in JohnSmith per l'utente corrente).

Nel percorso è possibile utilizzare le variabili di ambiente dell'utente, ad eccezione di `%username%` e `%userdomain%`.

Se questa impostazione è disabilitata, le impostazioni utente vengono salvate nello store utente corrente.

Se questa impostazione non è configurata qui, viene utilizzata l'impostazione corrispondente del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, le impostazioni utente vengono salvate nello store utente corrente.

### Active write back (Scrittura attiva)

I file e le cartelle (ma non le voci del Registro di sistema) modificati possono essere sincronizzati con lo store utente nel mezzo di una sessione, prima dello scollegamento.

Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, è abilitato.

Offline profile support (Supporto profilo offline)

Questo criterio consente ai profili di sincronizzarsi con lo store utente alla prima opportunità disponibile. È rivolto agli utenti di laptop o dispositivi mobili in roaming. Quando si verifica una disconnessione della rete, i profili rimangono intatti sul laptop o sul dispositivo anche dopo il riavvio o l'ibernazione. Man mano che gli utenti mobili lavorano, i loro profili vengono aggiornati localmente. Inoltre, alla fine vengono sincronizzati con lo store utente quando viene ristabilita la connessione di rete.

Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, i profili offline vengono disabilitati.

### Active write back registry (Scrittura attiva sul Registro di sistema)

Utilizzare questo criterio insieme ad Active write back (Scrittura attiva). Le voci del Registro di sistema modificate possono essere sincronizzate con lo store utente nel mezzo di una sessione.

Se non si configura questa impostazione qui, viene utilizzato il valore del file .ini.

Se non si configura questa impostazione qui o nel file .ini, l'opzione Active write back registry (Scrittura attiva sul Registro di sistema) è disabilitata.

#### Riscrittura attiva al momento del blocco e della disconnessione della sessione

Con questo criterio e il criterio **Active write back** (Riscrittura attiva) attivati, i file e le cartelle del profilo vengono riscritti solo quando una sessione è bloccata o disconnessa.

Con questo criterio ed entrambi i criteri del registro **Active write back** e **Active write back registry** (Registro di riscrittura attiva), le voci di registro vengono riscritte solo quando una sessione è bloccata o disconnessa.

### Offline profile support (Supporto profilo offline)

Abilita la funzionalità relativa ai profili offline. Questa funzionalità è destinata ai computer che vengono comunemente rimossi dalle reti. Ad esempio, laptop o dispositivi mobili non server o desktop.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, il supporto dei profili offline è disabilitato.

## Impostazioni dei criteri multipiattaforma

January 7, 2024

Questa sezione contiene le impostazioni dei criteri relative alla configurazione della funzionalità delle impostazioni **multipiattaforma di Profile Management**.

### Enable cross-platform settings (Abilita impostazioni multipiattaforma)

Per impostazione predefinita, per facilitare la distribuzione, le impostazioni multipiattaforma sono disabilitate. Attivare l'elaborazione abilitando questo criterio, ma solo dopo una pianificazione e un test approfonditi di questa funzionalità.

Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, le impostazioni multipiattaforma non vengono applicate.

### Cross-platform settings user groups (Gruppi di utenti per le impostazioni multipiattaforma)

Immettere uno o più gruppi di utenti Windows. Ad esempio, è possibile utilizzare questo criterio per elaborare solo i profili di un gruppo di utenti di prova. Se questo criterio è configurato, la funzionalità delle impostazioni multipiattaforma di Profile Management elabora solo i membri di questi gruppi di utenti. Se questo criterio è disabilitato, la funzionalità elabora tutti gli utenti specificati dal criterio Processed groups (Gruppi elaborati).

Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, vengono elaborati tutti i gruppi di utenti.

### Path to cross-platform definitions (Percorso delle definizioni multipiattaforma)

Questa impostazione identifica il percorso di rete dei file di definizione copiati dal pacchetto di download. Questo percorso deve essere un percorso UNC. Gli utenti devono disporre dell'accesso in lettura a questa posizione e gli amministratori devono disporre dell'accesso in scrittura. Il percorso deve essere una condivisione file SMB (Server Message Block) o CIFS (Common Internet File System).

Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, le impostazioni multipiattaforma non vengono applicate.

### Path to cross-platform settings store (Percorso dello store delle impostazioni multipiattaforma)

Imposta il percorso dello store delle impostazioni multipiattaforma, la cartella in cui vengono salvate le impostazioni multipiattaforma degli utenti. Gli utenti devono disporre dell'accesso in scrittura a quest'area. Il percorso può essere un percorso UNC assoluto o un percorso relativo alla Home directory.

Quest'area è l'area comune dello store utente in cui si trovano i dati del profilo condivisi da più piattaforme. Gli utenti devono disporre dell'accesso in scrittura a quest'area. Il percorso può essere un percorso UNC assoluto o un percorso relativo alla Home directory. È possibile utilizzare le stesse variabili dell'opzione **Path to user store** (Percorso dello store utente).

Se questo criterio è disabilitato, viene utilizzato il percorso Windows\PM_CP. Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, viene utilizzato il valore predefinito.

### Source for creating cross-platform settings (Origine per la creazione di impostazioni multipiattaforma)

Specifica una piattaforma come piattaforma di base se questo criterio è abilitato nell'unità organizzativa della piattaforma. Questo criterio esegue la migrazione dei dati dai profili della piattaforma di base allo store delle impostazioni multipiattaforma.

Il gruppo di profili di ogni piattaforma viene archiviato in un'unità organizzativa separata. È necessario decidere quali dati del profilo della piattaforma utilizzare per creare lo store delle impostazioni multipiattaforma. Viene indicato come "piattaforma di base". Si consideri che lo store delle impostazioni multipiattaforma contiene un file di definizione senza dati oppure i dati memorizzati nella cache in un profilo a piattaforma singola sono più recenti dei dati della definizione nello store. In questo caso, Profile Management esegue la migrazione dei dati dal profilo a piattaforma singola dello store a meno che non si disabilitino questi criteri.

> **Importante:**
>
> Se questo criterio è abilitato in più unità organizzative o più oggetti utente o macchina, la piattaforma a cui accede il primo utente diventa il profilo di base.
> Per impostazione predefinita, questo criterio è Abilitato.

## Impostazioni dei criteri del file system

January 7, 2024

Questa sezione contiene i criteri che impostano quanto segue:

- Quali file di un profilo utente sono sincronizzati tra il sistema in cui è installato il profilo e lo store utente
- Quali directory di un profilo utente sono sincronizzate tra il sistema in cui è installato il profilo e lo store utente

## Impostazioni dei criteri di esclusione

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per la configurazione di quali file e directory di un profilo utente vengano esclusi dal processo di sincronizzazione.

### Exclusion list - files (Elenco di esclusione - file)

Elenco dei file che vengono ignorati durante la sincronizzazione. I nomi dei file devono essere percorsi relativi al profilo utente (%USERPROFILE%). I caratteri jolly sono supportati nei nomi dei file e delle cartelle, ma solo i caratteri jolly nei nomi dei file vengono applicati in modo ricorsivo.

Esempi:

- `Desktop\Desktop.ini` ignora il file `Desktop.ini` nella cartella `Desktop`
- `%USERPROFILE%\*.tmp` ignora tutti i file con estensione `.tmp` nell'intero profilo
- `AppData\Roaming\MyApp\*.tmp` ignora tutti i file con estensione `.tmp` in una parte del profilo
- `Downloads\*\a.txt` ignora `a.txt` in qualsiasi sottocartella immediata della cartella `Downloads`.

Se questo criterio è disabilitato, nessun file viene escluso. Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, non viene escluso alcun file.

### Enable Default Exclusion List - directories (Abilita elenco di esclusione predefinito - directory)

Elenco predefinito di directory ignorate durante la sincronizzazione. Utilizzare questo criterio per specificare le directory di esclusione degli oggetti Criteri di gruppo senza doverle compilare manualmente.

Se si disabilita questo criterio, Profile Management non esclude alcuna directory per impostazione predefinita.

Se non si configura questo criterio qui, Profile Management utilizza il valore del file .ini. Se non si configura questo criterio qui o nel file .ini, Profile Management non esclude alcuna directory per impostazione predefinita.

### Exclusion list - directories (Elenco di esclusione - directory)

Elenco delle cartelle ignorate durante la sincronizzazione. I nomi delle cartelle devono essere specificati come percorsi relativi al profilo utente (%USERPROFILE%). I caratteri jolly nei nomi delle cartelle sono supportati, ma non vengono applicati in modo ricorsivo.

Esempio:

- `Desktop` ignora la cartella `Desktop` nel profilo utente

Se questo criterio è disabilitato, non vengono escluse cartelle. Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, non vengono escluse cartelle.

### Logon Exclusion Check (Controllo dell'esclusione dell'accesso)

Questa impostazione consente di configurare il comportamento di Profile Management se un profilo contenuto nello store utente contiene file o cartelle esclusi. Le possibili impostazioni dei criteri e le azioni corrispondenti sono elencate nella tabella seguente:

| Impostazione dei criteri | Azione |
| --- | --- |
| L'impostazione è disabilitata o il valore di "Synchronize excluded files or folders on logon" (Sincronizza file o cartelle esclusi all'accesso) è impostato sul valore predefinito | Profile Management sincronizza i file o le cartelle esclusi dallo store utenti con il profilo locale quando un utente esegue l'accesso. |
| L'impostazione è "Ignore excluded files or folders on logon"(Ignora file o cartelle esclusi all' accesso) | Profile Management ignora i file o le cartelle esclusi dallo store utenti quando un utente esegue l'accesso. |
| L'impostazione è "Delete excluded files or folder on logon"(Elimina file o cartelle esclusi all' accesso) | Profile Management elimina i file o le cartelle esclusi contenuti nello store utenti quando un utente esegue l'accesso. |
| L'impostazione non è configurata in Web Studio | Viene utilizzato il valore contenuto nel file .ini |
| L'impostazione non è configurata in Web Studio o nel file .ini | I file o le cartelle esclusi vengono sincronizzati dallo store utenti a un profilo locale quando un utente esegue l'accesso. |

### Large File Handling - Files to be created as symbolic links (Gestione di file di grandi dimensioni - File da creare come collegamenti simbolici)

Per migliorare le prestazioni di accesso ed elaborare file di grandi dimensioni, Profile Management crea un collegamento simbolico anziché copiare i file in questo elenco.

È possibile utilizzare caratteri jolly nei criteri che fanno riferimento ai file, ad esempio `!ctx_localappdata!\Microsoft\Outlook\*.OST`.

Per elaborare il file delle cartelle offline (`*.ost`) di Microsoft Outlook, assicurarsi che la cartella **Outlook** non sia esclusa per Profile Management.

Non è possibile accedere a tali file contemporaneamente in più sessioni.

## Impostazioni dei criteri di sincronizzazione

January 7, 2024

La sezione **Synchronization** (Sincronizzazione) descrive le impostazioni dei criteri per specificare i file e le cartelle in un profilo utente sincronizzati tra il sistema in cui è installato il profilo e lo store dell'utente.

### Directories to synchronize (Directory da sincronizzare)

Per impostazione predefinita, Profile Management sincronizza il profilo utente tra il sistema in cui è installato e lo store dell'utente. Se si esclude una cartella dalla sincronizzazione, questo criterio consente di includere nuovamente nella sincronizzazione le sottocartelle della cartella esclusa.

I percorsi di questo elenco devono essere relativi al profilo utente. I caratteri jolly nei nomi delle cartelle sono supportati, ma non vengono applicati in modo ricorsivo.

Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, vengono sincronizzate solo le cartelle non escluse nel profilo utente.

### Files to synchronize (File da sincronizzare)

Per impostazione predefinita, Profile Management sincronizza il profilo utente tra il sistema in cui è installato e lo store dell'utente. Se si esclude una cartella dalla sincronizzazione, questo criterio consente di includere nuovamente nella sincronizzazione i file all'interno della cartella esclusa.

I percorsi di questo elenco devono essere relativi al profilo utente. I caratteri jolly sono supportati nei nomi dei file e delle cartelle, ma solo i caratteri jolly nei nomi dei file vengono applicati in modo ricorsivo. I caratteri jolly non possono essere nidificati.

Esempi:

- `AppData\Local\Microsoft\Office\Access.qat` specifica un file sotto una cartella che è esclusa nella configurazione predefinita
- `AppData\Local\MyApp\*.cfg` specifica tutti i file con estensione `.cfg` nella cartella del profilo `AppData\Local\MyApp` e nelle sue sottocartelle

La disabilitazione di questo criterio ha lo stesso effetto dell'abilitazione e della configurazione di un elenco vuoto.

Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, vengono sincronizzati solo i file non esclusi nel profilo utente.

### Folders to mirror (Cartelle di cui eseguire il mirroring)

Questo criterio consente di risolvere i problemi relativi a qualsiasi cartella transazionale (nota anche come cartella referenziale). Tale cartella contiene file interdipendenti, dove un file fa riferimento all'altro.

Il mirroring delle cartelle consente a Profile Management di elaborare una cartella transazionale e il suo contenuto come un'unica entità, evitando il sovraccarico del profilo. Ad esempio, è possibile

eseguire il mirroring della cartella dei **cookie di Internet Explorer** in modo che Index.dat venga sincronizzato con i cookie che indicizza. In queste situazioni, l'ultima scrittura ha la priorità. Quindi i file nelle cartelle con mirroring che sono stati modificati in più di una sessione vengono sovrascritti dall'ultimo aggiornamento, con conseguente perdita di modifiche al profilo.

Ad esempio, la tabella seguente descrive come Index.dat fa riferimento ai cookie mentre un utente naviga in Internet:

| Scenario | Come Index.dat fa riferimento ai cookie |
|---|---|
| Un utente dispone di due sessioni di Internet Explorer, ciascuna su un server diverso, e visita siti diversi in ciascuna sessione. |I cookie di ogni sito vengono aggiunti al server appropriato.| I cookie di ciascun sito vengono aggiunti al server appropriato. |
|L'utente si scollega dalla prima sessione o nel mezzo di una sessione (se è configurata la funzione di riscrittura attiva) | I cookie della seconda sessione devono sostituire i cookie della prima sessione. |
|La prima e la seconda sessione vengono unite e i riferimenti ai cookie contenuti in Index.dat diventano obsoleti | L'ulteriore esplorazione nelle nuove sessioni comporta la ripetizione dell'unione e una cartella di cookie sovraccarica|

Il mirroring della cartella dei cookie risolve il problema. In questo caso, i cookie vengono sovrascritti dai cookie dell'ultima sessione ogni volta che l'utente si scollega. Quindi Index.dat rimane aggiornato.

Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, non viene eseguito il mirroring delle cartelle.

### Accelerate folder mirroring (Accelera il mirroring delle cartelle)

Con questo criterio e il criterio **Folders to mirror** (Cartelle di cui eseguire il mirroring) abilitati, **Profile Management archivia le cartelle di cui è stato eseguito il mirroring** su un disco virtuale basato su VHDX. Collega il disco virtuale durante gli accessi e lo stacca durante gli scollegamenti. L'abilitazione di questo criterio elimina la necessità di copiare le cartelle tra lo store utente e i profili locali e accelera il mirroring delle cartelle.

## Impostazioni dei criteri di reindirizzamento delle cartelle

January 7, 2024

Questa sezione contiene le impostazioni dei criteri che specificano se reindirizzare le cartelle comunemente visualizzate nei profili a un percorso di rete condiviso.

### Grant administrator access (Concedi accesso all'amministratore)

Questa impostazione consente a un amministratore di accedere ai contenuti delle cartelle reindirizzate di un utente.

> **Nota:**
>
> Questa impostazione concede le autorizzazioni agli amministratori che dispongono di accesso completo e illimitato al dominio.

Per impostazione predefinita, questa impostazione è disabilitata e agli utenti viene concesso l'accesso esclusivo ai contenuti delle cartelle reindirizzate.

### Include domain name (Includi nome di dominio)

Questa impostazione consente l'inclusione della variabile `%userdomain%` di ambiente come parte del percorso UNC. Questo percorso UNC è specificato per le cartelle reindirizzate.

Per impostazione predefinita, questa impostazione è disabilitata. E la variabile `%userdomain%` di ambiente non è inclusa all'interno del percorso UNC specificato per le cartelle reindirizzate.

## Impostazioni dei criteri AppData(Roaming)

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per il reindirizzamento del contenuto della cartella **AppData(Roaming)** a un percorso di rete condiviso.

### Percorso AppData(Roaming)

Questa impostazione specifica il percorso di rete a cui vengono reindirizzati i contenuti della cartella **AppData(Roaming)**.

Per impostazione predefinita, questa impostazione è disabilitata e non viene specificata alcuna posizione.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

### Impostazioni di reindirizzamento per AppData(Roaming)

Questa impostazione specifica come reindirizzare il contenuto della cartella **AppData(Roaming)**.

Per impostazione predefinita, i contenuti vengono reindirizzati a un percorso UNC. Per ulteriori informazioni, vedere la sezione Path to user store (Percorso dello store utente).

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

## Impostazioni dei criteri Contatti

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per il reindirizzamento del contenuto della cartella **Contacts** (Contatti) a un percorso di rete condiviso.

### Contacts path (Percorso contatti)

Questa impostazione specifica il percorso di rete a cui vengono reindirizzati i contenuti della cartella **Contacts** (Contatti).

Per impostazione predefinita, questa impostazione è disabilitata e non viene specificata alcuna posizione.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

### Impostazioni di reindirizzamento per Contatti

Questa impostazione specifica come reindirizzare il contenuto della cartella **Contacts** (Contatti).

Per impostazione predefinita, i contenuti vengono reindirizzati a un percorso UNC.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

## Impostazioni dei criteri Desktop

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per il reindirizzamento del contenuto della cartella `Desktop` a un percorso di rete condiviso.

### Desktop path (Percorso Desktop)

Questa impostazione specifica il percorso di rete a cui vengono reindirizzati i contenuti della cartella **Desktop**.

Per impostazione predefinita, questa impostazione è disabilitata e non viene specificata alcuna posizione.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

### Impostazioni di reindirizzamento per Desktop

Questa impostazione specifica come reindirizzare i contenuti della cartella **Desktop**.

Per impostazione predefinita, i contenuti vengono reindirizzati a un percorso UNC.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

## Impostazioni dei criteri Documenti

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per il reindirizzamento del contenuto della cartella **Documenti** a un percorso di rete condiviso.

### Documents path (Percorso Documenti)

Questa impostazione specifica il percorso di rete a cui vengono reindirizzati i file nella cartella **Documenti**.

Per impostazione predefinita, questa impostazione è disabilitata e non viene specificata alcuna posizione.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

L'impostazione **Documents path** (Percorso documenti) deve essere abilitata non solo per reindirizzare i file nella cartella **Documenti**, ma anche per reindirizzare i file alle cartelle **Musica**, **Immagini** e **Video**.

### Impostazioni di reindirizzamento per Documenti

Questa impostazione specifica come reindirizzare i contenuti della cartella **Documenti**.

Per impostazione predefinita, i contenuti vengono reindirizzati a un percorso UNC.

Per controllare come reindirizzare i contenuti della cartella **Documenti**, scegliere una delle seguenti opzioni:

- Redirect to the following UNC path (Reindirizza al seguente percorso UNC): reindirizza il contenuto al percorso UNC specificato nell'impostazione del criterio Documents path (Percorso Documenti).
- Redirect to the users home directory (Reindirizza alla Home directory degli utenti): reindirizza il contenuto alla Home directory degli utenti, in genere configurata come attributo #homeDirectory# per un utente in Active Directory.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

## Impostazioni dei criteri Download

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per il reindirizzamento del contenuto della cartella **Download** a un percorso di rete condiviso.

### Downloads path (Percorso Download)

Questa impostazione specifica il percorso di rete a cui vengono reindirizzati i file nella cartella **Download**.

Per impostazione predefinita, questa impostazione è disabilitata e non viene specificata alcuna posizione.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

### Impostazioni di reindirizzamento per Download

Questa impostazione specifica come reindirizzare il contenuto della cartella **Download**.

Per impostazione predefinita, i contenuti vengono reindirizzati a un percorso UNC.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

## Impostazioni dei criteri Preferiti

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per il reindirizzamento del contenuto della cartella **Preferiti** a un percorso di rete condiviso.

### Favorites path (Percorso Preferiti)

Questa impostazione specifica il percorso di rete a cui vengono reindirizzati i contenuti della cartella **Preferiti**.

Per impostazione predefinita, questa impostazione è disabilitata e non viene specificata alcuna posizione.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

### Impostazioni di reindirizzamento per Preferiti

Questa impostazione specifica come reindirizzare i contenuti della cartella **Preferiti**.

Per impostazione predefinita, i contenuti vengono reindirizzati a un percorso UNC.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

## Impostazioni dei criteri Collegamenti

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per il reindirizzamento del contenuto della cartella **Collegamenti** a un percorso di rete condiviso.

### Links path (Percorso Collegamenti)

Questa impostazione specifica il percorso di rete a cui vengono reindirizzati i contenuti della cartella **Collegamenti**.

Per impostazione predefinita, questa impostazione è disabilitata e non viene specificata alcuna posizione.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

### Impostazioni di reindirizzamento per Collegamenti

Questa impostazione specifica come reindirizzare il contenuto della cartella **Collegamenti**.

Per impostazione predefinita, i contenuti vengono reindirizzati a un percorso UNC.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

## Impostazioni dei criteri Musica

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per il reindirizzamento del contenuto della cartella **Musica** a un percorso di rete condiviso.

### Music path (Percorso Musica)

Questa impostazione specifica il percorso di rete a cui vengono reindirizzati i contenuti della cartella **Musica**.

Per impostazione predefinita, questa impostazione è disabilitata e non viene specificata alcuna posizione.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

### Impostazioni di reindirizzamento per Musica

Questa impostazione specifica come reindirizzare il contenuto della cartella **Musica**.

Per impostazione predefinita, i contenuti vengono reindirizzati a un percorso UNC.

Per controllare come reindirizzare il contenuto della cartella **Musica**, scegliere una delle seguenti opzioni:

- Redirect to the following UNC path (Reindirizza al seguente percorso UNC): reindirizza il contenuto al percorso UNC specificato nell'impostazione dei criteri Music path (Percorso Musica).
- Redirect relative to Documents folder (Reindirizza in una cartella relativa alla cartella Documenti): reindirizza il contenuto a una cartella relativa alla cartella Documenti.

Per reindirizzare il contenuto a una cartella relativa alla cartella **Documenti**, è necessario abilitare l'impostazione **Documents path** (Percorso Documenti).

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

## Impostazioni dei criteri Immagini

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per il reindirizzamento del contenuto della cartella **Immagini** a un percorso di rete condiviso.

### Pictures path (Percorso Immagini)

Questa impostazione specifica il percorso di rete a cui viene reindirizzato il contenuto della cartella **Immagini**.

Per impostazione predefinita, questa impostazione è disabilitata e non viene specificata alcuna posizione.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

### Impostazioni di reindirizzamento per Immagini

Questa impostazione specifica come reindirizzare il contenuto della cartella **Immagini**.

Per impostazione predefinita, i contenuti vengono reindirizzati a un percorso UNC.

Per controllare come reindirizzare il contenuto della cartella **Immagini**, scegliere una delle seguenti opzioni:

- Redirect to the following UNC path (Reindirizza al seguente percorso UNC): reindirizza il contenuto al percorso UNC specificato nell'impostazione dei criteri Pictures path (Percorso Immagini).
- Redirect relative to Documents folder (Reindirizza in una cartella relativa alla cartella Documenti): reindirizza il contenuto a una cartella relativa alla cartella Documenti.

Per reindirizzare il contenuto a una cartella relativa alla cartella **Documenti**, è necessario abilitare l'impostazione **Documents path** (Percorso Documenti).

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

## Impostazioni dei criteri Giochi salvati

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per il reindirizzamento del contenuto della cartella **Giochi salvati** a un percorso di rete condiviso.

### Impostazioni di reindirizzamento per Giochi salvati

Questa impostazione specifica come reindirizzare il contenuto della cartella **Giochi salvati**.

Per impostazione predefinita, i contenuti vengono reindirizzati a un percorso UNC.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

### Saved Games path (Percorso Giochi salvati)

Questa impostazione specifica il percorso di rete a cui vengono reindirizzati i contenuti della cartella **Giochi salvati**.

Per impostazione predefinita, questa impostazione è disabilitata e non viene specificata alcuna posizione.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

# Impostazioni dei criteri del menu Start

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per il reindirizzamento del contenuto della cartella **Menu Start** a un percorso di rete condiviso.

### Impostazioni di reindirizzamento per Menu Start

Questa impostazione specifica come reindirizzare i contenuti della cartella **Menu Start**.

Per impostazione predefinita, i contenuti vengono reindirizzati a un percorso UNC.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

### Start Menu path (Percorso Menu Start)

Questa impostazione specifica il percorso di rete a cui vengono reindirizzati i contenuti della cartella **Menu Start**.

Per impostazione predefinita, questa impostazione è disabilitata e non viene specificata alcuna posizione.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

# Impostazioni dei criteri Ricerche

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per il reindirizzamento del contenuto della cartella **Ricerche** a un percorso di rete condiviso.

### Impostazioni di reindirizzamento per Ricerche

Questa impostazione specifica come reindirizzare il contenuto della cartella **Ricerche**.

Per impostazione predefinita, i contenuti vengono reindirizzati a un percorso UNC.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

### Searches path (Percorso Ricerche)

Questa impostazione specifica il percorso di rete a cui vengono reindirizzati i contenuti della cartella **Ricerche**.

Per impostazione predefinita, questa impostazione è disabilitata e non viene specificata alcuna posizione.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

## Impostazioni dei criteri Video

January 7, 2024

Questa sezione contiene le impostazioni dei criteri per il reindirizzamento del contenuto della cartella **Video** a un percorso di rete condiviso.

### Impostazioni di reindirizzamento per Video

Questa impostazione specifica come reindirizzare il contenuto della cartella **Video**.

Per impostazione predefinita, i contenuti vengono reindirizzati a un percorso UNC.

Per controllare come reindirizzare i contenuti della cartella **Video**, scegliere una delle seguenti opzioni:

- Redirect to the following UNC path (Reindirizza al seguente percorso UNC): reindirizza il contenuto al percorso UNC specificato nell'impostazione dei criteri Video path (Percorso video).
- Redirect relative to Documents folder (Reindirizza in una cartella relativa alla cartella Documenti): reindirizza il contenuto a una cartella relativa alla cartella Documenti.

Per reindirizzare il contenuto a una cartella relativa alla cartella **Documenti**, è necessario abilitare l'impostazione **Documents path** (Percorso Documenti).

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

### Video path (Percorso Video)

Questa impostazione specifica il percorso di rete a cui vengono reindirizzati i contenuti della cartella **Video**.

Per impostazione predefinita, questa impostazione è disabilitata e non viene specificata alcuna posizione.

Se questa impostazione non è configurata qui, Profile Management non reindirizza la cartella specificata.

## Impostazioni dei criteri di log

January 7, 2024

Questa sezione contiene le impostazioni dei criteri che configurano la registrazione di Profile Management.

### Active Directory actions (Azioni di Active Directory)

Questa impostazione abilita o disabilita la registrazione dettagliata delle azioni eseguite in Active Directory.

Per impostazione predefinita, questa impostazione è disabilitata.

Quando si abilita questa impostazione, assicurarsi che sia abilitata anche l'impostazione **Enable logging** (Abilita registrazione).

Se questa impostazione non è configurata in Web Studio, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata in Web Studio o nel file .ini, viene registrato quanto segue:

- Errori
- Informazioni generali

### Common information (Informazioni comuni)

Questa impostazione abilita o disabilita la registrazione dettagliata delle informazioni comuni.

Per impostazione predefinita, questa impostazione è disabilitata.

Quando si abilita questa impostazione, assicurarsi che sia abilitata anche l'impostazione **Enable logging** (Abilita registrazione).

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata in Web Studio o nel file .ini, viene registrato quanto segue:

- Errori
- Informazioni generali

### Common warnings (Avvisi comuni)

Questa impostazione abilita o disabilita la registrazione dettagliata degli avvisi comuni.

Per impostazione predefinita, questa impostazione è disabilitata.

Quando si abilita questa impostazione, assicurarsi che sia abilitata anche l'impostazione **Enable logging** (Abilita registrazione).

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata in Web Studio o nel file .ini, viene registrato quanto segue:

- Errori
- Informazioni generali

### Enable logging (Abilita registrazione)

Questa impostazione abilita o disabilita la registrazione di Profile Management in modalità di debug (registrazione dettagliata). In modalità di debug, le informazioni sullo stato estese vengono registrate nei file di log in "%SystemRoot%\System32\Logfiles\UserProfileManager".

Per impostazione predefinita, questa impostazione è disabilitata e vengono registrati solo gli errori.

Citrix consiglia di abilitare questa impostazione solo se si stanno risolvendo i problemi relativi a Profile Management.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, vengono registrati solo gli errori.

### File system actions (Azioni del file system)

Questa impostazione abilita o disabilita la registrazione dettagliata delle azioni eseguite nel file system.

Per impostazione predefinita, questa impostazione è disabilitata.

Quando si abilita questa impostazione, assicurarsi che sia abilitata anche l'impostazione **Enable logging** (Abilita registrazione).

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata in Web Studio o nel file .ini, viene registrato quanto segue:

- Errori
- Informazioni generali

### File system notifications (Notifiche del file system)

Questa impostazione abilita o disabilita la registrazione dettagliata delle notifiche dei file system.

Per impostazione predefinita, questa impostazione è disabilitata.

Quando si abilita questa impostazione, assicurarsi che sia abilitata anche l'impostazione **Enable logging** (Abilita registrazione).

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata in Web Studio o nel file .ini, viene registrato quanto segue:

- Errori
- Informazioni generali

### Logoff (Scollega)

Questa impostazione abilita o disabilita la registrazione dettagliata degli scollegamenti degli utenti.

Per impostazione predefinita, questa impostazione è disabilitata.

Quando si abilita questa impostazione, assicurarsi che sia abilitata anche l'impostazione **Enable logging** (Abilita registrazione).

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata in Web Studio o nel file .ini, viene registrato quanto segue:

- Errori
- Informazioni generali

### Logon (Accedi)

Questa impostazione abilita o disabilita la registrazione dettagliata degli accessi degli utenti.

Per impostazione predefinita, questa impostazione è disabilitata.

Quando si abilita questa impostazione, assicurarsi che sia abilitata anche l'impostazione **Enable logging** (Abilita registrazione).

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata in Web Studio o nel file .ini, viene registrato quanto segue:

- Errori
- Informazioni generali

### Maximum size of the log file (Dimensioni massime del file di log)

Questa impostazione specifica le dimensioni massime consentite per il file di log di Profile Management, espresse in byte.

Per impostazione predefinita, questo valore è impostato su 1.048.576 byte (1 MB).

Citrix consiglia di aumentare le dimensioni di questo file a 5 MB o più, se si dispone di spazio su disco sufficiente. Se il file di registro supera la dimensione massima:

- Viene eliminato un backup esistente del file (.bak)
- Il file di registro viene rinominato in .bak
- Viene creato un nuovo file di registro

Il file di log viene creato in %SystemRoot%\System32\Logfiles\UserProfileManager.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, viene utilizzato il valore predefinito.

### Path to log file (Percorso del file di log)

Questa impostazione specifica un percorso alternativo per salvare il file di log di Profile Management.

Per impostazione predefinita, questa impostazione è disabilitata e i file di log vengono salvati nel percorso predefinito: %SystemRoot%\System32\Logfiles\UserProfileManager.

Il percorso può puntare a un'unità locale o a un'unità remota basata sulla rete (percorso UNC). I percorsi remoti possono essere utili in ambienti distribuiti di grandi dimensioni, ma potrebbero creare un notevole traffico di rete, il che potrebbe non essere appropriato per i file di log. Per le macchine virtuali di cui è stato effettuato il provisioning e con un disco rigido persistente, impostare un percorso locale per tale unità. Questa impostazione assicura che i file di registro vengano conservati al riavvio della macchina. Per le macchine virtuali senza un disco rigido persistente, l'impostazione di un percorso UNC consente di conservare i file di registro. Tuttavia, l'account di sistema delle macchine deve disporre dell'accesso in scrittura alla condivisione UNC. Utilizzare un percorso locale per tutti i laptop gestiti dalla funzionalità dei profili offline.

Se si utilizza un percorso UNC per i file di registro, Citrix consiglia di applicare un elenco di controllo di accesso appropriato alla cartella dei file di registro. Questa impostazione garantisce che solo gli account utente o computer autorizzati possano accedere ai file archiviati.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, viene utilizzata la posizione predefinita %SystemRoot%\System32\Logfiles\UserProfileManager.

### Personalized user information (Informazioni utente personalizzate)

Questa impostazione abilita o disabilita la registrazione dettagliata delle informazioni utente personalizzate.

Per impostazione predefinita, questa impostazione è disabilitata.

Quando si abilita questa impostazione, assicurarsi che sia abilitata anche l'impostazione **Enable logging** (Abilita registrazione).

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata in Web Studio o nel file .ini, viene registrato quanto segue:

- Errori
- Informazioni generali

### Policy values at logon and logoff (Valori dei criteri all'accesso e allo scollegamento)

Questa impostazione abilita o disabilita la registrazione dettagliata dei valori dei criteri quando un utente accede e si disconnette.

Per impostazione predefinita, questa impostazione è disabilitata.

Quando si abilita questa impostazione, assicurarsi che sia abilitata anche l'impostazione **Enable logging** (Abilita registrazione).

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata in Web Studio o nel file .ini, viene registrato quanto segue:

- Errori
- Informazioni generali

### Registry actions (Azioni del Registro di sistema)

Questa impostazione abilita o disabilita la registrazione dettagliata delle azioni eseguite nel Registro di sistema.

Per impostazione predefinita, questa impostazione è disabilitata.

Quando si abilita questa impostazione, assicurarsi che sia abilitata anche l'impostazione **Enable logging** (Abilita registrazione).

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata in Web Studio o nel file .ini, viene registrato quanto segue:

- Errori
- Informazioni generali

### Registry differences at logoff (Differenze del Registro di sistema allo scollegamento)

Questa impostazione abilita o disabilita la registrazione dettagliata di eventuali differenze nel Registro di sistema quando un utente si disconnette.

Per impostazione predefinita, questa impostazione è disabilitata.

Quando si abilita questa impostazione, assicurarsi che sia abilitata anche l'impostazione **Enable logging** (Abilita registrazione).

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata in Web Studio o nel file .ini, viene registrato quanto segue:

- Errori
- Informazioni generali

## Impostazioni dei criteri di gestione dei profili

January 7, 2024

Questa sezione include le impostazioni dei criteri che specificano il modo in cui Profile Management gestisce i profili degli utenti.

### Delay before deleting cached profiles (Attendi prima di eliminare i profili memorizzati nella cache)

Questa impostazione specifica un'estensione facoltativa del ritardo, espressa in minuti, prima che Profile Management elimini i profili memorizzati localmente nella cache allo scollegamento.

Il valore 0 elimina i profili immediatamente al termine del processo di scollegamento. Profile Management verifica la presenza di scollegamenti ogni minuto. Di conseguenza, un valore di 60 garantisce che i profili vengano eliminati tra uno e due minuti dopo lo scollegamento degli utenti. Questa azione dipende da quando si è verificato l'ultimo controllo. Estendere il ritardo è utile nei casi in cui un processo mantiene aperti i file o l'hive del Registro di sistema dell'utente durante lo scollegamento. Con profili di grandi dimensioni, questo processo può anche velocizzare lo scollegamento.

Per impostazione predefinita, questo valore è impostato su 0 e Profile Management elimina immediatamente i profili memorizzati localmente nella cache.

Quando si abilita questa impostazione, assicurarsi che sia abilitata anche l'opzione Delete locally cached profiles on logoff (Elimina i profili memorizzati nella cache locale allo scollegamento).

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, i profili vengono eliminati immediatamente.

### Delete locally cached profiles on logoff (Elimina i profili memorizzati nella cache locale allo scollegamento)

Questa impostazione specifica se i profili memorizzati localmente nella cache vengono eliminati dopo la disconnessione di un utente.

Quando questa impostazione è abilitata, la cache del profilo locale di un utente viene eliminata dopo la disconnessione. Citrix consiglia di abilitare questa impostazione per i server terminal.

Per impostazione predefinita, questa impostazione è disabilitata e viene mantenuta una cache del profilo locale degli utenti dopo lo scollegamento.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, i profili memorizzati nella cache non vengono eliminati.

### Local profile conflict handling (Gestione dei conflitti di profilo locali)

Questa impostazione configura il comportamento di Profile Management se esiste un profilo utente in entrambi i seguenti elementi:

- Store utenti
- Profilo utente Windows locale (non un profilo utente Citrix)

Per impostazione predefinita, Profile Management utilizza il profilo Windows locale, ma non lo modifica in alcun modo.

Per controllare il comportamento di Profile Management, scegliere una delle seguenti opzioni:

- Use local profile (Usa il profilo locale). Profile Management utilizza il profilo locale, ma non lo modifica in alcun modo.
- Delete local profile (Elimina profilo locale). Profile Management elimina il profilo utente locale di Windows, quindi importa il profilo utente Citrix dallo store utente.
- Rename local profile (Rinomina profilo locale). Profile Management rinomina il profilo utente locale di Windows (a scopo di backup), quindi importa il profilo utente Citrix dallo store utente.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, vengono utilizzati i profili locali esistenti.

### Migration of existing profiles (Migrazione dei profili esistenti)

Questa impostazione specifica i tipi di profilo migrati allo store utente durante l'accesso se un utente non dispone di un profilo corrente nello store utente.

Profile Management può eseguire la migrazione dei profili esistenti in tempo reale durante l'accesso se un utente non ha un profilo nello store utente. Successivamente, il profilo dello store utente viene utilizzato da Profile Management in entrambe le seguenti:

- Sessione corrente
- Qualsiasi altra sessione configurata con il percorso dello stesso store utenti

Per impostazione predefinita, i profili locali e mobili vengono migrati nello store utente durante l'accesso.

Per specificare i tipi di profilo migrati allo store utente durante l'accesso, scegliere una delle seguenti opzioni:

- Local and roaming profiles (Profili locali e mobili)
- Local (Locali)
- Roaming (Mobili)
- Nessuno (Disabilitato)

Se si seleziona **None** (Nessuno), il sistema utilizza il meccanismo di Windows esistente per creare profili, come in un ambiente in cui Profile Management non è installato.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, vengono migrati i profili locali e mobili esistenti.

### Automatic migration of existing application profiles (Migrazione automatica dei profili delle applicazioni esistenti)

Questa impostazione abilita o disabilita la migrazione automatica dei profili delle applicazioni esistenti tra diversi sistemi operativi. I profili dell'applicazione includono sia i dati dell'applicazione nella cartella `AppData` che le voci del Registro di sistema in `HKEY_CURRENT_USER\SOFTWARE`. Questa impostazione può essere utile nei casi in cui si desidera eseguire la migrazione dei profili delle applicazioni tra diversi sistemi operativi.

Ad esempio, supponiamo di aggiornare il sistema operativo (OS) da Windows 10 versione 1803 a Windows 10 versione 1809. Se questa impostazione è abilitata, Profile Management esegue automaticamente la migrazione delle impostazioni delle applicazioni esistenti a Windows 10 versione 1809 la prima volta che ogni utente accede. Di conseguenza, i dati dell'applicazione nella cartella `AppData` e le voci del Registro di sistema in HKEY_CURRENT_USER\SOFTWARE vengono migrati.

Se esistono più profili di applicazioni esistenti, Profile Management esegue la migrazione nel seguente ordine di priorità:

1. Profili con lo stesso tipo di sistema operativo (da sistema operativo a sessione singola a sistema operativo a sessione singola e da sistema operativo multisessione a sistema operativo multisessione).
2. Profili della stessa famiglia di sistemi operativi Windows, ad esempio da Windows 10 a Windows 10 o da Windows Server 2016 a Windows Server 2016).
3. Profili di una versione precedente del sistema operativo, ad esempio da Windows 7 a Windows 10 o da Windows Server 2012 a Windows 2016.
4. Profili del sistema operativo più vicino.

**Nota:** è necessario specificare il nome breve del sistema operativo includendo la variabile "!CTX_OSNAME!"nel percorso dello store utente. In questo modo Profile Management è in grado di individuare i profili delle applicazioni esistenti.

Se questa impostazione non è configurata qui, viene utilizzata l'impostazione del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, è disabilitata per impostazione predefinita.

### Path to the template profile (Percorso del profilo del modello)

Questa impostazione specifica il percorso del profilo che si desidera che Profile Management utilizzi come modello per creare profili utente.

Il percorso specificato deve essere il percorso completo della cartella contenente il file del Registro di sistema NTUSER.DAT ed eventuali altri file e cartelle necessari per il profilo del modello.

Nota: non includere NTUSER.DAT nel percorso. Ad esempio, con il file \\myservername\myprofiles\template\ntuse
impostare la posizione come \\myservername\myprofiles\template.

Utilizzare percorsi assoluti, che possono essere percorsi UNC o percorsi sulla macchina locale. Utilizzare quest'ultimo, ad esempio, per specificare un profilo del modello in modo permanente su un' immagine Citrix Provisioning Services. I percorsi relativi non sono supportati.

Nota: questa impostazione non supporta l'espansione degli attributi di Active Directory, delle variabili di ambiente di sistema o delle variabili %`USERNAME`% e %`USERDOMAIN`%.

Per impostazione predefinita, questa impostazione è disabilitata e vengono creati nuovi profili utente dal profilo utente predefinito sul dispositivo in cui un utente accede per la prima volta.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, non viene utilizzato alcun modello.

### Template profile overrides local profile (Il profilo del modello sostituisce il profilo locale)

Questa impostazione consente al profilo del modello di ignorare il profilo locale durante la creazione dei profili utente.

Si consideri che un utente non ha un profilo utente Citrix, ma ha un profilo utente Windows locale. In questo caso, per impostazione predefinita, il profilo locale viene utilizzato e migrato allo store utenti, se questo valore è abilitato. L'abilitazione di questa impostazione dei criteri consente al profilo del modello di sovrascrivere il profilo locale utilizzato durante la creazione dei profili utente.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, non viene utilizzato alcun modello.

### Template profile overrides roaming profile (Il profilo del modello sostituisce il profilo mobile)

Questa impostazione consente al profilo del modello di ignorare un profilo mobile durante la creazione di profili utente.

Si consideri che un utente non ha un profilo utente Citrix, ma ha un profilo utente Windows mobile. In questo caso, per impostazione predefinita, il profilo mobile viene utilizzato e migrato allo store utenti, se questo valore è abilitato. L'abilitazione di questa impostazione dei criteri consente al profilo del modello di ignorare il profilo mobile utilizzato durante la creazione dei profili utente.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, non viene utilizzato alcun modello.

### Template profile used as a Citrix mandatory profile for all logons (Profilo del modello utilizzato come profilo Citrix obbligatorio per tutti gli accessi)

Questa impostazione consente a Profile Management di utilizzare il profilo del modello come profilo predefinito per la creazione di tutti i profili utente.

Per impostazione predefinita, questa impostazione è disabilitata e vengono creati nuovi profili utente dal profilo utente predefinito sul dispositivo in cui un utente accede per la prima volta.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, non viene utilizzato alcun modello.

## Impostazioni dei criteri del Registro di sistema

January 7, 2024

Questa sezione contiene le impostazioni dei criteri che specificano quali chiavi del Registro di sistema sono incluse o escluse dall'elaborazione di Profile Management.

### Elenco di esclusione

Elenco delle chiavi del Registro di sistema nell'hive HKCU che vengono ignorate durante lo scollegamento.

Esempio: Software\Policies

Se questo criterio è disabilitato, non viene esclusa nessuna chiave del Registro di sistema. Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, non viene esclusa nessuna chiave del Registro di sistema.

### Inclusion list (Elenco di inclusione)

Elenco delle chiavi del Registro di sistema nell'hive HKCU che vengono elaborate durante lo scollegamento.

Esempio: Software\Adobe.

Se questo criterio è abilitato, vengono elaborate solo le chiavi presenti nell'elenco. Se questo criterio è disabilitato, viene elaborato l'hive HKCU completo. Se questo criterio non è configurato qui, viene utilizzato il valore del file .ini. Se questo criterio non è configurato qui o nel file .ini, tutti i criteri HKCU vengono elaborati.

### Enable Default Exclusion List - Profile Management 5.5 (Abilita elenco di esclusione predefinito - Profile Management 5.5)

Elenco predefinito delle chiavi del Registro di sistema nell'hive HKCU che non sono sincronizzate con il profilo utente. Utilizzare questo criterio per specificare i file di esclusione di oggetti Criteri di gruppo senza doverli compilare manualmente.

Se si disabilita questo criterio, Profile Management non esclude alcuna chiave del Registro di sistema per impostazione predefinita. Se non si configura questo criterio qui, Profile Management utilizza il valore del file .ini. Se non si configura questo criterio qui o nel file .ini, Profile Management non esclude alcuna chiave del Registro di sistema per impostazione predefinita.

### Backup di NTUSER.DAT

Consente un backup dell'ultima copia valida nota di NTUSER.DAT e il rollback in caso di danneggiamento.

Se non si configura questo criterio qui, Profile Management utilizza il valore del file .ini. Se non si configura questo criterio qui o nel file .ini, Profile Management non esegue il backup di NTUSER.DAT.

## Impostazioni dei criteri dei profili utente in streaming

January 7, 2024

Questa sezione contiene le impostazioni dei criteri che specificano il modo in cui Profile Management elabora i profili utente in streaming.

### Always cache (Memorizza sempre nella cache)

Questa impostazione specifica se Profile Management memorizza nella cache i file in streaming il più presto possibile dopo l'accesso di un utente. La memorizzazione nella cache dei file dopo l'accesso di un utente consente di risparmiare larghezza di banda della rete, migliorando l'esperienza utente.

Utilizzare questa impostazione con l'impostazione **Profile streaming** (Streaming profilo).

Per impostazione predefinita, questa impostazione è disabilitata e i file in streaming non vengono memorizzati nella cache il prima possibile dopo l'accesso di un utente.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, è disabilitata.

### Always cache size (Memorizza sempre nella cache in base alle dimensioni)

Questa impostazione specifica un limite inferiore, in MB, per le dimensioni dei file in streaming. Profile Management memorizza nella cache tutti i file di questa dimensione o di dimensioni superiori il prima possibile dopo l'accesso di un utente.

Per impostazione predefinita, il valore è impostato su 0 (zero) e viene utilizzata la funzionalità Cache entire profile (Memorizza nella cache l'intero profilo). Quando la funzionalità Cache entire profile (Memorizza nella cache l'intero profilo) è abilitata, Profile Management recupera tutti i contenuti del profilo nello store utente dopo l'accesso di un utente, come attività in background.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, è disabilitata.

### Profile streaming (Streaming del profilo)

Questa impostazione abilita e disabilita la funzionalità dei profili utente in streaming di Citrix. Se abilitata, i file e le cartelle del profilo vengono trasferiti dallo store dell'utente alla macchina locale solo quando gli utenti vi accedono dopo aver effettuato l'accesso. Le voci del Registro di sistema e i file nell'area in sospeso vengono recuperati immediatamente.

Per impostazione predefinita, lo streaming dei profili è disabilitato.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata qui o nel file .ini, è disabilitata.

### Streamed user profile groups (Gruppi di profili utente in streaming)

Questa impostazione specifica quali profili utente all'interno di un'unità organizzativa vengono trasmessi in streaming, in base ai gruppi di utenti di Windows.

Se abilitata, vengono trasmessi in streaming solo i profili utente all'interno dei gruppi di utenti specificati. Tutti gli altri profili utente vengono elaborati normalmente.

Per impostazione predefinita, questa impostazione è disabilitata e tutti i profili utente all'interno di un'unità organizzativa vengono elaborati normalmente.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata né qui né nel file .ini, vengono elaborati tutti i profili utente.

### Abilitare l'esclusione dello streaming dei profili

Quando l'esclusione dello streaming del profilo è abilitata:

- Profile Management non esegue lo streaming delle cartelle contenute nell'elenco di esclusione
- Tutte le cartelle vengono recuperate immediatamente dallo store utenti al computer locale quando un utente esegue l'accesso

Per ulteriori informazioni, vedere Streaming dei profili utente.

### Timeout for pending area lock files (Timeout per i file bloccati nell'area in sospeso)

Questa impostazione specifica il numero di giorni dopo i quali i file degli utenti vengono scritti nello store utente dall'area in sospeso, se lo store dell'utente rimane bloccato quando il suo server di archiviazione non risponde. Questo comportamento impedisce il sovraccarico nell'area in sospeso e assicura che lo store utente contenga sempre i file più aggiornati.

Per impostazione predefinita, questo valore è 1 (un) giorno.

Se questa impostazione non è configurata qui, viene utilizzato il valore del file .ini.

Se questa impostazione non è configurata né qui né nel file .ini, viene utilizzato il valore predefinito.

### Enable profile streaming for pending area (Abilitare lo streaming del profilo per l'area in sospeso)

Consente di abilitare la funzione di streaming del profilo per i file e le cartelle dell'area in sospeso.

L'area in sospeso viene utilizzata per garantire la coerenza del profilo mentre lo streaming del profilo è abilitato. Memorizza temporaneamente i file di profilo e le cartelle che sono stati modificati in sessioni concomitanti.

Per impostazione predefinita, questi criteri sono disabilitati e tutti i file e le cartelle che si trovano nell'area in sospeso vengono recuperati nel profilo locale all'accesso. Quando questo criterio è abilitato, i file che si trovano nell'area in sospeso vengono recuperati nel profilo locale solo quando vengono richiesti. Utilizzare il criterio con il criterio di streaming del profilo per garantire un'esperienza di accesso ottimale negli scenari che presentano sessioni concomitanti.

Il criterio si applica alle cartelle dell'area in sospeso quando il criterio Enable profile streaming for folders (Abilita streaming del profilo per le cartelle) è abilitato.

## Impostazioni dei criteri del livello di personalizzazione utente

January 7, 2024

Per abilitare il montaggio dei livelli utente all'interno di Virtual Delivery Agent, utilizzare i parametri di configurazione per specificare:

- In quale posizione sulla rete accedere ai livelli utente.
- Quali sono le dimensioni massime che i nuovi dischi dei livelli utente possono raggiungere.

A tale scopo, nell'elenco dei criteri disponibili vengono visualizzati questi due criteri:

- User Layer Repository Path (Percorso del repository del livello utente): immettere un percorso nel formato "\nome o indirizzo server\nome cartella"nel campo Value (Valore).
- User Layer Size GB (Dimensioni in GB del livello utente): la dimensione predefinita del livello utente (10 GB) è la dimensione minima consigliata da Citrix. Un livello utente è un disco con thin provisioning che si espande fino alle dimensioni impostate man mano che viene utilizzato lo spazio. Le dimensioni dei livelli utente non diminuiscono mai.

> **Nota:**
>
> L'aumento della dimensione del livello utente influisce sui nuovi livelli utente ed espande quelli esistenti. La diminuzione della dimensione del livello influisce solo sui nuovi livelli utente. I livelli utente esistenti non diminuiscono mai di dimensioni.

Per ulteriori informazioni, vedere Livello di personalizzazione utente.

## Impostazioni dei criteri Virtual Delivery Agent

January 7, 2024

La sezione Virtual Delivery Agent (VDA) contiene le impostazioni dei criteri che controllano la comunicazione tra il VDA e i controller per un sito.

Importante: il VDA richiede informazioni fornite da queste impostazioni per registrarsi con un Delivery Controller, se non si utilizza la funzione di aggiornamento automatico. Poiché queste informazioni sono necessarie per la registrazione, è necessario configurare le seguenti impostazioni utilizzando l'Editor Criteri di gruppo, a meno che non si forniscano queste informazioni durante l'installazione del VDA:

- Controller registration IPv6 netmask (Netmask IPv6 di registrazione controller)
- Controller registration port (Porta di registrazione del controller)
- Controller SIDs (SID controller)
- Controllers (Controller)
- Only use IPv6 controller registration (Utilizza solo la registrazione del controller IPv6)
- Sute GUID (GUID sito)

### Controller registration IPv6 netmask (Netmask IPv6 di registrazione controller)

Questa impostazione dei criteri consente agli amministratori di limitare il VDA solo a una sottorete preferita (anziché un indirizzo IP globale, se registrato). Questa impostazione specificare l'indirizzo

IPv6 e la rete in cui viene registrato il VDA. Il VDA si registra solo sul primo indirizzo corrispondente alla maschera di rete specificata. Questa impostazione è valida solo se l'impostazione dei criteri Only use IPv6 controller registration (Utilizza solo la registrazione del controller IPv6) è abilitata.

Per impostazione predefinita, questa impostazione è vuota.

### Controller registration port (Porta di registrazione del controller)

Utilizzare questa impostazione solo se l'impostazione **Enable auto update of controllers** (Abilita aggiornamento automatico dei controller) è disattivata.

Questa impostazione specifica il numero di porta TCP/IP utilizzato dal VDA per registrarsi con un controller quando si utilizza la registrazione basata sul Registro di sistema.

Per impostazione predefinita, il numero di porta è impostato su 80.

### Controller SIDs (SID controller)

Utilizzare questa impostazione solo se l'impostazione **Enable auto update of controllers** (Abilita aggiornamento automatico dei controller) è disattivata.

Questa impostazione specifica un elenco separato da spazi di identificatori di sicurezza (SID) del controller utilizzato dal VDA per registrarsi con un controller quando si utilizza la registrazione basata sul Registro di sistema. Questa impostazione è facoltativa e potrebbe essere utilizzata con l'impostazione **Controllers**per limitare l'elenco dei controller utilizzati per la registrazione.

Per impostazione predefinita, questa impostazione è vuota.

### Controllers (Controller)

Utilizzare questa impostazione solo se l'impostazione **Enable auto update of controllers** (Abilita aggiornamento automatico dei controller) è disattivata.

Questa impostazione specifica un elenco separato da spazi di nomi di dominio completi (FQDN) dei controller utilizzato dal VDA per registrarsi con un controller quando si utilizza la registrazione basata sul Registro di sistema. Questa impostazione è facoltativa e potrebbe essere utilizzata con l'impostazione **Controller SIDs** (SID controller).

Per impostazione predefinita, questa impostazione è vuota.

### Enable auto update of controllers (Abilita aggiornamento automatico dei controller)

Questa impostazione consente al VDA di registrarsi automaticamente con un controller dopo l'installazione.

Dopo la registrazione del VDA, il controller con cui si è registrato invia un elenco dei FQDN e dei SID correnti del controller al VDA. Il VDA scrive questo elenco nella posizione di archiviazione permanente. Inoltre ciascun Controller ogni 90 minuti verifica le informazioni sul Controller nel database del sito. Il Controller invia elenchi aggiornati ai propri VDA registrati se si verifica una delle seguenti situazioni:

- Un Controller è stato aggiunto o rimosso dopo l'ultima verifica
- Si è verificato un cambiamento di criteri

Il VDA accetta connessioni da tutti i controller inclusi nell'elenco più recente che ha ricevuto.

Per impostazione predefinita, questa impostazione è abilitata.

### Only use IPv6 controller registration (Utilizza solo la registrazione del controller IPv6)

Questa impostazione controlla il tipo di indirizzo utilizzato dal VDA per registrarsi con il controller:

- Quando è abilitata, il VDA si registra con il controller utilizzando l'indirizzo IPv6 della macchina. Quando il VDA comunica con il controller, utilizza il seguente ordine di indirizzi: indirizzo IP globale, Unique Local Address (ULA), indirizzo locale del collegamento (se non sono disponibili altri indirizzi IPv6).
- Quando l'impostazione è disabilitata, il VDA si registra e comunica con il controller utilizzando l'indirizzo IPv4 del computer.

Per impostazione predefinita, questa impostazione è disabilitata.

### Sute GUID (GUID sito)

Utilizzare questa impostazione solo se l'impostazione **Enable auto update of controllers** (Abilita aggiornamento automatico dei controller) è disattivata.

Questa impostazione specifica il GUID (Global Unique Identifier) del sito utilizzato dal VDA per registrarsi con un controller quando si utilizza la registrazione basata su Active Directory.

Per impostazione predefinita, questa impostazione è vuota.

## Impostazioni dei criteri HDX 3D Pro

January 7, 2024

La sezione HDX 3D Pro include le impostazioni dei criteri per l'abilitazione e la configurazione dello strumento di configurazione della qualità delle immagini per gli utenti. Questo strumento consente

agli utenti di ottimizzare l'uso della larghezza di banda disponibile. Per questa ottimizzazione, l'equilibrio tra qualità dell'immagine e reattività viene regolato in tempo reale.

### Enable lossless (Abilita senza perdita di dati)

Questa impostazione specifica se gli utenti possono abilitare e disabilitare la compressione senza perdita di dati utilizzando lo strumento di configurazione della qualità delle immagini. Per impostazione predefinita, gli utenti non hanno la possibilità di abilitare la compressione senza perdita di dati.

Si consideri che un utente abiliti la compressione senza perdita di dati. In questo caso, la qualità delle immagini viene automaticamente impostata sul valore massimo disponibile nello strumento di configurazione delle immagini. Per impostazione predefinita, è possibile utilizzare la compressione basata su GPU o CPU, in base alle funzionalità del dispositivo utente e del computer host.

### HDX 3D Pro quality settings (Impostazioni di qualità HDX 3D Pro)

Questa impostazione specifica i valori minimi e massimi disponibili per gli utenti nello strumento di configurazione della qualità delle immagini. Utilizzando questi valori, gli utenti possono definire l'intervallo di regolazione della qualità delle immagini nello strumento di configurazione della qualità delle immagini.

Specificare valori di qualità delle immagini compresi tra 0 e 100 inclusi. Il valore massimo deve essere maggiore o uguale al valore minimo.

## Impostazioni dei criteri di monitoraggio

January 7, 2024

La sezione **Monitoring** (Monitoraggio) include le impostazioni dei criteri per il monitoraggio dei processi, delle risorse e degli errori delle applicazioni.

L'ambito di queste politiche può essere definito in base a quanto segue:

- Sito
- Gruppo di consegna
- Tipo di gruppo di consegna
- Unità organizzativa
- Tag

## Criteri per il monitoraggio di processi e risorse

Ogni punto dati per CPU, memoria e processi viene raccolto dal VDA e memorizzato nel database di monitoraggio. L'invio dei punti dati dal VDA consuma la larghezza di banda della rete e la loro archiviazione occupa una notevole quantità di spazio nel database di monitoraggio. Si consideri di non voler monitorare né i dati delle risorse né i dati di processo o entrambi per un ambito specifico. Ad esempio, un gruppo di consegna o un'unità organizzativa specifici. In questo caso, si consiglia di disabilitare il criterio.

### Enable process monitoring (Abilita il monitoraggio dei processi)

Abilitare questa impostazione per consentire il monitoraggio dei processi in esecuzione su macchine con VDA. Le statistiche, ad esempio l'utilizzo della CPU e della memoria, vengono inviate al servizio di monitoraggio. Le statistiche vengono utilizzate per le notifiche in tempo reale e la creazione di report cronologici in Director.

Il valore predefinito per questa impostazione è Disabled (Disabilitato).

### Enable resource monitoring (Abilita il monitoraggio delle risorse)

Abilitare questa impostazione per consentire il monitoraggio dei contatori delle prestazioni critici sulle macchine con VDA. Le statistiche (ad esempio utilizzo della CPU e della memoria, IOPS e dati di latenza del disco) vengono inviate al servizio di monitoraggio. Le statistiche vengono utilizzate per le notifiche in tempo reale e la creazione di report cronologici in Director.

Il valore predefinito per questa impostazione è Enabled (Abilitato).

### Scalabilità

I dati della CPU e della memoria vengono inviati al database da ogni VDA a intervalli di 5 minuti. I dati dei processi (se abilitati) vengono inviati al database a intervalli di 10 minuti. I dati relativi a IOPS e alla latenza del disco vengono inviati al database a intervalli di 1 ora.

### Dati della CPU e della memoria

I dati della CPU e della memoria sono **abilitati** per impostazione predefinita. I valori di conservazione dei dati sono i seguenti (licenza Platinum):

| Granularità dei dati | Numero di giorni |
|---|---|
| Dati di 5 minuti | 1 giorno |
| Dati di 10 minuti | 7 giorni |
| Dati orari | 30 giorni |
| Dati giornalieri | 90 giorni |

**Dati relativi a IOPS e alla latenza del disco**

I dati relativi a IOPS e alla latenza del disco sono **abilitati** per impostazione predefinita. I valori di conservazione dei dati sono i seguenti (licenza Platinum):

| Granularità dei dati | Numero di giorni |
|---|---|
| Dati orari | 3 giorni |
| Dati giornalieri | 90 giorni |

Con le impostazioni di conservazione dei dati, sono necessari circa 276 KB di spazio su disco per archiviare quanto segue per un VDA nell'arco di un anno:

- CPU
- Memory (Memoria)
- IOPS
- Dati sulla latenza del disco

| Numero di macchine | Spazio di archiviazione approssimativo richiesto |
|---|---|
| 1 | 276 KB |
| 1K | 270 MB |
| 40K | 10,6 GB |

**Dati dei processi**

I dati dei processi sono **disabilitati** per impostazione predefinita. Si consiglia di abilitare i dati dei processi su un sottoinsieme di macchine in base alle esigenze. Le impostazioni predefinite di conservazione dei dati per i dati dei processi sono le seguenti:

| Granularità dei dati | Numero di giorni |
|---|---|
| Dati di 10 minuti | 1 giorno |
| Dati orari | 7 giorni |

Se i dati dei processi sono abilitati con le impostazioni di conservazione predefinite, consumerebbero circa 1,5 MB per VDA e 3 MB per VDA Servizi terminal (VDA TS) per un periodo di un anno.

| Numero di macchine | Spazio di archiviazione approssimativo richiesto per VDA | Spazio di archiviazione approssimativo richiesto per VDA TS |
|---|---|---|
| 1 | 1,5 MB | 3 MB |
| 1K | 1,5 GB | 3 GB |

> **Nota:**
>
> I numeri forniti in precedenza non includono lo spazio dell'indice e tutti i calcoli sono approssimativi e variano a seconda della distribuzione.

#### Configurazioni opzionali

È possibile modificare le impostazioni di conservazione predefinite in base alle proprie esigenze. Tuttavia, questa configurazione consuma spazio di archiviazione aggiuntivo. Abilitando le impostazioni riportate di seguito è possibile ottenere una maggiore precisione nei dati di utilizzo dei processi. Le configurazioni che possono essere abilitate sono:

**EnableMinuteLevelGranularityProcessUtilization**

**EnableDayLevelGranularityProcessUtilization**

Queste configurazioni possono essere abilitate dal cmdlet PowerShell Monitoring (Monitoraggio): Set-MonitorConfiguration

### Criteri per il monitoraggio degli errori delle applicazioni

Per impostazione predefinita, la scheda **Application Failure** (Errori applicazioni) visualizza solo gli errori delle applicazioni dei VDA con sistema operativo multisessione. Le impostazioni del monitoraggio degli errori delle applicazioni possono essere modificate con i criteri di monitoraggio seguenti:

#### Enable monitoring of application failures (Abilita il monitoraggio degli errori delle applicazioni)

Utilizzare questa impostazione per configurare il monitoraggio degli errori delle applicazioni per monitorare errori o problemi delle applicazioni (arresti anomali ed eccezioni non gestite) o entrambi. Disabilitare il monitoraggio degli errori delle applicazioni impostando il campo **Value** (Valore) su **None** (Nessuno).
Il valore predefinito per questa impostazione è Application faults only (Solo errori delle applicazioni).

#### Enable monitoring of application failures on Single-session OS VDAs (Abilita il monitoraggio degli errori delle applicazioni sui VDA con sistema operativo a sessione singola)

Per impostazione predefinita, vengono monitorati solo gli errori delle applicazioni ospitate sui VDA con sistema operativo multisessione. Per monitorare i VDA con sistema operativo a sessione singola, impostare il criterio su **Allowed** (Consentito).
Il valore predefinito per questa impostazione è **Prohibited** (Non consentito).

#### Elenco delle applicazioni escluse dal monitoraggio degli errori

Specificare un elenco di applicazioni che non devono essere monitorate in caso di errori.
Per impostazione predefinita, questo elenco è vuoto.

### Criterio per la raccolta di dati per le analisi

#### Raccolta dati VDA per le analisi

Utilizzare i criteri per abilitare o disabilitare il servizio Monitor di raccolta di metriche relative alle prestazioni dei VDA per le analisi di prestazioni e sicurezza. Per impostazione predefinita, i criteri sono **Allowed** (Consentiti). Impostare i criteri su **Prohibited** (Vietato) per interrompere la raccolta di dati dai VDA.

#### Inserire negli Appunti la raccolta di metadati per il monitoraggio della sicurezza

Utilizzare il criterio per abilitare o disabilitare la raccolta di metadati degli appunti da parte del servizio Broker per il monitoraggio, il controllo e la conformità della sicurezza. Per impostazione predefinita, il criterio è **Enabled** (Abilitato). Impostare il criterio su **Disabled** (Disabilitato) per interrompere la raccolta di dati dai VDA.

### Consigli per la pianificazione dello spazio di archiviazione

**Criterio di gruppo**. Se non si è interessati a monitorare i dati delle risorse o i dati dei processi, uno o entrambi possono essere disabilitati utilizzando i criteri di gruppo. Per ulteriori informazioni, vedere la sezione **Criteri di gruppo** di Creare criteri.

**Pulitura dei dati**. Le impostazioni predefinite per la conservazione dei dati possono essere modificate per pulire i dati in anticipo e liberare spazio di archiviazione. Per ulteriori informazioni sulle impostazioni di pulizia, vedere Granularità e conservazione dei dati in Accesso ai dati tramite l'API.

## Impostazioni dei criteri dell'IP virtuale

January 7, 2024

> **Importante:**
>
> Windows 10 Enterprise multisessione non supporta la virtualizzazione IP di Desktop remoto (IP virtuale) e Citrix non supporta né l'IP virtuale né il loopback virtuale in Windows 10 Enterprise multisessione.

La sezione **Virtual IP** (IP virtuale) include impostazioni dei criteri che controllano se le sessioni hanno il proprio indirizzo di loopback virtuale.

### Virtual IP loopback support (Supporto per loopback dell'IP virtuale)

Quando questa impostazione è abilitata, ogni sessione ha il proprio indirizzo di loopback virtuale. Se è disabilitata, le sessioni non hanno indirizzi di loopback individuali.

Per impostazione predefinita, questa impostazione è disabilitata.

### Virtual IP virtual loopback programs list (Elenco dei programmi di loopback virtuale dell'IP virtuale)

Questa impostazione specifica i file eseguibili dell'applicazione che possono utilizzare indirizzi di loopback virtuali. Quando si aggiungono programmi all'elenco, specificare solo il nome del file eseguibile. Non è necessario specificare l'intero percorso.

Per impostazione predefinita, non vengono specificati file eseguibili.

# Configurare le impostazioni di reindirizzamento delle porte COM e LPT utilizzando il Registro di sistema

January 7, 2024

Nelle versioni di VDA da 7.0 a 7.8, le impostazioni **della porta COM e della porta LPT** sono configurabili solo utilizzando il Registro di sistema. Per le versioni di VDA precedenti alla 7.0 e per le versioni di VDA 7.9 e successive, queste impostazioni sono configurabili in Web Studio. Per ulteriori informazioni, vedere Impostazioni dei criteri di reindirizzamento delle porte e Impostazioni dei criteri di larghezza di banda.

Le impostazioni dei criteri per il reindirizzamento della porta COM e della porta LPT si trovano in HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated sull'immagine o sulla macchina VDA.

Per abilitare il reindirizzamento della porta COM e della porta LPT, aggiungere nuove chiavi del Registro di sistema di tipo REG_DWORD, come segue:

Attenzione: la modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

| Chiave del Registro di sistema | Descrizione | Valori consentiti |
|---|---|---|
| AllowComPortRedirection | Consentire o vietare il reindirizzamento della porta COM | 1 (Consenti) o 0 (Vieta) |
| LimitComBw | Limite di larghezza di banda per il canale di reindirizzamento della porta COM | Valore numerico |
| LimitComBWPercent | Limite di larghezza di banda per il canale di reindirizzamento della porta COM come percentuale della larghezza di banda totale della sessione | Valore numerico compreso tra 0 e 100 |
| AutoConnectClientComPorts | Connettere automaticamente le porte COM dal dispositivo utente | 1 (Consenti) o 0 (Vieta) |

| Chiave del Registro di sistema | Descrizione | Valori consentiti |
|---|---|---|
| AllowLptPortRedirection | Consentire o vietare il reindirizzamento della porta LPT | 1 (Consenti) o 0 (Vieta) |
| LimitLptBw | Limite di larghezza di banda per il canale di reindirizzamento della porta LPT | Valore numerico |
| LimitLptBwPercent | Limite di larghezza di banda per il canale di reindirizzamento della porta LPT come percentuale della larghezza di banda totale della sessione | Valore numerico compreso tra 0 e 100 |
| AutoConnectClientLptPorts | Connettere automaticamente le porte LPT dal dispositivo utente | 1 (Consenti) o 0 (Vieta) |

Dopo aver configurato queste impostazioni, modificare i cataloghi della macchina per utilizzare la nuova immagine master o la macchina fisica aggiornata. I desktop vengono aggiornati con le nuove impostazioni allo scollegamento successivo degli utenti.

## Impostazioni dei criteri di Connector per Configuration Manager 2012

January 7, 2024

La sezione Connector per Configuration Manager 2012 contiene le impostazioni dei criteri per la configurazione dell'agente Citrix Connector 7.5.

> **Importante:**
>
> I criteri dei messaggi di avviso, scollegamento e riavvio si applicano solo alle distribuzioni ai cataloghi di macchine con sistema operativo multisessione gestiti manualmente o tramite Provisioning Services. Per questi cataloghi di macchine, il servizio del connettore avvisa gli utenti quando sono presenti installazioni di applicazioni o aggiornamenti software in sospeso.

Per i cataloghi gestiti da MCS, utilizzare Web Studio per avvisare gli utenti. Per i cataloghi del sistema operativo a sessione singola gestiti manualmente, utilizzare Configuration Manager per avvisare gli utenti. Per i cataloghi del sistema operativo a sessione singola gestiti da Provisioning Services, utilizzare Provisioning Services per avvisare gli utenti.

### Warning frequency interval (Intervallo di frequenza di avviso)

Questa impostazione definisce l'intervallo tra le visualizzazioni del messaggio di avviso per gli utenti.

Gli intervalli sono impostati utilizzando il formato ggg.hh:mm:ss, in cui:

- ggg corrisponde a "giorni", un parametro opzionale, con un intervallo compreso tra 0 e 999.
- hh corrisponde a "ore", con un intervallo compreso tra 0 e 23.
- mm corrisponde a "minuti", con un intervallo compreso tra 0 e 59.
- ss corrisponde a "secondi", con un intervallo compreso tra 0 e 59.

Per impostazione predefinita, l'impostazione dell'intervallo è di 1 ora (01:00:00).

### Warning message box body text (Testo della finestra del messaggio di avviso)

Questa impostazione contiene il testo modificabile del messaggio mostrato agli utenti, che li avvisa di aggiornamenti del software o manutenzione imminenti che richiedono lo scollegamento.

Per impostazione predefinita, il messaggio è: {TIMESTAMP} Save your work (Salvare il lavoro). The server goes offline for maintenance in {TIMELEFT} (Il server passerà alla modalità offline per manutenzione in {TIMELEFT}).

### Warning message box title (Titolo della finestra di messaggio di avviso)

Questa impostazione contiene il testo modificabile della barra del titolo del messaggio di avviso mostrato agli utenti.

Per impostazione predefinita, il titolo è: Upcoming Maintenance (Manutenzione imminente).

### Warning time period (Periodo di avvertimento)

Questa impostazione definisce quanto tempo prima della manutenzione viene visualizzato il messaggio di avviso.

L'ora è impostata utilizzando il formato ggg.hh:mm:ss, dove:

- ggg corrisponde a "giorni", un parametro opzionale, con un intervallo compreso tra 0 e 999.
- hh corrisponde a "ore", con un intervallo compreso tra 0 e 23.
- mm corrisponde a "minuti", con un intervallo compreso tra 0 e 59.
- ss corrisponde a "secondi", con un intervallo compreso tra 0 e 59.

Per impostazione predefinita, l'impostazione è 16 ore (16:00:00), il che indica che il primo messaggio di avviso viene visualizzato circa 16 ore prima della manutenzione.

### Final force logoff message box body text (Testo del messaggio di scollegamento forzato finale)

Questa impostazione contiene il testo modificabile del messaggio che avvisa gli utenti che è iniziato uno scollegamento forzato.

Per impostazione predefinita, il messaggio è: The server is currently going offline for maintenance (Il server sta passando alla modalità offline per la manutenzione)

### Final force logoff message box title (Titolo del messaggio di scollegamento forzato finale)

Questa impostazione contiene il testo modificabile della barra del titolo del messaggio finale di scollegamento forzato.

Per impostazione predefinita, il titolo è: Notification From IT Staff (Notifica da parte del personale IT).

### Force logoff grace period (Periodo di tolleranza dello scollegamento forzato)

Questa impostazione definisce il tempo che trascorre tra l'invio della notifica di scollegamento agli utenti e l'implementazione dello scollegamento forzato per eseguire la manutenzione in sospeso.

L'ora è impostata utilizzando il formato ggg.hh:mm:ss, dove:

- ggg corrisponde a "giorni", un parametro opzionale, con un intervallo compreso tra 0 e 999.
- hh corrisponde a "ore", con un intervallo compreso tra 0 e 23.
- mm corrisponde a "minuti", con un intervallo compreso tra 0 e 59.
- ss corrisponde a "secondi", con un intervallo compreso tra 0 e 59.

Per impostazione predefinita, l'impostazione del periodo di tolleranza dello scollegamento forzato è di 5 minuti (00:05:00).

### Force logoff message box body text (Testo del messaggio di scollegamento forzato)

Questa impostazione contiene il testo modificabile del messaggio che indica agli utenti di salvare il lavoro e scollegarsi prima di avviare uno scollegamento forzato.

Per impostazione predefinita, il messaggio contiene quanto segue: {TIMESTAMP} Save your work and log off (Salvare il lavoro e scollegarsi). The server goes offline for maintenance in {TIMELEFT} (Il server passerà alla modalità offline per manutenzione in {TIMELEFT}).

### Force logoff message box title (Titolo del messaggio di scollegamento forzato)

Questa impostazione contiene il testo modificabile della barra del titolo del messaggio di scollegamento forzato.

Per impostazione predefinita, il titolo è: Notification From IT Staff (Notifica da parte del personale IT).

### Image-managed mode (Modalità gestita da immagini)

L'agente del connettore rileva automaticamente se è in esecuzione su un clone di una macchina gestito da Provisioning Services o MCS. L'agente blocca gli aggiornamenti di Configuration Manager sui cloni gestiti da immagini e installa automaticamente gli aggiornamenti sull'immagine master del catalogo.

Dopo aver aggiornato un'immagine master, utilizzare Web Studio per orchestrare il riavvio dei cloni del catalogo MCS. L'agente del connettore orchestra automaticamente il riavvio dei cloni del catalogo PVS durante le finestre di manutenzione di Configuration Manager. Per ignorare questo comportamento in modo che il software sia installato sui cloni del catalogo da Configuration Manager, modificare la modalità gestita da immagini su Disabled (Disabilitata).

### Reboot message box body text (Testo del messaggio di riavvio)

Questa impostazione contiene il testo modificabile del messaggio che avvisa gli utenti quando il server sta per essere riavviato.

Per impostazione predefinita, il messaggio è: The server is currently going offline for maintenance (Il server è attualmente offline per la manutenzione).

### Regular time interval at which the agent task is to run (Intervallo di tempo regolare in base al quale l'attività dell'agente deve essere eseguita)

Questa impostazione determina la frequenza con cui viene eseguita l'attività dell'agente Citrix Connector.

L'ora è impostata utilizzando il formato ggg.hh:mm:ss, dove:

- ggg corrisponde a "giorni", un parametro opzionale, con un intervallo compreso tra 0 e 999.
- hh corrisponde a "ore", con un intervallo compreso tra 0 e 23.
- mm corrisponde a "minuti", con un intervallo compreso tra 0 e 59.
- ss corrisponde a "secondi", con un intervallo compreso tra 0 e 59.

Per impostazione predefinita, l'impostazione dell'intervallo di tempo normale è di 5 minuti (00:05:00).

# Gestione

January 7, 2024

La gestione di un sito Citrix Virtual Apps and Desktops copre vari elementi e attività.

### Licenze

Quando si crea un sito, è necessaria una connessione valida al Citrix License Server. In seguito, è possibile completare diverse attività relative alle licenze da Studio, tra cui l'aggiunta di licenze, la modifica dei tipi o dei modelli di licenze e la gestione degli amministratori delle licenze. È inoltre possibile accedere alla Console di amministrazione delle licenze da Studio.

### Applicazioni

Gestire le applicazioni nei Gruppi di consegna e, facoltativamente, nei gruppi di applicazioni.

### Zone

In una distribuzione a dispersione geografica, è possibile utilizzare le zone per mantenere le applicazioni e i desktop più vicini agli utenti finali, migliorando così le prestazioni. Quando si installa e configura un sito, tutti i controller, i cataloghi di macchine e le connessioni host si trovano in un'unica zona primaria. Successivamente, è possibile utilizzare Studio per creare zone satellite contenenti tali elementi. Dopo che il sito ha più di una zona, sarà possibile indicare in quale zona verranno inseriti tutti i cataloghi di macchine, le connessioni host o i controller aggiunti appena creati. È inoltre possibile spostare gli elementi da una zona all'altra.

### Connessioni e risorse

Se si utilizza un hypervisor o un altro servizio di hosting delle macchine che fornisce applicazioni e desktop agli utenti, si crea la prima connessione a tale hypervisor o all'altro servizio quando si crea un sito. I dettagli di archiviazione e rete per tale connessione costituiscono le sue risorse. In seguito, è possibile modificare tale connessione e le relative risorse e creare altre connessioni. È inoltre possibile gestire le macchine che utilizzano una connessione configurata.

### Cache host locale

La cache host locale consente la continuazione delle operazioni di intermediazione della connessione in un sito quando la connessione tra un Delivery Controller e il database del sito si interrompe.

### IP virtuale e loopback virtuale

La funzionalità di indirizzo IP virtuale di Microsoft fornisce a un'applicazione pubblicata un indirizzo IP univoco assegnato dinamicamente per ciascuna sessione. La funzione di loopback virtuale Citrix consente di configurare applicazioni che dipendono dalle comunicazioni con localhost per utilizzare un indirizzo di loopback virtuale univoco compreso nell'intervallo localhost.

### Delivery Controller

Questo articolo contiene considerazioni e procedure relative all'aggiunta e la rimozione di controller da un sito. Viene inoltre descritto come spostare i controller in un'altra zona o sito e come spostare un VDA in un altro sito.

### Registrazione dei VDA con i controller

Prima di poter aiutare a distribuire applicazioni e desktop, un VDA deve registrarsi (stabilire la comunicazione) con un controller. Gli indirizzi dei controller possono essere specificati in diversi modi, descritti in questo articolo. È fondamentale che i VDA dispongano di informazioni correnti quando i controller vengono aggiunti, spostati e rimossi nel sito.

### Sessioni

Mantenere l'attività della sessione è fondamentale per fornire la migliore esperienza utente. Diverse funzionalità possono ottimizzare l'affidabilità delle sessioni, ridurre gli inconvenienti, i tempi di inattività e la perdita di produttività.

- Affidabilità della sessione
- Riconnessione automatica del client
- ICA Kep-Alive
- Controllo di Workspace
- Roaming di sessione

### Uso della ricerca in Studio

Quando si desidera visualizzare informazioni su macchine, sessioni, cataloghi macchine, applicazioni o gruppi di consegna in Studio, utilizzare la funzionalità di ricerca flessibile.

### Tag

Utilizzare i tag per identificare elementi quali macchine, applicazioni, gruppi e criteri. Sarà quindi possibile personalizzare determinate operazioni da applicare agli elementi con un tag specifico.

### IPv4/IPv6

Citrix Virtual Apps and Desktops supporta le distribuzioni IPv4 pure, IPv6 pure e dual-stack che utilizzano reti IPv4 e IPv6 sovrapposte. In questo articolo vengono descritte e illustrate queste distribuzioni. Vengono inoltre descritte le impostazioni dei criteri Citrix che controllano l'utilizzo di IPv4 o IPv6.

### Profili utente

Per impostazione predefinita, Citrix Profile Management viene installato automaticamente quando si installa un VDA. Se si utilizza questa soluzione per il profilo, vedere questo articolo per informazioni generali. Vedere la documentazione di Profile Management per i dettagli.

### Acquisire tracce Citrix Diagnostic Facility (CDF)

L'utilità CDFControl è un controller di tracciamento eventi o consumer per l'acquisizione di messaggi di traccia Citrix Diagnostic Facility (CDF) visualizzati da vari provider di tracciamento Citrix. Il suo ruolo è risolvere problemi complessi relativi a Citrix, analizzare il supporto del filtro e raccogliere dati sulle prestazioni.

### Citrix Insight Services

Citrix Insight Services (CIS) è una piattaforma Citrix per la strumentazione, la telemetria e la generazione di informazioni aziendali.

### Citrix Scout

Citrix Scout raccoglie la diagnostica ed esegue controlli di integrità. È possibile utilizzarne i risultati per la manutenzione proattiva nella distribuzione di Citrix Virtual Apps and Desktops. Citrix offre un'analisi completa e automatizzata delle raccolte di diagnostica tramite Citrix Insight Services. È inoltre possibile utilizzare Scout per risolvere i problemi, in autonomia o con le indicazioni del supporto Citrix.

## Applicazioni

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

### Introduzione

Se la distribuzione utilizza solo gruppi di consegna (e non gruppi di applicazioni), si aggiungono le applicazioni ai gruppi di consegna. Se si dispone anche di gruppi di applicazioni, in genere si aggiungono le applicazioni ai gruppi di applicazioni. Questa guida fornisce una gestione più semplice. Un'applicazione deve sempre appartenere ad almeno un gruppo di consegna o a un gruppo di applicazioni.

Nella procedura guidata Add Applications (Aggiungi applicazioni) è possibile selezionare uno o più gruppi di consegna o uno o più gruppi di applicazioni, ma non entrambi. Sebbene sia possibile modificare in seguito l'associazione a gruppi di un'applicazione (ad esempio, spostando un'applicazione da un gruppo di applicazioni a un gruppo di consegna), le pratiche migliori sconsigliano l'aggiunta di tale complessità. Mantenere le proprie applicazioni in un unico tipo di gruppo.

Quando si associa un'applicazione a più gruppi, può crearsi un problema di visibilità se non si dispone di autorizzazioni sufficienti a visualizzare l'applicazione in tutti questi gruppi. In questi casi, vedere un amministratore con autorizzazioni di livello superiore o estendere il proprio ambito in modo da includere tutti i gruppi a cui è stata aggiunta l'applicazione.

Se si pubblicano due applicazioni con lo stesso nome (magari di gruppi diversi) per gli stessi utenti, modificare la proprietà `Application name (for user)` in Web Studio. In caso contrario, gli utenti vedranno nomi duplicati nell'app Citrix Workspace.

È possibile modificare le proprietà (impostazioni) di un'applicazione al momento dell'aggiunta o in un secondo momento. È inoltre possibile modificare la cartella di applicazioni in cui è posizionata l'applicazione, quando si aggiunge l'applicazione o in un secondo momento.

Per ulteriori informazioni, vedere:

- Creare gruppi di consegna
- Creare gruppi di applicazioni
- Tag

### Aggiungere applicazioni

È possibile aggiungere applicazioni quando si crea un gruppo di consegna o un gruppo di applicazioni. Tali procedure sono illustrate dettagliatamente in Creare gruppi di consegna e Creare gruppi di applicazioni. Nella procedura seguente viene descritto come aggiungere applicazioni dopo aver creato un gruppo.

Buono a sapersi:

- Non è possibile aggiungere applicazioni ai gruppi di consegna Accesso remoto PC.
- Non è possibile utilizzare la procedura guidata Add Application (Aggiungi applicazione) per rimuovere le applicazioni dai gruppi di consegna o dai gruppi di applicazioni. Questa è un'operazione separata.

Per aggiungere una o più applicazioni:

1. Selezionare **Applications** nel riquadro a sinistra di Studio, quindi selezionare **Add Applications** (Aggiungi applicazioni) nella barra delle azioni.
2. Viene avviata la procedura guidata con la pagina **Introduction**, che può essere rimossa dai futuri avvii della procedura guidata.

3. La procedura guidata guida l'utente attraverso le pagine **Groups** (Gruppi), **Applications** (Applicazioni) e **Summary** (Riepilogo). Al termine di ogni pagina, fare clic su **Next** (Avanti) fino a raggiungere la pagina **Summary** (Riepilogo).

Alternative al passaggio 1 se si desidera aggiungere applicazioni a un solo gruppo di consegna o a un solo gruppo di applicazioni:

- **Per aggiungere applicazioni a un solo gruppo di consegna:** nel passaggio 1 selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra di Web Studio, selezionare un gruppo di consegna nel riquadro centrale e quindi selezionare **Add Applications** (Aggiungi applicazioni) nella barra delle azioni. La procedura guidata non visualizza la pagina **Groups** (Gruppi).
- **Per aggiungere applicazioni a un solo gruppo di applicazioni:** nel passaggio 1 selezionare **Applications** nel riquadro a sinistra di Web Studio, selezionare un gruppo di applicazioni nel riquadro centrale e quindi selezionare la voce **Add Applications** (Aggiungi applicazioni) sotto il nome del gruppo di applicazioni nella barra delle azioni. La procedura guidata non visualizza la pagina **Groups** (Gruppi).

#### Pagina Groups

Questa pagina elenca tutti i gruppi di consegna del sito. Se sono stati creati anche gruppi di applicazioni, nella pagina sono elencati i gruppi di applicazioni e i gruppi di consegna. È possibile scegliere da uno o dall'altro gruppo, ma non da entrambi i gruppi. In altre parole, non è possibile aggiungere applicazioni a un gruppo di applicazioni e a un gruppo di consegna allo stesso tempo. Come orientamento generale, se si utilizzano gruppi di applicazioni, aggiungere applicazioni ai gruppi di applicazioni anziché ai gruppi di consegna.

Quando si aggiunge un'applicazione, selezionare la casella di controllo accanto ad almeno un gruppo di consegna (o gruppo di applicazioni, se disponibile). Ogni applicazione deve sempre essere associata ad almeno un gruppo.

#### Pagina delle applicazioni

Fare clic su **Add** per visualizzare le origini delle applicazioni.

- **Menu From Start:** applicazioni che vengono individuate su una macchina nei gruppi di consegna selezionati. Quando si seleziona questa origine, viene avviata una nuova pagina con un elenco delle applicazioni individuate. Selezionare le caselle di controllo delle applicazioni da aggiungere e quindi fare clic su **OK**.

  Questa origine non può essere selezionata se sono stati selezionati (1) gruppi di applicazioni senza gruppi di consegna associati, (2) gruppi di applicazioni selezionati con gruppi di consegna associati non contenenti macchine o (3) un gruppo di consegna non contenente macchine.

- **Manually:** applicazioni situate su un VDA nel gruppo di consegna o in altre parti della rete. Selezionando questa fonte si apre una nuova pagina in cui è possibile specificare un'applicazione da aggiungere nei seguenti modi:
  - Digitare il percorso dell'eseguibile, la directory di lavoro, gli argomenti della riga di comando facoltativi e i nomi visualizzati per amministratori e utenti.
  - Selezionare un'applicazione da un VDA del gruppo di consegna. A tale scopo, fare clic su **Browse** (Sfoglia), immettere le credenziali per accedere al VDA, attendere di essere connessi al VDA e quindi selezionare un'applicazione dal VDA. Le proprietà dell'applicazione selezionata compilano automaticamente i campi della pagina.
- **Existing** (Esistenti): applicazioni precedentemente aggiunte al sito. Quando si seleziona questa origine, viene avviata una nuova pagina con un elenco delle applicazioni individuate. Selezionare le caselle di controllo delle applicazioni da aggiungere e quindi fare clic su **OK**.

  Non è possibile selezionare questa origine se il sito non dispone di applicazioni.
- **App-V**: applicazioni contenute in pacchetti App-V. Quando si seleziona questa origine, viene avviata una nuova pagina in cui si seleziona il server App-V o la libreria di applicazioni. Nella schermata risultante, selezionare le caselle di controllo delle applicazioni da aggiungere e quindi fare clic su **OK**. Per ulteriori informazioni, vedere applications.Distribuire e rendere disponibili applicazioni App-V.

  Questa origine non può essere selezionata se App-V non è configurato per il sito.
- **Application Group**: gruppi di applicazioni. Quando si seleziona questa origine, viene avviata una nuova pagina con un elenco dei gruppi di applicazioni (sebbene siano elencate anche le applicazioni presenti in ciascun gruppo, è possibile selezionare solo il gruppo, non le singole applicazioni). Vengono aggiunte tutte le applicazioni attuali e future nei gruppi selezionati. Selezionare le caselle di controllo dei gruppi di applicazioni da aggiungere e quindi fare clic su **OK**.

  Questa origine non può essere selezionata se (1) non esistono gruppi di applicazioni o (2) se i gruppi di consegna selezionati non supportano i gruppi di applicazioni (ad esempio, gruppi di consegna con computer assegnati in modo statico).

Come indicato nella tabella, alcune origini presenti nell'elenco **Add** non possono essere selezionate se non esiste un'origine valida di quel tipo. Le origini che sono incompatibili (ad esempio, non è possibile aggiungere gruppi di applicazioni ai gruppi di applicazioni) non sono incluse nell'elenco. Le applicazioni già aggiunte ai gruppi scelti non possono essere selezionate.

È possibile modificare le proprietà (impostazioni) di un'applicazione da questa pagina o successivamente.

Per impostazione predefinita, le applicazioni aggiunte vengono inserite nella cartella dell'applicazione denominata `Applications`. È possibile modificare l'applicazione da questa pagina o

successivamente. Se si tenta di aggiungere un'applicazione e in quella cartella ne esiste già una con lo stesso nome, verrà richiesto di rinominare l'applicazione che si sta aggiungendo. È possibile accettare il nuovo nome offerto o rifiutarlo e quindi rinominare l'applicazione o selezionare una cartella diversa. Ad esempio, se `app` esiste già nella cartella **Applications** e si tenta di aggiungere un'altra applicazione denominata `app` a quella cartella, viene offerto il nuovo nome `app_1`.

#### Pagina Summary

Se si aggiungono 10 o meno applicazioni, i loro nomi sono elencati in **Applications to add** (Applicazioni da aggiungere). Se si aggiungono più di 10 applicazioni, ne è indicato il numero totale.

Esaminare le informazioni di riepilogo e quindi fare clic su **Finish**.

### Modificare l'associazione a un gruppo di un'applicazione

Dopo aver aggiunto un'applicazione, è possibile modificare i gruppi di consegna e i gruppi di applicazioni a cui è associata.

È possibile trascinare un'applicazione in un gruppo aggiuntivo. Questa è un'alternativa all'utilizzo dei comandi disponibili nella barra delle azioni.

Se un'applicazione è associata a più di un gruppo di consegna o di applicazioni, è possibile utilizzare la priorità di gruppo per specificare l'ordine in cui vengono controllati più gruppi per trovare le applicazioni. Per impostazione predefinita, tutti i gruppi hanno priorità 0 (la più elevata). I gruppi con la stessa priorità hanno il carico bilanciato.

Un gruppo di applicazioni può essere associato a gruppi di consegna contenenti macchine condivise (non private) in grado di distribuire applicazioni. È inoltre possibile selezionare gruppi di consegna contenenti macchine condivise che distribuiscono solo desktop, se (1) il gruppo di consegna contiene macchine condivise ed è stato creato con una versione di XenDesktop 7.x precedente alla 7.9 e (2) si dispone dell'autorizzazione `Edit delivery group`. Il tipo di gruppo di consegna viene convertito automaticamente in `desktops and applications` quando viene confermata la finestra di dialogo delle proprietà.

1. Accedere a Web Studio, selezionare **Applications** nel riquadro a sinistra, quindi selezionare l'applicazione.
2. Selezionare **Properties** (Proprietà) nella barra delle azioni.
3. Seleziona la pagina **Groups** (Gruppi).

    - Per aggiungere un gruppo, fare clic su **Add** e selezionare **Application Groups** (Gruppi di applicazioni) o **Delivery Groups** (Gruppi di consegna). Se non si è creato alcun gruppo di applicazioni, l'unica voce disponibile è **Delivery Groups**. Selezionare quindi uno o più

gruppi disponibili. I gruppi non compatibili con l'applicazione o già associati a essa non possono essere selezionati.
- Per rimuovere un gruppo, selezionare uno o più gruppi e quindi fare clic su **Remove** (Rimuovi). Se la rimozione dell'associazione di gruppo comporta che l'applicazione non viene più associata ad alcun gruppo, viene visualizzato un avviso che l'applicazione sarà eliminata.
- Per modificare la priorità di un gruppo, selezionare il gruppo e quindi fare clic su **Edit Priority** (Modifica priorità). Selezionare un valore di priorità e quindi fare clic su **OK**.

4. Al termine, fare clic su **Apply** per applicare le modifiche apportate e lasciare aperta la finestra oppure su **OK** per applicare le modifiche e chiudere la finestra.

### Duplicare, abilitare o disabilitare, rinominare o eliminare un'applicazione

Sono disponibili le seguenti azioni:

- **Duplicate:** potrebbe essere opportuno duplicare un'applicazione per creare una versione diversa con parametri o proprietà diversi. Quando si duplica un'applicazione, questa viene automaticamente rinominata con un suffisso univoco e posizionata accanto all'originale. Potrebbe anche essere opportuno duplicare un'applicazione per poi aggiungerla a un altro gruppo. Dopo la duplicazione, il modo più semplice per spostare un'applicazione è trascinarla.
- **Enable or disable:** l'attivazione e la disattivazione di un'applicazione è un'azione diversa dall'attivazione e dalla disabilitazione di un gruppo di consegna o di un gruppo di applicazioni.
- **Rename:** è possibile rinominare solo un'applicazione alla volta. Se si tenta di rinominare un'applicazione e ne esiste già una con lo stesso nome nella stessa cartella o nello stesso gruppo, viene richiesto di specificare un nome diverso.
- **Delete:** l'eliminazione di un'applicazione la rimuove dai gruppi di consegna e dai gruppi di applicazioni a cui è stata associata, ma non dall'origine utilizzata per aggiungere l'applicazione inizialmente. L'eliminazione di un'applicazione è un'azione diversa dalla rimozione da un gruppo di consegna o da un gruppo di applicazioni.

Per duplicare, abilitare, disabilitare, rinominare o eliminare un'applicazione:

1. Selezionare **Applications** nel riquadro a sinistra.
2. Selezionare una o più applicazioni nel riquadro centrale e quindi selezionare l'attività appropriata nella barra delle azioni.
3. Confermare l'azione, quando richiesto.

### Rimuovere le applicazioni da un gruppo di consegna

Un'applicazione deve essere associata (appartenere) ad almeno un gruppo di consegna o un gruppo di applicazioni. Se si tenta di rimuovere un'applicazione da un gruppo di consegna che

comporterebbe la rimozione dell'associazione di tale applicazione con qualsiasi gruppo di consegna o gruppo di applicazioni, viene notificato che l'applicazione verrà eliminata se si continua. Quando ciò accade, se si desidera distribuire l'applicazione, è necessario aggiungerla di nuovo da un'origine valida.

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo di consegna. Nel riquadro centrale inferiore, nella scheda **Applications**, selezionare l'applicazione che si desidera rimuovere.
3. Selezionare **Remove Application** (Rimuovi applicazione) nella barra delle azioni.
4. Confermare la rimozione.

### Rimuovere le applicazioni da un gruppo di applicazioni

Un'applicazione deve appartenere ad almeno un gruppo di consegna o un gruppo di applicazioni. Se si tenta di rimuovere un'applicazione da un gruppo di applicazioni con la conseguenza che tale applicazione non apparterrà più ad alcun gruppo, viene notificato che l'applicazione verrà eliminata se si continua. Quando ciò accade, se si desidera distribuire l'applicazione, è necessario aggiungerla di nuovo da un'origine valida.

1. Selezionare **Applications** nel riquadro a sinistra.
2. Selezionare il gruppo di applicazioni nel riquadro centrale, quindi selezionare una o più applicazioni.
3. Selezionare **Remove from Application Group** (Rimuovi dal gruppo di applicazioni) nella barra delle azioni.
4. Confermare la rimozione.

### Modificare le proprietà dell'applicazione

È possibile modificare le proprietà di una sola applicazione alla volta.

Per modificare le proprietà di un'applicazione:

1. Selezionare **Applications** nel riquadro a sinistra.
2. Selezionare un'applicazione e quindi selezionare **Edit Application Properties** (Modifica proprietà applicazione) nella barra delle azioni.
3. Selezionare la pagina contenente la proprietà che si desidera modificare.
4. Al termine, fare clic su **Apply** per applicare le modifiche apportate e mantenere aperta la finestra oppure su **OK** per applicare le modifiche e chiudere la finestra.

Nell'elenco seguente, la pagina viene mostrata tra parentesi.

| Proprietà | Pagina |
|---|---|
| Categoria/cartella in cui viene visualizzata l'applicazione nell'app Citrix Workspace | Delivery |
| Argomenti della riga di comando; vedere Passare parametri alle applicazioni pubblicate | Posizione |
| Gruppi di consegna e gruppi di applicazioni in cui l'applicazione è disponibile | Groups |
| Descrizione | Identification |
| Estensioni dei nomi di file e associazione di tipi di file: quali estensioni l'applicazione apre automaticamente | File Type Association |
| Icona | Delivery |
| Parole chiave per StoreFront | Identification |
| Limiti; vedere Configure application limits | Delivery |
| Nome: nomi visti dall'utente e dall'amministratore | Identification |
| Percorso dell'eseguibile; vedere Passare parametri alle applicazioni pubblicate | Posizione |
| Collegamento sul desktop dell'utente: abilitare o disabilitare | Delivery |
| Visibilità: limita gli utenti che possono visualizzare l'applicazione nell'app Citrix Workspace. È comunque possibile avviare un'applicazione invisibile. Per renderla non disponibile e invisibile, aggiungerla a un gruppo diverso. | Limit Visibility |
| Directory di lavoro | Posizione |

Le modifiche apportate alle applicazioni potrebbero non avere effetto per gli utenti correnti dell'applicazione finché non si scollegano dalle sessioni.

### Configurare i limiti delle applicazioni

Si configurano i limiti delle applicazioni per facilitare la gestione dell'uso delle applicazioni. Ad esempio, è possibile utilizzare i limiti delle applicazioni per gestire il numero di utenti che accedono a un'applicazione allo stesso tempo. Analogamente, i limiti delle applicazioni possono essere utilizzati

per gestire il numero di istanze simultanee delle applicazioni a uso intensivo di risorse. Tale limite può aiutare a mantenere le prestazioni del server e a prevenire il deterioramento del servizio.

Questa funzionalità limita il numero di lanci di applicazioni intermediati dal controller (ad esempio, dall'app Citrix Workspace e da StoreFront) e non il numero di applicazioni in esecuzione che possono essere avviate con altri metodi. Ciò significa che i limiti delle applicazioni assistono gli amministratori nella gestione dell'utilizzo simultaneo, ma non si applicano a tutti gli scenari. Ad esempio, i limiti delle applicazioni non possono essere applicati quando il controller è in modalità di interruzione.

Per impostazione predefinita, non c'è limite al numero di istanze di un'applicazione che possono essere eseguite allo stesso tempo. Esistono diverse impostazioni per il limite delle applicazioni. È possibile configurarne una o configurarle tutte.

- Numero massimo di istanze simultanee dell'applicazione da parte di tutti gli utenti del gruppo di consegna.
- Un'istanza dell'applicazione per utente all'interno del gruppo di consegna.
- Numero massimo di istanze simultanee dell'applicazione per macchina (solo PowerShell).

Se è configurato un limite, viene generato un messaggio di errore quando un utente tenta di avviare un'istanza dell'applicazione che supererà il limite configurato. Se è configurato più di un limite, viene segnalato un errore quando viene raggiunto il primo limite.

Esempi che utilizzano i limiti delle applicazioni:

- **Limite di numero massimo di istanze simultanee:** in un gruppo di consegna, è possibile configurare il numero massimo di istanze simultanee dell'applicazione `Alpha` su 15. Successivamente, gli utenti di quel gruppo di consegna hanno 15 istanze di tale applicazione in esecuzione allo stesso tempo. Se un utente di quel gruppo di consegna ora tenta di avviare `Alpha`, viene generato un messaggio di errore. L'applicazione `Alpha` non viene avviata perché supererebbe il limite di istanze dell'applicazione simultanee configurato (15).
- **Limite di applicazioni di una sola istanza per utente:** in un altro gruppo di consegna, si abilita l'opzione di un'istanza per utente per l'applicazione `Beta`. L'utente Tony completa l'avvio dell'applicazione `Beta`. Più tardi quello stesso giorno, mentre quell'applicazione è ancora in esecuzione nella sua sessione, Tony tenta di lanciare un'altra istanza di `Beta`. Viene generato un messaggio di errore e l'applicazione `Beta` non viene avviata perché supererebbe il limite di un'istanza per utente.
- **Limiti di numero massimo di istanze simultanee e di una istanza per utente:** in un altro gruppo di consegna, è possibile configurare un numero massimo di istanze simultanee di 10 e abilitare l'opzione di un'istanza per utente per l'applicazione `Delta`. Successivamente, quando 10 utenti di quel gruppo di consegna hanno ciascuno un'istanza di `Delta` esecuzione, qualsiasi altro utente del gruppo di consegna che tenta di avviare `Delta` riceverà un messaggio di errore. L'applicazione `Delta` non viene avviata. Se uno degli attuali 10 utenti di `Delta`

tenta di avviare una seconda istanza di tale applicazione, questi riceverà un messaggio di errore e la seconda istanza non verrà avviata.

- **Numero massimo di istanze simultanee per macchina e utilizzo di restrizioni tag:** l'applicazione `Charlie` ha requisiti di licenza e prestazioni che dettano quante istanze possono essere eseguite allo stesso tempo su un server specifico. Tali requisiti determinano anche quante istanze possono essere eseguite allo stesso tempo su tutti i server del sito.

  Il limite di istanze dell'applicazione per macchina influisce su qualsiasi server del sito (non solo sulle macchine di un particolare gruppo di consegna). Supponiamo che il proprio sito abbia tre server. Per l'applicazione `Charlie`, è possibile configurare il limite di istanze dell'applicazione per macchina a 2. Pertanto, non è consentito avviare più di sei istanze dell'applicazione `Charlie` in tutto il sito. Questo è un limite di due istanze di Charlie su ciascuno dei tre server.

  Per limitare l'utilizzo di un'applicazione solo a determinati computer all'interno di un gruppo di consegna (oltre a limitarne le istanze su tutte le macchine in tutto il sito):

  - Utilizzare la funzionalità di assegnazione di per queste macchine.
  - Configurare il limite di numero massimo di istanze per macchina per tale applicazione.

Se le applicazioni vengono avviate con metodi diversi dall'intermediazione del Controller (ad esempio, mentre un Controller è in modalità di interruzione) e i limiti configurati vengono superati, gli utenti non possono avviare più istanze fino a quando non chiudono istanze sufficienti a non superare più i limiti. Le istanze che hanno superato il limite non vengono arrestate forzatamente. Sarà consentito continuare fino a quando i loro utenti non le chiudono.

Se si disabilita il roaming di sessione, disabilitare il limite di una istanza dell'applicazione per utente. Se si abilita il limite di una istanza dell'applicazione per utente, non configurare nessuno dei due valori che consentono nuove sessioni su nuovi dispositivi. Per informazioni sul roaming, vedere Sessioni.

Per configurare il limite massimo di istanze per gruppo di consegna e il limite di una istanza per utente:

1. Selezionare **Applications** nel riquadro a sinistra, quindi selezionare un'applicazione.
2. Selezionare **Edit Application Properties** (Modifica proprietà dell'applicazione) nella barra delle azioni.
3. Nella pagina **Delivery** (Consegna), scegliere una delle seguenti opzioni.

   - **Allow unlimited use of the application** (Consenti l'uso illimitato dell'applicazione). Non c'è limite al numero di istanze in esecuzione allo stesso tempo. Questa è l'impostazione predefinita.
   - **Set limits for the application** (Imposta limiti per l'applicazione). Esistono due tipi di limite; specificarne uno o entrambi.

  - Specificare il numero massimo di istanze che possono essere eseguite allo stesso tempo per macchina
  - Limitare a un'istanza dell'applicazione per utente

4. Fare clic su **OK** per applicare la modifica e chiudere la finestra di dialogo oppure su **Apply** per applicare la modifica e lasciare aperta la finestra di dialogo.

Per configurare il limite massimo di istanze per macchina (solo PowerShell):

- In PowerShell (utilizzando l'SDK Remote PowerShell per le distribuzioni Citrix Cloud o l'SDK PowerShell per le distribuzioni locali), immettere il cmdlet `BrokerApplication` appropriato con il parametro `MaxPerMachineInstances`.
- Per istruzioni, utilizzare il cmdlet `Get-Help`. Ad esempio:

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

### Passare parametri alle applicazioni pubblicate

Utilizzare la pagina **Location** delle proprietà di un'applicazione per immettere la riga di comando e passare i parametri alle applicazioni pubblicate.

Quando si associa un'applicazione pubblicata a tipi di file, i simboli `"%*"` (simboli di percentuale e asterisco tra virgolette) vengono aggiunti alla fine della riga di comando per l'applicazione. Questi simboli fungono da segnaposto per i parametri passati ai dispositivi utente.

Se un'applicazione pubblicata non viene avviata quando è previsto, verificare che la riga di comando contenga i simboli corretti. Per impostazione predefinita, i parametri forniti dai dispositivi utente vengono convalidati quando vengono aggiunti i simboli `"%*"`. Per le applicazioni pubblicate che utilizzano parametri personalizzati forniti dal dispositivo utente, vengono aggiunti i simboli `"%**"` alla riga di comando per ignorare la convalida della riga di comando. Se questi simboli non sono presenti in una riga di comando per l'applicazione, aggiungerli manualmente.

Se il percorso del file eseguibile include nomi di directory con spazi (ad esempio `"C:\Program Files"`), racchiudere la riga di comando dell'applicazione tra virgolette per indicare che lo spazio appartiene alla riga di comando. Per fare ciò, aggiungere virgolette attorno al percorso e un altra coppia di virgolette attorno ai simboli %*. Assicurarsi di includere uno spazio tra le virgolette di chiusura per il percorso e tra le virgolette di apertura per i simboli %*.

Ad esempio, la riga di comando per l'applicazione pubblicata Windows Media Player è:

```
"C:\Program Files\Windows Media Player\mplayer1.exe""%*"
```

> **Nota:**
>
> Il numero massimo di caratteri, inclusi gli argomenti, nella riga di comando per l'avvio delle ap-

> plicazioni pubblicate è 203.

### Gestire le cartelle delle applicazioni

Per impostazione predefinita, le nuove applicazioni aggiunte vengono inserite in una cartella denominata **Applications**. È possibile specificare una cartella diversa quando si crea il gruppo di consegna, quando si aggiunge un'applicazione o successivamente.

Buono a sapersi:

- Non è possibile rinominare o eliminare la cartella Applications, ma è possibile spostare tutte le applicazioni in essa contenute in altre cartelle che si sono create.
- Il nome di una cartella può contenere 1-64 caratteri. Gli spazi sono consentiti.
- Le cartelle possono essere nidificate fino a cinque livelli.
- Le cartelle non devono necessariamente contenere applicazioni. Sono consentite le cartelle vuote.
- Le cartelle sono elencate alfabeticamente in Web Studio, a meno che non le si sposti o si specifichi una posizione diversa durante la creazione.
- È possibile avere più cartelle con lo stesso nome, purché si trovino in cartelle di livello superiore diverse. Allo stesso modo, è possibile avere più applicazioni con lo stesso nome, purché si trovino in cartelle diverse.
- È necessario disporre dell'autorizzazione `View Applications` per visualizzare le applicazioni nelle cartelle ed è necessario disporre dell'autorizzazione `Edit Application Properties` su tutte le applicazioni della cartella per rimuovere, rinominare o eliminare una cartella contenente applicazioni.
- La maggior parte delle procedure seguenti richiede azioni eseguibili nella barra delle azioni di Web Studio. In alternativa, è possibile utilizzare i menu di scelta rapida o trascinare l'elemento. Ad esempio, se si crea o si sposta una cartella in una posizione diversa da quella desiderata, è possibile trascinarla nella posizione corretta.

Per gestire le cartelle delle applicazioni, selezionare **Applications** nel riquadro a sinistra. Per istruzioni, utilizzare il seguente elenco.

- **Per visualizzare tutte le cartelle (escluse le cartelle nidificate):** fare clic su **Show all** (Mostra tutto) sopra l'elenco delle cartelle.
- **Per creare una cartella al livello più alto (non nidificata):** selezionare la cartella **Applications**. Per posizionare la nuova cartella in una cartella esistente diversa da **Applications**, selezionare quella cartella. Quindi, selezionare **Create Folder** (Crea cartella) nella barra delle azioni. Inserire un nome.
- **Per spostare una cartella:** selezionare la cartella e quindi selezionare **Move Folder** (Sposta cartella) nella barra delle azioni. È possibile spostare solo una cartella alla volta, a meno che

la cartella non contenga cartelle nidificate. Il modo più semplice per spostare una cartella è trascinarla.

- **Per rinominare una cartella:** selezionare la cartella, quindi selezionare **Rename Folder** (Rinomina cartella) nella barra delle azioni. Inserire un nome.
- **Per eliminare una cartella:** selezionare la cartella e quindi selezionare **Delete Folder** (Elimina cartella) nella barra delle azioni. Quando si elimina una cartella che contiene applicazioni e altre cartelle, vengono eliminati anche tali oggetti. L'eliminazione di un'applicazione rimuove l'assegnazione dell'applicazione dal gruppo di consegna. Tt non la rimuove dalla macchina.
- **Per spostare le applicazioni in una cartella:** selezionare una o più applicazioni. Quindi selezionare **Move Application** (Sposta applicazione) nella barra delle azioni. Selezionare la cartella.

È inoltre possibile inserire le applicazioni che si stanno aggiungendo in una cartella nella pagina **Application** durante la creazione di un gruppo di consegna o di un gruppo di applicazioni. Per impostazione predefinita, le applicazioni aggiunte vanno nella cartella **Applications**. Fare clic su **Change** (Modifica) per selezionare o creare una cartella.

### Controllare l'avvio locale delle applicazioni sui desktop pubblicati

Quando gli utenti avviano un'applicazione pubblicata da un desktop pubblicato, è possibile controllare se l'applicazione viene avviata in quella sessione desktop o come applicazione pubblicata. L'app Citrix Workspace cerca il percorso di installazione dell'applicazione nel Registro di sistema di Windows sul VDA e, se presente, avvia l'istanza locale dell'applicazione. In caso contrario, viene avviata un'istanza ospitata dell'applicazione. Se si avvia un'applicazione non installata sul VDA, viene avviata l'applicazione ospitata. Per ulteriori informazioni, vedere vPrefer launch.

In PowerShell (utilizzando l'SDK Remote PowerShell nelle distribuzioni Citrix Cloud o l'SDK PowerShell nelle distribuzioni locali), è possibile modificare questa azione.

Nell'applicazione `New-Broker` o nel cmdlet `Set-BrokerApplication`, utilizzare l'opzione `LocalLaunchDisabled`. Ad esempio:

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

Per impostazione predefinita, il valore di questa opzione è false (`-LocalLaunchDisabled $false`). Quando si avvia un'applicazione pubblicata da un desktop pubblicato, l'applicazione viene avviata in quella sessione desktop.

Se si imposta il valore dell'opzione su true (`-LocalLaunchDisabled $true`), viene avviata l'applicazione pubblicata. In questo modo viene creata una sessione aggiuntiva separata dal desktop pubblicato (utilizzando l'app Citrix Workspace per Windows) dell'applicazione pubblicata.

Requisiti e limiti:

- Il valore `ApplicationType` dell'applicazione deve essere `HostedOnDesktop`.
- Questa opzione è disponibile solo tramite l'apposito SDK PowerShell. Al momento non è disponibile nell'interfaccia grafica di Web Studio.
- Questa opzione richiede come minimo: StoreFront 3.14, Citrix Receiver per Windows 4.11 e Delivery Controller 7.17.

## Pacchetti di app

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Microsoft offre tre tecnologie di packaging per fornire applicazioni agli utenti: App-V, MSIX e MSIX App Attach. Questo articolo spiega come implementare e distribuire questi pacchetti di applicazioni utilizzando **Web Studio > Pacchetti app**:

- Distribuire e rendere disponibili applicazioni App-V
- Implementare e distribuire applicazioni MSIX e MSIX App Attach

### Distribuire e rendere disponibili applicazioni App-V

Questa sezione contiene le seguenti informazioni:

- Panoramica. Descrive i metodi di gestione utilizzati per fornire e gestire i pacchetti App-V.
- Procedure. Offre procedure per la distribuzione e la distribuzione di questi pacchetti.

#### Panoramica

Questa sezione descrive i metodi di gestione utilizzati per fornire e gestire i pacchetti App-V. Per ulteriori informazioni sui componenti e sui concetti con cui si interagisce durante la distribuzione di applicazioni in pacchetto App-V, vedere la documentazione Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-for-windows.

È possibile utilizzare i seguenti metodi per distribuire e gestire i pacchetti App-V:

- **Dual Admin** (Amministrazione doppia). I pacchetti di applicazioni sono configurati e gestiti sui server App-V. I server Citrix Virtual Apps and Desktops e App-V lavorano insieme per fornire e gestire pacchetti.

  Questo metodo richiede che Citrix Virtual Apps and Desktops aggiorni periodicamente la vista snapshot dello stato del server App-V. Ciò comporta costi in termini di hardware, infrastruttura e amministrazione. I server Citrix Virtual Apps and Desktops e App-V devono rimanere sincronizzati, in particolare per quanto riguarda le autorizzazioni degli utenti.

  Dual Admin funziona meglio nelle distribuzioni in cui App-V e il proprio ambiente sono strettamente associati:

  - **Server di gestione App-V**. Pubblica e gestisce il ciclo di vita dei pacchetti App-V e dei file di configurazione dinamici.
  - **Componente Citrix Personalization** installato su macchine VDA. Gestire la registrazione del server di pubblicazione App-V appropriato richiesto per gli avvii delle applicazioni.

  Questo metodo garantisce che il server di pubblicazione App-V sia sincronizzato per l'utente al momento appropriato. Il server di pubblicazione conserva altri aspetti del ciclo di vita del pacchetto, come l'aggiornamento all'accesso e i gruppi di connessione.

- **Single Admin** (Amministrazione singola). I pacchetti di applicazioni sono archiviati nelle condivisioni di rete. Citrix Virtual Apps and Desktops fornisce e gestisce i pacchetti in modo indipendente.

  Questo metodo riduce il sovraccarico perché i server App-V e l'infrastruttura di database non sono necessari nella distribuzione.

  In questo metodo, i pacchetti App-V vengono archiviati su una condivisione di rete e i relativi metadati vengono caricati da quella posizione sul proprio ambiente. Quindi il componente Citrix Personalization installato su macchine VDA gestisce e fornisce le applicazioni come segue:

  - Elaborare i file di configurazione della distribuzione e i file di configurazione utente all'avvio di un'applicazione.
  - Gestire tutti gli aspetti dei cicli di vita dei pacchetti sulla macchina host.

È possibile utilizzare entrambi i metodi di gestione contemporaneamente. In altre parole, quando si aggiungono applicazioni ai gruppi di consegna, le applicazioni possono provenire da pacchetti App-V situati su server App-V o su condivisioni di rete.

> **Nota:**
>
> Se si utilizzano entrambi i metodi di gestione contemporaneamente e il pacchetto App-V dispone di un file di configurazione dinamico in entrambe le posizioni, viene utilizzato il file che si trova nel server App-V (Dual Admin).

#### Procedure

Per supportare la distribuzione di applicazioni App-V, è necessario installare il componente Citrix Personalization su macchine VDA. Vedere Installare il componente Citrix Personalization su macchine VDA per i dettagli.

Per distribuire applicazioni in pacchetto App-V ai propri utenti, effettuare le seguenti operazioni:

1. Archiviare i pacchetti di applicazioni su condivisioni di rete.
2. Caricare i pacchetti applicativi nel proprio ambiente.
3. Aggiungere le applicazioni ai gruppi di consegna.
4. Per abilitare la consegna automatica di pacchetti App-V interdipendenti, creare gruppi di isolamento.

Per fare in modo che Citrix Virtual Apps and Desktops riconosca e applichi i file di configurazione dinamica di App-V nel metodo Single Admin, vedere questo blog di Citrix.

### Implementare e distribuire applicazioni MSIX e MSIX App Attach

Questa sezione contiene le seguenti informazioni:

- Panoramica. Descrive come vengono forniti e gestiti i pacchetti MSIX e MSIX App Attach.
- Procedure. Offre procedure per la distribuzione e la distribuzione di questi pacchetti.

#### Panoramica

Citrix Virtual Apps and Desktops offre applicazioni MSIX e MSIX App Attach agli utenti tramite il componente Citrix Personalization installato su macchine VDA. Questo componente gestisce tutti gli aspetti dei cicli di vita dei pacchetti sulla macchina host.

Per ulteriori informazioni su MSIX e MSIX App Attach, vedere la documentazione Microsoft: rispettivamente https://docs.microsoft.com/en-us/windows/msix/ e https://docs.microsoft.com/en-us/azure/virtual-desktop/what-is-app-attach.

#### Procedure

Per supportare la distribuzione di pacchetti MSIX e MSIX App Attach, è necessario installare il componente Citrix Personalization su macchine VDA. Vedere Installare il componente Citrix Personalization su macchine VDA per i dettagli.

Per distribuire applicazioni in pacchetto MSIX e MSIX App Attach ai propri utenti, effettuare le seguenti operazioni:

1. Archiviare i pacchetti di applicazioni su condivisioni di rete.
2. Caricare i pacchetti applicativi nel proprio ambiente.
3. Aggiungere le applicazioni ai gruppi di consegna.

### Installare il componente Citrix Personalization su macchine VDA

Il componente Citrix Personalization gestisce il processo di pubblicazione dei pacchetti di applicazioni nei formati App-V, MSIX e MSIX App Attach. Questo componente non viene installato per impostazione predefinita quando si installa un VDA. È possibile installare il componente durante o dopo l'installazione del VDA.

Per installarlo durante l'installazione del VDA, utilizzare uno dei seguenti metodi:

- Nella procedura guidata di installazione, andare alla pagina **Additional Components** (Componenti aggiuntivi), quindi selezionare la casella di controllo **Citrix Personalization for App-V - VDA** (Personalizzazione Citrix per App-V - VDA).
- Nell'interfaccia della riga di comando, utilizzare l'opzione **/includeadditional "Citrix Personalization for App-V –VDA"**.

Per installare il componente dopo l'installazione del VDA, effettuare le seguenti operazioni:

1. Sulla macchina VDA, accedere a **Pannello di controllo > Programmi > Programmi e funzionalità**, fare clic con il pulsante destro del mouse su **Citrix Virtual Delivery Agent**, quindi selezionare **Modifica**.
2. Nella procedura guidata visualizzata, passare alla pagina **Additional Components** (Componenti aggiuntivi) e quindi abilitare la casella di controllo **Citrix Personalization for App-V - VDA** (Personalizzazione Citrix per App-V - VDA).

> **Nota:**
>
> Il client desktop Microsoft App-V è il componente che esegue applicazioni virtuali dai pacchetti App-V sui dispositivi degli utenti. Windows 10 (1607 o versioni successive), Windows Server 2016 e Windows Server 2019 includono già questo software client App-V. È necessario abilitarlo solo su macchine VDA. Per ulteriori informazioni, consultare questo articolo della documentazione Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-enable-the-app-v-desktop-client.

### Archiviare pacchetti di applicazioni su condivisioni di rete

Dopo aver configurato l'infrastruttura, generare i pacchetti di applicazioni e archiviarli in un percorso di rete, ad esempio una condivisione di rete UNC o SMB oppure in una condivisione file di Azure.

I passaggi dettagliati sono i seguenti:

1. Generare pacchetti di applicazioni. Per ulteriori informazioni, vedere la documentazione Microsoft.
2. Archiviare i pacchetti di applicazioni in un percorso di rete:
    - Per **App-V Single Admin**: archiviare i pacchetti e i corrispondenti file di configurazione dinamica (App-V) in una condivisione di rete UNC o SMB o in una condivisione file di Azure.
    - Per **App-V Dual Admin**: pubblicare i pacchetti sul server di gestione App-V da un percorso UNC (la pubblicazione da URL HTTP non è supportata).
    - Per **MSIX e MSIX App Attach**: archiviare i pacchetti su una condivisione di rete UNC o SMB oppure su una condivisione di file di Azure.
3. Verificare che il VDA disponga dell'autorizzazione di lettura sul percorso di archiviazione del pacchetto:
    - Se si archiviano pacchetti in una condivisione di rete UNC o SMB nel dominio AD, concedere alla macchina VDA l'autorizzazione di lettura per il percorso di archiviazione. A tale scopo, è possibile concedere esplicitamente all'account AD della macchina l'autorizzazione di lettura per la condivisione o includere l'account in un gruppo AD che dispone di tale autorizzazione.
    - Se si archiviano pacchetti in una condivisione file di Azure, concedere innanzitutto l'autorizzazione di lettura a un account utente per il percorso di archiviazione in Azure. Quindi, configurare `ctxAppVService` in esecuzione sulla macchina VDA in modo che utilizzi quell'account utente per accedere al percorso di archiviazione del pacchetto. Consultare la sezione seguente per i passaggi dettagliati.

#### Modificare l'account di accesso dell'utente

Il VDA chiama `ctxAppVService` per accedere ai percorsi di archiviazione dei pacchetti. Per impostazione predefinita, `ctxAppVService` accede ai percorsi di archiviazione dei pacchetti utilizzando l'**account di sistema locale** della macchina. Questo tipo di autenticazione macchina funziona nei domini AD. Tuttavia, non funziona negli scenari di integrazione di AD e Azure AD, che richiedono l'autenticazione basata sull'account utente.

Se si archiviano pacchetti in una condivisione file di Azure, modificare l'account di accesso per `ctxAppVService` in un account utente che dispone dell'autorizzazione di lettura per il percorso di archiviazione del pacchetto. I passaggi dettagliati sono i seguenti:

1. Avviare **Services** (Servizi), fare clic con il pulsante destro del mouse su **ctxAppVService** e quindi selezionare **Properties** (Proprietà).

2. Nella scheda **Log on** (Accesso), selezionare **This account** (Questo account), immettere un account utente che dispone dell'autorizzazione di lettura per il percorso di archiviazione del pacchetto e quindi immettere due volte la password dell'utente.
3. Fare clic su **OK**.

## Caricare i pacchetti applicativi nel proprio ambiente

Dopo aver archiviato i pacchetti di applicazioni in una posizione di rete secondo necessità, caricarli sul proprio ambiente per la consegna. Se necessario, utilizzare uno dei seguenti metodi:

- Caricamento in blocco
- Caricamento uno ad uno

### Preparativi

Citrix Virtual Apps and Desktops utilizza una macchina VDA per configurare la connessione al percorso di rete per il rilevamento dei pacchetti. Pertanto, creare preventivamente un gruppo di consegna e accertarsi che almeno un VDA nel gruppo soddisfi i seguenti requisiti:

- Versione VDA:
  - Per scoprire i pacchetti App-V: 2203 o versioni successive
  - Per scoprire i pacchetti MSIX e MSIX App Attach: 2209 o versioni successive
- Personalizzazione Citrix per i componenti App-V: installata
- Autorizzazione sulla posizione del pacchetto: Lettura (vedere Passaggio 2: archiviare i pacchetti di applicazioni su condivisioni di rete per i dettagli).
- Alimentazione: attivata
- Stato: registrato

### Caricare pacchetti di applicazioni in blocco

Caricare i pacchetti in una posizione di rete nel proprio ambiente. Assicurarsi di avere a portata di mano i seguenti elementi prima del caricamento:

- Un gruppo di consegna che soddisfa i requisiti di Preparation (Preparazione)
- Il percorso della posizione di rete

Per caricare i pacchetti in blocco, effettuare le seguenti operazioni:

1. Nel riquadro di sinistra, selezionare **App Packages**.

2. Nella scheda **Sources** (Origini), fare clic sul pulsante **Add Source** (Aggiungi origine). Viene visualizzata la pagina **Add Source** (Aggiungi origine).
3. Nel campo **Name** (Nome), immettere un nome descrittivo per l'origine del pacchetto.
4. Nel campo **Delivery group** (Gruppo di consegna), fare clic su **Select a delivery group** (Seleziona un gruppo di consegna). Quindi, selezionare un gruppo di consegna che soddisfi i requisiti indicati in Preparation (Preparazione) e fare clic su **OK**.
5. Nel campo **Location type** (Tipo di posizione), selezionare il **server Microsoft App-V** o la **condivisione di rete** in base alla posizione in cui vengono archiviati i pacchetti, quindi completare le impostazioni corrispondenti:
   - Se si seleziona il **server Microsoft App-V**, immettere le seguenti informazioni:
     - URL del server di gestione. Esempio: `http://appv-server.example.com`
     - Credenziali di accesso dell'amministratore del server di gestione.
     - URL e numero di porta del server di pubblicazione. Esempio: `http://appv-server.example.com:3330`
   - Se è stato selezionata l'opzione **Network share** (Condivisione di rete), specificare le seguenti informazioni:
     - Immettere il percorso UNC della condivisione di rete. Esempio: `\\Package-Server\apps\`
     - Selezionare i tipi di pacchetti che si desidera caricare. Le opzioni includono App-V, MSIX e MSIX App Attach.
     - Specificare se cercare i pacchetti nelle sottocartelle.
6. Fare clic su **Add Source** (Aggiungi origine).

   La pagina Add Source (Aggiungi origine) si chiude e la nuova origine aggiunta viene visualizzata nell'elenco delle origini. Citrix Virtual Apps and Desktops carica i pacchetti nell'ambiente utilizzando un VDA nel gruppo di consegna. Al termine del caricamento, il campo Status (Stato) mostra *Import successful* (Importazione riuscita). I pacchetti corrispondenti vengono visualizzati nella scheda **Packages** (Pacchetti).

   > **Nota:**
   >
   > Per verificare la presenza di aggiornamenti dei pacchetti in una posizione di origine e importarli nel proprio ambiente, selezionare la posizione nell'elenco delle origini e fare clic su **Check for Package Updates** (Verifica aggiornamenti del pacchetto).

#### Caricare i pacchetti di applicazioni uno ad uno

Caricare un pacchetto di applicazioni da una condivisione di rete nel proprio ambiente. Prima del caricamento, assicurarsi di avere a portata di mano i seguenti elementi:

- Un gruppo di consegna che soddisfa i requisiti indicati in Preparation (Preparazione)
- Il percorso della posizione di rete

Per caricare un pacchetto nel proprio ambiente, effettuare le seguenti operazioni:

1. Nel riquadro di sinistra, selezionare **App Packages**.
2. Nella scheda **Packages** (Pacchetti), fare clic sul pulsante **Add Package** (Aggiungi pacchetto). Viene visualizzata la pagina **Add Package** (Aggiungi pacchetto).
3. Nel campo **Delivery group** (Gruppo di consegna), fare clic su **Select a delivery group** (Seleziona un gruppo di consegna). Quindi, selezionare un gruppo di consegna che soddisfi i requisiti indicati in Preparation (Preparazione) e fare clic su **OK**.
4. Nel campo **Package full path** (Percorso completo del pacchetto), immettere un percorso secondo necessità:
   - Per caricare più pacchetti contemporaneamente, inserirne i percorsi completi, separati da punto e virgola (`;`). Esempio: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - Per caricare tutti i pacchetti presenti in una condivisione di rete, immettere il percorso di archiviazione. Esempio: \package-Server\apps\
5. Fare clic su **Add Package** (Aggiungi pacchetto).

   Il pacchetto dell'applicazione viene visualizzato nella scheda **Packages** (Pacchetti).

### Aggiungere le applicazioni ai gruppi di consegna

Dopo il caricamento completo di un pacchetto di applicazioni, aggiungere le relative applicazioni a uno o più gruppi di consegna in base alle esigenze. Di conseguenza, gli utenti associati a tali gruppi di consegna possono accedere alle applicazioni.

Per aggiungere una o più applicazioni in un pacchetto a diversi gruppi di consegna, effettuare le seguenti operazioni:

1. Nel riquadro di sinistra, selezionare **App Packages**.
2. Nella scheda **Packages** (Pacchetti), selezionare un pacchetto secondo necessità.
3. Nella barra delle azioni, fare clic su **Add Delivery Groups** (Aggiungi gruppi di consegna). Viene visualizzata la pagina Add Delivery Groups (Aggiungi gruppi di consegna).
4. Selezionare una o più applicazioni nel pacchetto in base alle esigenze, quindi fare clic su **Next** (Avanti). Vengono visualizzati i gruppi di consegna con il tipo di consegna *Applications* (Applicazioni).

5. Nell'elenco dei gruppi di consegna, selezionare i gruppi a cui si desidera assegnare le applicazioni e quindi fare clic su **Next** (Avanti).
   **Nota:** se è stato selezionato un pacchetto MSIX o MSIX App Attach, nell'elenco vengono visualizzati solo i gruppi di consegna il cui livello funzionale è 2106 o successivo.
6. Fare clic su **Finish**.

È inoltre possibile aggiungere applicazioni pacchettizzate a un gruppo di consegna quando:

- Si crea un gruppo di consegna. Per ulteriori informazioni, vedere Creare gruppi di consegna.
- Si modificano dei gruppi di consegna o dei gruppi di applicazioni esistenti. Per ulteriori informazioni, consultare Aggiungere applicazioni.

## (Facoltativo) Creare gruppi di isolamento per i pacchetti App-V

È possibile creare gruppi di isolamento per abilitare la consegna automatica di pacchetti App-V interdipendenti.

> **Nota:**
>
> I gruppi di isolamento sono supportati per il metodo App-V Single Admin. Se si utilizza il metodo App-V Dual Admin, è possibile raggiungere lo stesso obiettivo creando *gruppi di connessione* nell'infrastruttura Microsoft App-V. Per ulteriori informazioni, consultare questo articolo della documentazione Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-connection-group-file.

### Informazioni sui gruppi di isolamento

Un gruppo di isolamento è una raccolta di pacchetti di applicazioni interdipendenti che devono essere eseguiti nella stessa sandbox di Windows per creare un ambiente virtuale. I gruppi di isolamento Citrix App-V sono simili ma non identici ai gruppi di connessione App-V. Un gruppo di isolamento include due tipi di pacchetti:

- Pacchetti di applicazioni **espliciti**. Applicazioni con requisiti di licenza specifici. È possibile limitare tali applicazioni a un intervallo specifico di utenti aggiungendole ai gruppi di consegna.
- Pacchetti di applicazioni **automatici**. Applicazioni sempre disponibili per tutti gli utenti indipendentemente dal fatto che vengano aggiunte ai gruppi di consegna.

Ad esempio, l'applicazione app-a richiede l'esecuzione di JRE 1.7. È possibile creare un gruppo di isolamento contenente app-a (contrassegnato come *Explicit* [Esplicito]) e JRE 1.7 (contrassegnato come *Automatic* [Automatico]). Successivamente, aggiungere il pacchetto App-V per app-a a uno o più gruppi di consegna. Quando un utente avvia app-a, JRE 1.7 viene distribuito automaticamente con esso.

Quando un utente avvia un'applicazione App-V contrassegnata come *Explicit* (Esplicita) in un gruppo di isolamento, Citrix Virtual Apps and Desktops verifica l'autorizzazione di accesso dell'utente all'applicazione nei gruppi di consegna. Se l'utente dispone dell'autorizzazione per accedere all'applicazione, tutti i pacchetti di applicazioni *automatici* nello stesso gruppo di isolamento vengono resi disponibili all'utente.

Non è necessario aggiungere i pacchetti *automatici* a nessun gruppo di consegna. Se è presente un altro pacchetto di applicazioni *esplicito* nel gruppo di isolamento, tale pacchetto viene reso disponibile all'utente solo se si trova nello stesso gruppo di consegna.

Per ulteriori informazioni sui gruppi isolati, vedere questo blog di Citrix.

**Creare un gruppo di isolamento App-V** Creare un gruppo di isolamento e aggiungervi pacchetti di applicazioni interdipendenti. I passaggi dettagliati sono i seguenti:

1. Nella scheda **Isolation Groups** (Gruppi di isolamento), fare clic su **Add Isolation Group** (Aggiungi gruppo di isolamento).
2. Immettere un nome e una descrizione per il gruppo di isolamento. Tutti i pacchetti di applicazioni nel proprio ambiente vengono visualizzati nell'elenco **Available Packages** (Pacchetti disponibili).
3. Dall'elenco **Available Packages** (Pacchetti disponibili), selezionare un'applicazione in base alle esigenze, quindi fare clic sulla freccia destra. L'applicazione selezionata dovrebbe ora essere visualizzata nell'elenco **Packages in Isolation Group** (Pacchetti nel gruppo di isolamento).
4. Nel campo **Deployment** (Distribuzione), selezionare **Explicit** (Esplicita) o **Automatic** (Automatica) per l'applicazione.
5. Ripetere i passaggi 2-3 per aggiungere altri pacchetti.
6. Per modificare l'ordine dei pacchetti nell'elenco, fare clic sulla freccia su o giù.
7. Fare clic su **Salva**.

> **Nota:**
>
> Le configurazioni dei gruppi di isolamento determinano la creazione di un gruppo di connessione App-V sul VDA. Gli scenari di distribuzione possono diventare complessi e il client App-V supporta pacchetti che si trovano in un solo gruppo di connessione attivo alla volta. Si consiglia di evitare di aggiungere lo stesso pacchetto a due diversi gruppi di isolamento aggiunti allo stesso gruppo di consegna.

## App Universal Windows Platform

January 7, 2024

Per informazioni sulle app Universal Windows Platform (UWP), vedere la seguente documentazione Microsoft:

- Cos'è un'app UWP (Universal Windows Platform)?
- Gestione pacchetti Windows

### Requisiti e limitazioni

Citrix Virtual Apps and Desktops supporta l'uso di app UWP con VDA sui seguenti computer Windows:

- Windows 10 e versioni successive
- Windows Server 2016 e versioni successive

La versione minima dei VDA deve essere la 7.11.

Le seguenti funzionalità di Citrix Virtual Apps and Desktops non sono supportate o limitate quando si utilizzano le app UWP:

- L'associazione di tipi di file non è supportata.
- L'accesso alle app locali non è supportato.
- Anteprima dinamica: se le app in esecuzione nella sessione si sovrappongono, l'anteprima mostra l'icona predefinita. Le API Win32 utilizzate per Dynamic Preview non sono supportate nelle app UWP.
- Remote Action Center: le app UWP possono utilizzare Action Center per visualizzare i messaggi nella sessione. Questi messaggi attualmente non vengono reindirizzati all'endpoint da visualizzare all'utente.

L'avvio di app UWP e app non UWP dallo stesso server non è supportato. Posizionare invece le app UWP e non UWP in gruppi di consegna o gruppi di applicazioni separati.

Poiché tutte le app UWP installate sul computer sono enumerate, Citrix consiglia di disabilitare l'accesso utente a Windows Store. In questo modo le app UWP installate da un utente non possono essere utilizzate da un utente diverso.

Durante il sideload, l'app UWP è installata sulla macchina ed è disponibile per essere utilizzata da altri utenti. Quando un altro utente avvia l'app, questa viene installata e il sistema operativo aggiorna il database AppX indicando "come installato"da quell'utente.

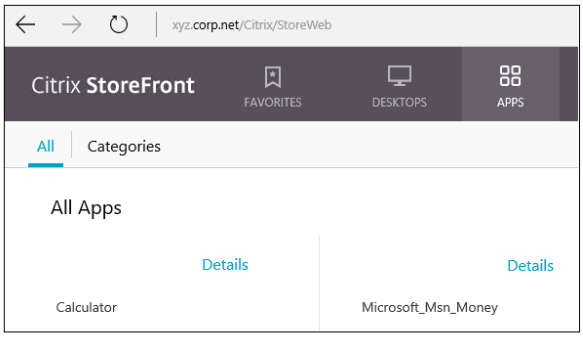
Uno scollegamento regolare avviato da un'app UWP pubblicata che è stata avviata in una finestra fissa o continua potrebbe impedire la chiusura della sessione VDA e lo scollegamento forzato dell'utente. Quando ciò si verifica, sono svariati processi rimanenti nella sessione del VDA a impedirne la corretta chiusura. Per risolvere questo problema, determinare quale processo impedisce la chiusura della sessione e quindi aggiungerlo al valore della chiave del Registro di sistema "LogoffCheckSysModules", seguendo le indicazioni riportate in CTX891671.

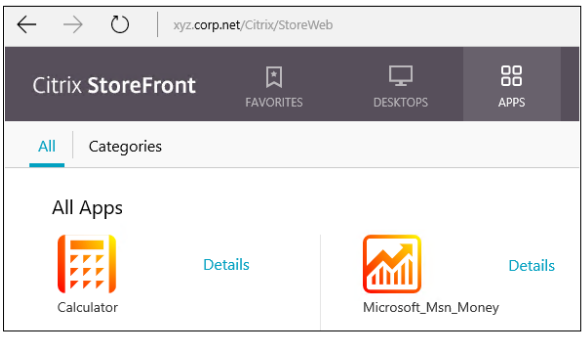
I nomi visualizzati e le descrizioni delle applicazioni per le app UWP potrebbero non avere nomi corretti. Modificare e correggere queste proprietà quando si aggiungono le applicazioni al gruppo di consegna.

Per dettagli di eventuali problemi aggiuntivi, vedere Problemi noti.

Attualmente, diverse app UWP hanno icone bianche con trasparenza abilitata, il che rende l'icona non visibile sullo sfondo bianco del display di StoreFront. Per evitare questo problema, è possibile modificare lo sfondo. Ad esempio, sulla macchina di StoreFront, modificare il file `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`. Alla fine del file, aggiungere `.storeapp-icon { background-image: radial-gradient( circle at top right, yellow, red ); }`. L'immagine seguente illustra il prima e il dopo relativi a questo esempio.




Before




After

In Windows Server 2016 e versioni successive, anche Server Manager potrebbe essere avviato all'avvio di un'app UWP. Per evitare che ciò si verifichi, è possibile disabilitare l'avvio automatico di Server Manager durante l'accesso con la chiave `HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon` del Registro di sistema. Per i dettagli, vedere https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/.

### Installare e pubblicare le app UWP

Il supporto delle app UWP è abilitato per impostazione predefinita.

Per installare una o più app UWP sui VDA (o su un'immagine master), utilizzare uno dei seguenti metodi:

- Completare un'installazione offline da Windows Store for Business, utilizzando uno strumento quale Deployment Image Servicing and Management (DISM) per distribuire le app sull'immagine desktop. Per ulteriori informazioni, vedere Gestione pacchetti Windows.
- Effettuare il sideload delle app. Per ulteriori informazioni, vedere Trasferire localmente le app line-of-business (LOB) nei dispositivi client Windows.
- Installare le app UWP per ciascun utente previsto direttamente da Windows Store for Business.

Per aggiungere (pubblicare) una o più app UWP in Citrix Virtual Apps o Citrix Virtual Desktops:

1. Dopo aver installato le app UWP sulla macchina, aggiungerle a un gruppo di consegna o a un gruppo di applicazioni. È possibile farlo quando si crea un gruppo o in seguito. Nella pagina **Applications** (Applicazioni), passare al menu **Add** e selezionare **From Start menu** (Dal menu Start).
2. Quando viene visualizzato l'elenco delle applicazioni, selezionare le app UWP che si desidera pubblicare.
3. Continuare la procedura guidata o chiudere la finestra di modifica.

Per disabilitare l'uso delle app universali su un VDA, aggiungere l'impostazione del Registro di sistema **EnableUWASeamlessSupport** in `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` e impostarla su **0**.

### Disinstallare le app UWP

Quando si disinstalla un'app UWP con un comando come `Remove-AppXPackage`, l'elemento viene disinstallato solo per gli amministratori. Per rimuovere l'app dalle macchine degli utenti che potrebbero aver avviato e utilizzato l'app, eseguire il comando di rimozione su ciascun computer. Non è possibile disinstallare il pacchetto AppX da tutti i computer degli utenti con un solo comando.

## Autoscale

January 7, 2024

Autoscale è una funzionalità che offre una soluzione coerente e ad alte prestazioni per la gestione proattiva delle macchine. Punta a raggiungere un equilibrio fra i costi e l'esperienza dell'utente.

Autoscale consente la gestione proattiva dell'alimentazione di tutte le macchine con sistema operativo a sessione singola e multisessione registrate in un gruppo di consegna.

Le funzionalità di Autoscale includono:

- Impostazioni basate sulla pianificazione e sul carico
- Timeout dinamici delle sessioni
- Scalabilità automatica delle macchine con tag (cloud burst)
- Notifiche di scollegamento dell'utente

### Piattaforme di hosting VDA supportate

Autoscale supporta tutte le piattaforme supportate da Citrix Virtual Apps and Desktops. Ciò include varie piattaforme di infrastruttura tra cui Citrix Hypervisor, Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere e molte altre. Per un elenco completo delle piattaforme supportate, vedere i Requisiti di sistema di Citrix Virtual Apps and Desktops.

> **Nota:**
>
> Quando si aggiungono connessioni a host cloud pubblici alla propria distribuzione, è necessario disporre della licenza Hybrid Rights. Per informazioni sulla licenza Hybrid Rights, vedere Transition and Trade-Up (TTU) with Hybrid Rights. Per informazioni sull'aggiunta di una licenza, vedere Creare un sito.

### Carichi di lavoro supportati

Autoscale supporta sia i gruppi di consegna di sistemi operativi sia multisessione che a sessione singola. Ci sono tre interfacce utente di cui essere a conoscenza:

- Interfaccia utente Autoscale per gruppi di consegna di sistemi operativi multisessione (in precedenza gruppi di consegna RDS)
- Interfaccia utente con scalabilità automatica per gruppi di consegna casuali (in pool) di sistemi operativi a sessione singola (in precedenza gruppi di consegna VDI in pool)
- Interfaccia utente Autoscale per gruppi di consegna statici di sistemi operativi a sessione singola (in precedenza gruppi di consegna VDI statici)

Per ulteriori informazioni sulle interfacce utente per diversi gruppi di consegna, vedere Interfacce utente di Autoscale.

### Vantaggi

La funzione Autoscale offre i seguenti vantaggi:

- Fornire un meccanismo unico e coerente per la gestione dell'accensione delle macchine di un gruppo di consegna.
- Garantire la disponibilità e controllare i costi alimentando le macchine con una gestione dell'accensione basata sul carico o su una pianificazione, o una combinazione di entrambi.
- Per monitorare parametri come il risparmio sui costi e l'utilizzo della capacità e per abilitare le notifiche, utilizzare Director.

### Video di 2 minuti

Il seguente video fornisce una panoramica rapida di Autoscale.

Si tratta di un video incorporato. Fare clic sul collegamento per guardare il video

## Guida introduttiva a Autoscale

January 7, 2024

Autoscale funziona a livello di gruppo di consegna. Gestisce in modo proattivo le macchine di un gruppo di consegna in base alle pianificazioni impostate.

Autoscale si applica a tutti i tipi di gruppo di consegna:

- Sistema operativo statico a sessione singola
- Sistema operativo casuale a sessione singola
- Sistema operativo casuale multisessione

Questo articolo descrive i concetti di base relativi ad Autoscale e fornisce indicazioni su come abilitare e configurare Autoscale per un gruppo di consegna.

### Concetti di base

Prima di iniziare, è bene apprendere i seguenti concetti di base di Autoscale:

- Pianificazioni
- Capacity buffer (Buffer di capacità)
- Indice di carico

#### Pianificazioni

Autoscale accende e spegne le macchine di un gruppo di consegna in base a una pianificazione impostata dall'utente.

Una pianificazione include il numero di macchine attive per ogni fascia oraria, con orari di punta e non di punta definiti.

Le impostazioni di pianificazione variano in base al tipo di gruppo di consegna. Per ulteriori informazioni, vedere:

- Gruppi di consegna di sistemi operativi multisessione

- Gruppi di consegna casuale di sistemi operativi a sessione singola
- Gruppi di consegna statici di sistemi operativi a sessione singola

#### Capacity buffer (Buffer di capacità)

Il buffer di capacità viene utilizzato per aggiungere capacità di riserva alla domanda corrente per tenere conto degli aumenti dinamici del carico. Ci sono due scenari da tenere presenti:

- Per i gruppi di consegna di sistemi operativi multisessione, il buffer di capacità è definito come una percentuale della capacità totale del gruppo di consegna in termini di indice di carico.
- Per i gruppi di consegna di sistemi operativi a sessione singola, il buffer di capacità è definito come una percentuale del numero totale di macchine incluse nel gruppo di consegna.

#### Indice di carico

> **IMPORTANTE:**
>
> L'indice di carico si applica solo ai gruppi di consegna multisessione.

La metrica dell'indice di carico determina la probabilità che una macchina riceva le richieste di accesso degli utenti. Viene calcolata utilizzando le impostazioni dei **criteri di gestione del carico Citrix** configurate per l'uso simultaneo di accesso, sessione, CPU, disco e memoria.

L'indice di carico varia da 0 a 10.000. Per impostazione predefinita, una macchina è considerata a pieno carico quando ospita 250 sessioni:

- La cifra "0"indica una macchina non caricata. Una macchina con un valore di indice di carico pari a 0 si trova a un carico di base.
- La cifra "10.000"indica una macchina a pieno carico che non può eseguire nessun'altra sessione.

### Abilitare o disabilitare Autoscale per un gruppo di consegna

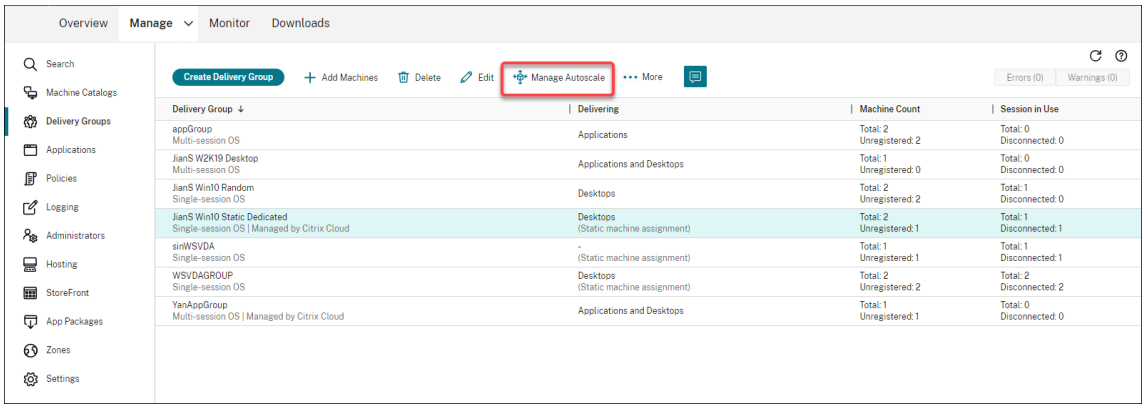
Autoscale è disabilitato per impostazione predefinita quando si crea un gruppo di consegna. Per abilitare e configurare Autoscale per un gruppo di consegna utilizzando Web Studio, seguire questi passaggi:

È inoltre possibile utilizzare i comandi PowerShell per abilitare e configurare Autoscale per un gruppo di consegna. Per ulteriori informazioni, vedere Comandi dell'SDK Broker PowerShell.

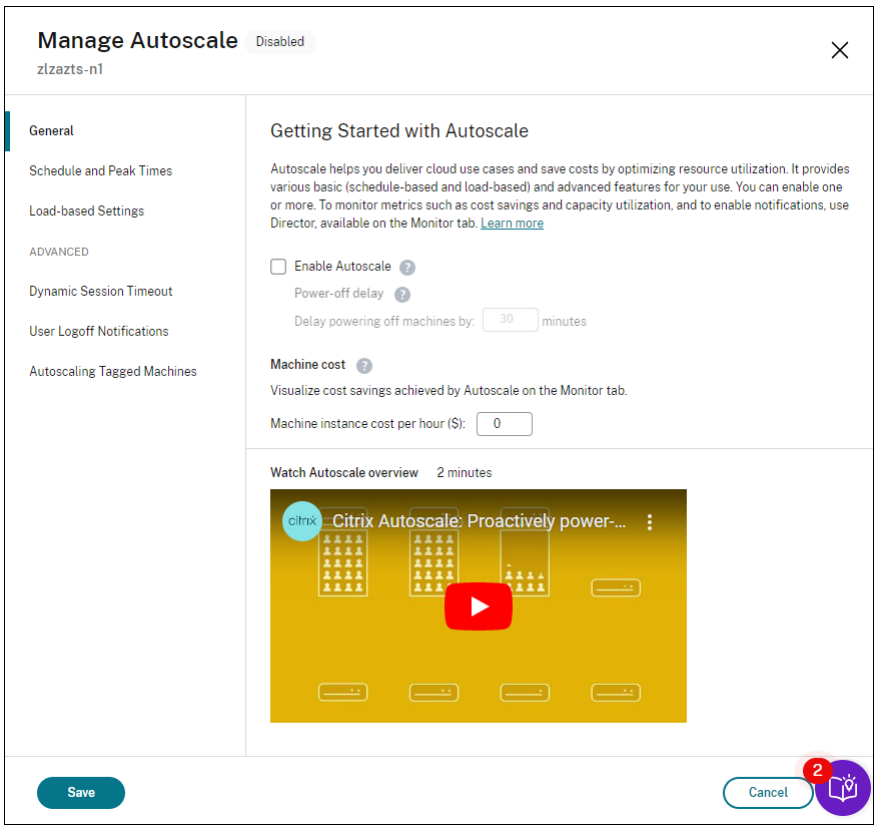
1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.

2. Selezionare il gruppo di consegna da gestire, quindi fare clic su **Manage Autoscale** (Gestione Autoscale).




3. Nella pagina **Manage Autoscale**, selezionare la casella di controllo **Enable Autoscale** per abilitare Autoscale. Dopo aver abilitato Autoscale, le opzioni presenti nella pagina sono abilitate.




4. Per modificare le impostazioni predefinite in base alle esigenze dell'organizzazione, completare le seguenti impostazioni:

   - Set up schedules (Imposta le pianificazioni)
   - Per spegnere i computer inattivi in modo più efficiente, utilizzare i Dynamic session timeouts (Timeout dinamici delle sessioni) e le User logoff notifications (Notifiche di scollega-

mento degli utenti)

- Per gestire in modo efficiente un sottoinsieme di macchine del gruppo di consegna, utilizzare l'impostazione Autoscaling tagged machines (Scalabilità automatica delle macchine con tag)

Per disattivare Autoscale, deselezionare la casella di controllo **Autoscale**. Le opzioni presenti nella pagina diventano grigie per indicare che l'opzione Autoscale è disabilitata per il gruppo di consegna selezionato.

> **Importante:**
>
> - Se si disabilita Autoscale, tutte le macchine gestite da Autoscale rimangono nello stato in cui si trovavano al momento della disattivazione.
> - Dopo aver disabilitato Autoscale, le macchine in stato di scarico vengono rimosse dallo stato di svuotamento. Per ulteriori informazioni sullo stato di svuotamento, vedere Stato di svuotamento.

### Monitorare le metriche

Dopo aver abilitato Autoscale per un gruppo di consegna, è possibile monitorare le seguenti metriche delle macchine gestite da Autoscale da Director.

- Utilizzo della macchina
- Risparmio stimato
- Notifiche di avviso per macchine e sessioni
- Stato della macchina
- Tendenze di valutazione del carico

> **Nota:**
>
> La prima volta che si abilita Autoscale per un gruppo di consegna, potrebbero essere necessari alcuni minuti per visualizzare i dati di monitoraggio per quel gruppo di consegna.
> I dati di monitoraggio rimangono disponibili se l'opzione Autoscale è abilitata e quindi disabilitata per il gruppo di consegna. Autoscale raccoglie i dati di monitoraggio a intervalli di 5 minuti.

Per ulteriori informazioni sulle metriche, vedere Monitorare le macchine gestite da Autoscale.

### Considerazioni importanti

Autoscale funziona a livello di gruppo di consegna. Viene configurato un gruppo di consegna alla volta. Gestisce l'accensione delle sole macchine del gruppo di consegna selezionato.

#### Registrazione della capacità e della macchina

Autoscale include solo le macchine registrate presso il sito al momento della determinazione della capacità. Le macchine accese non registrate non possono accettare richieste di sessione. Di conseguenza, non sono incluse nella capacità complessiva del gruppo di consegna.

#### Scalabilità su più cataloghi di macchine

In alcuni siti, potrebbero esserci più cataloghi di macchine associati a un singolo gruppo di consegna. Autoscale accende in modo casuale le macchine di ciascun catalogo per soddisfare i requisiti della pianificazione o della domanda di sessioni.

Ad esempio, un gruppo di consegna ha due cataloghi di macchine: il catalogo A ha tre macchine accese e il catalogo B ha una macchina accesa. Se Autoscale deve accendere una macchina aggiuntiva, potrebbe accendere una macchina del catalogo A o del catalogo B.

#### Provisioning di macchine e domanda di sessioni

Il catalogo di macchine associato al gruppo di consegna deve avere un numero sufficiente di macchine da accendere e spegnere all'aumentare e al diminuire della domanda. Se la domanda di sessioni supera il numero totale di macchine registrate nel gruppo di consegna, Autoscale garantisce che tutte le macchine registrate siano accese. Tuttavia, **Autoscale non effettua il provisioning di macchine aggiuntive**.

#### Considerazioni sulle dimensioni delle istanze

È possibile ottimizzare i costi se si dimensionano correttamente le istanze nei cloud pubblici. Consigliamo di eseguire il provisioning di istanze più piccole, fintanto che corrispondano ai requisiti di capacità e prestazioni del carico di lavoro.

Le istanze più piccole ospitano meno sessioni utente rispetto alle istanze più grandi. Pertanto Autoscale mette le macchine in stato di svuotamento molto più velocemente, perché lo scollegamento dell'ultima sessione utente impiega meno tempo. Di conseguenza, Autoscale spegne prima le istanze più piccole, riducendo così i costi.

#### Stato di svuotamento

Autoscale tenta di ridurre il numero di macchine accese del gruppo di consegna in base alla dimensione del pool configurato e al buffer di capacità.

Per raggiungere questo obiettivo, Autoscale mette le macchine in eccesso con il minor numero di sessioni in "stato di svuotamento"e le spegne quando tutte le sessioni vengono scollegate. Questo comportamento si verifica quando la domanda di sessioni diminuisce e la pianificazione richiede meno computer di quanti ne siano accesi.

Autoscale mette le macchine in eccesso in "stato di svuotamento"una per una, in base ai seguenti criteri:

- Se due o più macchine hanno lo stesso numero di sessioni attive, Autoscale scarica la macchina che è stata accesa per il ritardo di spegnimento specificato.

  In questo modo si evita di mettere le macchine accese di recente in stato di svuotamento perché è più probabile che quelle macchine abbiano il minor numero di sessioni.

- Se due o più macchine sono state accese per il ritardo di spegnimento specificato, Autoscale mette in stato di svuotamento tali macchine una in ordine casuale.

Le macchine in stato di svuotamento non ospitano più nuovi avvii di sessioni e sono in attesa che le sessioni esistenti vengano scollegate. Una macchina diventa candidata per l'arresto solo quando tutte le sessioni sono scollegate. Tuttavia, se non ci sono macchine immediatamente disponibili per l'avvio delle sessioni, Autoscale preferisce dirigere gli avvii di sessione su una macchina in stato di svuotamento piuttosto che accendere una macchina.

Una macchina viene tolta dallo stato di svuotamento quando viene soddisfatta una delle seguenti condizioni:

- La macchina è spenta.
- Autoscale è disabilitato per il gruppo di consegna a cui appartiene la macchina.
- Autoscale utilizza la macchina per soddisfare i requisiti di pianificazione o di domanda di carico. Questo caso si verifica quando la pianificazione (ridimensionamento basato su pianificazione) o la domanda corrente (ridimensionamento basato sul carico) richiede più macchine rispetto al numero di macchine attualmente accese.

> **Importante:**
>
> Se nessuna macchina è immediatamente disponibile per gli avvii delle sessioni, Autoscale preferisce dirigere gli avvii di sessione su una macchina in stato di svuotamento piuttosto che accendere una macchina. Una macchina in stato di svuotamento che ospita l'avvio di una sessione rimane in stato di svuotamento.

Per scoprire quali macchine sono in stato di svuotamento, utilizzare il comando `Get-BrokerMachine` di PowerShell. Ad esempio: `Get-BrokerMachine -DrainingUntilShutdown $true`. In alternativa, è possibile utilizzare la console Manage (Gestisci). Vedere Visualizzare le macchine in stato di svuotamento.

### Visualizzare le macchine in stato di svuotamento

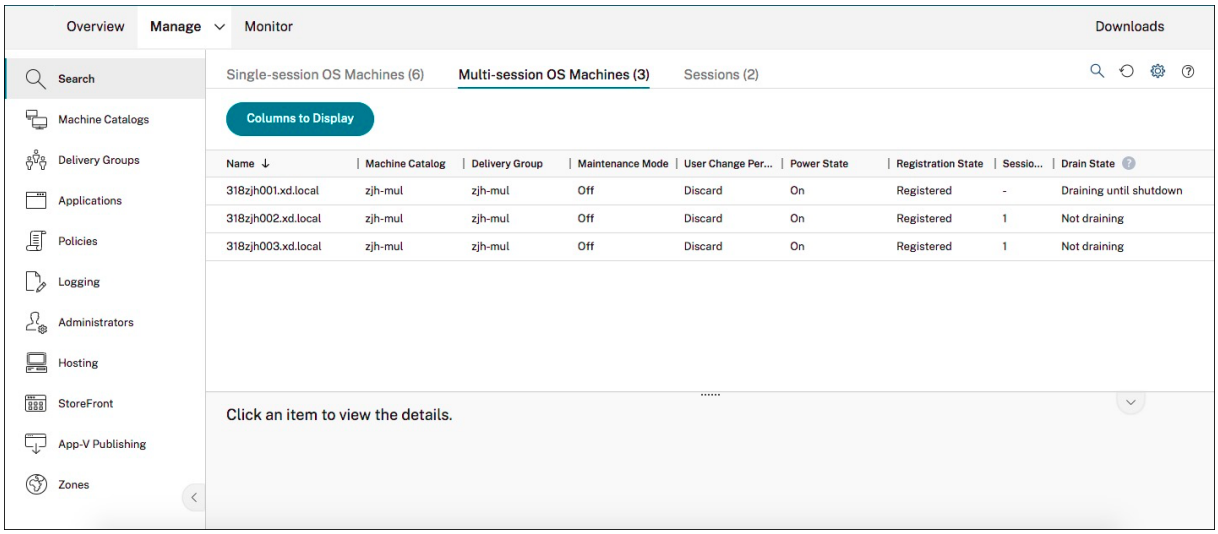
> **Nota:**
>
> Questa funzione si applica solo alle macchine multisessione.

In Web Studio, è possibile visualizzare le macchine in stato di svuotamento, per sapere quali macchine stanno per essere arrestate. Completare i seguenti passaggi:

1. Passare al nodo **Search** e quindi fare clic su **Columns to Display** (Colonne da visualizzare).
2. Nella finestra **Colonne da visualizzare**, selezionare la casella di controllo accanto a **Drain State** (Stato di svuotamento).
3. Fare clic su **Save** (Salva) per uscire dalla finestra **Columns to Display**.

La colonna **Drain State** può visualizzare le seguenti informazioni:

- **Draining until shutdown.** Viene visualizzato quando le macchine sono in stato di svuotamento finché non vengono spente.
- **Not draining.** Appare quando le macchine non sono ancora in stato di svuotamento.




### Ulteriori informazioni

Per ulteriori informazioni sul Autoscale, vedere Citrix Autoscale in Tech Zone.

## Impostazioni basate sulla pianificazione e sul carico

January 7, 2024

### Come Autoscale gestisce l'alimentazione delle macchine

Autoscale accende e spegne le macchine in base alla pianificazione selezionata. Autoscale consente di impostare più pianificazioni che includono giorni specifici della settimana e di regolare il numero di macchine disponibili in tali orari. Se ci si aspetta che un gruppo di utenti consumi le risorse macchina in un momento specifico in giorni specifici, Autoscale aiuta a fornire un'esperienza ottimizzata. Si noti che tali macchine saranno accese durante la pianificazione, indipendentemente dal fatto che ci siano o meno sessioni in esecuzione su di esse.

> **Nota:**
>
> Autoscale supporta qualsiasi macchina con alimentazione gestita.

La pianificazione si basa sul **fuso orario** del gruppo di consegna. Per modificare il fuso orario, è possibile modificare le impostazioni utente di un gruppo di consegna. Per ulteriori informazioni, vedere Gestire i gruppi di consegna.

Autoscale ha due orari predefiniti: *Weekdays* (da lunedì a venerdì) e *Weekend* (sabato e domenica). Per impostazione predefinita, la pianificazione **Weekdays** mantiene accesa una macchina dalle 07:00 alle 18:30 durante le ore di punta e non ne mantiene accesa nessuna durante le ore non di punta. Il buffer di capacità predefinito è impostato al 10% durante le ore di punta e non di punta. Per impostazione predefinita, la pianificazione **Weekend** non mantiene acceso nessun computer.

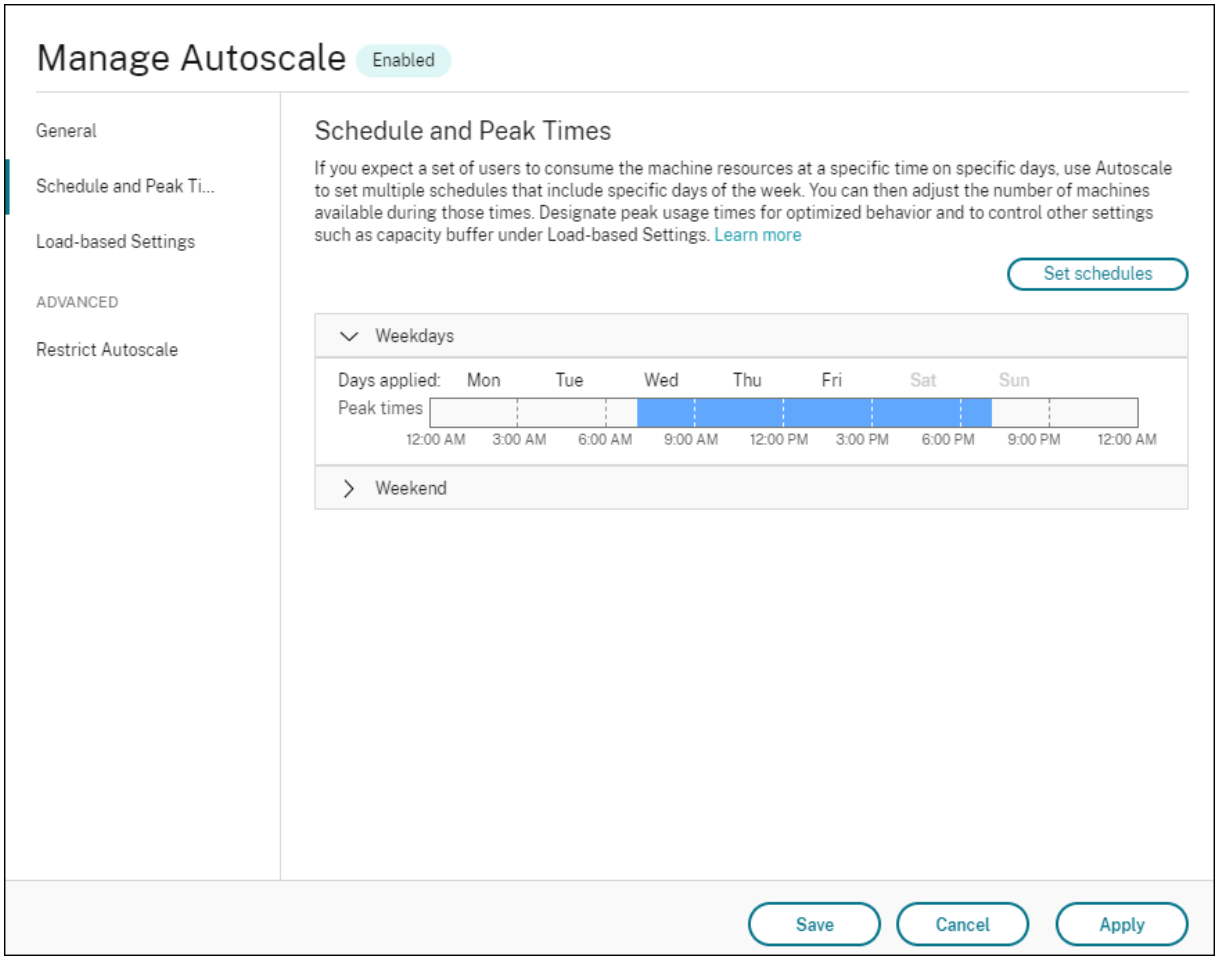
> **Nota:**
>
> Autoscale considera solo le macchine registrate nel sito come parte della capacità disponibile nei calcoli che effettua. "Registered"(Registrata) significa che la macchina è disponibile per l'uso o già in uso. In questo modo si garantisce che solo le macchine in grado di accettare sessioni utente siano incluse nella capacità del gruppo di consegna.

### Interfacce utente

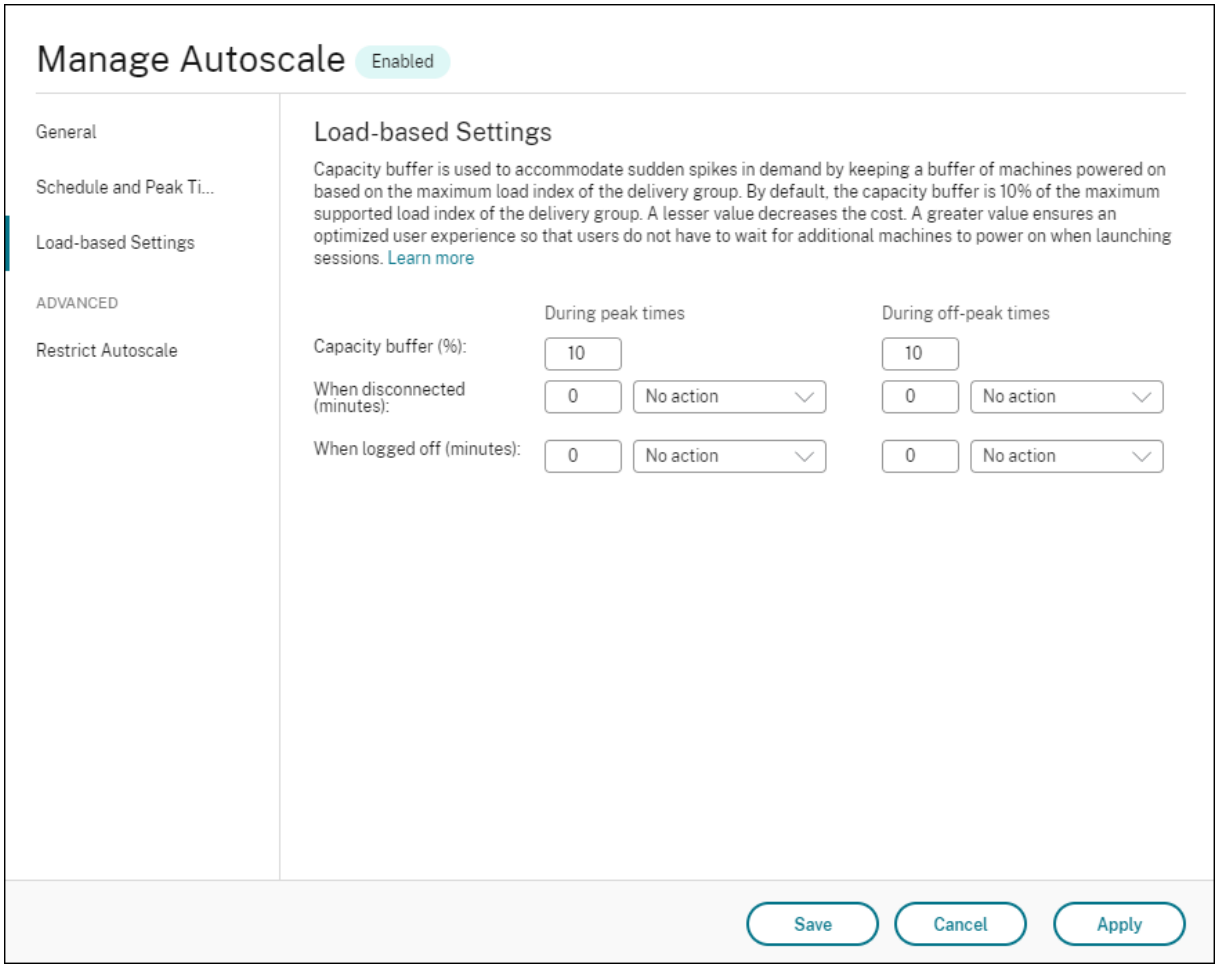
Esistono tre tipi di interfacce utente da tenere presenti.

Interfaccia utente per *gruppi di consegna statici con sistema operativo a sessione singola*:

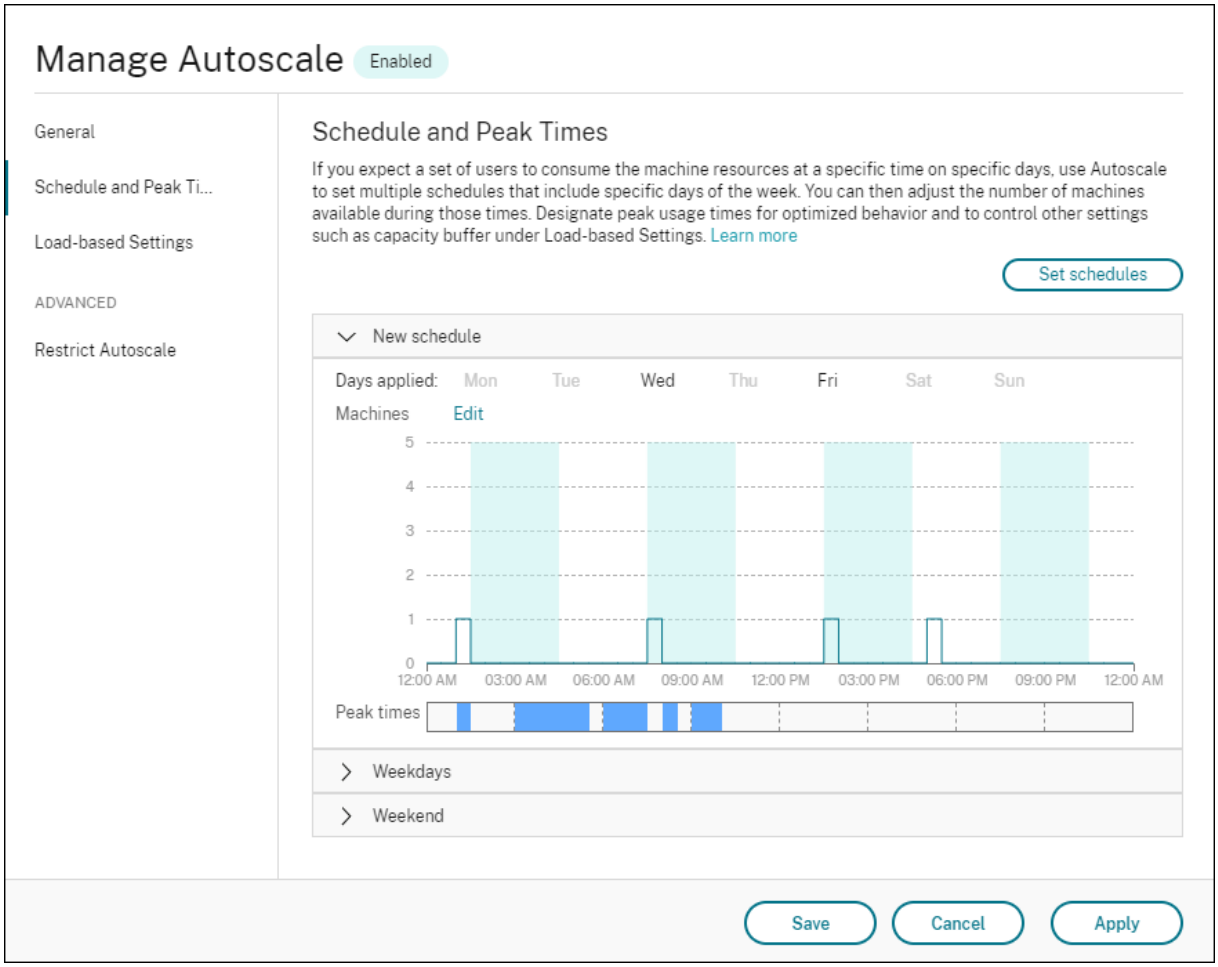


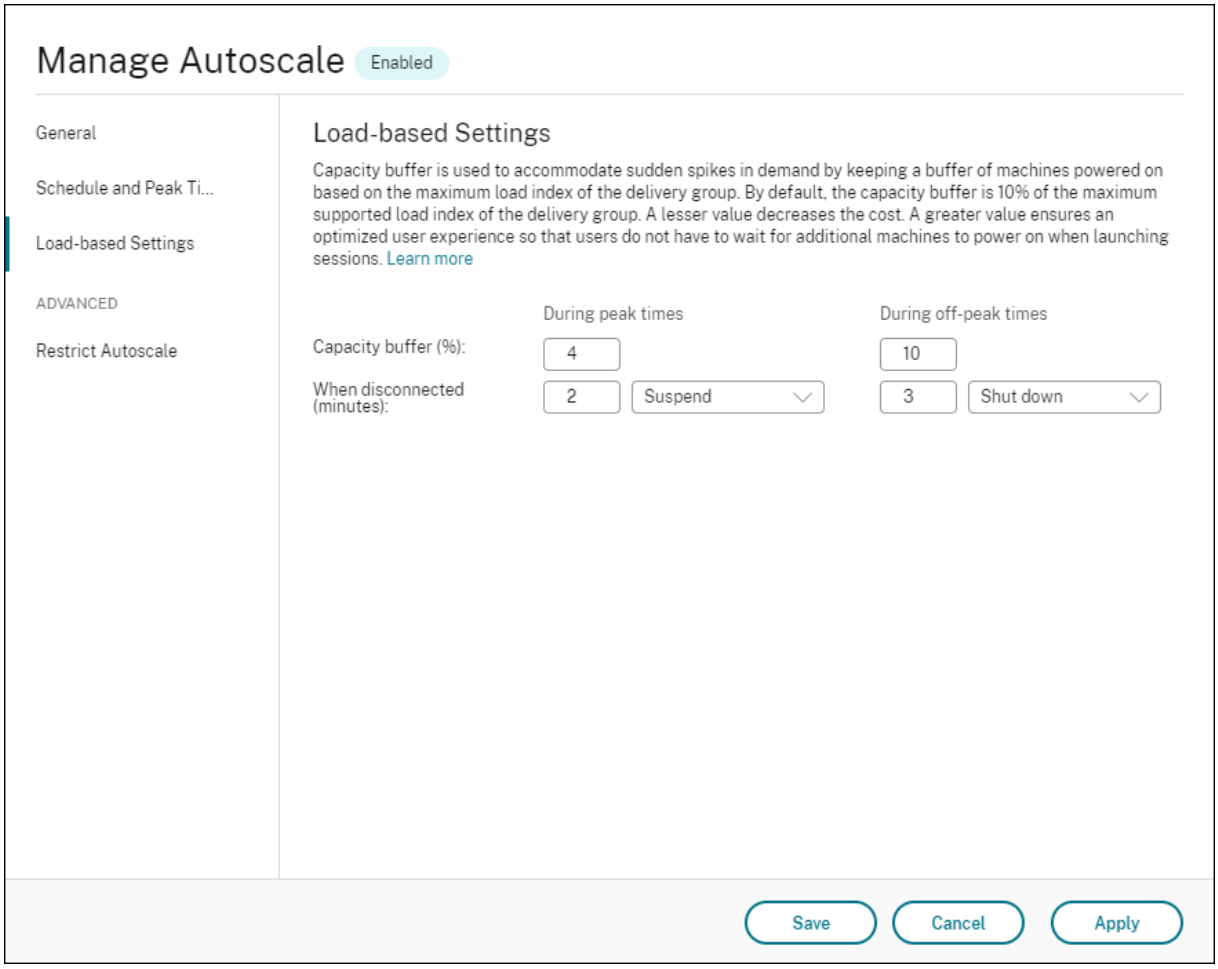



Interfaccia utente Autoscale per *gruppi di consegna casuali con sistema operativo a sessione singola*:

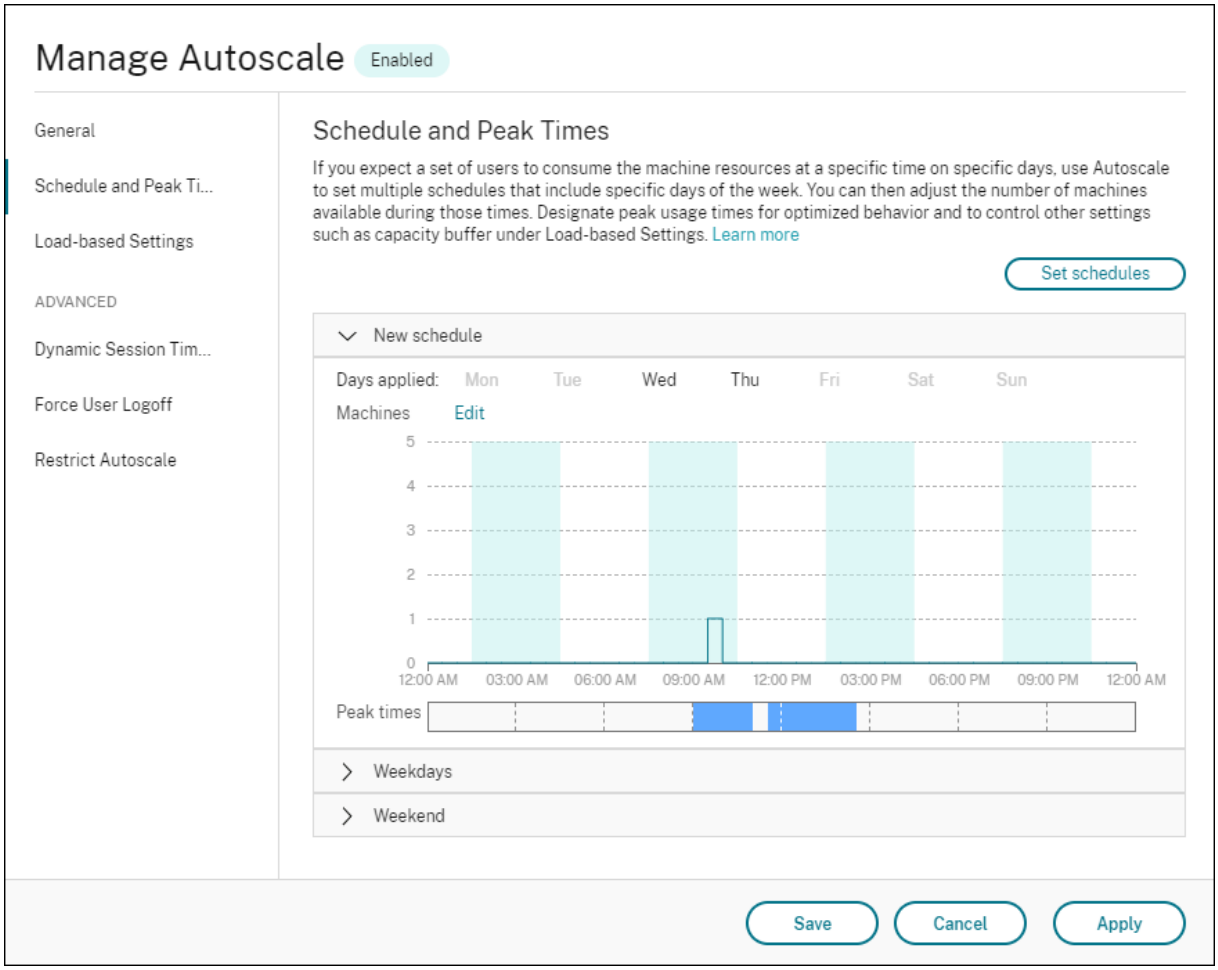


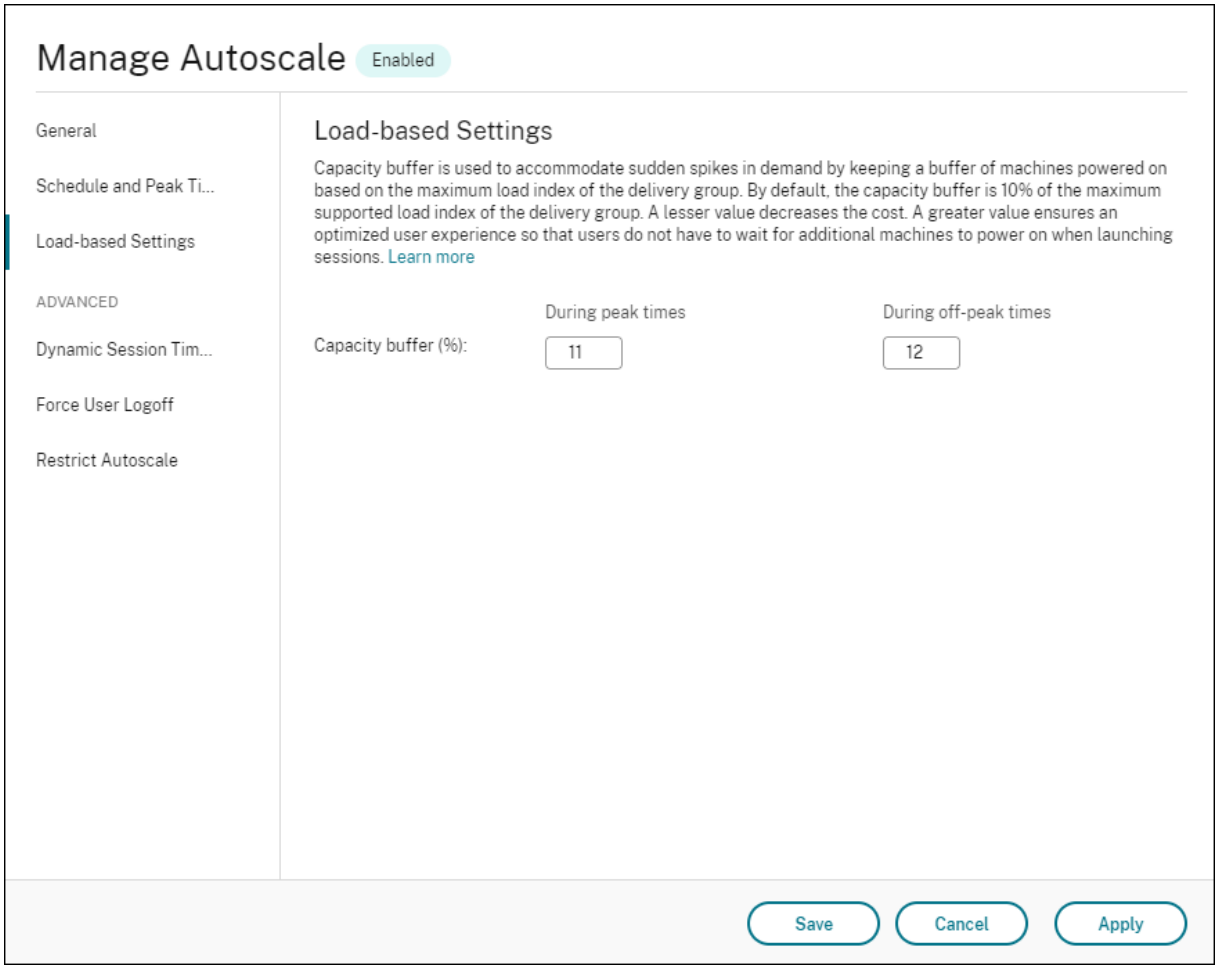



Interfaccia utente Autoscale per *gruppi di consegna di sistemi operativi multisessione*:






### Impostazioni basate sulla pianificazione

**Pianificazione Autoscale**. Consente di aggiungere, modificare, selezionare ed eliminare le pianificazioni.

**Giorni applicati**. Evidenzia i giorni applicati alla pianificazione selezionata. I giorni rimanenti sono in grigio.

**Edit**. Consente di assegnare le macchine rispetto a ciascuna ora esatta o mezz'ora. È possibile assegnare le macchine in base ai numeri e alle percentuali.

> **Nota:**
>
> - Questa opzione è disponibile solo nelle interfacce utente di Autoscale per i gruppi di consegna casuali con sistema operativo multisessione e a sessione singola.
> - L'istogramma accanto a **Edit** rappresenta il numero o la percentuale di macchine in esecuzione in diverse fasce orarie.
> - È possibile **assegnare macchine** rispetto a ciascuna fascia oraria facendo clic su **Edit** al di

sopra di **Peak times**. A seconda dell'opzione selezionata dal menu nella finestra **Machines to start** (Macchine da avviare), è possibile assegnare le macchine in base ai numeri o alle percentuali.
- Per i gruppi di consegna di sistemi operativi multisessione, è possibile impostare il numero minimo di macchine in esecuzione separatamente con incrementi granulari di 30 minuti nell'arco di ogni giorno. Per i gruppi di consegna casuale con sistema operativo a sessione singola, è possibile impostare il numero minimo di macchine in esecuzione separatamente con incrementi granulari di 60 minuti nell'arco di ogni giorno.

Per definire le proprie pianificazioni, attenersi alla seguente procedura:

1. Nella pagina **Schedule and Peak Times** (Pianificazione e orari di punta) della finestra **Manage Autoscale**, fare clic su **Set schedules** (Imposta pianificazioni).
2. Nella finestra **Edit Autoscale Schedules** (Modifica pianificazioni Autoscale), selezionare i giorni che si desidera applicare a ciascuna pianificazione. È inoltre possibile eliminare le pianificazioni secondo necessità.
3. Fare clic su **Done** (Fine) per salvare le pianificazioni e tornare alla pagina **Schedule and Peak Times**(Pianificazione e orari di punta).
4. Selezionare la pianificazione applicabile e configurarla secondo necessità.
5. Fare clic su **Apply** per uscire dalla finestra **Manage Autoscale** o per configurare le impostazioni su altre pagine.

**Importante:**

- Autoscale non consente che lo stesso giorno si sovrapponga in pianificazioni diverse. Ad esempio, se si seleziona il lunedì nella pianificazione2 dopo aver selezionato il lunedì nella pianificazione1, il lunedì viene cancellato automaticamente nella pianificazione1.
- Il nome di una pianificazione non fa distinzione tra maiuscole e minuscole.
- Il nome di una pianificazione non deve essere vuoto o contenere solo spazi.
- Autoscale consente di inserire spazi vuoti tra i caratteri.
- Il nome di una pianificazione non deve contenere i seguenti caratteri: \ / ; : # . * ? = < > | [ ] ( ) { } “‘.
- Autoscale non supporta nomi di pianificazione duplicati. Inserire un nome diverso per ciascuna pianificazione.
- Autoscale non supporta le pianificazioni vuote. Ciò significa che le pianificazioni senza giorni selezionati non vengono salvate.

**Nota:**

I giorni inclusi nel programma selezionato sono evidenziati, mentre quelli non inclusi sono in

> grigio.

### Impostazioni basate sul carico

**Ore di punta**. Consente di definire le ore di punta per i giorni applicati nella pianificazione selezionata. È possibile farlo facendo clic con il pulsante destro del mouse sul grafico a barre orizzontale. Dopo aver definito le ore di punta, le restanti ore non definite vengono impostate automaticamente su ore non di punta. Per **impostazione predefinita**, la fascia oraria dalle 7:00 alle 19:00 è definita orario di punta per i giorni inclusi nella pianificazione selezionata.

> **Importante:**
>
> - Nel caso dei gruppi di consegna di sistemi operativi multisessione, il grafico a barre delle ore di punta viene utilizzato per il buffer di capacità.
> - Nel caso dei gruppi di consegna di sistemi operativi a sessione singola, il grafico a barre delle ore di punta viene utilizzato per il buffer di capacità e controlla le azioni da attivare dopo lo scollegamento e/o la disconnessione.
> - È possibile definire gli orari di punta per i giorni inclusi in una pianificazione a un livello granulare di 30 minuti per i gruppi di consegna di sistemi operativi multisessione e a sessione singola. In alternativa, è possibile utilizzare il comando `New-BrokerPowerTimeScheme PowerShell`. Per ulteriori informazioni, vedere Comandi dell'SDK Broker PowerShell.

**Buffer di capacità**. Consente di mantenere un buffer di macchine accese. Un valore inferiore riduce il costo. Un valore superiore garantisce un'esperienza utente ottimizzata in modo che, all'avvio delle sessioni, gli utenti non debbano attendere l'accensione di altre macchine. Per impostazione predefinita, il buffer di capacità è del 10% per le ore di punta e non di punta. Se si imposta il buffer di capacità su 0 (zero), gli utenti potrebbero dover attendere l'accensione di altre macchine all'avvio delle sessioni. Autoscale consente di determinare il buffer di capacità separatamente per le ore di punta e non di punta.

### Impostazioni varie

> **Suggerimento:**
>
> - È possibile scegliere di configurare le impostazioni varie utilizzando l'SDK Broker PowerShell. Per ulteriori informazioni, vedere Comandi dell'SDK Broker PowerShell.
> - Per comprendere i comandi dell'SDK associati alle impostazioni di disconnessione e disconnessione, vedere https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy.

**Quando si è disconnessi**. Consente di specificare per quanto tempo una macchina disconnessa e bloccata rimane accesa dopo la disconnessione della sessione prima della sospensione o la chiusura della sessione. Se viene specificato un valore temporale, il computer viene sospeso o arrestato allo scadere del tempo di disconnessione specificato, a seconda dell'azione configurata. Per impostazione predefinita, non viene assegnata alcuna azione alle macchine disconnesse. È possibile definire separatamente azioni per le ore di punta e non di punta. A tale scopo, fare clic sulla freccia rivolta verso il basso e quindi selezionare una delle seguenti opzioni dal menu:

- **No action**. Se è selezionata questa opzione, dopo la disconnessione della sessione la macchina rimane accesa. Autoscale non agisce su di essa.
- **Suspend** Se è selezionata questa opzione, Autoscale mette in pausa la macchina senza spegnerla allo scadere del tempo di disconnessione specificato. Dopo aver selezionato **Suspend** si rende disponibile la seguente opzione.
  - **When no reconnection in (minutes)**. Le macchine sospese rimangono disponibili per gli utenti disconnessi quando questi si riconnettono, ma non sono disponibili per i nuovi utenti. Per rendere nuovamente disponibili le macchine a gestire tutti i carichi di lavoro, arrestarle. Specificare il timeout, in minuti, dopo il quale Autoscale le spegne.
- **Shut down**. Se è selezionata questa opzione, Autoscale arresta la macchina allo scadere del tempo di disconnessione specificato.

> **Nota:**
>
> Questa opzione è disponibile solo nelle interfacce utente di Autoscale per gruppi di consegna casuali e statici di sistemi operativi a sessione singola.

**When logged off**. Consente di specificare per quanto tempo una macchina rimane accesa dopo lo scollegamento della sessione prima di essere sospesa o arrestata. Se viene specificato un valore temporale, la macchina viene sospesa o arrestata allo scadere del tempo di disconnessione specificato, a seconda delle azioni configurate. Per impostazione predefinita, non viene assegnata alcuna azione alle macchine scollegate. È possibile definire separatamente azioni per le ore di punta e non di punta. A tale scopo, fare clic sulla freccia rivolta verso il basso e quindi selezionare una delle seguenti opzioni dal menu:

- **No action**. Se è selezionata questa opzione, dopo lo scollegamento della sessione la macchina rimane accesa. Autoscale non agisce su di essa.
- **Suspend** Se è selezionata questa opzione, Autoscale mette in pausa la macchina senza spegnerla allo scadere del tempo di scollegamento specificato.
- **Shut down**. Se è selezionata questa opzione, Autoscale arresta la macchina allo scadere del tempo di scollegamento specificato.

> **Nota:**
>
> Questa opzione è disponibile solo nell'interfaccia utente Autoscale per gruppi di consegna statici di sistemi operativi a sessione singola.

### Gestire l'alimentazione di macchine con sistema operativo a sessione singola che passano a un periodo di tempo diverso con sessioni disconnesse

> **Importante:**
>
> - Questo miglioramento si applica solo alle macchine con sistema operativo a sessione singola con sessioni disconnesse. Non si applica alle macchine con sistema operativo a sessione singola con sessioni scollegate.
> - Affinché questo miglioramento abbia effetto, è necessario abilitare l'opzione Autoscale per il gruppo di consegna applicabile. In caso contrario, le azioni dei criteri di disconnessione non vengono attivate durante la transizione da un periodo all'altro.

Nelle versioni precedenti, una macchina con sistema operativo a sessione singola che passava a un periodo di tempo in cui era necessaria un'azione (azione di disconnessione= "**Suspend**"o "**Shutdown"** ) rimaneva alimentata. Questo scenario si verificava se la macchina si disconnetteva durante un periodo di tempo (di punta o non di punta) in cui non era richiesta alcuna azione (azione di disconnessione = "**Nothing**").

A partire da questa versione, Autoscale mette in sospensione o arresta la macchina al termine del tempo di disconnessione specificato, a seconda dell'azione di disconnessione configurata per il periodo di tempo di destinazione.

Ad esempio, è possibile configurare i criteri di risparmio energia seguenti per un gruppo di consegna di sistemi operativi a sessione singola:

- Impostare `PeakDisconnectAction` su "Nothing"
- Impostare `OffPeakDisconnectAction` su "Shutdown"
- Impostare "OffPeakDisconnectTimeout"su "10"

> **Nota:**
>
> Per ulteriori informazioni sui criteri di risparmio energia per l'azione di disconnessione, vedere https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy e https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Nelle versioni precedenti, una macchina con sistema operativo a sessione singola con una sessione disconnessa durante i periodi di punta rimaneva accesa quando passava dai periodi di punta a quelli

non di punta. A partire da questa versione, le azioni dei criteri `OffPeakDisconnectAction` e `OffPeakDisconnectTimeout` vengono applicate alla macchina con sistema operativo a sessione singola durante la transizione da un periodo all'altro. Di conseguenza, la macchina viene spenta 10 minuti dopo la transizione al periodo fuori picco.

Nel caso in cui si desideri ripristinare il comportamento precedente (ovvero, non eseguire alcuna azione su macchine che passano dal periodo di punta a quello fuori picco o al periodo di punta con sessioni disconnesse), effettuare una delle seguenti operazioni:

- Impostare il valore del Registro di sistema "LegacyPeakTransitionDisconnectedBehaviour"su 1, (true; abilita il comportamento precedente). Per impostazione predefinita, il valore è 0 (false; attiva la disconnessione delle azioni dei criteri di risparmio energia durante la transizione da un periodo all'altro).
  - Percorso: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Nome: LegacyPeakTransitionDisconnectedBehaviour
  - Tipo: REG_DWORD
  - Dati: 0x00000001 (1)
- Configurare l'impostazione utilizzando il comando PowerShell`Set-BrokerServiceConfigurationD` . Ad esempio:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Una macchina deve soddisfare i seguenti criteri prima che le possano essere applicate le azioni dei criteri di risparmio energia durante la transizione da un periodo all'altro:

- Ha una sessione disconnessa.
- Non ha azioni di alimentazione in sospeso.
- Appartiene a un gruppo di consegna di sistemi operativi a sessione singola che passa a un periodo di tempo diverso.
- Ha una sessione che si disconnette durante un determinato periodo di tempo (di punta o non di punta) e passa a un periodo in cui viene assegnata un'azione di alimentazione.

### Come funziona il buffer di capacità

Il buffer di capacità viene utilizzato per aggiungere capacità di riserva alla domanda corrente per tenere conto degli aumenti dinamici del carico. Ci sono due scenari da tenere presenti:

- Per i gruppi di consegna di sistemi operativi multisessione, il buffer di capacità è definito come una percentuale della capacità totale del gruppo di consegna in termini di indice di carico. Per ulteriori informazioni sull'indice di carico, vedere Indice di carico.

- Per i gruppi di consegna di sistemi operativi a sessione singola, il buffer di capacità è definito come una percentuale della capacità totale del gruppo di consegna in termini di numero di macchine.

> **Nota:**
>
> Negli scenari in cui si limita Autoscale alle macchine con tag, il buffer di capacità è definito come una percentuale della capacità totale delle macchine con tag del gruppo di consegna in termini di indice di carico.

Autoscale consente di impostare il buffer di capacità separatamente per le ore di punta e non di punta. Un valore inferiore nel campo del buffer di capacità riduce il costo perché Autoscale alimenta una minore capacità di riserva. Un valore superiore garantisce un'esperienza utente ottimizzata in modo che gli utenti non debbano attendere l'accensione di altre macchine all'avvio delle sessioni. Per impostazione predefinita, il buffer di capacità è del 10%.

> **Importante:**
>
> Il buffer di capacità fa sì che le macchine vengano accese quando la capacità di riserva totale scende a un livello inferiore a "X"per cento della capacità totale del gruppo di consegna. In questo modo si riserva la percentuale richiesta di capacità di riserva.

### Gruppi di consegna di sistemi operativi multisessione

#### Quando vengono accese le macchine?

> **Importante:**
>
> Se viene selezionata una pianificazione, Autoscale accende tutte le macchine configurate per essere accese nella pianificazione. Autoscale mantiene acceso questo numero specificato di macchine durante la pianificazione, indipendentemente dal carico.

Quando il numero di macchine accese nel gruppo di consegna non è più in grado di soddisfare il buffer necessario per onorare la capacità del buffer in termini di indice di carico, Autoscale si alimenta su macchine aggiuntive. Ad esempio, supponiamo che il proprio gruppo di consegna disponga di 20 macchine e che 3 macchine siano programmate per essere accese come parte del ridimensionamento basato su pianificazione con un buffer di capacità del 20%. Alla fine, 4 macchine verranno accese quando non c'è carico. Questo perché è necessario un indice di carico 4 x 10.000 come buffer; quindi è necessario accendere almeno 4 macchine. Questo caso può verificarsi durante le ore di punta, durante l'aumento del carico sulle macchine, durante l'avvio di nuove sessioni e quando si aggiungono nuove macchine al gruppo di consegna. Notare che Autoscale funziona solo sulle macchine che soddisfano i seguenti criteri:

- Le macchine non sono in modalità di manutenzione.

- L'hypervisor su cui sono in esecuzione le macchine non è in modalità di manutenzione.
- Le macchine sono attualmente spente.
- Le macchine non hanno azioni relative all'alimentazione in sospeso.

#### Quando vengono spente le macchine?

> **Importante:**
>
> - Se viene selezionata una pianificazione, Autoscale spegne le macchine in base alla pianificazione.
> - Autoscale non spegne le macchine che nella pianificazione sono configurate per essere accese durante la pianificazione.

Quando ci sono macchine più che sufficienti a supportare il numero target di macchine accese (incluso il buffer) per il gruppo di consegna, Autoscale spegne le macchine aggiuntive. Questo caso può verificarsi durante le ore non di punta, durante la riduzione del carico sui computer, durante lo scollegamento delle sessioni e quando si rimuovono macchine dal gruppo di consegna. Autoscale spegne solo le macchine che soddisfano i seguenti criteri:

- Le macchine e l'hypervisor su cui sono in esecuzione le macchine non sono in modalità di manutenzione.
- Le macchine sono attualmente accese.
- Le macchine sono registrate come disponibili o in attesa di registrazione dopo l'avvio.
- Le macchine non hanno sessioni attive.
- Le macchine non hanno azioni relative all'alimentazione in sospeso.
- Le macchine soddisfano il ritardo di spegnimento specificato. Ciò significa che le macchine sono state accese per almeno "X"minuti, dove "X"è il ritardo di spegnimento specificato per il gruppo di consegna.

#### Esempio di scenario

Supponiamo di avere il seguente scenario:

- **Configurazione del gruppo di consegna**. Il gruppo di consegna la cui alimentazione si desidera venga gestita da Autoscale contiene 10 macchine (da M1 a M10).
- **Configurazione di Autoscale**
  - Il buffer di capacità è impostato al 10%.

  - Nessuna macchina è inclusa nella pianificazione selezionata.

Lo scenario viene eseguito nella seguente sequenza:

1. Nessun utente effettua l'accesso.
2. Le sessioni utente aumentano.
3. Vengono avviate altre sessioni utente.
4. Il carico della sessione utente diminuisce a causa della chiusura della sessione.
5. Il carico della sessione utente diminuisce ulteriormente fino a quando il carico della sessione non viene gestito solo da risorse locali.

Vedere sotto per i dettagli di come funziona Autoscale nello scenario di cui sopra.

- Nessun carico utente (stato iniziale)
  - Una macchina (ad esempio M1) è accesa. La macchina viene accesa a causa del buffer di capacità configurato. In questo caso, 10 (numero di macchine) x 10.000 (indice di carico) x 10% (buffer di capacità configurato) equivale a 10.000. Pertanto, viene accesa una macchina.
  - Il valore dell'indice di carico della macchina accesa (M1) è a un carico di base (l'indice di carico è uguale a 0).
- Il primo utente esegue l'accesso
  - La sessione è indirizzata a essere ospitata sulla macchina M1.
  - L'indice di carico della macchina accesa M1 aumenta e la macchina M1 non è più a un carico di base.
  - Autoscale inizia ad accendere una macchina aggiuntiva (M2) per soddisfare la domanda a causa del buffer di capacità configurato.
  - Il valore dell'indice di carico della macchina M2 è a un carico di base.
- Gli utenti aumentano il carico
  - Le sessioni hanno il carico distribuito fra le macchine M1 e M2. Di conseguenza, l'indice di carico delle macchine accese (M1 e M2) aumenta.
  - La capacità di riserva totale è ancora a un livello superiore a 10.000 in termini di indice di carico.
  - Il valore dell'indice di carico della macchina M2 non è più a un carico di base.
- Avvio di altre sessioni utente
  - Le sessioni hanno il carico distribuito su tutte le macchine (M1 e M2). Di conseguenza, l'indice di carico delle macchine alimentate (M1 e M2) aumenta ulteriormente.

  - Quando la capacità di riserva totale scende a un livello inferiore a 10.000 in termini di indice di carico, Autoscale inizia ad accendere una macchina aggiuntiva (M3) per soddisfare la domanda, dato il buffer di capacità configurato.
  - Il valore dell'indice di carico della macchina M3 è a un carico di base.

- Vengono avviate ancora più sessioni utente
  - Le sessioni hanno il carico distribuito su tutte le macchine (da M1 a M3). Di conseguenza, l'indice di carico delle macchine accese (da M1 a M3) aumenta.
  - La capacità di riserva totale è a un livello superiore a 10.000 in termini di indice di carico.
  - Il valore dell'indice di carico della macchina M3 non è più a un carico di base.

- Il carico della sessione utente diminuisce a causa della chiusura della sessione
  - Dopo che gli utenti si sono disconnessi dalle sessioni o dopo il timeout delle sessioni inattive, la capacità che si è liberata sulle macchine da M1 a M3 viene riutilizzata per ospitare sessioni avviate da altri utenti.
  - Quando la capacità di riserva totale aumenta fino a un livello superiore a 10.000 in termini di indice di carico, Autoscale mette una delle macchine (ad esempio M3) in stato di svuotamento. Di conseguenza, le sessioni avviate da altri utenti non vengono più indirizzate a quel computer a meno che non vi siano nuovi cambiamenti. Ad esempio, il carico dell'utente finale aumenta nuovamente o altre macchine diventano meno cariche.

- Il carico della sessione utente continua a diminuire
  - Dopo che tutte le sessioni sulla macchina M3 sono terminate e il ritardo di spegnimento specificato è scaduto, Autoscale spegne la macchina M3.
  - Dopo che più utenti hanno terminato le sessioni, la capacità liberata sulle macchine accese (M1 e M2) viene riutilizzata per ospitare sessioni avviate da altri utenti.
  - Quando la capacità di riserva totale aumenta fino a un livello superiore a 10.000 in termini di indice di carico, Autoscale mette una delle macchine (ad esempio M2) in stato di svuotamento. Di conseguenza, le sessioni avviate da altri utenti non vengono più indirizzate a quella macchina.

- Il carico della sessione utente continua a diminuire fino a quando non ci sono sessioni
  - Dopo che tutte le sessioni sulla macchina M2 sono terminate e il ritardo di spegnimento specificato è scaduto, Autoscale spegne la macchina M2.
  - Il valore dell'indice di carico della macchina accesa (M1) è a un carico di base. Autoscale non mette la macchina M1 in stato di svuotamento a causa del buffer di capacità configurato.

> **Nota:**
>
> Per i gruppi di consegna di sistemi operativi multisessione, tutte le modifiche al desktop vengono

> perse quando gli utenti si scollegano dalle sessioni. Tuttavia, se configurate, le impostazioni specifiche dell'utente vengono spostate insieme al profilo utente.

### Gruppi di consegna casuale di sistemi operativi a sessione singola

Il buffer di capacità viene utilizzato per gestire i picchi improvvisi della domanda mantenendo un buffer di macchine accese in base al numero totale di macchine incluse nel gruppo di consegna. Per impostazione predefinita, il buffer di capacità è pari al 10% del numero totale di macchine incluse nel gruppo di consegna.

Se il numero di macchine (incluso il buffer di capacità) supera il numero totale di macchine attualmente accese, vengono accese macchine aggiuntive per soddisfare la domanda. Se il numero di macchine (incluso il buffer di capacità) è inferiore al numero totale di macchine attualmente accese, le macchine in eccesso vengono arrestate o sospese, a seconda delle azioni configurate.

#### Esempio di scenario

Supponiamo di avere il seguente scenario:

- **Configurazione del gruppo di consegna**. Il gruppo di consegna la cui alimentazione si desidera venga gestita da Autoscale contiene 10 macchine (da M1 a M10).
- **Configurazione di Autoscale**
  - Il buffer di capacità è impostato al 10%.
  - Nessuna macchina è inclusa nella pianificazione selezionata.

Lo scenario viene eseguito nella seguente sequenza:

1. Nessun utente effettua l'accesso.
2. Le sessioni utente aumentano.
3. Vengono avviate altre sessioni utente.
4. Il carico della sessione utente diminuisce a causa della chiusura della sessione.
5. Il carico della sessione utente diminuisce ulteriormente fino a quando il carico della sessione non viene gestito solo da risorse locali.

Vedere sotto per i dettagli di come funziona Autoscale nello scenario di cui sopra.

- Nessun carico utente (stato iniziale)
  - Viene accesa una macchina (M1). La macchina viene accesa a causa del buffer di capacità configurato. In questo caso, 10 (numero di macchine) x 10% (buffer di capacità configurato) equivale a 1. Pertanto, viene accesa una macchina.

- Un primo utente esegue l'accesso
  - La prima volta che un utente esegue l'accesso per utilizzare un desktop, gli viene assegnato un desktop che fa parte di un pool di desktop ospitati su macchine accese. In questo caso, all'utente viene assegnato un desktop proveniente dalla macchina M1.
  - Autoscale inizia ad accendere una macchina aggiuntiva (M2) per soddisfare la domanda a causa del buffer di capacità configurato.
- Un secondo utente esegue l'accesso
  - All'utente viene assegnato un desktop proveniente dalla macchina M2.
  - Autoscale inizia ad accendere una macchina aggiuntiva (M3) per soddisfare la domanda a causa del buffer di capacità configurato.
- Un terzo utente esegue l'accesso
  - All'utente viene assegnato un desktop proveniente dalla macchina M3.
  - Autoscale inizia ad accendere una macchina aggiuntiva (M4) per soddisfare la domanda a causa del buffer di capacità configurato.
- Un utente si scollega
  - Dopo lo scollegamento di un utente o il timeout del desktop dell'utente, la capacità liberata (ad esempio M3) è disponibile come buffer. Di conseguenza, Autoscale inizia a spegnere la macchina M4 perché il buffer di capacità è configurato al 10%.
- Altri utenti si scollegano finché non ci sono più utenti
  - Dopo che più utenti si sono scollegati, Autoscale spegne le macchine (ad esempio M2 o M3).
  - Anche se non ci sono più utenti, Autoscale non spegne la macchina rimanente (ad esempio M1) perché quella macchina è riservata come capacità di riserva.

> **Nota:**
>
> Per i gruppi di consegna casuali di sistemi operativi a sessione singola, tutte le modifiche al desktop vengono perse quando gli utenti si scollegano dalle sessioni. Tuttavia, se configurate, le impostazioni specifiche dell'utente vengono spostate insieme al profilo utente.

### Gruppi di consegna statici di sistemi operativi a sessione singola

Il buffer di capacità viene utilizzato per gestire i picchi improvvisi della domanda mantenendo un buffer di macchine accese non assegnate in base al numero totale di macchine non assegnate incluse nel gruppo di consegna. Per impostazione predefinita, il buffer di capacità è pari al 10% del numero totale di macchine non assegnate incluse nel gruppo di consegna.

> **Importante:**
>
> Dopo che tutte le macchine del gruppo di consegna sono state assegnate, il buffer di capacità non svolge un ruolo nell'accensione o nello spegnimento delle macchine.

Se il numero di macchine (incluso il buffer di capacità) supera il numero totale di macchine attualmente accese, altre macchine non assegnate vengono accese per soddisfare la domanda. Se il numero di macchine (incluso il buffer di capacità) è inferiore al numero totale di macchine attualmente accese, le macchine in eccesso vengono spente o sospese, a seconda delle azioni configurate.

Per i gruppi di consegna statici di sistemi operativi a sessione singola, Autoscale:

- Accende le macchine assegnate durante le ore di punta e si spegne durante le ore non di punta solo quando la proprietà `AutomaticPowerOnForAssigned` del gruppo di consegna di sistemi operativi a sessione singola applicabile è impostata su true.
- Accende automaticamente una macchina nelle ore di punta se è spenta e la proprietà `AutomaticPowerOnForAssignedDuringPeak` del gruppo di consegna a cui appartiene è impostata su true.

Per capire come funziona il buffer di capacità con le macchine assegnate, considerare quanto segue:

- Il buffer di capacità funziona solo quando il gruppo di consegna ha una o più macchine non assegnate.
- Se il gruppo di consegna non ha macchine non assegnate (tutte le macchine nel gruppo di consegna sono state assegnate), il buffer di capacità non svolge un ruolo nell'accensione o nello spegnimento delle macchine.
- La proprietà `AutomaticPowerOnForAssignedDuringPeak` determina se le macchine assegnate vengono accese durante le ore di punta. Se è impostato su true, Autoscale mantiene le macchine accese durante le ore di punta. Autoscale le accende anche se sono spente.

#### Esempio di scenario

Supponiamo di avere il seguente scenario:

- **Configurazione del gruppo di consegna**. Il gruppo di consegna la cui alimentazione si desidera venga gestita da Autoscale contiene 10 macchine (da M1 a M10).
- **Configurazione di Autoscale**
  - Le macchine da M1 a M3 sono assegnate e le macchine da M4 a M10 non sono assegnate.
  - Buffer di capacità impostato al 10% per le ore di punta e non di punta.
  - Secondo il programma selezionato, l'alimentazione Autoscale gestisce le macchine tra le 09:00 e le 18:00.

Vedere sotto per i dettagli di come funziona Autoscale nello scenario di cui sopra.

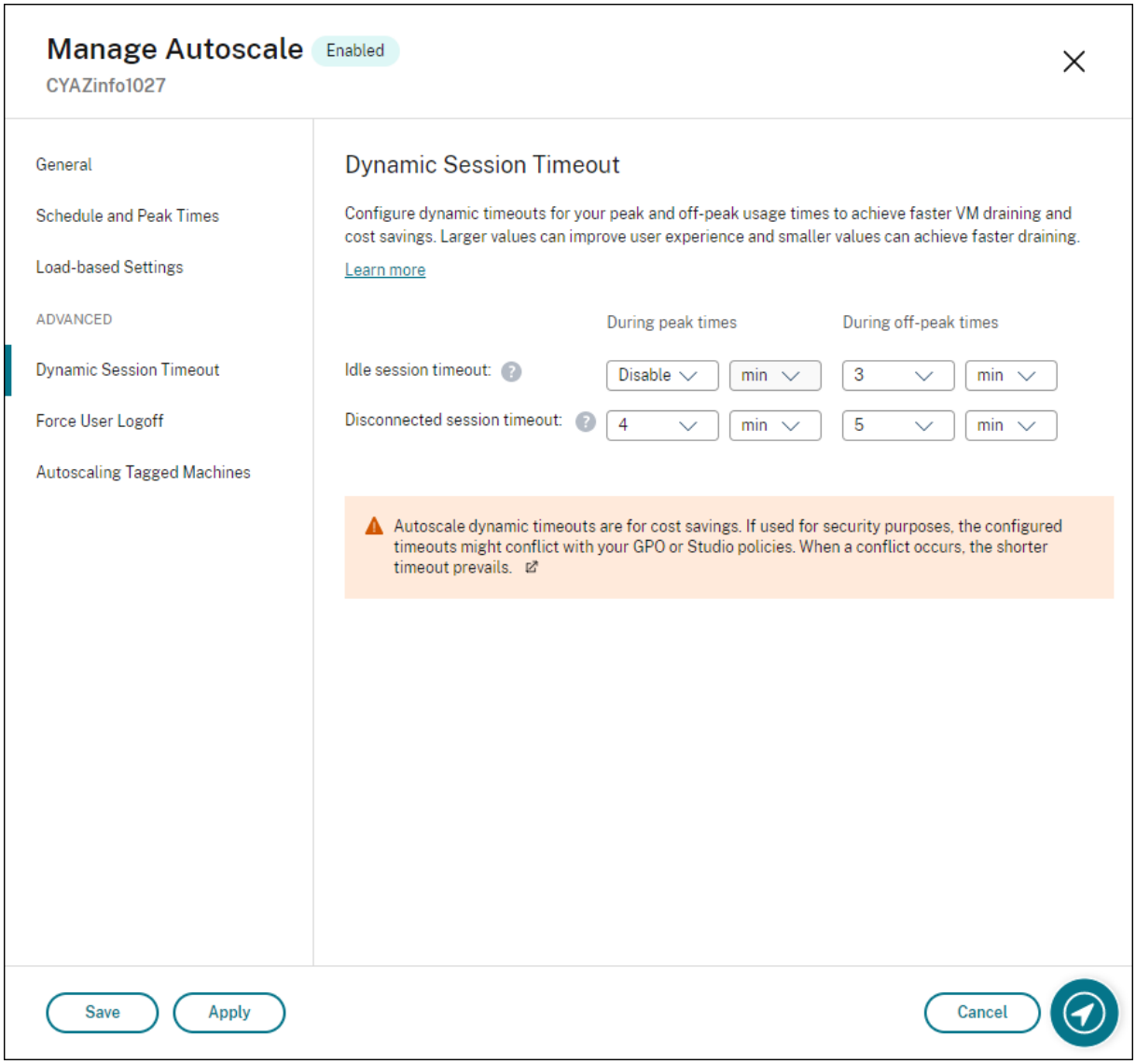
- Inizio del programma —09:00
  - Autoscale accende le macchine da M1 a M3.
  - Autoscale accende una macchina aggiuntiva (ad esempio M4) a causa del buffer di capacità configurato. La macchina M4 non è assegnata.
- Un primo utente esegue l'accesso
  - La prima volta che un utente esegue l'accesso per utilizzare un desktop, gli viene assegnato un desktop che fa parte di un pool di desktop ospitati su macchine accese non assegnate. In questo caso, all'utente viene assegnato un desktop proveniente dalla macchina M4. Gli accessi successivi di tale utente si connettono allo stesso desktop assegnato al primo utilizzo.
  - Autoscale inizia ad accendere una macchina aggiuntiva (ad esempio M5) per soddisfare la domanda a causa del buffer di capacità configurato.
- Un secondo utente esegue l'accesso
  - All'utente viene assegnato un desktop proveniente dalle macchine accese non assegnate. In questo caso, all'utente viene assegnato un desktop proveniente dalla macchina M5. Gli accessi successivi di tale utente si connettono allo stesso desktop assegnato al primo utilizzo.
  - Autoscale inizia ad accendere una macchina aggiuntiva (ad esempio M6) per soddisfare la domanda a causa del buffer di capacità configurato.
- Gli utenti si scollegano
  - Quando gli utenti si scollegano dai propri desktop o questi vanno in timeout, Autoscale mantiene accese le macchine da M1 a M5 nel periodo fra le 09:00 le 18:00. Quando questi utenti eseguono l'accesso la volta successiva, si connettono allo stesso desktop assegnato al primo utilizzo.
  - La macchina non assegnata M6 è in attesa di servire un desktop a un utente non assegnato in arrivo.
- Fine della pianificazione: 18:00
  - Alle 18:00, Autoscale spegne le macchine da M1 a M5.
  - Autoscale mantiene accesa la macchina non assegnata M6 a causa del buffer di capacità configurato. Quella macchina è in attesa di servire un desktop a un utente non assegnato in arrivo.
  - Nel gruppo di consegna, le macchine da M6 a M10 sono macchine non assegnate.

# Timeout dinamici delle sessioni

January 7, 2024

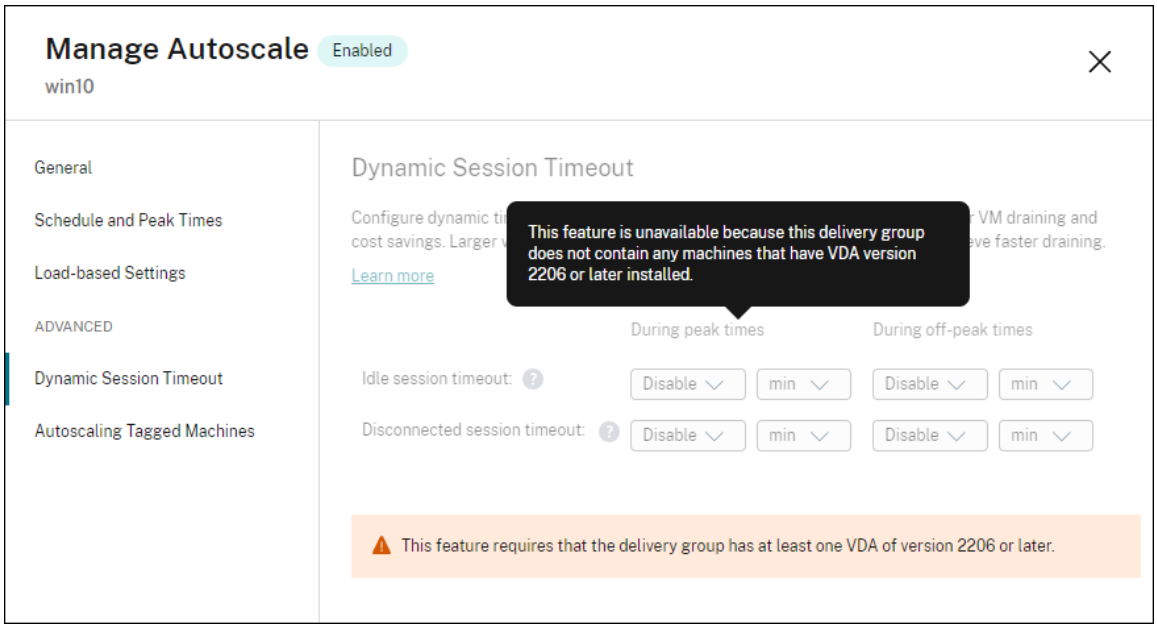
Questa funzione consente di configurare timeout di sessione disconnessa e inattiva per le ore di utilizzo di punta e non di punta per ottenere uno svuotamento della macchina più rapido e risparmi sui costi. Questa funzionalità si applica alle macchine con sistema operativo a sessione singola e multisessione. Un VDA segnala i tempi di inattività per le sessioni che sono rimaste inattive per più di 10 minuti, quindi i timeout dinamici delle sessioni non saranno in grado di disconnettere le sessioni inattive prima di 10 minuti di inattività. Un valore inferiore rimuove prima le sessioni persistenti, riducendo così i costi.



**Nota:**

- Questa funzionalità è sempre disponibile per i gruppi di consegna con sistema operativo multisessione.
- Per i gruppi di consegna di sistemi operativi a sessione singola, questa funzionalità si applica ai VDA della versione 2206 CR o successiva o 2203 LTSR CU3 o successiva. Verificare che i VDA siano stati registrati su Citrix Cloud almeno una volta. Quando non è disponibile, viene visualizzata la seguente interfaccia utente:




(Timeout dinamico della sessione non disponibile)

- I timeout dinamici di Autoscale consentono di risparmiare sui costi. Se utilizzati per scopi di sicurezza, i timeout configurati potrebbero entrare in conflitto con l'oggetto Criteri di gruppo o i criteri della console Manage. Quando si verifica un conflitto, prevale il timeout più breve.

**Timeout della sessione inattiva**. Abilita o disabilita un timer che specifica per quanto tempo viene mantenuta ininterrotta una connessione utente in assenza di input da parte dell'utente. Quando il timer scade, la sessione viene posizionata nello stato disconnesso e si applica il **Disconnected session timeout** (Tempo di scadenza di una sessione disconnessa). Se l'opzione **Disconnected session timeout** è disabilitata, la sessione non viene disconnessa.

**Importante:**

- Se si specifica un valore inferiore o uguale a 10 minuti (600 secondi), Autoscale disconnette le sessioni pertinenti dopo che sono rimaste inattive per 10 minuti. Questo perché Autoscale si basa sui tempi di inattività delle sessioni riportati dai VDA. I VDA segnalano i

> tempi di inattività solo per le sessioni che sono rimaste inattive per più di 10 minuti.
> - Una sessione inattiva verrà comunque messa in uno stato di disconnessione se l'utente interagisce con essa negli ultimi 5 minuti dal raggiungimento del timeout della sessione inattiva.

**Disconnected session timeout**. Abilita o disabilita un timer che specifica per quanto tempo un desktop disconnesso debba rimanere bloccato prima che la sessione venga terminata. Se è abilitato, la sessione disconnessa viene terminata alla scadenza del timer.

## Scalabilità automatica delle macchine con tag (cloud burst)

January 7, 2024

> **Nota:**
>
> Questa funzionalità in precedenza era chiamata Restrict Autoscale (Limita Autoscale).

### Introduzione

Autoscale offre la flessibilità necessaria per gestire solo un sottoinsieme di macchine di un gruppo di consegna. Per raggiungere questo obiettivo, applicare un tag a una o più macchine e quindi configurare Autoscale per gestire solo le macchine con tag.

Questa funzione può essere utile nei casi d'uso del cloud bursting, in cui si desidera utilizzare risorse locali (o istanze di cloud pubblico riservate) per gestire i carichi di lavoro prima che le risorse basate sul cloud soddisfino la domanda aggiuntiva (ovvero carichi di lavoro burst). Per consentire alle macchine locali (o alle istanze riservate) di affrontare prima i carichi di lavoro, è necessario utilizzare la restrizione tag insieme alla preferenza di zona.

La restrizione tag specifica che le macchine devono avere l'alimentazione gestita da Autoscale. La preferenza di zona specifica i computer presenti nella zona preferita che gestiscono le richieste di avvio degli utenti. Per maggiori informazioni, vedere Tag e Preferenza di zona.

Per la scalabilità automatica di determinate macchine con tag, è possibile utilizzare la console Manage (Gestione) o PowerShell.

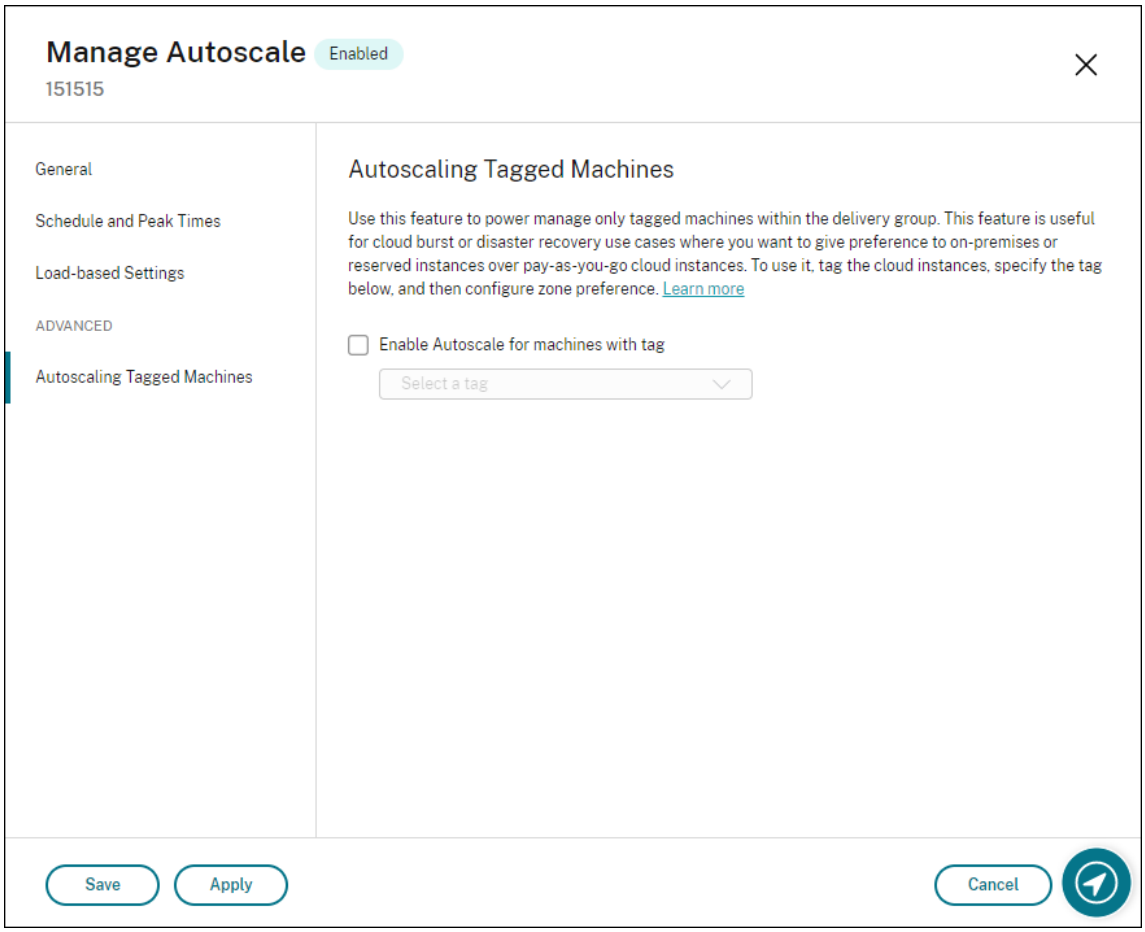
### Utilizzare la console Manage (Gestione) per scalare automaticamente determinate macchine con tag

Per scalare automaticamente alcune macchine con tag, completare i seguenti passaggi:

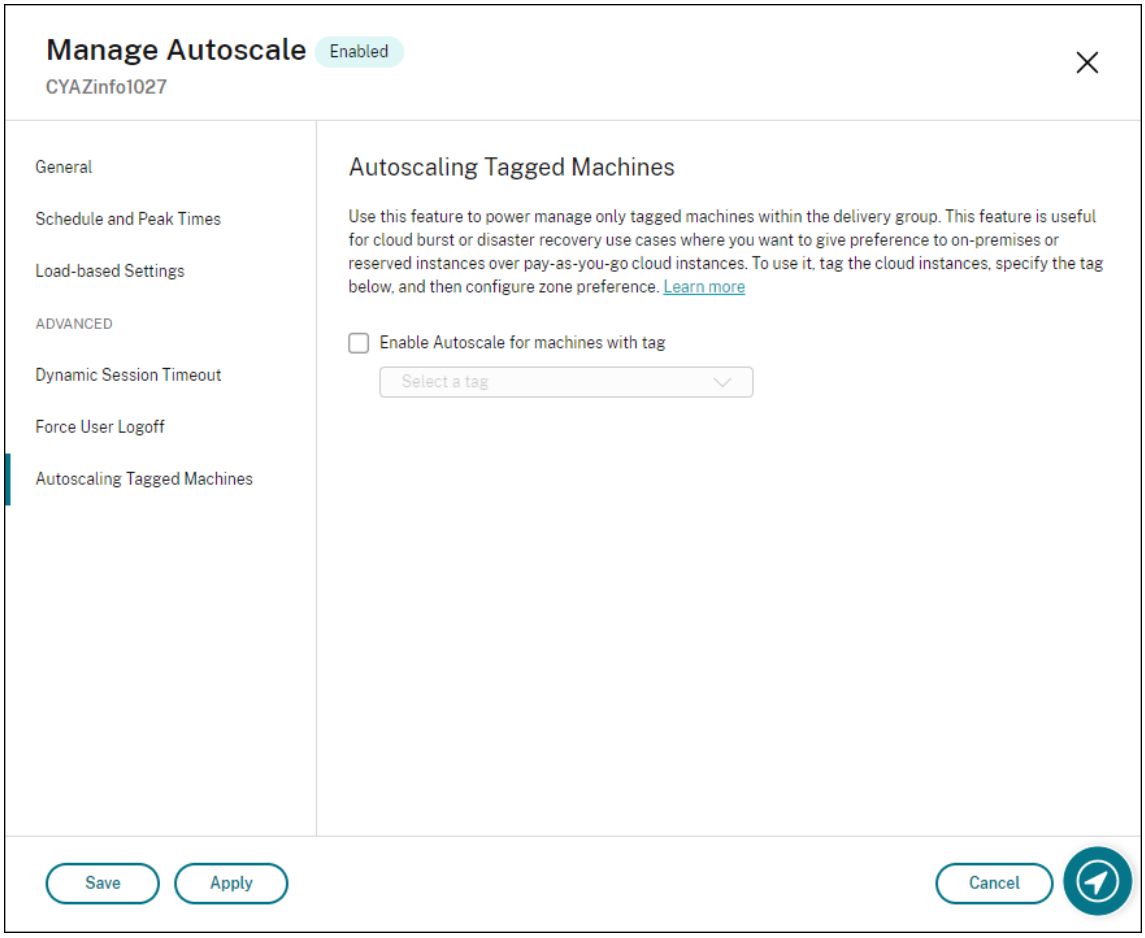
1. Creare un tag e applicarlo alle macchine pertinenti del gruppo di consegna. Per maggiori informazioni, vedere Gestire i tag e le restrizioni tag.
2. Selezionare il gruppo di consegna e quindi aprire la procedura guidata **Manage Autoscale**.
3. Nella pagina **Autoscaling Tagged Machines** (Scalabilità automatica delle macchine con tag), selezionare **Enable Autoscale for machines with tag** (Abilita Autoscale per le macchine con tag), selezionare un tag dall'elenco, quindi fare clic su **Apply** (Applica) per salvare le modifiche.

   Interfaccia utente per gruppi di consegna *statici* e *casuali* dei sistemi operativi a sessione singola:




   Interfaccia utente per *gruppi di consegna di sistemi operativi multisessione*:




**Avviso:**

- La scalabilità automatica delle macchine con un tag specifico potrebbe causare l'aggiornamento automatico dell'istogramma per riflettere il numero di macchine in base al tag. Nella pagina **Schedule and Peak Times** (Pianificazione e orari di punta), è possibile assegnare manualmente le macchine rispetto a ogni fascia oraria, se necessario.
- Non è possibile eliminare un tag che viene utilizzato sulle macchine con tag. Per eliminare il tag, è necessario prima rimuovere la limitazione tag.

Dopo aver applicato la limitazione tag, in un secondo momento si potrebbe decidere di rimuoverla dal gruppo di consegna. A tale scopo, andare alla pagina **Manage Autoscale > Autoscaling Tagged Machines** (Gestisci scalabilità automatica > Scalabilità automatica macchine con tag) e quindi deselezionare **Enable Autoscale for machines with tag** (Abilita Autoscale per macchine con tag).

**Avviso:**

- Se si rimuove il tag dalle macchine interessate senza deselezionare **Enable Autoscale for machines with tag** (Abilita Autoscale per macchine con tag), si potrebbe ricevere un avviso

> quando si apre la procedura guidata **Manage Autoscale** (Gestici Autoscale). Rimuovendo i tag dalle macchine, potrebbero non rimanere macchine da gestire con Autoscale perché il tag specificato in Autoscale è diventato non valido. Per risolvere l'avviso, andare alla pagina **Autoscaling Tagged Machines** (Scalabilità automatica delle macchine con tag), rimuovere il tag non valido, quindi fare clic su **Apply** (Applica) per salvare le modifiche.

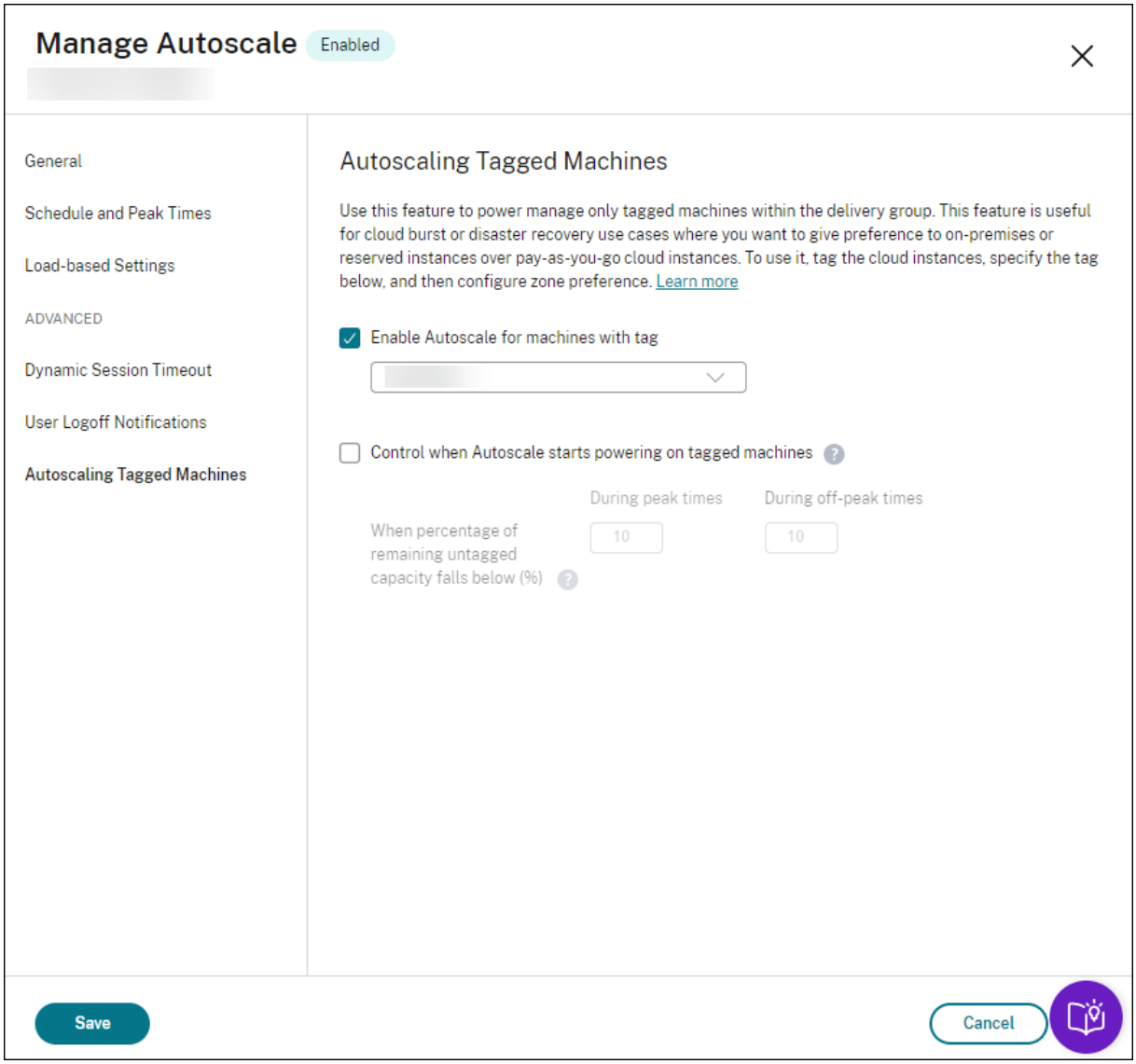
#### Controllare quando Autoscale attiva le risorse

È anche possibile controllare quando Autoscale inizia ad attivare le macchine con tag in base all'utilizzo di macchine senza tag. Ciò consente di ottimizzare ulteriormente il consumo dei carichi di lavoro del cloud pubblico o con tag.

A tale scopo, completare i seguenti passaggi:

1. Nella pagina **Autoscaling Tagged Machines** (Scalabilità automatica delle macchine con tag), selezionare **Control when Autoscale starts powering on tagged machines** (Controlla quando Autoscale inizia ad attivare le macchine con tag).
2. Immettere la quantità percentuale di utilizzo delle macchine senza tag che si desidera raggiungere sia per le ore di punta che per le ore non di punta, quindi fare clic su **Apply** (Applica). Valori supportati: 0-100.




(Controlla quando Autoscale inizia ad attivare le macchine con tag)

> **Suggerimento:**
>
> La percentuale controlla quando Autoscale inizia ad accendere i computer con tag. Quando la percentuale scende al di sotto della soglia (impostazione predefinita 10%), Autoscale inizia ad accendere i computer con tag. Quando la percentuale supera la soglia, Autoscale passa alla modalità di spegnimento. Quando si inserisce la percentuale, considerare due scenari:
>
> - Per gruppi di consegna con sistema operativo a sessione singola: il valore è definito come percentuale del numero totale di macchine senza tag in stato di inattività. Esempio: ci sono 10 macchine con sistema operativo a sessione singola senza tag. Quando ne rimane solo una senza sessione, Autoscale avvia l'accensione di una macchina con tag.
> - Per i gruppi di distribuzione con sistema operativo multisessione: il valore è definito come

> percentuale della capacità totale (in termini di indice di carico) delle macchine senza tag disponibili. Esempio: ci sono 10 macchine con sistema operativo multisessione senza tag. Quando sono caricate al 90%, Autoscale avvia l'alimentazione di una macchina con tag.

### Utilizzare PowerShell per scalare automaticamente alcune macchine con tag

Per utilizzare direttamente l'SDK di PowerShell, completare i seguenti passaggi:

1. **Creare un tag.** Utilizzare il comando PowerShell New-Brokertag per creare un tag.
   - Ad esempio: `$managed = New-BrokerTag Managed`. In questo caso, il tag è denominato "Managed". Per ulteriori informazioni sul comando PowerShell New-Brokertag, vedere https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/.
2. **Applicare il tag alle macchine**. Utilizzare il comando PowerShell Get-Brokermachine per applicare il tag alle macchine di un catalogo da sottoporre alla gestione dell'alimentazione con Autoscale.
   - Ad esempio: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`. In questo caso, il catalogo è denominato "cloud".
   - Per ulteriori informazioni sul comando PowerShell Get-Brokermachine, vedere https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/.

   > **Nota:**
   >
   > È possibile aggiungere nuove macchine al catalogo dopo aver applicato il tag. Il tag *NON* viene applicato automaticamente a quelle nuove macchine.

3. **Aggiungere macchine con tag al gruppo di consegna da sottoporre alla gestione dell'alimentazione con Autoscale.** Utilizzare il comando PowerShell Get-BrokerDesktopGroup per aggiungere una restrizione tag al gruppo di consegna che contiene le macchine (in altre parole, "limitare i lanci alle macchine con tag X").
   - Ad esempio: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. In questo caso, l'UID del gruppo di consegna è 1.
   - Per ulteriori informazioni sul comando Get-BrokerDesktopGroup PowerShell, vedere https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Dopo aver applicato la limitazione tag, in un secondo momento si potrebbe decidere di rimuoverla dal gruppo di consegna. A tale scopo, utilizzare il comando PowerShell Get-BrokerDesktopGroup.

Esempio: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscal $null`. In questo caso, l'UID del gruppo di consegna è 1.

> **Nota:**
>
> I computer senza tag si riavviano automaticamente dopo che gli utenti li hanno spenti Questo comportamento garantisce che si rendano disponibili più presto per gestire i carichi di lavoro. Questo può essere abilitato o disabilitato su un gruppo per desktop utilizzando la proprietà `AutomaticRestartForUntaggedMachines` di `Set-BrokerDesktopGroup`. Per ulteriori informazioni, vedere https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

### Esempio di scenario

Supponiamo di avere il seguente scenario:

- **Configurazione del catalogo di macchine**. Esistono due cataloghi di macchine (C1 e C2).
  - Il catalogo C1 contiene 5 macchine (da M1 a M5) che sono locali nelle distribuzioni locali.
  - Il catalogo C2 contiene 5 macchine (da M6 a M10) che sono remote nelle distribuzioni cloud.
- **Restrizioni tag**. Viene creato Un tag denominato "Cloud", che viene applicato alle macchine da M6 a M10 del catalogo C2.
- **Configurazione della zona**. Vengono create due zone (Z1 e Z2).
  - La zona Z1 contenente il catalogo C1 corrisponde alle distribuzioni locali.
  - La zona Z2 contenente il catalogo C2 corrisponde alle distribuzioni cloud.
- **Configurazione del gruppo di consegna**
  - Il gruppo di consegna contiene 10 macchine (da M1 a M10), 5 macchine dei cataloghi C1 (da M1 a M5) e 5 del catalogo C2 (da M6 a M10).
  - Le macchine da M1 a M5 vengono accese manualmente e rimangono accese per tutta la durata della programmazione.
- **Configurazione di Autoscale**
  - Il buffer di capacità è impostato al 10%.
  - Autoscale gestisce l'alimentazione delle sole macchine con il tag "Cloud". In questo caso, Autoscale gestisce l'alimentazione delle macchine cloud da M6 a M10.
- **Configurazione dell'applicazione o del desktop pubblicati**. Le preferenze di zona sono configurate per i desktop pubblicati (ad esempio), dove la Zona Z1 è preferita rispetto alla Zona Z2 per una richiesta di avvio dell'utente.

  - La zona Z1 è configurata come zona preferita (zona home) per i desktop pubblicati.

Lo scenario viene eseguito nella seguente sequenza:

1. Nessun utente effettua l'accesso.
2. Le sessioni utente aumentano.
3. Le sessioni utente aumentano ulteriormente fino a quando non vengono consumate tutte le macchine locali disponibili.
4. Vengono avviate altre sessioni utente.
5. La sessione utente diminuisce a causa della chiusura della sessione.
6. La sessione utente diminuisce ulteriormente fino a quando il carico della sessione non viene gestito solo da macchine locali.

Vedere sotto per i dettagli di come funziona Autoscale nello scenario di cui sopra.

- Nessun carico utente (stato iniziale)
  - Le macchine locali da M1 a M5 sono tutte accese.
  - Una macchina del cloud (ad esempio M6) viene accesa. La macchina viene accesa a causa del buffer di capacità configurato. In questo caso, 10 (numero di macchine) x 10.000 (indice di carico) x 10% (buffer di capacità configurato) equivale a 10.000. Pertanto, viene accesa una macchina.
  - Il valore dell'indice di carico di tutte le macchine accese (da M1 a M6) è a un carico di base (l'indice di carico è uguale a 0).
- Gli utenti effettuano l'accesso
  - Le sessioni sono indirizzate a essere ospitate su macchine da M1 a M5 tramite la preferenza di zona configurata e sono bilanciate dal carico su queste macchine locali.
  - Il valore dell'indice di carico delle macchine accese (da M1 a M5) aumenta.
  - Il valore dell'indice di carico della macchina accesa M6 è a un carico di base.
- Gli utenti aumentano il carico, consumando tutte le risorse locali
  - Le sessioni sono indirizzate a essere ospitate sulle macchine da M1 a M5 tramite la preferenza di zona configurata e il loro carico viene distribuito in modo equilibrato su queste macchine locali.
  - Il valore dell'indice di carico di tutte le macchine accese (da M1 a M5) ha raggiunto 10.000.
  - Il valore dell'indice di carico della macchina accesa M6 rimane a un carico di base.
- Un altro utente accede
  - La sessione supera la preferenza di zona e viene indirizzata a essere ospitata sulla macchina cloud M6.
  - Il valore dell'indice di carico di tutte le macchine accese (da M1 a M5) ha raggiunto 10.000.

  - Il valore dell'indice di carico della macchina accesa M6 aumenta e non è più a un carico di base. Quando la capacità di riserva totale scende a un livello inferiore a 10.000 in termini di indice di carico, Autoscale inizia ad accendere una macchina aggiuntiva (M7) per soddisfare la domanda, dato il buffer di capacità configurato. Si noti che potrebbe essere necessario del tempo per accendere la macchina M7. Quindi potrebbe esserci un ritardo fino a quando la macchina M7 non sarà pronta.

- Accedono altri utenti
  - Le sessioni vengono indirizzate a essere ospitate sulla macchina M6.
  - Il valore dell'indice di carico di tutte le macchine accese (da M1 a M5) ha raggiunto 10.000.
  - Il valore dell'indice di carico della macchina accesa M6 aumenta ulteriormente, ma la capacità di riserva totale è a un livello superiore a 10.000 in termini di indice di carico.
  - Il valore dell'indice di carico della macchina accesa M7 rimane a un carico di base.

- Accedono ancora più utenti
  - Dopo che la macchina M7 è pronta, le sessioni vengono indirizzate a essere ospitate sulle macchine M6 e M7 e il carico viene distribuito fra queste macchine.
  - Il valore dell'indice di carico di tutte le macchine accese (da M1 a M5) ha raggiunto 10.000.
  - Il valore dell'indice di carico della macchina M7 non è più a un carico di base.
  - Il valore dell'indice di carico delle macchine accese (M6 e M7) aumenta.
  - La capacità di riserva totale è ancora a un livello superiore a 10.000 in termini di indice di carico.

- Il carico della sessione utente diminuisce a causa della chiusura della sessione
  - Dopo che gli utenti si sono disconnessi dalle sessioni o dopo il timeout delle sessioni inattive, la capacità che si è liberata sulle macchine da M1 a M7 viene riutilizzata per ospitare sessioni avviate da altri utenti.
  - Quando la capacità di riserva totale aumenta fino a un livello superiore a 10.000 in termini di indice di carico, Autoscale mette una delle macchine cloud (da M6 a M7) in stato di svuotamento. Di conseguenza, le sessioni avviate da altri utenti non vengono più indirizzate a quella macchina (ad esempio M7) a meno che non vi siano nuovi cambiamenti; ad esempio se il carico dell'utente aumenta nuovamente o altre macchine cloud hanno un carico inferiore.

- Il carico della sessione utente diminuisce ulteriormente fino a quando una o più macchine cloud non sono più necessarie
  - Dopo che tutte le sessioni sulla macchina M7 sono terminate e il ritardo di spegnimento specificato è scaduto, Autoscale spegne la macchina M7.
  - Il valore dell'indice di carico di tutte le macchine accese (da M1 a M5) potrebbe scendere a un livello inferiore a 10.000.

  - Il valore dell'indice di carico della macchina accesa (M6) diminuisce.

- La sessione utente diminuisce ulteriormente fino a quando non sono necessarie macchine cloud.
  - Anche se non ci sono sessioni utente sulla macchina M6, Autoscale non la spegne perché è riservata come capacità di riserva.
  - Autoscale mantiene accesa la rimanente macchina cloud M6 dato il buffer di capacità configurato. Quella macchina è in attesa di servire un desktop a un utente in arrivo.
  - Le sessioni non sono indirizzate a essere ospitate sulla macchina M6 fintanto che le macchine locali hanno capacità disponibile.

## Notifiche di disconnessione dell'utente (in precedenza scollegamento forzato dell'utente)

January 7, 2024

> **Importante:**
>
> Questa funzionalità è disponibile solo nell'interfaccia utente di Autoscale per gruppi di consegna basati su app multisessione.

Per ottenere risparmi sui costi, Autoscale consente di forzare lo scollegamento dalle sessioni persistenti consentendo di inviare una notifica personalizzata agli utenti e specificare un periodo di prova dopo il quale le sessioni vengono disconnesse forzatamente. Questo viene fatto solo per le macchine in modalità di svuotamento e non per tutte le macchine accese. Per evitare potenziali perdite di dati causate dalla forzatura degli scollegamenti degli utenti, è possibile configurare questa funzionalità in modo che invii solo promemoria di scollegamento senza forzare lo scollegamento degli utenti.

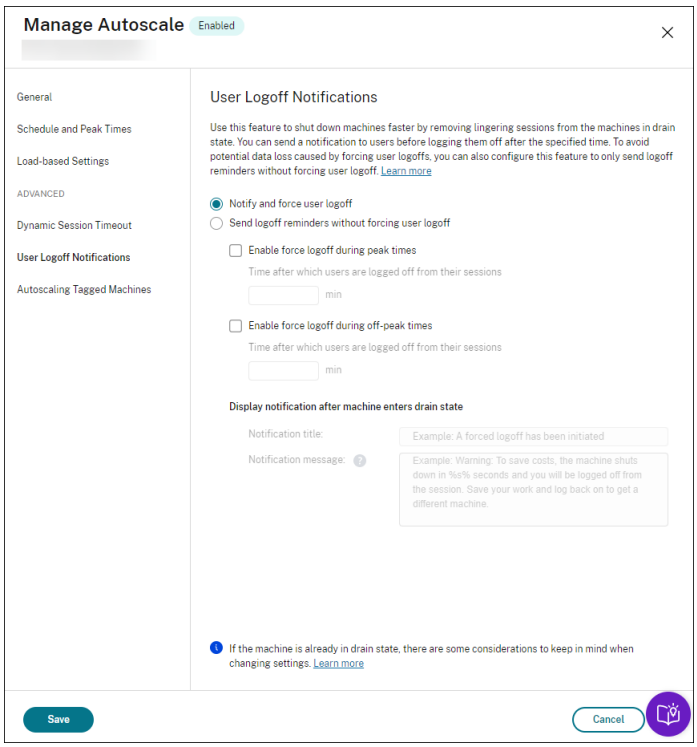
Sono disponibili le due opzioni seguenti:

- **Notify and force user logoff (Invia notifiche e forzare lo scollegamento degli utenti)**
- **Send logoff reminders without forcing user logoff (Invia promemoria di scollegamento senza forzare la disconnessione degli utenti)**

### Notify and force user logoff (Invia notifiche e forzare lo scollegamento degli utenti)

Se questa opzione è selezionata, Autoscale disconnette gli utenti dalle loro sessioni dopo gli orari specificati di seguito.




**Enable force logoff during peak times** (Abilita lo scollegamento forzato durante le ore di punta). Se questa opzione è selezionata, Autoscale scollega quegli utenti dalle loro sessioni durante le ore di punta allo scadere del tempo specificato.

**Enable force logoff during off-peak times** (Abilita lo scollegamento forzato durante le ore non di punta). Se questa opzione è selezionata, Autoscale scollega quegli utenti dalle loro sessioni durante le ore non di punta allo scadere del tempo specificato.

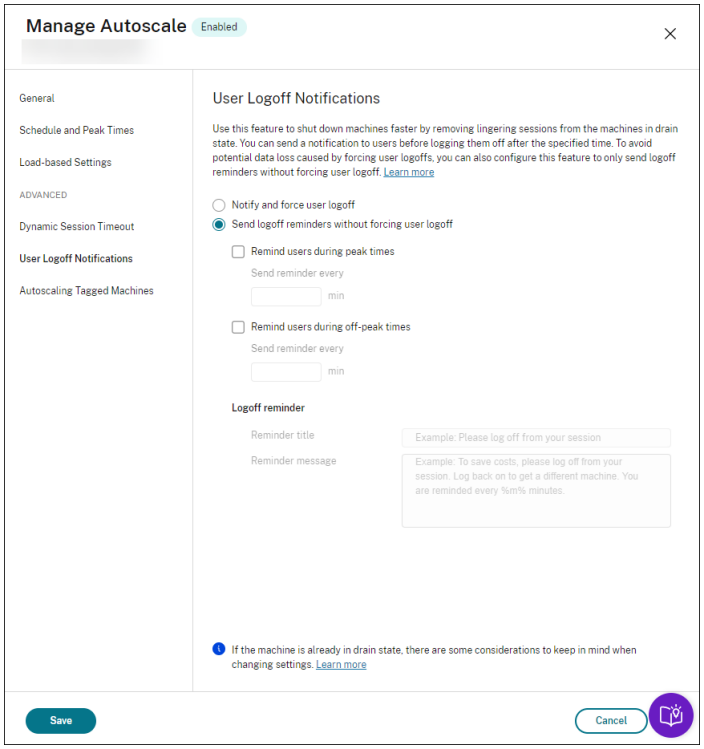
**Display notification after machine enters drain state** (Visualizza notifiche dopo che la macchina entra nello stato di svuotamento) Consente di inviare notifiche agli utenti dopo che la macchina entra in stato di svuotamento.

- **Notification title** (Titolo notifica). Consente di specificare un titolo della notifica da inviare agli utenti. Esempio: `A forced logoff has been initiated.`
- **Notification message** (Messaggio di notifica). Consente di specificare il contenuto della notifica da inviare agli utenti. È possibile utilizzare %s% o %m% come variabili per indicare l'ora specificata nel messaggio. Per esprimere il tempo in secondi, utilizzare %s%. Per esprimere il tempo in minuti, utilizzare %m%. Esempio: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`

### Send logoff reminders without forcing user logoff (Invia promemoria di scollegamento senza forzare la disconnessione degli utenti)

Se questa opzione è selezionata, gli utenti riceveranno un promemoria per scollegarsi dalla propria macchina dopo che è entrata nello stato di svuotamento. Questo promemoria può essere configurato per essere inviato all'intervallo specificato di seguito.




**Remind users during peak times** (Avvisa gli utenti durante le ore di punta). Se questa opzione è selezionata, gli utenti ricevono un promemoria per scollegarsi dalle proprie sessioni durante le ore di punta ogni X minuti (X indica il tempo specificato).

**Remind users during off-peak times** (Avvisa gli utenti durante le ore non di punta). Se questa opzione è selezionata, gli utenti ricevono un promemoria per scollegarsi dalle proprie sessioni durante le ore non di punta ogni X minuti (X indica il tempo specificato).

**Logoff reminder** (Promemoria di scollegamento). Consente di configurare il promemoria inviato agli utenti dopo che la loro macchina è entrata in stato di svuotamento.

- **Reminder title** (Titolo del promemoria). Consente di specificare un titolo per il promemoria da inviare agli utenti. Esempio: `Please log off from your session`.
- **Reminder message** (Messaggio di promemoria). Consente di specificare un messaggio da inviare agli utenti. Esempio: `Please log off from your session and log back on to save costs`.

### Considerazioni

Se la macchina è già in stato di svuotamento, considerare quanto segue quando si modificano le impostazioni:

- Se si modifica l'impostazione da **Send logoff reminders without forcing user logoff** (Invia promemoria di scollegamento senza forzare la disconnessione degli utenti) a **Notify and force user logoff** (Invia notifiche e forza lo scollegamento degli utenti), la nuova impostazione ha effetto immediato.
- Se si modifica l'impostazione da **Notify and force user logoff** (Invia notifica e forza lo scollegamento degli utenti) a **Send logoff reminders without forcing user logoff** (Invia promemoria di scollegamento senza forzare la disconnessione degli utenti), la nuova impostazione non avrà effetto fino alla volta successiva in cui la macchina entra in stato di svuotamento. L'utente è comunque costretto a scollegarsi.

## Comandi dell'SDK Broker PowerShell

January 7, 2024

È possibile configurare Autoscale per i gruppi di consegna utilizzando l'SDK Broker PowerShell. Per configurare Autoscale utilizzando i comandi di PowerShell, è necessario utilizzare l'SDK PowerShell versione 7.21.0.12 o successiva. Per ulteriori informazioni sulle SDK PowerShell, vedere SDK e API.

### Set-BrokerDesktopGroup

Disabilita o abilita un BrokerDesktopGroup esistente o ne modifica le impostazioni. Per ulteriori informazioni su questo cmdlet, vedere https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

#### Esempi

Per ulteriori informazioni su come utilizzare i cmdlet PowerShell per reimpostare un profilo, vedere gli esempi seguenti:

Abilitare Autoscale

- Supponiamo di voler abilitare Autoscale per il gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-AutoscalingEnabled
  $true
```

Configurare il buffer di capacità separatamente per le ore di punta e non di punta

- Si supponga di voler impostare il buffer di capacità al 20% per le ore di punta e al 10% per le ore non di punta per un gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakBufferSizePercent
  20 -OffPeakBufferSizePercent 10
```

Configurare l'impostazione del **timeout alla disconnessione**

- Si supponga di voler impostare il valore del **timeout alla disconnessione** su 60 minuti per le ore di punta e 30 minuti per le ore non di punta per un gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakDisconnectTimeout
  60 -OffPeakDisconnectTimeout 30
```

Configurare l'impostazione del **timeout allo scollegamento**

- Si supponga di voler impostare il valore del **timeout allo scollegamento** su 60 minuti per le ore di punta e 30 minuti per le ore non di punta per un gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakLogOffTimeout
  60 -OffPeakLogOffTimeout 30
```

Configurare l'impostazione del **ritardo di spegnimento**

- Supponiamo di voler impostare il ritardo di spegnimento su 15 minuti per un gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PowerOffDelay 15
```

Configurare un periodo di tempo durante il quale il ritardo di spegnimento non ha effetto

- Supponiamo che si voglia che il ritardo di spegnimento non abbia effetto finché non sono passati 30 minuti per un gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

```
- C:\PS> Set-BrokerDesktopGroup "MyDesktop"-SettlementPeriodBeforeAutoSh
  30.
```

Configurare il **costo dell'istanza della macchina**

- Supponiamo di voler impostare il costo orario dell'istanza della macchina a 0,2 dollari per un gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop"-MachineCost 0.2`

### New-BrokerPowerTimeScheme

Crea un BrokerPowerTimeScheme per un gruppo di consegna. Per ulteriori informazioni, vedere https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/.

#### Esempio

Si supponga di voler creare uno schema dei tempi di accensione per un gruppo di consegna il cui valore UID è 3. Il nuovo schema copre il fine settimana, il lunedì e il martedì. La fascia oraria dalle 8:00 alle 18:30 è definita come ora di punta per i giorni inclusi nello schema. Per le ore di punta, la dimensione del pool (il numero di macchine mantenute accese) è 20. Per le ore non di punta è 5. È possibile utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week'-DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

### Parametri per i timeout dinamici delle sessioni

I seguenti cmdlet Broker PowerShell SDK sono stati estesi per i timeout dinamici delle sessioni supportando svariati nuovi parametri:

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

Tali parametri comprendono:

- **DisconnectPeakIdleSessionAfterSeconds**: rappresenta il tempo in secondi dopo il quale una sessione inattiva viene disconnessa durante le ore di punta. Questa proprietà ha un valore predefinito pari a 0, che indica la disattivazione del comportamento a essa associato durante le ore

di punta. Un valore maggiore di 0 consente il comportamento associato al gruppo di consegna solo nelle ore di punta.

- **DisconnectOffPeakIdleSessionAfterSeconds**: rappresenta il tempo in secondi dopo il quale una sessione inattiva viene disconnessa durante le ore non di punta. Il valore predefinito di questa proprietà è 0, che indica la disattivazione del comportamento a essa associato durante le ore non di punta. Un valore maggiore di 0 abilita il comportamento associato al gruppo di consegna solo nelle ore non di punta.
- **LogoffPeakDisconnectedSessionAfterSeconds**: rappresenta il tempo in secondi dopo il quale una sessione disconnessa viene terminata durante le ore di punta. Il valore predefinito di questa proprietà è 0, che indica la disattivazione del comportamento a essa associato durante le ore di punta. Un valore maggiore di 0 abilita il comportamento associato al gruppo di consegna solo nelle ore di punta.
- **LogoffOffPeakDisconnectedSessionAfterSeconds**: rappresenta il tempo in secondi dopo il quale una sessione disconnessa viene terminata durante le ore non di punta. Il valore predefinito di questa proprietà è 0, che indica la disattivazione del comportamento a essa associato durante le ore non di punta. Un valore maggiore di 0 abilita il comportamento associato al gruppo di consegna solo nelle ore non di punta.

#### Esempio

Supponiamo di voler impostare il timeout della sessione di inattività a 3.600 secondi durante le ore di punta per un gruppo di consegna il cui nome è "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop"-DisconnectOffPeakIdleSessionAfte`
  `3600`

In questo modo si disconnettono le sessioni che sono rimaste inattive per più di 1 ora nelle ore non di punta per il gruppo desktop il cui nome è "MyDesktop".

## Citrix Insight Services

January 7, 2024

Citrix Insight Services (CIS) è una piattaforma Citrix per la strumentazione, la telemetria e la generazione di informazioni aziendali. Le sue capacità di strumentazione e telemetria consentono agli utenti tecnici (clienti, partner e ingegneri) di autodiagnosticare e risolvere i problemi e ottimizzare

i loro ambienti. Per i dettagli e le informazioni più recenti su CIS e su come funziona, vedere https://cis.citrix.com (sono richieste le credenziali dell'account Citrix).

Tutte le informazioni caricate su Citrix vengono utilizzate per scopi diagnostici e di risoluzione dei problemi e per migliorare la qualità, l'affidabilità e le prestazioni dei prodotti, in conformità con:

- Criteri di Citrix Insight Services disponibile all'indirizzo https://cis.citrix.com/legal
- Informativa sulla privacy di Citrix disponibile all'indirizzo https://www.citrix.com/about/legal/privacy.html

Questa versione di Citrix Virtual Apps and Desktops supporta le seguenti tecnologie.

- Analisi di installazione e aggiornamento di Citrix Virtual Apps and Desktops
- Programma di miglioramento dell'esperienza del cliente Citrix (CEIP)
- Citrix Call Home
- Citrix Scout

Oltre a CIS e Citrix Analytics (e a parte): i dati Google Analytics vengono raccolti (e in seguito caricati) automaticamente quando si installa (o si aggiorna) Studio. Dopo aver installato Studio, è possibile modificare questa impostazione con la chiave di registro HKLM\Software\Citrix\DesktopStudio\GAEnabled. Il valore 1 abilita la raccolta e il caricamento, il valore 0 disabilita la raccolta e il caricamento.

### Installare e aggiornare i dati analitici

Quando si utilizza il programma di installazione completo del prodotto per distribuire o aggiornare i componenti di Citrix Virtual Apps and Desktops, vengono raccolte informazioni anonime sul processo di installazione, che vengono archiviate sulla macchina in cui si sta installando/aggiornando il componente. Questi dati vengono utilizzati per aiutare Citrix a migliorare l'esperienza di installazione dei propri clienti.

Le informazioni sono archiviate localmente in %ProgramData%\Citrix\CTQs.

Il caricamento automatico di questi dati è abilitato per impostazione predefinita sia nell'interfaccia grafica che nella riga di comando del programma di installazione del prodotto completo.

- È possibile modificare il valore predefinito in un'impostazione del Registro di sistema. Se si modificano le impostazioni del Registro di sistema prima dell'installazione/aggiornamento, tale valore viene utilizzato quando si utilizza il programma di installazione del prodotto completo.
- È possibile ignorare l'impostazione predefinita se si effettua l'installazione o l'aggiornamento con l'interfaccia della riga di comando specificando un'opzione con il comando.

**Controllare i caricamenti automatici:**

- Impostazione del Registro di sistema che controlla il caricamento automatico dei dati analitici relativi a installazione/aggiornamento (impostazione predefinita= 1):
  - Posizione: HKLM:\Software\Citrix\MetaInstall
  - Nome: SendExperienceMetrics
  - Valore: 0= disabilitato, 1= abilitato
- Utilizzando PowerShell, il seguente cmdlet disabilita il caricamento automatico dei dati analitici di installazione/aggiornamento:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
    SendExperienceMetrics -PropertyType DWORD -Value 0
<!--NeedCopy-->
```

- Per disabilitare i caricamenti automatici con il comando XenDesktopServerSetup.exe o XenDesktopVDASetup.exe, includere l'opzione /`disableexperiencemetrics`.

  Per abilitare i caricamenti automatici con il comando XenDesktopServerSetup.exe o XenDesktopVDASetup.exe, includere l'opzione /`sendexperiencemetrics`.

## Programma di miglioramento dell'esperienza cliente Citrix

Quando si partecipa al Programma di miglioramento dell'esperienza cliente Citrix (CEIP), vengono inviate a Citrix statistiche anonime e informazioni sull'utilizzo per aiutare Citrix a migliorare la qualità e le prestazioni dei prodotti Citrix. Per ulteriori informazioni, visitare il sito Web all'indirizzo https://more.citrix.com/XD-CEIP.

### Registrazione durante la creazione o l'aggiornamento del sito

L'utente viene automaticamente registrato in CEIP quando crea un sito (dopo aver installato il primo Delivery Controller). Il primo caricamento dei dati avviene circa sette giorni dopo la creazione del sito.

È possibile interrompere la partecipazione in qualsiasi momento dopo aver creato il sito. Selezionare il nodo **Settings** nel riquadro sinistro di Web Studio (scheda **Supporto prodotto**) e disattivare l'impostazione del **Citrix Customer Experience Improvement Program**.

Quando si aggiorna una distribuzione di Citrix Virtual Apps and Desktops:

- Se si esegue l'aggiornamento da una versione che non supporta CEIP, viene chiesto se si desidera partecipare.
- Se si esegue l'aggiornamento da una versione che supporta CEIP e la partecipazione è stata abilitata, CEIP viene abilitato nel sito aggiornato.

- Se si esegue l'aggiornamento da una versione che supporta CEIP e la partecipazione è stata disabilitata, CEIP viene disabilitato nel sito aggiornato.
- Se si esegue l'aggiornamento da una versione che supporta CEIP e la partecipazione non è nota, viene chiesto se si desidera partecipare.

Le informazioni raccolte sono anonime, quindi non possono essere visualizzate dopo il caricamento su Citrix Insight Services.

#### Registrazione durante l'installazione di un VDA

Per impostazione predefinita, l'utente viene automaticamente registrato a CEIP quando installa un VDA di Windows. È possibile modificare questa impostazione predefinita in un'impostazione del Registro di sistema. Se si modifica l'impostazione del Registro di sistema prima di installare il VDA, viene utilizzato tale valore.

Impostazione del Registro di sistema che controlla la registrazione automatica in CEIP (impostazione predefinita= 1):

Posizione: HKLM: \Software\Citrix\Telemetry\CEIP
Nome:
Valore Enabled: 0= disabilitato, 1= abilitato

Per impostazione predefinita, la proprietà `Enabled` è nascosta nel Registro di sistema. Quando non viene specificata, la funzione di caricamento automatico è abilitata.

Utilizzando PowerShell, il seguente cmdlet disabilita la registrazione in CEIP:

```
1 New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
     Enabled -PropertyType DWORD -Value 0
2 <!--NeedCopy-->
```

I datapoint di runtime raccolti vengono periodicamente scritti come file in una cartella di output (impostazione predefinita: %programdata%/Citrix/VdaCeip).

Il primo caricamento dei dati avviene circa sette giorni dopo l'installazione del VDA.

#### Registrazione durante l'installazione di altri prodotti e componenti

È anche possibile partecipare a CEIP quando si installano prodotti, componenti e tecnologie Citrix correlati, come Citrix Provisioning, AppDNA, Citrix License Server, l'app Citrix Workspace per Windows, Universal Print Server e Session Recording. Per ulteriori informazioni sui valori predefiniti di installazione e partecipazione, vedere la relativa documentazione.

## Citrix Call Home

Quando si installano determinati componenti e funzionalità in Citrix Virtual Apps and Desktops, viene offerta l'opportunità di partecipare a Citrix Call Home. Call Home raccoglie i dati diagnostici e quindi carica periodicamente i pacchetti di telemetria contenenti tali dati direttamente su Citrix Insight Services (tramite HTTPS sulla porta predefinita 443) per l'analisi e la risoluzione dei problemi.

In Citrix Virtual Apps and Desktops, Call Home viene eseguito come servizio in background sotto il nome di Citrix Telemetry Service. Per ulteriori informazioni, visitare il sito Web all'indirizzo https://more.citrix.com/XD-CALLHOME.

La funzionalità di pianificazione di Call Home è disponibile anche in Citrix Scout. Per ulteriori informazioni, vedere Citrix Scout.

### Cosa viene raccolto

Il tracciamento di Citrix Diagnostic Facility (CDF) registra le informazioni che possono essere utili per la risoluzione dei problemi. Call Home raccoglie un sottoinsieme di tracce CDF che possono essere utili per la risoluzione dei problemi più comuni, ad esempio registrazioni VDA e avviamenti di applicazioni/desktop. Questa tecnologia è nota come tracciamento sempre attivo (AOT). I registri AOT vengono salvati sul disco nel percorso C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOT.

Call Home non raccoglie altre informazioni relative a Event Tracing for Windows (ETW), né può essere configurato per farlo.

Call Home raccoglie anche altre informazioni, come ad esempio:

- Registri creati da Citrix Virtual Apps and Desktops in `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
- Informazioni su Windows Management Instrumentation (WMI) nello spazio dei nomi Citrix.
- Elenco dei processi in esecuzione.
- Dettagli degli arresti anomali dei processi Citrix archiviati in %PROGRAM DATA%\Citrix\CDF.
- Informazioni sull'installazione e l'aggiornamento. Ciò può includere il registro completo del metainstaller del prodotto, i registri MSI non riusciti, l'output dall'analizzatore dei registri MSI, i registri di StoreFront, i registri di verifica della compatibilità delle licenze e i risultati dei test preliminari di aggiornamento del sito.

Le informazioni di tracciamento vengono compresse man mano che vengono raccolte. Il servizio di telemetria Citrix conserva un massimo di 10 MB di informazioni di tracciamento recenti compresse, con un limite di tempo massimo di otto giorni.

- La compressione dei dati consente a Call Home di mantenere un ingombro ridotto sul VDA.
- Le tracce vengono conservate in memoria per evitare gli IOP sulle macchine di cui è stato eseguito il provisioning.

- Il buffer di tracciamento utilizza un meccanismo circolare per conservare le tracce in memoria.

Call Home raccoglie i datapoint chiave elencati in Call Home key datapoints.

#### Riepilogo della configurazione e della gestione

È possibile registrarsi a Call Home quando si utilizza la procedura guidata di installazione completa del prodotto o una versione successiva, utilizzando i cmdlet di PowerShell. Al momento della registrazione, per impostazione predefinita, la diagnostica viene raccolta e caricata su Citrix ogni domenica alle 3:00 circa, ora locale. Il caricamento è effettuato in modo casuale con un intervallo di due ore dall'ora specificata. Ciò significa che si verifica un caricamento secondo la pianificazione predefinita tra le 3:00 e le 5:00.

Se non si desidera caricare informazioni di diagnostica secondo una pianificazione (o se si desidera modificarne una), è possibile utilizzare i cmdlet di PowerShell per raccogliere e caricare manualmente la diagnostica o archiviarli localmente.

Quando ci si registra per i caricamenti programmati di Call Home e si caricano manualmente le informazioni diagnostiche su Citrix, si fornisce l'account Citrix o le credenziali Citrix Cloud. Citrix scambia le credenziali con un token di caricamento utilizzato per identificare il cliente e caricare i dati. Le credenziali non vengono salvate.

Quando avviene un caricamento, viene inviata una notifica via e-mail all'indirizzo associato all'account Citrix.

Se si abilita Call Home quando si installa un componente, è possibile disattivarlo in un secondo momento.

#### Prerequisiti

- Il computer deve eseguire PowerShell 3.0 o versione successiva.
- Citrix Telemetry Service deve essere in esecuzione sul computer.
- La variabile di sistema `PSModulePath` deve essere impostata sul percorso di installazione della telemetria, ad esempio C:\Programmi\Citrix\Telemetry Service\.

#### Abilitare Call Home durante l'installazione dei componenti

**Durante l'installazione o l'aggiornamento di un VDA:** quando si installa o si aggiorna un Virtual Delivery Agent utilizzando l'interfaccia grafica del programma di installazione del prodotto completo, viene chiesto se si desidera partecipare a Call Home. Sono disponibili due opzioni:

- Participate in Call Home.

- Do not participate in Call Home.

Se si sta aggiornando un VDA e in precedenza ci si era registrati per Call Home, la pagina della procedura guidata non viene visualizzata.

**Durante l'installazione o l'aggiornamento del controller:** quando si installa o si aggiorna un Delivery Controller utilizzando l'interfaccia grafica, viene chiesto se si desidera partecipare a Call Home. Sono disponibili tre opzioni:

Quando si installa un controller, non è possibile configurare le informazioni contenute nella pagina di Call Home nella procedura guidata di installazione se tale server dispone di un oggetto Criteri di gruppo di Active Directory a cui è applicata l'impostazione dei criteri "Log on as a service". Per ulteriori informazioni, vedere CTX218094.

Se si sta aggiornando un controller e si è già registrati per Call Home, non viene chiesto se si desidera partecipare.

#### Cmdlet di PowerShell

La Guida di PowerShell fornisce la sintassi completa, incluse descrizioni di cmdlet e parametri non utilizzati in questi casi d'uso comuni.

Per utilizzare un server proxy per i caricamenti, vedere Configure a proxy server.

- **Abilitare i caricamenti pianificati:** le raccolte diagnostiche vengono caricate automaticamente su Citrix. Se non si immettono cmdlet aggiuntivi per una pianificazione personalizzata, viene utilizzata la pianificazione predefinita.

  ```
  1  $cred = Get-Credential
  2  Enable-CitrixCallHome -Credential $cred
  3  <!--NeedCopy-->
  ```

  Per confermare che i caricamenti pianificati sono abilitati, immettere `Get-CitrixCallHomeGet-CitrixCallHome`. Se sono abilitati, vengono restituiti `IsEnabled=True` e `IsMasterImage=False`.

- **Abilitare i caricamenti pianificati per le macchine create da un'immagine master:** l'abilitazione dei caricamenti pianificati in un'immagine master elimina la necessità di configurare ogni macchina creata nel catalogo macchine.

  ```
  Enable-CitrixCallHome -Credential $cred -MasterImage
  ```

  Per confermare che i caricamenti pianificati sono abilitati, immettere **Get-CitrixCallHome**. Se sono abilitati, vengono restituiti `IsEnabled=True` e `IsMasterImage=True`.

- **Creare una pianificazione personalizzata:** si crea una pianificazione giornaliera o settimanale per raccolte e caricamenti diagnostici.

```
$timespan = New-TimeSpan –Hours hours -Minutes minutes
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
    -UploadFrequency {
Daily|Weekly }

<!--NeedCopy-->
```

**Esempi:**

Il cmdlet seguente crea una pianificazione per raggruppare e caricare i dati ogni sera alle 10:20. Il parametro Hours utilizza l'orologio di 24 ore. Quando il valore del parametro `UploadFrequency` è Daily, il parametro `DayOfWeek` viene ignorato, se specificato.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
<!--NeedCopy-->
```

Per confermare la pianificazione, immettere `Get-CitrixCallHomeSchedule`. Nell'esempio precedente, viene restituito `StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`.

Il cmdlet seguente crea una pianificazione per raggruppare e caricare i dati alle 10:20 ogni mercoledì sera.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed -
    UploadFrequency Weekly
<!--NeedCopy-->
```

Per confermare la pianificazione, immettere `Get-CitrixCallHomeSchedule`. Nell'esempio precedente, viene restituito `StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`.

### Disabilitare Call Home

È possibile disabilitare Call Home utilizzando un cmdlet di PowerShell o tramite Citrix Scout.

I registri AOT vengono raccolti e salvati su disco, anche quando i caricamenti pianificati di Call Home sono disabilitati. Quando i caricamenti pianificati sono disabilitati, i registri AOT non vengono caricati automaticamente su Citrix. È possibile disabilitare la raccolta e l'archiviazione locale dei registri AOT.

**Disabilitare Call Home con PowerShell** Dopo aver eseguito il seguente cmdlet, i dati diagnostici non verranno caricati automaticamente su Citrix. È comunque possibile caricare dati diagnostici utilizzando i cmdlet di Citrix Scout o quelli PowerShell di telemetria.

`Disable-CitrixCallHome`

Per confermare che Call Home è disabilitato, immettere `Get-CitrixCallHome`. Se sono disabilitati, vengono restituiti `IsEnabled=False` e `IsMasterImage=False`.

**Disabilitare una pianificazione di raccolta con Citrix Scout** Per disabilitare una pianificazione di raccolta diagnostica utilizzando Citrix Scout, seguire le istruzioni fornite in Pianificare le raccolte. Nel passaggio 3, fare clic su **Off** per annullare la pianificazione per le macchine selezionate.

**Disabilitare la raccolta di registri AOT** Dopo aver eseguito il seguente cmdlet (con il campo `Enabled` impostato su **`false`**), i registri AOT non verranno raccolti.

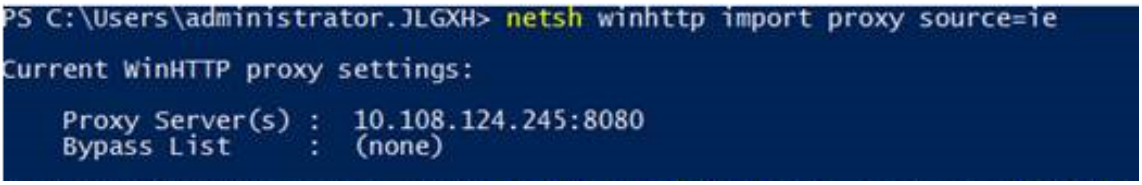
```
Enable-CitrixTrace -Listen'{ "trace":{ "enabled":false,"persistDirectory
":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds
":300 } } '
```

Il parametro `Listen` contiene argomenti in formato JSON.

#### Configurare un server proxy per i caricamenti di Call Home

Completare le seguenti attività sul computer in cui è abilitato Call Home. I diagrammi di esempio inseriti nella procedura seguente contengono l'indirizzo del server e la porta 10.158.139.37:3128. Le informazioni indicate nell'ambiente in uso saranno diverse.

1. Aggiungere informazioni sul server proxy nel browser. In Internet Explorer, selezionare **Opzioni Internet > Connessioni > Impostazioni LAN**. Selezionare **Usa un server di proxy per la rete LAN** e inserire l'indirizzo del server proxy e il numero di porta.
2. In PowerShell, eseguire `netsh winhttp import proxy source=ie`.




3. Utilizzando un editor di testo, modificare il file di configurazione TelemetryService.exe, che si trova in C:\Programmi\Citrix\Telemetry Service. Aggiungere le informazioni indicate nella casella rossa.


4. Riavviare Telemetry Service.

Eseguire i cmdlet Call Home in PowerShell.

### Raccogliere e caricare manualmente le informazioni diagnostiche

È possibile utilizzare il sito Web CIS per caricare un pacchetto di informazioni diagnostiche su CIS. È inoltre possibile utilizzare i cmdlet di PowerShell per raccogliere e caricare informazioni di diagnostica in CIS.

Per caricare un pacchetto utilizzando il sito Web CIS:

1. Accedere a Citrix Insight Services utilizzando le credenziali del proprio account Citrix.
2. Selezionare **My Workspace**.
3. Selezionare **Healthcheck** e quindi passare alla posizione in cui si trovano i propri dati.

CIS supporta diversi cmdlet di PowerShell che gestiscono i caricamenti di dati. Questa documentazione copre i cmdlet per due casi comuni:

- Utilizzare il cmdlet `Start-CitrixCallHomeUpload` per raccogliere e caricare manualmente un pacchetto di informazioni diagnostiche in CIS. Il pacchetto non viene salvato localmente.
- Utilizzare il cmdlet `Start-CitrixCallHomeUpload` per raccogliere manualmente i dati e archiviare localmente un pacchetto di informazioni diagnostiche. Ciò consente di visualizzare in anteprima i dati. Successivamente, utilizzare il cmdlet `Send-CitrixCallHomeBundle` per caricare manualmente una copia del pacchetto in CIS. I dati salvati in origine rimangono a livello locale.

La Guida di PowerShell fornisce la sintassi completa, incluse descrizioni di cmdlet e parametri non utilizzati in questi casi d'uso comuni.

Quando si immette un cmdlet per caricare dati in CIS, viene richiesto di confermare il caricamento. Se il cmdlet scade prima del completamento del caricamento, verificare lo stato del caricamento nel registro eventi di sistema. La richiesta di caricamento potrebbe essere rifiutata se il servizio sta già eseguendo un caricamento.

**Raccogliere i dati e caricare il pacchetto su CIS:**

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath
    string] [-Description string] [-IncidentTime string] [-SRNumber
    string] [-Name string] [-UploadHeader string] [-AppendHeaders string
    ] [-Collect string] [<CommonParameters>]
<!--NeedCopy-->
```

**Raccogliere i dati e salvarli localmente:**

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
    Description string] [-IncidentTime string] [-SRNumber string] [-Name
     string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
    strings] [<CommonParameters>]
<!--NeedCopy-->
```

Sono validi i seguenti parametri:

- **Credential:** indirizza il caricamento al CIS.
- **InputPath:** posizione del file zip da includere nel pacchetto. Potrebbe trattarsi di un file aggiuntivo richiesto dal supporto Citrix. Accertarsi di includere l'estensione.zip.
- **OutputPath:** posizione in cui vengono salvate le informazioni di diagnostica. Questo parametro è necessario quando si salvano i dati di Call Home localmente.
- **Description and Incident Time:** informazioni in formato libero sul caricamento.
- **SRNumber:** numero di incidente del supporto tecnico Citrix.
- **Name:** nome che identifica il pacchetto.
- **UploadHeader:** stringa formattata JSON che specifica le intestazioni di caricamento caricate in CIS.
- **AppendHeaders:** stringa formattata JSON che specifica le intestazioni aggiunte caricate in CIS.
- **Collect:** stringa formattata JSON che specifica quali dati raccogliere o omettere, nella forma { 'collector': {'enabled':Boolean}}, dove Boolean è vero o falso.
  I valori di raccolta validi sono:
  - 'wmi'
  - 'process'

  - ‘registry
  - ‘crashreport’
  - ‘trace’
  - ‘file’
  - ‘msi’
  - ‘localdata’
  - ‘sitedata’
  - ‘sfb’

  Per impostazione predefinita, tutti i valori di raccolta tranne ‘sfb’sono abilitati.

  Il valore di raccolta ‘sfb’è progettato per essere utilizzato su richiesta per diagnosticare i problemi di Skype for Business. Oltre al parametro ‘enabled’, il raccoglitore ‘sfb’supporta i parametri ‘account’e ‘accounts’per specificare gli utenti target. Utilizzare una delle forme seguenti:

  - “-Collect “{‘sfb’:{‘account’:’domain\\user1’}}”
  - “-Collect “{‘sfb’:{‘accounts’:[‘domain\\\user1’, ‘domain\\\user2’]}}”

- **Parametri comuni:** vedere la guida di PowerShell.

**Caricare i dati precedentemente salvati localmente:**

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<
CommonParameters>]
```

Il parametro `Path` specifica la posizione del pacchetto salvato in precedenza.

**Esempi:**

Il cmdlet seguente richiede un caricamento dei dati di Call Home (esclusi i dati provenienti dal valore di raccolta WMI) in CIS. Questi dati si riferiscono a errori di registrazione dei VDA Citrix Provisioning, che sono stati rilevati alle 14:30 per il caso di assistenza Citrix 123456. Oltre ai dati di Call Home, nel pacchetto caricato viene incorporato il file “c:\Diagnostics\ExtraData.zip”.

```
C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.
    zip" -Description "Registration failures with Citrix Provisioning
    VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "
    RegistrationFailure-021812016" -Collect "{
 'wmi':{
 'enabled':false }
  }
 " -UploadHeader "{
 'key1':'value1' }
 " -AppendHeaders "{
 'key2':'value2' }
 "
<!--NeedCopy-->
```

Il cmdlet seguente salva i dati di Call Home relativi al caso di supporto Citrix 223344, annotato alle 8:15. Dati salvati nel file mydata.zip su una condivisione di rete. Oltre ai dati di Call Home, nel pacchetto salvato verrà incorporato il file "c:\Diagnostics\ExtraData.zip".

```
C:\PS>Start-CitrixCallHomeUpload -OutputPath \mynetwork\myshare\mydata.
    zip -InputPath "c:\Diagnostics\ExtraData.zip" -Description "
    Diagnostics for incident number 223344" -IncidentTime "8:15" -
    SRNumber 223344
<!--NeedCopy-->
```

Il cmdlet seguente carica il pacchetto di dati salvato in precedenza.

```
$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle  – Credential $cred -Path \mynetwork\
    myshare\mydata.zip
<!--NeedCopy-->
```

## Citrix Scout

January 7, 2024

### Introduzione

Citrix Scout raccoglie la diagnostica ed esegue controlli di integrità. È possibile utilizzare i risultati per mantenere la distribuzione di Citrix Virtual Apps and Desktops. Citrix offre un'analisi completa e automatizzata delle raccolte di diagnostica tramite Citrix Insight Services. È inoltre possibile utilizzare Scout per risolvere i problemi, in autonomia o con le indicazioni del supporto Citrix.

È possibile caricare i file di raccolta inviandolo a Citrix per l'analisi e la guida da parte Citrix Support. In alternativa, è possibile salvare una raccolta localmente per la revisione personale e in seguito caricare il file di raccolta inviandolo a Citrix per l'analisi.

Scout offre le seguenti procedure:

- **Collect:** esegue una raccolta di diagnostica una tantum sui computer selezionati in un sito. È quindi possibile caricare il file inviandolo a Citrix o salvarlo localmente.
- **Trace & Reproduce:** avvia un tracciamento manuale sulle macchine selezionate. Quindi l'utente ricrea i problemi su quelle macchine. Dopo aver ricreato il problema, il tracciamento viene arrestato. Scout quindi raccoglie altri dati diagnostici e carica il file inviandolo a Citrix o lo salva localmente.
- **Schedule:** pianifica le raccolte di diagnostica per l'esecuzione quotidiana o settimanale a un orario specificato sulle macchine selezionate. Il file viene caricato automaticamente inviandolo a Citrix.

- **Health Check:** esegue controlli che valutano lo stato e la disponibilità del sito e dei suoi componenti. È possibile eseguire controlli di integrità per i Delivery Controller, i Virtual Delivery Agent (VDA), i server StoreFront e i server delle licenze Citrix. Se vengono rilevati problemi durante i controlli, Scout fornisce un rapporto dettagliato. Ogni volta che viene avviato, Scout verifica la presenza di script di controllo dello stato aggiornati. Se sono disponibili nuove versioni, Scout le scarica automaticamente, per utilizzarle la prossima volta che verranno eseguiti i controlli dello stato.

> **Nota:**
>
> Le procedure **Trace & Reproduce**, **Schedule**e **Health Check** non sono attualmente disponibili per Linux VDA.

L'interfaccia grafica descritta in questo articolo è il modo principale di usare Scout. In alternativa, è possibile utilizzare PowerShell per configurare le raccolte e i caricamenti diagnostici una tantum o pianificati. Vedere Call Home.

Dove eseguire Scout:

- In una distribuzione locale, eseguire Scout da un Delivery Controller per acquisire la diagnostica o eseguire controlli su uno o più Virtual Delivery Agent (VDA), Delivery Controller, server StoreFront e server delle licenze. È inoltre possibile eseguire Scout da un VDA per raccogliere la diagnostica locale.
- In un ambiente Citrix Cloud che utilizza Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops), eseguire Scout da un VDA per raccogliere la diagnostica locale.

Il registro per l'applicazione Scout è memorizzato in `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log`. Questo file può essere utilizzato per la risoluzione dei problemi.

### Cosa viene raccolto

La diagnostica raccolta da Scout include i file di registro del tracciamento di Citrix Diagnostic Facility (CDF). È incluso anche un sottoinsieme di tracce CDF denominato Always-on Tracing (AOT). Le informazioni fornite da AOT possono essere utili per la risoluzione di problemi comuni come le registrazioni VDA e l'avvio di applicazioni/desktop. Non vengono raccolte altre informazioni su Event Tracing for Windows (ETW).

La raccolta comprende:

- Voci di registro create da Citrix Virtual Apps and Desktops in `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
- Informazioni su Windows Management Instrumentation (WMI) nello **spazio dei nomi Citrix**.
- Processi in esecuzione.

- Dettagli degli arresti anomali dei processi Citrix archiviati in %PROGRAMDATA%\Citrix\CDF.
- Informazioni sui criteri Citrix, in formato CSV.
- Informazioni sull'installazione e l'aggiornamento. La raccolta può includere il registro del metainstaller del prodotto completo, i registri MSI non riusciti, l'output dall'analizzatore di registri MSI, i registri di StoreFront, i registri di verifica della compatibilità delle licenze e i risultati dei test preliminari di aggiornamento del sito.

Informazioni sul tracciamento:

- Le informazioni di tracciamento vengono compresse man mano che vengono raccolte, mantenendo un ingombro ridotto sulla macchina.
- Su ogni macchina, il Citrix Telemetry Service conserva le informazioni di tracciamento recenti compresse per un massimo di otto giorni.
- A partire da Citrix Virtual Apps and Desktops 7 1808, le tracce AOT vengono salvate sul disco locale per impostazione predefinita. Nelle versioni precedenti, le tracce erano conservate in memoria. Percorso predefinito = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`.
- A partire da Citrix Virtual Apps and Desktops 7 1811, le tracce AOT salvate nelle condivisioni di rete vengono raccolte con altre diagnostiche.
- È possibile modificare la dimensione massima (impostazione predefinita= 10 MB) e la durata della sezione, utilizzando il cmdlet `Enable-CitrixTrace` o la stringa `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen` del Registro di sistema.
- Le tracce si aggiungono al file fino a quando il file non raggiunge il 10% di `MaxSize`.

Per un elenco dei datapoint raccolti da Scout, vedere Datapoint chiave di Call Home.

### Configurazione di Scout

Scout può essere configurato per funzionare sui VDA Linux. Per ulteriori informazioni sui VDA Linux e la telemetria, vedere Integrate with the Citrix Telemetry Service

Il VDA Linux potrebbe modificare automaticamente la porta del socket `ctxtelemetry` o la porta per il servizio di telemetria. In tal caso, è necessario configurare la porta manualmente.

1. Passare a C:\Programmi\Citrix\Telemetry Service
2. Aprire il file di configurazione ScoutUI.exe.
3. Modificare il valore di LinuxVDATelemetryServicePort o di LinuxVDATelemetryWakeupPort per farlo corrispondere a ciò che è stato configurato sul VDA Linux:

- `<add key="LinuxVDATelemetryServicePort"value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort"value="7503"/>`

1. Salvare le modifiche e chiudere il file.

2. Aprire di nuovo Scout per assicurarsi che carichi la configurazione più recente.

## Informazioni sui controlli di integrità

I dati del controllo di integrità sono memorizzati nelle cartelle alla voce `C:\ProgramData\Citrix\TelemetryService\`.

### Controlli dello stato del sito

I controlli dello stato del sito sono inclusi in Environment Test Service, che fornisce una valutazione completa dei servizi FlexCast Management Architecture (FMA). Oltre a verificare la disponibilità del servizio, questi controlli cercano altri indicatori di integrità quali le connessioni al database.

I controlli di integrità del sito vengono eseguiti sui Delivery Controllers. A seconda delle dimensioni del sito, il completamento di questi controlli può richiedere tempi variabili fino a un'ora.

**Controlli di configurazione del Delivery Controller** Nell'ambito dei controlli di integrità del sito. I controlli di configurazione dei Delivery Controller verificano se esistono i problemi seguenti, in base alle raccomandazioni di Citrix per i siti Virtual Apps and Desktops:

- Uno o più Delivery Controller sono in stato di errore.
- C'è un solo Delivery Controller nel sito.
- I Delivery Controller sono di versioni diverse fra loro.

Oltre a soddisfare le autorizzazioni e i requisiti per i controlli di integrità, i controlli di configurazione dei Delivery Controller richiedono:

- Almeno un controller acceso.
- Il servizio broker in esecuzione su un controller.
- Una connessione funzionante dal controller al database del sito.

### Controlli di integrità dei VDA

I controlli di integrità dei VDA identificano le possibili cause di problemi comuni di registrazione, avvio della sessione e reindirizzamento del fuso orario relativamente ai VDA.

Per la registrazione sul VDA, Scout controlla:

- Installazione del software VDA
- Appartenenza al dominio macchina VDA
- Disponibilità delle porte di comunicazione VDA

- Stato del servizio VDA
- Configurazione del firewall di Windows
- Comunicazione con il controller
- Sincronizzazione temporale con il controller
- Stato di registrazione del VDA

Per gli avvii delle sessioni su VDA, Scout verifica:

- Disponibilità della porta di comunicazione di avvio della sessione
- Stato dei servizi di avvio della sessione
- Configurazione di Windows firewall all'avvio della sessione
- Licenze di accesso client di VDA Remote Desktop Services
- Percorso di avvio dell'applicazione VDA
- Impostazioni del registro di avvio della sessione

Per quanto riguarda il reindirizzamento del fuso orario sul VDA, Scout controlla:

- Installazione dell'hotfix di Windows
- Installazione dell'hotfix di Citrix
- Impostazioni dei criteri di gruppo Microsoft
- Impostazioni dei criteri di gruppo Citrix

Per il Profile Management su VDA, Scout controlla:

- Rilevamento di Hypervisor
- Rilevamento di Provisioning
- Citrix Virtual Apps and Desktops
- Configurazione del vDisk personale
- Store utenti
- Rilevamento dello stato del servizio Profile Management
- Test di hook di Winlogon.exe

Per eseguire controlli sul Profile Management, è necessario installare e abilitare Profile Management sul VDA. Per ulteriori informazioni sui controlli di configurazione Profile Management, vedere l'articolo CTX132805del Knowledge Center.

#### Controlli di integrità di StoreFront

I controlli di StoreFront verificano quanto segue:

- Il servizio Citrix Default Domain è in esecuzione
- Il servizio Citrix Credential Wallet è in esecuzione
- Connessione dal server StoreFront alla porta 88 di Active Directory

- Connessione dal server StoreFront alla porta 389 di Active Directory
- L'URL di base ha un nome di dominio completo valido
- È possibile recuperare l'indirizzo IP corretto dall'URL di base
- Il pool di applicazioni IIS utilizza .NET 4.0
- Indica se il certificato è associato alla porta SSL per l'URL dell'host
- Se la catena di certificati è completa
- Se i certificati sono scaduti
- Se un certificato scade a breve (entro 30 giorni)

#### Controlli del License Server

I controlli del License Server verificano quanto segue:

- Connessione al License Server dal Delivery Controller
- Stato dell'accesso remoto del firewall del License Server
- Stato del servizio di Citrix Licensing
- Stato del periodo di tolleranza del server delle licenze
- Connessione alle porte del License Server
- Se il daemon del fornitore Citrix (CITRIX) è in esecuzione
- Se gli orologi di sistema sono sincronizzati
- Se il servizio di licenze Citrix è in esecuzione con l'account di servizio locale
- Presenza del file `CITRIX.opt`
- Data di idoneità di Customer Success Services
- Aggiornamento del server delle licenze Citrix
- Indica se il certificato del License Server si trova nello store radice dei certificati attendibili del Delivery Controller

Oltre a soddisfare le autorizzazioni e i requisiti per i controlli di integrità, il License Server deve essere unito a un dominio. In caso contrario, il License Server non viene rilevato.

### Eseguire i controlli di integrità

La procedura di controllo dell'integrità comprende la selezione delle macchine, l'avvio del controllo e la revisione del rapporto dei risultati.

1. Avviare Scout. Dal menu **Start** della macchina, selezionare **Citrix > Citrix Scout**. Nella pagina di apertura, fare clic su **Health Check** (Controllo di integrità).
2. Selezionare le macchine. Fare clic su **Find machine** per trovare le macchine. Nella pagina **Select machines** sono elencati tutti i VDA, i Delivery Controller e i License Server rilevati nel sito. È possibile filtrare la visualizzazione per nome di macchina. Selezionare la casella di controllo

accanto a ogni macchina da cui si desidera raccogliere la diagnostica, quindi fare clic su **Continue**.

Per aggiungere altri tipi di componenti (ad esempio server StoreFront e macchine VDA), vedere Aggiungere macchine manualmente e Importare macchine VDA. Non è possibile aggiungere manualmente i Citrix Provisioning Server o i License Server.

Scout avvia automaticamente i test di verifica su ogni macchina selezionata, assicurandosi che soddisfi i criteri elencati alla voce Verification tests. Se la verifica non riesce, viene pubblicato un messaggio nella colonna **Status** e la casella di controllo della macchina viene deselezionata. È possibile eseguire una delle operazioni seguenti:

- Risolvere il problema e quindi selezionare nuovamente la casella di controllo della macchina. Questo innesca un nuovo tentativo dei test di verifica.
- Saltare quella macchina (lasciare la casella di controllo deselezionata). I controlli di integrità non vengono eseguiti su quella macchina.

Al termine dei test di verifica, fare clic su **Continue**.

3. Eseguire i controlli di integrità sulle macchine selezionate. Il riepilogo elenca le macchine in cui vengono eseguiti i test (i computer selezionati che hanno superato i test di verifica). Fare clic su **Start Checking** (Avvia controlli).

   Durante e dopo i controlli:

   - La colonna **Status** indica lo stato di controllo corrente di una macchina.
   - Per interrompere tutti i controlli in corso, fare clic su **Stop Checking** (Interrompi controlli) nell'angolo in basso a destra della pagina. Non è possibile annullare il controllo di integrità di una singola macchina, ma solo di tutte le macchine selezionate. Le informazioni provenienti dalle macchine che hanno completato i controlli vengono conservate.
   - Al termine dei controlli su tutte le macchine selezionate, il pulsante **Stop Checking** nell'angolo in basso a destra diventa **Done** (Fatto).
   - Se un controllo non riesce, è possibile fare clic su **Retry** (Riprova) nella colonna **Action**.
   - Se un controllo viene completato senza rilevare problemi, la colonna **Action** è vuota.
   - Se un controllo rileva problemi, fare clic su **View Details** (Visualizza dettagli) per visualizzare i risultati.
   - Dopo che è stato controllato il controllo di tutte le macchine selezionate, non fare clic su **Back** (Indietro). Se lo si fa, i risultati del controllo andranno persi.

4. Una volta completati i controlli, fare clic su **Done** per tornare alla pagina di apertura di Scout.

#### Risultati del controllo di integrità

Nei controlli Citrix che generano report, i rapporti contengono:

- Ora e data in cui è stato generato il report dei risultati
- Macchine che sono state controllate
- Condizioni che il controllo ha cercato sulle macchine interessate

### Autorizzazioni e requisiti

Autorizzazioni:

- Per raccogliere la diagnostica:
  - È necessario essere un amministratore locale e un utente di dominio per ciascuna macchina da cui si raccolgono i dati diagnostici.
  - È necessario disporre dell'autorizzazione per scrivere nella directory LocalAppData su ciascuna macchina.
- Per eseguire i controlli di integrità:
  - È necessario appartenere al gruppo di utenti del dominio.
  - È necessario essere un amministratore completo o disporre di un ruolo personalizzato con autorizzazioni di sola lettura ed **Run Environment Tests** (di esecuzione test ambiente) nel sito.
  - Impostare il criterio di esecuzione degli script su almeno `RemoteSigned` per consentire l'esecuzione degli script. Ad esempio: `Set-ExecutionPolicy RemoteSigned`. **Nota:** possono essere validi anche altri privilegi di esecuzione script.
- Usare **Run as administrator** (Esegui come amministratore) all'avvio di Scout.

Per ogni macchina da cui si raccolgono i dati diagnostici o si eseguono controlli di integrità:

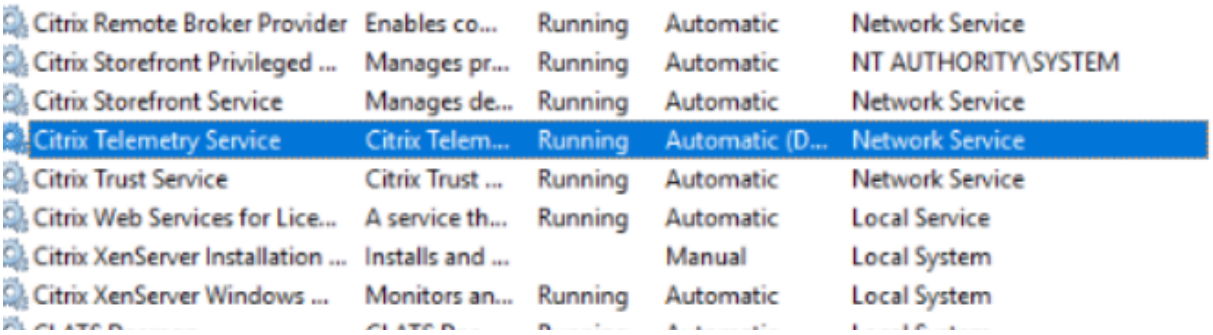
- Scout deve essere in grado di comunicare con la macchina.
- La condivisione di file e stampanti deve essere attivata.
- PSRemoting e WinRM devono essere abilitati. Il computer deve anche avere in esecuzione PowerShell 3.0 o versione successiva.
- Citrix Telemetry Service deve essere in esecuzione sul computer.
- L'accesso a Windows Management Infrastructure (WMI) deve essere abilitato sul computer.
- Per impostare una pianificazione per la raccolta diagnostica, il computer deve eseguire una versione Scout compatibile.

Non utilizzare il simbolo del dollaro ($) nei nomi utente specificati nei nomi di percorso. Impedisce la raccolta di informazioni diagnostiche.

Scout esegue test di verifica sulle macchine selezionate, per assicurarsi che questi requisiti siano soddisfatti.

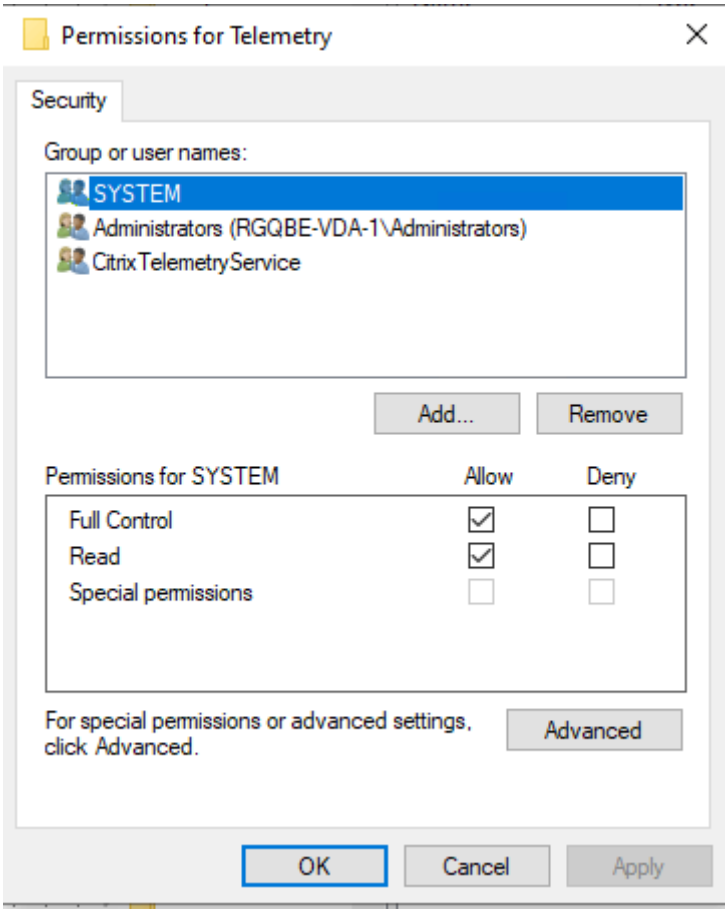
 

Il servizio di telemetria per Windows viene eseguito sul servizio di rete.



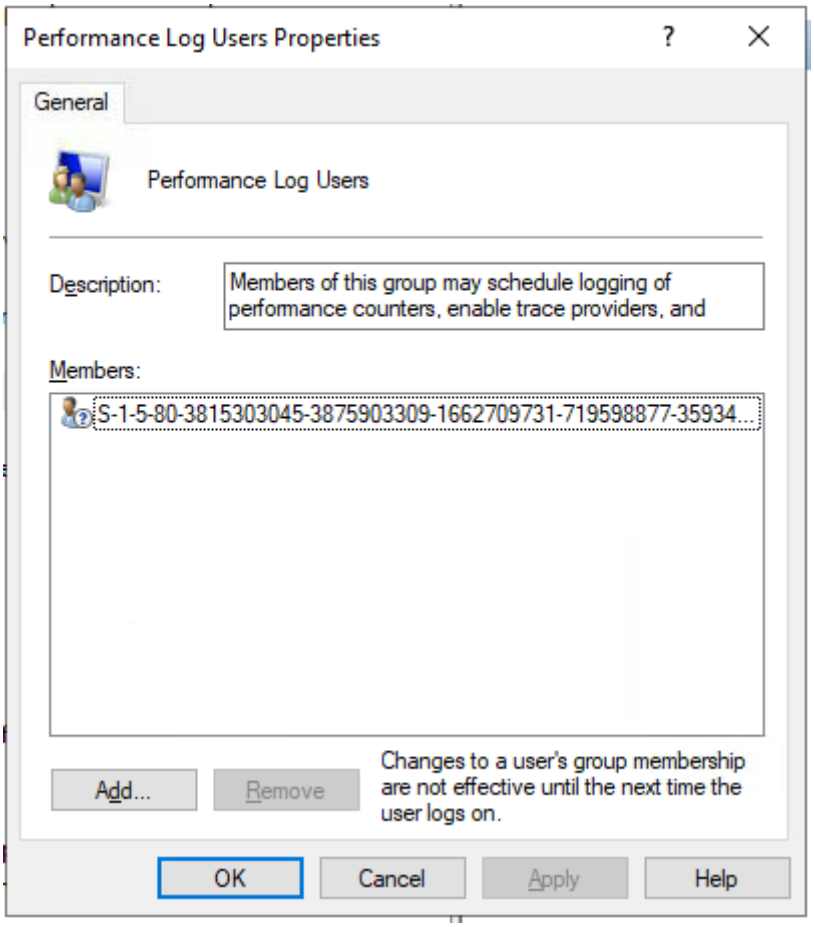

La cartella di traccia AOT viene salvata in `C:\ProgramData\Citrix\TelemetryService\CitrixAOT`.

Solo gli utenti del gruppo Amministratore, del sistema e del SID del servizio di telemetria dispongono dell'autorizzazione per accedere al Registro di sistema `HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry`.




Il SID del servizio di telemetria rimane nel gruppo Performance Log Users dopo la disinstallazione del servizio di telemetria, ma è possibile rimuoverlo manualmente.




### Test di verifica

Prima dell'avvio di una raccolta diagnostica o di un controllo di integrità, vengono automaticamente eseguiti test di verifica su ogni macchina selezionata. Questi test assicurano che siano soddisfatti i requisiti. Se un test fallisce in una macchina, Scout visualizza un messaggio, con le azioni correttive suggerite.

- **Scout cannot reach this machine** (Scout non riesce a raggiungere questa macchina): assicurarsi che:
  - La macchina sia accesa.
  - La connessione di rete funzioni correttamente. Ciò può includere la verifica che il firewall sia configurato correttamente.
  - La condivisione di file e stampanti sia attivata. Per istruzioni, vedere la documentazione Microsoft.
- **Enable PSRemoting and WinRM** (Abilitare PSRemoting e WinRM): è possibile abilitare la comunicazione remota di PowerShell e WinRM allo stesso tempo. Utilizzando **Run as administrator**

(Esegui come amministratore), eseguire il cmdlet `Enable-PSRemoting`. Per ulteriori informazioni, vedere la Guida di Microsoft relativa al cmdlet.

- **Scout requires PowerShell 3.0 (minimum)** (Scout richiede PowerShell 3.0 (minimo)): installare PowerShell 3.0 (o versione successiva) sul computer, quindi abilitare la comunicazione remota di PowerShell.
- **Unable to access LocalAppData directory on this machine** (Impossibile accedere alla directory LocalAppData su questo computer): assicurarsi che l'account disponga dell'autorizzazione per scrivere nella directory LocalAppData sul computer.
- **Cannot locate Citrix Telemetry Service** (Impossibile individuare Citrix Telemetry Service): assicurarsi che Citrix Telemetry Service sia installato e avviato sulla macchina.
- **Cannot get schedule** (Impossibile ottenere la pianificazione): aggiornare la macchina (come minimo) a XenApp e XenDesktop 7.14.
- **WMI is not running on the machine** (WMI non è in esecuzione sul computer): assicurarsi che l'accesso a Windows Management Instrumentation (WMI) sia abilitato.
- **WMI connections blocked** (Connessioni WMI bloccate): abilitare WMI nel servizio Windows Firewall.
- **Newer version of Citrix Telemetry Service required** (richiesta una versione più recente di Citrix Telemetry Service): (la versione è selezionata solo per Collect and Trace & Reproduce) aggiornare la versione di Telemetry Service sul computer (vedere Installare e aggiornare). Se non si aggiorna il servizio, il computer non è incluso nelle azioni **Collect** (Raccogli) e **Trace & Reproduce** (Traccia e riproduci).
- **Scout cannot connect to the systemd socket on this machine** (Scout non è in grado di connettersi al socket systemd su questa macchina): Assicurarsi che:
  - La porta 7503 sia aperta. Verificare che systemd ctxtelemetry.socket sia in ascolto sulla porta 7503 della macchina. La porta potrebbe essere diversa se la porta ctxtelemetry.socket è stata cambiata. Vedere Configurazione di Scout per regolare le porte.
  - La connessione di rete funzioni correttamente. Ciò potrebbe includere la verifica che il firewall sia configurato correttamente.
- **The Linux VDA Telemetry Service is not started on this machine** (Il servizio di telemetria Linux VDA non viene avviato su questa macchina): Assicurarsi che:
  - La porta 7502 sia aperta. Verificare che Linux VDA Telemetry Service sia installato e avviato sul computer. La porta potrebbe essere diversa se la porta del servizio di telemetria è stata modificata. Vedere Configurazione di Scout per regolare le porte.
  - La connessione di rete funzioni correttamente. Ciò potrebbe includere la verifica che il firewall sia configurato correttamente.

### Compatibilità con la versione

Questa versione di Scout (3.x) è pensata per essere eseguita su controller e VDA Citrix Virtual Apps and Desktops (o almeno XenApp e XenDesktop 7.14).

Una versione precedente di Scout è fornita con versioni di XenApp e XenDesktop precedenti alla 7.14. Per informazioni su quella versione precedente, vedere CTX130147.

Se si aggiorna un controller o un VDA in versione precedente alla versione 7.14 (o a una versione successiva supportata), la versione precedente di Scout viene sostituita con la versione corrente.

| Funzionalità | Scout 2.23 | Scout 3.0 |
|---|---|---|
| Supporta Citrix Virtual Apps and Desktops (oltre a XenApp e XenDesktop dalla versione 7.14 alla 7.18) | Sì | Sì |
| Supporta XenDesktop 5.x, 7.1-7.13 | Sì | No |
| Supporta XenApp 6.x, da 7.5 a 7.13 | Sì | No |
| In dotazione con il prodotto | 7.1–7.13 | A partire da 7.14 |
| Scaricabile dall'articolo CTX | Sì | No |
| Cattura di tracce CDF | Sì | Sì |
| Acquisizione del tracciamento sempre attivo (AOT) | No | Sì |
| Consente la raccolta di dati diagnostici | Fino a 10 macchine allo stesso tempo (per impostazione predefinita) | Illimitato (a seconda della disponibilità delle risorse) |
| Consente l'invio di dati diagnostici a Citrix | Sì | Sì |
| Consente il salvataggio locale dei dati diagnostici | Sì | Sì |
| Supporta le credenziali Citrix Cloud | No | Sì |
| Supporta le credenziali Citrix | Sì | Sì |
| Supporta il server proxy per i caricamenti | Sì | Sì |
| Regola gli orari | N/A | Sì |

| Funzionalità | Scout 2.23 | Scout 3.0 |
|---|---|---|
| Supporto script | Riga di comando (solo controller locale) | PowerShell utilizzando i cmdlet Call Home (qualsiasi computer con il servizio di telemetria installato) |
| Controlli di integrità | No | Sì |
| Mascheramento dei dati | No | A partire da 3.17 |

### Installare e aggiornare

Per impostazione predefinita, Scout viene installato o aggiornato automaticamente nell'ambito di Citrix Telemetry Service quando si installa o si aggiorna un VDA o un controller.

Se si omette Citrix Telemetry Service quando si installa un VDA o si rimuove il servizio in un secondo momento, eseguire `TelemetryServiceInstaller_xx.msi` dalla cartella `x64\Virtual Desktop Components` o dalla cartella `x86\Virtual Desktop Components` sul supporto di installazione Citrix Virtual Apps and Desktops.

Quando si seleziona l'azione **Collect** o l'azione **Trace & Reproduce**, si riceve una notifica se una macchina sta eseguendo una versione precedente di Citrix Telemetry Service. Citrix consiglia di utilizzare l'ultima versione supportata. Se non si aggiorna Telemetry Service su quella macchina, questo non è incluso nelle azioni **Collect** e **Trace & Reproduce**. Per aggiornare Telemetry Service, utilizzare la stessa procedura utilizzata per l'installazione.

### Autorizzazione al caricamento

Se si prevede di caricare raccolte di diagnostica su Citrix, è necessario disporre di un account Citrix o Citrix Cloud (queste sono le credenziali utilizzate per accedere ai download di Citrix o accedere al Citrix Cloud Control Center). Dopo che le credenziali del proprio account sono state convalidate, viene emesso un token.

Se si esegue l'autenticazione con un account Citrix Cloud o un account Citrix Cloud, fare clic su un collegamento per accedere a Citrix Cloud utilizzando HTTPS con il browser predefinito. Dopo che sono state inserite le credenziali di Citrix Cloud, viene visualizzato il token. Copiare il token e incollarlo in Scout. È quindi possibile continuare la procedura guidata Scout.

Il token è memorizzato localmente sulla macchina su cui è in esecuzione Scout. Per abilitare l'utilizzo di tale token alla successiva esecuzione di **Collect** o **Trace & Reproduce**, selezionare la casella di controllo **Store token and skip this step in the future** (Memorizza token e salta questo passaggio in futuro).

È necessario riautorizzare ogni volta che si seleziona **Schedule** (Pianifica) nella pagina di apertura di Scout. Non è possibile utilizzare un token memorizzato durante la creazione o la modifica di una pianificazione.

#### Usare un proxy per i caricamenti

Se si desidera utilizzare un server proxy per caricare raccolte su Citrix, è possibile indicare a Scout di utilizzare le impostazioni proxy configurate per le proprietà Internet del browser. In alternativa, è possibile specificare l'indirizzo IP e il numero di porta del server proxy.

### Trovare una macchina

Per le procedure **Collect**, **Trace & Reproduce**e **Schedule**, Scout elenca i controller e i VDA che rileva automaticamente.

Quando si esegue Scout Health Check (Controllo di integrità Scout) dal Delivery Controller, fare clic su **Find machine** (Trova macchina) per rilevare le macchine, inclusi controller di consegna, VDA, server licenze e server StoreFront.

Quando si esegue Scout Health Check da una macchina collegata al dominio che non è Delivery Controller, Scout non è in grado di rilevare automaticamente le macchine. È necessario aggiungere le macchine manualmente o importare le macchine VDA.

### Aggiungere macchine manualmente

Dopo che Scout ha elencato i controller e i VDA individuati, è possibile aggiungere manualmente altre macchine nella distribuzione, come i server StoreFront, i server di licenza e i server di Citrix Provisioning.

Quando si eseguono i controlli di integrità:

- I Citrix License Server del dominio vengono rilevati automaticamente. Non è possibile aggiungere manualmente i License Server.
- I controlli di integrità attualmente non supportano i server Citrix Provisioning.

In qualsiasi pagina Scout che elenca le macchine rilevate, fare clic su **+ Add machine** (Aggiungi macchina). Digitare il nome di dominio completo della macchina che si desidera aggiungere e quindi fare clic su **Continue**. Ripetere l'operazione per aggiungere altre macchine, se necessario. Sebbene l'immissione di un alias DNS invece di un FQDN possa sembrare valida, i controlli di integrità potrebbero non riuscire.

Le macchine aggiunte manualmente vengono sempre visualizzate in cima all'elenco delle macchine, al di sopra delle macchine rilevate.

Un modo semplice per identificare una macchina aggiunta manualmente è il pulsante di eliminazione rosso all'estremità destra della riga. Solo le macchine aggiunte manualmente hanno quel pulsante. Le macchine rilevate non ce l'hanno.

Per rimuovere una macchina aggiunta manualmente, fare clic sul pulsante rosso all'estremità destra della riga. Confermare l'eliminazione. Ripetere l'operazione per eliminare altre macchine aggiunte manualmente.

Scout ricorda le macchine aggiunte manualmente fino a quando l'utente non le rimuove. Quando si chiude e poi si riapre Scout, le macchine aggiunte manualmente sono ancora elencate in cima all'elenco.

Le tracce CDF non vengono raccolte quando si utilizza **Trace & Reproduce** sui server StoreFront. Tuttavia, vengono raccolte tutte le altre informazioni sulle tracce.

### Importare macchine VDA

È possibile importare macchine VDA nella distribuzione durante l'esecuzione dei controlli di integrità.

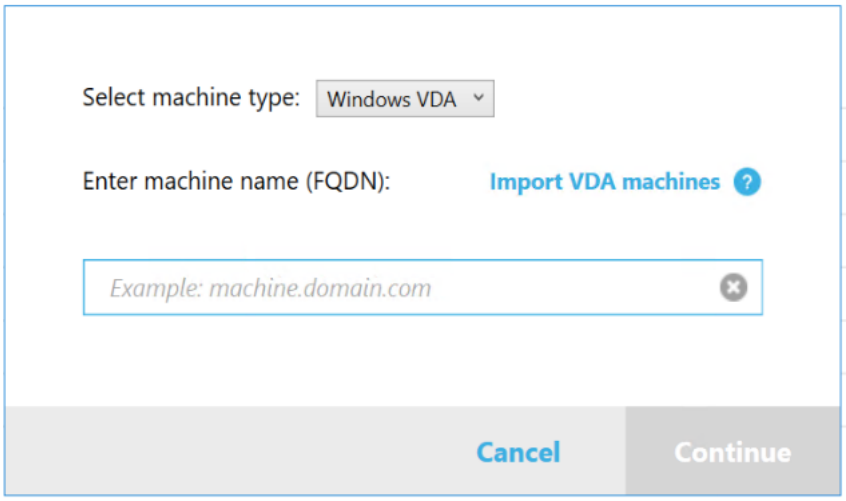
1. Su Delivery Controller o Connector, generare il file dell'elenco dei computer con il comando PowerShell. Su Connector è necessario inserire le credenziali Citrix e selezionare il cliente nella finestra di dialogo a comparsa.

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList
   .txt
   ```

2. Copiare il file machineList.txt nel computer collegato al dominio da cui si desidera avviare Scout Health Check.
3. Nella pagina Scout Health Check, fare clic su **Add Machine**.
4. Selezionare il tipo di macchina **Windows VDA**.
5. Fare clic su **Import VDA machines** (Importa macchine VDA).
6. Selezionare il file machineList.txt.
7. Fare clic su **Open**.

Le macchine VDA importate sono elencate nella pagina Scout Health Check.




### Raccogliere la diagnostica

La procedura **Collect** comprende la selezione delle macchine, l'avvio della raccolta di diagnostica e quindi il caricamento del file contenente la raccolta su Citrix o il salvataggio locale.

1. Avviare Scout. Dal menu **Start** della macchina, selezionare **Citrix > Citrix Scout**. Nella pagina di apertura, fare clic su **Collect**.
2. Selezionare le macchine.

   - Su un controller, la pagina **Select machines** elenca tutti i VDA e i controller del sito. È possibile filtrare la visualizzazione per nome di macchina. Per aggiungere altre macchine manualmente (come i server StoreFront o Citrix Provisioning), vedere Aggiungere macchine manualmente.
   - Su altri componenti (come i server VDA), l'elenco della pagina **Select machines** contiene solo il computer locale. L'aggiunta manuale di macchine non è supportata.

   Selezionare la casella di controllo accanto a ogni macchina da cui si desidera raccogliere la diagnostica, quindi fare clic su **Continue**.

   Scout avvia automaticamente i test di verifica su ogni macchina selezionata, assicurando che soddisfi i criteri elencati alla voce Verification tests. Se la verifica non riesce, viene pubblicato un messaggio nella colonna **Status** e la casella di controllo del computer non è selezionata. È possibile eseguire una delle operazioni seguenti:

   - Risolvere il problema e quindi selezionare di nuovo la casella di controllo del computer. Questo innesca un nuovo tentativo dei test di verifica.
   - Saltare quella macchina (lasciare la casella di controllo deselezionata). La diagnostica non verrà raccolta da quella macchina.

Al termine dei test di verifica, fare clic su **Continue**.

3. Raccogliere la diagnostica. Il riepilogo elenca tutte le macchine da cui viene raccolta la diagnostica (le macchine selezionate che hanno superato i test di verifica). Fare clic su **Start Collecting** (Avvia raccolta).

   Durante la raccolta:

   - La colonna **Status** indica lo stato di raccolta corrente di un computer.
   - Per interrompere una raccolta in corso su un singolo computer, fare clic su **Cancel** nella colonna **Action** relativa a quel computer.
   - Per interrompere tutte le raccolte in corso, fare clic su **Stop Collection** (Interrompi raccolta) nell'angolo in basso a destra della pagina. La diagnostica delle macchine che hanno completato la raccolta viene mantenuta. Per riprendere la raccolta, fare clic su **Retry** nella colonna **Action** per ciascun computer.
   - Al termine della raccolta per tutte le macchine selezionate, il pulsante **Stop Collection** nell'angolo in basso a destra diventa **Continue**.
   - Per raccogliere nuovamente la diagnostica, fare clic su **Collect Again** (Raccogli di nuovo) nella colonna **Action** di quella macchina. La nuova raccolta sovrascrive la precedente.
   - Se una raccolta non riesce, è possibile fare clic su **Retry** nella colonna **Action** . Solo le raccolte riuscite vengono caricate o salvate.
   - Al termine della raccolta per tutte le macchine selezionate, non fare clic su **Back**. Se si fa clic su di esso, la raccolta viene persa.

   Al termine della raccolta, fare clic su **Continue**.

4. Salvare o caricare la raccolta. Scegliere se caricare il file su Citrix o salvarlo sul computer locale.

   Se si sceglie di caricare il file ora, andare al passaggio 5.

   Se si sceglie di salvare il file in locale:

   - Viene visualizzata una finestra di dialogo **Salva** di Windows. Passare alla posizione desiderata.
   - Al termine del salvataggio locale, il percorso del file viene visualizzato e corredato di collegamento. È possibile visualizzare il file. È possibile caricare il file in un secondo momento su Citrix. Vedere CTX136396.

   Fare clic su **Done** per tornare alla pagina di apertura di Scout. Non è necessario completare ulteriori passaggi in questa procedura.

5. Eseguire l'autenticazione per i caricamenti e, facoltativamente, specificare un proxy. Per ulteriori informazioni, vedere Autorizzazione al caricamento.

   - Se non si è effettuata l'autenticazione tramite Scout, continuare da questo passaggio.

- Se si è effettuata l'autenticazione tramite Scout, il token di autorizzazione memorizzato viene utilizzato per impostazione predefinita. Se si desidera eseguire questa operazione, selezionare questa opzione e fare clic su **Continue**. Non vengono richieste le credenziali per questa raccolta. Procedere dal passaggio 6.
- Se si era già effettuata l'autenticazione, ma si desidera effettuarla di nuovo e ottenere un nuovo token, fare clic su **Change/Reauthorize** (Cambia/Riautorizza) e continuare da questo passaggio.

Scegliere se si desidera utilizzare le credenziali Citrix o le credenziali Citrix Cloud per autenticare il caricamento. Fare clic su **Continue** (Continua). La pagina delle credenziali viene visualizzata solo se non si utilizza un token memorizzato.

Nella pagina delle credenziali:

- Se si desidera utilizzare un server proxy per il caricamento del file, fare clic su **Configure proxy**. È possibile indicare a Scout di utilizzare le impostazioni del proxy configurate per le proprietà Internet del proprio browser. In alternativa, è possibile immettere l'indirizzo IP e il numero di porta del server proxy. Chiudere la finestra di dialogo del proxy.
- Per un account Citrix Cloud, fate clic su **Generate token**. Il browser predefinito viene avviato su una pagina Citrix Cloud in cui viene visualizzato un token. Copiare il token e incollarlo nella pagina Scout.
- Per un account Citrix, inserire le proprie credenziali.

Al termine, fare clic su **Continue**.

6. Inserire le informazioni sul caricamento.

   - Il campo del nome contiene il nome predefinito del file per la diagnostica raccolta. Questo è sufficiente per la maggior parte delle raccolte, anche se è possibile modificare il nome. Se si elimina il nome predefinito e si lascia vuoto il campo del nome, viene utilizzato il nome predefinito.
   - Facoltativamente, specificare un numero di richiesta di assistenza Citrix di 8 cifre.
   - Nel campo facoltativo **Description** (Descrizione), descrivere il problema e indicare quando si è verificato, se applicabile.

   Al termine, fare clic su **Start Upload** (Avvia caricamento).

   Durante il caricamento, la parte inferiore sinistra della pagina contiene la percentuale approssimativa di caricamento completato. Per annullare un caricamento in corso, fare clic su **Stop Upload** (Interrompi caricamento).

   Al termine del caricamento, l'URL della posizione viene visualizzato e corredato di collegamento. È possibile seguire il collegamento alla posizione in Citrix per visualizzare l'analisi del caricamento oppure copiare il collegamento.

   Fare clic su **Done** per tornare alla pagina di apertura di Scout.

### Tracciare e riprodurre

La procedura **Trace and Reproduce** comprende la selezione delle macchine, l'avvio del tracciamento, la riproduzione dei problemi, il completamento della raccolta diagnostica e quindi il caricamento del file su Citrix o il salvataggio locale.

Questa procedura è simile alla procedura **Collect** standard. Consente tuttavia di avviare una traccia sulle macchine e quindi di ricreare i problemi su di esse. Tutte le raccolte di diagnostica includono informazioni sulla traccia AOT. Questa procedura aggiunge tracce CDF per facilitare la risoluzione dei problemi.

1. Avviare Scout. Dal menu **Start** della macchina, selezionare **Citrix > Citrix Scout**. Nella pagina di apertura, fare clic su **Trace & Reproduce** (Tracciare e riprodurre).
2. Selezionare le macchine. La pagina **Select machines** (Seleziona macchine) elenca tutti i VDA e i controller del sito. È possibile filtrare la visualizzazione per nome di macchina. Selezionare la casella di controllo accanto a ogni macchina da cui si desidera raccogliere tracce e diagnostica. Quindi fare clic su **Continue**.

   Per aggiungere altre macchine manualmente (come i server StoreFront o Citrix Provisioning), vedere Aggiungere macchine manualmente.

   Scout avvia automaticamente i test di verifica su ogni macchina selezionata, assicurandosi che soddisfi i criteri elencati alla voce Verification tests. Se la verifica non riesce su un computer, viene pubblicato un messaggio nella colonna **Status** e la casella di controllo del computer non è selezionata. È possibile eseguire una delle operazioni seguenti:

   - Risolvere il problema e quindi selezionare di nuovo la casella di controllo del computer. Questo innesca un nuovo tentativo dei test di verifica.
   - Saltare quella macchina (lasciare la casella di controllo deselezionata). La diagnostica e le tracce non vengono raccolte da quella macchina.

   Al termine dei test di verifica, fare clic su **Continue**.
3. Iniziare il tracciamento. Il riepilogo elenca tutte le macchine da cui vengono raccolte le tracce. Fare clic su **Start Tracing** (Avvia tracciamento).

   Su uno o più computer selezionati, riprodurre i problemi riscontrati. La raccolta di tracce continua mentre lo si fa. Quando si è finito di riprodurre il problema, fare clic su **Continue** in Scout. Questo blocca il tracciamento.

   Dopo aver interrotto il tracciamento indicare se è stato riprodotto il problema durante il tracciamento.
4. Raccogliere la diagnostica dalle macchine. Fare clic su **Start Collecting** (Avvia raccolta). Durante la raccolta:

- La colonna **Status** indica lo stato di raccolta corrente di un computer.
- Per interrompere una raccolta in corso su un singolo computer, fare clic su **Cancel** nella colonna **Action** relativa a quel computer.
- Per interrompere tutte le raccolte in corso, fare clic su **Stop Collection** (Interrompi raccolta) nell'angolo in basso a destra della pagina. La diagnostica delle macchine che hanno completato la raccolta viene mantenuta. Per riprendere la raccolta, fare clic su **Retry** nella colonna **Action** per ciascun computer.
- Al termine della raccolta per tutte le macchine selezionate, il pulsante **Stop Collection** nell'angolo in basso a destra diventa **Continue**.
- Per raccogliere nuovamente la diagnostica da una macchina, fare clic su **Collect Again** nella colonna **Action** della macchina. La nuova raccolta sovrascrive la precedente.
- Se una raccolta non riesce, è possibile fare clic su **Retry** nella colonna **Action** . Solo le raccolte riuscite vengono caricate o salvate.
- Al termine della raccolta per tutte le macchine selezionate, non fare clic su **Back**. Se lo si fa, la raccolta va persa.

Al termine della raccolta, fare clic su **Continue**.

5. Salvare o caricare la raccolta. Scegliere se caricare il file su Citrix o salvarlo localmente.

   Se si sceglie di caricare il file ora, andare al passaggio 6.

   Se si sceglie di salvare il file in locale:

   - Viene visualizzata una finestra di dialogo Salva di Windows. Selezionare la posizione desiderata.
   - Al termine del salvataggio locale, il percorso del file viene visualizzato e corredato di collegamento. È possibile visualizzare il file. Ricordare: è possibile caricare il file in un secondo momento da Citrix; vedere CTX136396 per informazioni su Citrix Insight Services.

   Fare clic su **Done** per tornare alla pagina di apertura di Scout. Non è necessario completare ulteriori passaggi in questa procedura.

6. Eseguire l'autenticazione per i caricamenti e, facoltativamente, specificare il proxy. Vedere Autorizzazione al caricamento per i dettagli di questo processo.

   - Se non si è effettuata l'autenticazione tramite Scout, continuare da questo passaggio.
   - Se si è effettuata l'autenticazione tramite Scout, il token di autorizzazione memorizzato viene utilizzato per impostazione predefinita. Se questo è ciò che si intende fare, scegliere questa opzione e fare clic su **Continue**. Non vengono richieste le credenziali per questa raccolta. Andare al passaggio 7.
   - Se si era già effettuata l'autenticazione, ma si desidera effettuarla di nuovo e ottenere un nuovo token, fare clic su **Change/Reauthorize** (Cambia/Riautorizza) e continuare da questo passaggio.

Scegliere se si desidera utilizzare le credenziali Citrix o le credenziali Citrix Cloud per autenticare il caricamento. Fare clic su **Continue** (Continua). La pagina delle credenziali viene visualizzata solo se non si utilizza un token memorizzato.

Nella pagina delle credenziali:

- Se si desidera utilizzare un server proxy per il caricamento del file, fare clic su **Configure proxy**. È possibile indicare a Scout di utilizzare le impostazioni del proxy configurate per le proprietà Internet del proprio browser. In alternativa, è possibile immettere l'indirizzo IP e il numero di porta del server proxy. Chiudere la finestra di dialogo del proxy.
- Per un account Citrix Cloud, fate clic su **Generate token**. Il browser predefinito viene avviato su una pagina Citrix Cloud in cui viene visualizzato un token. Copiare il token e incollarlo nella pagina Scout.
- Per un account Citrix, inserire le proprie credenziali.

Al termine, fare clic su **Continue**.

7. Fornire informazioni sul caricamento.

   Inserire i dettagli di caricamento:

   - Il campo del nome contiene il nome predefinito del file per la diagnostica raccolta. Questo è sufficiente per la maggior parte delle raccolte, anche se è possibile modificare il nome. Se si elimina il nome predefinito e si lascia vuoto il campo del nome, viene utilizzato il nome predefinito.
   - Facoltativamente, specificare un numero di richiesta di assistenza Citrix di 8 cifre.
   - Nel campo facoltativo Description, descrivere il problema e indicare quando si è verificato, se applicabile.

   Al termine, fare clic su **Start Upload** (Avvia caricamento).

   Durante il caricamento, la parte in basso a sinistra della pagina indica la percentuale di caricamento completata. Per annullare un caricamento in corso, fare clic su **Stop Upload** (Interrompi caricamento).

   Al termine del caricamento, l'URL della posizione viene visualizzato e corredato di collegamento. È possibile seguire il collegamento alla posizione in Citrix per visualizzare l'analisi del caricamento oppure copiare il collegamento.

   Fare clic su **Done** per tornare alla pagina di apertura di Scout.

## Abilitare la raccolta di registri aggiuntivi

La funzione **Enable additional log collection** (Abilita raccolta registri aggiuntivi) consente di utilizzare la funzione di traccia e riproduzione con più strumenti, come perfmon, Netsh, DebugView e Wireshark.

> **Nota:**
>
> Questo vale solo per le macchine locali.

Per impostare una raccolta di registri aggiuntivi:

1. Avviare Citrix Scout.
2. Fare clic sull'ingranaggio **Settings** .
3. Fare clic su **Enable additional log collection with more tools** (Abilita raccolta di registri aggiuntivi con altri strumenti).
4. Fare clic su **Salva**.

Per raccogliere registri aggiuntivi:

1. Nella pagina principale di Scout, fare clic su **Trace & Reproduce** (Traccia e riproduci).
2. Nella pagina **Select machines** (Seleziona macchine), fare clic sull'ingranaggio sul lato destro della macchina locale.
3. Nella pagina Select the tools require for logging:**** (Selezionare gli strumenti necessari per la registrazione:), fare clic su **Download Tools** (Strumenti di download).
4. Nella pagina **Download Tools**, selezionare gli strumenti che si desidera utilizzare e fare clic su **Download**. Gli strumenti vengono quindi scaricati, ad eccezione di Wireshark. Wireshark può essere scaricato e installato solo manualmente.
   Nota: se si sceglie di scaricare altri strumenti manualmente, è necessario estrarre il contenuto del file .zip scaricato in `C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\<toolname>`. Ad esempio, se si scarica il file DebugView.zip, decomprimere il contenuto del file in `C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\`.
5. Nella pagina **Select the tools require for logging:** (Selezionare gli strumenti necessari per la registrazione:) fare clic su **Refresh Status** (Aggiorna stato). Tutti gli strumenti selezionati vengono visualizzati come **Present** nella colonna Status.
6. Selezionare gli strumenti per la registrazione, quindi fare clic su **Next** (Avanti).
7. Seguire le istruzioni riportate in Trace and Reproduce (Tracciare e riprodurre).
8. Dopo il completamento, controllare i registri contenuti nel file zip. I registri sono compressi nella cartella *CDCLogs*.

> **Nota:**
>
> Se lo strumento Procmon è selezionato per il tracciamento, i log di Process Monitor possono diventare rapidamente di grandi dimensioni. Assicurarsi di selezionare solo gli strumenti necessari. È inoltre possibile monitorare le dimensioni dei registri in *%temp%\Scout-CDC-Log*.

### Pianificare le raccolte

> **Nota:**
>
> Al momento è possibile pianificare le raccolte, ma non le verifiche di integrità.

La procedura di pianificazione comprende la selezione delle macchine e quindi l'impostazione o l'annullamento della pianificazione. Le raccolte pianificate vengono caricate automaticamente su Citrix. È possibile salvare le raccolte pianificate localmente utilizzando l'interfaccia di PowerShell. Vedere Citrix Call Home.

1. Avviare Scout. Dal menu Start della macchina, selezionare **Citrix > Citrix Scout**. Nella pagina di apertura, fare clic su **Schedule** (Pianifica).
2. Selezionare le macchine. Sono elencati tutti i VDA e i controller presenti nel sito. È possibile filtrare la visualizzazione per nome di macchina.

   Quando sono stati installati VDA e controller utilizzando l'interfaccia grafica, se si imposta una pianificazione Call Home (vedere Citrix Call Home), Scout visualizza tali impostazioni, per impostazione predefinita. È possibile utilizzare questa versione di Scout per avviare le raccolte pianificate per la prima volta o modificare una pianificazione configurata in precedenza.

   Anche se è stato abilitato/disabilitato Call Home nelle singole macchine durante l'installazione dei componenti, una pianificazione configurata in Scout influisce su tutte le macchine selezionate.

   Selezionare la casella di controllo accanto a ogni macchina da cui si desidera raccogliere la diagnostica, quindi fare clic su **Continue**.

   Per aggiungere altre macchine manualmente (come i server StoreFront o Citrix Provisioning), vedere Aggiungere macchine manualmente.

   Scout avvia automaticamente i test di verifica su ciascuna delle macchine selezionate, assicurandosi che soddisfino i criteri indicati in Verification tests. Se la verifica non riesce su un computer, viene pubblicato un messaggio nella colonna **Status** e la casella di controllo del computer non è selezionata. È possibile eseguire una delle operazioni seguenti:

   - Risolvere il problema e quindi selezionare di nuovo la casella di controllo del computer. Questo innesca un nuovo tentativo dei test di verifica.
   - Saltare quella macchina (lasciare la casella di controllo deselezionata). La diagnostica (o il tracciamento) non viene raccolto da quella macchina.

   Al termine dei test di verifica, fare clic su **Continue**.

   La pagina di riepilogo elenca i computer a cui sono applicate le pianificazioni. Fare clic su **Continue** (Continua).
3. Impostare il programma. Indicare quando si desidera raccogliere la diagnostica. Ricordare: la pianificazione influisce su tutte le macchine selezionate.

- Per configurare un programma settimanale per le macchine selezionate, fare clic su **Weekly**. Scegliere il giorno della settimana. Inserire l'ora (orologio di 24 ore) dell'inizio della raccolta.
- Per configurare una pianificazione giornaliera per i computer selezionati, fare clic su **Daily**. Inserire l'ora (orologio di 24 ore) dell'inizio della raccolta.
- Per annullare una pianificazione esistente per i computer selezionati (e non sostituirla con un'altra), fare clic su **Off**. Ciò annulla qualsiasi pianificazione precedentemente configurata per tali macchine.

Fare clic su **Continue** (Continua).

4. Eseguire l'autenticazione per i caricamenti e, facoltativamente, specificare un proxy. Vedere Autorizzazione al caricamento per i dettagli di questo processo. Ricordare: non è possibile utilizzare un token memorizzato per l'autenticazione quando si lavora con una pianificazione di Scout.

   Scegliere se si desidera utilizzare le credenziali Citrix o le credenziali Citrix Cloud per autenticare il caricamento. Fare clic su **Continue** (Continua).

   Nella pagina delle credenziali:

   - Se si desidera utilizzare un server proxy per il caricamento del file, fare clic su **Configure proxy**. È possibile indicare a Scout di utilizzare le impostazioni del proxy configurate per le proprietà Internet del proprio browser. In alternativa, è possibile immettere l'indirizzo IP e il numero di porta del server proxy. Chiudere la finestra di dialogo del proxy.
   - Per un account Citrix Cloud, fate clic su **Generate token**. Il browser predefinito viene avviato su una pagina Citrix Cloud in cui viene visualizzato un token. Copiare il token e incollarlo nella pagina Scout.
   - Per un account Citrix, inserire le proprie credenziali.

   Al termine, fare clic su **Continue**.

   Rivedere la pianificazione configurata. Fare clic su **Done** per tornare alla pagina di apertura di Scout.

   Durante una raccolta, il registro dell'applicazione Windows di ciascuna macchina selezionata contiene voci relative alla raccolta e al caricamento.

### Mascheramento dei dati

Le informazioni diagnostiche raccolte con Citrix Scout potrebbero contenere informazioni sensibili a problemi di sicurezza. La funzione di mascheramento dei dati di Citrix Scout consente di mascherare i dati sensibili contenuti nei file di diagnostica prima di caricarli su Citrix.

Il mascheramento dei dati Scout è configurato per mascherare l'indirizzo IP, i nomi di computer, i nomi di dominio, i nomi utente, i nomi degli hypervisor, i nomi dei gruppi di consegna, i nomi dei cataloghi, i nomi delle applicazioni e i SID.

> **Nota:**
>
> Le tracce CDF sono crittografate e non possono essere mascherate.
>
> I log di Linux VDA sono compressi in formato `.tar.gz2` e non possono essere mascherati.

#### Raccogliere nuova diagnostica ed eseguire il mascheramento dei dati

Per utilizzare la funzione di mascheramento dei dati di Citrix Scout, avviare Scout dalla riga di comando.

1. In Windows, aprire il prompt dei comandi come amministratore.
2. Andare alla directory in cui è installato Scout: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Avviare Scout: `ScoutUI.exe datamasking`.
4. Fare clic su **Collect** o su **Trace & Reproduce** per raccogliere la diagnostica.
5. Al termine della raccolta, selezionare **Enable data masking** (Abilita mascheramento dei dati). Questa opzione è abilitata per impostazione predefinita.
6. Configurare il mascheramento dati. È possibile utilizzare le regole predefinite o personalizzarle.
7. Scegliere se caricare o salvare la raccolta di diagnostica.
    - Se si seleziona **Upload the diagnostics collection to Citrix** (Carica la raccolta di diagnostica su Citrix), i file di diagnostica mascherati vengono caricati su Citrix.
    - Se si seleziona **Save the diagnostics collection on your local machine** (Salva la raccolta di diagnostica sul computer locale), sia la diagnostica originale che quella mascherata vengono salvate nella posizione specificata.

#### Eseguire il mascheramento dei dati di diagnostica esistente

1. In Windows, aprire il prompt dei comandi come amministratore.
2. Andare alla directory in cui è installato Scout: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Avviare Scout direttamente in modalità di mascheramento dei dati: `ScoutUI.exe datamasking filePath`.
4. Selezionare "Enable data masking"(Abilita mascheramento dei dati) per continuare. Questa opzione è abilitata per impostazione predefinita.
5. Configurare il mascheramento dati. È possibile eseguire il mascheramento dei dati con le regole predefinite o personalizzarle.

6. Scegliere se caricare o salvare la raccolta di diagnostica.
    - Se si seleziona **Upload the diagnostics collection to Citrix** (Carica la raccolta di diagnostica su Citrix), i file di diagnostica mascherati vengono caricati su Citrix.
    - Se si seleziona **Save the diagnostics collection on your local machine** (Salva la raccolta di diagnostica sul computer locale), sia la diagnostica originale che quella mascherata vengono salvate nella posizione specificata.

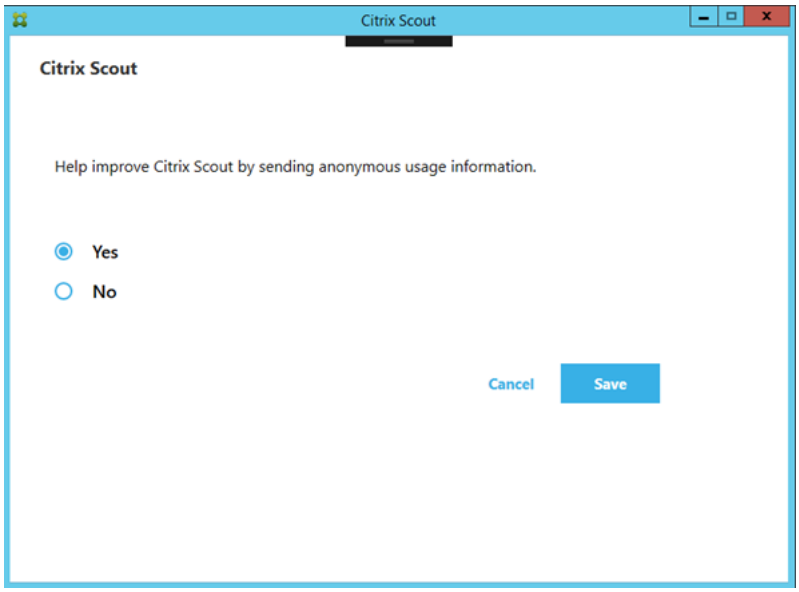
#### File di dati mascherati e posizioni dei file di mappatura

Dopo aver caricato o salvato la raccolta di diagnostica, fare clic sul collegamento per aprire la diagnostica originale e quella mascherata e aprire il file delle informazioni di mappatura.

### Raccolta dei dati di utilizzo

Quando si utilizza Scout, Citrix utilizza Google Analytics per raccogliere dati anonimi sull'utilizzo finalizzati allo sviluppo di funzionalità e di miglioramenti futuri dei prodotti. La raccolta dei dati è abilitata per impostazione predefinita.

Per modificare la raccolta e il caricamento dei dati di utilizzo, fare clic sul simbolo dell'ingranaggio **Impostazioni** nell'interfaccia utente di Scout. È quindi possibile scegliere se inviare le informazioni selezionando **Sì** o **No** e quindi facendo clic su **Save**.



# Raccogliere una traccia di Citrix Diagnostic Facility (CDF) all'avvio del sistema

January 7, 2024

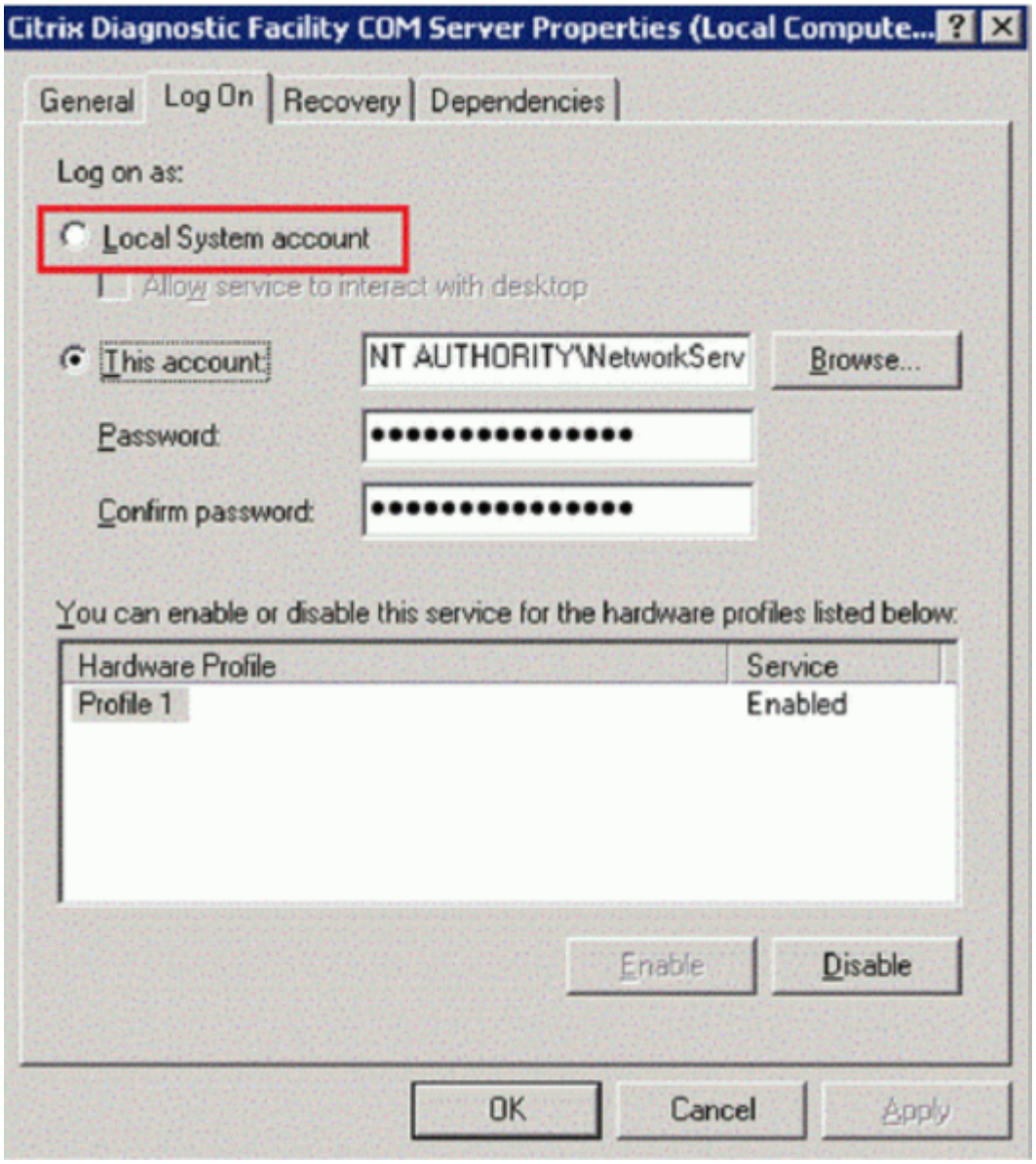
L'utilità CDFControl è un controller di tracciamento eventi o consumer per l'acquisizione di messaggi di traccia Citrix Diagnostic Facility (CDF) visualizzati da vari provider di tracciamento Citrix. Il suo ruolo è risolvere problemi complessi relativi a Citrix, analizzare il supporto del filtro e raccogliere dati sulle prestazioni. Per scaricare l'utilità CDFControl, vedere CTX111961.

## Usare l'account del sistema locale

Per utilizzare l'account del sistema locale per il servizio server CDF COM, attenersi alla seguente procedura:

1. Fare clic su **Esegui** nel menu **Start**.
2. Digitare `services.msc` nella finestra di dialogo e fare clic su **OK**.
3. Selezionare il servizio **Citrix Diagnostics Facility COM Server** e scegliere **Proprietà**.
4. Fare clic sulla scheda **Log On** e abilitare l'account del **sistema locale**. Quindi fare clic su **OK**.



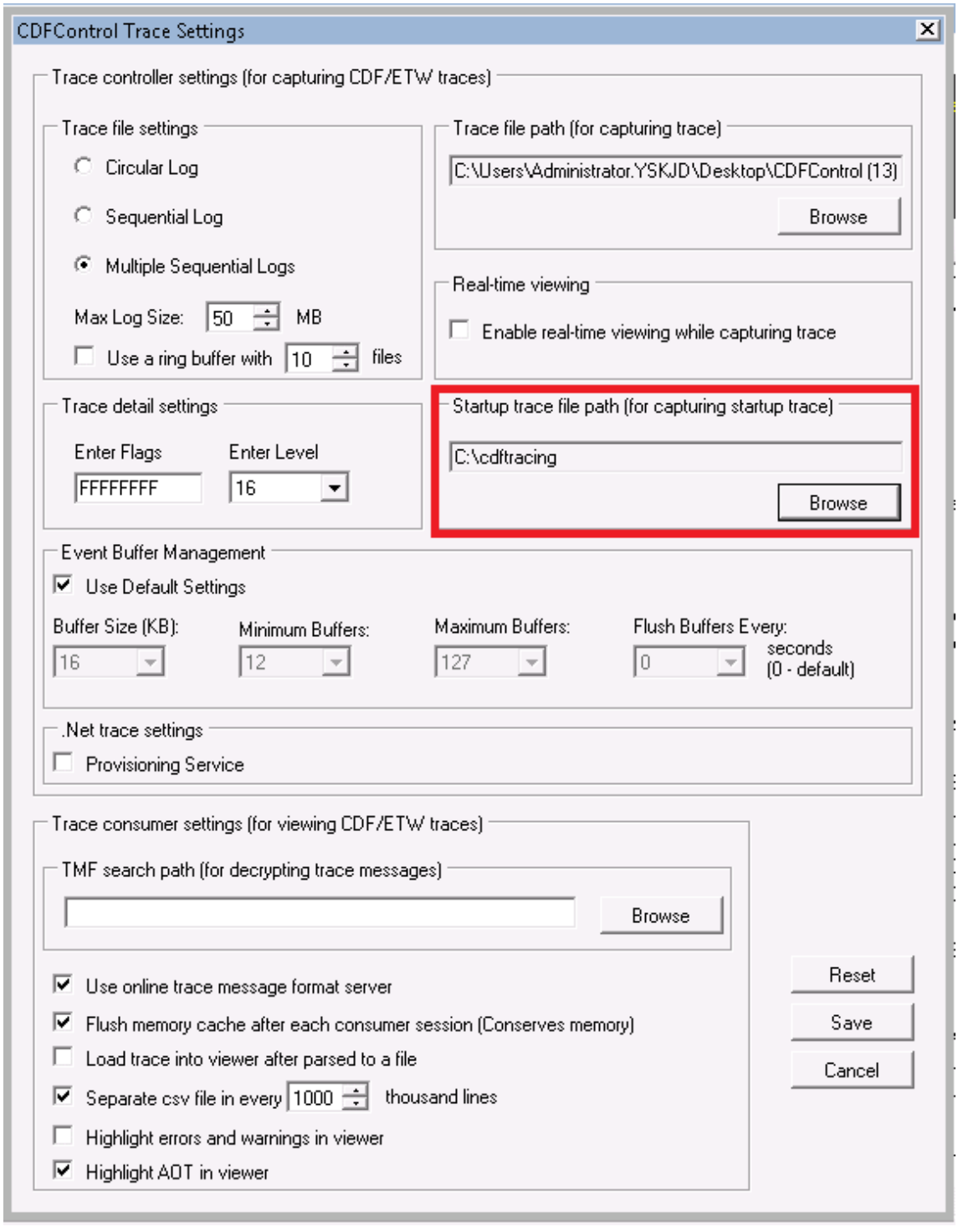

5. Riavviare il servizio.

### Raccogliere una traccia all'avvio del sistema

Utilizzare la procedura seguente per raccogliere una traccia CDF all'avvio del sistema. Sono necessari i privilegi di amministratore.

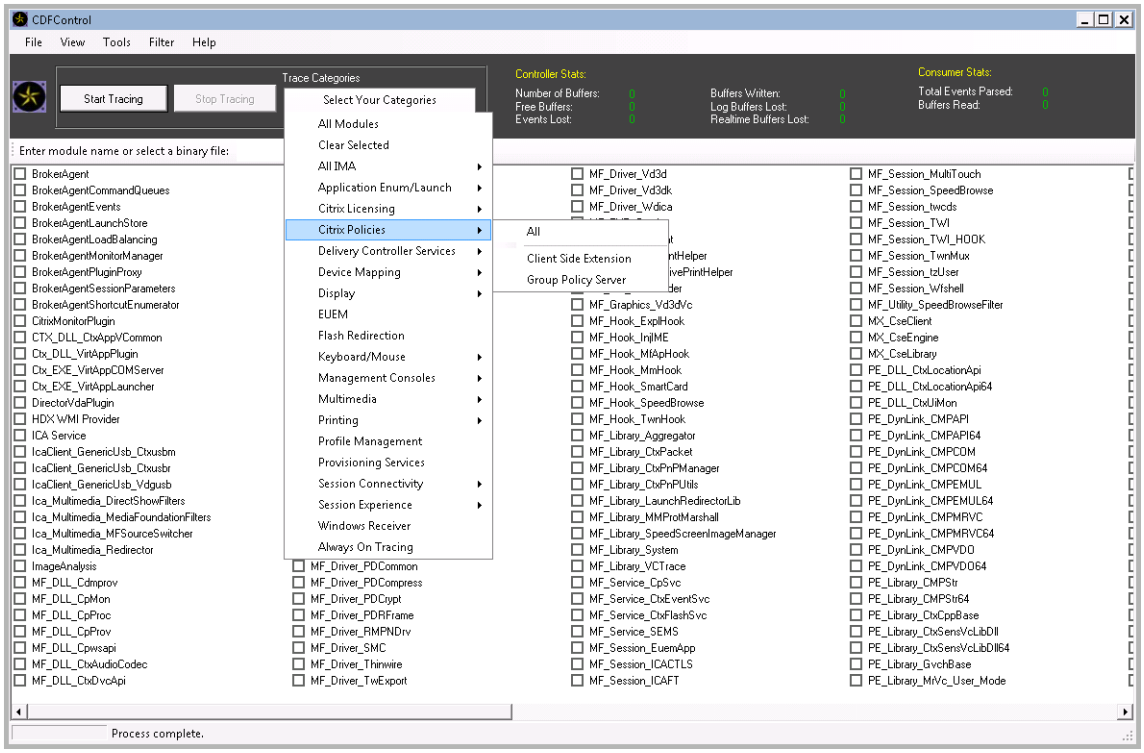
1. Avviare **CDFControl** e selezionare **Options** dal menu **Tools** .
2. Specificare il percorso del file di tracciamento nella sezione **Startup trace file path for capturing startup trace** (Percorso del file di tracciamento di avvio per l'acquisizione della traccia di avvio). Quindi fare clic su **Save**.




3. Selezionare le **categorie di tracciamento** consigliate da Citrix Support. (Nell'esempio seguente è selezionato **Citrix Policies**. Questa selezione è solo un esempio. Consigliamo di abilitare i provider per il problema specifico che si sta risolvendo.)




4. Selezionare **Startup Tracing** (Tracciamento all'avvio) e selezionare **Enable** (Attiva) dal menu **Tools** (Strumenti).

   Dopo aver selezionato **Enable**, la barra animata inizia a scorrere. Questa attività non influisce sulla procedura. Continuare spostandosi al passaggio successivo.

5. Dopo aver abilitato **Startup Tracing**, chiudere l'**utilità CDFControl** e riavviare il sistema.

6. Avviare l'utilità **CDFControl**. Dopo che il sistema si riavvia e viene visualizzato l'errore, disabilitare il tracciamento all'avvio selezionando **Startup Tracing** dal menu **Tools** e facendo clic su **Disable**.

7. Arrestare il servizio server **COM Citrix Diagnostics Facility**.

8. Andare al percorso del file di traccia specificato nel passaggio 2 e raccogliere il file di registro di traccia (.etl) per l'analisi.

9. Avviare il servizio server **Citrix Diagnostics Facility COM**.

## Amministrazione delegata

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Il modello di amministrazione delegata offre la flessibilità necessaria per adeguarsi al modo in cui l'organizzazione desidera delegare le attività di amministrazione, utilizzando il controllo basato su ruoli e su oggetti. L'amministrazione delegata supporta distribuzioni di tutte le dimensioni e consente di configurare una maggiore granularità delle autorizzazioni man mano che la distribuzione si fa più complessa. L'amministrazione delegata utilizza tre concetti: amministratori, ruoli e ambiti.

- **Amministratori:** un amministratore rappresenta una singola persona o un gruppo di persone identificate dal proprio account Active Directory. Ogni amministratore è associato a una o più coppie di ruoli e di ambiti.
- **Ruoli:** un ruolo rappresenta una funzione lavorativa e ad esso sono associate autorizzazioni definite. Ad esempio, il ruolo di Amministratore del gruppo di consegna dispone di autorizzazioni quali "Create Delivery Group"(Crea gruppo di consegna) e "Remove Desktop from Delivery Group"(Rimuovi desktop dal gruppo di consegna). Un amministratore può disporre di più ruoli per un sito, quindi una stessa persona può essere un amministratore del gruppo di consegna e del catalogo macchine. I ruoli possono essere incorporati o personalizzati.

  I ruoli predefiniti sono:

| Ruolo | Autorizzazioni |
| --- | --- |
| Full Administrator (Amministratore completo) | Può eseguire tutte le attività e le operazioni. Un amministratore completo viene sempre combinato con l'ambito All (Tutto). |

| Ruolo | Autorizzazioni |
| --- | --- |
| Read Only Administrator (Amministratore di sola lettura) | Può visualizzare tutti gli oggetti negli ambiti specificati oltre alle informazioni globali, ma non può modificare nulla. Ad esempio, un amministratore di sola lettura con ambito= Londra può visualizzare tutti gli oggetti globali (ad esempio Registrazione configurazione) e tutti gli oggetti con ambito Londra (ad esempio, Gruppi di consegna di Londra). Tuttavia, tale amministratore non può visualizzare gli oggetti nell'ambito di New York (supponendo che gli ambiti Londra e New York non si sovrappongano). |
| Help Desk Administrator (Amministratore dell'helpdesk) | Può visualizzare i gruppi di consegna e gestire le sessioni e i computer associati a tali gruppi. Può visualizzare il catalogo macchine e le informazioni sull'host per i gruppi di consegna che segue. Può inoltre eseguire operazioni di gestione delle sessioni e gestione dell'alimentazione della macchina per le macchine di tali gruppi di consegna. |
| Machine Catalog Administrator (Amministratore del catalogo macchine) | Può creare e gestire i cataloghi di macchine e il provisioning delle macchine in essi elencate. Può creare cataloghi macchine dall'infrastruttura di virtualizzazione, dai Provisioning Services e dalle macchine fisiche. Questo ruolo può gestire immagini di base e installare software, ma non può assegnare applicazioni o desktop agli utenti. |
| Delivery Group Administrator (Amministratore di gruppo di consegna) | Può distribuire applicazioni, desktop e macchine, nonché gestire le sessioni associate. Può inoltre gestire configurazioni di applicazioni e desktop, ad esempio criteri e impostazioni di risparmio energia. |
| Host Administrator (Amministratore host) | Può gestire le connessioni host e le relative impostazioni delle risorse associate. Non può distribuire macchine, applicazioni o desktop agli utenti. |

In alcune edizioni del prodotto, è possibile creare ruoli personalizzati in base ai requisiti dell'organizzazione e delegare le autorizzazioni con maggiori dettagli. È possibile utilizzare ruoli personalizzati per allocare le autorizzazioni in base alla granularità di un'azione o di un'attività in una console.

- **Ambiti:** un ambito rappresenta una raccolta di oggetti. Gli ambiti vengono utilizzati per raggruppare gli oggetti in modo rilevante per l'organizzazione (ad esempio, l'insieme di gruppi di consegna utilizzato dal team vendite). Gli oggetti possono trovarsi in più di un ambito; gli oggetti possono essere etichettati con uno o più ambiti. C'è un ambito incorporato: "Tutto", che contiene tutti gli oggetti. Il ruolo Amministratore completo è sempre associato all'ambito Tutto.

### Esempio

Società XYZ ha deciso di gestire applicazioni e desktop in base al relativo reparto (Account, Vendite e Magazzino) e al sistema operativo desktop (Windows 7 o Windows 8). L'amministratore ha creato cinque ambiti, quindi ha etichettato ciascun gruppo di consegna con due ambiti: uno per il reparto in cui vengono utilizzati e uno per il sistema operativo che utilizzano.

Sono stati creati i seguenti amministratori:

| Amministratore | Ruoli | Ambiti |
|---|---|---|
| dominio/fred | Full Administrator (Amministratore completo) | Tutto (il ruolo Amministratore completo ha sempre l'ambito Tutto) |
| dominio/rob | Read Only Administrator (Amministratore di sola lettura) | Tutte |
| dominio/heidi | Amministratore di sola lettura, Amministratore dell'helpdesk | Tutte le vendite |
| dominio/warehouseadmin | Help Desk Administrator (Amministratore dell'helpdesk) | Magazzino |
| dominio/peter | Amministratore dei gruppi di consegna, Amministratore del catalogo macchine | Win7 |

- Fred è un amministratore completo e può visualizzare, modificare ed eliminare tutti gli oggetti presenti nel sistema.
- Rob può visualizzare tutti gli oggetti presenti nel sito ma non modificarli o eliminarli.
- Heidi può visualizzare tutti gli oggetti ed eseguire attività di helpdesk nei gruppi di consegna nell'ambito Vendite. Ciò le consente di gestire le sessioni e le macchine associate a tali gruppi;

non può apportare modifiche al gruppo di consegna, ad esempio aggiungere o rimuovere macchine.
- Chiunque sia membro del gruppo di sicurezza di warehouseadmin di Active Directory può visualizzare ed eseguire attività di helpdesk sui computer che fanno parte dell'ambito Magazzino.
- Peter è uno specialista di Windows 7 e può gestire tutti i cataloghi di macchine Windows 7 e può fornire applicazioni, desktop e computer Windows 7, indipendentemente dall'ambito di reparto in cui si trovano. L'amministratore ha preso in considerazione la decisione di rendere Peter un amministratore completo per l'ambito Win7. Tuttavia, ha poi deciso di non farlo, perché un amministratore completo ha anche diritti completi su tutti gli oggetti che non sono ambiti, come "Sito"e "Amministratore".

## Come utilizzare l'amministrazione delegata

In genere, il numero di amministratori e la granularità delle autorizzazioni dipendono dalle dimensioni e dalla complessità della distribuzione.

- Nelle distribuzioni di piccole dimensioni o quelle prova di concetto, uno o pochi amministratori fanno tutto. Non ci sono deleghe. In questo caso, creare ciascun amministratore con il ruolo Amministratore completo incorporato, che dispone dell'ambito Tutto.
- Nelle distribuzioni più grandi con più macchine, applicazioni e desktop, è necessario delegare di più. Diversi amministratori potrebbero avere responsabilità funzionali (ruoli) più specifiche. Ad esempio, due sono Amministratori completi e altri sono Amministratori dell'helpdesk. Inoltre, un amministratore può gestire solo determinati gruppi di oggetti (ambiti), ad esempio i cataloghi di macchine. In questo caso, creare nuovi ambiti, oltre ad amministratori con uno dei ruoli incorporati e gli ambiti appropriati.
- Le distribuzioni ancora più grandi potrebbero richiedere più ambiti (o ambiti più specifici), oltre ad amministratori diversi con ruoli non convenzionali. In questo caso, modificare o creare più ambiti, creare ruoli personalizzati e creare ogni amministratore con un ruolo predefinito o personalizzato, oltre ad ambiti nuovi ed esistenti.

Per flessibilità e semplicità di configurazione, è possibile creare ambiti quando si crea un amministratore. È inoltre possibile specificare ambiti durante la creazione o la modifica di cataloghi di macchine o connessioni.

## Creare e gestire gli amministratori

Quando si crea un sito come amministratore locale, l'account utente diventa automaticamente un amministratore completo con autorizzazioni complete su tutti gli oggetti. Dopo la creazione di un sito, gli amministratori locali non dispongono di privilegi speciali.

Il ruolo di amministratore completo ha sempre l'ambito Tutto. Non è possibile modificarlo.

Per impostazione predefinita, è abilitato un amministratore. La disattivazione di un amministratore potrebbe essere necessaria se si sta creando l'amministratore in quel momento, ma tale persona non inizierà a svolgere compiti di amministrazione fino a un secondo momento. Per gli amministratori abilitati esistenti, è possibile disabilitare molti di essi durante la riorganizzazione degli oggetti/ambiti, quindi riattivarli quando si è pronti a utilizzare la configurazione aggiornata. Non è possibile disabilitare un amministratore completo se, così facendo, non rimane alcun amministratore completo. La casella di controllo abilita/disabilita è disponibile quando si crea, copia o modifica un amministratore.

Quando si elimina una coppia ruolo/ambito durante la copia, la modifica o l'eliminazione di un amministratore, viene eliminata solo la relazione tra il ruolo e l'ambito di tale amministratore. Non viene eliminato né il ruolo né l'ambito. Inoltre, l'eliminazione non influisce su nessun altro amministratore configurato con tale coppia di ruolo/ambito.

Per creare e gestire gli amministratori, seguire questi passaggi:

1. Accedere a Web Studio, fare clic su **Administrators** nel riquadro a sinistra e quindi fare clic sulla scheda **Administrators**.
2. Seguire le istruzioni per l'attività da completare:
    - **Creare un amministratore:** fare clic su **Create Administrator** (Crea amministratore) nella barra delle azioni. Digitare o individuare il nome dell'account utente, selezionare o creare un ambito e quindi selezionare un ruolo. Il nuovo amministratore è abilitato per impostazione predefinita; è possibile modificare questa impostazione.
    - **Copiare un amministratore:** selezionare l'amministratore e quindi fare clic su **Copy Administrator** nella barra delle azioni. Digitare o individuare il nome dell'account utente. È possibile selezionare e quindi modificare o eliminare qualsiasi coppia ruolo/ambito e aggiungerne di nuove. Il nuovo amministratore è abilitato per impostazione predefinita; è possibile modificare questa impostazione.
    - **Modificare un amministratore:** selezionare l'amministratore e quindi fare clic su **Edit Administrator** (Modifica amministratore) nella barra delle azioni. È possibile modificare o eliminare una o più delle coppie ruolo/ambito e aggiungerne di nuove.
    - **Eliminare un amministratore:** selezionare l'amministratore e fare clic su **Delete Administrator** (Elimina amministratore) nella barra delle azioni. Non è possibile eliminare un amministratore completo se, così facendo, non rimane alcun amministratore completo.

Nel riquadro superiore vengono visualizzati gli amministratori creati. Selezionare un amministratore per visualizzarne i dettagli nel riquadro inferiore. La colonna **Warnings** (Avvisi) indica se le coppie ruolo/ambito associate all'amministratore contengono ruoli o ambiti inutilizzabili. Se una coppia di ruoli e ambiti associati contiene ruoli o ambiti inutilizzabili, viene visualizzato il seguente messaggio di avviso:

- Associated role or scope not usable (Ruolo o ambito associato non utilizzabile)

> **Importante:**
>
> Se una coppia di ruoli e ambiti associati contiene ruoli o ambiti o coppie ruolo/ambito inutilizzabili, viene visualizzato un messaggio di avviso.

Per rimuovere la coppia ruolo/ambito dall'amministratore, completare una delle seguenti operazioni:

- Eliminare la coppia ruolo/ambito.
    1. Nella barra delle azioni fare clic su **Edit Administrator** (Modifica amministratore).
    2. Nella finestra **Administrator Name and Details** selezionare la coppia ruolo/ambito e quindi fare clic su **Delete**.
    3. Fare clic su **Save** per uscire.
- Eliminare l'amministratore.
    1. Nella barra delle azioni fare clic su **Delete Administrator** (Elimina amministratore).
    2. Nella finestra di conferma, fare clic su **Delete**.

### Creare e gestire ruoli

Quando gli amministratori creano o modificano un ruolo, possono abilitare solo le autorizzazioni di cui dispongono essi stessi. Ciò impedisce agli amministratori di creare un ruolo con più autorizzazioni di quelle di cui dispongono attualmente e di assegnarlo a se stessi (o modificare un ruolo già assegnato).

I nomi dei ruoli possono contenere fino a 64 caratteri Unicode; non possono contenere: barra rovesciata, barra, punto e virgola, due punti, cancelletto, virgola, asterisco, punto interrogativo, segno di uguale, freccia sinistra o destra, barra verticale, parentesi quadra aperta o chiusa, parentesi tonda aperta o chiusa, virgolette o apostrofo. Le descrizioni possono contenere fino a 256 caratteri Unicode.

Non è possibile modificare o eliminare un ruolo predefinito. Non è possibile eliminare un ruolo personalizzato se viene utilizzato da un amministratore.

> **Nota:**
>
> Solo alcune edizioni di prodotto supportano i ruoli personalizzati. Solo le edizioni che supportano i ruoli personalizzati hanno voci correlate nella barra delle azioni.

Per creare e gestire i ruoli, seguire questi passaggi:

1. Accedere a Web Studio, fare clic su **Administrators** nel riquadro a sinistra, quindi fare clic sulla scheda **Roles**.

2. Seguire le istruzioni per l'attività da completare:

    - **Visualizzare i dettagli del ruolo:** selezionare il ruolo. Nel riquadro inferiore sono elencati i tipi di oggetto e le autorizzazioni associate al ruolo. Fare clic sulla scheda **Administrators** nel riquadro inferiore per visualizzare un elenco degli amministratori che attualmente dispongono di questo ruolo.
    - **Creare un ruolo personalizzato:** fare clic su **Create Role** (Crea ruolo) nella barra delle azioni. Immettere un nome e una descrizione. Selezionare i tipi di oggetto e le autorizzazioni.
    - **Copiare un ruolo:** selezionare il ruolo e quindi fare clic su **Copy Role** (Copia ruolo) nella barra delle azioni. Modificare il nome, la descrizione, i tipi di oggetto e le autorizzazioni in base alle esigenze.
    - **Modificare un ruolo personalizzato:** selezionare il ruolo e quindi fare clic su **Edit Role** (Modifica ruolo) nella barra delle azioni. Modificare il nome, la descrizione, i tipi di oggetto e le autorizzazioni in base alle esigenze.
    - **Eliminare un ruolo personalizzato:** selezionare il ruolo e quindi fare clic su **Delete Role** (Elimina ruolo) nella barra delle azioni. Quando richiesto, confermare l'eliminazione.

## Creare e gestire ambiti

Quando si crea un sito, l'unico ambito disponibile è l'ambito "Tutti", che non può essere eliminato.

È possibile creare ambiti utilizzando la procedura descritta di seguito. È inoltre possibile creare ambiti quando si crea un amministratore; ogni amministratore deve essere associato ad almeno una coppia ruolo/ambito. Quando si creano o si modificano desktop, cataloghi di macchine, applicazioni o host, è possibile aggiungerli a un ambito esistente. Se non li si aggiunge a un ambito, rimangono parte dell'ambito "Tutto".

La creazione del sito non può essere inserita in un ambito così come gli oggetti di amministrazione (ambiti e ruoli) delegati. Tuttavia, gli oggetti che non è possibile inserire in un ambito sono inclusi nell'ambito "Tutto". Gli amministratori completi hanno sempre l'ambito Tutto. Le macchine, le azioni relative all'alimentazione, i desktop e le sessioni non vengono direttamente inseriti in ambiti. Agli amministratori possono essere assegnate autorizzazioni su questi oggetti tramite i cataloghi di computer associati o i gruppi di consegna.

Regole per la creazione e la gestione degli ambiti:

- I nomi di ambito possono contenere fino a 64 caratteri Unicode. I nomi dei ruoli non possono contenere: barra rovesciata, barra, punto e virgola, due punti, cancelletto, virgola, asterisco, punto interrogativo, segno di uguale, freccia sinistra o destra, barra verticale, parentesi quadra aperta o chiusa, parentesi tonda aperta o chiusa, virgolette o apostrofo.
- Le descrizioni degli ambiti possono contenere fino a 256 caratteri Unicode.

- Quando si copia o si modifica un ambito, tenere presente che la rimozione di oggetti dall'ambito può rendere tali oggetti inaccessibili all'amministratore. Se l'ambito modificato è associato a uno o più ruoli, assicurarsi che gli aggiornamenti dell'ambito non rendano inutilizzabile alcuna coppia ruolo/ambito.

Per creare e gestire gli ambiti, seguire questi passaggi:

1. Accedere a Web Studio, fare clic su **Administrators** nel riquadro a sinistra, quindi fare clic sulla scheda **Scopes**.
2. Seguire le istruzioni per l'attività da completare:
    - **Creare un ambito:** fare clic su **Create new Scope** (Crea nuovo ambito) nella barra delle azioni. Immettere un nome e una descrizione. Per includere tutti gli oggetti di un tipo particolare (ad esempio gruppi di consegna), selezionare il tipo di oggetto. Per includere oggetti specifici, espandere il tipo e selezionare i singoli oggetti (ad esempio, i gruppi di consegna utilizzati dal team vendite).
    - **Copiare un ambito:** selezionare l'ambito e quindi fare clic su **Copy Scope** (Copia ambito) nella barra delle azioni. Immettere un nome e una descrizione. Modificare i tipi di oggetto e gli oggetti in base alle esigenze.
    - **Modificare un ambito:** selezionare l'ambito e quindi fare clic su **Edit Scope** (Modifica ambito) nella barra delle azioni. Modificare il nome, la descrizione, i tipi di oggetto e gli oggetti in base alle esigenze.
    - **Eliminare un ambito:** selezionare l'ambito e quindi fare clic su **Delete Scope** (Elimina ambito) nella barra delle azioni. Quando richiesto, confermare l'eliminazione.

### Creare report

È possibile creare due tipi di report di amministrazione delegata:

- Un report HTML che elenca le coppie ruolo/ambito associate a un amministratore e le singole autorizzazioni per ogni tipo di oggetto (ad esempio gruppi di consegna e cataloghi macchine). È possibile generare questo report da Web Studio.

  Per creare questo report , seguire questi passaggi:

  1. Accedere a Web Studio, fare clic su **Administrators** nel riquadro a sinistra
  2. Selezionare un amministratore, quindi fare clic su **Create report** nella barra delle azioni.

  È inoltre possibile richiedere questo report durante la creazione, la copia o la modifica di un amministratore.
- Report HTML o CSV che associa tutti i ruoli predefiniti e personalizzati alle autorizzazioni. È possibile generare questo report eseguendo uno script PowerShell denominato OutputPermissionMapping.ps1.

Per eseguire questo script, è necessario essere un amministratore completo, un amministratore di sola lettura o un amministratore personalizzato con l'autorizzazione per la lettura dei ruoli. Lo script si trova in: Programmi\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts.

Sintassi:

```
OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-
AdminAddress string] [-Show] [CommonParameters]
```

| Parametro | Descrizione |
|---|---|
| -Help | Visualizza la Guida dello script. |
| -Csv | Specifica l'output CSV. Predefinito= HTML |
| -Path string | Dove scrivere l'output. Predefinito= stdout |
| -AdminAddress string | Indirizzo IP o nome host del Delivery Controller a cui connettersi. Predefinito= localhost |
| -Show | (Valido solo quando viene specificato anche il parametro -Path) Quando si scrive l'output in un file, -Show fa aprire l'output in un programma appropriato, ad esempio un browser Web. |
| CommonParameters | Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer e OutVariable. Per ulteriori informazioni, vedere la documentazione di Microsoft. |

Nell'esempio seguente viene scritta una tabella HTML in un file denominato Roles.html e la tabella viene aperta in un browser Web.

```
1 & "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
2 Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
3 -Path Roles.html  – Show
4 <!--NeedCopy-->
```

Nell'esempio seguente viene scritta una tabella CSV in un file denominato Roles.csv. La tabella non viene visualizzata.

```
1 & "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
2 Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
3  – CSV -Path Roles.csv
4 <!--NeedCopy-->
```

Dal prompt dei comandi di Windows, il comando di esempio precedente è:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
-CSV -Path Roles.csv"
<!--NeedCopy-->
```

## Delivery Controller

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Il Delivery Controller è il componente lato server responsabile della gestione dell'accesso utente, oltre alla mediazione e all'ottimizzazione delle connessioni. I controller forniscono inoltre i servizi di creazione di macchine che creano immagini di desktop e server.

Un sito deve avere almeno un controller. Dopo aver installato il controller iniziale, è possibile aggiungere altri controller al momento della creazione di un sito o in seguito. Si traggono due vantaggi principali dall'avere più di un controller in un sito.

- **Ridondanza:** come procedura consigliata, in un sito di produzione, è bene avere sempre almeno due controller su diversi server fisici. Se un controller fallisce, gli altri possono gestire le connessioni e amministrare il sito.
- **Scalabilità:** man mano che l'attività del sito cresce, aumenta anche l'utilizzo della CPU da parte dell'attività del controller e del database. Controller aggiuntivi consentono di gestire più utenti e più applicazioni e richieste desktop e possono migliorare la capacità di risposta complessiva.

Ciascun controller comunica direttamente con il database del sito. In un sito con più di una zona, i controller presenti in ogni zona comunicano con il database del sito nella zona principale.

> **Importante:**
>
> Non modificare il nome del computer o l'appartenenza al dominio di un controller dopo la configurazione del sito.

### Come si registrano i VDA con i controller

Prima di poter essere utilizzato, un VDA deve registrarsi (stabilire una comunicazione) con un Delivery Controller nel sito. Per informazioni sulla registrazione dei VDA, vedere Registrazione dei VDA con i controller.

### Aggiungere, rimuovere o spostare i controller

Per aggiungere, rimuovere o spostare un controller, è necessario disporre delle autorizzazioni del ruolo del server e del ruolo del database elencate nell'articolo Database.

L'installazione di un controller in un nodo in un cluster SQL o un'installazione di mirroring SQL non è supportata.

Quando si aggiunge un Delivery Controller a un sito, assicurarsi di aggiungere credenziali di accesso per quella macchina a qualsiasi SQL Server di replica utilizzato per la disponibilità elevata.

Se la distribuzione utilizza il mirroring del database:

- Prima di aggiungere, rimuovere o spostare un controller, assicurarsi che entrambi i database principali e mirroring siano in esecuzione. Inoltre, se si utilizzano script con SQL Server Management Studio, abilitare la modalità SQLCMD prima di eseguire gli script.
- Per verificare il mirroring dopo l'aggiunta, la rimozione o lo spostamento di un controller, eseguire il cmdlet PowerShell `Get-configdbconnection`. Tale cmdlet assicura che il partner di failover sia stato impostato nella stringa di connessione al mirror.

Dopo aver aggiunto, rimosso o spostato un controller:

- Se l'aggiornamento automatico è abilitato, i VDA ricevono un elenco aggiornato di controller entro 90 minuti.
- Se l'aggiornamento automatico non è abilitato, assicurarsi che l'impostazione dei criteri del controller o la chiave del Registro di sistema ListOfDDCs siano aggiornate per tutti i VDA. Dopo aver spostato un controller in un altro sito, aggiornare l'impostazione del criterio o la chiave del Registro di sistema su entrambi i siti.

#### Aggiungere un controller

È possibile aggiungere controller quando si crea un sito e successivamente. Non è possibile aggiungere controller installati con una versione precedente di questo software a un sito creato con questa versione.

1. Eseguire il programma di installazione su un server contenente un sistema operativo supportato. Installare il componente Delivery Controller e tutti gli altri componenti principali desiderati. Completare l'installazione guidata.

2. Se non si è ancora creato un sito, eseguire Citrix Site Manager su questo controller per creare un sito. L'indirizzo IP di questo controller viene aggiunto automaticamente al nuovo sito.

   Se si prevede di generare script che inizializzano i database, aggiungere i controller prima di generare gli script.

3. Se si è già creato un sito, seguire questi passaggi:

   a) Eseguire Citrix Site Manager su questo controller, fare clic su **Join an existing site** (Unisciti a un sito esistente) e digitare l'indirizzo di un controller del sito a cui si desidera partecipare.
   b) Eseguire Studio configuration tool per aggiungere il controller a Web Studio.

### Rimuovere un controller

La rimozione di un controller da un sito non disinstalla il software Citrix né alcun altro componente. Tale azione rimuove il controller dal database in modo che non possa più essere utilizzato per mediare le connessioni ed eseguire altre attività. Se si rimuove un controller, lo si può riaggiungere in un secondo momento nello stesso sito o in un altro sito. Un sito richiede almeno un controller, quindi non è possibile rimuovere l'ultimo controller elencato in Web Studio.

Quando si rimuove un controller da un sito, l'accesso del controller al server dei database non viene rimosso. Ciò evita di rimuovere potenzialmente un accesso utilizzato dai servizi di altri prodotti sulla stessa macchina. Se non è più necessario, l'accesso deve essere rimosso manualmente. L'autorizzazione del ruolo del server `securityadmin` è necessaria per rimuovere l'accesso.

Dopo aver rimosso un controller:

- I VDA che utilizzano l'aggiornamento automatico si registrano nuovamente con altri controller disponibili. Questa nuova registrazione si verifica solo se il meccanismo di aggiornamento automatico è abilitato e i VDA possono raggiungere altri controller (nella stessa zona secondaria del controller rimosso o nella zona primaria per le distribuzioni locali).
- Informazioni sul controller di aggiornamento in Citrix StoreFront. Per ulteriori informazioni, vedere Manage Controllers.
- In Citrix StoreFront, aggiornare gli URL di Secure Ticket Authority (STA) per l'accesso remoto tramite Citrix Gateway. Per maggiori informazioni, vedere Manage Secure Ticket Authorities.
- In Citrix Gateway, aggiornare tutti gli eventuali URL STA dei server virtuali. Per ulteriori informazioni, vedere Citrix Gateway.

> **Importante:**
>
> Non rimuovere il controller da Active Directory finché non lo si è rimosso dal sito.

1. Assicurarsi che il controller sia acceso in modo che Web Studio si carichi in meno di un'ora. Una volta che Web Studio carica il controller che si desidera rimuovere, assicurarsi che tutti i servizi che si trovano sul Controller siano in esecuzione e che il Controller sia spento.
2. Accedere a Web Studio e selezionare **Settings** nel riquadro a sinistra:
3. Individuare il riquadro **Delivery Controller** e fare clic su **Edit**.
4. Nella pagina **Manage Delivery Controller**, selezionare il controller che si desidera rimuovere.
5. Selezionare **Remove Controller** (Rimuovi controller). Se non si dispone dei ruoli e delle autorizzazioni corretti per il database, viene offerta la possibilità di generare uno script che consente all'amministratore del database di rimuovere il controller per l'utente.

   Web Studio esegue un controllo preliminare prima di rimuovere un controller. È possibile rimuovere un controller se è spento e non si trova nel seguente stato di servizio:

   - Unknown (Sconosciuto)
   - Errore in sospeso
   - Versione precedente
   - Versione più recente
   - Cambio di versione in corso
   - Caratteristiche obbligatorie mancanti

   Se il controller non è spento e si trova in uno degli stati di servizio indicati, Web Studio richiede di spegnere il controller.
6. È necessario rimuovere l'account macchina del controller dal server dei database. Prima di rimuoverlo, verificare che l'account non sia utilizzato da un altro servizio.

Dopo aver utilizzato Web Studio per rimuovere un controller, il traffico verso quel controller potrebbe rimanere attivo per un breve periodo di tempo per garantire il corretto completamento delle attività correnti. Se si desidera forzare la rimozione di un controller in breve tempo, Citrix consiglia di arrestare il server in cui è stato installato o di rimuovere quel server da Active Directory. Quindi, riavviare gli altri controller del sito per garantire che non ci siano ulteriori comunicazioni con il controller rimosso.

#### Spostare un controller in un'altra zona

Se il sito contiene più di una zona, è possibile spostare un controller in un'altra zona. Vedere Zones per informazioni su come questo spostamento può influire sulla registrazione dei VDA e su altre operazioni.

1. Selezionare **Zone** nel riquadro a sinistra.
2. Selezionare un'area nel riquadro centrale, quindi selezionare un controller.
3. Selezionare **Move Items** (Sposta elementi) nella barra delle azioni.

4. Nella pagina **Move Items** che viene visualizzata, selezionare la zona in cui si desidera portare il controller.
5. Fare clic su **Salva**.

### Spostare un VDA in un altro sito

Se è stato eseguito il provisioning di un VDA utilizzando Citrix Provisioning o il VDA è un'immagine esistente, è possibile spostare il VDA in un altro sito (dal sito 1 al sito 2) durante l'aggiornamento o quando si sposta in un sito di produzione un'immagine di VDA creata in un sito di test. I VDA sottoposti a provisioning mediante Machine Creation Services (MCS) non possono essere spostati da un sito all'altro. MCS non supporta la modifica del ListOfDDCs che un VDA controlla per registrarsi con un controller. I VDA sottoposti a provisioning mediante MCS controllano sempre il ListOfDDCs associato al sito in cui sono stati creati.

Esistono due modi per spostare un VDA in un altro sito: utilizzare il programma di installazione o i criteri Citrix.

**Programma di installazione** Eseguire il programma di installazione e aggiungere un controller, specificando il nome di dominio completo (voce DNS) di un controller nel sito 2.

Specificare controller nel programma di installazione solo quando non viene utilizzata l'impostazione del criterio dei controller.

**Editor dei criteri di gruppo** L'esempio seguente sposta più VDA da un sito a un altro.

1. Creare un criterio nel sito 1 che contenga le impostazioni seguenti, quindi filtrare il criterio a livello di gruppo di consegna per avviare una migrazione di VDA tra i siti a fasi.
    - Controller: contenenti FQDN (voci DNS) di uno o più controller nel sito 2.
    - Abilita l'aggiornamento automatico dei controller: impostato su Disabilitato.
2. Ogni VDA del gruppo di consegna viene avvisato del nuovo criterio entro 90 minuti. Il VDA ignora l'elenco dei controller che riceve (poiché l'aggiornamento automatico è disabilitato); seleziona uno dei controller specificati nel criterio, che elenca i controller nel sito 2.
3. Quando il VDA si registra correttamente con un controller nel sito 2, riceve il ListOfDDCs e le informazioni sui criteri del sito 2, che ha l'aggiornamento automatico abilitato per impostazione predefinita. Il controller con cui è stato registrato il VDA nel sito 1 non è nell'elenco inviato dal controller del sito 2. Quindi il VDA si registra nuovamente, scegliendo tra i controller inclusi nell'elenco del sito 2. Da quel momento in poi, il VDA viene aggiornato automaticamente con le informazioni del sito 2.

Per informazioni su come utilizzare l'Editor criteri di gruppo, consultate la documentazione dei criteri di Citrix.

## Supporto di IPv4/IPv6

January 7, 2024

Questa versione supporta distribuzioni di IPv4 puro, IPv6 puro e dual-stack che utilizzano reti IPv4 e IPv6 sovrapposte.

I seguenti componenti supportano solo IPv4. Tutti gli altri supportano IPv4 e IPv6.

- Citrix Provisioning
- Citrix Hypervisor
- Virtual Delivery Agent (VDA) non controllati dall'impostazione dei criteri **Only use IPv6 Controller registration** (Usa solo registrazione con IPv6 Controller)

Le comunicazioni IPv6 sono controllate con due impostazioni dei criteri Citrix relative alla connessione del VDA.

- **Impostazione principale che impone l'uso di IPv6:** Only use IPv6 Controller registration (Utilizzare solo la registrazione del controller IPv6).

  Questa impostazione dei criteri controlla il tipo di indirizzo utilizzato dal VDA per registrarsi con il Delivery Controller.

  Quando l'impostazione è abilitata, il VDA registra e comunica con il controller utilizzando un unico indirizzo IPv6 scelto in base all'ordine di precedenza seguente: indirizzo IP globale, Unique Local Address (ULA), indirizzo locale del collegamento (solo se non sono disponibili altri indirizzi IPv6).

  Quando l'impostazione è disabilitata, il VDA si registra e comunica con il controller utilizzando l'indirizzo IPv4 del computer. Questo è il valore predefinito.

  Se un team utilizza frequentemente una rete IPv6, pubblicare i desktop e le applicazioni per gli utenti di quel team in base a un'immagine o a un'unità organizzativa (OU) in cui è abilitata l'impostazione del criterio **Only use IPv6 Controller registration**.

  Se un team utilizza frequentemente una rete IPv4, pubblicare i desktop e le applicazioni di quegli utenti in base a un'immagine o a un'unità organizzativa che ha disabilitato l'impostazione del criterio **Only use IPv6 Controller registration**.

- **Impostazione dipendente che definisce una maschera di rete IPv6:** Controller registration IPv6 netmask (Maschera di rete IPv6 di registrazione controller).

Una macchina può avere più indirizzi IPv6. Questa impostazione dei criteri consente agli amministratori di limitare il VDA a una sottorete preferita, anziché a un IP globale, se ce n'è uno registrato. Questa impostazione specifica la rete in cui si registra il VDA. Il VDA si registra solo sul primo indirizzo corrispondente alla maschera di rete specificata.

Questa impostazione è valida solo quando è abilitata l'impostazione **Only use IPv6 Controller registration policy** (Utilizza solo la registrazione del controller IPv6). Impostazione predefinita= stringa vuota

### Considerazioni sulla distribuzione

Se l'ambiente contiene sia reti IPv4 che IPv6, creare configurazioni separate per i client solo IPv4 e per i client che possono accedere alla rete IPv6. È possibile utilizzare la denominazione, l'assegnazione manuale del gruppo Active Directory o i filtri SmartAccess per differenziare gli utenti.
La riconnessione della sessione potrebbe non riuscire se la connessione viene avviata su una rete IPv6 e si tenta di connettersi di nuovo da un client che ha solo accesso IPv4.

NOTA - Queste considerazioni non si applicano se la risoluzione DNSè abilitata

## Licenze per Citrix Virtual Apps and Desktops tramite Web Studio

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Da Web Studio, è possibile gestire e monitorare le licenze, se il server delle licenze si trova nello stesso dominio di Studio o in un dominio attendibile. Per informazioni sulle attività di licenza, vedere la documentazione sulle licenze e la sezione Licenze multi-tipo.

Nella tabella seguente sono elencate le edizioni e i modelli di licenza supportati:

| Prodotti | Edizioni | Modelli di licenza |
|---|---|---|
| Citrix Virtual Apps | Premium, Advanced, Standard | Simultanea |
| Citrix Virtual Desktops | Premium, Advanced, Standard | Utente/dispositivo e simultanea |

Per ulteriori informazioni, vedere Concurrent license e User/device license.

### Versione Current Release (CR) e Long Term Service Release (LTSR) supportata

La tabella seguente riporta la **versione minima LS compatibile** per Citrix Virtual Apps and Desktops, XenApp e XenDesktop. Per ulteriori informazioni sulle date del ciclo di vita dei prodotti Citrix, vedere la Matrice dei prodotti.

> **Importante:**
>
> Le informazioni riportate nella tabella seguente sono fornite solo per la compatibilità del prodotto. Citrix consiglia vivamente di utilizzare sempre l'ultima versione disponibile di Citrix License Server per beneficiare di eventuali miglioramenti funzionali o di sicurezza che potrebbe contenere.
>
> **Nota:**
>
> Il License Server VPX è obsoleto e non riceverà ulteriori correzioni di manutenzione o di sicurezza. Si consiglia ai clienti che utilizzano la versione 11.16.6 o precedenti di License Server VPX di eseguire la migrazione alla versione più recente di License Server per Windows appena possibile.

| Versione attuale | Versione LS minima compatibile |
|---|---|
| 2305 | 11.17.2.0 Build 35000 |
| 2303 | 11.17.2.0 Build 35000 |
| 2212 | 11.17.2.0 Build 35000 |
| 2209 | 11.17.2.0 Build 35000 |
| 2206 | 11.17.2.0 Build 35000 |
| 2203 | 11.17.2.0 Build 35000 |
| 2112 | 11.17.2.0 Build 35000 |
| 2109 | 11.17.2.0 Build 35000 |
| 2106 | 11.17.2.0 Build 35000 |
| 2103 | 11.16.3.0 Build 28000 |

| Rilascio servizio a lungo termine | Versione LS minima compatibile |
|---|---|
| 2203 LTSR | 11.17.2.0 Build 35000 |

| Rilascio servizio a lungo termine | Versione LS minima compatibile |
|---|---|
| 1912 LTSR | 11.16.3.0 Build 28000 |
| 7.15 LTSR | 11.15.0.0 Build 24100 |
| 7.6 LTSR | 11.14.0.1 Build 21103 |

Per informazioni sui prodotti legacy e sulle versioni dei prodotti, fare riferimento alla matrice dei prodotti legacy.

È necessario essere un amministratore delle licenze completo per completare le seguenti attività. Per visualizzare le informazioni sulla licenza in Web Studio, un amministratore deve disporre almeno dell'autorizzazione di amministrazione delegata per le licenze di lettura. I ruoli integrati Amministratore completo e Amministratore di sola lettura dispongono di tale autorizzazione.

### Scaricare e installare una licenza da Citrix utilizzando Web Studio

1. Accedere a Web Studio e selezionare **Licensing** nel riquadro a sinistra:
2. Selezionare **Allocate licenses** (Alloca licenze) nella barra delle azioni.
3. Immettete il codice di accesso alla licenza, ricevuto in un'e-mail da Citrix dopo l'acquisto o il rinnovo delle licenze.
4. Selezionare un prodotto e scegliere **Allocate Licenses**. Tutte le licenze disponibili per quel prodotto vengono assegnate e scaricate. Dopo aver assenato e scaricato tutte le licenze per un codice di accesso alle licenze specifico, non è possibile utilizzare nuovamente tale codice. Per effettuare altre transazioni con lo stesso codice, accedere a My Account.

### Aggiungere licenze memorizzate sul computer locale o sulla rete

1. Accedere a Web Studio e selezionare **Licensing** nel riquadro a sinistra:
2. Selezionare **Add Licenses** (Aggiungi licenze) nella barra delle azioni.
3. Individuare un file di licenza e aggiungerlo al server licenze.

### Cambiare il server licenze

1. Accedere a Web Studio e selezionare **Licensing** nel riquadro a sinistra:
2. Selezionare **Change License Server** (Modifica server licenze) nella barra delle azioni.
3. Digitare l'indirizzo del server licenze nel modulo*name:port*, dove "name" è un indirizzo DNS, NetBIOS o IP. Se non si specifica un numero di porta, viene utilizzata la porta predefinita (27000).

### Selezionare il tipo di licenza da utilizzare

- Quando si configura il sito, dopo aver specificato il server delle licenze, viene richiesto di selezionare il tipo di licenza da utilizzare. Se sul server non sono presenti licenze, viene selezionata automaticamente l'opzione di utilizzare il prodotto per un periodo di prova di 30 giorni senza licenza.
- Se sul server sono presenti licenze, ne vengono visualizzati i dettagli ed è possibile selezionarne una. In alternativa, è possibile aggiungere un file di licenza al server e selezionarlo.

### Modificare l'edizione del prodotto e il modello di licenza

1. Accedere a Web Studio e selezionare **Licensing** nel riquadro a sinistra:
2. Selezionare **Edit Product Edition** (Modifica edizione prodotto) nella barra delle azioni.
3. Aggiornare le opzioni appropriate.

Per accedere a License Administration Console, selezionare **License Administration Console** (Console di amministrazione licenze) nella barra delle azioni. La console viene visualizzata immediatamente oppure, se il dashboard è configurato come protetto da password, vengono richieste le credenziali di License Administration Console. Per informazioni dettagliate su come utilizzare la console, vedere la documentazione sulle licenze.

> **Nota:**
>
> Quando si cambia licenza in Web Studio, la modifica impiega fino a 5 minuti per essere visualizzata in Citrix Director. Ad esempio, se si passa da Advanced a Premium o viceversa.

### Aggiungere un amministratore delle licenze

1. Accedere a Web Studio e selezionare **Licensing** nel riquadro a sinistra:
2. Selezionare la scheda **Licensing Administrators** (Amministratori licenze).
3. Selezionare **Add licensing administrator** (Aggiungi amministratore licenze) nella barra delle azioni.
4. Individuare l'utente che si desidera aggiungere come amministratore e scegliere le autorizzazioni.

### Modificare le autorizzazioni di un amministratore delle licenze o eliminare un amministratore di licenze

1. Accedere a Web Studio e selezionare **Licensing** nel riquadro a sinistra:
2. Selezionare la scheda **Licensing Administrators** e selezionare l'amministratore.

3. Selezionare **Edit licensing administrator** (Modifica amministratore licenze) o **Delete licensing administrator** (Elimina amministratore licenze) nella barra delle azioni.

### Aggiungere un gruppo di amministratori di licenze

1. Accedere a Web Studio e selezionare **Licensing** nel riquadro a sinistra:
2. Selezionare la scheda **Licensing Administrators** (Amministratori licenze).
3. Selezionare **Add licensing administrator group** (Aggiungi gruppo amministratore licenze) nella barra delle azioni.
4. Individuare il gruppo da far agire come gruppo di amministratori delle licenze e scegliere le autorizzazioni. L'aggiunta di un gruppo Active Directory fornisce le autorizzazioni di amministratore delle licenze agli utenti di quel gruppo.

### Modificare le autorizzazioni di un gruppo di amministratori di licenze o eliminare un gruppo di amministratori di licenze

1. Accedere a Web Studio e selezionare **Licensing** nel riquadro a sinistra:
2. Selezionare la scheda **Licensing Administrators** e selezionare il gruppo di amministratori.
3. Selezionare **Edit licensing administrator group** (Modifica gruppo di amministratori delle licenze) o **Delete licensing administrator group** (Elimina gruppo di amministratori delle licenze) nella barra delle azioni.

### Visualizzare le informazioni sulla licenza

Accedere a Web Studio e selezionare **Licensing** nel riquadro a sinistra: Viene visualizzato un riepilogo dell'utilizzo della licenza e delle impostazioni per il sito con un elenco di tutte le licenze attualmente installate sul server licenze specificato.

Assicurarsi che le impostazioni di licenza per il sito, che includono il tipo di prodotto, l'edizione della licenza e il modello di licenza, corrispondano alle licenze utilizzate dal License Server configurato. In caso contrario, potrebbe essere necessario scaricare o allocare le licenze in uscita per corrispondere alle impostazioni di licenza del sito.

### Visualizzare gli avvisi di scadenza della licenza

Web Studio cerca le date di scadenza dei file di licenza in Citrix License Server. Web Studio avvisa gli amministratori nella scheda Overview se i file di licenza stanno per scadere o sono già scaduti.

### Collegamenti correlati

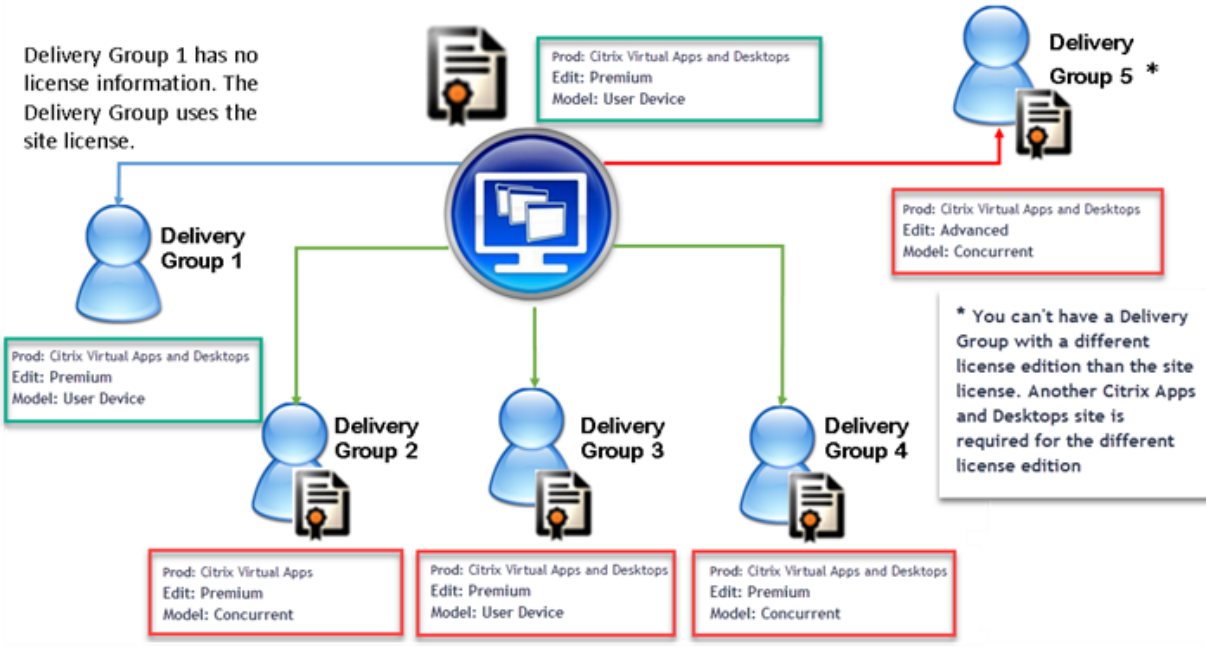
- Vedere Abbonamento Citrix on-premise per licenze al dettaglio annuali e a termine.
- Vedere Transition and Trade-Up (TTU) with Hybrid Rights.

## Licenze multi-tipo

January 7, 2024

Le licenze multi-tipo supportano il consumo di diversi tipi di licenza per i gruppi di consegna su un singolo sito di Citrix Virtual Apps and Desktops. Il **tipo** è una singola combinazione di ID prodotto (XDT o MPS) e Modello (UserDevice o Concurrent). I gruppi di consegna devono utilizzare la stessa Product Edition (PLT/Premium o ENT/Advanced) configurata a livello di sito. Tenere presenti le Considerazioni particolari alla fine di questo articolo quando si intende configurare le licenze multi-tipo per le distribuzioni di Citrix Virtual Apps and Desktops.

Se le licenze multi-tipo non sono configurate, è possibile utilizzare diversi tipi di licenza solo quando sono configurati per siti separati. I gruppi di consegna utilizzano la licenza del sito. Per importanti limitazioni di notifica quando sono configurate le licenza multi-tipo, vedere Considerazioni particolari.




Per determinare i gruppi di consegna che utilizzano i diversi tipi di licenza, utilizzare questi cmdlet Broker PowerShell:

- New-BrokerDesktopGroup

- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

Per installare le licenze, utilizzare:

- Citrix Studio
- Citrix Licensing Manager
- citrix.com

Le date di Customer Success Services sono specifiche per ciascun file di licenza e per ciascun prodotto e modello. I gruppi di consegna impostati in modo diverso potrebbero avere date di Customer Success Services diverse fra loro.

### Considerazioni particolari

Le licenze multi-tipo hanno funzionalità diverse rispetto alle normali licenze di Citrix Virtual Apps and Desktops.

Non ci sono avvisi e notifiche da parte di Director o Studio per i gruppi di consegna configurati per utilizzare un tipo diverso dalla configurazione del sito:

- Nessuna informazione quando si avvicinano i limiti della licenza o l'attivazione o la scadenza del periodo di tolleranza supplementare.
- Nessuna notifica quando un gruppo specifico ha un problema.

I gruppi di consegna configurati per licenze multi-tipo consumano SOLO quel tipo di licenza e non tornano alla configurazione del sito quando sono completamente consumati.

Sebbene i nomi delle versioni di licenza Citrix Virtual Apps Standard e Citrix Virtual Desktops Standard indichino che sono entrambe Standard, non sono la stessa edizione. Le licenze multi-tipo non sono disponibili con le licenze Citrix Virtual Apps Standard e Citrix Virtual Desktop Standard.

### Matrice di compatibilità delle licenze

Questa tabella indica in dettaglio i vecchi nomi dei prodotti, i nuovi nomi di prodotto e i nomi delle funzionalità associate. Le quattro colonne di compatibilità specificano quali combinazioni di prodotti e modelli di licenza sono compatibili con le licenze multi-tipo. CCU e CCS indicano le licenze simultanee e UD indica le licenze utente/dispositivo.

| Old Name | New Name | Feature | Multi-type licensing compatibility | | | |
|---|---|---|---|---|---|---|
| | | | STD | ADV | ENT | PLT |
| Citrix XenApp Standard | Citrix XenApp Standard | MPS_STD_CCU | X | | | |
| Citrix XenApp Advanced | Citrix Virtual Apps Standard | MPS_ADV_CCU | | X | | |
| Citrix XenApp Enterprise | Citrix Virtual Apps Advanced | MPS_ENT_CCU | | | X | |
| Citrix XenApp Platinum | Citrix Virtual Apps Premium | MPS_PLT_CCU | | | | X |
| Citrix XenApp Advanced | Citrix Virtual Apps Standard | MPS_ADV_CCU | | X | | |
| Citrix XenDesktop VDI Edition (XDT-U) | Citrix Virtual Desktops Standard- Per User/Device | XDT_STD_UD | X | | | |
| Citrix XenDesktop VDI Edition (XDT-C) | Citrix Virtual Desktops Standard - Concurrent | XDT_STD_CCS | X | | | |
| Citrix XenDesktop Enterprise Edition (XDT-C) | Citrix Virtual Apps and Desktops Advanced - Concurrent | XDT_ENT_CCS | | | X | |
| Citrix XenDesktop Enterprise Edition (XDT-U) | Citrix Virtual Apps and Desktops Advanced - Per User/Device | XDT_ENT_UD | | | X | |
| Citrix XenDesktop Platinum Edition (XDT-C) | Citrix Virtual Apps and Desktops Premium - Concurrent | XDT_PLT_CCS | | | | X |
| Citrix XenDesktop Platinum Edition (XDT-U) | Citrix Virtual Apps and Desktops Premium - Per User/Device | XDT_PLT_UD | | | | X |

### SDK PowerShell Broker

L'oggetto **DesktopGroup** dispone di queste due proprietà che è possibile manipolare utilizzando i cmdlet New-BrokerDesktopGroup e Set-BrokerDesktopGroup associati.

| Nome | Valore | Restrizione |
|---|---|---|
| LicenseModel | Parametro (Concurrent [simultanea] o UserDevice [UtenteDispositivo]) che specifica il modello di licenza per il gruppo. Se non viene specificato nulla, viene utilizzato il modello di licenza a livello di sito. | Se l'interruttore di funzionalità è disabilitato, il tentativo di impostare una proprietà ha esito negativo. |
| ProductCode | Stringa di testo XDT (per Citrix Virtual Desktops) o MPS (per Citrix Virtual Apps) che specifica l'ID prodotto di licenza per il gruppo. Se non viene specificato nulla, viene utilizzato il codice prodotto a livello di sito. | Se l'interruttore di funzionalità è disabilitato, il tentativo di impostare una proprietà ha esito negativo. |

Per ulteriori informazioni su LicenseModel e ProductCode, vedere about_broker_licensing.

#### New-BrokerDesktopGroup

Crea un gruppo desktop per la gestione dell'intermediazione di gruppi di desktop. Per ulteriori informazioni su questo cmdlet, vedere https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/.

#### Set-BrokerDesktopGroup

Disabilita o abilita un gruppo di desktop di intermediazione esistente o ne modifica le impostazioni. Per ulteriori informazioni su questo cmdlet, vedere https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/

#### Get-BrokerDesktopGroup

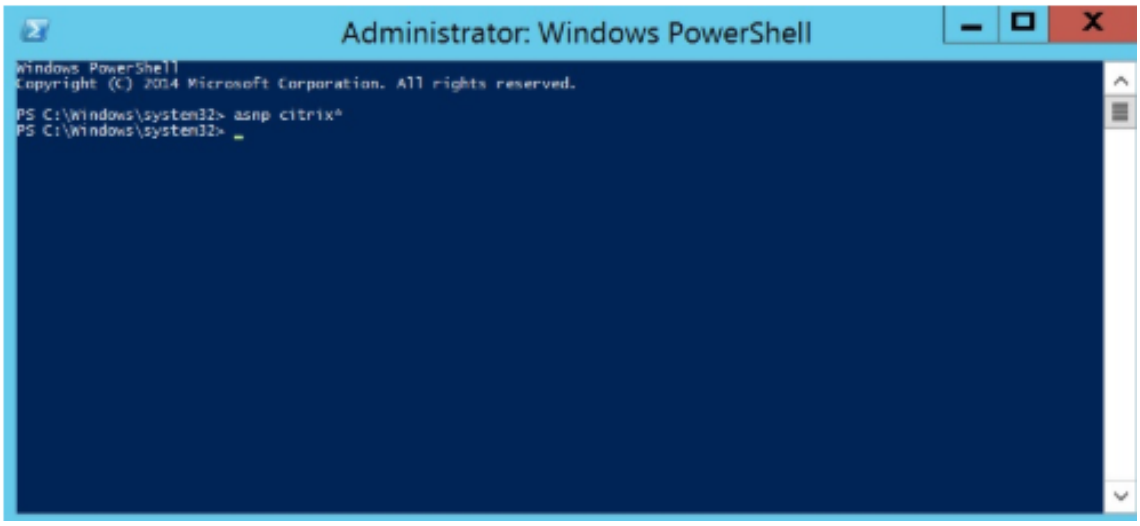
Recupera i gruppi desktop che corrispondono ai criteri specificati. L'output del cmdlet Get-BrokerDesktopGroup include le proprietà **ProductCode** e **LicenseModel** del gruppo. Se le proprietà non sono state impostate utilizzando New-BrokerDesktopGroup o Set-BrokerDesktopGroup, vengono restituiti valori nulli. Se in caso di valori nulli, vengono utilizzati il modello di licenza e il codice prodotto a livello di sito. Per ulteriori informazioni su questo cmdlet, vedere https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/.

### Configurare diversi prodotti e modelli di licenza per gruppo di consegna

> **Nota:**
>
> non è possibile configurare due o più tipi diversi di prodotti, edizioni o modelli di licenza configurati su un singolo gruppo di consegna. Se si dispone di diversi tipi di prodotti, edizioni o modelli di licenza, configurarli in gruppi di consegna separati.

1. Aprire PowerShell con diritti di amministrazione e aggiungere lo snap-in Citrix.

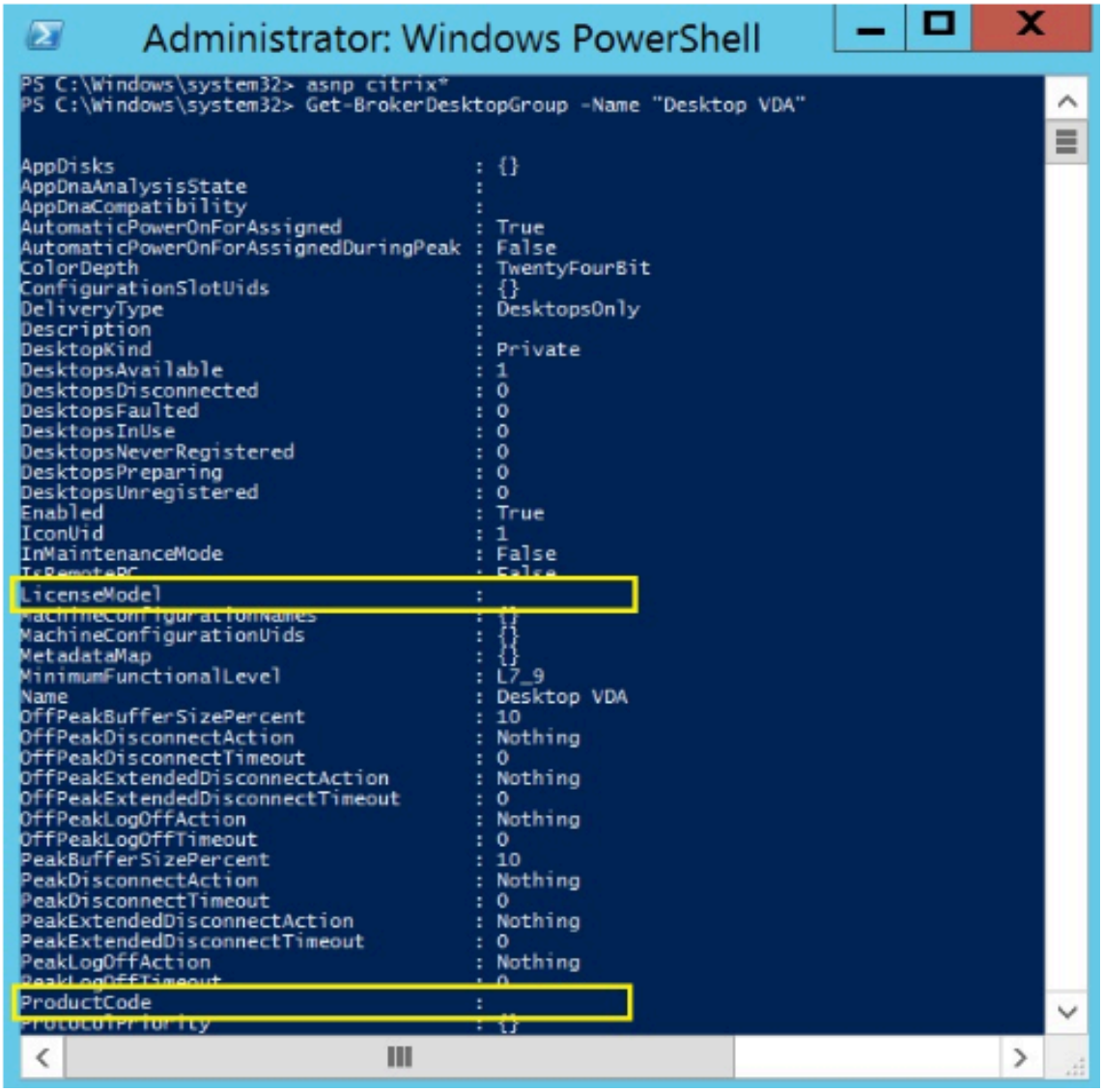
 




2. Eseguire il comando **Get-BrokerDesktopGroup** —**Name** “**DeliveryGroupName**” per visualizzare la configurazione corrente della licenza. Trovare i parametri **LicenseModel** e **ProductCode**. Se non si erano configurati questi parametri prima, potrebbero essere vuoti.

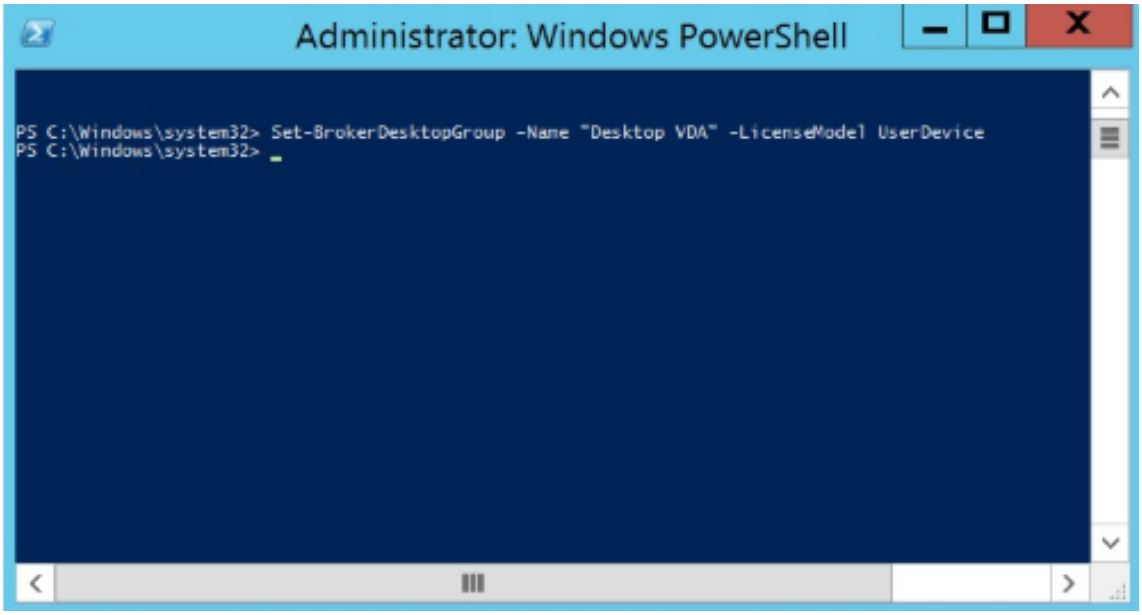
   > **Nota:**
   >
   > Se un gruppo di consegna non ha le informazioni sulla licenza impostate, l’impostazione predefinita è **Site level Site license** (Licenza sito a livello di sito).

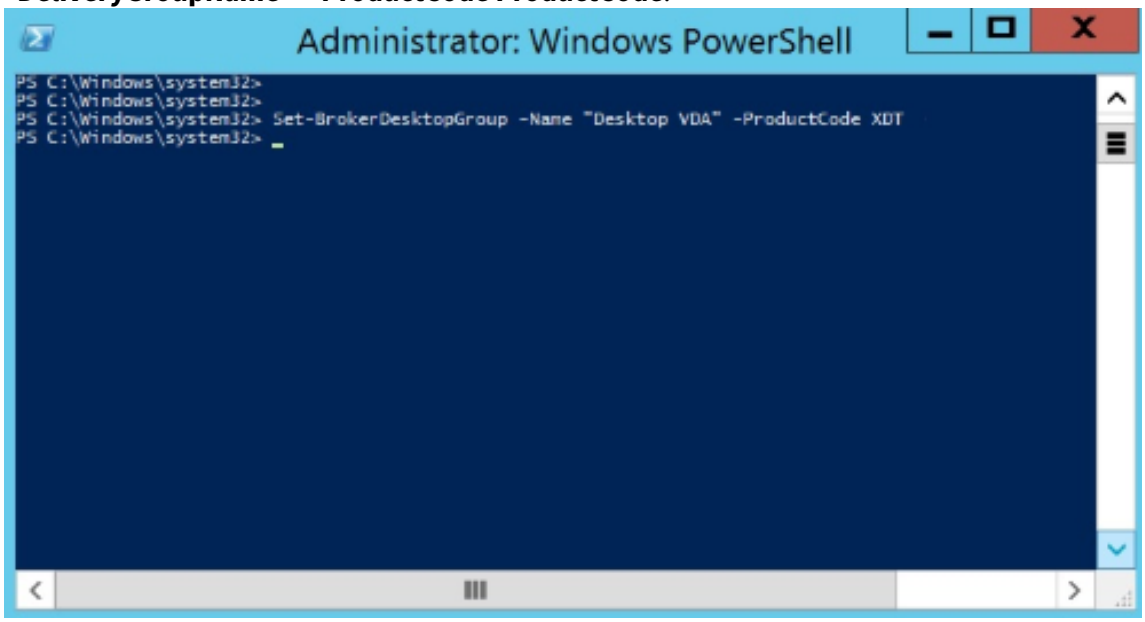



3. Modificare il modello di licenza eseguendo il comando: **Set-BrokerDesktopGroup —Name "DeliveryGroupName"—LicenseModel LicenseModel**.



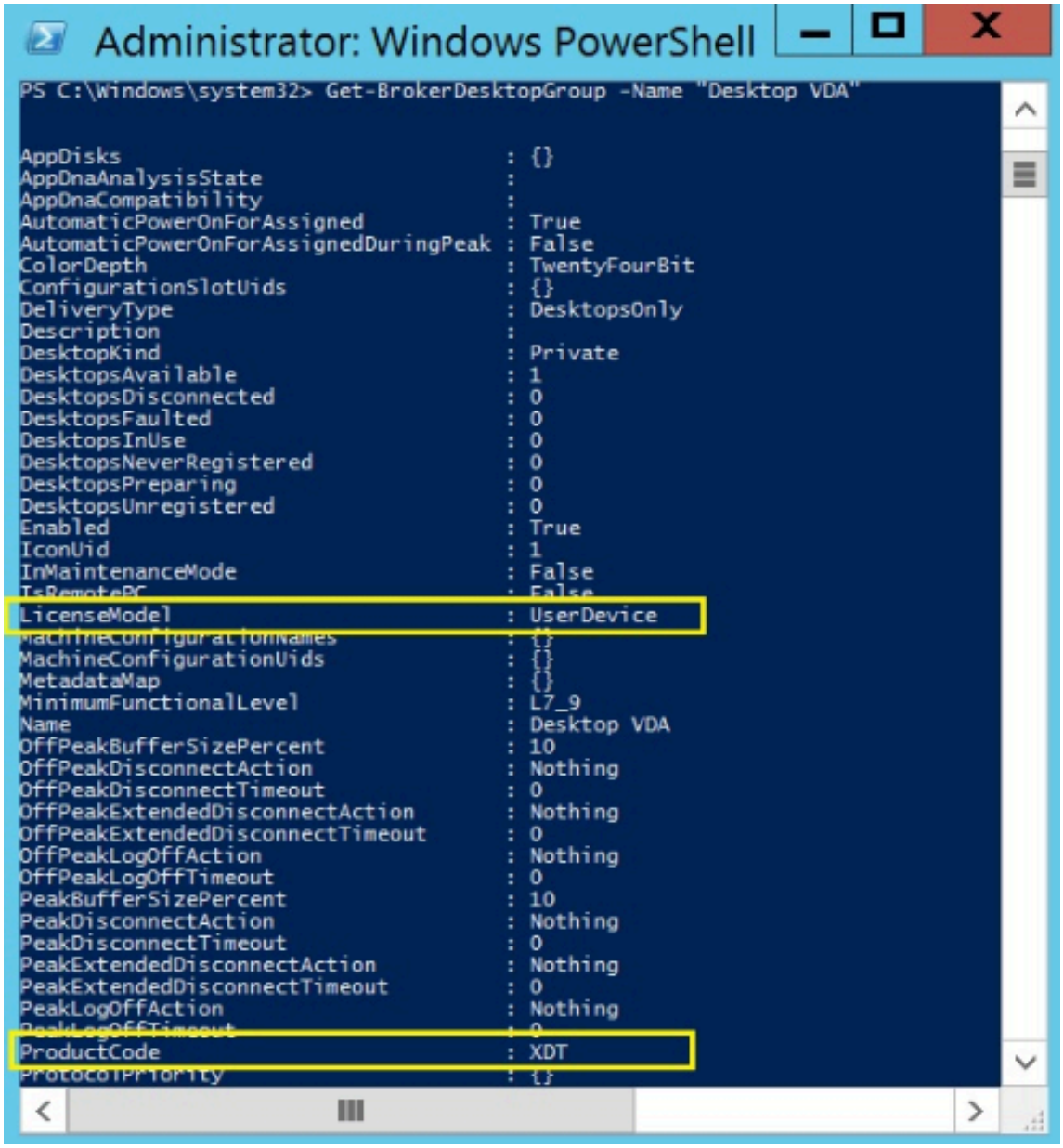

4. Modificare il prodotto con licenza eseguendo il comando: **Set-BrokerDesktopGroup** —**Name "DeliveryGroupName"**—**ProductCode ProductCode**.




5. Immettere il comando **Get-BrokerDesktopGroup** —**Name "DeliveryGroupName"** per convalidare le modifiche.

> **Nota:**
>
> Non è possibile combinare edizioni diverse nello stesso sito. Ad esempio, le licenze Premium e Advanced. Sono necessari più siti se si dispone di licenze con diverse edizioni.

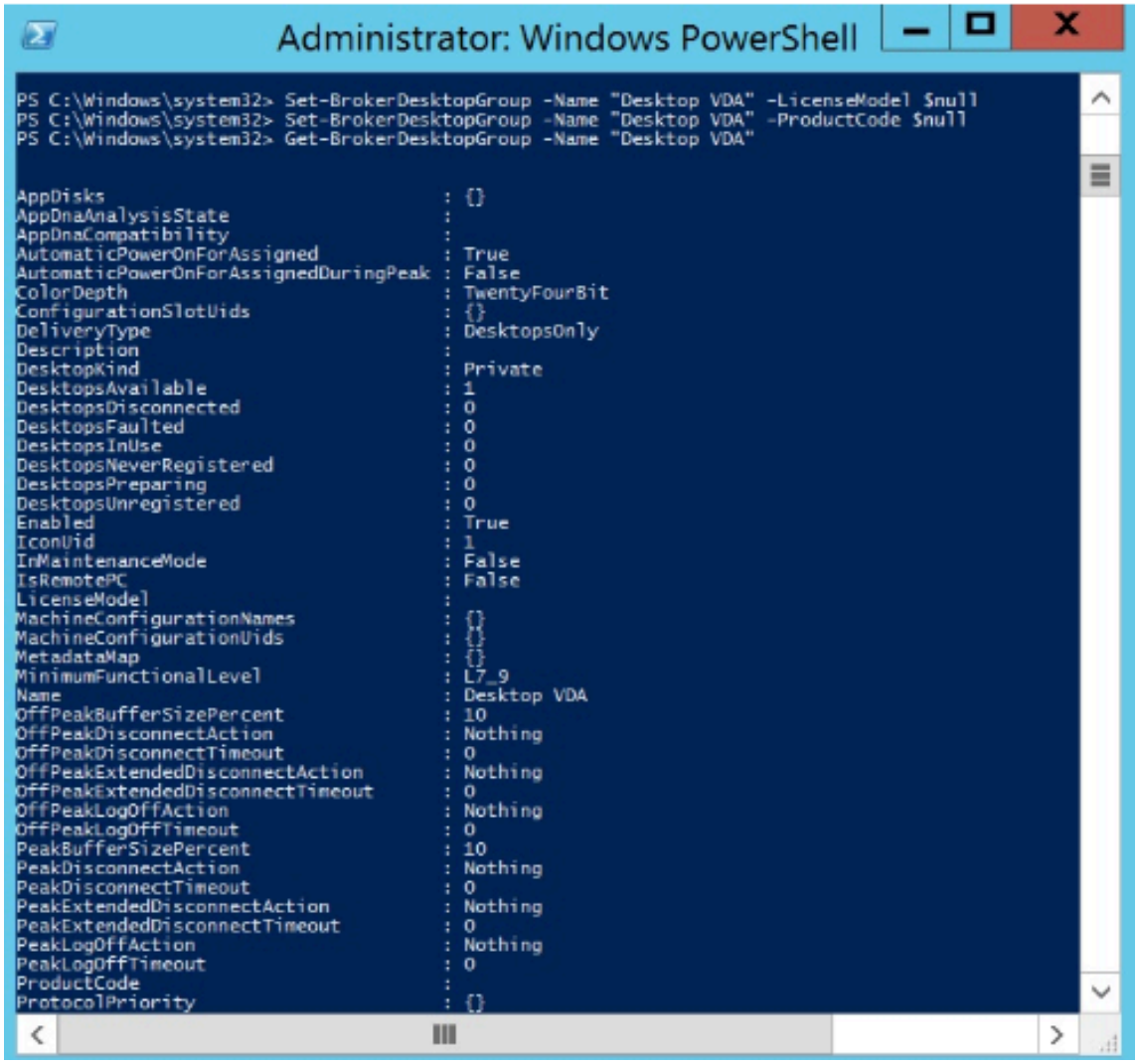
 




6. Rimuovere la configurazione della licenza eseguendo gli stessi comandi **Set-BrokerDesktopGroup** descritti nei passaggi precedenti e impostare il valore su **$null**.

> **Nota:**
>
> Studio non visualizza la configurazione della licenza per ciascun gruppo di consegna. Utilizzare PowerShell per visualizzare la configurazione corrente.




### Esempio

Questo esempio di cmdlet PowerShell illustra l'impostazione di licenze multi-tipo per due gruppi di consegna esistenti e crea e imposta un terzo gruppo di consegna.

Per visualizzare il prodotto concesso su licenza e il modello di licenza associati a un gruppo di consegna, utilizzare il cmdlet **Get-BrokerDesktopGroup** PowerShell.

1. Abbiamo impostato il primo gruppo di consegna per XenApp e per Concurrent (modello di licenza simultanea).

   **Set-BrokerDesktopGroup -Name "Delivery group for Citrix Virtual Apps Premium Concurrent"(Gruppo di consegna per Citrix Virtual Apps Premium simultanea) - ProductCode MPS -LicenseModel Concurrent**

2. Abbiamo impostato il secondo gruppo di consegna per XenDesktop e Concurrent.

**Set-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium Concurrent”(Gruppo di consegna per Citrix Virtual Desktops Premium simultanea) -ProductCode XDT -LicenseModel Concurrent**

3. Creiamo e impostiamo il terzo gruppo di consegna per XenDesktop e UserDevice.

   **New-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium UserDevice”(Gruppo di consegna per Citrix Virtual Desktops Premium UserDevice) -PublishedName “MyDesktop”-DesktopKind Private -ProductCode XDT -LicenseModel UserDevice**

## Domande frequenti per le licenze

January 7, 2024

> **Nota:**
>
> - Per le risorse di continuità aziendale correlate alla pandemia di COVID-19, vedere CTX27055.
> - Per informazioni generali sul mantenimento della continuità aziendale, vedere Business Continuity —on demand.
> - Per ulteriori informazioni sull’attuale Citrix License Server, vedere Licenze.

### Licenze Citrix

#### Come posso ottenere il mio file di licenza?

Inviamo il codice di accesso alla licenza in un messaggio e-mail. Esistono tre modi per generare file di licenza utilizzando il codice di accesso alla licenza:

- La pagina **Manage Licenses** (Gestisci licenze) dalla pagina MyAccount su `citrix.com`. Per ulteriori informazioni, vedere Gestire le licenze su citrix.com.
- Web Studio per allocare l’acquisto e il file di licenza viene installato automaticamente su Citrix License Server.
- Citrix Licensing Manager all’interno di Citrix License Server per allocare l’acquisto e installare il file di licenza. Per ulteriori informazioni, vedere Installare le licenze.

### Come assegnare la licenza su myaccount?

Vedere Allocate licenses.

### Come aggiungere licenze assegnate al server licenze?

Vedere Modify licenses.

### Quali porte TCP utilizzano le licenze Citrix?

- Il numero della porta del License Server è 27000
- Il numero di porta del daemon del fornitore è 7279
- Il numero della porta Web della console di gestione è 8082
- Il numero della porta di Web Service for Licensing è 8083

### Cos'è Citrix License Server?

Citrix License Server è un sistema che consente di condividere le licenze in tutta la rete. Per ulteriori informazioni, vedere Licensing operations overview.

### È possibile virtualizzare Citrix License Server o unirlo a un cluster?

Sì. È possibile virtualizzare Citrix License Server o unirlo a un cluster. Per ulteriori informazioni, vedere Clustered License Servers.

### Quali vantaggi si rendono disponibili se virtualizzo Citrix License Server?

La virtualizzazione di Citrix License Server fornisce una soluzione ridondante. Questa soluzione consente la mobilità tra più server fisici senza la necessità di tempi di inattività.

### Ci sono limitazioni da considerare se virtualizzo Citrix License Server?

N.

### Citrix License Server gestisce tutte le licenze per la distribuzione di Citrix Virtual Apps and Desktops?

Citrix License Server gestisce tutte le licenze ricevute per Citrix Virtual Apps and Desktops, ad eccezione delle licenze che si trovano in Premium Edition utilizzate con Citrix Gateway. I server di licenze integrati nelle appliance di rete come richiesto per i dispositivi di rete orientati alla sicurezza gestiscono tali licenze.

### Cos'è Citrix Licensing Manager?

Citrix Licensing Manager consente il download e l'allocazione dei file di licenza dal License Server su cui è stato installato Citrix Licensing Manager. Citrix Licensing Manager è il metodo di gestione del License Server consigliato e consente quanto segue:

- Registrazione del codice breve del License Server su Citrix Cloud e facile rimozione della registrazione.
- Configurare account utente e gruppo.
- Utilizzare il dashboard per visualizzare le licenze installate, in uso, scadute e disponibili e le date di Customer Success Services.
- Esportare i dati di utilizzo delle licenze per l'utilizzo nei rapporti.
- Configurare il periodo di conservazione dei dati di utilizzo storici. Il periodo di conservazione dei dati predefinito è di 180 giorni.
- Installazione semplificata dei file di licenza sul License Server utilizzando un codice di accesso alla licenza o un file scaricato.
- Abilitare e disabilitare il periodo di tolleranza supplementare.
- Configurare Customer Experience Improvement Program (CEIP) e Call Home
- Controlla automaticamente o manualmente le licenze di rinnovo di Customer Success Services e avvisa o installa le licenze se trovate.
- Notifica lo stato del License Server: licenza di avvio mancante, problemi di tempo, errori di caricamento.
- Modificare queste porte:
  - License Server (impostazione predefinita 27000)
  - Vendor Daemon (impostazione predefinita 7279)
  - Web Services for Licensing (impostazione predefinita 8083)

Per ulteriori informazioni, vedere Citrix Licensing Manager.

### Dov'è Citrix License Administration Console?

La License Administration Console non è più supportata ed è stata rimossa dal License Server versione 11.16.6. Si consiglia di utilizzare Citrix Licensing Manager.

È possibile utilizzare Studio per gestire e monitorare le licenze, a condizione che il License Server si trovi nello stesso dominio di Studio o in un dominio attendibile.

Per ulteriori informazioni, vedere Citrix Licensing Manager.

#### Cos'è il periodo di assegnazione della licenza?

Il periodo di assegnazione della licenza è il termine in cui una licenza Citrix Virtual Apps and Desktops viene assegnata a un utente o a un dispositivo. Il periodo di assegnazione della licenza predefinito è di 90 giorni.

#### Come faccio a sapere quante licenze ha acquistato la mia organizzazione?

Tutte le licenze acquistate sono disponibili per la revisione e l'accesso in qualsiasi momento (24 ore su 24, 7 giorni su 7) dalla casella degli strumenti sicura **Manage Licenses** (Gestisci licenze) nella pagina **Il mio account** in https://www.citrix.com.

#### Come faccio a sapere quante licenze sono in uso in qualsiasi momento?

Citrix Licensing Manager e Studio forniscono dettagli in tempo reale sull'utilizzo della licenza.

#### Ripristino d'emergenza e manutenzione di License Server

Per informazioni sul ripristino d'emergenza e la manutenzione del License Server, vedere Disaster recovery and maintenance nella documentazione di Citrix Licensing.

### Licenze di Citrix Virtual Apps and Desktops

#### Come viene concesso in licenza Citrix Virtual Apps and Desktops?

Il sistema di concessione licenza di Citrix Virtual Apps and Desktops offre modelli di licenza per utente/dispositivo e simultanei.

**Utente/dispositivo:**

Il modello utente/dispositivo flessibile si allinea a:

- Utilizzo desktop a livello aziendale.
- Licenza di virtualizzazione desktop Microsoft sottostante.
- Licenze simultanee per clienti con utenti che necessitano solo di accesso occasionale ai desktop e alle app virtuali.

La licenza utente/dispositivo consente agli utenti di accedere ai desktop e alle app virtuali da un numero illimitato di dispositivi. Le licenze per dispositivo consentono un numero illimitato di accesso dell'utente ai desktop e alle app virtuali da un singolo dispositivo. Questo approccio offre la massima flessibilità e migliora l'allineamento alle licenze Microsoft per la virtualizzazione dei desktop.

> **Importante:**
>
> Non è possibile allocare manualmente le licenze a un utente o a un dispositivo. Le licenze vengono assegnate da License Server o dal servizio cloud. Con la licenza utente/dispositivo, una volta assegnata una licenza, questa non può essere assegnata a un altro utente fino a dopo 90 giorni di inattività.

**Simultanee:**

Le licenze simultanee consentono la connessione a un numero illimitato di app e desktop virtuali per qualsiasi utente e dispositivo. Una licenza viene consumata solo durante una sessione attiva. Se la sessione si disconnette o viene terminata, la licenza viene riportata nel pool.

Per ulteriori informazioni sulle licenze utente/dispositivo, vedere User/device license e per informazioni sulle licenze simultanee vedere Concurrent license.

### È possibile provare Citrix Virtual Apps and Desktops prima di acquistare le licenze?

Sì. È possibile scaricare il software Citrix Virtual Apps and Desktops ed eseguirlo in modalità di prova. La modalità di prova consente di utilizzare Citrix Virtual Apps and Desktops in locale per 30 giorni, per 10 connessioni, senza licenza. Per ulteriori informazioni, vedere Licenze di valutazione.

Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops) per Citrix Cloud è disponibile per il servizio di prova basato sull'approvazione. Rivolgersi al proprio rappresentante Citrix per ulteriori dettagli.

### In che modo Citrix definisce la simultaneità per Citrix Virtual Apps and Desktops?

Il modello di simultaneità di Citrix Virtual Apps and Desktops consente una sola connessione a un numero illimitato di app e desktop virtuali per qualsiasi utente e dispositivo. Una licenza viene consumata solo durante una sessione attiva. Se la sessione si disconnette o viene terminata, la licenza viene riportata nel pool per essere riemessa. Per ulteriori informazioni, vedere Concurrent license.

### Posso distribuire più edizioni di licenze Citrix Virtual Apps and Desktops su un License Server comune?

Sì. License Server gestisce contemporaneamente licenze per Citrix Virtual Apps and Desktops. Si consiglia di installare la versione più recente di License Server. Se non si è certi che la versione di License Server sia la più aggiornata, verificarla confrontando la propria versione con il numero presente sul sito di download di Citrix.

**Un singolo sito può utilizzare le licenze di Citrix Virtual Apps che quelle di Citrix Virtual Apps and Desktops?**

A seconda della versione, un singolo sito Citrix Virtual Apps o Citrix Virtual Apps and Desktops può supportare entrambi i modelli di licenza: utente/dispositivo o simultanea. Un singolo sito Citrix Virtual Apps o Citrix Virtual Apps and Desktops può supportare una sola edizione. Per ulteriori informazioni, vedere Licenze multi-tipo.

Le versioni minime che supportano le licenze multi-tipo sono XenApp e XenDesktop 7.15 Long Term Service Release (LTSR) e Citrix Virtual Apps and Desktops 7 1808.

**È possibile selezionare Citrix Virtual Apps simultaneo come modello di prodotto se sono installate licenze simultanee di Citrix Virtual Apps and Desktops o Citrix Virtual Apps and Desktops sul License Server?**

Se si utilizza Citrix Virtual Apps come funzionalità di Citrix Virtual Apps and Desktops Advanced o Premium Edition, il modello di licenza di Citrix Virtual Apps è lo stesso dell'Advanced o Premium Edition di Citrix Virtual Apps and Desktops. Se si è acquistato Citrix Virtual Apps and Desktops, configurare la licenza come Citrix Virtual Apps and Desktops anche se si prevede di utilizzare solo la funzionalità Citrix Virtual Apps. Selezionare Citrix Virtual Apps come modello di prodotto solo se sono installate licenze autonome simultanee di Citrix Virtual Apps sul License Server.

**Quali componenti del prodotto sono inclusi in ogni edizione di Citrix Virtual Apps e di Citrix Virtual Apps and Desktops?**

Per uno schema completo delle funzionalità per edizione, vedere Citrix Virtual Apps and Desktops features.

**Come posso dotare di licenza gli ambienti Citrix Virtual Desktops in conformità con l'EULA di Citrix Virtual Apps and Desktops?**

Per distribuire Citrix Virtual Apps and Desktops in base al modello di licenza utente/dispositivo o simultaneo in conformità con l'EULA di Citrix Virtual Apps and Desktops, applicare i file di licenza al License Server. Il License Server controlla e monitora la conformità delle licenze. Consigliamo di configurare il prodotto in base a ciò che si è acquistato. Ad esempio, se si acquista Citrix Virtual Apps and Desktops Premium, ma si desidera utilizzare solo la funzionalità Citrix Virtual Apps, configurare il prodotto in Citrix Virtual Apps and Desktops per soddisfare la conformità. Per ulteriori informazioni, vedere il Product License Compliance Center.

**Come posso dotare di licenza gli ambienti Citrix Virtual Apps in conformità con l'EULA di Citrix Virtual Apps?**

Per distribuire Citrix Virtual Apps secondo il modello di licenza simultanea in conformità con l'EULA di Citrix Virtual Apps, applicare i file di licenza al License Server. Il License Server controlla e monitora la conformità delle licenze.

**Esiste un requisito di licenza per le opzioni di servizio Citrix Virtual Apps and Desktops: Long Term Service Release (LTSR) o Current Release (CR)?**

Le opzioni di servizio di Citrix Virtual Apps and Desktops, quali la Long Term Service Release, sono un vantaggio del programma Customer Success Services. È necessario disporre di Customer Success Services attivo per beneficiare dei vantaggi della LTSR. Per ulteriori informazioni, vedere Citrix Virtual Apps, Citrix Virtual Apps and Desktops e Citrix Hypervisor Servicing Options.

**Come funzionano le ore in pool del servizio Remote Browser Isolation (RBI)?**

Quando si acquista un minimo di 25 utenti del servizio, si ricevono 5000 ore di diritti per utilizzare il servizio, in comune tra tutti gli utenti. Gli acquisti successivi di diritti utente non aumentano il diritto alle ore in comune. Per aumentare le ore di servizio a cui si ha diritto, acquistare pacchetti aggiuntivi.

**Posso usare Remote PC Access con licenze CCU?**

Sì.

Per informazioni su Remote PC Access, vedere Accesso remoto al PC.

## Licenze utente o dispositivo

**In che modo Citrix assegna licenze agli utenti nel modello di licenza utente/dispositivo?**

Con il modello di licenza utente/dispositivo, il License Server assegna la licenza a un ID utente univoco. Consente a un singolo utente connessioni illimitate da dispositivi illimitati. Se un utente si connette a un desktop o a un dispositivo, l'utente richiede una licenza assegnatagli per accedere a un desktop o un'applicazione virtuale. Il License Server o il servizio cloud assegna la licenza. Non è possibile assegnare queste licenze manualmente. La licenza viene assegnata all'utente, non al dispositivo condiviso. Una volta assegnata una licenza, questa non può essere assegnata a un altro utente fino a dopo 90 giorni di inattività. Per ulteriori informazioni, vedere Licenza utente/dispositivo.

### In che modo Citrix definisce un dispositivo con licenza nel modello di licenza utente/dispositivo?

Un dispositivo con licenza richiede un ID dispositivo endpoint univoco. Nel modello utente/dispositivo un dispositivo è qualsiasi apparecchiatura autorizzata per l'uso da parte di qualsiasi individuo per accedere alle istanze di Citrix Virtual Apps and Desktops. Per un dispositivo condiviso, una singola licenza utente/dispositivo di Citrix Virtual Apps and Desktops può supportare più utenti che condividono il dispositivo. Ad esempio, un dispositivo condiviso può essere una workstation in classe o una workstation clinica in un ospedale.

### Posso convertire le mie licenze simultanee di Citrix Virtual Desktops Standard Edition nel modello utente/dispositivo?

Non è possibile convertire le licenze simultanee di Citrix Virtual Desktops Standard Edition in licenze per utente/dispositivo Citrix Virtual Desktops Standard Edition. Analogamente, non è possibile convertire le licenze utente/dispositivo di Citrix Virtual Desktops Standard Edition in licenze simultanee di Citrix Virtual Desktops Standard Edition.

Se si dispone di licenze simultanee di Citrix Virtual Desktops Standard Edition e si desidera il modello di licenza utente/dispositivo, eseguire l'aggiornamento a Citrix Virtual Apps and Desktops Advanced o Premium Edition.

| Da | A standard simultanea | A standard utente/dispositivo | Ad avanzata utente/dispositivo | A Premium utente/dispositivo |
|---|---|---|---|---|
| Licenze simultanee Citrix Virtual Desktops Standard Edition | N/A | La conversione da simultanee a utente/dispositivo NON è consentita | Non è possibile convertire i modelli di licenza, ma è possibile eseguire l'aggiornamento a Citrix Virtual Apps and Desktops Advanced o Premium Edition. | Non è possibile convertire i modelli di licenza, ma è possibile eseguire l'aggiornamento a Citrix Virtual Apps and Desktops Advanced o Premium Edition. |
| Licenze per utente/dispositivo di Citrix Virtual Desktops Standard Edition | La conversione da utente/dispositivo a simultanea NON è consentita | N/A | N/A | N/A |

**Quali sono le differenze di funzionamento fra licenze simultanee e le licenze utente/dispositivo?**

Basiamo le licenze simultanee sulle connessioni simultanee dei dispositivi. Una licenza simultanea è in uso solo quando un dispositivo ha stabilito una connessione attiva. Una volta terminata la connessione, la licenza concorrente ritorna al pool di licenze per l'uso immediato. Consigliamo questo modello di licenza per l'utilizzo occasionale. Le licenze utente/dispositivo vengono noleggiate per un periodo e non sono disponibili per altri utenti fino alla scadenza del contratto di locazione.

**Con il modello utente/dispositivo, possiamo assegnare licenze sia agli utenti che ai dispositivi della stessa azienda?**

Sì. Possono essere presenti entrambi i tipi nella stessa azienda. License Server assegna in modo ottimale licenze a utenti o dispositivi in base all'utilizzo. Non è possibile assegnare queste licenze manualmente.

**Come faccio a decidere quanti utenti o dispositivi dotare di licenza?**

Valutare i requisiti del caso d'uso per determinare il numero appropriato di licenze. La licenza utente/dispositivo consente l'accesso illimitato a desktop virtuali e app virtuali illimitati da un numero illimitato di dispositivi. Le licenze simultanee consentono l'accesso illimitato a desktop virtuali e app virtuali illimitati da un singolo dispositivo utilizzabile da un numero illimitato di utenti. Considerare la seguente formula:

```
(Number of total users) – (number of users that only access
   exclusively
 with shared devices) + (number shared devices) = total number
 of licenses to buy.

For example, there are 1000 total users at the hospital. If 700 of them
    access only
Citrix Virtual Desktops from 300 shared devices in the hospital, the
   number of
licenses to purchase is 1000 – 700 + 300 = 600 licenses.
<!--NeedCopy-->
```

**Nel modello utente/dispositivo, qual è il numero massimo di dispositivi che un utente con licenza può utilizzare per connettersi al mio ambiente?**

Ogni utente con licenza ha il diritto di utilizzare un numero illimitato di dispositivi connessi o non in linea.

**Nel modello utente/dispositivo, qual è il numero massimo di utenti che possono accedere a un dispositivo con licenza?**

Ogni dispositivo con licenza può servire un numero illimitato di utenti all'interno di un'organizzazione.

**Nel modello utente/dispositivo, qual è il numero massimo di desktop virtuali o applicazioni Web RBI che un utente con licenza può utilizzare in qualsiasi momento?**

Ogni utente con licenza può connettersi a un numero illimitato di desktop virtuali o applicazioni Web.

**Posso acquistare licenze di Citrix Virtual Apps and Desktops per aumentare il numero di utenti/dispositivi con licenza nel mio ambiente Citrix Virtual Apps and Desktops esistente?**

Sì. È possibile acquistare licenze di Citrix Virtual Apps and Desktops per aumentare il numero di utenti/dispositivi con licenza nell'ambiente Citrix Virtual Apps and Desktops esistente.

**Come posso rilasciare una licenza per utente/dispositivo autorizzata?**

Per rilasciare l'assegnazione di un utente/dispositivo autorizzato, utilizzare l'utilità `udadmin` in conformità con i termini dell'EULA. Il License Server assegna quindi la licenza al successivo utente/dispositivo appropriato. Per ulteriori informazioni, vedere Display or release licenses for users or devices.

**Cosa succede se supero il numero di licenze per utente/dispositivo acquistate?**

Le licenze utente/dispositivo includono uno scoperto del 10%, che viene incluso quando vengono generate le licenze. Lo scoperto è incluso anche nel numero di licenze installate. Se il picco di utilizzo supera il numero di licenze installate incluso lo scoperto, l'accesso a un numero maggiore di utenti viene negato. Acquistare e distribuire una nuova licenza per consentire l'accesso a un numero maggiore di utenti.

Se tutte le licenze sono in uso, incluso lo scoperto della licenza, il periodo di tolleranza supplementare consente connessioni illimitate a un prodotto. Il periodo di tolleranza supplementare dà il tempo di determinare il motivo per cui è stato superato il numero massimo di licenze e per acquistare più licenze senza creare disagi per gli utenti. Questo periodo dura fino al termine di 15 giorni o fino a quando si installano più licenze al dettaglio, a seconda di quale evento si verifichi prima. Per ulteriori informazioni, vedere Periodo di tolleranza supplementare.

Director visualizza gli stati del periodo di tolleranza. Per ulteriori informazioni, vedere Pannelli della dashboard di Director.

**Qual è il numero massimo di applicazioni virtuali che un utente con licenza può utilizzare in qualsiasi momento?**

Ogni utente con licenza può connettersi a un numero illimitato di applicazioni virtuali.

**Cosa succede se un utente con licenza lascia la mia organizzazione?**

Quando un utente con licenza esistente lascia l'organizzazione, è possibile rilasciare la licenza di tale utente senza notificare Citrix. Utilizzare l'utilità `udadmin` per rilasciare la licenza. Se non si rilascia la licenza, License Server rilascia automaticamente qualsiasi licenza dopo 90 giorni di inattività. Queste informazioni sono soggette ai termini specificati nell'EULA.

**Cosa succede se un utente con licenza è assente per un periodo prolungato?**

Se un utente con licenza esistente è assente per un periodo prolungato, è possibile rilasciare la licenza senza avvisare Citrix, in modo che diventi disponibile per essere riassegnata. Utilizzare l'utilità `udadmin` per rilasciare la licenza.

**Cosa succede se sostituiamo un dispositivo con licenza nell'organizzazione?**

Se si sostituisce un dispositivo con licenza esistente, è possibile rilasciare la licenza senza avvisare Citrix in modo che diventi disponibile per essere riassegnata. Utilizzare l'utilità `udadmin` per rilasciare la licenza.

**Cosa succede se un dispositivo con licenza è fuori servizio per un periodo prolungato?**

Quando un dispositivo con licenza esistente è fuori servizio per un periodo prolungato, è possibile rilasciare la licenza senza avvisare Citrix, in modo che diventi disponibile per essere riassegnata. Utilizzare l'utilità `udadmin` per rilasciare le licenze. Se non si rilascia la licenza, License Server rilascia automaticamente qualsiasi licenza dopo 90 giorni di inattività. Queste informazioni sono soggette ai termini specificati nell'EULA.

**Posso scambiare le licenze utente con licenze dispositivo e viceversa dopo aver assegnato le licenze a un dispositivo o a un utente?**

Sì. Questa modifica avviene automaticamente. License Server assegna licenze a utenti o dispositivi in base all'andamento dell'utilizzo. Se l'andamento dell'utilizzo cambia, il License Server potrebbe cambiare l'assegnazione in base al nuovo utilizzo. License Server assegna sempre le licenze nel modo

più economico per il cliente. Inoltre, License Server monitora le licenze per identificare le licenze **inutilizzate** dopo il periodo di assegnazione di 90 giorni. È possibile riassegnare le licenze identificate come inutilizzate dopo il periodo di assegnazione di 90 giorni ad altri utenti o dispositivi.

## Licenze simultanee

### Con il modello simultaneo, qual è il numero massimo di desktop virtuali che un utente con licenza di Citrix Virtual Apps and Desktops può utilizzare in qualsiasi momento?

Un endpoint può servire molti utenti e consente connessioni illimitate.

### Posso distribuire licenze simultanee da una versione precedente di Citrix Virtual Apps and Desktops e nuove licenze per utente/dispositivo o simultanee su un singolo License Server?

Sì. È possibile continuare a utilizzare lo stesso License Server per supportare le distribuzioni con licenza utente/dispositivo o simultanea.

### Posso distribuire licenze simultanee e licenze utente/dispositivo o simultanee su un singolo License Server?

Sì. È possibile continuare a utilizzare lo stesso License Server per supportare distribuzioni con licenza simultanea e utente/dispositivo o simultanea.

### Le edizioni Advanced e Premium di Citrix Virtual Apps and Desktops includono licenze simultanee Citrix Virtual Apps?

Le licenze per utente/dispositivo Advanced e Premium di Citrix Virtual Apps and Desktops includono licenze simultanee di Citrix Virtual Apps solo per la compatibilità. Queste licenze simultanee sono utilizzabili solo con le versioni precedenti del prodotto che non sono compatibili con le licenze utente/dispositivo. L'uso delle licenze di compatibilità simultanee incluse con le licenze utente/dispositivo è consentito solo con queste versioni: versioni di XenApp precedenti alla 6.5 e versioni di XenDesktop precedenti alla 5.0 Service Pack 1.

### Cosa succede se supero il numero di licenze simultanee acquistato?

Se tutte le licenze sono in uso, il periodo di tolleranza supplementare consente connessioni illimitate a un prodotto. Il periodo di tolleranza supplementare dà il tempo di determinare il motivo per cui è stato superato il numero massimo di licenze e per acquistare più licenze senza creare disagi per gli

utenti. Questo periodo dura fino al termine di 15 giorni o fino a quando si installano più licenze al dettaglio, a seconda di quale evento si verifichi prima. Per ulteriori informazioni, vedere Periodo di tolleranza supplementare.

Director visualizza gli stati del periodo di tolleranza. Per ulteriori informazioni, vedere Pannelli della dashboard di Director.

## Licenze per scoperto

### Come posso ottenere le licenze per lo scoperto?

I prodotti (escluso Citrix Cloud) che supportano modelli di licenza utente/dispositivo, utente o dispositivo includono una funzione di scoperto delle licenze che consente di utilizzare un numero limitato di licenze aggiuntive per impedire la negazione dell'accesso. Offriamo qualsiasi funzione di scoperto per comodità, non come diritto di licenza. Le licenze simultanee e server non contengono scoperto. Le licenze per lo scoperto utilizzate devono essere acquistate entro 30 giorni dal primo utilizzo, ma l'uso non è limitato a 30 giorni. Citrix si riserva il diritto di rimuovere eventuali funzioni di scoperto nelle nuove versioni dei prodotti. Per ulteriori informazioni, vedere Scoperto della licenza.

### Come posso identificare uno scoperto di licenza?

È possibile visualizzare le informazioni sull'utilizzo, incluso il numero di licenze in scoperto, in Citrix Licensing Manager. Anche Studio anche informazioni sull'utilizzo dello scoperto.

### Cosa succede quando viene consumata una licenza per lo scoperto?

Viene assegnata una delle licenze installate per consentire l'accesso all'ambiente Citrix Virtual Apps and Desktops. Questa licenza per scoperto fornisce lo stesso accesso e la stessa funzionalità delle altre licenze.

### Posso ricevere un avviso quando vengono consumate le licenze per lo scoperto?

Al momento, non sono previsti avvisi specifici quando vengono consumate licenze per lo scoperto.

### Per quanto tempo si può consumare una licenza per lo scoperto?

Acquistare le licenze di scoperto utilizzate entro 30 giorni dal primo utilizzo.

### Altre informazioni sulle licenze specifiche di prodotti

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management
- Citrix Gateway
- Citrix Hypervisor
- Licenze Citrix

## Cache host locale

January 7, 2024

Per garantire che il database del sito Citrix Virtual Apps and Desktops sia sempre disponibile, Citrix consiglia di iniziare con una distribuzione di SQL Server con tolleranza di errore, seguendo le procedure consigliate per l'alta disponibilità di Microsoft. Per le funzionalità di alta disponibilità di SQL Server supportate, vedere Database. Tuttavia, se vi sono problemi di rete e interruzioni del collegamento, può risultare impossibile per gli utenti connettersi alle proprie applicazioni o desktop.

La funzione cache host locale consente la continuazione delle operazioni di intermediazione della connessione in un sito quando si verifica un'interruzione. Un'interruzione si verifica quando la connessione tra un Delivery Controller e il database del sito non riesce in un ambiente Citrix locale. La cache host locale si attiva quando il database del sito è inaccessibile per 90 secondi.

A partire da XenApp e XenDesktop 7.16, la funzione di leasing della connessione (una funzione delle versioni precedenti che precedeva l'alta disponibilità) è stata rimossa dal prodotto e non è più disponibile.

### Contenuto di dati

La cache host locale include le seguenti informazioni, che sono un sottoinsieme delle informazioni contenute nel database principale:

- Identità degli utenti e dei gruppi a cui vengono assegnati diritti sulle risorse pubblicate dal sito.
- Identità degli utenti che attualmente utilizzano o che hanno recentemente utilizzato le risorse pubblicate dal sito.
- Identità delle macchine VDA (incluse le macchine Accesso remoto PC) configurate nel sito.
- Identità (nomi e indirizzi IP) delle macchine client Citrix Receiver utilizzate attivamente per connettersi alle risorse pubblicate.

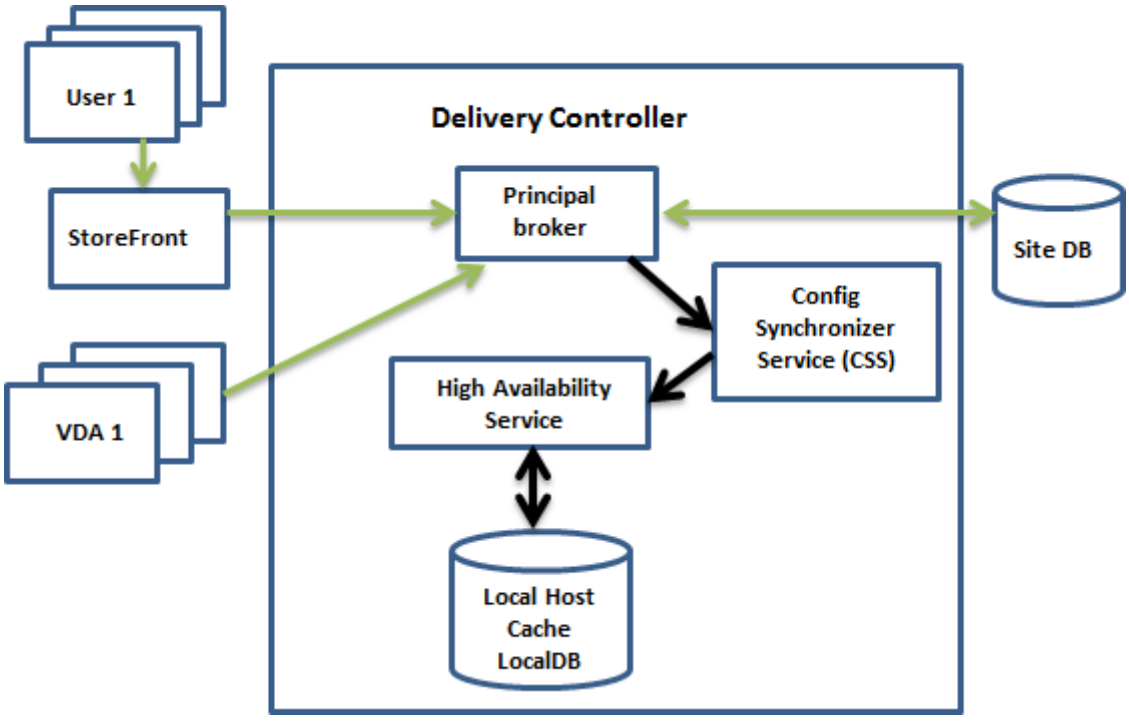
 

Contiene inoltre informazioni per le connessioni attualmente attive che sono state stabilite mentre il database principale non era disponibile:

- Risultati di tutte le analisi endpoint del computer client eseguite da Citrix Receiver.
- Identità delle macchine dell'infrastruttura (quali NetScaler Gateway e server StoreFront) coinvolte nel sito.
- Date, orari e tipi delle attività recenti svolte dagli utenti.

## Come funziona

L'immagine seguente illustra i componenti della cache host locale e i percorsi di comunicazione durante le normali operazioni.




### Durante le normali operazioni

- Il *broker principale* (Citrix Broker Service) che si trova su un controller accetta richieste di connessione da StoreFront. Il broker comunica con il database del sito per connettere gli utenti con i VDA registrati con il controller.
- Citrix Config Synchronizer Service (CSS) controlla il broker circa ogni 5 minuti per verificare se sono state apportate modifiche. Tali modifiche possono essere avviate dall'amministratore (ad esempio la modifica di una proprietà di un gruppo di consegna) o le azioni di sistema (come le assegnazioni di macchine).

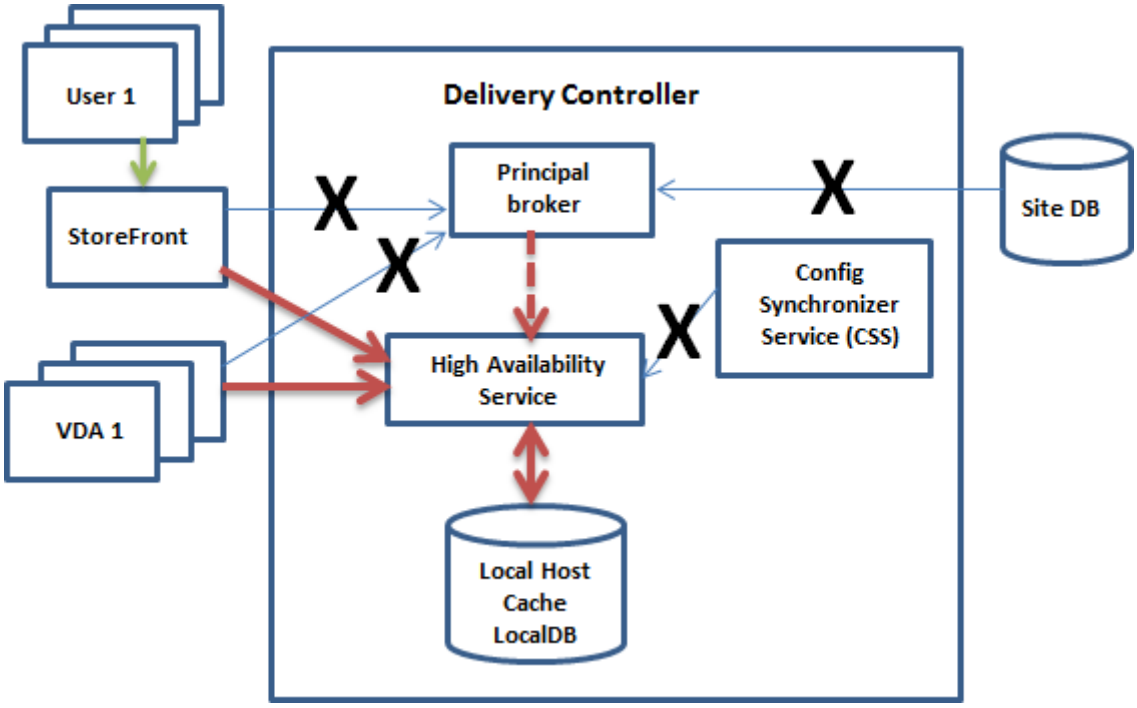
- Se la configurazione è cambiata dopo il controllo precedente, CSS sincronizza (copia) le informazioni con un broker secondario presente nel controller. Il broker secondario è noto anche come servizio High Availability.

  Vengono copiati tutti i dati di configurazione, non solo gli elementi che sono cambiati dopo il controllo precedente. Il CSS importa i dati di configurazione in un database Microsoft SQL Server Express LocalDB sul controller. Questo database viene denominato database della cache host locale. CSS assicura che le informazioni contenute nel database della cache host locale corrispondano alle informazioni presenti nel database del sito. Il database della cache host locale viene ricreato a ogni sincronizzazione.

  Microsoft SQL Server Express LocalDB (utilizzato dal database della cache host locale) viene installato automaticamente quando si installa un controller. È possibile vietarne l'installazione quando si installa un controller dalla riga di comando. Il database della cache host locale non può essere condiviso tra i controller. Non è necessario eseguire il backup del database della cache host locale. Viene ricreato ogni volta che viene rilevata una modifica della configurazione.

- Se non vi sono state modifiche dopo l'ultimo controllo, non vengono copiati dati.

L'immagine seguente illustra come cambiano i percorsi di comunicazione se il broker principale perde il contatto con il database del sito (quando inizia un'interruzione).




**Durante un'interruzione**

Quando inizia un'interruzione:

- Il broker secondario inizia l'ascolto e l'elaborazione delle richieste di connessione.
- Quando inizia l'interruzione, il broker secondario non dispone dei dati di registrazione VDA correnti, ma quando un VDA comunica con esso, viene attivato un processo di registrazione. Durante tale processo, il broker secondario riceve anche le informazioni sulla sessione corrente relative a quel VDA.
- Mentre il broker secondario gestisce le connessioni, il broker principale continua a monitorare la connessione. Quando la connessione viene ripristinata, il broker principale chiede al broker secondario di interrompere l'ascolto delle informazioni sulla connessione e ricomincia a svolgere le operazioni di mediazione. La volta successiva che un VDA comunica con il broker principale, viene attivato un processo di registrazione. Il broker secondario rimuove le registrazioni VDA che sono rimaste dall'interruzione precedente. Il CSS riprende la sincronizzazione delle informazioni quando rileva che sono state apportate modifiche della configurazione nella distribuzione.

Nell'improbabile caso in cui un'interruzione inizi durante una sincronizzazione, l'importazione corrente viene eliminata e viene utilizzata l'ultima configurazione nota.

Nel registro eventi sono disponibili informazioni su sincronizzazioni e interruzioni.

Non è previsto alcun limite di tempo per il funzionamento in modalità di interruzione.

La transizione tra modalità normale e di interruzione non influisce sulle sessioni esistenti. Influisce solo sul lancio di nuove sessioni.

È inoltre possibile attivare intenzionalmente un'interruzione. Per dettagli su perché e come farlo, vedere Forzare un'interruzione.

#### Siti con più controller

Tra le altre attività che svolge, il CSS fornisce regolarmente al broker secondario informazioni su tutti i controller della zona. Se la distribuzione non è dotata di più zone, questa azione ha effetto su tutti i controller del sito. Avendo queste informazioni, ogni broker secondario conosce tutti i broker secondari peer in esecuzione sugli altri controller della zona.

I broker secondari comunicano tra loro su un canale separato. Questi broker utilizzano un elenco alfabetico di nomi FQDN delle macchine su cui sono in esecuzione per determinare (scegliere) quale broker secondario medierà le operazioni nella zona in caso di interruzione. Durante l'interruzione, tutti i VDA si registrano presso il broker secondario scelto. I broker secondari non scelti della zona rifiutano attivamente le richieste di connessione e di registrazione VDA in entrata.

Se un broker secondario scelto si arresta durante un'interruzione, viene scelto un altro broker secondario al suo posto e i VDA si registrano presso il broker secondario appena scelto.

In caso di interruzione, se un controller viene riavviato:

- Se quel controller non è il broker scelto, il riavvio non ha alcun impatto.
- Se il controller è il broker scelto, ne viene scelto un altro, facendo registrare i VDA. Dopo l'accensione, il controller riavviato assume automaticamente il ruolo di mediazione, facendo nuovamente registrare i VDA. In questo scenario, durante le registrazioni le prestazioni possono risentirne.

Se si spegne un controller durante le normali operazioni e quindi lo si accende durante un'interruzione, la cache host locale non può essere utilizzata su quel controller se viene scelto come broker.

Nei registri eventi sono disponibili informazioni sulla scelta dei broker.

### Cosa non è disponibile durante un'interruzione e altre differenze

Non è previsto alcun limite di tempo per il funzionamento in modalità di interruzione. Tuttavia, Citrix consiglia di ripristinare la connettività nel modo più rapido possibile.

Durante un'interruzione:

- Non è possibile utilizzare Studio.
- È disponibile un accesso limitato a PowerShell SDK.
  - È necessario innanzitutto:
    * Aggiungere una chiave `EnableCssTestMode` del Registro di sistema con un valore di 1: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    * Usare la porta 89: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
  - Dopo aver eseguito questi comandi, è possibile accedere a:
    * Tutti i cmdlet `Get-Broker*`.
- Le credenziali Hypervisor non possono essere ottenute dal servizio host. Tutte le macchine sono in stato di alimentazione sconosciuto e non è possibile emettere operazioni di alimentazione. Tuttavia, le macchine virtuali dell'host che sono alimentate possono essere utilizzate per le richieste di connessione.
- Una macchina assegnata può essere utilizzata solo se l'assegnazione si è verificata durante le normali operazioni. Non è possibile effettuare nuove assegnazioni durante un'interruzione.
- La registrazione e la configurazione automatica delle macchine Accesso remoto al PC non sono possibili. Tuttavia, le macchine che sono state registrate e configurate durante il normale funzionamento sono utilizzabili.

- Le applicazioni ospitate da server e gli utenti desktop potrebbero utilizzare più sessioni rispetto ai limiti di sessione configurati, se le risorse si trovano in zone diverse.
- Gli utenti possono avviare applicazioni e desktop solo da VDA registrati nella zona contenente il broker secondario attualmente attivo/scelto. Gli avvii tra una zona e l'altra (da un broker secondario in una zona a un VDA in una zona diversa) non sono supportati durante un'interruzione.
- Se si verifica un'interruzione del database del sito prima dell'inizio di un riavvio pianificato per i VDA di un gruppo di consegna, i riavvii iniziano al termine dell'interruzione. Questo può avere risultati imprevisti. Per ulteriori informazioni, vedere Riavvii pianificati ritardati a causa di un'interruzione del database.
- La preferenza di zona non può essere configurata. Se è configurata, le preferenze non vengono prese in considerazione per l'avvio della sessione.
- Le restrizioni sui tag in cui i tag vengono utilizzati per designare le zone non sono supportate per l'avvio delle sessioni. Quando sono configurate restrizioni di tag e l'opzione di controllo avanzato di integrità di uno store StoreFront è abilitata, alcune delle sessioni potrebbero non avviarsi.

### Supporto di applicazioni e desktop

La cache host locale supporta applicazioni e desktop ospitati da server e desktop statici (assegnati).

La cache host locale supporta i VDA desktop nei gruppi di consegna in pool, come indicato di seguito:

- Per impostazione predefinita, i VDA desktop con gestione dell'alimentazione in gruppi di consegna in pool (creati da MCS o Citrix Provisioning) con la proprietà `ShutdownDesktopsAfterUse` abilitata non sono disponibili per le nuove connessioni durante un evento della cache host locale. È possibile modificare questa impostazione predefinita per consentire l'utilizzo di tali desktop durante l'evento della cache host locale.

  Tuttavia, non è possibile fare affidamento sulla gestione dell'alimentazione durante l'interruzione. La gestione dell'alimentazione riprende dopo il ripresa delle normali operazioni. Inoltre, tali desktop potrebbero contenere dati dell'utente precedente, perché non sono stati riavviati.
- Per ignorare il comportamento predefinito, è necessario abilitarlo in tutto il sito e per ogni gruppo di consegna interessato. Eseguire i seguenti cmdlet PowerShell.

  A livello del sito:

  ```
  Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
  ```

  Per ogni gruppo di consegna interessato, eseguire il seguente comando PowerShell:

```
Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
 $true
```

L'attivazione di questa funzione nel sito e nei gruppi di consegna non influisce sul funzionamento della proprietà `ShutdownDesktopsAfterUse` configurata durante le normali operazioni.

> **Importante:**
>
> Senza abilitare ReuseMachinesWithoutShutdownInOutageAllowed a livello di sito e ReuseMachinesWithoutShutdownInOutage a livello di gruppo di consegna, tutti i tentativi di avvio della sessione di VDA desktop ad alimentazione gestita in gruppi di consegna in pool non riusciranno durante un evento Local Host Cache.

#### Considerazioni sulle dimensioni della RAM

Il servizio LocalDB può utilizzare circa 1,2 GB di RAM (fino a 1 GB per la cache del database e 200 MB per l'esecuzione di SQL Server Express LocalDB). Il broker secondario può utilizzare fino a 1 GB di RAM se un'interruzione dura un intervallo prolungato, durante il quale si verificano molti accessi (ad esempio, 12 ore con 10.000 utenti). Questi requisiti di memoria si aggiungono ai normali requisiti di RAM per il controller, quindi potrebbe essere necessario aumentare la capacità totale della RAM.

Se si utilizza un'installazione di SQL Server Express per il database del sito, il server avrà due processi sqlserver.exe.

#### Considerazioni sulla configurazione del core e del socket della CPU

La configurazione della CPU di un controller, soprattutto il numero di core disponibili per SQL Server Express LocalDB, influisce direttamente sulle prestazioni della cache dell'host locale, ancor più dell'allocazione della memoria. Questo sovraccarico della CPU viene osservato solo durante il periodo di interruzione quando il database è irraggiungibile e il broker secondario è attivo.

Sebbene LocalDB possa utilizzare più core (fino a 4), è limitato a un solo socket. L'aggiunta di più socket non migliora le prestazioni (ad esempio, 4 socket con 1 core ciascuna). Citrix consiglia invece di utilizzare più socket con più core. Nei test Citrix, una configurazione 2x3 (2 socket, 3 core) ha fornito prestazioni migliori rispetto alle configurazioni 4x1 e 6x1.

#### Considerazioni sull'archiviazione

Man mano che gli utenti accedono alle risorse durante un'interruzione, LocalDB si ingrandisce. Ad esempio, durante un test di accesso/scollegamento eseguito con 10 accessi al secondo, il database è cresciuto di 1 MB ogni 2-3 minuti. Quando riprende il normale funzionamento, il database locale viene

ricreato e lo spazio viene restituito. Tuttavia, deve essere disponibile spazio sufficiente sull'unità in cui è installato LocalDB per consentire l'aumento di dimensioni del database durante un'interruzione. La cache host locale include anche più I/O durante un'interruzione: circa 3 MB di scritture al secondo, accompagnate da diverse centinaia di migliaia di letture.

#### Considerazioni sulle prestazioni

Durante un'interruzione, un broker secondario gestisce tutte le connessioni, quindi nei siti (o zone) che bilanciano il carico tra più controller durante le normali operazioni, il broker secondario eletto potrebbe dover gestire molte più richieste del normale durante un'interruzione. Pertanto, le richieste della CPU saranno più elevate. Ciascun broker secondario del sito (zona) deve essere in grado di gestire il carico aggiuntivo imposto dal database della cache host locale e da tutti i VDA interessati, poiché il broker secondario selezionato durante un'interruzione può cambiare.

Limiti VDI:

- In una distribuzione VDI a zona singola, durante un'interruzione è possibile gestire in modo efficace fino a 10.000 VDA.
- In una distribuzione VDI multi-zona, durante un'interruzione, è possibile gestire in modo efficace fino a 10.000 VDA in ogni zona fino a un massimo di 40.000 VDA nel sito. Ad esempio, durante un'interruzione ognuno dei seguenti siti può essere gestito in modo efficace:
  - Un sito con quattro zone, ciascuna contenente 10.000 VDA.
  - Un sito con sette zone, una contenente 10.000 VDA e sei contenenti 5.000 VDA ciascuna.

Durante un'interruzione vi possono essere ripercussioni sulla gestione del carico all'interno del sito. Possono essere superati i valutatori del carico (e in particolare le regole del conteggio delle sessioni).

Durante il tempo richiesto a tutti i VDA per registrarsi con un broker secondario, tale servizio potrebbe non avere informazioni complete sulle sessioni correnti. Pertanto, una richiesta di connessione da parte di un utente durante tale intervallo può comportare l'avvio di una nuova sessione, anche se era possibile riconnettersi a una sessione esistente. Questo intervallo (mentre il "nuovo"broker secondario acquisisce informazioni sulla sessione da tutti i VDA durante la nuova registrazione) è inevitabile. Le sessioni connesse all'avvio di un'interruzione non sono colpite durante l'intervallo di transizione, ma potrebbero risentirne nuove sessioni e riconnessioni di sessione.

Questo intervallo si verifica ogni volta che i VDA devono registrarsi:

- Inizia un'interruzione: quando si esegue la migrazione da un broker principale a un broker secondario.
- Errore del broker secondario durante un'interruzione: durante la migrazione da un broker secondario che non è riuscito a un broker secondario appena eletto.

- Ripristino da un'interruzione: quando le normali operazioni riprendono e il broker principale riprende il controllo.

È possibile ridurre l'intervallo abbassando il valore del Registro di sistema `HeartbeatPeriodMs` del Citrix Broker Protocol (valore predefinito = 600000 ms, ovvero 10 minuti). Questo valore di heartbeat è doppio rispetto all'intervallo utilizzato dal VDA per i ping, quindi il valore predefinito genera un ping ogni 5 minuti.

Ad esempio, il seguente comando porta il valore di heartbeat a cinque minuti (300000 millisecondi), il che si traduce in un ping ogni 2,5 minuti:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name
HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

Prestare attenzione quando si cambia il valore di heartbeat. L'aumento della frequenza si traduce in un carico maggiore sui controller sia in modalità normale che in modalità di interruzione.

L'intervallo non può essere completamente eliminato, indipendentemente dalla rapidità con cui si registra il VDA.

Il tempo necessario per la sincronizzazione tra broker secondari aumenta con il numero di oggetti (come VDA, applicazioni, gruppi). Ad esempio, la sincronizzazione di 5000 VDA potrebbe richiedere 10 minuti o più per essere completata.

#### Differenze rispetto alle versioni di XenApp 6.x

Questa implementazione della cache host locale condivide il nome della funzionalità di cache host locale in XenApp 6.x e versioni precedenti di XenApp, ma ha subito miglioramenti significativi. Questa implementazione è più robusta e immune alla corruzione. I requisiti di manutenzione sono ridotti al minimo, ad esempio eliminando la necessità di comandi `dsmaint` periodici. Questa cache host locale è un'implementazione completamente diversa dal punto di vista tecnico.

### Gestire la cache host locale

Per il corretto funzionamento della cache host locale, il criterio di esecuzione di PowerShell su ciascun controller deve essere impostato su RemoteSigned, Unrestricted o Bypass.

#### SQL Server Express LocalDB

Il software Microsoft SQL Server Express LocalDB utilizzato dalla cache host locale viene installato automaticamente quando si installa un controller o si aggiorna un controller da una versione precedente alla 7.9. Solo il broker secondario comunica con questo database. Non è possibile utilizzare i cmdlet

PowerShell per apportare alcuna modifica a questo database. LocalDB non può essere condiviso tra i controller.

Il software di database SQL Server Express LocalDB viene installato indipendentemente dal fatto che la cache host locale sia abilitata o meno.

Per impedirne l'installazione, installare o aggiornare il controller utilizzando il comando `XenDesktopServerSe` `.exe` includendo l'opzione `/exclude "Local Host Cache Storage (LocalDB)"`. Tuttavia, tenere presente che la funzione cache host locale non funzionerà senza il database e non sarà possibile utilizzare un database diverso con il broker secondario.

L'installazione di questo database LocalDB non influisce sull'installazione di SQL Server Express per l'utilizzo come database del sito.

Per informazioni sulla sostituzione di una versione precedente di SQL Server Express LocalDB con una versione più recente, vedere Sostituzione di SQL Server Express LocalDB.

#### Impostazioni predefinite dopo l'installazione e l'aggiornamento del prodotto

Durante una nuova installazione di Citrix Virtual Apps and Desktops (versione minima 7.16), la cache host locale è abilitata.

Dopo un aggiornamento (alla versione 7.16 o successiva), la cache host locale viene attivata se sono presenti meno di 10.000 VDA nell'intera distribuzione.

#### Abilitare e disabilitare la cache host locale

- Per abilitare cache host locale, immettere:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  Per determinare se la cache host locale è abilitata, immettere `Get-BrokerSite`. Controllare che la proprietà `LocalHostCacheEnabled` sia `True`.

- Per disabilitare la cache host locale, immettere:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

Ricordare: a partire da XenApp e XenDesktop 7.16, il leasing di connessione (la funzionalità che ha preceduto la cache host locale a partire dalla versione 7.6) è stato rimosso dal prodotto e non è più disponibile.

### Verificare che la cache dell'host locale funzioni

Per verificare che la cache host locale sia correttamente configurata e in funzione:

- Assicurarsi che le importazioni di sincronizzazione siano completate correttamente. Controllare i registri degli eventi.
- Assicurarsi che il database SQL Server Express LocalDB sia stato creato su ciascun Delivery Controller. Ciò conferma che il broker secondario può subentrare, se necessario.
  - Nel server del Delivery Controller, passare a `C:\Windows\ServiceProfiles\NetworkService`.
  - Verificare che vengano creati `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf`.
- Forzare un'interruzione sui Delivery Controller. Dopo aver verificato che la cache locale host funziona, ricordare di rimettere tutti i controller in modalità normale. Questa operazione può richiedere circa 15 minuti.

### Registri eventi

I registri eventi indicano quando si verificano sincronizzazioni e interruzioni. Nei registri del visualizzatore eventi, la modalità di interruzione viene definita *modalità HA*. *

**Servizio Config Synchronizer:**

Durante le normali operazioni, possono verificarsi gli eventi di cui sotto quando il CSS importa i dati di configurazione nel database della cache host locale utilizzando il broker cache host locale.

- 503: Citrix Config Sync Service ha ricevuto una configurazione aggiornata. Questo evento indica l'inizio del processo di sincronizzazione.
- 504: Citrix Config Sync Service ha importato una configurazione aggiornata. L'importazione della configurazione è stata completata correttamente.
- 505: Citrix Config Sync Service non è riuscito a effettuare un'importazione. L'importazione della configurazione non è stata completata correttamente. Se è disponibile, viene utilizzata una precedente configurazione riuscita in caso di interruzione. Tuttavia, sarà obsoleta rispetto alla configurazione corrente. Se non è disponibile alcuna configurazione precedente, il servizio non può partecipare alla mediazione della sessione durante un'interruzione. In questo caso, consultare la sezione Risoluzione dei problemi e contattare il Supporto Citrix.
- 507: Citrix Config Sync Service ha abbandonato un'importazione perché il sistema è in modalità di interruzione e viene utilizzato il broker cache host locale per la mediazione. Il servizio ha ricevuto una nuova configurazione, ma l'importazione è stata abbandonata a causa di un'interruzione. Questo è un comportamento previsto.
- 510: nessun dato di configurazione del Configuration Service ricevuto dal servizio di configurazione principale.
- 517: si è verificato un problema di comunicazione con il Broker principale.
- 518: lo script Config Sync si è interrotto perché il Broker secondario (High Availability Service) non è in esecuzione.

**High Availability Service:**

Questo servizio è noto anche come broker cache host locale.

- 3502: si è verificata un'interruzione e il broker cache host locale sta eseguendo operazioni di mediazione.
- 3503: è stata risolta un'interruzione e sono riprese le normali operazioni.
- 3504: indica quale broker cache host locale viene scelto, oltre ad altri broker cache host locale coinvolti nella scelta.
- 3507: fornisce un aggiornamento dello stato della cache host locale ogni 2 minuti; questo indica che la modalità Cache host locale è attiva sul broker selezionato. Contiene un riepilogo dell'interruzione, inclusa la durata dell'interruzione, la registrazione del VDA e le informazioni sulla sessione.
- 3508: annuncia che la cache host locale non è più attiva sul broker scelto e le normali operazioni sono state ripristinate. Contiene un riepilogo dell'interruzione che include la durata dell'interruzione, il numero di macchine registrate durante l'evento della cache host locale e il numero di avvii riusciti durante l'evento LHC.
- 3509: notifica che la cache host locale è attiva sui broker non scelti. Contiene una durata di interruzione ogni 2 minuti e indica il broker scelto.
- 3510: annuncia che la cache host locale non è più attiva sui broker non scelti. Contiene la durata dell'interruzione e indica il broker scelto.

## Forzare un'interruzione

Potrebbe essere utile forzare deliberatamente un'interruzione.

- Se la rete continua a disattivarsi e riattivarsi. Forzare un'interruzione fino a quando non vengono risolti i problemi di rete impedisce la transizione continua tra modalità normale e di interruzione (e le frequenti tempeste di registrazione VDA che ne derivano).
- Per verificare un piano di ripristino di emergenza.
- Per aiutare a garantire che cache host locale funzioni correttamente.
- Durante la sostituzione o la manutenzione del server del database del sito.

Per forzare un'interruzione, modificare il registro di ciascun server contenente un Delivery Controller. In `HKLM\Software\Citrix\DesktopServer\LHC`, creare e impostare `OutageModeForced` come `REG_DWORD` su `1`. Questa impostazione indica al broker cache host locale di accedere alla modalità di interruzione, indipendentemente dallo stato del database. Impostando il valore su `0` si fa uscire il broker cache host locale dalla modalità di interruzione.

Per verificare gli eventi, monitorare il file di log `Current_HighAvailabilityService` al percorso `C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`.

### Risoluzione dei problemi

Sono disponibili diversi strumenti per la risoluzione dei problemi quando un'importazione di sincronizzazione nel database della cache host locale non riesce e viene pubblicato un evento 505.

**CDF tracing:** contiene opzioni per i moduli `ConfigSyncServer` e `BrokerLHC`. Queste opzioni, insieme ad altri moduli broker, probabilmente identificheranno il problema.

**Report:** se un'importazione di sincronizzazione non riesce, è possibile generare un rapporto. Questo rapporto si arresta all'oggetto che causa l'errore. Questa funzione di report influisce sulla velocità di sincronizzazione, pertanto Citrix consiglia di disabilitarla quando non è in uso.

Per abilitare e produrre un report di traccia CSS, immettere il seguente comando:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

Il report HTML è pubblicato all'indirizzo `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.html`.

Dopo aver generato il report, immettere il seguente comando per disabilitare la funzione di reporting:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

**Export the broker configuration (Esporta la configurazione del broker):** fornisce la configurazione esatta per scopi di debug.

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

Ad esempio, `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`.

#### Comandi PowerShell della cache host locale

È possibile gestire la cache host locale (LHC) sui Delivery Controller utilizzando i comandi PowerShell.

Il modulo PowerShell si trova nella seguente posizione sui Delivery Controller:

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **Importante:**
>
> Eseguire questo modulo solo sui Delivery Controller.

**Importare il modulo PowerShell** Per importare il modulo, eseguire il seguente comando sul Delivery Controller.

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

**Comandi PowerShell per gestire LHC** I seguenti comandi consentono di attivare e gestire la modalità LHC sui Delivery Controller.

| Cmdlet | Funzione |
| --- | --- |
| `Enable-LhcForcedOutageMode` | Mettere il broker in modalità LHC. I file di database LHC devono essere stati creati correttamente dal servizio ConfigSync per assicurare che `Enable-LhcForcedOutageMode` funzioni correttamente. Questo cmdlet forza LHC solo sul Delivery Controller su cui è stato eseguito. Affinché LHC diventi attivo, questo comando deve essere eseguito su tutti i Delivery Controller all'interno della zona. |
| `Disable-LhcForcedOutageMode` | Consente di escludere il Broker dalla modalità LHC. Questo cmdlet disabilita solo la modalità LHC sul Delivery Controller su cui è stato eseguito. `Disable-LhcForcedOutageMode` deve essere eseguito su tutti i Delivery Controller all'interno della zona. |
| `Set-LhcConfigSyncIntervalOverride` | Imposta l'intervallo con cui Citrix Config Synchronizer Service (CSS) verifica se sono state apportate modifiche alla configurazione all'interno del sito. L'intervallo di tempo può variare da 60 secondi (un minuto) a 3600 secondi (un'ora). Questa impostazione si applica solo al Delivery Controller in cui è stata eseguita. Per garantire la coerenza tra i Delivery Controller, è consigliabile eseguire questo cmdlet in ciascun Delivery Controller. Ad esempio: `Set-LhcConfigSyncIntervalOverride -Seconds 1200` |

| Cmdlet | Funzione |
| --- | --- |
| `Clear-LhcConfigSyncIntervalOverride` | Imposta l'intervallo con cui Citrix Config Synchronizer Service (CSS) verifica le modifiche alla configurazione all'interno del sito sul valore predefinito di 300 secondi (cinque minuti). Questa impostazione si applica solo al Delivery Controller in cui è stata eseguita. Per garantire la coerenza tra i Delivery Controller, è consigliabile eseguire questo cmdlet in ciascun Delivery Controller. |
| `Enable-LhcHighAvailabilitySDK` | Consente l'accesso a tutti i cmdlet `Get-Broker*` all'interno del Delivery Controller in cui è stato eseguito. |
| `Disable-LhcHighAvailabilitySDK` | Disabilita l'accesso ai cmdlet Broker all'interno del Delivery Controller in cui è stato eseguito. |

> **Nota:**
>
> - Utilizzare la porta 89 quando si eseguono i cmdlet `Get-Broker*` nel Delivery Controller. Ad esempio:
>   - `Get-BrokerMachine -AdminAddress localhost:89`
> - Quando non è in modalità LHC, l'LHC Broker sul Delivery Controller contiene solo le informazioni di configurazione.
> - Durante la modalità LHC, il broker LHC presente sul Delivery Controller selezionato contiene le seguenti informazioni:
>   - Stati delle risorse
>   - Dettagli della sessione
>   - Registrazioni dei VDA
>   - Informazioni sulla configurazione

## Gestire le chiavi di sicurezza

January 7, 2024

> **Importante:**
>
> - È necessario utilizzare questa funzione in combinazione con StoreFront 1912 LTSR CU2 o versioni successive.
> - La funzionalità Secure XML è supportata solo su Citrix ADC e Citrix Gateway versione 12.1 e successive.
>
> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Mediante questa funzione è possibile consentire solo alle macchine StoreFront e Citrix Gateway approvati di comunicare con i Delivery Controller. Dopo aver attivato questa funzione, tutte le richieste che non contengono la chiave vengono bloccate. Utilizzare questa funzione per aggiungere un ulteriore livello di sicurezza per proteggere dagli attacchi provenienti dalla rete interna.

Un flusso di lavoro generale per utilizzare questa funzione è il seguente:

1. Abilitare Web Studio per visualizzare le impostazioni delle funzionalità.
2. Configurare le impostazioni del proprio sito.
3. Configurare le impostazioni di StoreFront.
4. Configurare le impostazioni di Citrix ADC.

### Abilita Web Studio per visualizzare le impostazioni delle funzionalità

Per impostazione predefinita, le impostazioni per le chiavi di sicurezza sono nascoste da Web Studio. Per consentire a Web Studio di visualizzarli, utilizzare PowerShell SDK come segue:

1. Eseguire l'SDK PowerShell di Citrix Virtual Apps and Desktops.
2. In una finestra di comando, eseguire i comandi seguenti:
    - `Add-PSSnapIn Citrix*`. Questo comando aggiunge gli snap-in Citrix.
    - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

Per ulteriori informazioni sull'SDK PowerShell, vedere SDK e API.

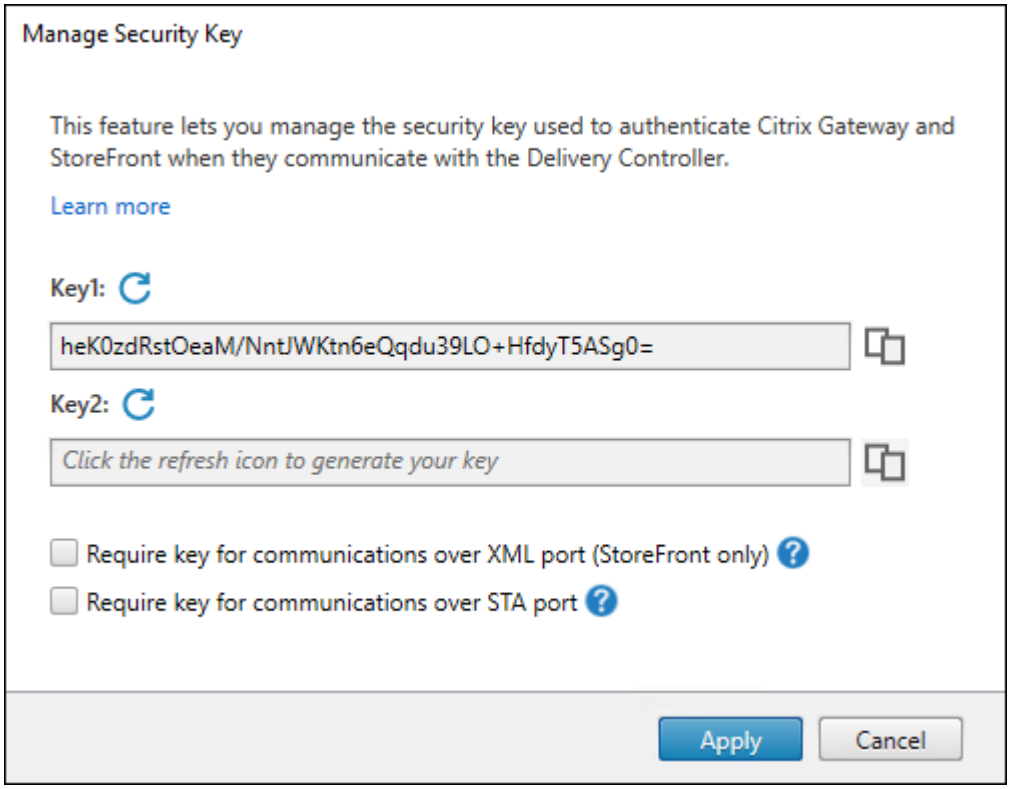
 

## Configurare le impostazioni del sito

È possibile utilizzare Web Studio o PowerShell per configurare le impostazioni delle chiavi di sicurezza per il sito.

### Utilizzare Web Studio

1. Accedere a Web Studio e selezionare **Settings** nel riquadro a sinistra:
2. Individuare il riquadro **Manage security key** (Gestisci chiave di sicurezza) e fare clic su **Edit**. Viene visualizzata la pagina **Manage Security Key**.




3. Fare clic sull'icona di aggiornamento per generare le chiavi.

> **Importante:**
>
> - Vi sono due chiavi disponibili per l'uso. È possibile utilizzare la stessa chiave o chiavi diverse per le comunicazioni tramite le porte XML e STA. Si consiglia di utilizzare solo una chiave alla volta. La chiave non utilizzata viene utilizzata solo per la rotazione delle chiavi.
> - Non fare clic sull'icona di aggiornamento per aggiornare la chiave già in uso, altrimenti vi sarà un'interruzione del servizio.

4. Selezionare dove è richiesta una chiave per le comunicazioni:

- **Require key for communications over XML port (solo StoreFront)**. Se questa opzione è selezionata, viene richiesta una chiave per autenticare le comunicazioni tramite la porta XML. StoreFront comunica con Citrix Cloud su questa porta. Per informazioni sulla modifica della porta XML, vedere l'articolo CTX127945 del Knowledge Center.
- **Require key for communications over STA port**. Se questa opzione selezionata, è richiesta una chiave per autenticare le comunicazioni sulla porta STA. Citrix Gateway e StoreFront comunicano con Citrix Cloud su questa porta. Per informazioni sulla modifica della porta STA, vedere l'articolo CTX101988 del Knowledge Center.

5. Fare clic su **Save** per applicare le modifiche e chiudere la finestra.

#### Utilizzare PowerShell

Di seguito sono riportati i passaggi di PowerShell equivalenti alle operazioni di Web Studio.

1. Eseguire l'SDK Remote PowerShell di Citrix Virtual Apps and Desktops.
2. In una finestra di comando, eseguire il comando seguente:
   - `Add-PSSnapIn Citrix*`
3. Eseguire i seguenti comandi per generare una chiave e impostare Key1:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Eseguire i seguenti comandi per generare una chiave e impostare Key2:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. Eseguire uno o entrambi i comandi seguenti per abilitare l'utilizzo di una chiave nell'autenticazione delle comunicazioni:
   - Per autenticare le comunicazioni tramite la porta XML:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - Per autenticare le comunicazioni tramite la porta STA:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

Per indicazioni guida e sintassi, vedere la Guida dei comandi di PowerShell.

### Configurare le impostazioni di StoreFront

Dopo aver completato la configurazione del proprio sito, è necessario configurare le impostazioni pertinenti di StoreFront utilizzando PowerShell.

Sul server StoreFront eseguire i seguenti comandi di PowerShell:

- Per configurare la chiave per le comunicazioni tramite la porta XML, utilizzare i comandi `Get-STFStoreServie` e `Set-STFStoreService`. Ad esempio:

  - `PS C:\> Set-STFStoreFarm $farm -Farmtype XenDesktop -Port 80 -TransportType HTTP -Servers <domain name1, domain name2> -XMLValidationEnabled $true -XMLValidationSecret <the key you generated in Web Studio>`

- Per configurare la chiave per le comunicazioni tramite la porta STA, utilizzare il comando `New-STFSecureTicketAuthority`. Ad esempio:

  - `PS C:\> $sta = New-STFSecureTicketAuthority –StaUrl <STA URL > -StaValidationEnabled $true -StavalidationSecret <the key you generated in Web Studio>`

Per indicazioni guida e sintassi, vedere la Guida dei comandi di PowerShell.

### Configurare le impostazioni di Citrix ADC

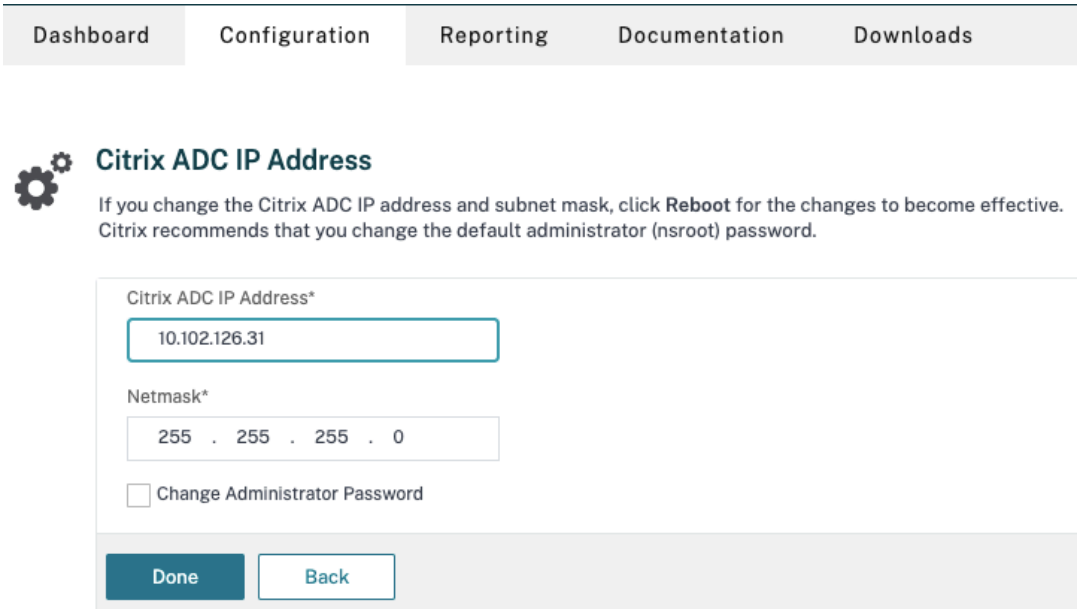
> **Nota:**
>
> La configurazione di questa funzionalità per Citrix ADC non è necessaria a meno che non si utilizzi Citrix ADC come gateway. Se si utilizza Citrix ADC, seguire questa procedura:

1. Assicurarsi che sia stata applicata la seguente configurazione dei prerequisiti:

   - Sono configurati i seguenti indirizzi IP relativi a Citrix ADC.

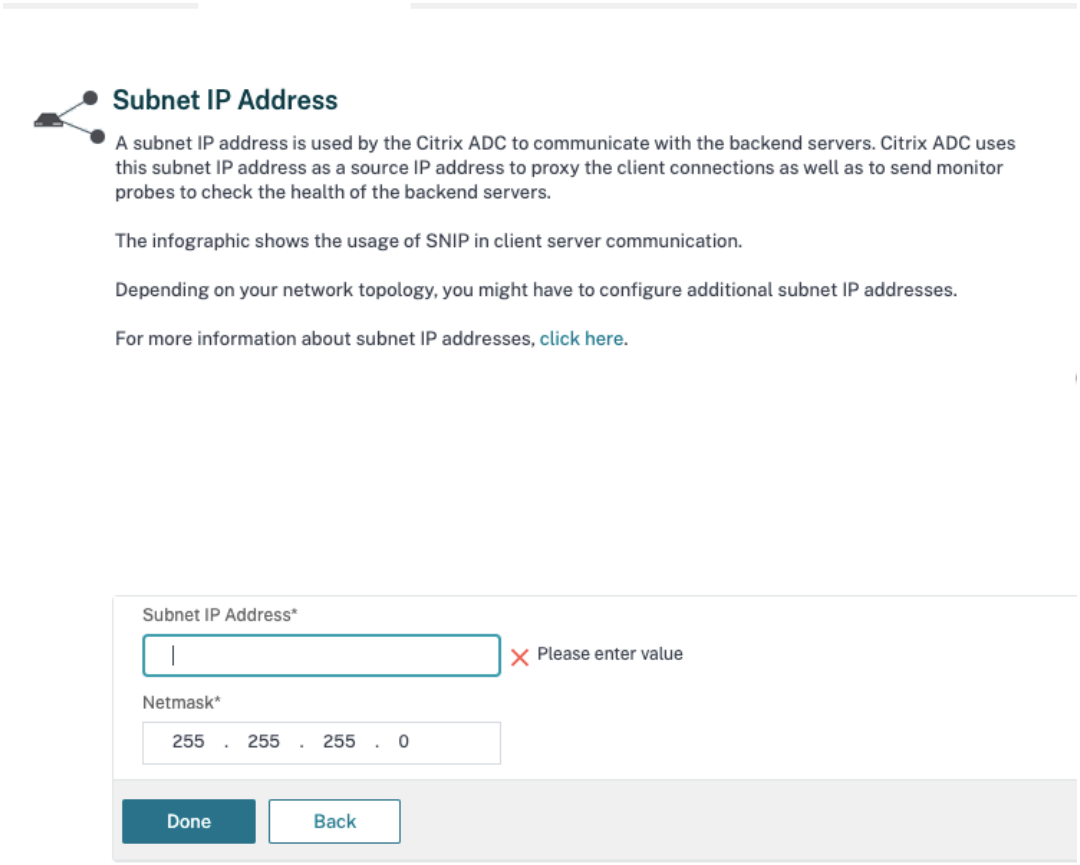
     – Indirizzo Citrix ADC Management IP (NSIP) per l'accesso alla console Citrix ADC. Per ulteriori informazioni, vedere Configurazione dell'indirizzo NSIP.



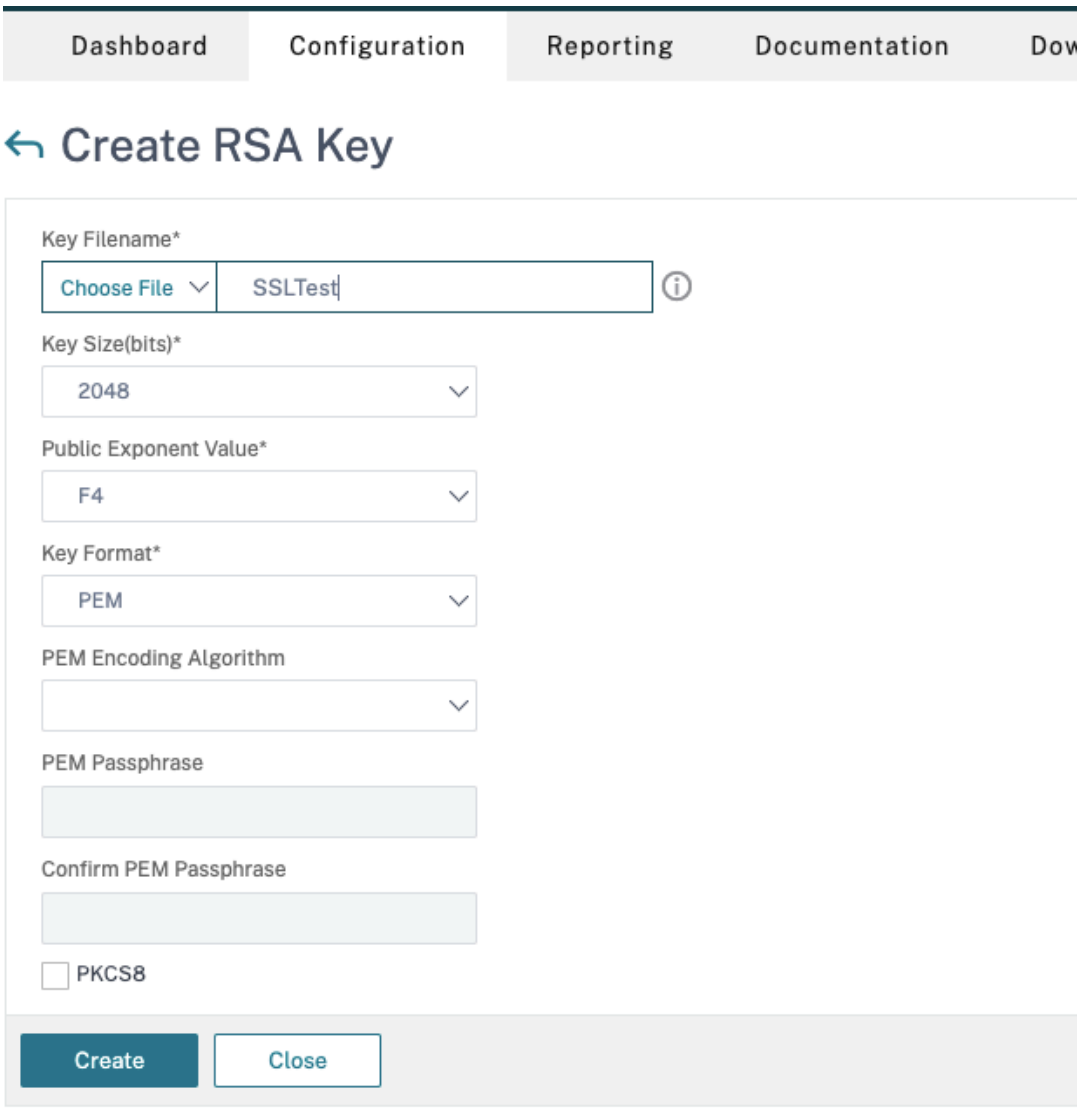

- Indirizzo IP della subnet (SNIP) per abilitare la comunicazione tra l'appliance Citrix ADC e i server back-end. Per ulteriori informazioni, vedere Configurazione degli indirizzi IP delle subnet.
- Indirizzo IP virtuale Citrix Gateway e indirizzo IP virtuale dell'unità di bilanciamento del carico per accedere all'appliance ADC per l'avvio della sessione. Per ulteriori informazioni, vedere Creare un server virtuale.



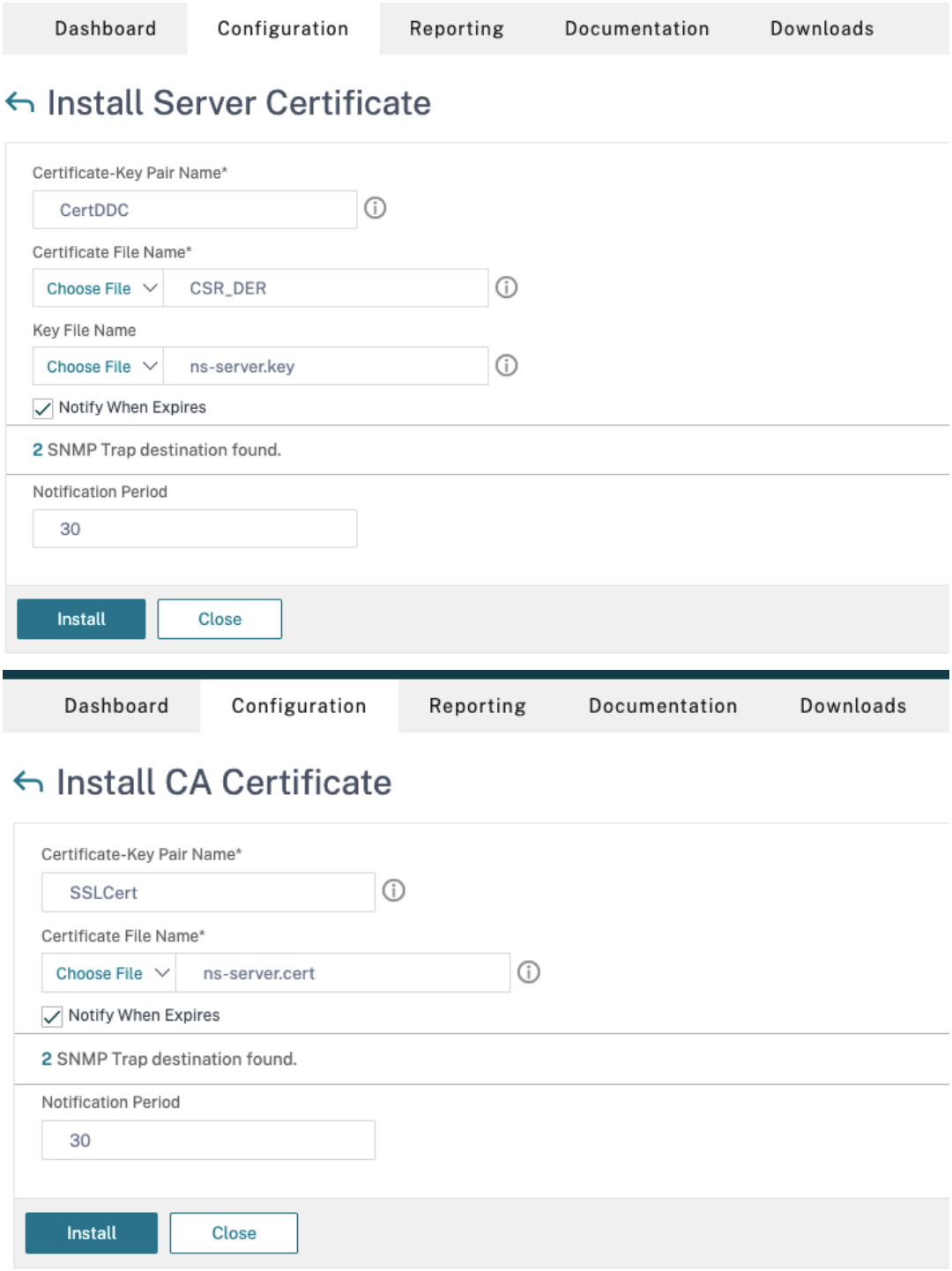

- Le modalità e le funzionalità richieste nell'appliance Citrix ADC sono abilitate.
  - Per abilitare le modalità, nella GUI di Citrix ADC andare a **System (Sistema) > Settings (Impostazioni) > Configure Mode (Configura modalità)**.
  - Per abilitare le funzionalità, nella GUI di Citrix ADC andare a **System (Sistema) > Settings (Impostazioni) > Configure Basic Features (Configura funzionalità di base)**.
- Le configurazioni relative ai certificati sono complete.
  - Viene creata la richiesta di firma del certificato (CSR). Per ulteriori informazioni, vedere Creare un certificato.



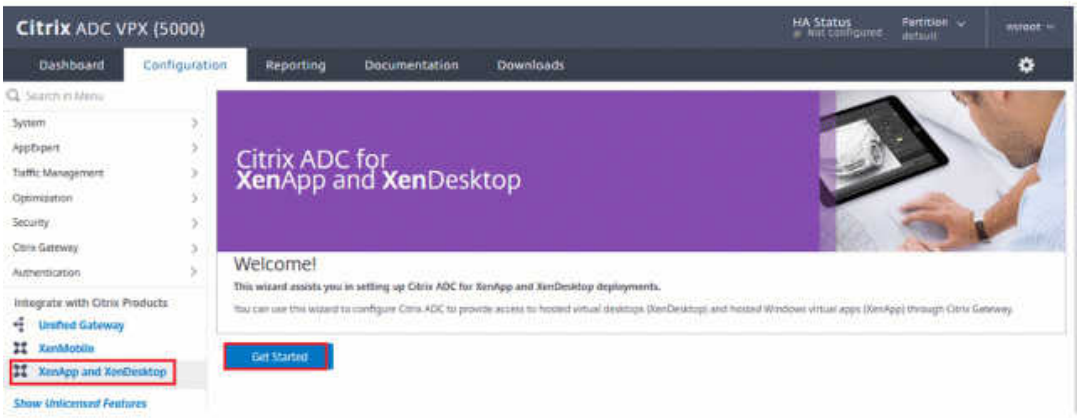

- I certificati del server e CA e i certificati radice sono installati. Per ulteriori informazioni, vedere Installazione, collegamento e aggiornamenti.



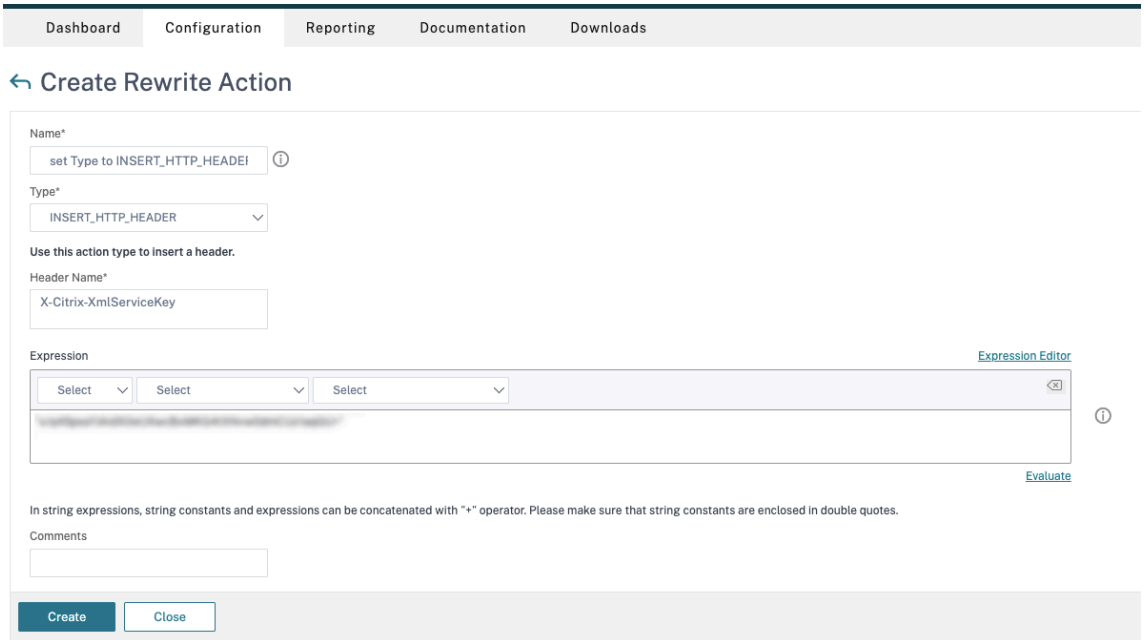

- È stato creato un Citrix Gateway per Citrix Virtual Desktops. Verificare la connettività facendo clic sul pulsante **Test STA Connectivity** (Verifica connettività STA) per confermare che i server virtuali sono online. Per ulteriori informazioni, vedere Configurazione di Citrix ADC per Citrix Virtual Apps and Desktops.




2. Aggiungere un'azione di riscrittura. Per ulteriori informazioni, vedere Configurazione di un'azione di riscrittura.

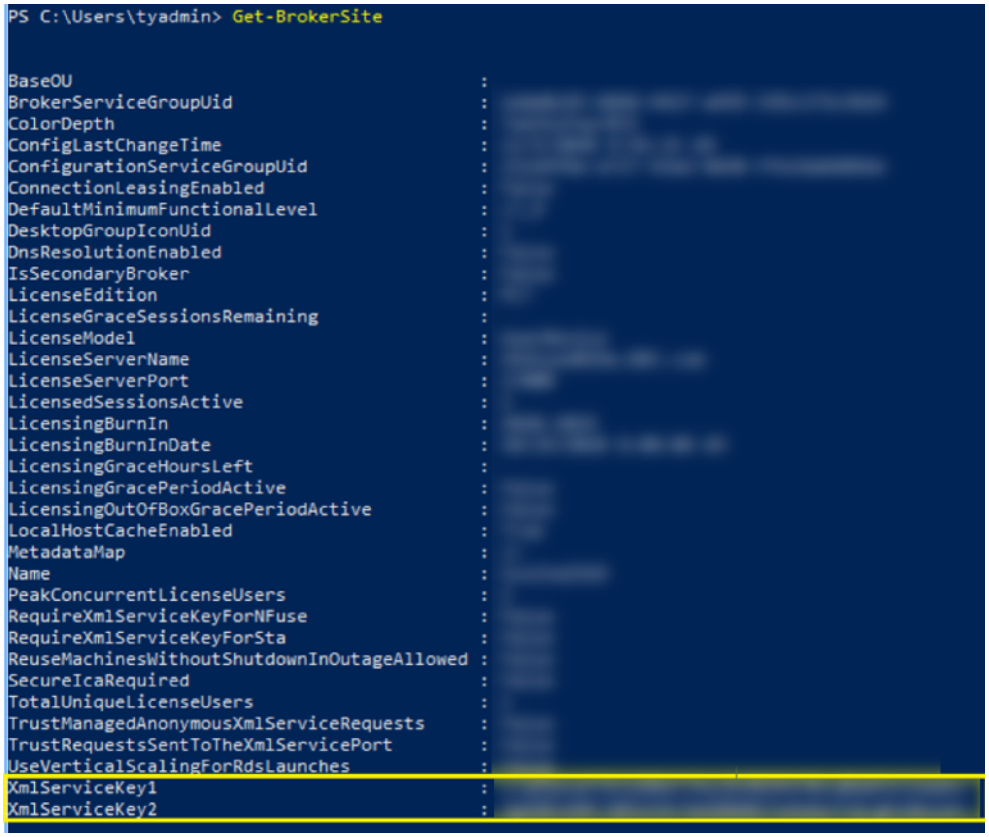
   a) Accedere ad **AppExpert > Rewrite (Riscrivi) > Actions (Azioni)**.
   b) Fare clic su **Add** (Aggiungi) per aggiungere una nuova azione di riscrittura. È possibile assegnare all'azione un nome come "set Type to INSERT_HTTP_HEADER"(imposta Tipo su INSERT_HTTP_HEADER).




   a) In **Type** (Tipo), selezionare **INSERT_HTTP_HEADER**.
   b) In **Header Name** (Nome intestazione), immettere X-Citrix-XmlServiceKey.

c) In **Expression** (Espressione), aggiungere <`XmlServiceKey1 value`> con le virgolette. È possibile copiare il valore XmlServiceKey1 dalla configurazione del Delivery Controller desktop.

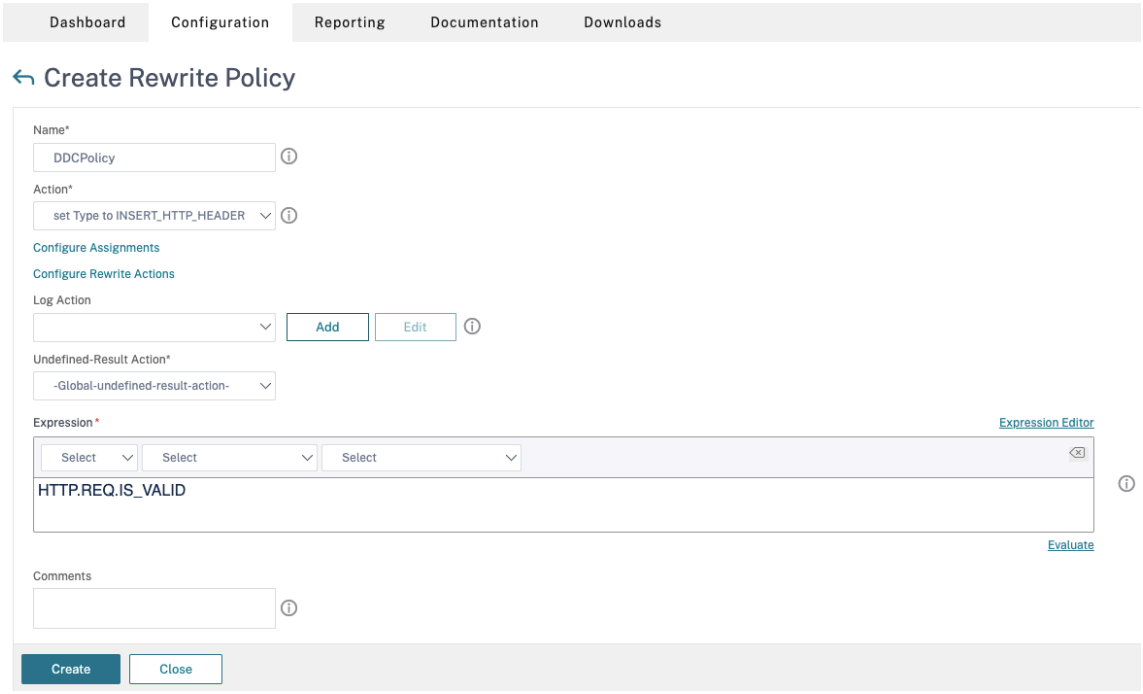



3. Aggiungere un criterio di riscrittura. Per ulteriori informazioni, vedere Configurazione di un criterio di riscrittura.

   a) Accedere ad **AppExpert > Rewrite (Riscrivi) > Policies (Criteri)**.

   b) Fare clic su **Add** (Aggiungi) per aggiungere un nuovo criterio.




a) In **Action** (Azione), selezionare l'azione creata nel passaggio precedente.
b) In **Expression** (Espressione), aggiungere HTTP.REQ.IS_VALID.
c) Fare clic su **OK**.

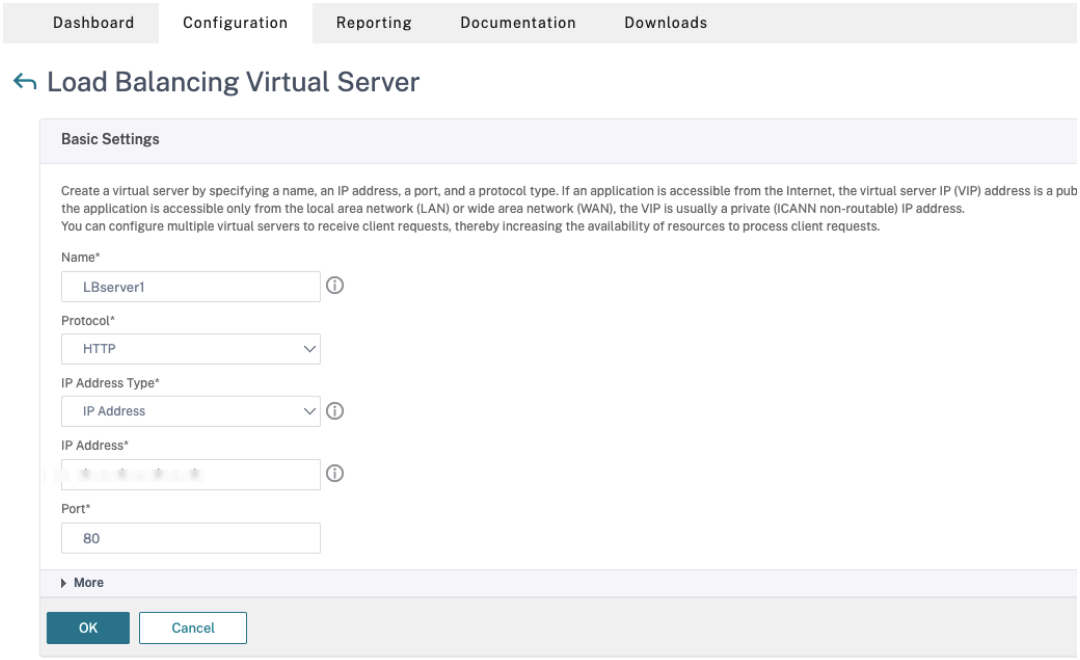
4. Impostare il bilanciamento del carico. È necessario configurare un server virtuale di bilanciamento del carico per ciascun server STA. In caso contrario, le sessioni non vengono avviate.

   Per ulteriori informazioni, vedere Impostare il bilanciamento del carico di base.

   a) Creare un server virtuale di bilanciamento del carico.

      - Andare a **Traffic Management (Gestione del traffico) > Load Balancing (Bilanciamento del carico) > Servers (Server)**.
      - Nella pagina **Virtual Servers** (Server virtuali), fare clic su **Add** (Aggiungi).

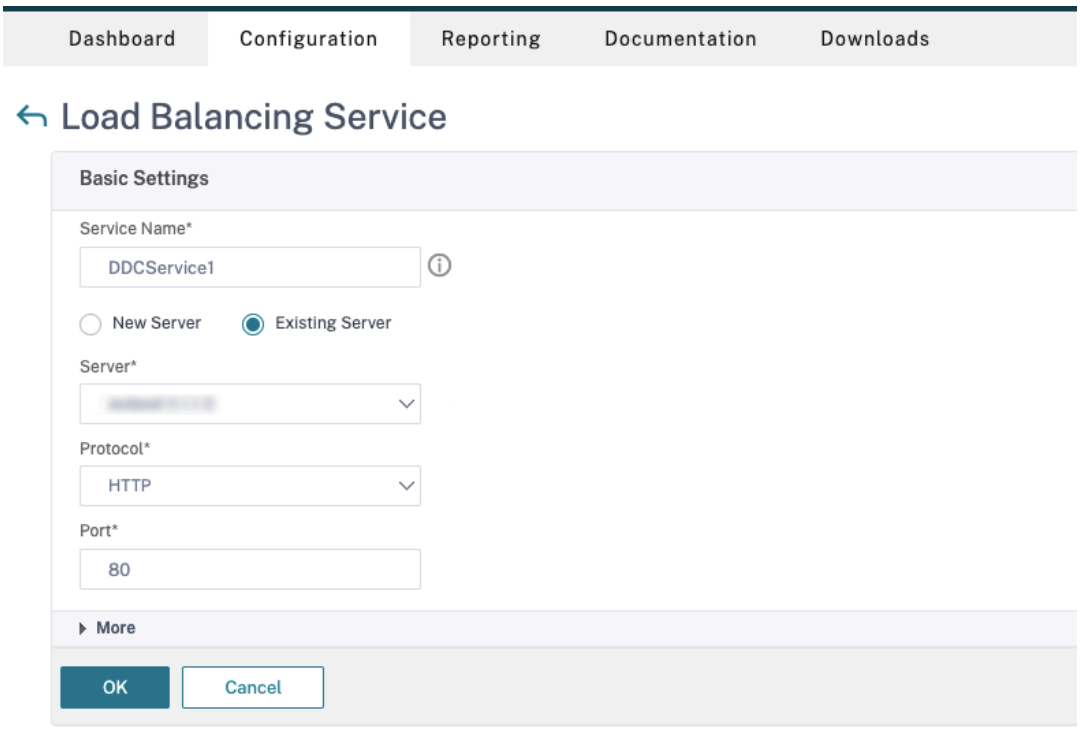



- In **Protocol** (Protocollo), selezionare **HTTP**.
- Aggiungere l'indirizzo IP virtuale di bilanciamento del carico e in **Port** (Porta) selezionare **80**.
- Fare clic su **OK**.

b) Creare un servizio di bilanciamento del carico.

- Andare a **Traffic Management (Gestione del traffico) > Load Balancing (Bilanciamento del carico) > Services (Servizi)**.

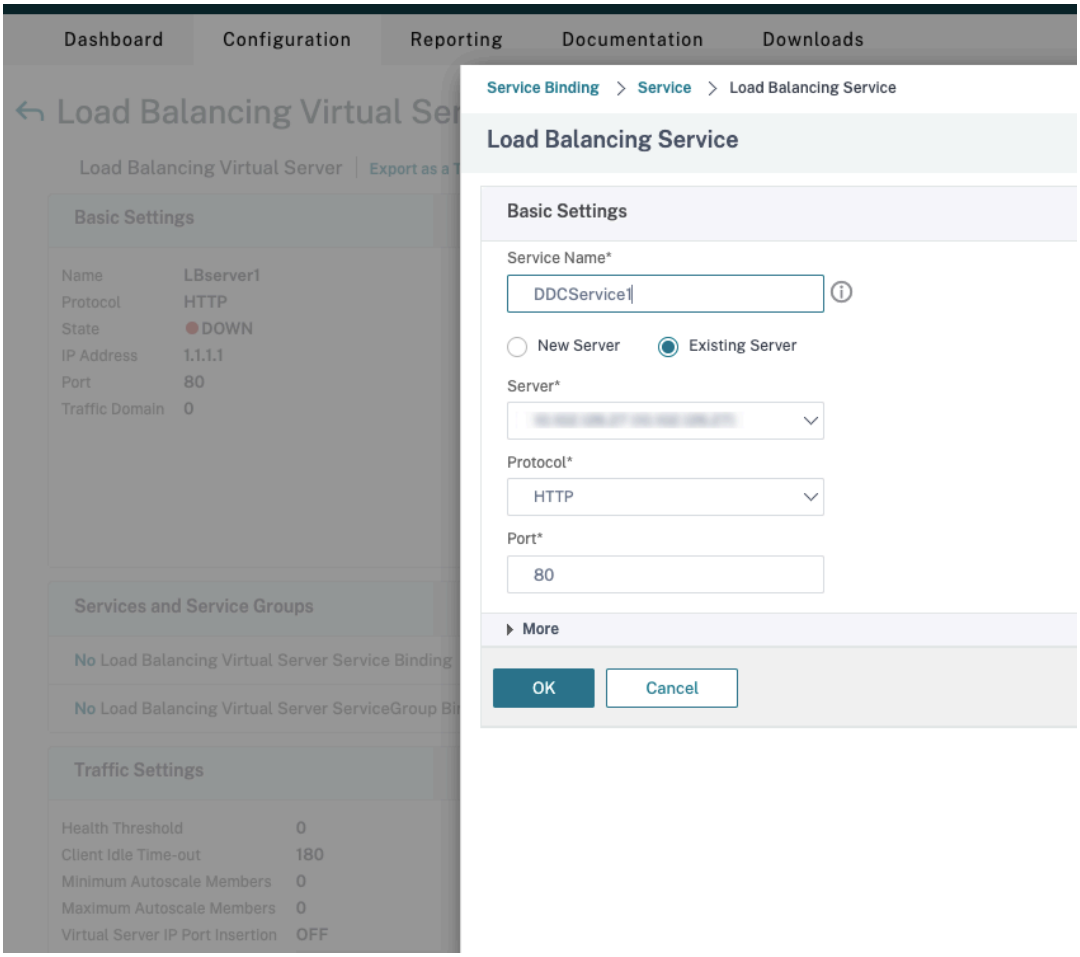



- In **Existing Server** (Server esistente), selezionare il server virtuale creato nel passaggio precedente.
- In **Protocol** (Protocollo), selezionare **HTTP** e in **Port** (Porta) selezionare **80**.
- Fare clic su **OK** e quindi su **Done** (Fine).

c) Associare il servizio al server virtuale.

- Selezionare il server virtuale creato in precedenza e fare clic su **Edit** (Modifica).
- In **Services and Service Groups** (Servizi e gruppi di servizi), fare clic su **No Load Balancing Virtual Server Service Binding** (Nessuna associazione del servizio del server virtuale con bilanciamento del carico).

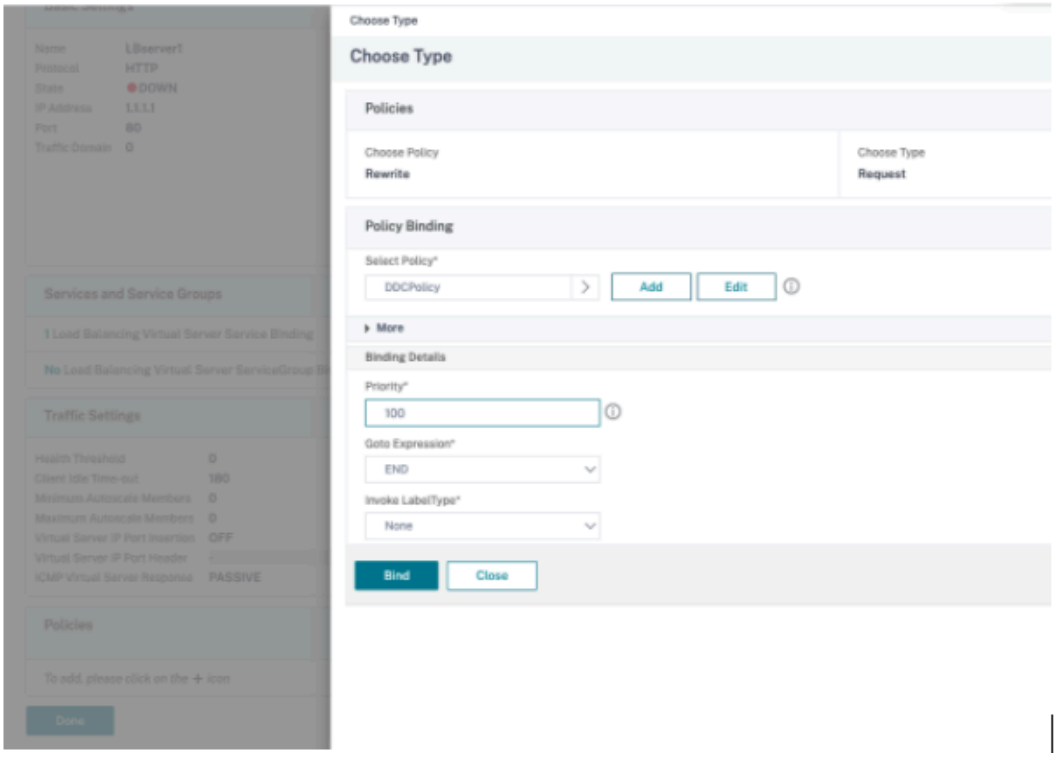



- In **Service Binding** (Associazione a servizio), selezionare il servizio creato in precedenza.
- Fare clic su **Bind** (Associa).

d) Associare il criterio di riscrittura creato in precedenza al server virtuale.

- Selezionare il server virtuale creato in precedenza e fare clic su **Edit** (Modifica).
- In **Advanced Settings** (Impostazioni avanzate), fare clic su **Policies** (Criteri), quindi nella sezione **Policies** (Criteri) fare clic su **+**.

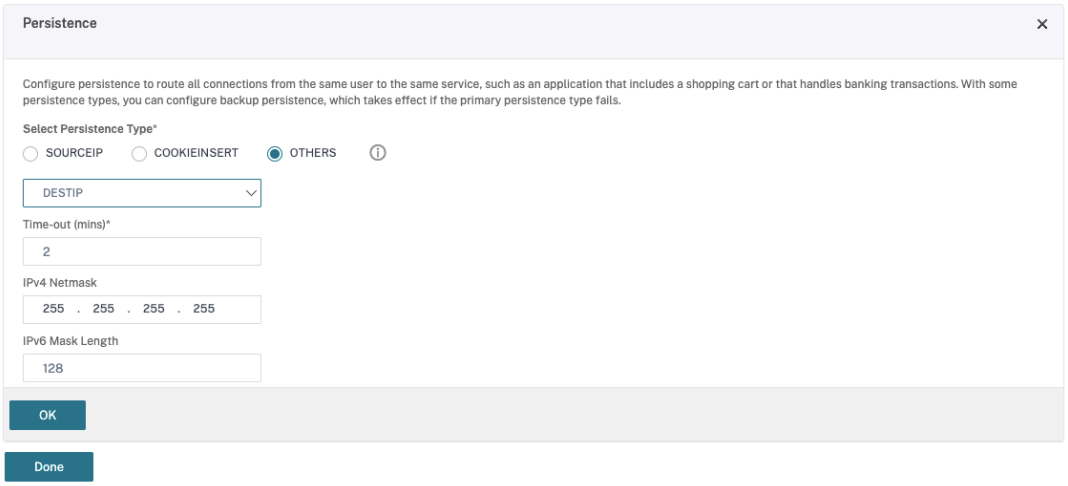



- In **Choose Policy** (Scegli criterio), selezionare **Rewrite** (Riscrivi) e in **Choose Type** (Scegli tipo) selezionare **Request** (Richiesta).
- Fare clic su **Continue** (Continua).
- In **Select Policy** (Seleziona criterio), selezionare il criterio di riscrittura creato in precedenza.
- Fare clic su **Bind** (Associa).
- Fare clic su **Done** (Fine).

e) Impostare la persistenza per il server virtuale, se necessario.

- Selezionare il server virtuale creato in precedenza e fare clic su **Edit** (Modifica).
- In **Advanced Settings** (Impostazioni avanzate), fare clic su **Persistence** (Persistenza).




- Selezionare il tipo di persistenza **Others** (Altro).
- Selezionare **DESTIP** per creare sessioni di persistenza in base all'indirizzo IP del servizio selezionato dal server virtuale (l'indirizzo IP di destinazione).
- In **IPv4 Netmask** (Netmask IPv4), aggiungere la stessa maschera di rete del DDC.
- Fare clic su **OK**.

f) Ripetere questi passaggi anche per l'altro server virtuale.

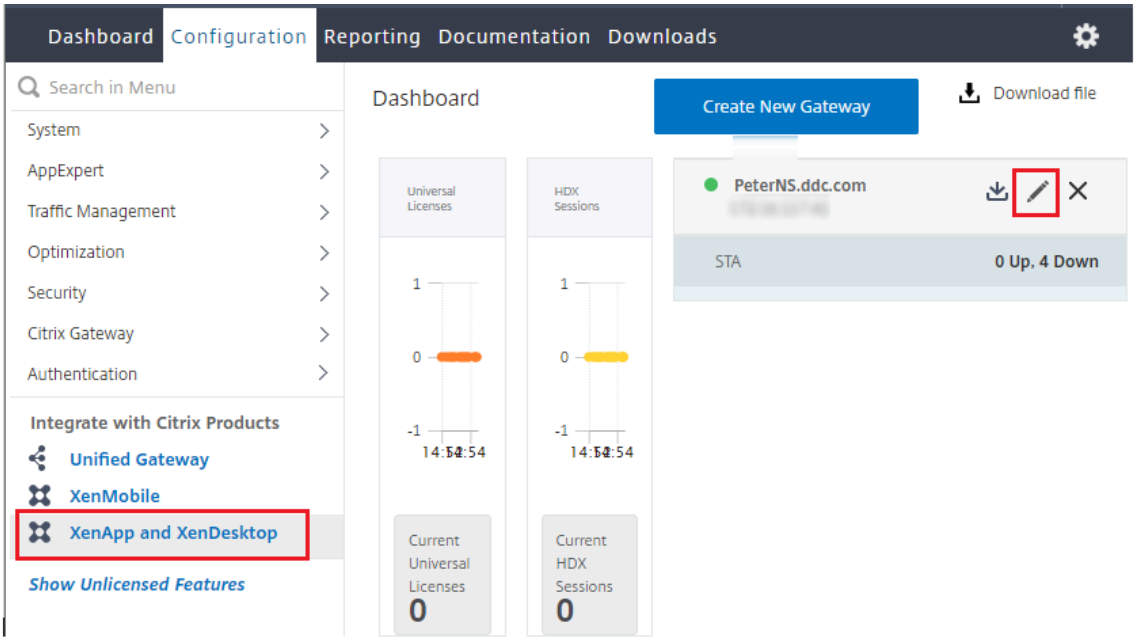
**La configurazione cambia se l'appliance Citrix ADC è già configurata con Citrix Virtual Desktops**

Se è già stata configurata l'appliance Citrix ADC con Citrix Virtual Desktops, per utilizzare la funzionalità Secure XML è necessario apportare le seguenti modifiche alla configurazione.

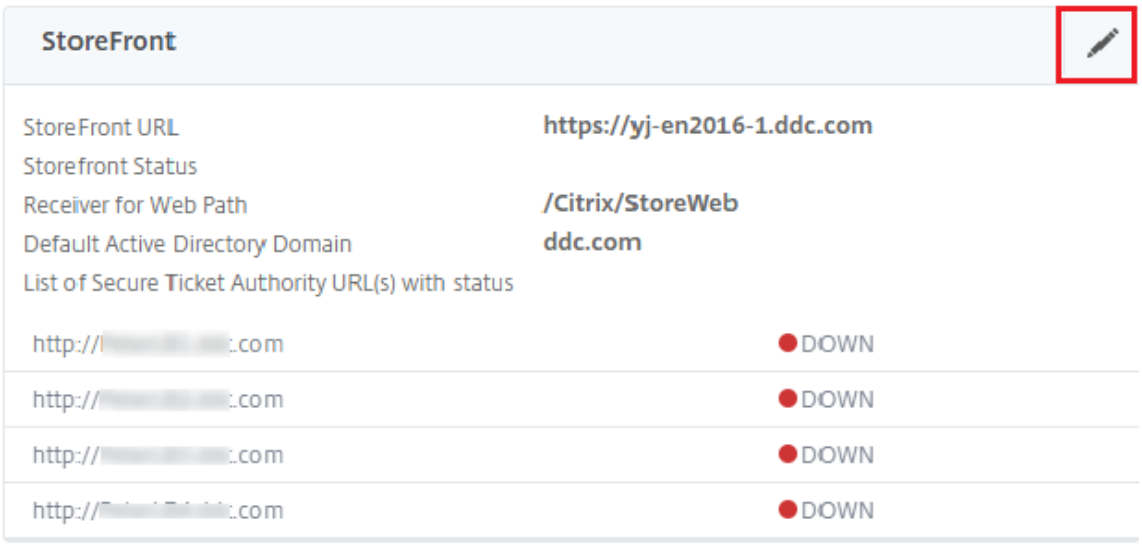
- Prima dell'avvio della sessione, modificare l'**URL Security Ticket Authority** del gateway per utilizzare i nomi di dominio completi dei server virtuali di bilanciamento del carico.
- Assicurarsi che il parametro `TrustRequestsSentToTheXmlServicePort` sia impostato su False. Per impostazione predefinita, il parametro `TrustRequestsSentToTheXmlServicePort` è impostato su False. Tuttavia, se il cliente ha già configurato Citrix ADC per Citrix Virtual Desktops, `TrustRequestsSentToTheXmlServicePort` è impostato su True.

1. Nella GUI di Citrix ADC, accedere a **Configuration (Configurazione) > Integrate with Citrix Products (Integra con i prodotti Citrix)** e fare clic su **XenApp and XenDesktop** (XenApp e XenDesktop).
2. Selezionare l'istanza del gateway e fare clic sull'icona di modifica.



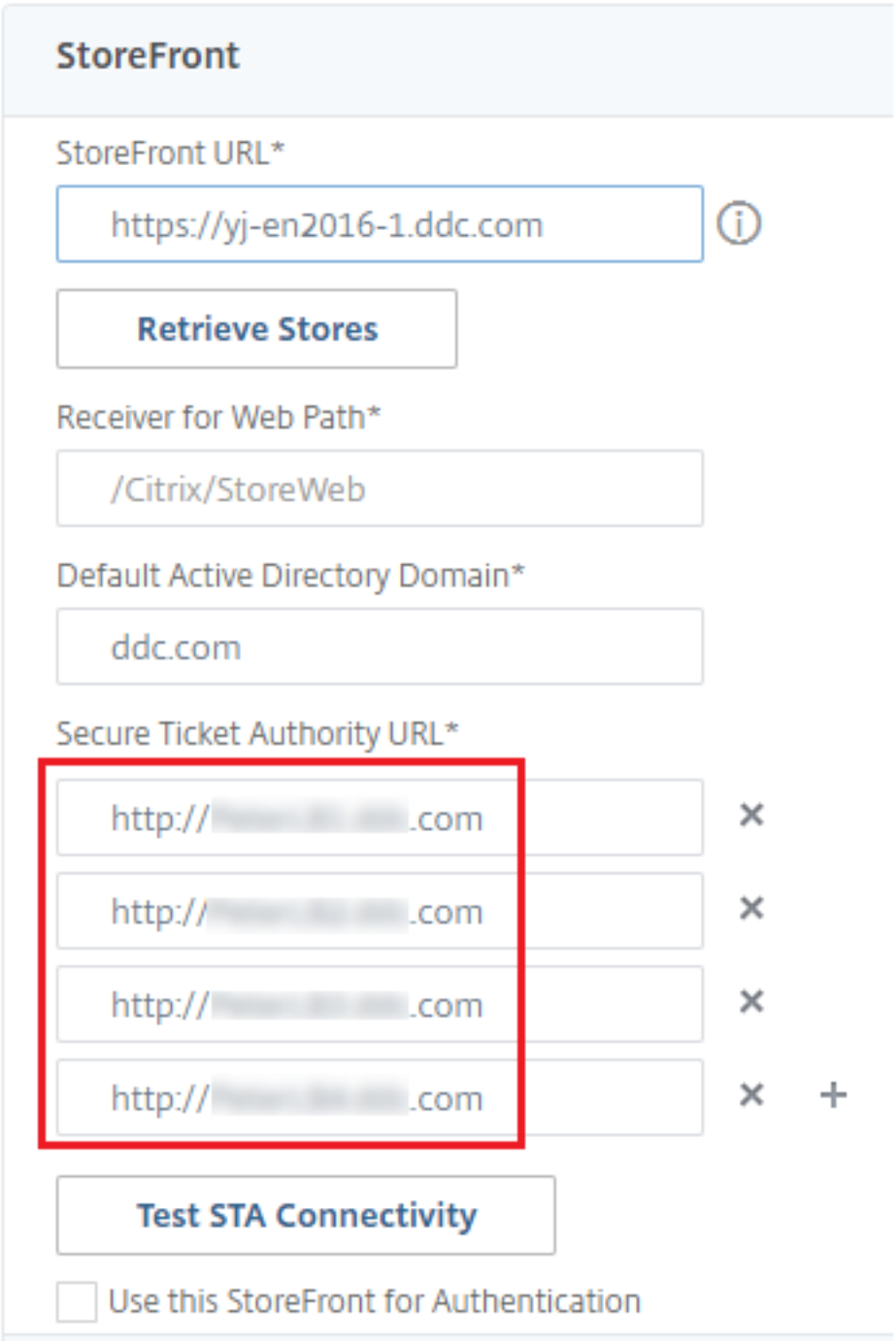

3. Nel riquadro StoreFront, fare clic sull'icona di modifica.




4. Aggiungere l'**URL Secure Ticket Authority**.

   - Se la funzionalità Secure XML è abilitata, l'URL STA deve essere l'URL del servizio di bilanciamento del carico.
   - Se la funzionalità Secure XML è disabilitata, l'URL STA deve essere l'URL di STA (indirizzo del DDC) e il parametro TrustRequestsSentToTheXmlServicePort sul DDC deve essere impostato su True.




## Sessioni

January 7, 2024

Mantenere l'attività della sessione è fondamentale per fornire la migliore esperienza utente. La

perdita di connettività dovuta a reti inaffidabili, latenza di rete altamente variabile e limitazioni di portata dei dispositivi wireless può essere frustrante per l'utente. Spostarsi rapidamente tra i dispositivi e accedere alle stesse applicazioni ad ogni accesso è una priorità per molti utenti mobili come gli operatori sanitari.

Le funzionalità descritte in questo articolo ottimizzano l'affidabilità delle sessioni, riducono gli inconvenienti, i tempi di inattività e la perdita di produttività; utilizzando queste funzionalità, gli utenti mobili possono spostarsi rapidamente e facilmente tra i dispositivi.

È inoltre possibile disconnettere un utente da una sessione, disconnettere una sessione e configurare il prelancio e la permanenza della sessione; vedere Gestire i gruppi di consegna

## Affidabilità della sessione

Session Reliability (Affidabilità delle sessioni) mantiene attive le sessioni e le mantiene sullo schermo dell'utente quando la connettività di rete viene interrotta. Gli utenti continuano a vedere l'applicazione che stanno utilizzando fino al ripristino della connettività di rete.

Questa funzione è particolarmente utile per gli utenti mobili con connessioni wireless. Ad esempio, un utente con connessione wireless entra in una galleria ferroviaria e perde momentaneamente la connettività. Normalmente, la sessione viene disconnessa, scomparendo dallo schermo dell'utente e l'utente deve riconnettersi alla sessione disconnessa. Con la funzione di affidabilità della sessione, la sessione rimane attiva sulla macchina. Per indicare la perdita di connettività, lo schermo dell'utente si blocca e il cursore diventa una clessidra rotante fino a quando la connettività non riprende al termine della galleria. L'utente continua ad accedere allo schermo durante l'interruzione e può riprendere l'interazione con l'applicazione quando viene ripristinata la connessione di rete. La funzione di affidabilità della sessione riconnette gli utenti senza richieste di riautenticazione.

Gli utenti dell'app Citrix Workspace non possono ignorare l'impostazione del controller.

È possibile utilizzare la funzione di affidabilità della sessione con Transport Layer Security (TLS). TLS crittografa solo i dati inviati tra il dispositivo utente e Citrix Gateway.

Abilitare e configurare l'affidabilità della sessione con le seguenti impostazioni dei criteri:

- L'impostazione dei criteri di connessione per l'affidabilità della sessione consente o impedisce l'affidabilità della sessione.
- L'impostazione del criterio di timeout per l'affidabilità della sessione ha un valore predefinito di 180 secondi o tre minuti. Sebbene sia possibile estendere la quantità di tempo in cui l'affidabilità della sessione mantiene aperta una sessione, questa funzione è progettata per la comodità dell'utente. Pertanto, non richiede all'utente la riautenticazione. Più si prolunga il tempo in cui una sessione viene mantenuta aperta, più aumentano le probabilità che un utente possa distrarsi e allontanarsi dal proprio dispositivo. Tali azioni possono potenzialmente lasciare la sessione accessibile a utenti non autorizzati.

- Le connessioni di affidabilità della sessione in entrata utilizzano la porta 2598, a meno che non si modifichi il numero di porta nell'impostazione del criterio del numero di porta di affidabilità della sessione.
- Per impedire agli utenti di riconnettersi a sessioni interrotte senza doversi autenticare nuovamente, utilizzare la funzione Auto Client Reconnect. È possibile configurare l'impostazione dei criteri di Auto Client Reconnect per richiedere agli utenti di riconnettersi nuovamente durante la riconnessione a sessioni interrotte.

Se si utilizza sia l'affidabilità della sessione che la riconnessione automatica del client, le due funzionalità funzionano in sequenza. L'affidabilità della sessione chiude (o disconnette) la sessione utente dopo il periodo di tempo specificato nell'impostazione del timeout dell'affidabilità della sessione. A quel punto avranno effetto le impostazioni di riconnessione automatica del client, che tentano di riconnettere l'utente alla sessione disconnessa.

### Riconnessione automatica del client

Con la funzione di riconnessione automatica del client, l'app Citrix Workspace è in grado di rilevare disconnessioni involontarie delle sessioni ICA e di ricollegare automaticamente gli utenti alle sessioni interessate. Quando questa funzione è abilitata sul server, gli utenti non devono riconnettersi manualmente per continuare a lavorare.

L'app Citrix Workspace tenta di riconnettersi alla sessione finché la connessione non viene ristabilita o fino a quando l'utente annulla i tentativi di riconnessione.

Per le sessioni desktop, l'app Citrix Workspace tenta di riconnettersi alla sessione per un periodo specificato, se non nel caso in cui vi è una riconnessione corretta o l'utente annulla i tentativi di riconnessione. Per impostazione predefinita, questo periodo è di cinque minuti. Per modificare questo periodo, modificare la seguente impostazione del Registro di sistema sul dispositivo utente (dove `seconds` è il numero di secondi dopo i quali non vengono effettuati più tentativi di riconnessione della sessione).

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds
; DWORD;<seconds>
```

Abilitare e configurare la riconnessione automatica del client con le seguenti impostazioni dei criteri:

- **Auto Client Reconnect:** abilita o disabilita la riconnessione automatica tramite l'app Citrix Workspace dopo che una connessione è stata interrotta.
- **Auto Client Reconnect authentication:** abilita o disabilita l'obbligo di autenticazione dell'utente dopo la riconnessione automatica.
- **Auto Client Reconnect logging:** abilita o disabilita la registrazione degli eventi di riconnessione nel registro eventi. La registrazione è disabilitata per impostazione predefinita. Quando

la registrazione è abilitata, il registro di sistema del server acquisisce informazioni sugli eventi di riconnessione automatica riusciti e non riusciti. Ogni server memorizza le informazioni sugli eventi di riconnessione nel proprio registro di sistema. Il sito non fornisce un registro combinato degli eventi di riconnessione per tutti i server.

> **Nota:**
>
> La riconnessione automatica del client senza riautenticazione è supportata solo per l'autenticazione tramite password. Se si utilizza Federated Authentication Service o l'autenticazione tramite smart card, la riconnessione automatica del client senza riautenticazione non è supportata. In questi casi, gli utenti vengono reindirizzati alla schermata di accesso.

La riconnessione automatica utente incorpora un meccanismo di autenticazione basato sulle credenziali utente crittografate. Al primo accesso di un utente, il server crittografa e memorizza le credenziali utente in memoria. Il server crea e invia inoltre un cookie contenente la chiave di crittografia all'app Citrix Workspace. L'app Citrix Workspace invia la chiave al server per la riconnessione. Il server decrittografa le credenziali e le invia all'accesso di Windows per l'autenticazione. Quando i cookie scadono, gli utenti devono autenticarsi nuovamente per riconnettersi alle sessioni.

I cookie non vengono utilizzati se si abilita l'impostazione di Auto Client Reconnect. Viene invece visualizzata una finestra di dialogo per gli utenti che richiedono le credenziali quando l'app Citrix Workspace tenta di riconnettersi automaticamente.

Per la massima protezione delle credenziali e delle sessioni utente, utilizzare la crittografia per tutte le comunicazioni tra i client e il sito.

Disabilitare la riconnessione automatica del client sull'app Citrix Workspace per Windows utilizzando il file icaclient.adm. Per ulteriori informazioni, vedere la documentazione dell'app Citrix Workspace per Windows.

Le impostazioni delle connessioni influiscono anche sulla riconnessione automatica del client:

- Per impostazione predefinita, la funzione Auto Client Reconnect è abilitata tramite le impostazioni dei criteri a livello di sito, come descritto in precedenza. La riautenticazione dell'utente non è richiesta. Tuttavia, se la connessione TCP ICA di un server è configurata per reimpostare le sessioni quando si interrrompe un collegamento di comunicazione, la riconnessione automatica non avviene. La riconnessione automatica del client funziona solo se il server disconnette le sessioni quando è presente una connessione interrotta o scaduta. In questo contesto, la connessione TCP ICA fa riferimento alla porta virtuale di un server (anziché a un'effettiva connessione di rete) che viene utilizzata per le sessioni su reti TCP/IP.
- Per impostazione predefinita, la connessione TCP ICA su un server è impostata per disconnettere le sessioni in caso di connessioni interrotte o scadute. Le sessioni disconnesse rimangono intatte nella memoria di sistema e sono disponibili per la riconnessione tramite l'app Citrix Workspace.

- La connessione può essere configurata per ripristinare o disconnettere le sessioni con connessioni interrotte o scadute. Quando una sessione viene reimpostata, il tentativo di riconnessione avvia una nuova sessione. Invece di riportare un utente nello stesso punto dell'applicazione in uso, l'applicazione viene riavviata.
- Se il server è configurato per reimpostare le sessioni, la riconnessione automatica del client crea una nuova sessione. In questo processo gli utenti dovranno immettere le proprie credenziali per accedere al server.
- La riconnessione automatica può non riuscire se l'app Citrix Workspace o il plug-in inviano informazioni di autenticazione errate, problema che potrebbe verificarsi durante un attacco, o se il server determina che è trascorso troppo tempo da quando ha rilevato la connessione interrotta.

### ICA Kep-Alive

L'abilitazione della funzione ICA Keep-Alive impedisce la disconnessione delle connessioni interrotte. Se la funzione è abilitata, quando il server non rileva attività, viene impedito a Servizi Desktop remoto di disconnettere la sessione. Esempi di mancanza di attività sono nessuna variazione dell'orologio, nessun movimento del mouse, nessun aggiornamento dello schermo. Il server invia pacchetti keep-alive ogni pochi secondi per rilevare se la sessione è attiva. Se la sessione non è più attiva, il server contrassegna la sessione come disconnessa.

> **Importante:**
>
> ICA Keep-Alive funziona solo se non si utilizza l'affidabilità della sessione. L'affidabilità della sessione ha i propri meccanismi per impedire la disconnessione delle connessioni interrotte. Configurare ICA Keep-Alive solo per le connessioni che non utilizzano l'affidabilità della sessione.

Le impostazioni ICA Keep-Alive sostituiscono le impostazioni keep-alive configurate in Criteri di gruppo Windows.

Abilitare e configurare ICA Keep-Alive con le seguenti impostazioni dei criteri:

- **ICA keep-alive timeout (Timeout ICA keep-alive)** specifica l'intervallo (1-3600 secondi) utilizzato per inviare messaggi ICA keep-alive. Non configurare questa opzione se si desidera che il software di monitoraggio della rete chiuda le connessioni inattive in ambienti in cui le connessioni interrotte sono così rare che consentire agli utenti di riconnettersi alle sessioni non è un problema.

  L'intervallo predefinito è 60 secondi: i pacchetti ICA Keep-Alive vengono inviati ai dispositivi utente ogni 60 secondi. Se un dispositivo utente non risponde in 60 secondi, lo stato delle sessioni ICA diventa disconnesso.

- **ICA keep alives:** invia o impedisce l'invio di messaggi ICA keep-alive.

### Controllo di Workspace

Il controllo di Workspace consente a desktop e applicazioni di seguire un utente da un dispositivo all'altro. Questa possibilità di roaming consente all'utente di accedere a tutti i desktop o di aprire le applicazioni da qualsiasi luogo semplicemente effettuando l'accesso, senza dover riavviare i desktop o le applicazioni su ciascun dispositivo. Ad esempio, il controllo dell'area di lavoro può aiutare gli operatori sanitari di un ospedale che devono spostarsi rapidamente tra diverse workstation e accedere allo stesso insieme di applicazioni a ogni accesso. Se si configurano le opzioni di controllo dell'area di lavoro per consentirlo, questi lavoratori possono disconnettersi da più applicazioni su un dispositivo client e quindi riconnettersi per aprire le stesse applicazioni su un dispositivo client diverso.

Il controllo dell'area di lavoro influisce sulle seguenti attività:

- **Accesso:** per impostazione predefinita, il controllo dell'area di lavoro consente agli utenti di riconnettersi automaticamente a tutti i desktop e le applicazioni in esecuzione durante l'accesso, senza doverli riaprire manualmente. Attraverso il controllo dell'area di lavoro, gli utenti possono aprire desktop o applicazioni disconnessi, oltre a quelli che sono attivi su un altro dispositivo client. La disconnessione da un desktop o da un'applicazione li lascia in esecuzione sul server. Se si hanno utenti in roaming che devono mantenere alcuni desktop o applicazioni in esecuzione su un dispositivo client mentre si riconnettono a un sottoinsieme dei loro desktop o applicazioni su un altro dispositivo client, è possibile configurare il comportamento di riconnessione di accesso per aprire solo i desktop o le applicazioni precedentemente disconnessi dall'utente.
- **Riconnessione:** dopo aver effettuato l'accesso al server, gli utenti possono riconnettersi a tutti i desktop o alle applicazioni in qualsiasi momento facendo clic su Riconnetti. Per impostazione predefinita, Reconnect apre i desktop o la applicazioni che sono disconnessi, oltre a quelli attualmente in esecuzione su un altro dispositivo client. È possibile configurare Reconnect per aprire solo i desktop o le applicazioni da cui l'utente si è disconnesso in precedenza.
- **Scollegamento:** per gli utenti che aprono desktop o applicazioni tramite StoreFront, è possibile configurare il comando **Log Off** perchè scolleghi l'utente da StoreFront e da tutte le sessioni attive o solo da StoreFront.
- **Disconnessione:** gli utenti possono disconnettersi da tutti i desktop e le applicazioni in esecuzione contemporaneamente, senza dover disconnettersi da ciascuno individualmente.

Il controllo dell'area di lavoro è disponibile solo per gli utenti dell'app Citrix Workspace che accedono a desktop e applicazioni tramite una connessione Citrix StoreFront. Per impostazione predefinita, il controllo dell'area di lavoro è disabilitato per le sessioni di desktop virtuale, ma è abilitato per le applicazioni ospitate. La condivisione delle sessioni non avviene per impostazione predefinita tra i desktop pubblicati e le applicazioni pubblicate in esecuzione all'interno di tali desktop.

I criteri utente, le mappature delle unità client e le configurazioni stampante cambiano come necessario quando un utente si sposta su un nuovo dispositivo client. I criteri e le mappature vengono

applicati nel modo corretto per il dispositivo client in cui l'utente ha effettuato l'accesso alla sessione. Ad esempio, un operatore sanitario si scollega da un dispositivo nel pronto soccorso e quindi accede a una postazione di lavoro nel laboratorio radiologico. I criteri, le mappature delle stampanti e le mappature delle unità client appropriate per la sessione nel laboratorio radiologico vengono applicati all'avvio della sessione.

È possibile personalizzare la scelta delle stampanti visibili agli utenti quando cambiano posizione. È inoltre possibile controllare se gli utenti possono stampare su stampanti locali, quanta larghezza di banda viene consumata quando gli utenti si connettono in remoto e altri aspetti della loro esperienza di stampa.

Per informazioni sull'attivazione e la configurazione del controllo dell'area di lavoro per gli utenti, vedere la documentazione di StoreFront.

### Roaming di sessione

> **Nota:**
>
> Le seguenti informazioni guidano l'utente nella configurazione del roaming delle sessioni utilizzando PowerShell. È anche possibile utilizzare invece Web Studio. Per ulteriori informazioni, vedere Gestire i gruppi di consegna.

Per impostazione predefinita, le sessioni sono in roaming fra i dispositivi client con l'utente. Quando l'utente avvia una sessione e si sposta su un altro dispositivo, viene utilizzata la stessa sessione e le applicazioni sono disponibili su entrambi i dispositivi. Seguono le applicazioni, indipendentemente dal dispositivo o dall'esistenza di sessioni correnti. Spesso seguono anche stampanti e altre risorse assegnate all'applicazione.

Sebbene questo comportamento predefinito offra molti vantaggi, potrebbe non essere l'ideale in tutti i casi. È possibile impedire il roaming di sessione utilizzando PowerShell SDK.

Esempio 1: un professionista medico utilizza due dispositivi, un PC desktop su cui compila un modulo assicurativo e un tablet su cui esamina le informazioni sul paziente.

- Se il roaming di sessione è abilitato, entrambe le applicazioni vengono visualizzate su entrambi i dispositivi (un'applicazione avviata su un dispositivo è visibile su tutti i dispositivi in uso). Ciò potrebbe non soddisfare i requisiti di sicurezza.
- Se il roaming di sessione è disabilitato, il registro paziente non viene visualizzato sul PC desktop e il modulo assicurativo non viene visualizzato sul tablet.

Esempio 2: un responsabile della produzione lancia un'applicazione sul PC nel suo ufficio. Il nome e la posizione del dispositivo determinano quali stampanti e altre risorse sono disponibili per quella sessione. Più tardi, si reca in un ufficio nell'edificio accanto per una riunione che richiederà l'uso di una stampante.

- Quando il roaming di sessione è abilitato, il responsabile della produzione probabilmente non sarebbe in grado di accedere alle stampanti più vicine alla sala riunioni, perché le applicazioni lanciate in precedenza nel suo ufficio hanno determinato l'assegnazione di stampanti e altre risorse vicino a quella posizione.
- Quando il roaming di sessione è disabilitato e accede a un altro computer (utilizzando le stesse credenziali), viene avviata una nuova sessione e le stampanti e le risorse che si trovano nelle vicinanze saranno disponibili.

#### Configurare il roaming di sessione

Per configurare il roaming di sessione, utilizzare i cmdlet delle regole dei criteri di autorizzazione riportati di seguito con la proprietà "SessionReconnection". Facoltativamente, è anche possibile specificare la proprietà "LeasingBehavior".

Per le sessioni di desktop:

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Per le sessioni delle applicazioni:

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Dove `value` può essere uno dei valori seguenti:

- **Always** (Sempre): le sessioni sono sempre in roaming, indipendentemente dal dispositivo client e dal fatto che la sessione sia connessa o disconnessa. Questo è il valore predefinito.
- **DisconnectedOnly** (Solo disconnnesse): riconnettersi solo alle sessioni già disconnesse; in caso contrario, avviare una nuova sessione Le sessioni possono eseguire il roaming tra i dispositivi client prima disconnettendoli o utilizzando Workspace Control per eseguire il roaming esplicitamente. Non viene mai utilizzata una sessione attiva connessa da un altro dispositivo client. Viene invece lanciata una nuova sessione.
- **SameEndpointOnly** (Solo stesso endpoint): un utente riceve una sessione univoca per ciascun dispositivo client che utilizza. Questo disabilita completamente il roaming. Gli utenti possono riconnettersi solo allo stesso dispositivo utilizzato in precedenza nella sessione.

La proprietà "LeasingBehavior"è descritta di seguito.

**Effetti di altre impostazioni:**

La disattivazione del roaming di sessione è influenzata dal limite dell'applicazione **Allow only one instance of the application per user** (Consenti solo un'istanza dell'applicazione per utente) impostato nelle proprietà dell'applicazione nel gruppo di consegna.

- Se si disabilità il roaming di sessione, disabilitare il limite di applicazione "Allow only one instance…".
- Se si abilita il limite di applicazione "Allow only one instance…", non configurare nessuno dei due valori che consentono nuove sessioni su nuovi dispositivi.

### Intervallo di accesso

Se una macchina virtuale contenente un VDA desktop si chiude prima del completamento del processo di accesso, è possibile assegnare più tempo al processo. Il valore predefinito per la versione 7.6 e le successive è 180 secondi (il valore predefinito per le versioni 7.0-7.5 è 90 secondi).

Sul computer (o sull'immagine master utilizzata in un catalogo di macchine), impostare la seguente chiave di registro:

Chiave:`HKLM\SOFTWARE\Citrix\PortICA`

- Valore: `AutoLogonTimeout`
- Tipo: `DWORD`
- Specificare un tempo decimale in secondi, nell'intervallo 0-3600.

Se si modifica un'immagine master, aggiornare il catalogo.

Questa impostazione si applica solo alle macchine virtuali con VDA desktop. Microsoft controlla il timeout di accesso sulle macchine con server VDA.

## Tag

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

### Introduzione

I tag sono stringhe che identificano elementi come macchine, applicazioni, desktop, gruppi di consegna, gruppi di applicazioni e criteri. Dopo aver creato un tag e averlo aggiunto a un elemento, è possibile personalizzare determinate operazioni per applicarle solo agli elementi che hanno un tag specificato.

- Personalizzare le schermate di ricerca in Web Studio.

  Ad esempio, per visualizzare solo le applicazioni ottimizzate per i tester, creare un tag denominato "test"e quindi aggiungerlo (applicarlo) a tali applicazioni. A quel punto è possibile filtrare la ricerca in Web Studio con il tag "test".

- Pubblicare applicazioni da un gruppo di applicazioni o desktop specifici da un gruppo di consegna, considerando solo un sottoinsieme di macchine in gruppi di consegna selezionati. Questa funzionalità è denominata *restrizione tag*.

  Con le restrizioni tag, è possibile utilizzare le macchine esistenti per più di un'attività di pubblicazione, risparmiando i costi associati alla distribuzione e alla gestione di macchine aggiuntive. Una restrizione tag può essere spiegata come una suddivisione (o la creazione di partizioni) delle macchine che fanno parte di un gruppo di consegna. La sua funzionalità è simile, ma non identica, ai gruppi di lavoro nelle versioni di XenApp precedenti alla 7.x.

  L'utilizzo di un gruppo di applicazioni o di desktop con una restrizione tag può essere utile per isolare e risolvere i problemi di un sottoinsieme di computer in un gruppo di consegna.

- Pianificare riavvii periodici per un sottoinsieme di macchine inclusi in un gruppo di consegna.

  L'utilizzo di una restrizione di tag per le macchine consente di utilizzare nuovi cmdlet PowerShell per configurare più pianificazioni di riavvio per sottoinsiemi di macchine inclusi in un gruppo di consegna. Per esempi e dettagli, vedere Gestire i gruppi di consegna.

- Personalizza l'applicazione (assegnazione) dei criteri Citrix in base a un sottoinsieme di computer in gruppi di consegna, tipi di gruppo di consegna o OU che hanno (o non hanno) un tag specificato.

  Ad esempio, se si desidera applicare un criterio Citrix solo alle workstation più potenti, aggiungere un tag denominato "high power"a tali macchine. Quindi, nella pagina **Assign Policy** (Assegna criterio) della creazione guidata criteri, selezionare il tag e la casella di controllo **Enable** (Abilita). È inoltre possibile aggiungere un tag a un gruppo di consegna e quindi applicare un criterio Citrix a tale gruppo. Per i dettagli, vedere Creare criteri.

È possibile applicare tag a:

- Macchine
- Applicazioni
- Cataloghi macchine (solo PowerShell; vedere Tag sui cataloghi di macchine)
- Gruppi di consegna
- Gruppi di applicazioni

È possibile configurare una restrizione tag che può essere configurata durante la creazione o la modifica di quanto segue in Web Studio:

- Un desktop in un gruppo di consegna condiviso

- Un gruppo di applicazioni

## Restrizioni tag per un desktop o un gruppo di applicazioni

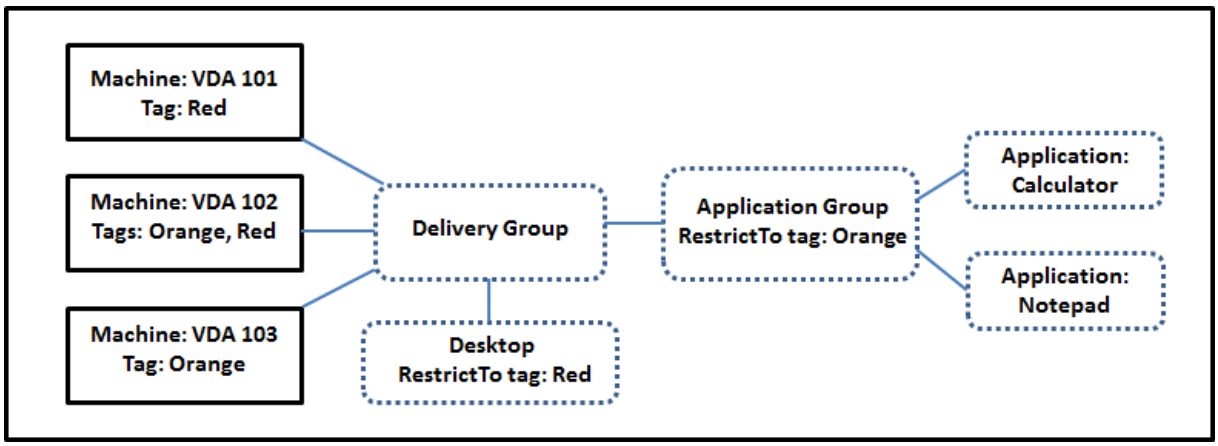
Una restrizione tag prevede diversi passaggi:

- Creare il tag e aggiungerlo (applicarlo) alle macchine.
- Creare o modificare un gruppo con la restrizione tag (in altre parole, "limitare i lanci alle macchine con tag x").

Una restrizione tag estende il processo di selezione della macchina del broker. Il broker seleziona una macchina da un gruppo di consegna associato soggetto a criteri di accesso, a elenchi utenti configurati, a preferenze di zona e a prontezza di avvio, oltre alla limitazione tag (se presente). Per le applicazioni, il broker torna ad altri gruppi di consegna in ordine di priorità, applicando le stesse regole di selezione macchine per ciascun gruppo di consegna considerato.

### Esempio 1: layout semplice

Questo esempio presenta un semplice layout che utilizza restrizioni di tag per limitare le macchine che vengono considerate per l'avvio di alcuni desktop e applicazioni. Il sito dispone di un gruppo di consegna condiviso, un desktop pubblicato e un gruppo di applicazioni configurato con due applicazioni.




- Sono stati aggiunti tag a ciascuna delle tre macchine (VDA 101-103).
- Il desktop del gruppo di consegna condiviso è stato creato con una restrizione tag denominata "Rosso". Un desktop può essere lanciato solo su macchine di quel gruppo di consegna che hanno il tag "Rosso": VDA 101 e 102.
- Il gruppo di applicazioni è stato creato con la restrizione dei tag "arancione", quindi ciascuna delle sue applicazioni (Calcolatrice e Blocco note) può essere avviata solo sulle macchine di quel gruppo di consegna che hanno il tag "arancione": VDA 102 e 103.

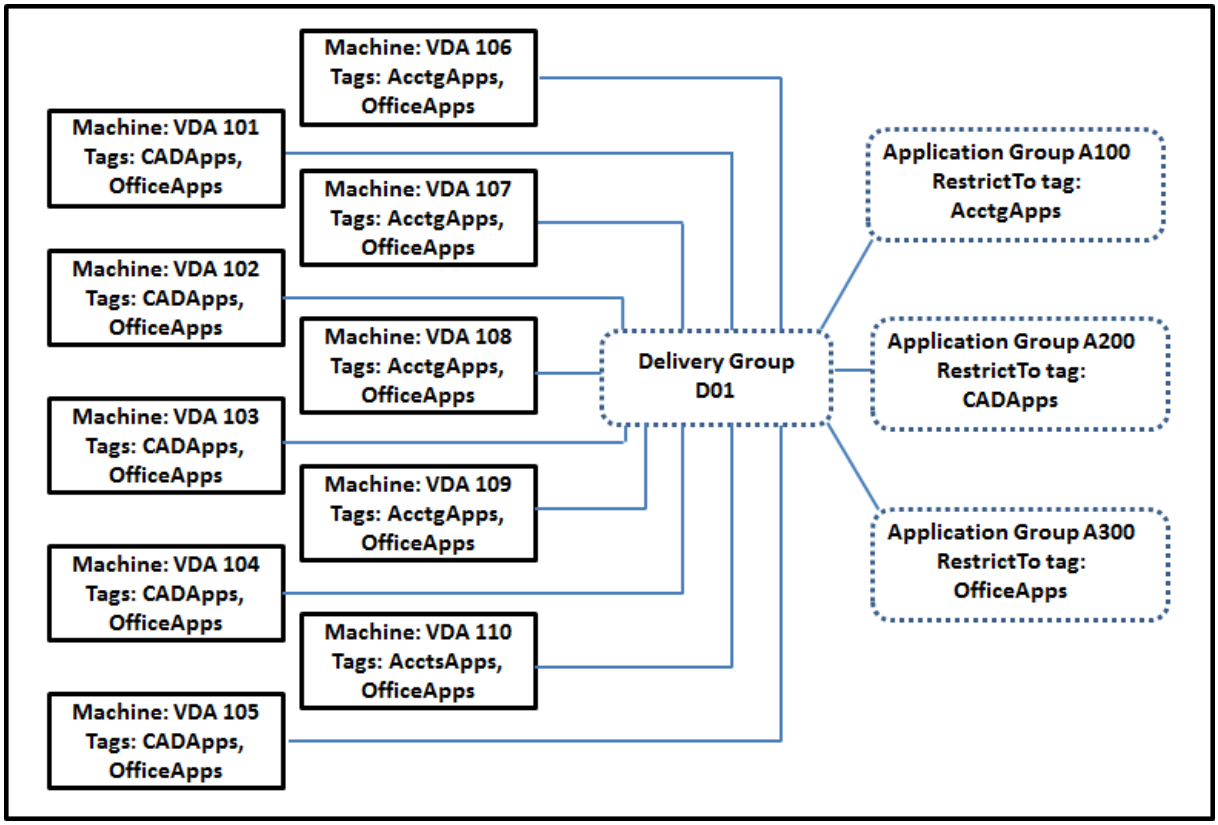
 

La macchina VDA 102 ha entrambi i tag (rosso e arancione), quindi può essere presa in considerazione per l'avvio delle applicazioni e del desktop.

### Esempio 2: layout più complesso

Questo esempio contiene diversi gruppi di applicazioni creati con restrizioni tag. Ciò si traduce nella capacità di fornire più applicazioni con meno macchine di quante sarebbero altrimenti necessarie se si utilizzassero solo gruppi di consegna.

Come configurare l'esempio 2 mostra i passaggi utilizzati per creare e applicare i tag, quindi configurare le restrizioni tag in questo esempio.




Questo esempio utilizza 10 macchine (VDA 101-110), un gruppo di consegna (D01) e tre gruppi di applicazioni (A100, A200, A300). Applicando tag a ciascuna macchina e specificando le restrizioni tag durante la creazione di ciascun gruppo di applicazioni:

- Gli utenti contabili del gruppo possono accedere alle app di cui hanno bisogno su cinque macchine (VDA 101—105)
- I progettisti CAD del gruppo possono accedere alle app di cui hanno bisogno su cinque macchine (VDA 106-110)
- Gli utenti del gruppo che necessitano di applicazioni Office possono accedere alle app Office su 10 computer (VDA 101-110)

Vengono utilizzate solo 10 macchine, con un solo gruppo di consegna. L'utilizzo dei gruppi di consegna da soli (senza gruppi di applicazioni) richiederebbe un numero doppio di macchine, poiché una macchina può appartenere a un solo gruppo di consegna.

## Gestire i tag e le restrizioni tag

I tag vengono creati, aggiunti (applicati), modificati ed eliminati dagli elementi selezionati tramite l'azione **Manage Tags** (Gestisci tag) in Web Studio.

Eccezione: I tag utilizzati per le assegnazioni dei criteri vengono creati, modificati ed eliminati tramite l'azione **Manage Tags** in Web Studio. Tuttavia, i tag vengono applicati (assegnati) quando si crea il criterio. Vedere Creare criteri per i dettagli.

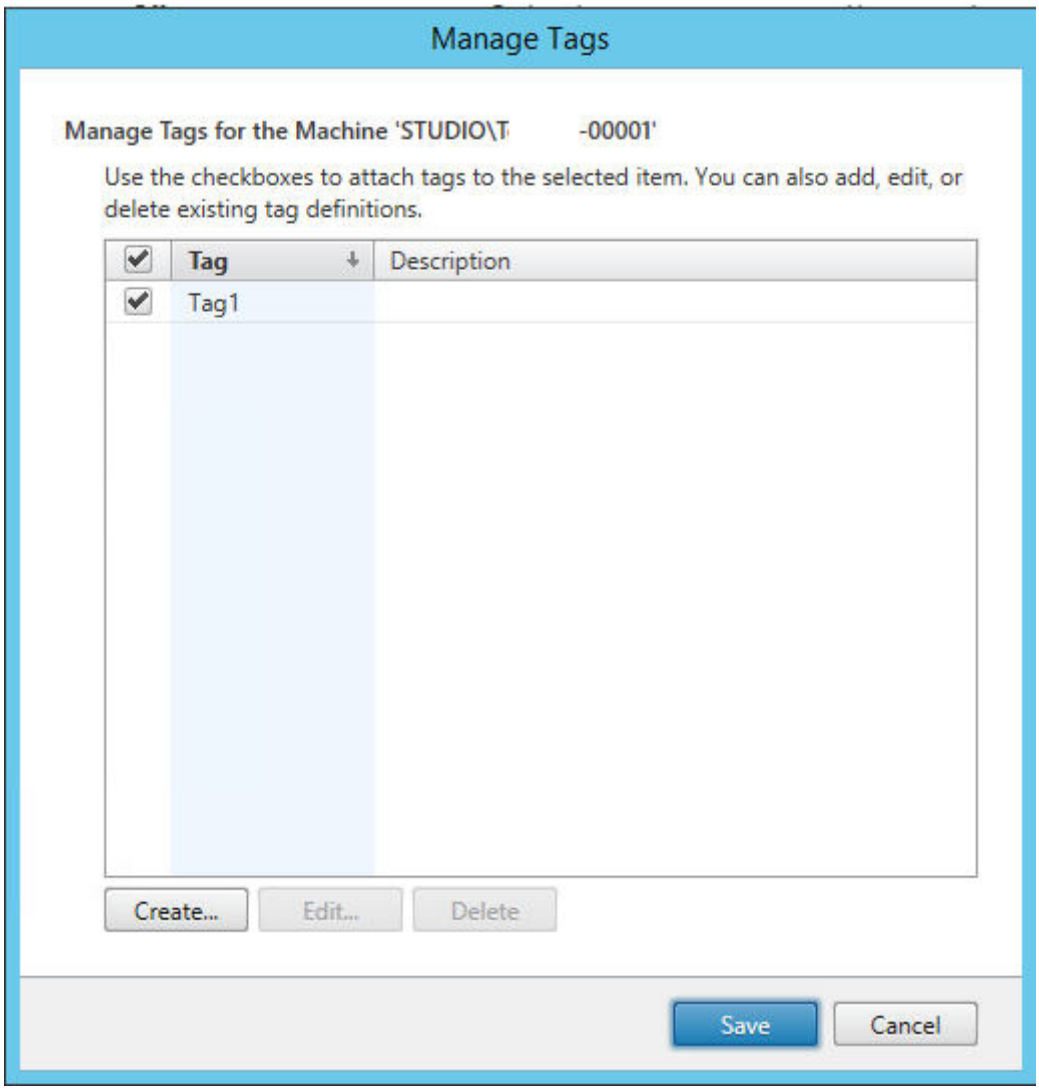
Le restrizioni tag vengono configurate quando si creano o modificano desktop nei gruppi di consegna e quando si creano e modificano gruppi di applicazioni.

### Utilizzare le finestre di dialogo Manage Tags in Studio

In Web Studio, selezionare gli elementi a cui si desidera applicare un tag (uno o più computer, applicazioni, un desktop, un gruppo di consegna o un gruppo di applicazioni) e quindi selezionare **Manage Tags** nella barra delle azioni. Nella finestra di dialogo sono elencati tutti i tag creati nel Sito, non solo per gli elementi selezionati.

- Una casella di controllo contenente un segno di spunta indica che il tag è già stato aggiunto agli elementi selezionati. Nell'acquisizione dello schermo sottostante, alla macchina selezionata viene applicato il tag denominato "Tag1".
- Se sono stati selezionati più elementi, una casella di controllo contenente un trattino indica che alcuni, ma non tutti gli elementi selezionati, hanno aggiunto quel tag.




Le seguenti azioni sono disponibili nella finestra di dialogo **Manage Tags** . Non mancare di leggere Avvertenze per quando si lavora con i tag.

- **Per creare un tag:**

  Fare clic su **Create** (Crea). Immettere un nome e una descrizione. I nomi dei tag devono essere univoci e non fanno distinzione tra maiuscole e minuscole Quindi fare clic su **OK**. La creazione di un tag non lo applica automaticamente agli elementi selezionati. Utilizzare le caselle di controllo per applicare il tag.

- **Per aggiungere (applicare) uno o più tag:**

  Abilitare la casella di controllo accanto al nome del tag. Se sono stati selezionati più elementi e la casella di controllo accanto a un tag contiene un trattino (che indica che il tag è già applicato ad alcuni degli elementi selezionati, ma non tutti), quando lo si sostituisce con un segno di spunta influisce su tutte le macchine selezionate.

Se si tenta di aggiungere un tag a una o più macchine e tale tag viene utilizzato come restrizione in un gruppo di applicazioni, tale azione può comportare la disponibilità di tali macchine per l'avvio. Se è quello che si intendeva fare, procedere.

- **Per rimuovere uno o più tag:**

  Deselezionare la casella di controllo accanto al nome del tag. Se sono stati selezionati più elementi e la casella di controllo accanto a un tag contiene un trattino (che indica che il tag è già applicato ad alcuni degli elementi selezionati, ma non tutti), svuotando la casella di controllo si elimina il tag da tutte le macchine selezionate.

  Se si tenta di rimuovere un tag da una macchina che utilizza tale tag come restrizione, tenere presente che l'azione può influire su quali macchine vengono considerate per l'avvio. Se è quello che si intendeva fare, procedere.

- **Per modificare un tag:**

  Selezionare un tag e fare clic su **Edit**. Immettere un nuovo nome, una descrizione o entrambi. È possibile modificare solo un tag alla volta.

- **Per eliminare uno o più tag:**

  Selezionare i tag e fare clic su **Delete**. La finestra di dialogo Delete Tag indica quanti elementi utilizzano attualmente i tag selezionati (ad esempio "2 macchine"). Fare clic su un elemento per visualizzare ulteriori informazioni. Ad esempio, facendo clic su un elemento "2 macchine", vengono visualizzati i nomi delle due macchine a cui è stato applicato il tag. Confermare se si desidera eliminare i tag.

  Non è possibile utilizzare Web Studio per eliminare un tag utilizzato come restrizione. Innanzitutto, modificare il gruppo di applicazioni e rimuovere la restrizione tag o selezionare un tag diverso.

Quando si è finito di utilizzare la finestra di dialogo **Manage Tags**, fare clic su **Save**.

Per verificare se a una macchina sono stati applicati dei tag: selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro di sinistra. Selezionare un gruppo di consegna, quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni. Selezionare una macchina nel riquadro centrale e quindi selezionare la scheda **Tags** nel riquadro **Details**.

#### Gestire le restrizioni tag

La configurazione di una restrizione tag è un processo in più passaggi: prima si crea il tag e lo si aggiunge/applica alle macchine. Quindi, si aggiunge la restrizione al gruppo di applicazioni o al desktop.

- **Creare e applicare il tag:**

Creare il tag e aggiungerlo (applicarlo) alle macchine interessate dalla restrizione dei tag, utilizzando le azioni **Manage Tags** descritte in precedenza.

- **Per aggiungere una restrizione tag a un gruppo di applicazioni:**

  Creare o modificare il gruppo di applicazioni. Nella pagina **Delivery Groups**, selezionare **Restrict launches to machines with the tag** (Limita avvii alle macchine con il tag) e quindi selezionare il tag dall'elenco.

- **Per modificare o rimuovere la restrizione tag relativa a un gruppo di applicazioni:**

  Modificare il gruppo. Nella pagina **Delivery Groups** selezionare un tag diverso dall'elenco o rimuovere completamente la restrizione tag deselezionando **Restrict launches to machines with the tag**.

- **Per aggiungere una restrizione tag a un desktop:**

  Creare o modificare un gruppo di consegna. Fare clic su **Add** o **Edit** nella pagina **Desktop**. Nella finestra di dialogo Add Desktop (Aggiungi desktop), selezionare **Restrict launches to machines with the tag** (Limita avvii alle macchine con il tag) e quindi selezionare il tag dal menu.

- **Per modificare o rimuovere la limitazione tag relativa a un gruppo di consegna:**

  Modificare il gruppo. Nella pagina Desktop, fare clic su **Edit**. Nella finestra di dialogo selezionare un tag diverso dall'elenco o rimuovere completamente la restrizione tag deselezionando **Restrict launches to machines with the tag**.

#### Avvertenze per quando si lavora con i tag

Un tag applicato a un elemento può essere utilizzato per scopi diversi, quindi tenere presente che l'aggiunta, la rimozione e l'eliminazione di un tag può avere effetti non voluti. È possibile utilizzare un tag per ordinare gli schermi delle macchine nel campo di ricerca di Web Studio. È possibile utilizzare lo stesso tag di una restrizione durante la configurazione di un gruppo di applicazioni o di un desktop. Il tag limita le macchine prese in considerazione per l'avvio solo a quelle di gruppi di consegna specificati che hanno quel tag.

Quando si tenta di aggiungere un tag alle macchine dopo che è stato configurato come restrizione di tag per un desktop o un gruppo di applicazioni, viene visualizzato un avviso. L'aggiunta di tale tag potrebbe rendere le macchine disponibili per l'avvio di applicazioni o desktop aggiuntivi. Se è quello che si intendeva fare, procedere. In caso contrario, è possibile annullare l'operazione.

Ad esempio, supponiamo che si crei un gruppo di applicazioni con la restrizione tag "Rosso". Successivamente, si aggiungono diverse altre macchine negli stessi gruppi di consegna utilizzati da quel gruppo di applicazioni. Se si tenta di aggiungere il tag "Rosso"a tali macchine, Web Studio visualizza un messaggio con un contenuto tipo: "Il tag "Rosso"viene utilizzato come restrizione nei seguenti

gruppi di applicazioni. L'aggiunta di questo tag potrebbe rendere le macchine selezionate disponibili all'avvio delle applicazioni di questo gruppo di applicazioni."È quindi possibile confermare o annullare l'aggiunta di quel tag a quelle macchine aggiuntive.

Analogamente, se un gruppo di applicazioni utilizza un tag per limitare gli avvii, Web Studio avverte che non è possibile eliminare il tag finché non si modifica il gruppo rimuovendo il tag come restrizione. Se è stato consentito eliminare un tag utilizzato come restrizione in un gruppo di applicazioni, ciò potrebbe comportare l'avvio delle applicazioni su tutti i computer inclusi nei gruppi di consegna associati al gruppo di applicazioni. Lo stesso divieto di eliminare un tag si applica se il tag viene utilizzato come restrizione per gli avvii di desktop. Dopo aver modificato il gruppo di applicazioni o i desktop del gruppo di consegna per rimuovere la restrizione tag, è possibile eliminare il tag.

Le macchine potrebbero non avere tutte lo stesso insieme di applicazioni. Un utente può appartenere a più di un gruppo di applicazioni, ognuno con una restrizione tag diversa e insiemi di computer diversi o sovrapposti inclusi in gruppi di consegna. La tabella seguente elenca come viene deciso quali macchine prendere in considerazione.

| **Quando è stata aggiunta un'applicazione a** | **Queste macchine incluse nei gruppi di consegna selezionati sono prese in considerazione per l'avvio.** |
|---|---|
| Un gruppo di applicazioni senza restrizioni tag | Qualsiasi macchina. |
| Un gruppo di applicazioni con restrizione tag A | Macchine a cui è applicato il tag A. |
| Due gruppi di applicazioni, uno con restrizione tag A e l'altro con restrizione tag B | Macchine con tag A e tag B. Se non ce ne sono disponibili, le macchine con tag A o tag B. |
| Due gruppi di applicazioni, uno con restrizione tag A e l'altro senza restrizioni tag | Macchine che hanno il tag A. Se non ce ne sono disponibili, allora qualsiasi macchina. |

Se si è utilizzata una restrizione tag in una pianificazione di riavvio del computer, eventuali modifiche apportate che influiscono sulle applicazioni di tag o sulle restrizioni influiscono sul successivo ciclo di riavvio del computer. Non influisce sui cicli di riavvio in corso mentre vengono apportate le modifiche.

#### Come configurare l'esempio 2

La sequenza seguente mostra i passaggi da seguire per creare e applicare tag, quindi per configurare le restrizioni tag per i gruppi di applicazioni illustrati nel secondo esempio.

VDA e applicazioni sono già stati installati sulle macchine e il gruppo di consegna è stato creato.

Creare e applicare tag alle macchine:

1. In Web Studio, selezionare il gruppo di consegna D01 e quindi **View Machines** (Visualizza macchine) nella barra delle azioni.
2. Selezionare le macchine VDA 101-105 e quindi selezionare **Manage Tags** nella barra delle azioni.
3. Nella finestra di dialogo Manage Tags fare clic su **Create** e quindi creare un tag denominato `CADApps`. Fare clic su **OK**.
4. Fare di nuovo clic su **Create** e creare un tag denominato OfficeApps. Fare clic su **OK**.
5. Mentre si è ancora nella finestra di dialogo **Manage Tags**, aggiungere (applicare) i tag appena creati alle macchine selezionate attivando le caselle di controllo accanto al nome di ciascun tag (`CADApps` e `OfficeApps`). Al termine, chiudere la finestra di dialogo.
6. Selezionare il gruppo di consegna D01, selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.
7. Selezionare le macchine VDA 106-110 e quindi selezionare **Manage Tags** nella barra delle azioni.
8. Nella finestra di dialogo **Manage Tags** fare clic su **Create**. Creare un tag denominato `AcctgApps`. Fare clic su **OK**.
9. Applicare il tag `AcctgApps` appena creato e il tag `OfficeApps` alle macchine selezionate facendo clic sulle caselle di controllo accanto ai nomi dei rispettivi tag, quindi chiudere la finestra di dialogo.

Creare i gruppi di applicazioni con restrizioni tag.

1. In Web Studio, selezionare **Applications** nel riquadro di sinistra, selezionare la scheda **Application Groups**, quindi selezionare **Create Application Group** nella barra delle azioni. Viene avviata la procedura guidata di creazione gruppo applicazioni.
2. Nella pagina **Delivery Groups** della procedura guidata, selezionare il gruppo di consegna D01. Selezionare **Restrict launches to machines with tag** (Limita lanci su macchine con tag), quindi selezionare il tag `AcctgApps` dall'elenco.
3. Completare la procedura guidata, specificando gli utenti contabili e le applicazioni di contabilità. Quando si aggiunge l'applicazione, scegliere l'origine **From Start menu** (Dal menu Start), che cerca l'applicazione sulle macchine che hanno il tag `AcctgApps`. Nella pagina **Summary**, assegnare al gruppo il nome `A100`.
4. Ripetere i passaggi precedenti per creare il gruppo di applicazioni `A200`, specificando le macchine che hanno il tag `CADApps`, oltre agli utenti e alle applicazioni appropriati.
5. Ripetere i passaggi per creare il gruppo di applicazioni `A300`, specificando le macchine che hanno il tag `OfficeApps`, oltre agli utenti e alle applicazioni appropriati.

#### Tag sui cataloghi di macchine

È possibile utilizzare i tag sui cataloghi delle macchine. La sequenza complessiva di operazioni per creare un tag e quindi applicarlo a un catalogo è la stessa descritta in precedenza. Tuttavia, l'applicazione di tag ai cataloghi è supportata solo tramite l'interfaccia PowerShell. Non è possibile utiliz-

zare Web Studio per applicare un tag a un catalogo o rimuovere un tag da un catalogo. Il catalogo visualizzato in Web Studio non indica se è applicato un tag.

Riepilogo: è possibile utilizzare Web Studio o PowerShell per creare o eliminare un tag da utilizzare in un catalogo. Utilizzare PowerShell per applicare il tag al catalogo.

Ecco alcuni esempi di utilizzo di tag con cataloghi:

- Un gruppo di consegna ha macchine provenienti da diversi cataloghi, ma si desidera che un' operazione (ad esempio una pianificazione di riavvio) riguardi solo le macchine di un catalogo specifico. Ciò si può ottenere applicando un tag a quel catalogo.
- In un gruppo di applicazioni, si desidera limitare le sessioni di applicazione alle macchine di un catalogo specifico. Ciò si può ottenere applicando un tag a quel catalogo.

Cmdlet PowerShell interessati:

- È possibile passare oggetti catalogo a cmdlet come `Add-BrokerTag` e `Remove-BrokerTag` .
- `Get-BrokerTagUsage` mostra quanti cataloghi contengono tag.
- `Get-BrokerCatalog` ha una proprietà denominata `Tags`.

Ad esempio, i cmdlet seguenti aggiungono un tag denominato `fy2018` al catalogo denominato `acctg`:
`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`. Il tag è stato creato in precedenza utilizzando Web Studio o PowerShell.

Per ulteriori informazioni e per la sintassi, vedere la guida dei cmdlet PowerShell.

### Ulteriori informazioni

Post del blog: Come assegnare desktop a server specifici.

## Utilizzare la ricerca in Studio

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Utilizzare la funzione di ricerca per visualizzare informazioni su macchine, sessioni, cataloghi di macchine, applicazioni o gruppi di consegna specifici. Dopo aver selezionato **Search** in Web Studio, sono disponibili diverse opzioni:

- Utilizzare le schede per elencare i computer in base al tipo (sistema operativo a sessione singola o multisessione) o per elencare tutte le sessioni.
- Inserire il nome nella casella di ricerca.
- Selezionare l'icona del filtro per eseguire una ricerca avanzata. Selezionare la freccia verso il basso per visualizzare un elenco della proprietà di ricerca. Selezionare il segno più per creare un'espressione con le proprietà dell'elenco.

Per salvare la ricerca, selezionare l'icona con i puntini di sospensione (...) e quindi selezionare **Save As** (Salva con nome). La ricerca viene visualizzata nell'elenco **Saved searches**. Per accedere all'elenco, selezionare la casella di ricerca. Per eliminare le ricerche salvate, selezionare la casella di ricerca e fare clic su **Clear**.

Quando si utilizzano i filtri per eseguire una ricerca avanzata, la finestra **Add filters** (Aggiungi filtri) viene visualizzata in primo piano, lasciando invariata la vista di sfondo. Dopo aver selezionato **Search**, vengono visualizzati i risultati della ricerca corrispondenti, con i criteri di filtro visualizzati accanto a **Filter**. Quando si chiude la finestra **Add filters**, i risultati rimangono. Per cancellare i filtri, selezionare l'icona X accanto ai criteri di filtro.

### Cercare cataloghi di macchine o gruppi di consegna

Non è possibile eseguire ricerche dal nodo **Machine Catalogs** o **Delivery Groups** perché la casella di ricerca non è disponibile. Utilizzare invece il nodo **Search** per cercare cataloghi di macchine o gruppi di consegna. Nel nodo **Search**, selezionare l'icona del filtro, aggiungere i filtri come segue e quindi selezionare **Search**.

Per visualizzare più criteri di ricerca, selezionare il segno più. Rimuovere i criteri di ricerca selezionando l'icona del cestino.

### Personalizzare le colonne da visualizzare

Quando si personalizzano le colonne, è possibile visualizzare le colonne contrassegnate con l' etichetta **Degrades performance** (Riduce le prestazioni). La selezione di tali colonne potrebbe ridurre le prestazioni della console. Dopo aver completato la personalizzazione, la tabella si aggiorna per visualizzare le colonne selezionate. La loro presenza potrebbe causare ritardi quando si aggiorna la tabella.

Se la personalizzazione contiene colonne che riducono le prestazioni, viene richiesto di determinare se conservarle. Il messaggio viene visualizzato dopo che si aggiorna la finestra del browser o ci si

scollega dalla console e quindi si accede. Se si decide di conservare le colonne, tenere presente le seguenti considerazioni:

- Per garantire le prestazioni della console, non è possibile aggiornare la tabella più di una volta al minuto. Questa restrizione si applica a tutte le schede: **Single-session OS Machines** (Macchine con sistema operativo a sessione singola), **Multi-session OS Machines** (Macchine con sistema operativo multisessione) e **Sessions** (Sessioni). Se si ha necessità di aggiornamenti più frequenti, rimuovere tutte le colonne che riducono le prestazioni.

### Esportare i risultati della ricerca in un file CSV

È possibile esportare i risultati della ricerca (fino a 10.000 articoli) in un file CSV. Il file viene salvato nella posizione di download predefinita del browser.

Questa funzionalità è disponibile sia per le macchine che per le sessioni. Per esportare i risultati della ricerca, fare clic sull'icona di esportazione nell'angolo in alto a destra. Il completamento dell'esportazione potrebbe richiedere fino a 1 minuto.

In ogni scheda del nodo Search (Cerca), non è possibile eseguire un'altra esportazione mentre è in corso un'esportazione.

### Suggerimenti per migliorare una ricerca

Tenere presenti i seguenti suggerimenti quando si utilizza la funzione di ricerca:

- Nel nodo **Search**, selezionare una colonna qualsiasi per ordinare gli elementi.
- Per visualizzare più caratteristiche da includere nella visualizzazione in cui è possibile cercare e ordinare, selezionare **Columns to Display** (Colonne da visualizzare) o fare clic su qualsiasi colonna e selezionare **Columns to Display**. Nella finestra **Columns to Display**, selezionare la casella di controllo accanto agli elementi da visualizzare e selezionare **Save** per uscire.

  > **Nota:**
  >
  > Gli elementi che riducono le prestazioni sono contrassegnati dall'etichetta **Degrades performance** .

- Per individuare un dispositivo utente connesso a una macchina, utilizzare **Client (IP)** e **Is**, quindi immettere l'indirizzo IP del dispositivo.
- Per individuare le sessioni attive, utilizzare **Session State**, **Is** e **Connected**.
- Per elencare tutte le macchine di un gruppo di consegna, selezionare **Delivery Groups** nel riquadro di sinistra. Selezionare il gruppo, quindi selezionare **View Machines** (Visualizza macchine) dalla barra delle azioni o dal menu di scelta rapida.

Quando si eseguono operazioni di ordinamento, tenere presenti le seguenti considerazioni:

- Se il numero di elementi non supera 5.000, è possibile fare clic su qualsiasi colonna per ordinare gli elementi in essa contenuti. Quando il numero supera 5.000, è possibile ordinare solo per nome o per utente corrente (a seconda della scheda in cui ci si trova). Per abilitare l'ordinamento, utilizzare i filtri per ridurre il numero di elementi a 5.000 o meno.
- Quando il numero di elementi è superiore a 500 ma non superiore a 5.000:
  - Tutti i dati vengono memorizzati nella cache locale per migliorare le prestazioni di ordinamento. Nelle schede **Single-session OS Machines** e**Multi-session OS Machines** si memorizzano nella cache i dati la prima volta che si fa clic su una colonna (qualsiasi colonna tranne la colonna **Name**) per l'ordinamento. Nella scheda **Sessions**, si memorizzano i dati nella cache la prima volta che si fa clic su una colonna (qualsiasi colonna tranne la colonna **Current User** (Utente corrente)) per ordinare. Di conseguenza, il completamento dell'ordinamento richiede più tempo. Per prestazioni più veloci, ordinare per nome o utente corrente oppure utilizzare i filtri per ridurre il numero di elementi.
  - Il seguente messaggio sotto la tabella indica che i dati sono memorizzati nella cache: Last refreshed: <`the time when you refreshed the table`>. In tal caso, le operazioni di ordinamento si basano su elementi che sono stati caricati in precedenza. Questi elementi potrebbero non essere aggiornati. Per aggiornarli, fare clic sull'icona di aggiornamento.

## Impostazioni

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

È possibile usare Web Studio per gestire queste impostazioni:

- Gestire l'autenticazione
- Programma di miglioramento dell'esperienza cliente Citrix
- Rimuovere i Delivery Controller
- Modificare il database di registrazione

- Impostare data e ora
- Abilitare l'assegnazione automatica di più utenti per l'accesso remoto al PC
- Abilitare la risoluzione DNS
- Abilitare l'attendibilità XML
- Gestire la chiave di sicurezza
- Impostare il timeout di inattività per la console Studio

### Gestire l'autenticazione

Per impostazione predefinita, gli utenti si autenticano su Web Studio utilizzando le proprie credenziali di dominio (nome utente e password). È possibile abilitare l'autenticazione integrata di Windows in modo che gli utenti possano accedere a Studio con le proprie credenziali di Windows, utilizzando Kerberos o NTLM. La disabilitazione dell'accesso con credenziali di dominio non è supportata.

> **Importante**
>
> L'autenticazione integrata di Windows non funziona quando Web Studio è configurato come proxy per i Delivery Controller.

Dopo aver abilitato l'opzione **Integrated Windows authentication** (Autenticazione Windows integrata), al successivo accesso gli utenti accedono automaticamente. Come utente, se non si riesce ad accedere automaticamente, seguire questi passaggi per configurare il browser Web in modo da consentire l'autenticazione Windows integrata.

Per Google Chrome:

1. Dal Pannello di controllo, selezionare Opzioni Internet.
2. Selezionare la scheda **Avanzate**.
3. Selezionare **Abilita l'autenticazione Windows integrata**.
4. Selezionare la scheda **Sicurezza**.
5. Selezionare **Intranet locale > Siti > Avanzate**.
6. Nella casella **Aggiungi questo sito Web all'area**:
    - Se Web Studio e Delivery Controller risiedono sullo stesso server, digitare l'URL dell'host che esegue Web Studio.
    - In caso contrario, digitare un dominio jolly. Esempio: se il Delivery Controller è in `ddc.domain.com`, digitare `*.domain.com`.
7. Fare clic su **Aggiungi > Chiudi**

Per Mozilla Firefox:

1. Dal browser, digitare `about:config` nella casella dell'URL.
2. Nella casella **Cerca**, digitare `network negotiate`.
3. Fare clic con il pulsante destro del mouse **su network.negotiate-auth.trusted-uris** e selezionare **Modifica**.
4. Nella casella **Inserisci il valore della stringa**:
   - Se Web Studio e il Delivery Controller risiedono sullo stesso server, aggiungere un elenco separato da virgole di URL e/o alias che fanno riferimento al nome del server che ospita Web Studio.
   - In caso contrario, aggiungere gli URL in questo modo. Esempio: se il Delivery Controller è in `ddc.domain.com`, digitare `*.domain.com`.

Dopo aver configurato il browser, è possibile fare clic su **Windows integrated sign-in** (Accesso integrato di Windows) nella pagina di accesso per riprovare.

Quando Web Studio e Delivery Controller sono installati su macchine diverse, affinché l'autenticazione integrata di Windows funzioni, è necessario abilitare l'opzione **Allow cross-origin access** (Consenti l'accesso multiorigine).

Seguire questi passaggi per **abilitare l'accesso multiorigine**:

1. Selezionare la casella di controllo **Allow cross-origin access**.
2. Aggiungere l'URL del server Web Studio all'elenco degli indirizzi consentiti.
3. Nel campo **Enter URL** (Inserisci URL), inserire l'URL. Fare clic su **Add** (Aggiungi) per aggiungerne altri, se necessario.

   > **Nota**
   >
   > - L'URL deve essere nel formato corretto:`<scheme>://<hostname>`. Assicurarsi che non contenga percorsi o barre finali.
   > - Sono supportati indirizzi IP e FQDNS. Quando si aggiunge un URL, assicurarsi che corrisponda al modo in cui si accede a Web Studio. Ad esempio, se si accede a Web Studio utilizzando un indirizzo IP, aggiungere l'URL basato sull'indirizzo IP all'elenco.
   > - Se si utilizza una porta non predefinita, assicurarsi di includere il numero di porta.

4. Fare clic su **Add** (Aggiungi) per aggiungerne altri, se necessario.
5. Al termine, fare clic su **Done** (Fine) per salvare e uscire.

### Impostare il fuso orario

Per personalizzare il formato di data e ora in base alle proprie preferenze, seguire questi passaggi:

1. Accedere a Web Studio e selezionare **Settings** nel riquadro a sinistra.
2. Individuare il riquadro **Date and time** (Data e ora) e fare clic su **Edit** per configurare le seguenti opzioni:
    - **Time format** (Formato ora):
        - Selezionare questa opzione per visualizzare l'ora utilizzando un orologio a 12 ore (09:00pm, ad esempio) o un orologio a 24 ore (21:00, ad esempio).
    - **Date format** (Formato data):
        - Configurare il formato della data in base alle proprie preferenze, ad esempio gg/MM/aaaa.
    - **Time zone** (Fuso orario):
        - **UTC:** visualizza la data e l'ora in UTC in tutta l'interfaccia utente. Passando il mouse sulla data e l'ora vengono visualizzate le informazioni nel fuso orario locale.
        - **Local time zone** (Fuso orario locale): consente di visualizzare la data e l'ora nel fuso orario locale in tutta l'interfaccia utente. Passando il mouse sulla data e l'ora vengono visualizzate le informazioni in UTC.

### Abilitare la risoluzione DNS

Per presentare i nomi DNS anziché gli indirizzi IP nel file ICA, seguire questi passaggi:

1. Accedere a Web Studio e selezionare **Settings** nel riquadro a sinistra.
2. Attivare l'impostazione **Enable DNS resolution** (Abilita risoluzione DNS).

### Impostare il timeout di inattività per la console Studio

È possibile impostare il tempo di inattività dopoil quale gli amministratori si disconnettono automaticamente dalla console Studio.

1. Accedere a Web Studio e selezionare **Settings** nel riquadro a sinistra.
2. Digitare una durata compresa tra 10 minuti e 24 ore.
3. Per applicare questa impostazione, aggiornare la pagina o uscire e quindi accedere nuovamente.

# Profili utente

January 7, 2024

Per impostazione predefinita, Citrix Profile Management viene installato silenziosamente sulle immagini master quando si installa Virtual Delivery Agent, ma non è necessario utilizzare Profile Management come soluzione di profilo.

Per soddisfare le diverse esigenze degli utenti, è possibile utilizzare i criteri Citrix Virtual Apps and Desktops per applicare diversi comportamenti relativi al profilo alle macchine di ciascun gruppo di consegna. Ad esempio, un gruppo di consegna potrebbe richiedere profili obbligatori Citrix, il cui modello è memorizzato in una posizione di rete, mentre un altro gruppo di consegna richiede profili di roaming Citrix archiviati in un'altra posizione con diverse cartelle reindirizzate.

- Se altri amministratori dell'organizzazione sono responsabili dei criteri di Citrix Virtual Apps and Desktops, collaborare con loro per assicurarsi che impostino i criteri per il profilo nei gruppi di consegna.
- I criteri di Profile Management possono essere impostati anche in Criteri di gruppo, nel file .ini di Profile Management e localmente sulle singole macchine virtuali. Questi diversi modi di definire il comportamento del profilo vengono letti nel seguente ordine:

  1. Criteri di gruppo (file .adm o .admx)
  2. Criteri di Citrix Virtual Apps and Desktops nel nodo Policy
  3. Criteri locali sulla macchina virtuale a cui l'utente si connette
  4. File .ini di Profile Management

  Ad esempio, se si configura lo stesso criterio sia nei criteri di gruppo che nel nodo Policy, il sistema legge l'impostazione dei criteri nei criteri di gruppo e ignora l'impostazione dei criteri di Citrix Virtual Apps and Desktops.

Qualunque sia la soluzione di profilo scelta, gli amministratori di Director possono accedere alle informazioni diagnostiche e risolvere i problemi dei profili utente. Per ulteriori informazioni, vedere la documentazione di Director.

## Configurazione automatica

Il tipo di desktop viene rilevato automaticamente, in base all'installazione di Virtual Delivery Agent e, in aggiunta alle scelte di configurazione effettuate in Studio, vengono impostati di conseguenza i valori predefiniti di Profile Management.

I criteri regolati da Profile Management sono illustrati nella tabella seguente. Tutte le impostazioni dei criteri non predefinite vengono mantenute e non vengono sovrascritte da questa funzionalità. Vedere

la documentazione di Profile Management per informazioni su ciascun criterio. I tipi di macchine che creano profili influiscono sui criteri che vengono regolati. I fattori principali sono il fatto che le macchine siano persistenti o sottoposte a provisioning e che siano condivise da più utenti o dedicate a un solo utente.

I sistemi persistenti hanno un qualche tipo di archiviazione locale, il cui contenuto persiste quando il sistema si spegne. I sistemi persistenti potrebbero utilizzare tecnologie di archiviazione come le SAN per fornire l'imitazione del disco locale. Invece i sistemi sottoposti a provisioning vengono creati "al volo"da un disco di base e da un qualche tipo di disco di identità. L'archiviazione locale viene solitamente imitata da un disco RAM o da un disco di rete, quest'ultimo spesso fornito da una SAN con un collegamento ad alta velocità. La tecnologia di provisioning è generalmente Citrix Provisioning o Machine Creation Services (o equivalente di terze parti). A volte i sistemi sottoposti a provisioning dispongono di archiviazione locale persistente. Questi sono classificati come persistenti.

Insieme, questi due fattori definiscono i seguenti tipi di macchina:

- **Sia persistente che dedicata**. Alcuni esempi sono le macchine con sistema operativo a sessione singola con assegnazione statica e archiviazione locale persistente create con Machine Creation Services, le workstation fisiche e i computer portatili.
- **Sia persistente che condivisa**. Alcuni esempi sono le macchine con sistema operativo multisessione create con Machine Creation Services e i server Citrix Virtual Apps.
- **Sia con provisioning che dedicate**. Alcuni esempi sono le macchine OS a sessione singola con assegnazione statica ma senza archiviazione persistente create con Citrix Provisioning Service (in Citrix Virtual Desktops).
- **Sia con provisioning che condivise**. Alcuni esempi sono le macchine con sistema operativo a sessione singola con assegnazione casuale create con Citrix Provisioning Service (in Citrix Virtual Desktops) e i server Citrix Virtual Apps.

Per i diversi tipi di macchine sono suggerite le seguenti impostazioni dei criteri di Profile Management. Funzionano bene nella maggior parte dei casi, ma potrebbe essere utile deviare da essi a seconda dei requisiti della propria distribuzione.

> **Importante:**
>
> I criteri **Delete locally cached profiles on logoff** (Elimina i profili dalla cache locale allo scollegamento), **Profile streaming** (Streaming dei profili) e **Always cache** (Memorizza sempre nella cache) vengono applicati dalla funzione di configurazione automatica. Regolare manualmente gli altri criteri.

**Macchine persistenti**

| Criterio | Sia persistente che dedicata | Sia persistente che condivisa |
|---|---|---|
| Delete locally cached profiles on logoff (Elimina i profili memorizzati nella cache locale allo scollegamento) | Disabilitato | Abilitato |
| Profile streaming (Streaming del profilo) | Disabilitato | Abilitato |
| Always cache (Memorizza sempre nella cache) | Abilitato (nota 1) | Disabilitato (nota 2) |
| Active write back (Scrittura attiva) | Disabilitato | Disabilitato (nota 3) |
| Process logons of local administrators (Elabora accessi degli amministratori locali) | Abilitato | Disabilitato (nota 4) |

**Macchine con provisioning**

| Criterio | Sia con provisioning che dedicate | Sia con provisioning che condivise |
|---|---|---|
| Delete locally cached profiles on logoff (Elimina i profili memorizzati nella cache locale allo scollegamento) | Disabilitato (nota 5) | Abilitato |
| Profile streaming (Streaming del profilo) | Abilitato | Abilitato |
| Always cache (Memorizza sempre nella cache) | Disabilitato (nota 6) | Disabilitato |
| Active write back (Scrittura attiva) | Abilitato | Abilitato |
| Process logons of local administrators (Elabora accessi degli amministratori locali) | Abilitato | Abilitato (nota 7) |

1. Poiché lo **streaming dei profili** è disabilitato per questo tipo di macchina, l'impostazione **Always cache** viene sempre ignorata.
2. Disabilitare **Always cache**. Tuttavia, è possibile assicurarsi che i file di grandi dimensioni vengano caricati nei profili prima possibile dopo l'accesso abilitando questo criterio e utilizzan-

dolo per definire un limite di dimensioni file (in MB). Qualsiasi file di dimensioni pari o superiori o superiori viene memorizzato nella cache locale prima possibile.

3. Disabilitare **Active write back** (Riscrittura attiva) tranne per salvare le modifiche nei profili degli utenti in roaming tra i server Citrix Virtual Apps. In questo caso, abilitare questo criterio.
4. Disabilitare **Process logons of local administrators** (Elabora accessi degli amministratori locali) ad eccezione dei desktop condivisi ospitati. In questo caso, abilitare questo criterio.
5. Disabilitare **Delete locally cached profiles on logoff** (Elimina i profili memorizzati nella cache locale allo scollegamento) Questa impostazione mantiene i profili memorizzati nella cache locale. Poiché le macchine vengono reimpostate allo scollegamento, ma sono assegnate ai singoli utenti, gli accessi sono più veloci se i loro profili vengono memorizzati nella cache.
6. Disabilitare **Always cache**. Tuttavia, è possibile assicurarsi che i file di grandi dimensioni vengano caricati nei profili prima possibile dopo l'accesso abilitando questo criterio e utilizzandolo per definire un limite di dimensioni file (in MB). Qualsiasi file di dimensioni pari o superiori o superiori viene memorizzato nella cache locale prima possibile.
7. Abilitare **Process logons of local administrators**, tranne che per i profili degli utenti in roaming tra i server Citrix Virtual Apps and Desktops. In questo caso, disabilitare questo criterio.

### Reindirizzamento cartelle

Il reindirizzamento delle cartelle consente di memorizzare i dati utente su condivisioni di rete diverse dalla posizione in cui sono memorizzati i profili. Il reindirizzamento delle cartelle riduce le dimensioni del profilo e il tempo di caricamento, ma potrebbe influire sulla larghezza di banda della rete. Il reindirizzamento delle cartelle non richiede l'utilizzo di profili utente Citrix. È possibile scegliere di gestire autonomamente i profili utente e comunque reindirizzare le cartelle.

Configurare il reindirizzamento delle cartelle utilizzando i criteri Citrix in Studio.

- Assicurarsi che le posizioni di rete utilizzate per archiviare il contenuto delle cartelle reindirizzate siano disponibili e dotate delle autorizzazioni corrette. Le proprietà della posizione sono convalidate.
- Le cartelle reindirizzate vengono configurate sulla rete e vengono popolate con contenuti tratti dai desktop virtuali degli utenti all'accesso.

Configurare il reindirizzamento delle cartelle utilizzando solo i criteri Citrix o gli oggetti dei criteri di gruppo di Active Directory, non entrambi. La configurazione del reindirizzamento delle cartelle utilizzando entrambi i motori di criteri potrebbe determinare un comportamento imprevedibile.

### Reindirizzamento avanzato delle cartelle

Nelle distribuzioni con più sistemi operativi, è possibile che alcuni profili di un utente siano condivisi da tutti i sistemi operativi. Il resto del profilo non è condiviso e viene utilizzato solo da un sistema oper-

ativo. Per garantire un'esperienza utente coerente nei diversi sistemi operativi, è necessaria una configurazione diversa per ciascun sistema operativo, ovvero il reindirizzamento avanzato delle cartelle. Ad esempio, diverse versioni di un'applicazione in esecuzione su due sistemi operativi potrebbero dover leggere o modificare un file condiviso, quindi si decide di reindirizzarlo in un unica posizione di rete a cui entrambe le versioni possono accedere a tale file condiviso. In alternativa, poiché il contenuto della cartella **Start Menu** è strutturato in modo diverso in due sistemi operativi, si decide di reindirizzare una sola cartella, non entrambe. Questo approccio separa la cartella **Start Menu** e il relativo contenuto su ciascun sistema operativo, garantendo un'esperienza coerente per gli utenti.

Se la distribuzione richiede un reindirizzamento avanzato delle cartelle, è necessario comprendere la struttura dei dati del profilo degli utenti e determinare quali parti possono essere condivise tra i sistemi operativi. Può determinarsi un comportamento imprevedibile a meno che il reindirizzamento delle cartelle non venga utilizzato correttamente.

Per reindirizzare le cartelle nelle distribuzioni avanzate:

- Utilizzare un gruppo di consegna separato per ciascun sistema operativo.
- Cercare di comprendere dove le proprie applicazioni virtuali, incluse quelle sui desktop virtuali, memorizzano i dati e le impostazioni degli utenti e come sono strutturati i dati.
- Per i dati di profilo condivisi che possono essere in roaming sicuro (poiché sono strutturati in modo identico in ciascun sistema operativo), reindirizzare le cartelle che li contengono in ciascun gruppo di consegna.
- Per i dati di profilo non condivisi che non possono essere in roaming, reindirizzare la cartella che li contiene solo in uno dei gruppi desktop, in genere quella con il sistema operativo più utilizzato o quella in cui i dati sono più rilevanti. In alternativa, per i dati non condivisi che non possono essere in roaming tra i sistemi operativi, reindirizzare le cartelle che li contengono su entrambi i sistemi in posizioni di rete separate.

#### Esempio di distribuzione avanzata

La distribuzione dispone di applicazioni, incluse versioni di Microsoft Outlook e Internet Explorer, in esecuzione su desktop e applicazioni Windows 10, incluse altre versioni di Outlook e Internet Explorer, fornite da Windows Server 2019. Sono stati già configurati due gruppi di consegna per i due sistemi operativi. Gli utenti desiderano accedere allo stesso insieme di **Contatti** e **Preferiti** in entrambe le versioni delle due applicazioni.

**Importante:** le seguenti decisioni e consigli sono validi per i sistemi operativi e la distribuzione descritti. Nell'organizzazione, le cartelle che si sceglie di reindirizzare e la scelta di condividerle o meno dipendono da vari fattori che sono unici per la distribuzione specifica.

- Utilizzando i criteri applicati ai gruppi di consegna, è possibile scegliere le seguenti cartelle da reindirizzare.

| Cartella | Reindirizzata in Windows 10? | Reindirizzata in Windows Server 2019? |
|---|---|---|
| Documenti personali | Sì | Sì |
| Dati applicazioni | No | No |
| Contatti | Sì | Sì |
| Desktop | Sì | No |
| Download | No | No |
| Preferiti | Sì | Sì |
| Collegamenti | Sì | No |
| Musica | Sì | Sì |
| Immagini | Sì | Sì |
| Video | Sì | Sì |
| Ricerche | Sì | No |
| Giochi salvati | No | No |
| Menu Start | Sì | No |

- Per le cartelle condivise e reindirizzate:
  - Dopo aver analizzato la struttura dei dati salvati dalle diverse versioni di Outlook e Internet Explorer, si decide che è sicuro condividere le cartelle **Contatti** e **Preferiti**.
  - Si sa che la struttura delle cartelle **Documenti**, **Musica**, **Immagini** e **Video** è standard per tutti i sistemi operativi. Quindi è sicuro archiviare queste cartelle nella stessa posizione di rete per ciascun gruppo di consegna.
- Per le cartelle non condivise e reindirizzate:
  - Non reindirizzare la cartella Desktop, Collegamenti, Ricerche o **Menu Start** nel gruppo di consegna di Windows Server perché i dati contenuti in queste cartelle sono organizzati in modo diverso nei due sistemi operativi. Pertanto non può essere condivisa.
  - Per garantire un comportamento prevedibile di questi dati non condivisi, è necessario reindirizzarli solo nel gruppo di consegna di Windows 10. Windows 10 viene utilizzato più spesso dagli utenti nel loro lavoro quotidiano. Gli utenti accedono solo occasionalmente alle applicazioni fornite da Windows Server. Inoltre, in questo caso i dati non condivisi sono più rilevanti per un ambiente desktop piuttosto che per un ambiente applicativo. Ad esempio, i collegamenti sul desktop vengono memorizzate nella cartella **Desktop** e

potrebbero essere utili se provengono da un computer Windows 10 ma non da un computer Windows Server.

- Per le cartelle non reindirizzate:
  - Non si desidera ingombrare i server con i file scaricati dagli utenti, quindi si sceglie di non reindirizzare la cartella Download
  - I dati provenienti da singole applicazioni possono causare problemi di compatibilità e prestazioni, quindi si decide di non reindirizzare la cartella Dati applicazioni.

Per ulteriori informazioni sul reindirizzamento delle cartelle, vedere Panoramica del reindirizzamento delle cartelle, dei file non in linea e dei profili utente in roaming.

### Reindirizzamento delle cartelle ed esclusioni

In Citrix Profile Management (ma non in Studio), un miglioramento delle prestazioni consente di impedire l'elaborazione delle cartelle utilizzando esclusioni. Se si utilizza questa funzione, non escludere le cartelle reindirizzate. Le funzioni di reindirizzamento e di esclusione delle cartelle funzionano insieme. Assicurandosi che non vengano escluse cartelle reindirizzate si consente a Profile Management di spostarle nuovamente nella struttura di cartelle del profilo e si preserva l'integrità dei dati se in seguito si decide di non reindirizzarle. Per ulteriori informazioni sulle esclusioni, vedere Includere ed escludere elementi.

## Registrazione dei VDA

April 3, 2024

### Introduzione

> **Nota:**
>
> In un ambiente locale, i VDA si registrano con un Delivery Controller. In un ambiente con servizio Citrix Cloud, i VDA si registrano con un Cloud Connector. In un ambiente ibrido, alcuni VDA si registrano con un Delivery Controller mentre altri si registrano con un Cloud Connector.

Prima di poter essere utilizzato, un VDA deve registrarsi (stabilire una comunicazione) con uno o più controller o Cloud Connector nel sito. Il VDA trova un controller o un connettore controllando un elenco denominato `ListofDDCs`. Il `ListOfDDCs` di un VDA contiene voci DNS che indicano il VDA ai Controller o ai Cloud Connector presenti nel sito. Per ottenere il bilanciamento del carico, il VDA

distribuisce automaticamente le connessioni tra tutti i controller o i Cloud Connector inclusi nell'elenco.

Perché la registrazione VDA è così importante?

- Dal punto di vista della sicurezza, la registrazione è un'operazione sensibile. Si sta stabilendo una connessione tra il controller o il Cloud Connector e il VDA. Per un'operazione così sensibile, il comportamento previsto è quello di rifiutare la connessione se tutto non è in perfetta forma. Si stanno di fatto stabilendo due canali di comunicazione separati: da VDA a Controller o Cloud Connector e da Controller o Cloud Connector a VDA. La connessione utilizza Kerberos, quindi la sincronizzazione dell'ora e le questioni di appartenenza al dominio sono inflessibili. Kerberos utilizza Service Principal Names (SPN), quindi non è possibile utilizzare IP con bilanciamento del carico\nome host.
- Se un VDA non dispone di informazioni accurate e aggiornate su Controller o Cloud Connector durante l'aggiunta e la rimozione di Controller (o Cloud Connector), il VDA potrebbe rifiutare gli avvii di sessione che sono mediati da un Controller o Cloud Connector non elencato. Le voci non valide possono ritardare l'avvio del software del sistema desktop virtuale. Un VDA non accetta una connessione da un controller o Cloud Connector sconosciuto e non attendibile.

Oltre a `ListofDDCs`, il `ListOfSIDs` (ID di sicurezza) indica quali computer contenuti in `ListofDDCs` sono attendibili. `ListofSIDs` può essere utilizzato per ridurre il carico su Active Directory o per evitare possibili minacce alla sicurezza da parte di un server DNS compromesso. Per ulteriori informazioni, vedere ListOfSIDs.

Se un `ListofDDCs` specifica più controller o Cloud Connector, il VDA tenta di connettersi ad essi in ordine casuale. In una distribuzione locale, `ListofDDCs` può contenere anche gruppi di controller. Il VDA tenta di connettersi a ciascun controller di un gruppo prima di passare ad altre voci del `ListofDDCs`.

Citrix Virtual Apps and Desktops verifica automaticamente la connettività ai controller o ai Cloud Connector configurati durante l'installazione dei VDA. Vengono visualizzati messaggi di errore se non è possibile raggiungere un controller o un Cloud Connector. Se si ignora un avviso indicante che non è possibile contattare un controller o Cloud Connector (o quando non si specificano indirizzi di controller o Cloud Connector durante l'installazione di VDA), compaiono messaggi che lo ricordano.

### Metodi per configurare gli indirizzi dei controller o Cloud Connector

L'amministratore sceglie il metodo di configurazione da utilizzare quando il VDA si registra per la prima volta (la registrazione iniziale). Durante la registrazione iniziale, viene creata una cache persistente sul VDA. Durante le registrazioni successive, il VDA recupera l'elenco dei controller o dei Cloud Connector dalla cache locale, a meno che non venga rilevata una modifica della configurazione.

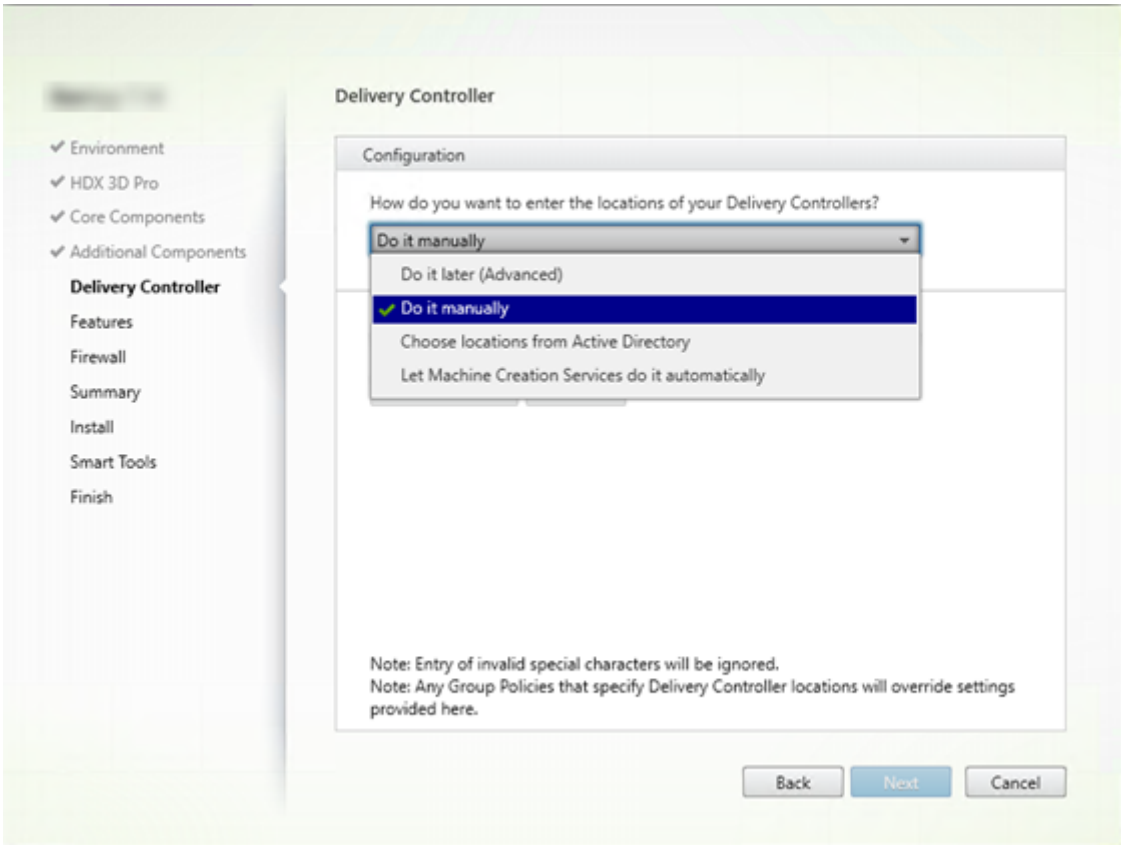
Il modo più semplice di recuperare tale elenco durante le registrazioni successive è utilizzare la funzione di aggiornamento automatico. L'aggiornamento automatico è abilitato per impostazione predefinita. Per ulteriori informazioni, vedere Aggiornamento automatico.

Esistono diversi metodi per configurare gli indirizzi dei controller o del Cloud Connector su un VDA.

- Basato su criteri (LGPO o Criteri di gruppo)
- Basato sul registro (manuale, Preferenze Criteri di gruppo (GPP), specificato durante l'installazione di VDA)
- Basato su unità organizzative di Active Directory (rilevamento dell'unità organizzativa legacy)
- Basato su MCS (personality.ini)

Si specifica il metodo di registrazione iniziale quando si installa un VDA. Se si disabilita l'aggiornamento automatico, il metodo selezionato durante l'installazione dei VDA viene utilizzato per le registrazioni successive.

L'immagine seguente mostra la pagina **Delivery Controller** della procedura guidata di installazione VDA.



#### Basato su criteri (LGPO\Criteri di gruppo)

Citrix consiglia di utilizzare un oggetto Criteri di gruppo per la registrazione iniziale del VDA. Ha la massima priorità. Sebbene l'aggiornamento automatico sia elencato come massima priorità, l'aggiornamento automatico viene utilizzato solo dopo la registrazione iniziale. La registrazione basata su criteri offre i vantaggi di centralizzazione dell'utilizzo di Criteri di gruppo per la configurazione.

Per specificare questo metodo, completare entrambi i passaggi seguenti:

- Nella pagina **Delivery Controller** della procedura guidata di installazione VDA, selezionare **Do it later (advanced)** (Fai in seguito (avanzato)). La procedura guidata ricorda più volte di specificare gli indirizzi del controller, anche se non li si sta specificando durante l'installazione del VDA (la registrazione del VDA è così importante).
- Abilitare o disabilitare la registrazione VDA basata su criteri tramite i criteri Citrix con l'impostazione `Virtual Delivery Agent Settings > Controllers`. Se la sicurezza è la massima priorità, usare l'impostazione `Virtual Delivery Agent Settings > Controller SIDs`.

Questa impostazione è memorizzata in `HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`.

#### Basato sul registro

Per specificare questo metodo, completare uno dei seguenti passaggi:

- Nella pagina **Delivery Controller** della procedura guidata di installazione VDA, selezionare **Do it manually** (Eseguire manualmente). Quindi, immettere il nome di dominio completo di un controller installato e quindi fare clic su **Add**. Se sono stati installati più controller, aggiungerne gli indirizzi.
- Per un'installazione VDA dalla riga di comando, utilizzare l'opzione /controllers e specificare le gli indirizzi completi dei controller o dei Cloud Connector installati.

Queste informazioni sono memorizzate nel valore del Registro di sistema `ListOfDDCs` sotto la chiave del Registro di sistema `HKLM\Software\Citrix\VirtualDesktopAgent` o `HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`.

È inoltre possibile configurare questa chiave del Registro di sistema manualmente o utilizzare Preferenze Criteri di gruppo (GPP). Questo metodo potrebbe essere preferibile al metodo basato su criteri (ad esempio, se si desidera l'elaborazione condizionale di controller o Cloud Connector diversi, ad esempio: utilizzare XDC-001 per i computer con nome che inizia con XDW-001-).

Aggiornare la chiave `ListOfDDCs` del Registro di sistema, che elenca i nomi di dominio completi di tutti i controller o Cloud Connector presenti nel sito. Questa chiave è l'equivalente dell'unità organizzativa del sito di Active Directory.

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs` (`REG_SZ`)

Se la posizione `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent` del Registro di sistema contiene entrambe le chiavi `ListOfDDCs` e `FarmGUID`, la chiave `ListOfDDCs` viene utilizzata per l'individuazione di controller o Cloud Connector. `FarmGUID` è presente se è stata specificata un'unità organizzativa del sito durante l'installazione del VDA. Questo metodo potrebbe essere utilizzato nelle distribuzioni legacy.

Facoltativamente, aggiornare la chiave `ListOfSIDs` del Registro di sistema (per ulteriori informazioni, vedere ListOfSIDs:

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs` (`REG_SZ`)

Ricordare: se si abilita anche la registrazione VDA basata su criteri tramite i criteri Citrix, questa ignora le impostazioni specificate durante l'installazione del VDA, poiché si tratta di un metodo con priorità più elevata.

#### Basato su Active Directory (legacy)

Questo metodo è supportato principalmente per la compatibilità con le versioni precedenti e non è raccomandato. Se lo si sta ancora utilizzando, Citrix suggerisce di passare a un altro metodo.

Per specificare questo metodo, completare entrambi i passaggi seguenti:

- Nella pagina **Delivery Controller** della procedura guidata di installazione VDA, selezionare **Choose locations from Active Directory** (Scegli posizioni da Active Directory).
- Usare lo script `Set-ADControllerDiscovery.ps1` (disponibile su ogni controller). Inoltre, configurare la voce `FarmGuid` del Registro di sistema su ciascun VDA in modo che punti all'unità organizzativa corretta. Questa impostazione può essere configurata utilizzando Criteri di gruppo.

#### Basato su MCS

Se si utilizza MCS per il provisioning delle VM, MCS imposta l'elenco dei controller o dei Cloud Connector. Questa funzione è attiva con l'aggiornamento automatico. Durante la creazione del catalogo, MCS inserisce l'elenco dei controller o dei Cloud Connector nel file `Personality.ini` durante il provisioning iniziale. L'aggiornamento automatico mantiene aggiornato l'elenco.

Per specificare questo metodo, nella pagina **Delivery Controller** della procedura guidata di installazione VDA, selezionare **Let Machine Creation Services do it** (Lascialo fare a Machine Creation Services).

#### Revisione e consigli

Come best practice:

- Utilizzare il metodo di registrazione di Criteri di gruppo per la registrazione iniziale.
- Utilizzare l'aggiornamento automatico (abilitato per impostazione predefinita) per mantenere aggiornato l'elenco dei controller.
- In una distribuzione multizona, utilizzare Criteri di gruppo per la configurazione iniziale (con almeno due controller o Cloud Connector). Puntare i VDA sui Controller o i Cloud Connector locali della loro zona. Utilizzare l'aggiornamento automatico per mantenerli aggiornati. L'aggiornamento automatico ottimizza automaticamente l'elenco `ListofDDCs` per i VDA nelle zone satellite.
- Elencare più di un controller sulla chiave `ListOfDDCs` del Registro di sistema, separati da uno spazio o una virgola, per evitare problemi di registrazione se un controller non è disponibile. Ad esempio:

```
DDC7x.xd.local DDC7xHA.xd.local

32-bit: HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
   ListOfDDCs

HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
   ListOfDDCs (REG_SZ)
<!--NeedCopy-->
```

- Assicurarsi che tutti i valori elencati in `ListofDDCs` siano mappati su un nome di dominio completo valido per evitare ritardi nella registrazione all'avvio.

### Aggiornamento automatico

L'aggiornamento automatico (introdotto in XenApp e XenDesktop 7.6) è abilitato per impostazione predefinita. È il metodo più efficiente per mantenere aggiornate le registrazioni VDA. Sebbene non sia utilizzato per la registrazione iniziale, il software di aggiornamento automatico scarica e memorizza l'elenco `ListofDDCs` in una cache persistente sul VDA al momento della registrazione iniziale. Questo processo viene eseguito per ogni VDA. La cache contiene anche le informazioni sui criteri della macchina, le quali assicurano che le impostazioni dei criteri vengano mantenute fra un riavvio e l'altro.

L'aggiornamento automatico è supportato quando si utilizza MCS o Citrix Provisioning per eseguire il provisioning di macchine, a eccezione della cache lato server Citrix Provisioning. La cache lato server non è uno scenario comune perché non esiste uno spazio di archiviazione persistente per l'aggiornamento automatico della cache.

Per specificare questo metodo:

- Abilitare o disabilitare l'aggiornamento automatico tramite un criterio Citrix contenente l'impostazione `Virtual Delivery Agent Settings` > `Enable auto update of Controllers`. Questa impostazione è abilitata per impostazione predefinita.

Come funziona:

- Ogni volta che un VDA si ri-registra (ad esempio, dopo il riavvio del computer), la cache viene aggiornata. Ogni controller o Cloud Connector controlla anche il database del sito ogni 90 minuti. Se è stato aggiunto o rimosso un controller o un Cloud Connector dall'ultimo controllo o se vi è stato un cambiamento dei criteri che influisce sulla registrazione VDA, il controller o il Cloud Connector invia un elenco aggiornato ai VDA registrati e la cache viene aggiornata. Il VDA accetta connessioni da tutti i controller o i Cloud Connector nell'elenco memorizzato nella cache più recente.
- Se un VDA riceve un elenco che non include il controller o il Cloud Connector con cui viene registrato (in altre parole, il controller o il Cloud Connector sono stati rimossi dal sito), il VDA si registra nuovamente scegliendo tra i controller o i Cloud Connector inclusi nell'elenco `ListofDDCs`.

Esempio:

- Una distribuzione dispone di tre controller: VDA A, B e C. Un VDA si registra con il controller B (specificato durante l'installazione del VDA).
- Successivamente, al sito vengono aggiunti due controller (D ed E). Entro 90 minuti, i VDA ricevono gli elenchi aggiornati e quindi accettano le connessioni dai controller A, B, C, D ed E (il carico non viene distribuito equamente a tutti controller fino al riavvio dei VDA).
- Successivamente, il controller B viene spostato in un altro sito. Entro 90 minuti, i VDA nel sito originale ricevono elenchi aggiornati perché c'è stata una modifica del controller dopo l'ultimo controllo. Il VDA originariamente registrato con il controller B (che non è più presente nell'elenco) si registra nuovamente, scegliendo tra i controller inclusi nell'elenco corrente (A, C, D ed E).

In una distribuzione multizona, l'aggiornamento automatico in una zona satellite memorizza automaticamente nella cache tutti i controller locali. Tutti i controller della zona principale sono memorizzati nella cache in un gruppo di backup. Se non sono disponibili controller locali nella zona satellite, viene tentata la registrazione con i controller della zona principale.

Come illustrato nell'esempio seguente, il file di cache contiene nomi host e un elenco degli ID di sicurezza (`ListofSIDs`). Il VDA non esegue query sui SID, il che riduce il carico di Active Directory.


È possibile recuperare il file cache con una chiamata WMI. Tuttavia, viene memorizzato in una posizione leggibile solo dall'account SYSTEM.

> **Importante:**
>
> Queste informazioni sono fornite solo a scopo informativo. NON MODIFICARE QUESTO FILE. Qualsiasi modifica a questo file o cartella comporta una configurazione non supportata.

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation"-Class "
Citrix_VirtualDesktopInfo"-Property "PersistentDataLocation"
```

Se è necessario configurare manualmente l'elenco `ListofSIDs` per motivi di sicurezza (in un processo distinto dalla riduzione del carico di Active Directory), non è possibile utilizzare la funzionalità di aggiornamento automatico. Per i dettagli, vedere ListOfSIDs.

#### Eccezione alla priorità di aggiornamento automatico

Sebbene l'aggiornamento automatico di solito abbia la priorità più alta fra tutti i metodi di registrazione VDA e sostituisca le impostazioni di altri metodi, esiste un'eccezione. Gli elementi `NonAutoListOfDDCs` presenti nella cache specificano il metodo di configurazione iniziale del VDA. L'aggiornamento automatico monitora queste informazioni. Se il metodo di registrazione iniziale cambia, il processo di registrazione salta l'aggiornamento automatico e utilizza il metodo di priorità configurato più alto. Questo processo può essere utile quando si sposta un VDA in un altro sito (ad esempio durante il ripristino d'emergenza).

### Considerazioni sulla configurazione

Visualizza una configurazione di registrazione VDA comune.

Si tratta di un video incorporato. Fare clic sul collegamento per guardare il video

Visualizza le fasi di registrazione del VDA.

Si tratta di un video incorporato. Fare clic sul collegamento per guardare il video

Considerare quanto segue durante la configurazione di elementi che possono influire sulla registrazione dei VDA.

#### Indirizzi dei controller o dei Cloud Connector

Indipendentemente dal metodo utilizzato per specificare controller o Cloud Connector, Citrix consiglia di utilizzare un indirizzo con nome di dominio completo. Un indirizzo IP non è considerato una configurazione attendibile, perché è più facile compromettere un IP rispetto a un record DNS. Se si compila `ListofSIDs` manualmente, è possibile utilizzare un IP in un `ListofDDCs`. Tuttavia, il nome di dominio completo è comunque consigliato.

#### Bilanciamento del carico

Come notato in precedenza, il VDA distribuisce automaticamente le connessioni tra tutti i controller o i Cloud Connector inclusi nell'elenco `ListofDDCs`. La funzionalità di failover e bilanciamento del carico è integrata nel Citrix Brokering Protocol (CBP). Se si specificano più controller o Cloud Connector nella configurazione, la registrazione va automaticamente in failover tra di essi, se necessario. Con l'aggiornamento automatico, il failover automatico si verifica automaticamente per tutti i VDA.

Per motivi di sicurezza, non è possibile utilizzare un sistema di bilanciamento del carico di rete, come Citrix ADC. La registrazione VDA utilizza l'autenticazione reciproca Kerberos, in cui il client (VDA) deve dimostrare la propria identità al servizio (controller). Tuttavia, il controller o il Cloud Connector devono dimostrare la propria identità al VDA. Ciò significa che il VDA e il controller o il Cloud Connector agiscono contemporaneamente come server e client. Come notato all'inizio di questo articolo, ci sono due canali di comunicazione: da VDA a controller/Cloud Connector e da controller/Cloud Connector a VDA.

Un componente di questo processo è denominato Service Principal Name (SPN), che è memorizzato come proprietà in un oggetto computer di Active Directory. Quando si connette a un controller o a un Cloud Connector, il VDA deve specificare con chi desidera comunicare. Questo indirizzo è un SPN. Se si utilizza un IP con bilanciamento del carico, l'autenticazione Kerberos reciproca riconosce correttamente che l'IP non appartiene al controller o al Cloud Connector previsto.

Per ulteriori informazioni, vedere:

- Introduzione a Kerberos
- Autenticazione reciproca con Kerberos

#### L'aggiornamento automatico sostituisce CNAME

La funzione di aggiornamento automatico sostituisce la funzione CNAME (alias DNS) che era disponibile nelle versioni di XenApp e XenDesktop precedenti alla 7.x. La funzionalità CNAME è disabilitata

a partire da XenApp e XenDesktop 7. Usare l'aggiornamento automatico anziché CNAME. Se è necessario utilizzare CNAME, vedere CTX137960. Perché l'aliasing DNS funzioni in modo coerente, evitare di utilizzare sia l'aggiornamento automatico che il CNAME allo stesso tempo.

#### Gruppi di controller/Cloud Connector

In alcuni scenari, potrebbe essere bene elaborare controller o Cloud Connector in gruppi, dove un gruppo è il preferito e l'altro gruppo viene utilizzato in caso di failover se tutti i controller/Cloud Connector si arrestano. Ricordare che i controller o i Cloud Connector sono selezionati casualmente dall'elenco, quindi il raggruppamento può aiutare a applicarne l'uso preferenziale.

Questi gruppi sono destinati all'uso all'interno di un singolo sito (non più siti).

Usare le parentesi per specificare i gruppi di controller o i Cloud Connector. Ad esempio, con quattro controller (due primari e due di backup), un raggruppamento potrebbe essere:

```
(XDC-001.cdz.lan XDC-002.cdz.lan)(XDC-003.cdz.lan XDC-004.cdz.lan)
```

In questo esempio, i controller del primo gruppo (001 e 002) vengono elaborati per primi. Se entrambi si arrestano, vengono elaborati i controller del secondo gruppo (003 e 004).

Con XenDesktop 7.0 o versioni successive, è necessario eseguire un ulteriore passaggio per utilizzare la funzione **Registration Groups** (Gruppi di registrazione). È necessario scegliere **Prohibit** (Vieta) in corrispondenza del criterio **Enable Auto Update of Controller** (Abilita aggiornamento automatico del controller) da Studio.

### ListOfSIDs

L'elenco dei controller che un VDA può contattare per la registrazione è denominato `ListofDDCs`. Un VDA deve anche sapere quali controller considerare attendibili; i VDA non considerano automaticamente attendibili i controller inclusi nell'elenco `ListofDDCs`. L'elenco `ListofSIDs` (ID di sicurezza) identifica i controller attendibili. I VDA tentano di registrarsi solo con controller attendibili.

Nella maggior parte degli ambienti, l'elenco `ListofSIDs` viene generato automaticamente a partire dall'elenco `ListofDDCs`. È possibile utilizzare una traccia CDF per leggere `ListofSIDs`.

In genere, non è necessario modificare manualmente `ListofSIDs`. Esistono diverse eccezioni. Le prime due eccezioni non sono più valide perché sono disponibili tecnologie più recenti.

- **Ruoli separati per i controller:** prima che venissero introdotte le zone in XenApp e XenDesktop 7.7, l'elenco `ListofSIDs` veniva configurato manualmente quando per la registrazione veniva utilizzato solo un sottoinsieme di controller. Ad esempio, se si utilizzavano XDC-001 e XDC-002 come broker XML e XDC-003 e XDC-004 per la registrazione VDA, venivano specificati tutti

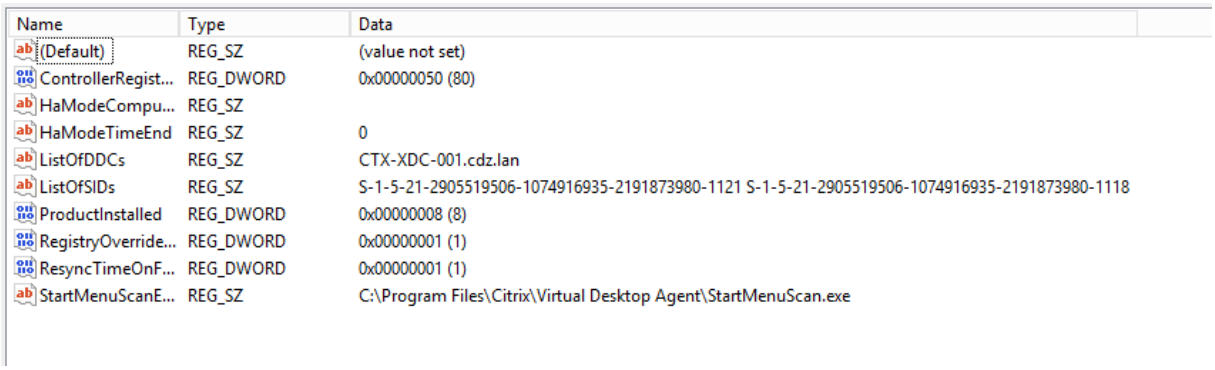
i controller inclusi nell'elenco `ListofSIDs` e XDC-003 e XDC-004 nell'elenco `ListofDDCs`. Questa configurazione non è tipica né consigliata. Non utilizzarla negli ambienti più recenti. Usare invece le zone.

- **Riduzione del carico di Active Directory:** prima che la funzionalità di aggiornamento automatico venisse introdotta in XenApp e XenDesktop 7.6, l'elenco `ListofSIDs` era utilizzato per ridurre il carico dei controller di dominio. Precompilando l'elenco `ListofSIDs`, è possibile saltare la risoluzione dai nomi DNS ai SID. Tuttavia, la funzione di aggiornamento automatico rimuove la necessità di questo lavoro, poiché questa cache persistente contiene SID. Citrix consiglia di mantenere abilitata la funzione di aggiornamento automatico.
- **Sicurezza:** in alcuni ambienti altamente protetti, i SID dei controller attendibili sono stati configurati manualmente per evitare possibili minacce alla sicurezza da parte di un server DNS compromesso. Tuttavia, in tal caso, è necessario disabilitare anche la funzione di aggiornamento automatico. In caso contrario, viene utilizzata la configurazione dalla cache persistente.

Quindi, a meno che non si abbia un motivo specifico per farlo, non modificare l'elenco `ListofSIDs`.

Se è necessario modificare l'elenco `ListofSIDs`, creare una chiave del Registro di sistema denominata `ListOfSIDs` (`REG_SZ`) in `HKLM\Software\Citrix\VirtualDesktopAgent`. Il valore è un elenco dei SID attendibili, separati da spazi se ne esiste più di uno.

Nell'esempio seguente, viene utilizzato un controller per la registrazione VDA (`ListofDDCs`), ma vengono utilizzati due controller per l'intermediazione (ListOfSIDs).



| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| ControllerRegist... | REG_DWORD | 0x00000050 (80) |
| HaModeCompu... | REG_SZ | |
| HaModeTimeEnd | REG_SZ | 0 |
| ListOfDDCs | REG_SZ | CTX-XDC-001.cdz.lan |
| ListOfSIDs | REG_SZ | S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118 |
| ProductInstalled | REG_DWORD | 0x00000008 (8) |
| RegistryOverride... | REG_DWORD | 0x00000001 (1) |
| ResyncTimeOnF... | REG_DWORD | 0x00000001 (1) |
| StartMenuScanE... | REG_SZ | C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe |

### Ricerca del controller durante la registrazione del VDA

Quando un VDA tenta di registrarsi, l'agente Broker esegue prima una ricerca DNS nel dominio locale per garantire che il controller specificato possa essere raggiunto.

Se nella ricerca iniziale non viene trovato il controller, l'agente Broker può avviare una query top-down di fallback in AD. Questa query cerca in tutti i domini e si ripete frequentemente. Se l'indirizzo del controller non è valido (se, ad esempio, l'amministratore ha inserito un nome di dominio completo errato durante l'installazione del VDA), l'attività di tale query può potenzialmente portare a una

condizione DDoS (Distributed Denial of Service) sul controller di dominio.

La seguente chiave del Registro di sistema controlla se l'agente Broker utilizza la query top-down di fallback quando non è in grado di individuare un controller durante la ricerca iniziale.

`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`

- Nome: `DisableDdcWildcardNameLookup`
- Tipo: `DWORD`
- Valore: `1` (predefinito) o `0`

Quando l'impostazione è `1`, la ricerca di fallback è disattivata. Se la ricerca iniziale del controller non riesce, l'agente Broker smette di cercare. Questa è l'impostazione predefinita.
Quando l'impostazione è `0`, la ricerca di fallback è abilitata. Se la ricerca iniziale del controller non riesce, viene avviata la ricerca top-down di fallback.

### Sequenziamento di binding LDAP durante la registrazione VDA utilizzando un controller di dominio di sola lettura

Quando un VDA si registra con un controller di dominio di sola lettura (RODC), il Broker Agent deve selezionare il/i binding LDAP (Light Directory Access Protocol) da ignorare. Per effettuare questa selezione, il Broker Agent richiede una chiave di registro adeguata.

Se non viene fornita una chiave di registro o il campo della chiave di registro è vuoto, la registrazione VDA con il RODC richiede più tempo, perché deve passare attraverso la sequenza di binding LDAP originale.

Per modificare la sequenza di binding LDAP, è stata aggiunta la chiave di registro `ListofIgnoredBindings` a `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`. L'uso di `ListofIgnoredBindings` consente di modificare la sequenza di associazione LDAP, se necessario, e quindi di velocizzare la registrazione VDA con un RODC.

- Nome: `ListofIgnoredBindings`
- Tipo: `REG_SZ`
- Valori: `DefaultPath`, `DomainPath`, `PDCPath`

Il valore è un elenco di opzioni di percorso di binding, ciascuna separata da una virgola. La chiave di registro ignorerà tutti i valori che non riconosce come validi.

### Risoluzione dei problemi di registrazione VDA

Come indicato in precedenza, un VDA deve essere registrato con un Delivery Controller o un Cloud Connector per essere preso in considerazione all'avvio di sessioni di mediazione. I VDA non registrati

possono causare un sottoutilizzo di risorse altrimenti disponibili. Esistono vari motivi per cui un VDA potrebbe non essere registrato, molti dei quali sono risolvibili da un amministratore. Studio fornisce informazioni sulla risoluzione dei problemi nella procedura guidata di creazione del catalogo e dopo la creazione di un gruppo di consegna.

- **Identificazione dei problemi durante la creazione del catalogo di macchine:** nella procedura guidata di creazione del catalogo, dopo che sono state aggiunte le macchine esistenti, l'elenco dei nomi degli account del computer indica se ogni macchina è adatta per l'aggiunta al catalogo. Passare il mouse sull'icona accanto a ogni macchina per visualizzare un messaggio informativo su quella macchina.

  Se il messaggio identifica una macchina problematica, è possibile rimuoverla (utilizzando il pulsante **Remove**) o aggiungerla. Ad esempio, se un messaggio indica che non sono state ottenute informazioni su una macchina (forse perché non era mai stata registrata), è possibile scegliere di aggiungere comunque la macchina.

  Il livello funzionale di un catalogo controlla quali caratteristiche del prodotto sono disponibili per le macchine presenti nel catalogo. Per utilizzare le funzionalità introdotte nelle nuove versioni dei prodotti potrebbe essere necessario l'uso di un nuovo VDA. L'impostazione di un livello funzionale rende disponibili tutte le funzionalità introdotte in quella versione (e nelle successive, se il livello funzionale non cambia) per le macchine del catalogo. Tuttavia, le macchine di quel catalogo con una versione di VDA precedente non possono registrarsi.

- **Identificazione dei problemi dopo la creazione dei gruppi di consegna:** dopo la creazione di un gruppo di consegna, Studio visualizza i dettagli delle macchine associate a quel gruppo.

  Il riquadro dei dettagli di un gruppo di consegna indica il numero di macchine che devono essere registrate ma non lo sono. In altre parole, potrebbero esserci una o più macchine accese e non in modalità di manutenzione, ma non attualmente registrate con un Controller. Quando si visualizza una macchina non registrata che dovrebbe esserlo, vedere la scheda **Troubleshoot** (Risoluzione dei problemi) nel riquadro dei dettagli per individuare le possibili cause e leggere le azioni correttive consigliate.

#### Ulteriori informazioni sulla risoluzione dei problemi di registrazione VDA

- Per ulteriori informazioni sui livelli funzionali, vedere Versioni e livelli funzionali dei VDA.
- Per ulteriori informazioni sulla risoluzione dei problemi relativi alla registrazione dei VDA, vedere CTX136668.
- È inoltre possibile utilizzare i controlli di integrità di Citrix Scout per risolvere i problemi di registrazione VDA e di avvio della sessione. Per i dettagli, vedere Informazioni sui controlli di integrità.

# IP virtuale e loopback virtuale

January 7, 2024

> **Importante:**
>
> Windows 10 Enterprise multisessione non supporta la virtualizzazione IP di Desktop remoto (IP virtuale) e Citrix non supporta né l'IP virtuale né il loopback virtuale in Windows 10 Enterprise multisessione.

Le funzionalità Virtual IP e di loopback virtuale sono supportate sulle macchine Windows Server 2016. Queste funzionalità non si applicano alle macchine con sistema operativo desktop Windows.

La funzionalità di indirizzo IP virtuale di Microsoft fornisce a un'applicazione pubblicata un indirizzo IP univoco assegnato dinamicamente per ciascuna sessione. La funzione di loopback virtuale Citrix consente di configurare applicazioni che dipendono dalle comunicazioni con localhost (127.0.0.1 per impostazione predefinita) per l'uso di un indirizzo di loopback virtuale univoco compreso nell'intervallo localhost (127.*).

Alcune applicazioni, quali CRM e Computer Telephony Integration (CTI), utilizzano un indirizzo IP per indirizzamento, licenza, identificazione o altri scopi che richiedono un indirizzo IP univoco o un indirizzo di loopback. Altre applicazioni potrebbero essere collegate a una porta statica, quindi i tentativi di avviare istanze aggiuntive di un'applicazione in un ambiente multiutente non riescono perché la porta è in uso. Per assicurare che tali applicazioni funzionino correttamente in un ambiente Citrix Virtual Apps, è necessario un indirizzo IP univoco per ciascun dispositivo.

L'IP virtuale e il loopback virtuale sono funzionalità indipendenti. È possibile utilizzare una delle due o entrambe.

Sinossi dell'azione dell'amministratore:

- Per utilizzare Microsoft Virtual IP, abilitarlo e configurarlo sul server Windows (Le impostazioni dei criteri Citrix non sono necessarie).
- Per utilizzare il loopback virtuale Citrix, configurare due impostazioni in un criterio Citrix.

## IP virtuale

Quando l'IP virtuale è abilitato e configurato sul server Windows, ogni applicazione configurata in esecuzione in una sessione sembra avere un indirizzo univoco. Gli utenti accedono a queste applicazioni su un server Citrix Virtual Apps nello stesso modo in cui accedono a qualsiasi altra applicazione pubblicata. Un processo richiede un IP virtuale in uno dei seguenti casi:

- Il processo utilizza un numero di porta TCP hardcoded

- Il processo utilizza socket Windows e richiede un indirizzo IP univoco o un numero di porta TCP specificato

Per determinare se un'applicazione deve utilizzare indirizzi IP virtuali:

1. Ottenete lo strumento TCPView da Microsoft. Questo strumento elenca tutte le applicazioni che collegano indirizzi IP e porte specifici.
2. Disabilitare la funzione Risolvi indirizzi IP in modo da visualizzare gli indirizzi anziché i nomi host.
3. Avviare l'applicazione e utilizzare TCPView per vedere quali indirizzi IP e quali porte sono aperte dall'applicazione e quali nomi di processo stanno aprendo queste porte.
4. Configurare tutti i processi che aprono l'indirizzo IP del server, 0.0.0.0 o 127.0.0.1.
5. Per garantire che un'applicazione non apra lo stesso indirizzo IP su una porta diversa, avviare un'altra istanza dell'applicazione.

#### Come funziona la virtualizzazione IP di Microsoft Remote Desktop (RD)

- Sul server Microsoft deve essere abilitato l'indirizzamento IP virtuale.

  Ad esempio, in un ambiente Windows Server 2016, da Server Manager espandere **Servizi Desktop remoto > Connessioni host sessione Desktop remoto** per abilitare la funzionalità di virtualizzazione IP Desktop remoto e configurare le impostazioni per assegnare dinamicamente gli indirizzi IP utilizzando il server DHCP (Dynamic Host Configuration Protocol) per quella sessione o per quel programma. Per istruzioni, vedere la documentazione Microsoft.

- Dopo aver attivato la funzione, all'avvio della sessione il server richiede gli indirizzi IP assegnati dinamicamente dal server DHCP.

- La funzione Virtualizzazione IP Desktop remoto assegna indirizzi IP alle connessioni desktop remote per sessione o per programma. Se si assegnano indirizzi IP a più programmi, questi hanno lo stesso indirizzo IP per sessione.

- Dopo aver assegnato un indirizzo a una sessione, la sessione utilizza l'indirizzo virtuale anziché l'indirizzo IP principale del sistema ogni volta che vengono effettuate le seguenti chiamate: `bind`¸`closesocket`¸`connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`.

Quando si utilizza la funzionalità di virtualizzazione IP Microsoft all'interno della configurazione di hosting di sessione Desktop remoto, le applicazioni vengono associate a specifici indirizzi IP inserendo un componente "filtro"tra l'applicazione e le chiamate di funzione Winsock. L'applicazione vede quindi solo l'indirizzo IP corretto da utilizzare. Qualsiasi tentativo da parte dell'applicazione di ascoltare le comunicazioni TCP o UDP è associato automaticamente all'indirizzo IP virtuale allocato

(o indirizzo di loopback). Le connessioni di origine aperte dall'applicazione provengono dall'indirizzo IP associato all'applicazione.

Nelle funzioni che restituiscono un indirizzo (ad esempio `GetAddrInfo()`, controllato da un criterio di Windows), se viene richiesto l'indirizzo IP dell'host locale, l'IP virtuale esamina l'indirizzo IP restituito e lo modifica per corrispondere all'indirizzo IP virtuale della sessione. Le applicazioni che tentano di ottenere l'indirizzo IP del server locale tramite tali funzioni di nome vedono solo l'indirizzo IP virtuale univoco assegnato a quella sessione. Questo indirizzo IP viene spesso utilizzato nelle chiamate socket successive, quali bind o connect. Per ulteriori informazioni sui criteri di Windows, vedere Virtualizzazione IP RDS in Windows Server.

Spesso, un'applicazione richiede di collegarsi a una porta per l'ascolto sull'indirizzo 0.0.0.0. Quando un'applicazione esegue questa operazione e utilizza una porta statica, non è possibile avviare più istanze dell'applicazione. La funzione di indirizzo IP virtuale cerca anche 0.0.0.0 in questi tipi di chiamata e modifica la chiamata in ascolto sull'indirizzo IP virtuale specifico, che consente a più di un'applicazione di ascoltare sulla stessa porta dello stesso computer perché sono tutte in ascolto su indirizzi diversi. La chiamata viene modificata solo se si trova in una sessione ICA e se la funzione di indirizzo IP virtuale è abilitata. Ad esempio, se due istanze di un'applicazione in esecuzione in sessioni diverse provano entrambe a collegarsi a tutte le interfacce (0.0.0.0) e a una porta specifica (ad esempio 9000), queste si associano a VIPAddress1:9000 e a VIPAddress2:9000 e non vi sono conflitti.

### Loopback virtuale

L'abilitazione delle impostazioni dei criteri di loopback IP virtuale Citrix consente a ogni sessione di disporre del proprio indirizzo di loopback per la comunicazione. Quando un'applicazione utilizza l'indirizzo localhost (impostazione predefinita= 127.0.0.1) in una chiamata Winsock, la funzione di loopback virtuale sostituisce semplicemente 127.0.0.1 con 127.X.X.X, dove X.X.X è una rappresentazione dell'ID sessione + 1. Ad esempio, un ID di sessione 7 è 127.0.0.8. Nell'improbabile caso in cui l'ID di sessione superi il quarto ottetto (più di 255), l'indirizzo passa all'ottetto successivo (127.0.1.0), fino al massimo di 127.255.255.255.

Un processo richiede il loopback virtuale in uno dei seguenti casi:

- Il processo utilizza l'indirizzo di loopback del socket Windows (localhost) (127.0.0.1)
- Il processo utilizza un numero di porta TCP hardcoded

Utilizzare le impostazioni dei criteri di loopback virtuale per le applicazioni che utilizzano un indirizzo di loopback per la comunicazione tra processi. Non è richiesta alcuna configurazione aggiuntiva. Il loopback virtuale non dipende dall'IP virtuale, quindi non è necessario configurare il server Microsoft.

- Supporto loopback IP virtuale. Se abilitata, questa impostazione dei criteri consente a ogni sessione di avere il proprio indirizzo di loopback virtuale. Questa impostazione è disabilitata

per impostazione predefinita. La funzionalità si applica solo alle applicazioni specificate con l'impostazione dei criteri di elenco dei programmi di loopback virtuale Virtual IP.
- Elenco dei programmi di loopback virtuale Virtual IP. Questa impostazione dei criteri specifica le applicazioni che utilizzano la funzione di loopback IP virtuale. Questa impostazione si applica solo quando è abilitata l'impostazione del criterio di supporto per il loopback Virtual IP.

**Funzionalità correlata**

È possibile utilizzare le seguenti impostazioni del Registro di sistema per garantire che il loopback virtuale abbia la preferenza rispetto all'IP virtuale. Questa funzione è chiamata loopback preferito. Tuttavia, procedere con cautela:

- Utilizzare il loopback preferito solo se sono abilitati sia l'IP virtuale che il loopback virtuale. In caso contrario, si potrebbero avere risultati non intenzionali.
- La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Eseguire regedit sui server in cui risiedono le applicazioni.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP
- Nome: PreferLoopback, Tipo: REG_DWORD, Data: 1
- Nome: PreferLoopbackProcesses, Tipo: REG_MULTI_SZ, Dati: <elenco dei processi>

## Zone

January 7, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Le distribuzioni che si estendono su posizioni ampiamente disperse connesse da una WAN possono affrontare sfide dovute alla latenza e all'affidabilità della rete. Esistono due opzioni per attenuare queste sfide:

- Distribuire più siti, ognuno con il proprio database del sito SQL Server.

  Questa opzione è consigliata per le distribuzioni aziendali di grandi dimensioni. Più siti vengono gestiti separatamente e ognuno richiede il proprio database del sito SQL Server. Ogni sito è una distribuzione separata di Citrix Virtual Apps.

- Configurare più zone all'interno di un singolo sito.

  La configurazione delle zone può aiutare gli utenti che si trovano in regioni remote a connettersi alle risorse senza necessariamente costringere le loro connessioni ad attraversare grandi segmenti della WAN. L'utilizzo di zone consente una gestione efficace del sito da una singola console Web Studio, Citrix Director e dal database del sito. Ciò consente di risparmiare sui costi relativi a distribuzione, personale, licenze e gestione di più siti contenenti database separati in posizioni remote.

  Le zone possono essere utili per implementazioni di tutte le dimensioni. È possibile utilizzare le zone per mantenere le applicazioni e i desktop più vicini agli utenti finali, migliorando le prestazioni. Una zona può avere uno o più controller installati localmente per ridondanza e resilienza, ma non è necessario.

  Il numero di controller configurati nel sito può influire sulle prestazioni di alcune operazioni, ad esempio l'aggiunta di nuovi controller al sito stesso. Per evitare ciò, si consiglia di limitare il numero di zone del sito Citrix Virtual Apps o Citrix Virtual Desktops a non più di 50.

  Quando la latenza di rete delle zone è superiore a 250 ms RTT, si consiglia di distribuire più siti anziché zone.

In questo articolo il termine locale si riferisce alla zona in discussione. Ad esempio, "Un VDA si registra con un controller locale"significa che un VDA si registra con un controller nella zona in cui si trova il VDA.

Le zone di questa versione sono simili, ma non identiche alle zone di XenApp versione 6.5 e precedenti. Ad esempio, in questa implementazione di zone, non ci sono raccoglitori di dati. Tutti i controller del sito comunicano con un database del sito nella zona principale. Inoltre, il failover e le zone preferite funzionano in modo diverso in questa versione.

## Tipi di zona

Un sito ha sempre una zona principale. Può anche facoltativamente avere una o più zone satellite. Le zone satellite possono essere utilizzate per il ripristino d'emergenza, i data center distanti geograficamente, le filiali, un cloud o una zona di disponibilità in un cloud.

**Zona primaria:**

La zona principale ha il nome predefinito "Primaria". Questa zona contiene il database del sito di SQL Server (e i server SQL ad alta disponibilità, se utilizzati), Web Studio, Director, Citrix StoreFront, Citrix

License Server e Citrix Gateway. Conservare sempre il database del sito nella zona principale.

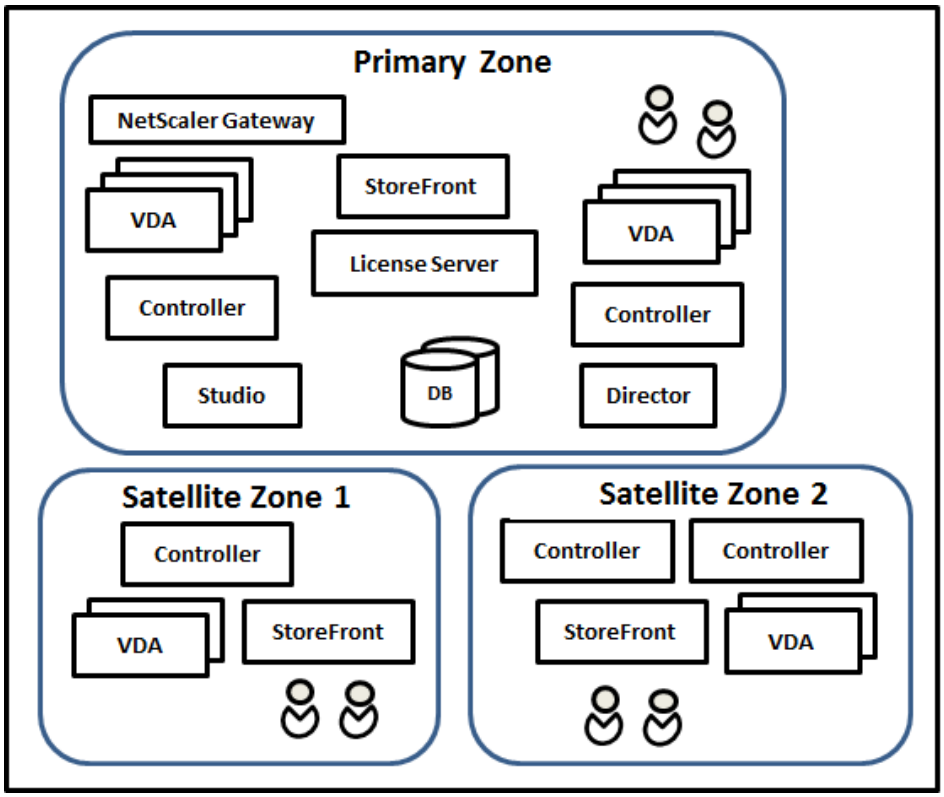
La zona principale dovrebbe avere almeno due controller per la ridondanza. La zona principale può avere VDA con applicazioni strettamente collegate al database e all'infrastruttura.

**Zona satellite:**

Una zona satellite contiene uno o più VDA, controller, server StoreFront e server Citrix Gateway. Nelle normali operazioni, i controller che si trovano in una zona satellite comunicano direttamente con il database della zona principale.

Una zona satellite, in particolare se di grandi dimensioni, potrebbe contenere anche un hypervisor utilizzato per il provisioning e l'archiviazione di macchine per quella zona. Quando si configura una zona satellite, è possibile associare a essa un hypervisor o un'altra connessione di servizio. Assicurarsi che tutti i cataloghi che utilizzano tale connessione si trovino nella stessa zona.

Un sito può avere zone satellite di diverse configurazioni, in base alle esigenze e all'ambiente specifici. La figura seguente illustra una zona primaria ed esempi di zone satellite.




Nell'illustrazione:

- **Zona principale:** contiene due controller, Web Studio, Director, StoreFront, License Server e il database del sito (più distribuzioni SQL Server ad alta disponibilità). La zona principale contiene anche diversi VDA e un Citrix Gateway.
- **Zona satellite 1: VDA con controller:** la zona satellite 1 contiene un controller, VDA e un server

StoreFront. I VDA di questa zona satellite si registrano con il controller locale. Il controller locale comunica con il database del sito e il server licenze nella zona principale.

Se la WAN non riesce, la funzione cache host locale consente al controller della zona satellite di continuare a eseguire l'intermediazione delle connessioni ai VDA in quella zona. Tale distribuzione può essere efficace in un ufficio in cui i lavoratori utilizzano un sito StoreFront locale e il controller locale per accedere alle risorse locali.

- **Zona satellite 2: VDA con controller ridondanti:** La zona satellite 2 contiene due controller, dei VDA e un server StoreFront. Questo è il tipo di zona più resiliente, che offre protezione contro un guasto simultaneo della WAN e di uno dei controller locali.

### Dove si registrano i VDA e dove i controller vanno in failover

In un sito contenente zone principali e zone satellite, con VDA alla versione minima 7.7:

- Un VDA che si trova nella zona principale si registra con un controller nella zona principale. Un VDA che si trova nella zona principale non tenta mai di registrarsi con un controller in una zona satellite.
- Se possibile, un VDA che si trova in una zona satellite si registra con un controller locale. Questo è considerato il controller preferito. Se non sono disponibili controller locali (ad esempio, perché non possono accettare più registrazioni VDA o perché le registrazioni non sono riuscite), il VDA tenterà di registrarsi con un controller nella zona principale. In questo caso, il VDA rimane registrato nella zona principale, anche se un controller che si trova in una zona satellite diventa nuovamente disponibile. Un VDA che si trova in una zona satellite non tenta mai di registrarsi con un controller in un'altra zona satellite.
- Quando l'aggiornamento automatico è abilitato per il rilevamento di VDA dei controller e si specifica un elenco di indirizzi di controller durante l'installazione di VDA, un controller viene selezionato casualmente da tale elenco per la registrazione iniziale (indipendentemente dalla zona in cui risiede il controller). Dopo il riavvio della macchina con quel VDA, il VDA inizierà a preferire la registrazione con un controller che si trova nella sua zona locale.
- Se un controller che si trova in una zona satellite presenta errori, se è possibile viene eseguito il failover su un altro controller locale. Se non sono disponibili controller locali, viene eseguito il failover su un controller nella zona principale.
- Se si sposta un controller facendolo entrare o uscire da una zona e l'aggiornamento automatico è abilitato, i VDA di entrambe le zone ricevono elenchi aggiornati che indicano quali controller sono locali e quali si trovano nella zona principale, in modo che sappiano con chi possono registrarsi e accettare connessioni.
- Se si sposta un catalogo in un'altra zona, i VDA del catalogo si registrano nuovamente con i controller nella zona in cui è stato spostato il catalogo. Quando si sposta un catalogo in un'altra zona, assicurarsi che questa zona e la zona con la connessione host associata siano ben

connesse. Se la larghezza di banda è limitata o ad alta latenza, spostare la connessione host nella stessa zona contenente il catalogo di macchine associato.

Se tutti i controller della zona principale riportano problemi:

- Web Studio non può connettersi al sito.
- Non è possibile effettuare connessioni a VDA nella zona principale.
- Le prestazioni del sito si riducono fino a quando i controller della zona principale non sono disponibili.

Per i siti contenenti versioni di VDA precedenti alla 7.7:

- Un VDA che si trova in una zona satellite accetta le richieste dei controller nella loro zona locale e nella zona principale. I VDA di versione minima 7.7 possono accettare richieste di controller da altre zone satellite.
- Un VDA che si trova in una zona satellite si registra con un controller nella zona principale o nella zona locale in modo casuale. I VDA di versione minima 7.7 preferiscono la zona locale.

## Preferenza di zona

Per utilizzare la funzione di preferenza di zona, è necessario utilizzare come minimo StoreFront 3.7 e Citrix Gateway 11.0-65.x.

In un sito multi-zona, la funzione di preferenza di zona offre all'amministratore maggiore flessibilità per controllare quale VDA viene utilizzato per avviare un'applicazione o un desktop.

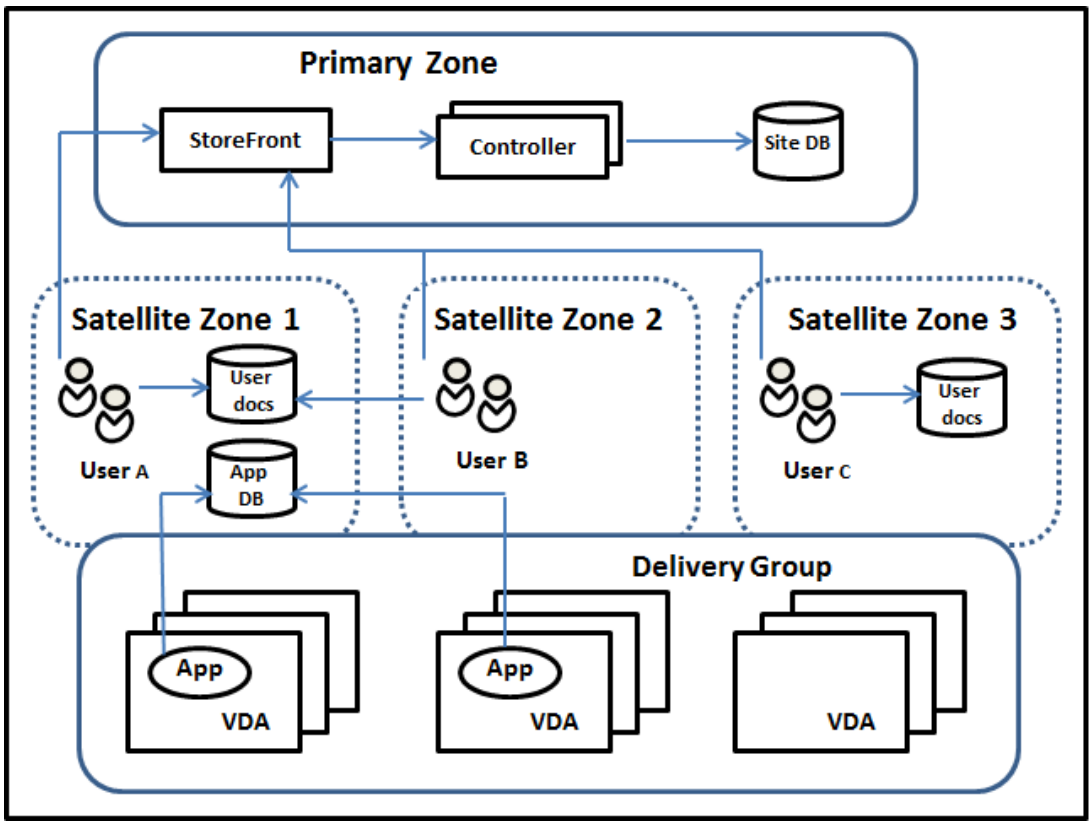
### Come funziona la preferenza di zona

Esistono tre forme di preferenza di zona. Potrebbe essere preferibile utilizzare un VDA in una determinata zona, a seconda dei fattori seguenti:

- Dove sono memorizzati i dati dell'applicazione. Tale posizione viene denominata posizione home dell'applicazione.
- La posizione in cui sono memorizzati i dati home dell'utente, ad esempio un profilo o una condivisione domestica. Questa è denominata home utente.
- La posizione corrente dell'utente (in cui è in esecuzione l'app Citrix Workspace). Questa viene denominata posizione dell'utente.

L'immagine seguente mostra un esempio di configurazione multi-zona.




In questo esempio, i VDA sono distribuiti tra tre zone satellite, ma sono tutti nello stesso gruppo di consegna. Pertanto, il broker potrebbe scegliere quale VDA utilizzare per una richiesta di avvio dell'utente. Questo esempio indica che esistono diverse posizioni in cui gli utenti possono eseguire gli endpoint dell'app Citrix Workspace:

- L'utente A sta utilizzando un dispositivo con l'app Citrix Workspace nella zona satellite 1.
- L'utente B sta utilizzando un dispositivo nella zona satellite 2.
- I documenti di un utente possono essere memorizzati in varie posizioni.
  - Gli utenti A e B utilizzano una condivisione che si trova nella zona satellite 1.
  - L'utente C utilizza una condivisione proveniente dalla zona satellite C.
  - Una delle applicazioni pubblicate utilizza un database situato nella zona satellite 1.

È possibile associare un utente o un'applicazione a una zona, configurando una zona home per l'utente o l'applicazione. Il broker del Delivery Controller utilizza quindi tali associazioni per aiutare a selezionare la zona in cui verrà avviata una sessione, se sono disponibili risorse. È possibile effettuare le seguenti operazioni:

- Configurare la zona home di un utente aggiungendo un utente a una zona.
- Configurare la zona home di un'applicazione modificando le proprietà dell'applicazione.

Un utente o un'applicazione possono disporre di una sola zona home alla volta. Un'eccezione per

gli utenti può essere quando vi sono abbonamenti a più zone a causa dell'appartenenza al gruppo di utenti; vedere la sezione "Altre considerazioni". Tuttavia, anche in questo caso, il broker utilizza una sola zona home.

Sebbene le preferenze di zona per utenti e applicazioni possano essere configurate, il broker seleziona solo una zona preferita per un avvio. L'ordine di priorità predefinito per la selezione della zona preferita è applicazioni home > home utente > posizione utente. È possibile limitare la sequenza; vedere Personalizzare la preferenza della zona. Quando un utente avvia un'applicazione:

- Se tale applicazione ha un'associazione di zona configurata (una home dell'applicazione), la zona preferita è la zona home per quell'applicazione.
- Se l'applicazione non dispone di un'associazione di zona configurata, ma ce l'ha l'utente (una home utente), la zona preferita è la zona home di quell'utente.
- Se né l'applicazione né l'utente hanno un'associazione di zona configurate, la zona preferita è la zona in cui l'utente esegue un'istanza dell'app Citrix Workspace (la posizione utente). Se tale zona non è definita, viene utilizzata una selezione casuale di VDA e zona. Viene applicato il bilanciamento del carico a tutti i VDA che si trovano nella zona preferita. Se non esiste una zona preferita, il bilanciamento del carico viene applicato a tutti i VDA che si trovano nel gruppo di consegna.

#### Personalizzare la preferenza della zona

Quando si configura (o si rimuove) una zona home di un utente o un'applicazione, è inoltre possibile limitare ulteriormente il modo in cui viene utilizzata la preferenza di zona.

- **Uso obbligatorio della zona home utente:** in un gruppo di consegna, è possibile richiedere che una sessione sia avviata solo nella zona home dell'utente (se configurata) senza failover su un'altra zona se la zona home non ha risorse disponibili. Questa restrizione è utile quando è necessario evitare il rischio di copiare profili di grandi dimensioni o file di dati tra una zona e l'altra. In altre parole, quando è preferibile negare l'avvio di una sessione piuttosto che avviare la sessione in un'altra zona.
- **Uso obbligatorio della zona home dell'applicazione:** analogamente, quando si configura una zona home per un'applicazione, è possibile richiedere che l'applicazione venga avviata solo in quella zona, senza failover su una zona diversa se non sono disponibili risorse nella zona home dell'applicazione.
- **Nessuna area home dell'applicazione e ignora la zona home utente configurata:** se non si specifica una zona home per un'applicazione, è inoltre possibile indicare che non vengano considerate zone utente configurate all'avvio dell'applicazione. Ad esempio, è preferibile che gli utenti eseguano un'applicazione su un VDA vicino al proprio dispositivo, utilizzando la preferenza della zona di posizione dell'utente, anche se alcuni utenti potrebbero avere una zona home diversa.

### In che modo le zone preferite influenzano l'uso della sessione

Quando un utente avvia un'applicazione o un desktop, il broker preferisce utilizzare la zona preferita anziché utilizzare una sessione esistente.

Se l'utente che avvia un'applicazione o un desktop dispone già di una sessione adatta per la risorsa che viene avviata (ad esempio una sessione che può utilizzare la condivisione di sessione per un'applicazione o una sessione che sta già eseguendo la risorsa che si sta avviando), ma tale sessione è in esecuzione su un VDA in una zona diversa dalla zona preferita per l'utente/applicazione, il sistema potrebbe creare una nuova sessione. Ciò soddisfa l'avvio nella zona corretta (se questa ha capacità disponibile), prima di riconnettersi a una sessione in una zona meno preferita per i requisiti di sessione di quell'utente.

Per evitare una sessione orfana che non può più essere raggiunta, è consentita la riconnessione alle sessioni disconnesse esistenti, anche se si trovano in una zona non preferita.

L'ordine di desiderabilità perché le sessioni soddisfino un avvio è il seguente:

1. Riconnettere a una sessione esistente nella zona preferita.
2. Riconnettere a una sessione disconnessa esistente in una zona diversa dalla zona preferita.
3. Avviare una nuova sessione nella zona preferita.
4. Riconnettere a una sessione esistente connessa in una zona diversa dalla zona preferita.
5. Avviare una nuova sessione in una zona diversa dalla zona preferita.

### Altre considerazioni sulle preferenze di zona

- Se si configura una zona home per un gruppo di utenti (ad esempio un gruppo di sicurezza), gli utenti di quel gruppo (tramite l'appartenenza diretta o indiretta) vengono associati alla zona specificata. Tuttavia, un utente può essere membro di più gruppi di sicurezza e pertanto potrebbe avere una zona principale diversa configurata tramite l'appartenenza ad altri gruppi. In questi casi, la determinazione della zona home dell'utente può essere ambigua.

Se un utente dispone di una zona home configurata che non è stata acquisita tramite l'appartenenza al gruppo, tale zona viene utilizzata per le preferenze di zona. Tutte le associazioni di zona acquisite tramite l'appartenenza al gruppo vengono ignorate.

Se l'utente ha più associazioni di zone diverse acquisite esclusivamente tramite l'appartenenza al gruppo, il broker ne sceglie una in modo casuale. Una volta che il broker ha fatto questa scelta, questa zona viene utilizzata per i successivi avviamenti delle sessioni, fino a quando l'appartenenza al gruppo dell'utente non cambia.

- La preferenza della zona di posizione utente richiede il rilevamento dell'app Citrix Workspace sul dispositivo endpoint da parte del Citrix Gateway attraverso il quale tale dispositivo si sta

connettendo. Il Citrix Gateway deve essere configurato per associare intervalli di indirizzi IP a zone particolari e l'identità di zona rilevata deve essere passata tramite StoreFront al controller.

Per ulteriori informazioni sulle preferenze della zona, vedere Elementi interni della preferenza zona.

### Considerazioni, requisiti e procedure consigliate

- È possibile posizionare i seguenti elementi in una zona: controller, cataloghi di macchine, connessioni host, utenti e applicazioni. Se un catalogo utilizza una connessione host, assicurarsi che il catalogo e la connessione siano nella stessa zona. Tuttavia, se è disponibile una connessione a larghezza di banda elevata a bassa latenza, questi elementi possono trovarsi in zone diverse.
- Quando si posizionano elementi in una zona satellite, ciò influisce sul modo in cui il sito interagisce con essi e con altri oggetti a essi correlati.
  - Quando i controller vengono inseriti in una zona satellite, si presume che tali macchine abbiano una buona connettività (locale) agli hypervisor e ai VDA presenti nella stessa zona. I controller di quella zona satellite vengono quindi utilizzati di preferenza rispetto ai controller della zona primaria per la gestione di tali hypervisor e macchine VDA.
  - Quando una connessione hypervisor viene inserita in una zona satellite, si presume che tutti gli hypervisor gestiti tramite tale connessione hypervisor risiedano anch'essi in quella zona satellite. I controller di quella zona satellite vengono quindi utilizzati di preferenza rispetto ai controller della zona primaria quando si comunica con quella connessione hypervisor.
  - Quando un catalogo di macchine viene inserito in una zona satellite, si presume che tutte le macchine VDA presenti in quel catalogo si trovino nella zona satellite. I controller locali vengono utilizzati di preferenza rispetto ai controller della zona principale quando si tenta di registrarsi al sito, una volta che il meccanismo di aggiornamento automatico dell'elenco di controller è stato attivato dopo la prima registrazione di ciascun VDA.
  - Anche le istanze di Citrix Gateway possono essere associate alle zone. Questo viene fatto nell'ambito della configurazione di StoreFront Optimal HDX Routing anziché, come per gli altri elementi qui descritti, nell'ambito della configurazione del sito. Quando un Citrix Gateway è associato a una zona, è preferibile utilizzarlo quando si utilizzano connessioni HDX a macchine VDA di quella zona.
- Quando si crea un sito di produzione e quindi si crea il primo catalogo e il gruppo di consegna, tutti gli elementi si trovano nella zona principale: non è possibile creare zone satellite fino a dopo il completamento della configurazione iniziale. Se si crea un sito vuoto, inizialmente la zona principale conterrà solo un controller. È possibile creare zone satellite prima o dopo la creazione di un catalogo e di un gruppo di consegna.

- Quando si crea la prima zona satellite contenente uno o più elementi, tutti gli altri elementi del sito rimangono nella zona principale.
- La zona principale è denominata "Primaria"per impostazione predefinita; è possibile modificare tale nome. Sebbene Web Studio indichi quale zona è la zona principale, è consigliabile utilizzare un nome facilmente identificabile per essa. La zona principale può essere riassegnata (ovvero è possibile rendere principale un'altra zona), ma deve sempre contenere il database del sito ed eventuali server ad alta disponibilità.
- Conservare sempre il database del sito nella zona principale.
- Dopo aver creato una zona, successivamente è possibile spostare gli elementi da una zona all'altra. Questa flessibilità consente potenzialmente di separare gli elementi che funzionano meglio nelle immediate vicinanze. Ad esempio, lo spostamento di un catalogo in una zona diversa dalla connessione (host) che crea le macchine del catalogo può influire sulle prestazioni. Considerare i potenziali effetti non voluti prima di spostare elementi da una zona all'altra. Mantenere un catalogo e la connessione host utilizzata nella stessa zona o in zone ben collegate (ad esempio, tramite una rete a bassa latenza e larghezza di banda elevata).
- Per prestazioni ottimali, installare Web Studio e Director solo nella zona principale. È possibile accedere a Web Studio e Director da una zona satellite (ad esempio, una zona satellite contenente controller da utilizzare come failover se la zona principale diventa inaccessibile) perché si tratta di applicazioni Web.
- Idealmente, Citrix Gateway presente in una zona satellite viene utilizzato per le connessioni utente che entrano in quella zona da altre zone o posizioni esterne, anche se è possibile utilizzarlo per le connessioni all'interno della zona.
- Ricordare: per utilizzare la funzione di preferenza zona, è necessario utilizzare StoreFront 3.7 e Citrix Gateway 11.0-65.x.

#### Limiti di qualità della connessione

I controller della zona satellite eseguono le interazioni SQL direttamente con il database del sito. Ciò impone alcuni limiti alla qualità del collegamento tra la zona satellite e la zona principale contenente il database del sito. I limiti specifici dipendono dal numero di VDA e sessioni utente sui VDA che sono distribuiti nella zona satellite. Le zone satellite con solo pochi VDA e poche sessioni possono funzionare con una connessione al database di qualità inferiore rispetto alle zone satellite con un numero elevato di VDA e sessioni.

Per ulteriori informazioni, vedere Miglioramenti delle query di blocco SQL e latenza.

#### L'impatto della latenza sulle prestazioni di intermediazione

Sebbene le zone consentano agli utenti di utilizzare collegamenti a latenza più elevata a condizione che vi sia un broker locale, la latenza aggiuntiva influisce inevitabilmente sull'esperienza dell'utente finale. Per la maggior parte del lavoro che svolgono, gli utenti sperimentano la lentezza causata dai viaggi di andata e ritorno tra controller della zona satellite e il database del sito.

Per l'avvio delle applicazioni, si verificano ulteriori ritardi mentre il processo di intermediazione di sessione identifica i VDA adatti a cui inviare le richieste di avvio della sessione.

### Creare e gestire le zone

Un amministratore completo può eseguire tutte le attività di creazione e gestione delle zone. Tuttavia, è anche possibile creare un ruolo personalizzato che consente di creare, modificare o eliminare una zona. Lo spostamento di elementi tra le zone non richiede autorizzazioni relative alla zona (eccetto l'autorizzazione di lettura della zona); tuttavia, è necessario disporre dell'autorizzazione di modifica per gli elementi che si stanno spostando. Ad esempio, per spostare un catalogo da una zona a un'altra, è necessario disporre dell'autorizzazione di modifica per quel catalogo. Per ulteriori informazioni, vedere Amministrazione delegata.

**Se si utilizza Citrix Provisioning:** la console Citrix Provisioning non è a conoscenza delle zone, pertanto consigliamo di utilizzare Web Studio per creare cataloghi per le zone satellite. Creare il catalogo in Web Studio, specificando la zona satellite corretta. Quindi utilizzare la console Citrix Provisioning per eseguire il provisioning delle macchine che si trovano in quel catalogo. Se si crea il catalogo utilizzando la procedura guidata di Citrix Provisioning, il catalogo viene inserito nella zona principale. È necessario utilizzare Web Studio per spostarlo nella zona satellite in un secondo momento.

#### Creare una zona

1. Accedere a Web Studio.
2. Selezionare **Zones** nel riquadro a sinistra.
3. Selezionare **Create zone** (Crea zona) nella barra delle azioni.
4. Immettere un nome e una descrizione per la zona (facoltativa). Il nome deve essere univoco all'interno del sito.
5. Selezionare gli elementi da collocare nella nuova zona. È possibile filtrare o cercare l'elenco di elementi da cui è possibile selezionare. È inoltre possibile creare una zona vuota, semplicemente non selezionando alcun elemento.
6. Fare clic su **Salva**.

In alternativa a questo metodo, è possibile selezionare uno o più elementi in Web Studio e quindi selezionare **Creare zone** nella barra delle azioni.

### Modificare il nome o la descrizione di una zona

1. Accedere a Web Studio.
2. Selezionare **Zones** nel riquadro a sinistra.
3. Selezionare una zona nel riquadro centrale e quindi selezionare **Edit Zone** nella barra delle azioni.
4. Modificare il nome della zona, la sua descrizione o entrambi. Se si modifica il nome della zona principale, assicurarsi che la zona rimanga facilmente identificabile come zona principale.
5. Fare clic su **Save** (Salva) o su **Apply** (Applica).

### Spostare gli elementi da una zona a un'altra

1. Accedere a Web Studio.
2. Selezionare **Zones** nel riquadro a sinistra.
3. Selezionare una zona nel riquadro centrale, quindi selezionare uno o più elementi.
4. Trascinare gli elementi nell'area di destinazione o selezionare **Move Items** (Sposta elementi) nella barra delle azioni, quindi specificare la zona in cui spostarli.

Un messaggio di conferma elenca gli elementi selezionati e chiede se si è sicuri di volerli spostare tutti.

**Ricordare:** quando un catalogo utilizza una connessione host a un hypervisor o a un altro servizio, posizionare sia il catalogo che la connessione nella stessa zona. In caso contrario, le prestazioni potrebbero risentirne. Quando se ne sposta uno, spostare anche l'altro.

### Eliminare una zona

Una zona deve essere vuota prima di poter essere eliminata. Non è possibile eliminare la zona principale.

1. Accedere a Web Studio.
2. Selezionare **Zones** nel riquadro a sinistra.
3. Selezionare una zona nel riquadro centrale.
4. Selezionare **Delete Zone** (Elimina zona) nella barra delle azioni. Se la zona non è vuota (ossia se contiene elementi), viene chiesto di scegliere la zona in cui verranno spostati gli elementi.
5. Confermare l'eliminazione.

### Aggiungere una zona home per un utente

La configurazione di una zona home per un utente è anche nota come *aggiunta di un utente a una zona*.

1. Accedere a Web Studio.
2. Selezionare **Zones** nel riquadro a sinistra, quindi selezionare una zona nel riquadro centrale.
3. Selezionare **Add Users to Zone** (Aggiungi utenti alla zona) nella barra delle azioni.
4. Nella finestra di dialogo **Add Users to Zone** (Aggiungi utenti alla zona) fare clic su **Add** e quindi selezionare gli utenti e i gruppi di utenti da aggiungere alla zona. Se si specificano utenti che hanno già una zona home, un messaggio offre due opzioni: **Yes**= aggiungere solo gli utenti specificati che non dispongono di una zona home; **No**= tornare alla finestra di dialogo di selezione utente.
5. Fare clic su **OK**.

Per gli utenti che dispongono di una zona home configurata, è possibile richiedere che le sessioni vengano avviate solo dalla loro zona home:

1. Creare o modificare un gruppo di consegna.
2. Nella pagina **Users** (Utenti), selezionare la casella di controllo **Sessions must launch in a user's home zone, if configured** (Le sessioni devono essere avviate nella zona home di un utente, se configurata).

Tutte le sessioni avviate da un utente in quel gruppo di consegna devono essere avviate dai computer nella zona home di quell'utente. Se un utente del gruppo di consegna non dispone di una zona home configurata, questa impostazione non ha alcun effetto.

#### Rimuovere una zona home per un utente

Questa procedura è nota anche come rimozione di un utente da una zona.

1. Accedere a Web Studio.
2. Selezionare **Zones** nel riquadro a sinistra, quindi selezionare una zona nel riquadro centrale.
3. Selezionare **Remove Users from Zone** (Rimuovi utenti dalla zona) nella barra delle azioni.
4. Nella finestra di dialogo **Add Users to Zone** (Aggiungi utenti alla zona) fare clic su **Remove** e quindi selezionare gli utenti e i gruppi da rimuovere dalla zona. Questa azione rimuove gli utenti solo dalla zona; questi utenti rimangono nei gruppi di consegna e nei gruppi di applicazioni a cui appartengono.
5. Confermare la rimozione quando richiesto.

#### Gestione delle zone home per le applicazioni

La configurazione di una zona home per un'applicazione è nota anche come aggiunta di un'applicazione a una zona. Per impostazione predefinita, in un ambiente multi-zona, un'applicazione non dispone di una zona principale.

La zona home di un'applicazione è specificata nelle proprietà dell'applicazione. È possibile configurare le proprietà dell'applicazione quando si aggiunge l'applicazione a un gruppo o in seguito.

- Quando si crea un gruppo di consegna, si crea un gruppo di applicazioni o si aggiungono applicazioni a gruppi esistenti, selezionare **Properties** nella pagina **Applications** della procedura guidata.
- Per modificare le proprietà di un'applicazione dopo l'aggiunta dell'applicazione, selezionare **Applications** nel riquadro di sinistra. Selezionare un'applicazione e quindi selezionare **Edit Application Properties** (Modifica proprietà applicazione) nella barra delle azioni.

Nella pagina **Zones** delle proprietà/impostazioni dell'applicazione:

- Se si desidera che l'applicazione abbia una zona home:
  - Selezionare il pulsante di opzione **Use the selected zone to decide per decidere** (Usa la zona selezionata) e quindi selezionare la zona.
  - Se si desidera che l'applicazione venga avviata solo dalla zona selezionata (e non da nessun'altra zona), selezionare la casella di controllo sotto la selezione della zona.
- Se non si desidera che l'applicazione disponga di una zona home:
  - Selezionare il pulsante di opzione **Do not configure a home zone** (Non configurare una zona home).
  - Se non si desidera che il broker consideri alcuna delle zone utente configurate all'avvio di questa applicazione, selezionare la casella di controllo sotto il pulsante di opzione. In questo caso, non vengono utilizzate le zone home né dell'applicazione né dell'utente per determinare dove avviare l'applicazione.

### Altre azioni che richiedono di specificare zone

Dopo aver creato almeno una zona satellite, è possibile specificare una zona quando si aggiunge una connessione host o si crea un catalogo.

Di solito, la zona principale è quella predefinita. Quando si utilizza Machine Creation Services per creare un catalogo, viene selezionata automaticamente la zona configurata per la connessione host.

Se il sito non contiene zone satellite, si presuppone che la zona sia la principale e la casella di selezione della zona non viene visualizzata.

## Monitor

January 7, 2024

Gli amministratori e il personale dell'helpdesk possono monitorare i siti di Citrix Virtual Apps and Desktops utilizzando una varietà di funzionalità e strumenti. Utilizzando questi strumenti, è possibile monitorare:

- Sessioni utente e utilizzo della sessione
- Prestazioni di accesso
- Connessioni e macchine, inclusi guasti
- Valutazione del carico
- Tendenze storiche
- Infrastructure (Infrastruttura)

### Citrix Director

Director è uno strumento web in tempo reale che è possibile utilizzare per il monitoraggio e la risoluzione dei problemi e per eseguire attività di supporto per gli utenti finali.

Per maggiori dettagli, vedere gli articoli su Director.

### Accesso di configurazione

La registrazione della configurazione consente agli amministratori di tenere traccia delle modifiche amministrative apportate a un sito. La registrazione della configurazione può aiutare gli amministratori a diagnosticare e risolvere i problemi dopo aver apportato modifiche alla configurazione, assistere nella gestione delle modifiche e nel tenere traccia delle configurazioni e segnalare l'attività di amministrazione.

È possibile visualizzare e generare report sulle informazioni registrate da Studio. È inoltre possibile visualizzare gli elementi registrati in Director con la visualizzazione Trend (Tendenze) per fornire notifiche sulle modifiche alla configurazione. Questa funzionalità è utile per gli amministratori che non hanno accesso a Studio.

La visualizzazione Trends (Tendenze) fornisce i dati storici delle modifiche alla configurazione per un determinato periodo di tempo, in modo che gli amministratori possano valutare quali modifiche sono state apportate al sito, quando sono state apportate e chi le ha apportate per individuare la causa di un problema. Questa visualizzazione ordina le informazioni di configurazione in tre categorie:

- Errori di connessione
- Macchine a sessione singola che presentano problemi
- Macchine multisessione che presentano problemi

Per informazioni dettagliate su come abilitare e configurare la registrazione della configurazione, vedere Registrazione della configurazione. Gli articoli su Director descrivono come visualizzare le informazioni registrate da tale strumento.

### Registri eventi

I servizi disponibili in Citrix Virtual Apps and Desktops registrano gli eventi che si verificano. I log eventi vengono utilizzati per monitorare e risolvere i problemi operativi.

Per ulteriori informazioni, vedere Registri eventi. Anche gli articoli sulle singole funzionalità potrebbero contenere informazioni sugli eventi.

## Registrazione della configurazione

January 7, 2024

La registrazione della configurazione è una funzionalità che acquisisce le modifiche alla configurazione del sito e le attività amministrative nel database. Questa funzionalità è abilitata per impostazione predefinita. È possibile utilizzare il contenuto registrato per:

- Diagnosticare e risolvere i problemi dopo aver apportato modifiche alla configurazione. Il log fornisce una traccia degli spostamenti.
- Facilitare la gestione delle modifiche e tenere traccia delle configurazioni.
- Segnalare le attività di amministrazione.

È possibile impostare delle preferenze per la registrazione della configurazione, visualizzare i log di configurazione e generare report HTML e CSV da Citrix Studio. È possibile filtrare le visualizzazioni dei log di configurazione in base agli intervalli di date e ai risultati della ricerca full-text. La registrazione obbligatoria, se abilitata, impedisce che vengano apportate modifiche alla configurazione, a meno che non possano essere registrate. Se si dispone dell'autorizzazione appropriata, è possibile eliminare voci dal log di configurazione. Non è possibile utilizzare la funzione di registrazione della configurazione per modificare il contenuto del log.

La registrazione della configurazione utilizza un SDK PowerShell e il servizio di registrazione dalla configurazione. Il servizio di registrazione della configurazione viene eseguito su tutti i controller del sito. Se un controller presenta un problema, il servizio su un altro controller gestisce automaticamente le richieste di registrazione.

Per impostazione predefinita, la funzionalità di registrazione della configurazione è abilitata e utilizza il database creato durante la creazione del sito (il database di configurazione del sito). È possibile specificare una posizione diversa per il database. Il database di registrazione della configurazione supporta le stesse funzionalità di disponibilità elevata del database di configurazione del sito.

L'accesso alla registrazione della configurazione è controllato tramite l'amministrazione delegata, con le autorizzazioni Edit Logging Preferences (Modifica preferenze di registrazione) e View Configuration Logs (Visualizza log di configurazione).

La lingua dei registri di configurazione viene impostata al momento della creazione. Ad esempio, un registro creato in inglese viene letto in inglese, indipendentemente dalle impostazioni internazionali del lettore.

### Cosa viene registrato

Vengono registrate le modifiche alla configurazione e le attività amministrative avviate dagli script di Studio, Director e PowerShell. Esempi di modifiche alla configurazione registrate includono l'utilizzo (creazione, modifica, eliminazione, assegnazione) di quanto segue:

- Cataloghi di macchine
- Gruppi di consegna (inclusa la modifica delle impostazioni di gestione dell'alimentazione)
- Ruoli e ambiti dell'amministratore
- Risorse e connessioni host
- Criteri Citrix tramite Studio

Esempi di modifiche amministrative registrate includono:

- Gestire l'alimentazione di una macchina virtuale o di un desktop utente
- Studio o Director che invia un messaggio a un utente

Le seguenti operazioni non vengono registrate:

- Operazioni automatizzate come l'attivazione della gestione in pool delle macchine virtuali.
- Azioni dei criteri implementate tramite la Console Gestione Criteri di gruppo (GPMC); utilizzare gli strumenti Microsoft per visualizzare i log di tali azioni.
- Modifiche apportate tramite il Registro di sistema, accesso diretto al database o da fonti diverse da Studio, Director o PowerShell.
- Quando la distribuzione viene inizializzata, la registrazione della configurazione diventa disponibile quando la prima istanza del servizio di registrazione della configurazione si registra con il servizio di configurazione. Pertanto, le prime fasi della configurazione non vengono registrate (ad esempio, quando lo schema del database viene ottenuto e applicato o quando viene inizializzato un hypervisor).

### Gestire la registrazione della configurazione

Per impostazione predefinita, la registrazione della configurazione utilizza il database creato durante la creazione di un sito (noto anche come database di configurazione del sito). Citrix consiglia di utilizzare una posizione separata per il database di registrazione della configurazione (e il database di monitoraggio) per i seguenti motivi:

- È probabile che la strategia di backup per il database di registrazione della configurazione differisca dalla strategia di backup per il database di configurazione del sito.
- Il volume di dati raccolti per la registrazione della configurazione (e il servizio di monitoraggio) potrebbe influire negativamente sullo spazio disponibile per il database di configurazione del sito.
- Divide il singolo punto di errore per i tre database.

Le versioni dei prodotti che non supportano la registrazione della configurazione non hanno un nodo Logging (Registrazione) in Studio.

## Abilitare e disabilitare la registrazione della configurazione e la registrazione obbligatoria

Per impostazione predefinita, la registrazione della configurazione è abilitata e la registrazione obbligatoria è disabilitata.

1. Accedere a Web Studio e selezionare **Logging** nel riquadro a sinistra.
2. Selezionare **Preferences** (Preferenze) nella barra delle azioni. La finestra di dialogo di registrazione della configurazione contiene informazioni sul database e indica se la registrazione della configurazione e la registrazione obbligatoria sono abilitate o disabilitate.
3. Selezionare l'azione desiderata:

   Per abilitare la registrazione della configurazione, selezionare **Enable** (Abilita). Questa è l'impostazione predefinita. Se non è possibile scrivere nel database, le informazioni di registrazione vengono eliminate, ma l'operazione continua.

   Per disabilitare la registrazione della configurazione, selezionare **Disable** (Disabilita). Se la registrazione era precedentemente abilitata, i log esistenti rimangono leggibili con l'SDK PowerShell.

   Per abilitare la registrazione obbligatoria, selezionare **Prevent changes to the site configuration when the database is not available** (Impedisci modifiche alla configurazione del sito quando il database non è disponibile). Nessuna modifica alla configurazione o attività amministrativa normalmente registrata è consentita, a meno che non possa essere scritta nel database di registrazione della configurazione. È possibile abilitare la registrazione obbligatoria solo quando la registrazione della configurazione è abilitata (quando l'opzione **Enable** [Abilita] è selezionata). Se il servizio di registrazione della configurazione presenta un problema e la disponibilità elevata non è in uso, si presume l'utilizzo della registrazione obbligatoria. In questi casi, le operazioni normalmente registrate non vengono eseguite.

   Per disabilitare la registrazione obbligatoria, selezionare **Allow changes when to the site configuration when the database is not available** (Consenti modifiche alla configurazione del

sito quando il database non è disponibile). Sono consentite modifiche alla configurazione e attività amministrative, anche se non è possibile accedere al database di registrazione della configurazione. Questa è l'impostazione predefinita.

### Modificare la posizione del database di registrazione della configurazione

Non è possibile modificare la posizione del database quando è abilitata la registrazione obbligatoria, poiché la modifica della posizione include un breve intervallo di disconnessione che non può essere registrato.

1. Creare un server di database utilizzando una versione supportata di SQL Server.
2. Accedere a Web Studio e selezionare **Logging** nel riquadro a sinistra.
3. Selezionare **Preferences** (Preferenze) nella barra delle azioni.
4. Nella finestra di dialogo Logging Preferences (Preferenze di registrazione), selezionare **Change logging database** (Modifica database di registrazione).
5. Nella finestra di dialogo Change logging database (Modifica database di registrazione), specificare la posizione del server contenente il nuovo server del database. Vedere Formati degli indirizzi di database per i formati validi.
6. Per consentire a Studio di creare il database, fare clic su **OK**. Quando richiesto, fare clic su **OK** e il database viene creato automaticamente. Studio tenta di accedere al database utilizzando le credenziali dell'utente di Studio corrente. Se l'operazione non riesce, viene richiesto di specificare le credenziali dell'utente del database. Studio carica quindi lo schema del database nel database (le credenziali vengono conservate solo durante la creazione del database).
7. Per creare il database manualmente, fare clic su **Generate database script** (Genera script di database). Lo script generato include istruzioni per la creazione manuale del database. Prima di caricare lo schema, assicurarsi che il database sia vuoto e che almeno un utente disponga dell'autorizzazione di accesso e modifica del database.

I dati di registrazione della configurazione nel database precedente non vengono importati nel nuovo database. I log non possono essere aggregati da entrambi i database durante il recupero dei log. La prima voce di log nel nuovo database di registrazione della configurazione indica che si è verificata una modifica nel database, ma non identifica il database precedente.

### Visualizzare il contenuto del log di configurazione

Quando si avviano le modifiche alla configurazione e le attività amministrative, le operazioni di alto livello create da Studio e Director sono elencate nel riquadro centrale superiore di Studio. Un'operazione di alto livello comporta una o più chiamate di servizio e SDK, che sono operazioni di basso livello. Quando si seleziona un'operazione di alto livello nel riquadro superiore, il riquadro inferiore visualizza le operazioni di basso livello.

Se un'operazione non riesce prima del completamento, l'operazione di log potrebbe non essere completata nel database. Ad esempio, un record di avvio non avrà alcun record di arresto corrispondente. In questi casi, il log indica che mancano informazioni. Quando si visualizzano i log in base a intervalli di tempo, vengono visualizzati i registri incompleti se i dati nei log corrispondono ai criteri. Ad esempio, se vengono richiesti tutti i log degli ultimi cinque giorni ed è presente un log con un'ora di inizio negli ultimi cinque giorni ma senza ora di fine, viene incluso.

Quando si utilizza uno script che chiama i cmdlet PowerShell, se si crea un'operazione di basso livello senza specificare un'operazione padre di alto livello, la registrazione della configurazione crea un'operazione surrogata di alto livello.

Per visualizzare il contenuto del log di configurazione, selezionare **Logging** (Registrazione) nel riquadro di navigazione di Studio. Per impostazione predefinita, il riquadro centrale elenca cronologicamente i contenuti del log (prima le voci più recenti), separati per data. È possibile effettuare le seguenti operazioni:

- Ordinare la visualizzazione per intestazione di colonna.
- Filtrare la visualizzazione specificando un intervallo di giorni o inserendo il testo nella casella **Search** (Cerca). Per tornare alla visualizzazione standard dopo aver utilizzato la ricerca, eliminare il testo nella casella **Search** (Cerca).

### Generare report

È possibile generare report CSV e HTML contenenti i dati del log di configurazione.

- Il report CSV contiene tutti i dati di registrazione a partire da un intervallo di tempo specificato. I dati gerarchici nel database vengono semplificati in una singola tabella CSV. Nessun aspetto dei dati ha la precedenza nel file. Non viene utilizzata alcuna formattazione e non si presume che i dati risultino leggibili dalle persone. Il file (denominato MyReport) contiene i dati in un formato universalmente vederebile. I file CSV vengono spesso utilizzati per l'archiviazione dei dati o come origine dati per uno strumento di reportistica o di manipolazione dei dati come Microsoft Excel.
- Il report HTML fornisce una forma leggibile dei dati di registrazione per un intervallo di tempo specificato. Fornisce una vista strutturata e navigabile per la revisione delle modifiche. Un report HTML comprende due file, denominati Summary (Riepilogo) e Details (Dettagli). Il file Summary (Riepilogo) elenca le operazioni di alto livello: quando si è verificata ogni operazione, chi l'ha eseguita e il risultato. Facendo clic sul collegamento **Details** (Dettagli) accanto a ciascuna operazione si accede alle operazioni di basso livello nel file Details (Dettagli), che fornisce ulteriori informazioni.

Per generare un report del log di configurazione, selezionare **Logging** (Registrazione) nel riquadro di navigazione di Studio, quindi selezionare **Create custom report** (Crea report personalizzato) nella

barra delle azioni.

- Selezionare l'intervallo di date per il report.
- Selezionare il formato del report: CSV, HTML o entrambi.
- Individuare la posizione in cui si desidera salvare il report.

### Eliminare il contenuto del log di configurazione

Per eliminare il log di configurazione, è necessario disporre di alcune autorizzazioni per l'amministrazione delegata e per il database di SQL Server.

- **Amministrazione delegata**: è necessario disporre di un ruolo di amministrazione delegata che consenta di leggere la configurazione della distribuzione. Il ruolo Full administrator (Amministratore completo) dispone di questa autorizzazione. Per un ruolo personalizzato, deve essere selezionata l'opzione Read Only (Sola lettura) o Manage (Gestisci) nella categoria Other permissions (Altre autorizzazioni).

  Per creare un backup dei dati di registrazione della configurazione prima di eliminarli, anche per il ruolo personalizzato deve essere selezionata l'opzione Read Only (Sola lettura) o Manage (Gestisci) nella categoria Logging Permissions (Autorizzazioni di registrazione).

- **Database SQL Server:** è necessario disporre dell'accesso a SQL Server con l'autorizzazione per eliminare i record dal database. Ci sono due modi per farlo:

  - Utilizzare un accesso al database SQL Server con un ruolo del server sysadmin, che consente di eseguire qualsiasi attività sul server del database. In alternativa, i ruoli server `serveradmin` o `setupadmin` consentono di eseguire operazioni di eliminazione.
  - Se la distribuzione richiede maggiore sicurezza, utilizzare un accesso al database diverso da sysadmin mappato a un utente del database che dispone dell'autorizzazione per eliminare i record dal database.

    1. In SQL Server Management Studio, creare un accesso a SQL Server con un ruolo server diverso da "sysadmin".
    2. Mappare l'accesso a un utente nel database. SQL Server crea automaticamente un utente nel database con lo stesso nome dell'accesso.
    3. In Database role membership (Appartenenza al ruolo di database), specificare almeno uno dei membri del ruolo per l'utente del database: `ConfigurationLoggingSchema_ROLE` o `dbowner`.

    Per ulteriori informazioni, vedere la documentazione di SQL Server Management Studio.

Per eliminare i log di configurazione:

1. Accedere a Web Studio e selezionare **Logging** nel riquadro a sinistra.

2. Selezionare **Delete logs** (Elimina log) nella barra delle azioni.
3. Viene chiesto se si desidera creare un backup dei log prima che vengano eliminati. Se si sceglie di creare un backup, individuare la posizione in cui viene salvato l'archivio di backup. Il backup viene creato come file CSV.

Dopo aver cancellato i log di configurazione, l'eliminazione del log è la prima attività registrata nel log vuoto. Tale voce fornisce dettagli su chi ha eliminato i log e quando.

## Registri eventi

January 7, 2024

I seguenti articoli elencano e descrivono gli eventi che possono essere registrati dai servizi disponibili in Citrix Virtual Apps and Desktops.

Queste informazioni non sono complete. I lettori devono vedere i singoli articoli sulle funzionalità per ulteriori informazioni sugli eventi.

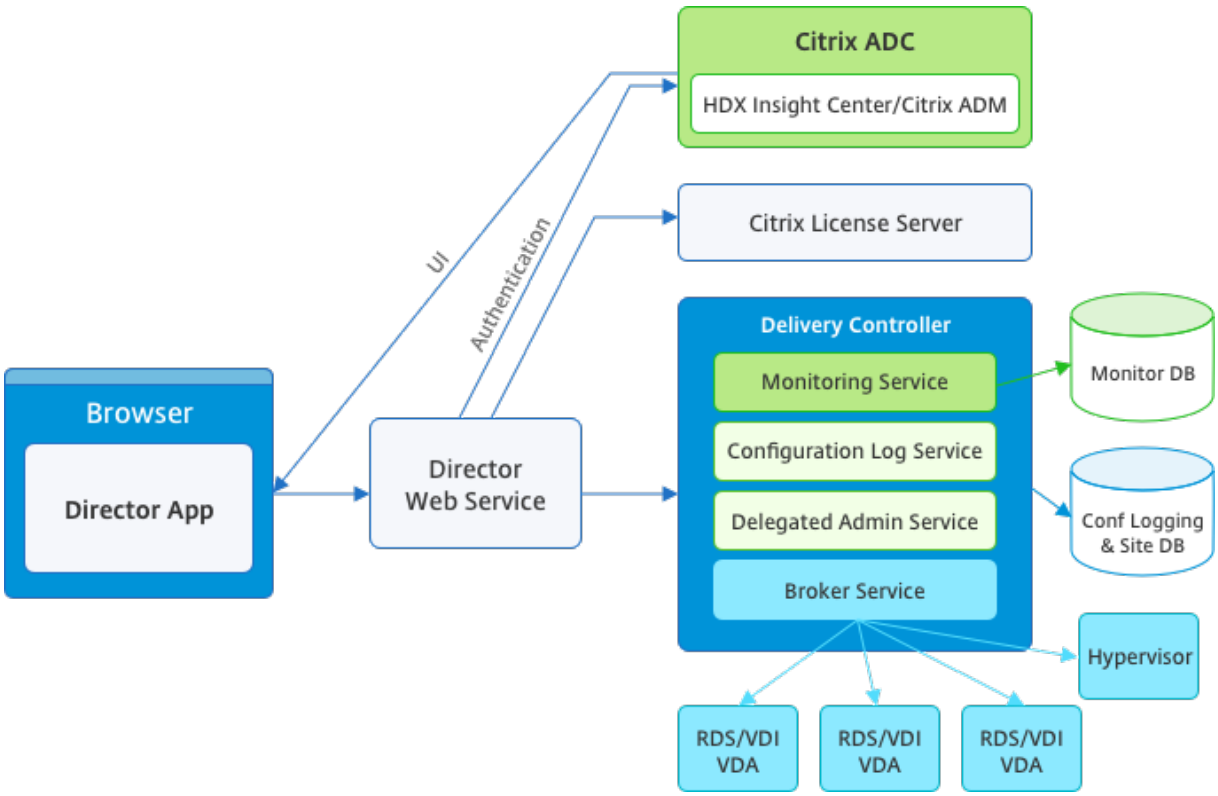
- Eventi del servizio Broker Citrix
- Eventi dell'SDK del servizio FMA Citrix
- Eventi del servizio di configurazione Citrix
- Eventi del servizio di amministrazione delegata Citrix

## Director

January 7, 2024

Director è una console di monitoraggio e risoluzione dei problemi per Citrix Virtual Apps and Desktops.




Director può accedere a:

- Dati in tempo reale provenienti dal Broker Agent mediante una console unificata integrata con Analytics, Performance Manager e Network Inspector. Le seguenti analisi alimentate da Citrix ADM per identificare i colli di bottiglia dovuti alla rete nell'ambiente Citrix Virtual Apps o Desktops:
  - Gestione delle prestazioni per la garanzia del funzionamento e della capacità
  - Analisi delle tendenze storiche e della rete
- Dati storici memorizzati nel database Monitor per accedere al database di registrazione della configurazione.
- Dati ICA provenienti da Citrix Gateway utilizzando Citrix ADM.
  - Visibilità sull'esperienza dell'utente finale per applicazioni virtuali, desktop e utenti per Citrix Virtual Apps o Desktop.
  - Correlazione dei dati di rete con i dati delle applicazioni e le metriche in tempo reale per una risoluzione efficace dei problemi.
  - Integrazione con lo strumento di monitoraggio Citrix Virtual Desktop 7 Director.

Director utilizza una dashboard per la risoluzione dei problemi che fornisce il monitoraggio storico e in tempo reale dello stato del sito Citrix Virtual Apps o Desktops. Questa funzione consente di vedere i guasti in tempo reale, fornendo una migliore idea dell'esperienza degli utenti finali.

Per ulteriori informazioni sulla compatibilità delle funzionalità di Director con Delivery Controller (DC), VDA e qualsiasi altro componente dipendente, vedere Matrice di compatibilità delle funzionalità.

> **Nota:**
>
> Con la divulgazione delle vulnerabilità del canale laterale ad esecuzione speculativa Meltdown e Spectre, Citrix consiglia di installare patch di mitigazione pertinenti. Queste patch potrebbero influire sulle prestazioni di SQL Server. Per ulteriori informazioni, vedere l'articolo del supporto Microsoft Protect SQL Server from attacks on Spectre and Meltdown side-channel vulnerabilities (protezione dalle vulnerabilità di campionamento dei dati di Spectre e Meltdown). Citrix consiglia di testare la scalabilità e pianificare i carichi di lavoro prima di installare le patch negli ambienti di produzione.

Director viene installato per impostazione predefinita come sito Web su Delivery Controller. Per i prerequisiti e altri dettagli, vedere la documentazione sui Requisiti di sistema relativa a questa versione. Per informazioni specifiche sull'installazione e la configurazione di Director, vedere Installazione e configurazione di Director.

### Accedere a Director

Il sito web di Director è https o `http://<Server FQDN>/Director`.

Se uno dei siti di una distribuzione multisito è inattivo, l'accesso richiede un po'più tempo perché tenta di connettersi al sito non attivo.

### Utilizzare Director con autenticazione smart card PIV

Director ora supporta l'autenticazione smart card basata su PIV (Personal Identity Verification) per l'accesso. Questa funzionalità è utile per le organizzazioni e gli enti pubblici che utilizzano l'autenticazione basata su smart card per il controllo degli accessi.
L'autenticazione con smart card richiede una configurazione specifica sul server Director e in Active Directory. I passaggi di configurazione sono descritti in dettaglio in Configurare l'autenticazione con smart card PIV.

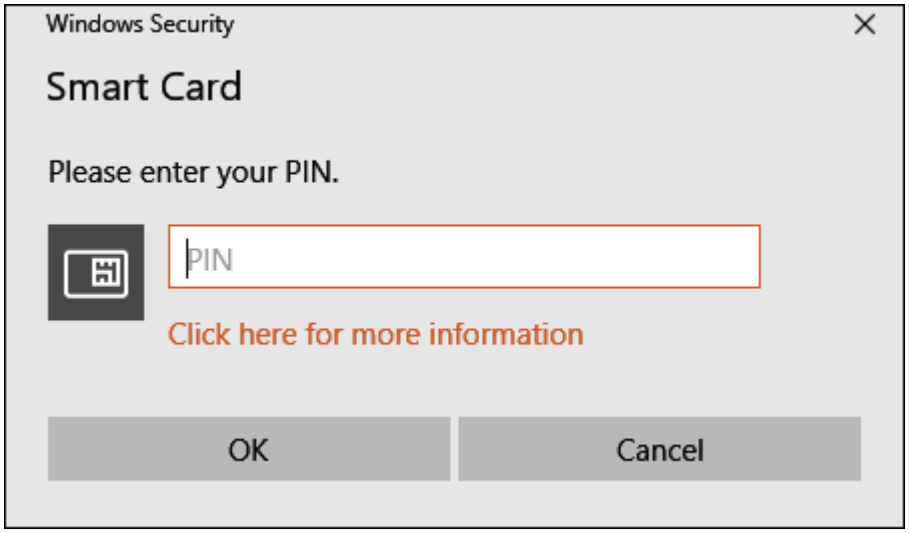
> **Nota:**
>
> L'autenticazione con smart card è supportata solo per gli utenti dello stesso dominio Active Directory.

Dopo aver eseguito la configurazione richiesta, è possibile accedere a Director utilizzando una smart card:

1. Inserire la smart card nel lettore di smart card.

2. Aprire un browser e passare all'URL di Director, `https://<directorfqdn>/Director`.
3. Selezionare un certificato utente valido dall'elenco visualizzato.
4. Immettere il token della smart card.




5. Dopo l'autenticazione, è possibile accedere a Director senza richiedere ulteriori credenziali nella pagina di accesso di Director.

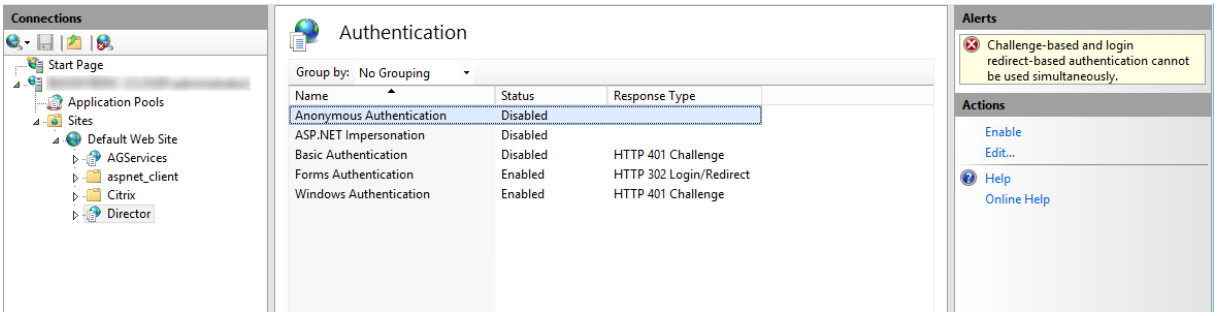
### Utilizzare Director con l'autenticazione integrata di Windows

Con l'autenticazione integrata di Windows (IWA), gli utenti appartenenti al dominio ottengono l'accesso diretto a Director senza dover reinserire le proprie credenziali nella pagina di accesso di Director. I prerequisiti per l'utilizzo dell'autenticazione integrata di Windows e di Director sono i seguenti:

- Attivare l'autenticazione integrata di Windows sul sito Web IIS che ospita Director. Quando si installa Director, vengono attivate le autenticazioni moduli e anonime. Per supportare l'autenticazione integrata di Windows e Director, disabilitare l'autenticazione anonima e abilitare l'autenticazione di Windows. L?autenticazione moduli deve rimanere impostata su Abilitata per l'autenticazione di utenti non di dominio.

  1. Avviare Gestione IIS.
  2. Andare a **Sites** (Siti) > **Default Web Site** (Sito Web predefinito) > **Director**.
  3. Selezionare **Authentication** (Autenticazione).
  4. Fare clic con il pulsante destro del mouse su **Autenticazione anonima** e selezionare **Disabilita**.
  5. Fare clic con il pulsante destro del mouse su **Autenticazione di Windows**e selezionare **Abilita**.




- Configurare l'autorizzazione di delega di Active Directory per il computer in cui viene eseguito Director. La configurazione è necessaria solo se Director e Delivery Controller sono installati su computer separati.

    1. Nel computer in cui viene eseguito Active Directory aprire Active Directory Management Console.
    2. In Active Directory Management Console passare a **Nome dominio** > **Computer.** Selezionare il computer in cui è in esecuzione Director.
    3. Fare clic con il pulsante destro del mouose e selezionare **Proprietà**.
    4. In Proprietà selezionare la scheda **Delega**.
    5. Selezionare l'opzione **Considera attendibile il computer per la delega a qualsiasi servizio (solo Kerberos)**.

- Il browser utilizzato per accedere a Director deve supportare l'autenticazione integrata di Windows. In Firefox e Chrome potrebbero essere necessari ulteriori passaggi di configurazione. Per ulteriori informazioni, vedere la documentazione del browser.
- Il servizio di monitoraggio deve eseguire Microsoft .NET Framework 4.5.1 o versione successiva supportata come da elenco dei requisiti di sistema per Director. Per ulteriori informazioni, vedere Requisiti di sistema.

Quando un utente si scollega da Director o se la sessione è scaduta, viene visualizzata la pagina di accesso. Dalla pagina di accesso, l'utente può impostare il tipo di autenticazione **su Accesso automatico** o **Credenziali utente**.

## Visualizzazioni dell'interfaccia

Director fornisce diverse visualizzazioni dell'interfaccia su misura per particolari amministratori. Le autorizzazioni del prodotto determinano ciò che viene visualizzato e i comandi disponibili.

Ad esempio, gli amministratori dell'helpdesk vedono un'interfaccia personalizzata per le attività dell'helpdesk. Director consente agli amministratori dell'helpdesk di cercare l'utente che segnala un problema e di visualizzare l'attività associata a tale utente. Ad esempio, lo stato delle applicazioni e dei processi dell'utente. Possono risolvere rapidamente i problemi eseguendo azioni quali la chiusura di

un'applicazione o un processo che non risponde, lo shadowing delle operazioni sul computer dell'utente, il riavvio del computer o il ripristino del profilo utente.

Al contrario, gli amministratori completi vedono e gestiscono l'intero sito e possono eseguire comandi per più utenti e computer. La dashboard fornisce una panoramica degli aspetti chiave di una distribuzione, ad esempio lo stato delle sessioni, gli accessi degli utenti e l'infrastruttura del sito. Le informazioni vengono aggiornate ogni minuto. Se si verificano problemi, vengono visualizzati automaticamente i dettagli relativi al numero e al tipo di errori che si sono verificati.

Per ulteriori informazioni sui vari ruoli e le relative autorizzazioni in Director, vedere Amministrazione delegata e Director

### Raccolta dei dati di utilizzo da parte di Google Analytics

Il servizio Director inizia a utilizzare Google Analytics per raccogliere i dati di utilizzo dopo l'installazione di Director. Vengono raccolte statistiche sull'utilizzo delle pagine Trends e analisi delle chiamate API OData. La raccolta di dati analitici è conforme all'Informativa sulla privacy di Citrix. La raccolta dati è abilitata per impostazione predefinita quando si installa Director.

Per disattivare la raccolta dei dati di Google Analytics, modificare la chiave del Registro di sistema sul computer in cui è installato Director. Se la chiave del Registro di sistema non esiste, crearla e impostarla sul valore desiderato. Aggiornare l'istanza di Director dopo aver modificato il valore della chiave del Registro di sistema.

**Attenzione:** l'utilizzo non corretto dell'Editor del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'editor del Registro di sistema a proprio rischio. Citrix consiglia di eseguire il backup del Registro di sistema di Windows prima di modificarlo.

Posizione: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Nome: DisableGoogleAnalytics

Valore: 0 = abilitato (predefinito), 1 = disabilitato

È possibile utilizzare il seguente cmdlet PowerShell per disabilitare la raccolta dati da parte di Google Analytics:

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
    DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

### Guida alle nuove funzionalità

Director dispone di una guida all'interno del prodotto che utilizza Pendo per fornire informazioni sulle nuove funzionalità rilasciate nella versione corrente di Director. La rapida panoramica abbinata a messaggi appropriati all'interno del prodotto aiuta a comprendere le novità del prodotto.

Per disattivare questa funzionalità, modificare la chiave del Registro di sistema come descritto di seguito nel computer in cui è installato Director. Se la chiave del Registro di sistema non esiste, crearla e impostarla sul valore desiderato. Aggiornare l'istanza di Director dopo aver modificato il valore della chiave del Registro di sistema.

> **Attenzione:**
>
> l'utilizzo non corretto dell'Editor del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'editor del Registro di sistema a proprio rischio. Citrix consiglia di eseguire il backup del Registro di sistema di Windows prima di modificarlo.

Posizione: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Nome: DisableGuidedHelp

Valore: 0 = abilitato (predefinito), 1 = disabilitato

È possibile utilizzare il cmdlet PowerShell seguente per disattivare la guida all'interno del prodotto:

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
    -PropertyType DWORD -Value 1
```

## Installazione e configurazione

April 3, 2024

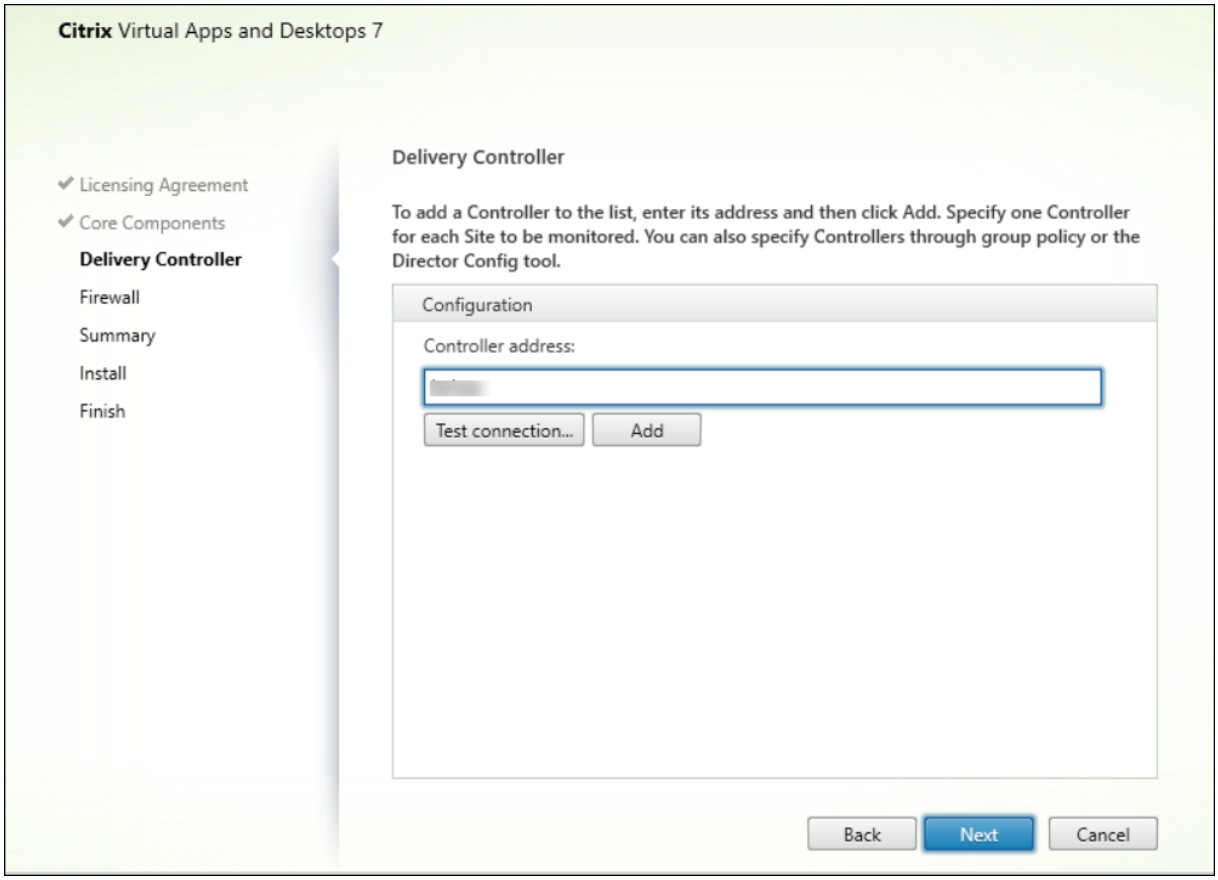
### Installare Director

Installare Director utilizzando il programma di installazione ISO completo del prodotto per Citrix Virtual Apps and Desktops, che verifica i prerequisiti, installa eventuali componenti mancanti, imposta il sito Web di Director ed esegue la configurazione di base. Per i prerequisiti e altri dettagli, vedere la documentazione sui Requisiti di sistema relativa a questa versione. Questa versione di Director non

è compatibile con le distribuzioni di Virtual Apps precedenti alla 6.5 o con le distribuzioni di Virtual Desktops precedenti alla 7.
La configurazione predefinita fornita dal programma di installazione ISO gestisce le distribuzioni tipiche. Se Director non è stato incluso durante l'installazione, utilizzare il programma di installazione ISO per aggiungere Director. Per aggiungere ulteriori componenti, eseguire nuovamente il programma di installazione ISO e selezionare i componenti da installare. Per informazioni sull'utilizzo del programma di installazione ISO, vedere Installare i componenti principali nella documentazione di installazione. Citrix consiglia di eseguire l'installazione utilizzando solo il programma di installazione ISO completo del prodotto, non il file con estensione MSI.

Quando Director è installato sul controller, viene configurato automaticamente con localhost come indirizzo del server e Director comunica con il controller locale per impostazione predefinita. Per installare Director su un server dedicato remoto rispetto a un controller, viene richiesto di immettere l'FQDN o l'indirizzo IP di un controller.




> **Nota:**
>
> Fare clic su **Add** (Aggiungi) per aggiungere il controller da monitorare.

Director comunica con il controller specificato per impostazione predefinita. Specificare un solo indirizzo di controller per ogni sito monitorato. Director rileva automaticamente tutti gli altri controller

nello stesso sito e passa a tali controller se il controller specificato presenta un problema.

> **Nota:**
>
> Director non bilancia il carico tra i controller.

Per proteggere le comunicazioni tra il browser e il server Web, Citrix consiglia di implementare TLS nel sito Web IIS che ospita Director. Per istruzioni, fare riferimento alla documentazione su IIS di Microsoft. Non è necessaria la configurazione di Director per abilitare TLS.

## Distribuire e configurare Director

Quando Director viene utilizzato in un ambiente contenente più di un sito, assicurarsi di sincronizzare gli orologi di sistema su tutti i server in cui sono installati controller, Director e altri componenti principali. In caso contrario, i siti potrebbero non essere visualizzati correttamente in Director.

> **Importante:**
>
> Per proteggere la sicurezza dei nomi utente e delle password inviati utilizzando testo normale attraverso la rete, consentire le connessioni di Director utilizzando solo HTTPS e non HTTP. Alcuni strumenti sono in grado di leggere nomi utente e password in testo normale nei pacchetti di rete HTTP (non crittografati), il che può creare un potenziale rischio per la sicurezza per gli utenti.

### Configurare le autorizzazioni

Per accedere a Director, gli amministratori con le autorizzazioni per Director devono essere utenti di dominio di Active Directory e devono disporre dei seguenti diritti:

- Diritti di lettura in tutte le foreste di Active Directory in cui eseguire ricerche (vedere Configurazione avanzata).
- Ruoli di amministratore delegato configurati (vedere Amministrazione delegata e Director).
- Per lo shadowing degli utenti, gli amministratori devono essere configurati utilizzando un criterio di gruppo Microsoft per Assistenza remota di Windows. Inoltre:
  - Durante l'installazione dei VDA, assicurarsi che la funzionalità Assistenza remota di Windows sia abilitata su tutti i dispositivi utente (opzione selezionata per impostazione predefinita).
  - Quando si installa Director su un server, assicurarsi che l'applicazione Assistenza remota di Windows sia installata (opzione selezionata per impostazione predefinita). Tuttavia, è disabilitata sul server per impostazione predefinita. Non è necessario abilitare la funzionalità perché Director fornisca assistenza agli utenti finali. Citrix consiglia di lasciare disabilitata la funzionalità per migliorare la sicurezza sul server.

- Per consentire agli amministratori di avviare Assistenza remota di Windows, concedere loro le autorizzazioni richieste utilizzando le impostazioni dei Criteri di gruppo Microsoft appropriate per Assistenza remota. Per informazioni, vedere CTX127388: Come abilitare l'assistenza remota per Desktop Director.

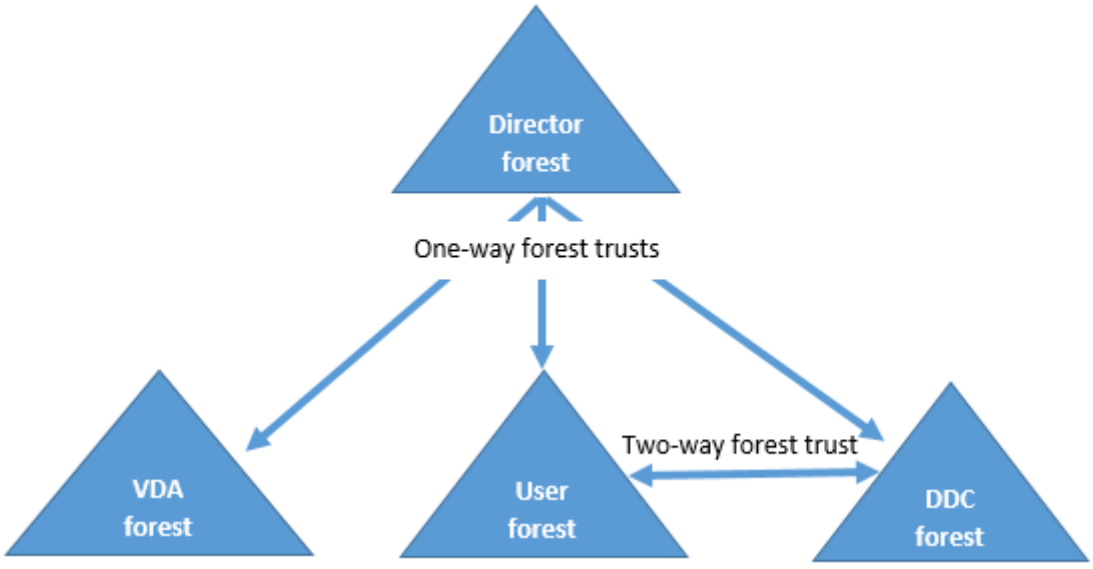
## Configurazione avanzata

January 7, 2024

Director può supportare ambienti multi-foresta con una configurazione foresta in cui utenti, Delivery Controller (DC), VDA e Director si trovano in foreste diverse. Ciò richiede una corretta configurazione delle relazioni di trust tra le foreste e delle impostazioni di configurazione.

### Configurazione consigliata in un ambiente multi-foresta

La configurazione consigliata richiede la creazione di relazioni di trust delle foreste in uscita e in entrata tra le foreste con autenticazione a livello di dominio.




La relazione di trust di Director consente di risolvere i problemi nelle sessioni utente, nei VDA e nei Delivery Controller situati in foreste diverse.

La configurazione avanzata richiesta per il supporto di più foreste da parte di Director è controllata tramite le impostazioni definite in Internet Information Services (IIS) Manager.

> **Importante:**
>
> Quando si modifica un'impostazione in IIS, il servizio Director riavvia e disconnette automaticamente gli utenti.

Per configurare le impostazioni avanzate utilizzando IIS:

1. Aprire la console di Internet Information Services (IIS) Manager.
2. Andare al sito Web di Director sotto il sito Web predefinito.
3. Fare doppio clic su **Application Settings** (Impostazioni applicazione).
4. Fare doppio clic su un'impostazione per modificarla.
5. Fare clic su **Add** (Aggiungi) per aggiungere una nuova impostazione.

Director utilizza Active Directory per individuare utenti e cercare più informazioni su utenti e computer. Per impostazione predefinita, Director esegue ricerche nel dominio o nella foresta in cui:

- L'account dell'amministratore è un membro.
- Il server Web di Director è un membro (se diverso).

Director tenta di eseguire ricerche a livello di foresta utilizzando il catalogo globale di Active Directory. Se non si dispone delle autorizzazioni per eseguire ricerche a livello di foresta, la ricerca viene eseguita solo all'interno del dominio.

La ricerca o la visualizzazione di dati da un altro dominio o foresta di Active Directory richiede che i domini o le foreste in cui eseguire ricerche vengano impostati esplicitamente. Configurare la seguente impostazione Applications (Applicazioni) sul sito Web di Director in IIS Manager:

```
Connector.ActiveDirectory.Domains = (user),(server)
```

Gli attributi di valore user (utente) e server rappresentano rispettivamente i domini dell'utente Director (amministratore) e del server Director.

Per abilitare le ricerche da un dominio o da una foresta aggiuntivi, aggiungere il nome del dominio all'elenco, come illustrato in questo esempio:

```
Connector.ActiveDirectory.Domains = (user),(server),\<domain1\>,\<
    domain2\>
```

Per ogni dominio dell'elenco, Director tenta di eseguire ricerche a livello di foresta. Se non si dispone delle autorizzazioni per eseguire ricerche a livello di foresta, la ricerca viene eseguita solo all'interno del dominio.

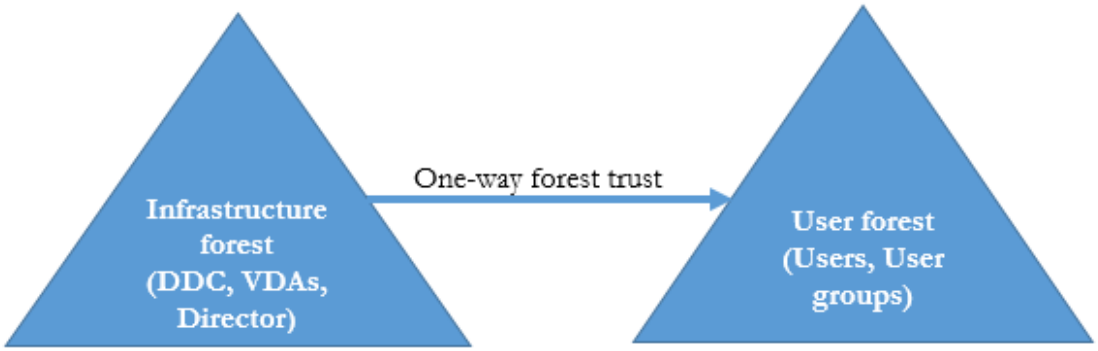
### Configurazione del gruppo locale del dominio

La maggior parte dei provider di servizi Citrix (CSP) dispone di configurazioni di ambiente simili composte da VDA, DC e Director nella foresta Infrastructure (Infrastruttura). Gli utenti o i record del gruppo

di utenti appartengono alla foresta Client (Cliente). È presente un trust in uscita unidirezionale dalla foresta Infrastructure (Infrastruttura) alla foresta Client (Cliente).

Gli amministratori CSP in genere creano un gruppo locale di dominio nella foresta Infrastructure (Infrastruttura) e aggiungono gli utenti o i gruppi di utenti nella foresta Client (Cliente) a questo gruppo locale di dominio.




Director può supportare una configurazione multi-foresta come questa e monitorare le sessioni degli utenti configurati utilizzando gruppi locali di dominio.

1. Aggiungere le seguenti impostazioni Applications (Applicazioni) al sito Web di Director in IIS Manager:

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true

   DomainLocalGroupSearchDomains= \<domain1\>,\<domain2\>
   ```

   <domain1><domain2> sono nomi delle foreste in cui è presente il gruppo locale di dominio.

2. Assegnare il gruppo locale di dominio ai gruppi di consegna in Web Studio.
3. Riavviare IIS e accedere di nuovo a Director perché le modifiche abbiano effetto. Ora Director può monitorare e mostrare le sessioni di questi utenti.

### Aggiungere siti a Director

Se Director è già installato, configurarlo in modo che funzioni con più siti. A tale scopo, utilizzare IIS Manager Console su ciascun server Director per aggiornare l'elenco degli indirizzi del server nelle impostazioni dell'applicazione.

Aggiungere un indirizzo di un controller di ciascun sito nella seguente impostazione:

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
<!--NeedCopy-->
```

SiteAController e SiteBController sono gli indirizzi dei Delivery Controller di due siti diversi.

### Disabilitare la visibilità delle applicazioni in esecuzione in Activity Manager

Per impostazione predefinita, Activity Manager in Director visualizza un elenco di tutte le applicazioni in esecuzione per la sessione di un utente. Queste informazioni vengono visualizzate da tutti gli amministratori che hanno accesso alla funzionalità Activity Manager in Director. Per i ruoli Delegated Administrator (Amministratore delegato) sono compresi i ruoli Full Administrator (Amministratore completo), Delivery Group Administrator (Amministratore del gruppo di consegna) e Help Desk Administrator (Amministratore dell'helpdesk).

Per proteggere la privacy degli utenti e delle applicazioni che eseguono, è possibile disattivare l'elenco delle applicazioni in esecuzione nella scheda **Applications**.

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non garantisce che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

1. Sul VDA, modificare la chiave del Registro di sistema in HKEY_LOCAL_MACHINE\Software\Citrix\Director\Task
   Per impostazione predefinita, la chiave è impostata su 1. Modificare il valore su 0, il che significa che le informazioni non vengono raccolte dal VDA e quindi non vengono visualizzate in Activity Manager (Gestione attività).
2. Sul server con Director installato, modificare l'impostazione che controlla la visibilità delle applicazioni in esecuzione. Per impostazione predefinita, il valore è "true", il che consente la visibilità delle applicazioni in esecuzione nella scheda Applications (Applicazioni). Se il valore viene modificato in "false", la visibilità viene disabilitata. Questa opzione ha effetto solo su Activity Manager (Gestione attività) in Director, non sul VDA.
   Modificare il valore della seguente impostazione:
   UI.TaskManager.EnableApplications = false

> **Importante:**
>
> Per disabilitare la visualizzazione delle applicazioni in esecuzione, apportare entrambe le modifiche per assicurarsi che i dati non vengano visualizzati in Activity Manager (Gestione attività).

## Configurare l'autenticazione con smart card PIV

January 10, 2024

Questo articolo elenca la configurazione richiesta sul server di Director e in Active Directory per abilitare la funzionalità di autenticazione con smart card.

> **Nota:**
>
> L'autenticazione con smart card è supportata solo per gli utenti dello stesso dominio Active Directory.

## Configurazione del server di Director

Eseguire i seguenti passaggi di configurazione sul server di Director:

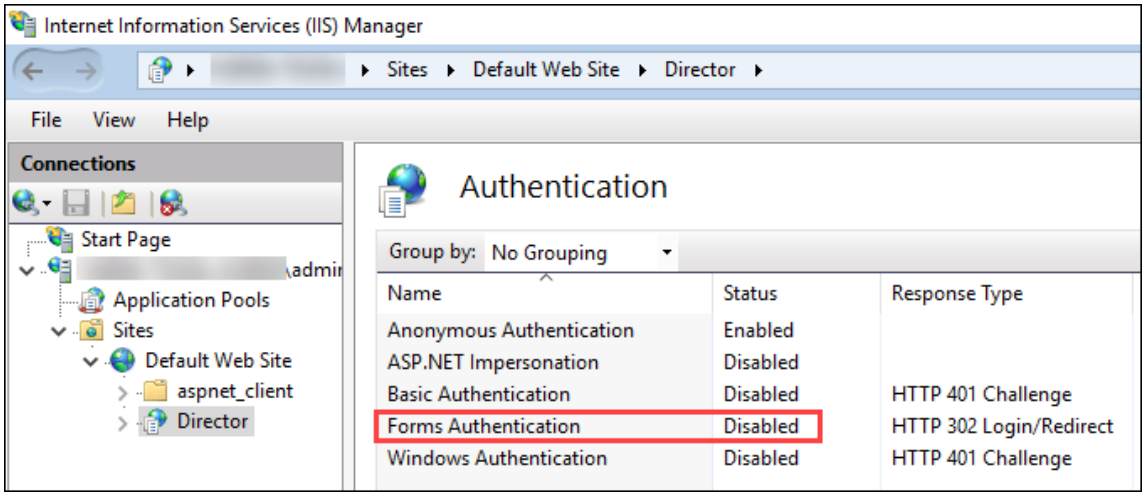
1. Installare e abilitare l'autenticazione con mapping dei certificati client. Seguire la procedura per l'**autenticazione con mapping dei certificati client utilizzando le istruzioni di Active Directory** nel documento di Microsoft Autenticazione con mapping dei certificati client.
2. Disabilitare l'autenticazione dei moduli sul sito di Director.

   Avviare Gestione IIS.

   Andare a **Sites** (Siti) > **Default Web Site** (Sito Web predefinito) > **Director**.

   Selezionare **Authentication** (Autenticazione).

   Fare clic con il pulsante destro del mouse su **Forms Authentication** (Autenticazione moduli) e selezionare **Disable** (Disabilita).




3. Configurare l'URL di Director per il protocollo più sicuro https (anziché HTTP) per l'autenticazione dei certificati client.

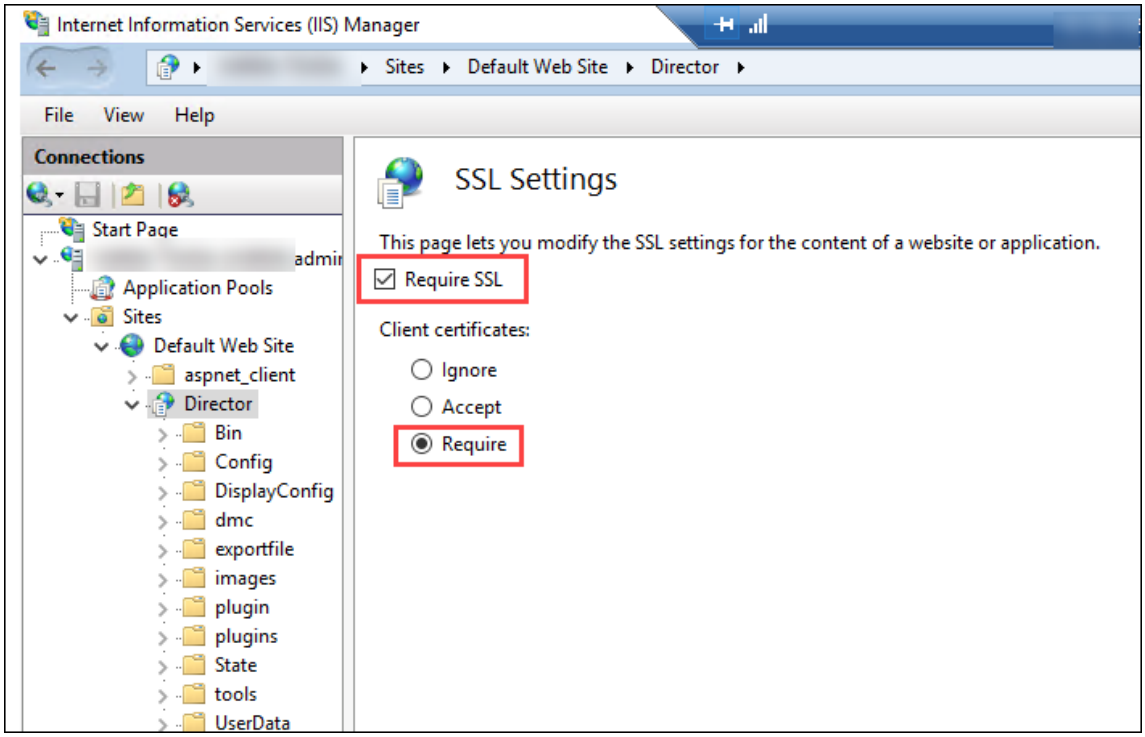
   a) Avviare Gestione IIS.

   b) Andare a **Sites** (Siti) > **Default Web Site** (Sito Web predefinito) > **Director**.

   c) Selezionare **SSL Settings** (Impostazioni SSL).

d) Selezionare **Require SSL** (Richiedi SSL) e **Client certificates** (Certificati client) > **Require** (Richiedi).




4. Aggiornare web.config. Aprire il file web.config (disponibile in c:\inetpub\wwwroot\Director) utilizzando un editor di testo.

Sotto l'elemento principale `<system.webServer>`, aggiungere il seguente snippet come primo elemento secondario:

```
<defaultDocument>
   <files>
       <add value="LogOn.aspx"/>
   </files>
</defaultDocument>
```

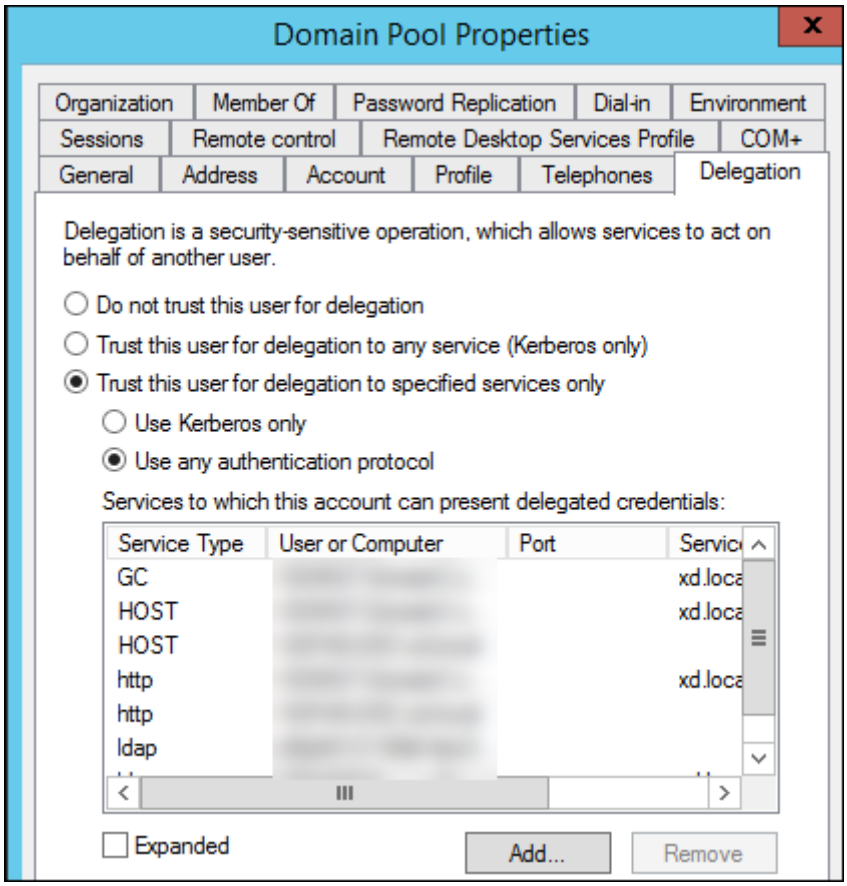
### Configurazione di Active Directory

Per impostazione predefinita, l'applicazione Director viene eseguita con la proprietà di identità **Application Pool** (Pool di applicazioni). L'autenticazione con smart card richiede una delega in base alla quale l'identità dell'applicazione Director deve disporre dei privilegi Trusted Computing Base (TCB) sull'host del servizio.

Citrix consiglia di creare un account di servizio separato per l'identità Application Pool (Pool di applicazioni). Creare l'account del servizio e assegnare i privilegi TCB secondo le istruzioni nell'articolo MSDN di Microsoft Protocol Transition with Constrained Delegation Technical Supplement.

Assegnare l'account di servizio appena creato al pool di applicazioni di Director. La figura seguente illustra la finestra di dialogo delle proprietà di un account di servizio di esempio, Domain Pool.



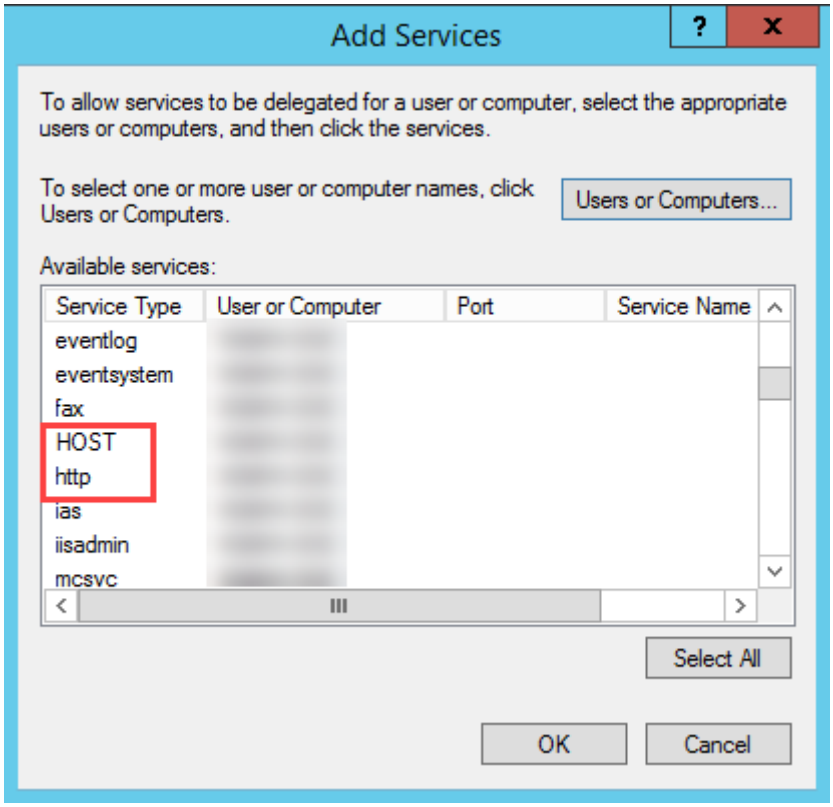

Configurare i seguenti servizi per questo account:

- Delivery Controller: HOST, HTTP
- Director: HOST, HTTP
- Active Directory: GC, LDAP

Per configurare:

1. Nella finestra di dialogo delle proprietà dell'account utente, fare clic su **Add** (Aggiungi).
2. Nella finestra di dialogo **Add Services** (Aggiungi servizi), fare clic su Users (Utenti) o Computers (Computer).
3. Selezionare il nome host del Delivery Controller.
4. Dall'elenco **Available services** (Servizi disponibili), selezionare HOST and HTTP (HOST e HTTP) come **Service Type** (Tipo di servizio).




Analogamente, aggiungere tipi di servizio per gli host **Director** e **Active Directory**.

### Creare record relativi al nome dell'entità servizio

È necessario creare un account di servizio per ogni server Director e per gli IP virtuali (VIP) con bilanciamento del carico utilizzati per accedere a un pool di server Director. È necessario creare i record dei nomi delle entità servizio (SPN) per configurare una delega all'account di servizio appena creato.

- Per creare un record SPN per un server Director, utilizzare il comando seguente:

```
1   setspn -a http/<directorServer>.<domain_fqdn> <domain>\<
       DirectorAppPoolServiceAcct>
2
3  <!--NeedCopy-->
```

- Use the following command to create an SPN record for a load-balanced VIP:

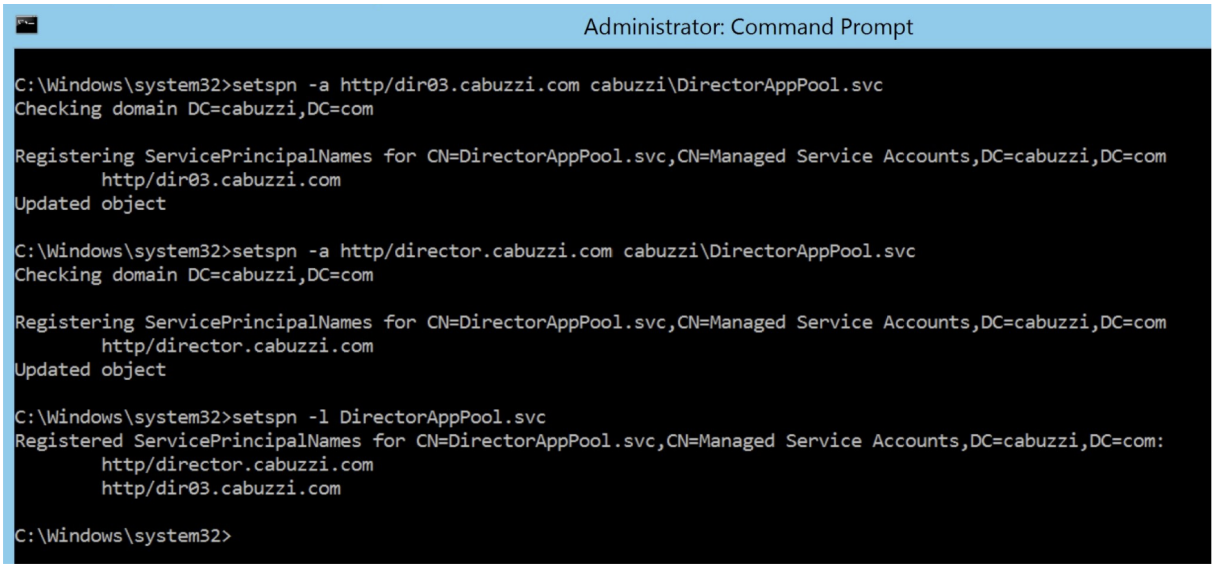
```
1   setspn -S http/<DirectorFQDN> <domain>\<
       DirectorAppPoolServiceAcct>
2
3  <!--NeedCopy-->
```

- Utilizzare il comando seguente per visualizzare o verificare gli SPN creati:

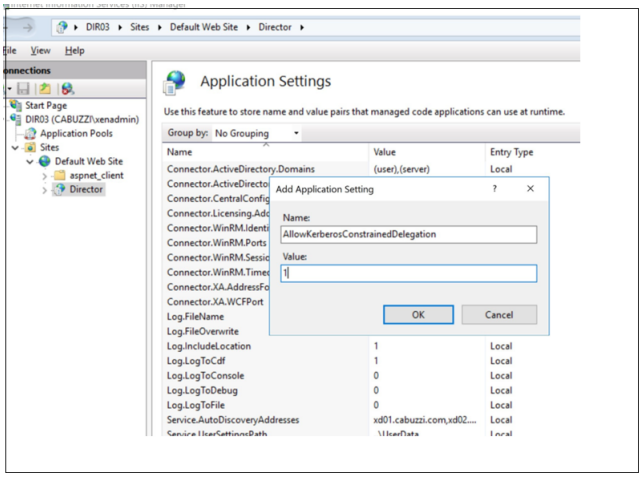
```
1  setspn  – l <DirectorAppPoolServiceAcct>
```

```
2
3   <!--NeedCopy-->
```

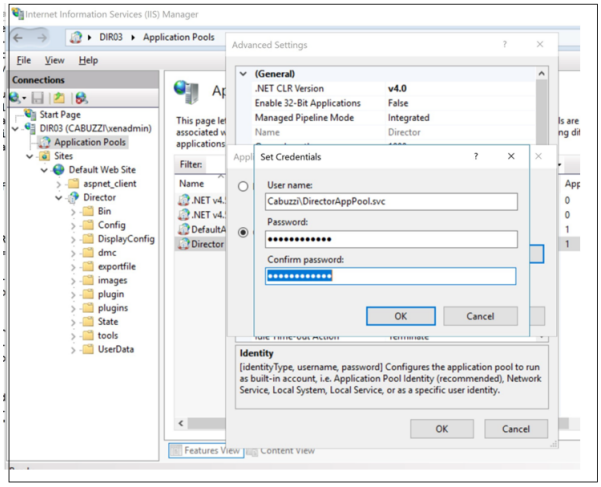



- Select the Director virtual directory in the left pane and double click **Application Settings**. Inside the Application Settings window, click **Add** and ensure **AllowKerberosConstrained-Delegation** is set to 1.




- Select **Application Pools** in the left-hand pane, then right-click the Director application pool and select **Advanced Settings**.
- Select **Identity**, click the ellipses (“…”) to enter the service account domain\logon and password credentials. Close the IIS console.




- From an elevated command prompt, change the directory to C:\Windows\System32\inetsrv and enter the following commands:

```
appcmd.exe set config "Default Web Site" -section:system.webServer
    /security/authentication/clientCertificateMappingAuthentication /
    enabled:"True" /commit:apphost

<!--NeedCopy-->
```

```
appcmd.exe set config "Default Web Site" -section:system.
    webServer/security/access /sslFlags:"Ssl, SslNegotiateCert" /
    commit:apphost
\`\`\`

![Prompt dei comandi](/en-us/citrix-virtual-apps-desktops/2308/media/
    dir-smart-card-auth-5-scaled.png)

## Configurazione del browser Firefox

Per utilizzare il browser Firefox, installare il driver PIV disponibile
    alla pagina [OpenSC 0.17.0](https://github.com/OpenSC/OpenSC/
    releases/tag/0.17.0). Per istruzioni sull'installazione e la
    configurazione, vedere [Installazione passo-passo del modulo OpenSC
    PKCS#11 in Firefox](https://github.com/OpenSC/OpenSC/wiki/Installing
    -OpenSC-PKCS%2311-Module-in-Firefox,-Step-by-Step).
Per informazioni sull'utilizzo della funzionalità di autenticazione con
    smart card in Director, vedere la sezione [Utilizzare Director con
    l'autenticazione con smart card basata su PIV](/it-it/citrix-virtual
    -apps-desktops/2308/director.html#use-director-with-piv-smart-card-
    authentication) dell'articolo su Director.<!--NeedCopy-->
```

# Configurare l'analisi di rete

January 7, 2024

> **Nota:**
> la disponibilità di questa funzionalità dipende dalla licenza dell'organizzazione e dalle autorizzazioni di amministratore.

Director si integra con Citrix ADM per fornire analisi di rete e gestione delle prestazioni:

- L'analisi di rete utilizza i report HDX Insight di Citrix ADM per fornire una visualizzazione contestuale di applicazioni e desktop della rete. Con questa funzionalità, Director fornisce analisi avanzate del traffico ICA nella distribuzione.
- La gestione delle prestazioni fornisce la conservazione storica e la reportistica sulle tendenze. Mettendo a confronto la conservazione storica dei dati con la valutazione in tempo reale, è possibile creare report sulle tendenze, tra cui le tendenze relative alla capacità e allo stato.

Dopo aver abilitato questa funzionalità in Director, i report HDX Insight forniscono a Director informazioni aggiuntive:

- La scheda Network (Rete) nella pagina Trends (Tendenze) mostra gli effetti di latenza e larghezza di banda per applicazioni, desktop e utenti nell'intera distribuzione.
- La pagina User Details (Dettagli utente) mostra informazioni sulla latenza e sulla larghezza di banda specifiche di una determinata sessione utente.

**Limitazioni:**

- Nella vista Trends (Tendenze), i dati di accesso della connessione HDX non vengono raccolti per VDA precedenti alla versione 7. Per i VDA precedenti, i dati del grafico vengono visualizzati come 0.

Per abilitare l'analisi di rete, è necessario installare e configurare Citrix ADM in Director. Director richiede Citrix ADM versione 11.1 Build 49.16 o successiva. MAS è un'appliance virtuale che viene eseguita su Citrix Hypervisor. Utilizzando l'analisi di rete, Director comunica e raccoglie le informazioni relative alla distribuzione.

Per ulteriori informazioni, vedere la documentazione di Citrix ADM.

> **Nota:**
>
> Citrix NetScaler Insight Center ha raggiunto la data di fine manutenzione il 15 maggio 2018. Vedere la matrice dei prodotti Citrix. Integrare Director con Citrix ADM per l'analisi di rete. Per

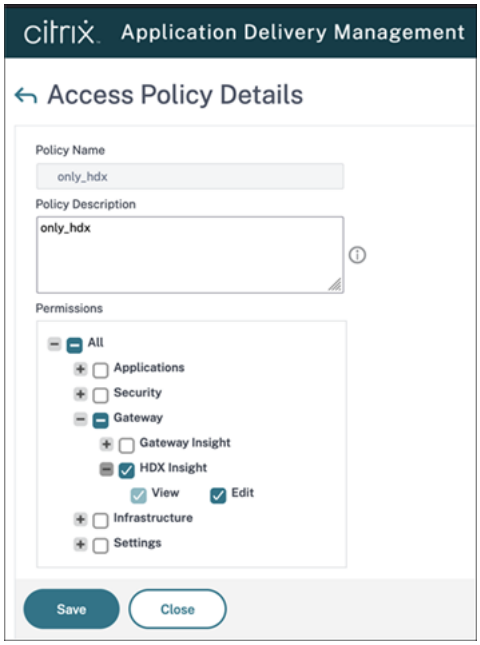
 

migrare NetScaler Insight Center a Citrix ADM, vedere Eseguire la migrazione da NetScaler Insight Center a Citrix ADM.

1. Sul server in cui è installato Director, individuare lo strumento della riga di comando Director-Config in C:\inetpub\wwwroot\Director\tools ed eseguirlo con il parametro /confignetscaler da un prompt dei comandi.
2. Quando richiesto, immettere il nome della macchina Citrix ADM (FQDN o indirizzo IP), il nome utente, la password, il tipo di connessione HTTPS (consigliato rispetto ad HTTP) e scegliere l'integrazione Citrix ADM.
3. Per verificare le modifiche, disconnettersi e riconnettersi.

**Nota:**

Per motivi di sicurezza, si consiglia di creare un ruolo personalizzato per l'integrazione di ADM con Director con un'autorizzazione sufficiente per accedere solo a HDX Insight.




Per ulteriori informazioni, vedere Configure access policies (Configurare i criteri di accesso).

## Amministrazione delegata e Director

January 7, 2024

L'amministrazione delegata utilizza tre concetti: amministratori, ruoli e ambiti. Le autorizzazioni si basano sul ruolo di amministratore e sull'ambito di questo ruolo. Ad esempio, a un amministratore

potrebbe essere assegnato un ruolo di amministratore dell'helpdesk in cui l'ambito riguarda la responsabilità per gli utenti finali in un solo sito.

Per informazioni sulla creazione di amministratori delegati, vedere l'articolo principale sull'amministrazione delegata.

Le autorizzazioni amministrative determinano l'interfaccia di Director che viene visualizzata agli amministratori e le attività che possono eseguire. Le autorizzazioni determinano:

- Le viste a cui l'amministratore può accedere, denominate collettivamente come "vista".
- Desktop, macchine e sessioni che l'amministratore può visualizzare e con cui può interagire.
- I comandi che l'amministratore può eseguire, ad esempio lo shadowing della sessione di un utente o l'abilitazione della modalità di manutenzione.

Anche i ruoli e le autorizzazioni predefiniti determinano il modo in cui gli amministratori utilizzano Director:

| Ruolo di amministratore | Autorizzazioni in Director |
| --- | --- |
| Full Administrator (Amministratore completo) | Ha accesso completo a tutte le viste e può eseguire tutti i comandi, incluso lo shadowing della sessione di un utente, l'abilitazione della modalità di manutenzione e l'esportazione dei dati delle tendenze. |
| Delivery group Administrator (Amministratore del gruppo di consegna) | Ha accesso completo a tutte le viste e può eseguire tutti i comandi, incluso lo shadowing della sessione di un utente, l'abilitazione della modalità di manutenzione e l'esportazione dei dati delle tendenze. |
| Read Only Administrator (Amministratore di sola lettura) | Può accedere a tutte le viste e visualizzare tutti gli oggetti in ambiti specifici e informazioni globali. Può scaricare report dai canali HDX ed esportare i dati delle tendenze utilizzando l'opzione Export (Esporta) nella vista Trends (Tendenze). Non può eseguire altri comandi o modificare elementi nelle viste. |

| Ruolo di amministratore | Autorizzazioni in Director |
| --- | --- |
| Help Desk Administrator (Amministratore dell'helpdesk) | Può accedere solo alle viste Help Desk (Helpdesk) e User Details (Dettagli utente) e può visualizzare solo gli oggetti che l'amministratore è delegato a gestire. Può fare lo shadowing della sessione di un utente ed eseguire comandi per quell'utente. Può eseguire operazioni in modalità di manutenzione. Può utilizzare le opzioni di controllo dell'alimentazione per macchine con sistema operativo a sessione singola. Non può accedere alle viste Dashboard, Trends (Tendenze), Alerts (Avvisi) o Filters (Filtri). Non può utilizzare le opzioni di controllo dell'alimentazione per macchine con sistema operativo multisessione. |
| Machine catalog administrator (Amministratore del catalogo macchine) | Può accedere solo alla pagina Machine Details (Dettagli macchina) (ricerca basata su macchina). |
| Host Administrator (Amministratore host) | Nessun accesso. Questo amministratore non è supportato per Director e non può visualizzare i dati. |

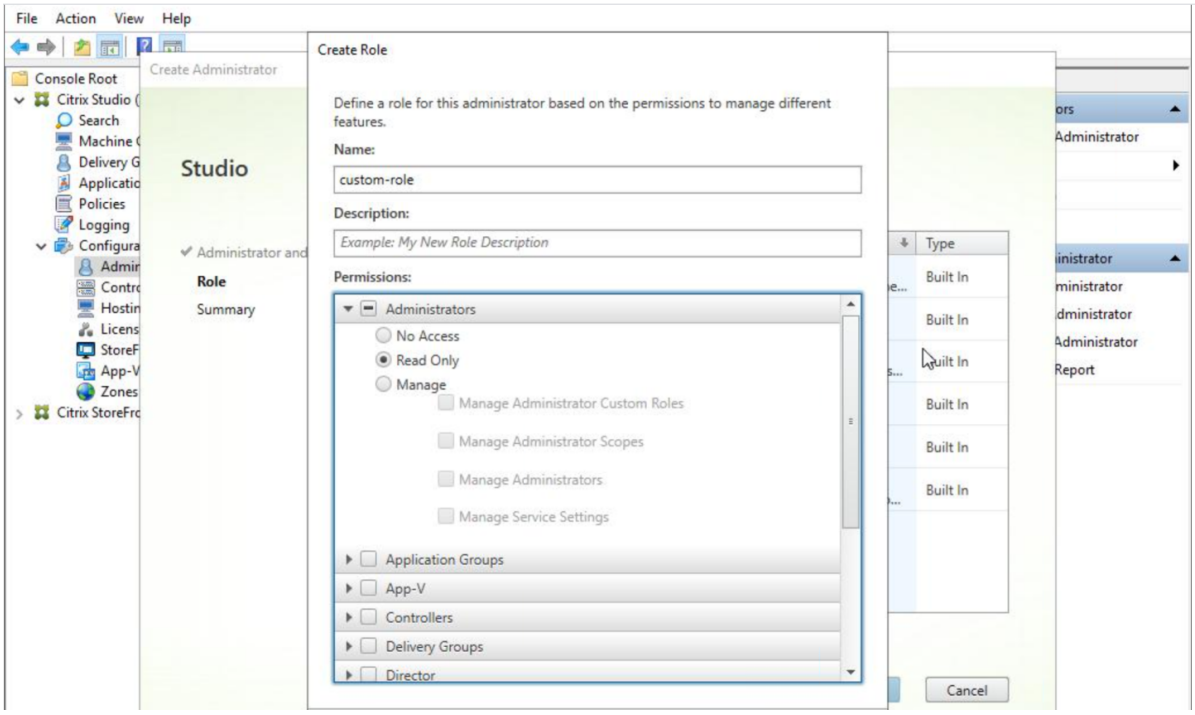
### Configurare ruoli personalizzati per gli amministratori di Director

In Studio è anche possibile configurare ruoli personalizzati specifici per Director, in modo da soddisfare più strettamente i requisiti dell'organizzazione e delegare le autorizzazioni in modo più flessibile. Ad esempio, è possibile limitare il ruolo Help Desk administrator (Amministratore dell'helpdesk) predefinito in modo che l'amministratore non possa disconnettere le sessioni.

Se si crea un ruolo personalizzato con le autorizzazioni di Director, è necessario assegnare a tale ruolo altre autorizzazioni generiche:

- Autorizzazione del Delivery Controller per accedere a Director - accesso almeno in sola lettura nel nodo Administrator
- Autorizzazioni ai gruppi di consegna per visualizzare i dati relativi a tali gruppi di consegna in Director - accesso almeno in sola lettura



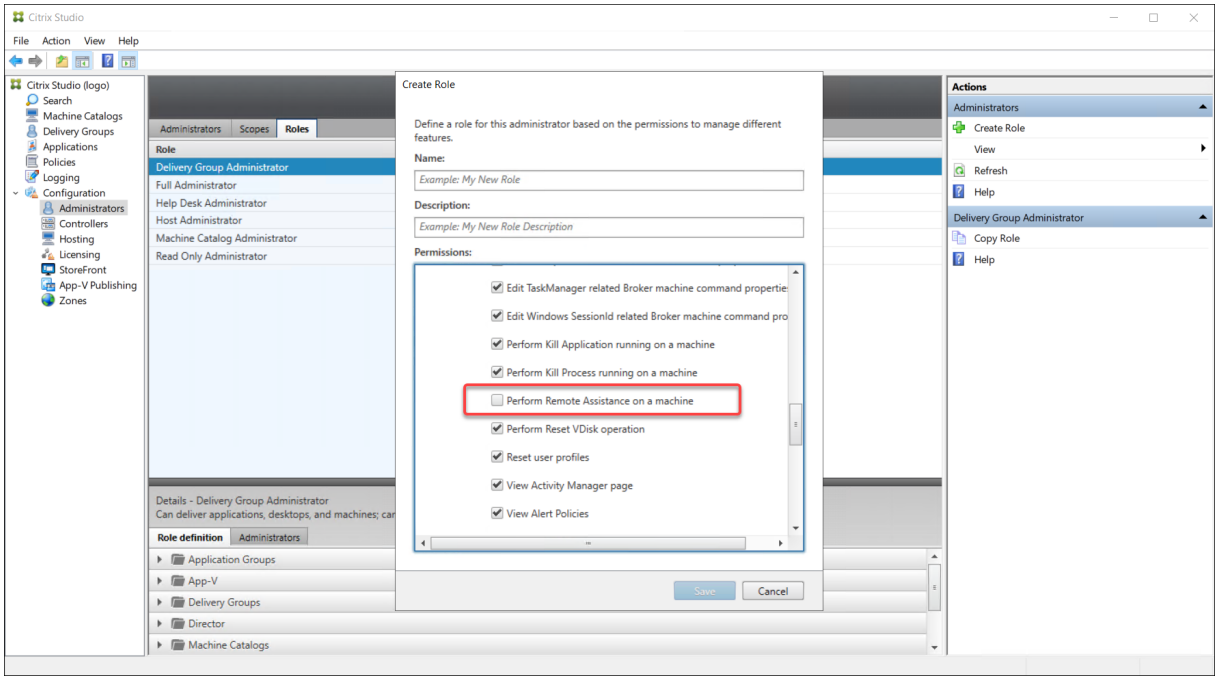

In alternativa, è possibile creare un ruolo personalizzato copiando un ruolo esistente e includendo autorizzazioni aggiuntive per viste diverse. Ad esempio, è possibile copiare il ruolo Help Desk (Helpdesk) e includere le autorizzazioni per visualizzare le pagine Dashboard o Filters (Filtri).

Selezionare le autorizzazioni di Director per il ruolo personalizzato, che includono:

- Perform Kill Application running on a machine (Forza l'interruzione di un'applicazione in esecuzione su una macchina)
- Perform Kill Process running on a machine (Forza l'interruzione di un processo in esecuzione su una macchina)
- Perform Remote Assistance on a machine (Esegui l'assistenza remota su una macchina)
- Reset user profiles (Reimposta i profili utente)
- View Client Details page (Visualizza pagina Dettagli client)
- View Dashboard page (Visualizza pagina Dashboard)
- View Filters page (Visualizza pagina Filtri)
- View Machine Details page (Visualizza pagina Dettagli macchina)
- Pagina View Trends (Visualizza tendenze)
- View User Details page (Visualizza pagina Dettagli utente)

In questo esempio, l'autorizzazione Shadowing (Perform Remote Assistance on a machine) (Shadowing [Esegui assistenza remota su una macchina]) è disabilitata.




Un'autorizzazione può avere dipendenze da altre autorizzazioni per diventare applicabile all'interfaccia utente. Ad esempio, la selezione dell'autorizzazione **Perform Kill Application running on a machine** (Forza l'interruzione di un'applicazione in esecuzione su una macchina) abilita la funzionalità **End Application** (Termina applicazione) solo nei pannelli per i quali il ruolo dispone dell'autorizzazione. È possibile selezionare le seguenti autorizzazioni per i pannelli:

- View Filters page (Visualizza pagina Filtri)
- View User Details page (Visualizza pagina Dettagli utente)
- View Machine Details page (Visualizza pagina Dettagli macchina)
- View Client Details page (Visualizza pagina Dettagli client)

Inoltre, dall'elenco delle autorizzazioni per gli altri componenti, prendere in considerazione queste autorizzazioni dei gruppi di consegna:

- Enable/disable maintenance mode of a machine using delivery group membership (Abilita/disabilita la modalità di manutenzione di una macchina utilizzando l'appartenenza al gruppo di consegna).
- Perform power operations on Windows Desktop machines using delivery group membership (Esegui operazioni di gestione dell'alimentazione su macchine desktop Windows utilizzando l'appartenenza al gruppo di consegna).
- Perform session management on machines using delivery group membership (Esegui la gestione delle sessioni sulle macchine utilizzando l'appartenenza al gruppo di consegna).

# Distribuzione sicura di Director

January 7, 2024

Questo articolo evidenzia le aree che potrebbero avere un impatto sulla sicurezza del sistema durante la distribuzione e la configurazione di Director.

## Configurare Microsoft Internet Information Services (IIS)

È possibile configurare Director con una configurazione IIS limitata.

### Limiti di riciclaggio del pool di applicazioni

È possibile impostare i seguenti limiti di riciclaggio del pool di applicazioni:

- Limite di memoria virtuale: 4.294.967.295
- Limite di memoria privata: la dimensione della memoria fisica del server StoreFront
- Limite richieste: 4.000.000.000

### Estensioni dei nomi file

È possibile non consentire le estensioni dei nomi di file non elencate.

Director richiede queste estensioni dei nomi di file in Request Filtering (Richiedi filtraggio):

- .aspx
- .css
- .html
- .js
- .png
- .svc
- .png
- .json
- .woff
- .woff2
- .ttf

Director richiede i seguenti verbi HTTP in Request Filtering (Richiedi filtraggio). È possibile non consentire i verbi non elencati.

- GET

- POST
- HEAD

Director non richiede:

- Filtri ISAPI
- Estensioni ISAPI
- Programmi CGI
- Programmi FastCGI

> **Importante:**
>
> - Director richiede Full Trust (Attendibilità totale). Non impostare il livello globale di attendibilità di .NET su High (Alto) o su un valore inferiore.
> - Director mantiene un pool di applicazioni separato. Per modificare le impostazioni di Director, selezionare il sito di Director e modificarlo.

### Configurare i diritti utente

Quando Director è installato, ai relativi pool di applicazioni viene concesso quanto segue:

- Diritto di accesso **Log on as a service** (Accedi come servizio)
- Privilegi **Adjust memory quotas for a process** (Regola le quote di memoria per un processo), **Generate security audits** (Genera audit di sicurezza) e **Replace a process level token** (Sostituisci un token a livello di processo)

I diritti e i privilegi menzionati sono normali comportamenti di installazione quando vengono creati pool di applicazioni.

Non è necessario modificare questi diritti utente. Questi privilegi non vengono utilizzati da Director e vengono automaticamente disabilitati.

### Comunicazioni di Director

In un ambiente di produzione, utilizzare i protocolli IPSec (Internet Protocol Security) o HTTPS per proteggere i dati che vengono trasferiti tra Director e i server.

IPSec è un insieme di estensioni standard del protocollo Internet che fornisce comunicazioni autenticate e crittografate con integrità dei dati e protezione della riproduzione. Poiché IPSec è un insieme di protocolli a livello di rete, i protocolli di livello superiore possono utilizzarlo senza modifiche. HTTPS utilizza i protocolli TLS (Transport Layer Security) per fornire una crittografia avanzata dei dati.

> **Nota:**
>
> - Citrix consiglia vivamente di limitare l'accesso alla console di Director all'interno della rete intranet.
> - Citrix consiglia vivamente di non abilitare connessioni non protette a Director in un ambiente di produzione.
> - Le comunicazioni sicure da Director richiedono una configurazione separata per ciascuna connessione.
> - Il protocollo SSL non è consigliato. Utilizzare invece il protocollo TLS, che è più sicuro.
> - Proteggere le comunicazioni con Citrix ADC utilizzando TLS, non IPSec.

Per proteggere le comunicazioni tra i server di Director e Citrix Virtual Apps and Desktops (per il monitoraggio e i report), vedere Sicurezza dell'accesso ai dati.

Per proteggere le comunicazioni tra Director e Citrix ADC (per Citrix Insight), vedere Configurare l'analisi di rete.

Per proteggere le comunicazioni tra Director e il server delle licenze, vedere Proteggere la console di amministrazione delle licenze.

### Separazione della sicurezza di Director

È possibile distribuire qualsiasi applicazione Web nello stesso dominio Web (nome di dominio e porta) di Director. Tuttavia, qualsiasi rischio per la sicurezza in tali applicazioni Web può potenzialmente ridurre la sicurezza della distribuzione di Director. Laddove è richiesto un maggiore grado di separazione della sicurezza, Citrix consiglia di distribuire Director in un dominio Web separato.

## Configurazione di siti locali con Citrix Analytics for Performance

April 3, 2024

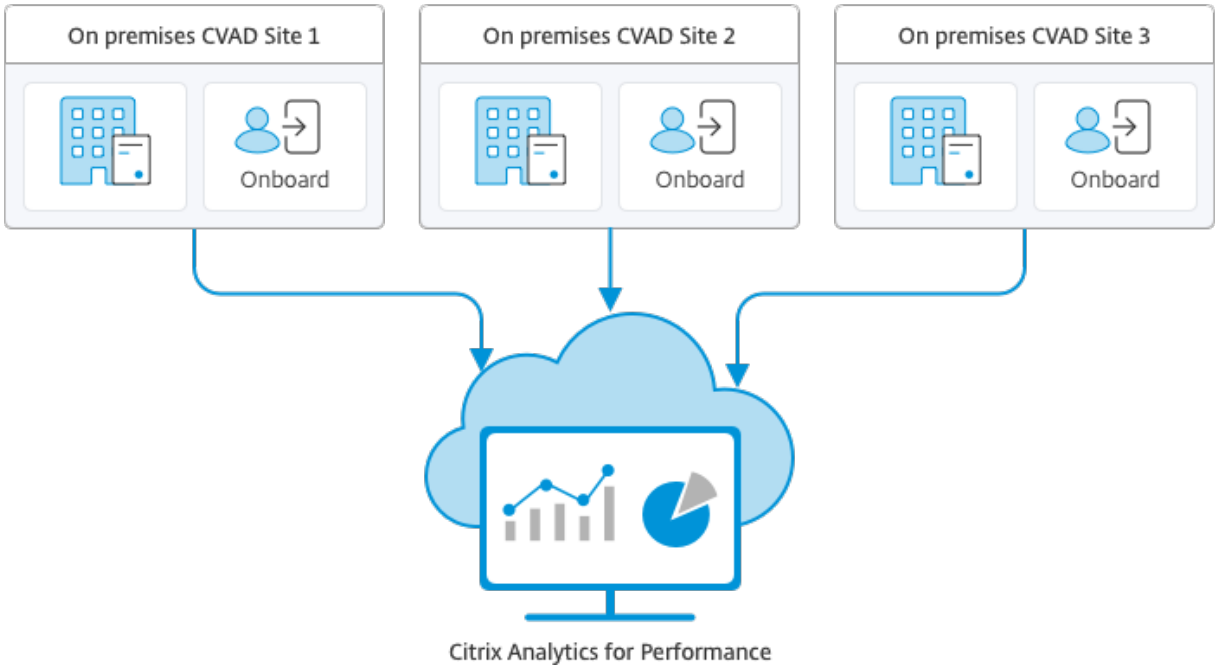
Citrix Analytics for Performance (Performance Analytics) è la soluzione completa di monitoraggio delle prestazioni del servizio cloud Citrix Analytics. Performance Analytics fornisce informazioni approfondite e analisi avanzate basate sulle metriche delle prestazioni. Performance Analytics aiuta a monitorare e visualizzare l'utilizzo e le metriche delle prestazioni di uno o più siti Citrix Virtual Apps and Desktops dell'organizzazione.

Per ulteriori informazioni su Performance Analytics, vedere l'articolo su Performance Analytics.

È possibile inviare dati sulle prestazioni dal sito a Citrix Analytics for Performance in Citrix Cloud per sfruttare le funzionalità avanzate di analisi delle prestazioni. Per visualizzare e utilizzare Performance

Analytics, è necessario innanzitutto configurare i siti locali con Citrix Analytics for Performance dalla scheda **Analytics** (Analisi) in **Director**.




Performance Analytics accede ai dati in modo sicuro e nessun dato viene trasferito da Citrix Cloud all'ambiente locale.

### Prerequisiti

Per configurare Citrix Analytics for Performance da Director, non è necessario installare nuovi componenti. Assicurarsi che siano soddisfatti i seguenti requisiti:

- La versione di Delivery Controller e Director sia la 1912 CU2 o successiva. Per ulteriori informazioni, vedere Matrice di compatibilità delle funzionalità.

> **Nota:**
>
> - La configurazione del sito locale con Citrix Analytics for Performance di Director potrebbe non riuscire se il Delivery Controller esegue una versione di Microsoft .NET Framework precedente alla 4.8. Come soluzione alternativa, aggiornare .NET Framework del Delivery Controller alla versione 4.8. LCM-9255.
> - Quando si configura un sito locale che esegue Citrix Virtual Apps and Desktops versione 2012 con Citrix Analytics for Performance di Director, la configurazione potrebbe riportare un errore dopo un paio d'ore o dopo il riavvio di Citrix Monitor Service nel Delivery Controller. In questo caso, la scheda Analytics indica lo stato Not Connected. Come soluzione alternativa, creare una cartella di crittografia nel Registro di sistema in Delivery Controller,

> Posizione: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor, Folder Name: Encryption. Verificare che l'account CitrixMonitor disponga dell'accesso di controllo completo nella cartella Encryption. Riavviare il servizio Citrix Monitor.DIR-14324.

- L'accesso alla scheda **Analytics** (Analisi) per eseguire questa configurazione è disponibile solo per gli amministratori completi.
- Per consentire a Performance Analytics di accedere alle metriche delle prestazioni, l'accesso a Internet in uscita è disponibile su tutti i Delivery Controller e sulle macchine su cui è installato Director. In particolare, assicurare l'accessibilità ai seguenti URL:
  - Registrazione della chiave Citrix: `https://*.citrixnetworkapi.net/`
  - Citrix Cloud: `https://*.citrixworkspacesapi.net/`
  - Citrix Analytics: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/`

    Nel caso in cui i Delivery Controller e le macchine Director si trovino all'interno di una intranet e l'accesso a Internet in uscita sia disponibile tramite un server proxy, assicurare quanto segue:
- Il server proxy deve consentire l'elenco precedente di URL.
- Aggiungere la configurazione di cui sotto nei file web.config e citrix.monitor.exe.config di Director. Accertarsi di aver aggiunto questa configurazione all'interno dei tag di **configurazione**:

```
<system.net>
    <defaultProxy>
        <proxy  usesystemdefault = "false"  proxyaddress = "http
            ://<your_proxyserver_address>:80" bypassonlocal = "
            true"  />
    </defaultProxy>
</system.net>
```

  - Il file web.config di Director si trova in `C:\inetpub\wwwroot\Director\web.config` sulla macchina in cui è installato Director.
  - Il file citrix.monitor.exe.config si trova in `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` sulla macchina in cui è installato il Delivery Controller.

  Questa impostazione è fornita da Microsoft su IIS. Per ulteriori informazioni, vedere `https://docs.microsoft.com/en-us/dotnet/framework/network-programming/proxy-configuration`.

  Il campo **defaultproxy** nel file di configurazione controlla l'accesso in uscita di Director e del servizio di monitoraggio. La configurazione e la comunicazione con Performance Analytics richiedono che il campo **defaultproxy** sia impostato su **true**. È possibile che i criteri in uso impostino questo campo su false. In questo caso, è necessario impostare manualmente il

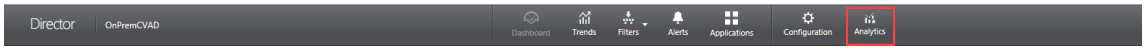
campo su true. Effettuare un backup dei file di configurazione prima di apportare le modifiche. Riavviare il servizio di monitoraggio sul Delivery Controller perché le modifiche abbiano effetto.

- Si ha diritto a utilizzare il servizio Citrix Cloud per Citrix Analytics for Performance.
- L'account Citrix Cloud è un account amministratore con diritti all'esperienza di registrazione del prodotto. Per ulteriori informazioni sulle autorizzazioni di amministratore, vedere Modificare le autorizzazioni di amministratore.

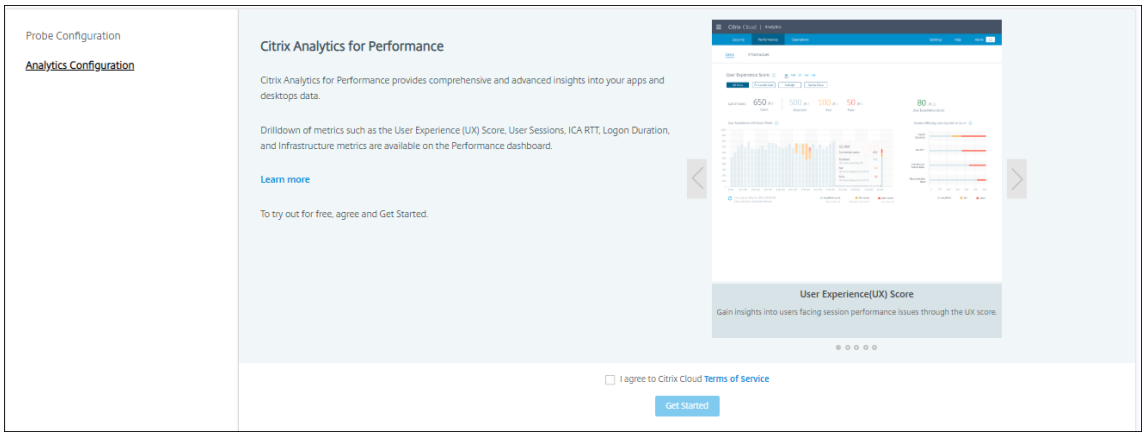
## Passaggi di configurazione

Dopo aver verificato i prerequisiti, procedere come segue:

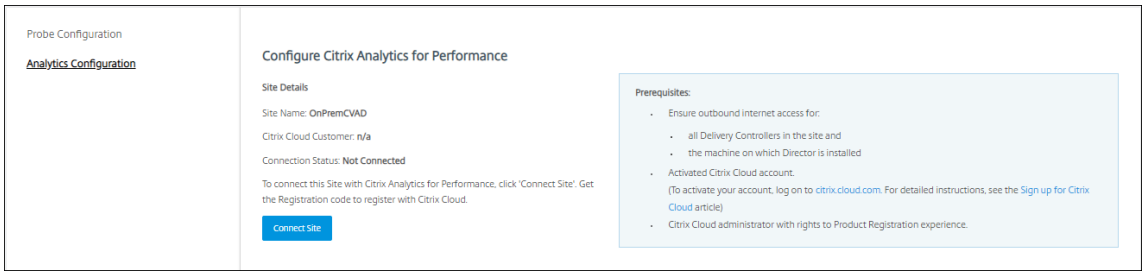
1. Accedere a Director come amministratore completo e selezionare il sito che si desidera configurare con Performance Analytics.
2. Fare clic sulla scheda **Analytics** (Analisi). Viene visualizzata la pagina **Configuration** (Configurazione).




3. Esaminare i passaggi, selezionare i termini di servizio e fare clic su **Get Started** (Inizia).

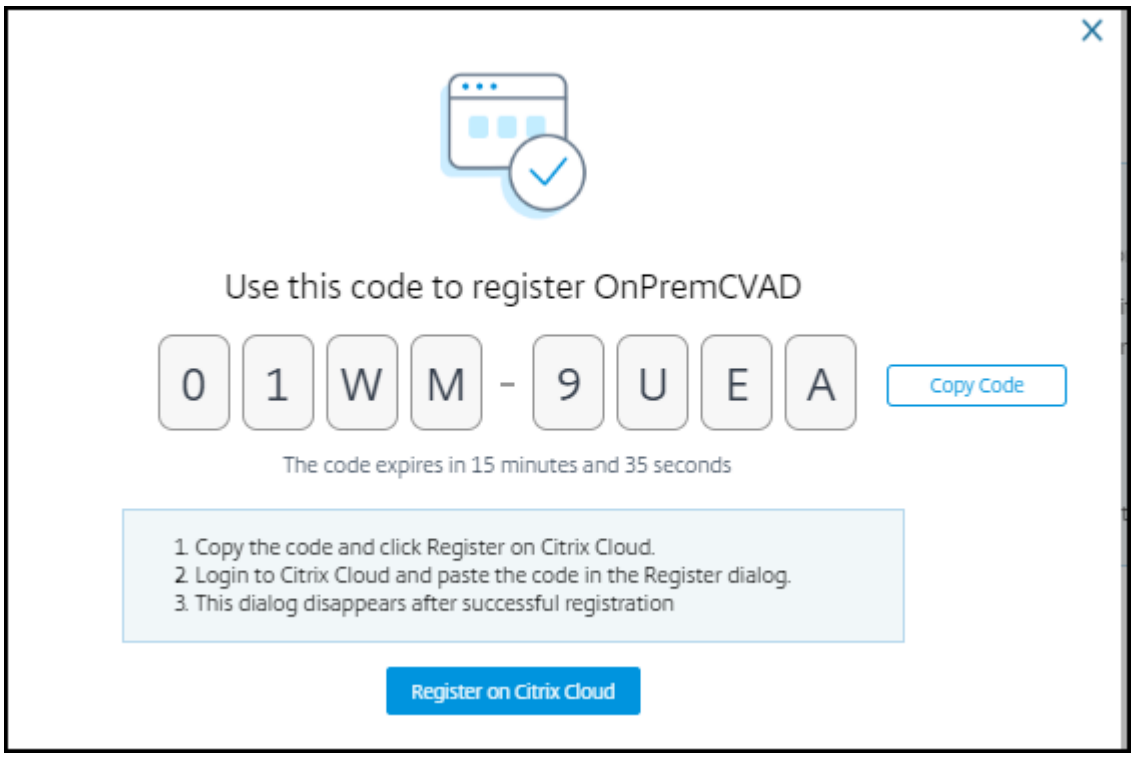



4. Rivedere i prerequisiti e assicurarsi che siano soddisfatti. Controllare i dettagli del sito.
5. Fare clic su **Connect Site** (Connetti sito) per avviare il processo di configurazione.



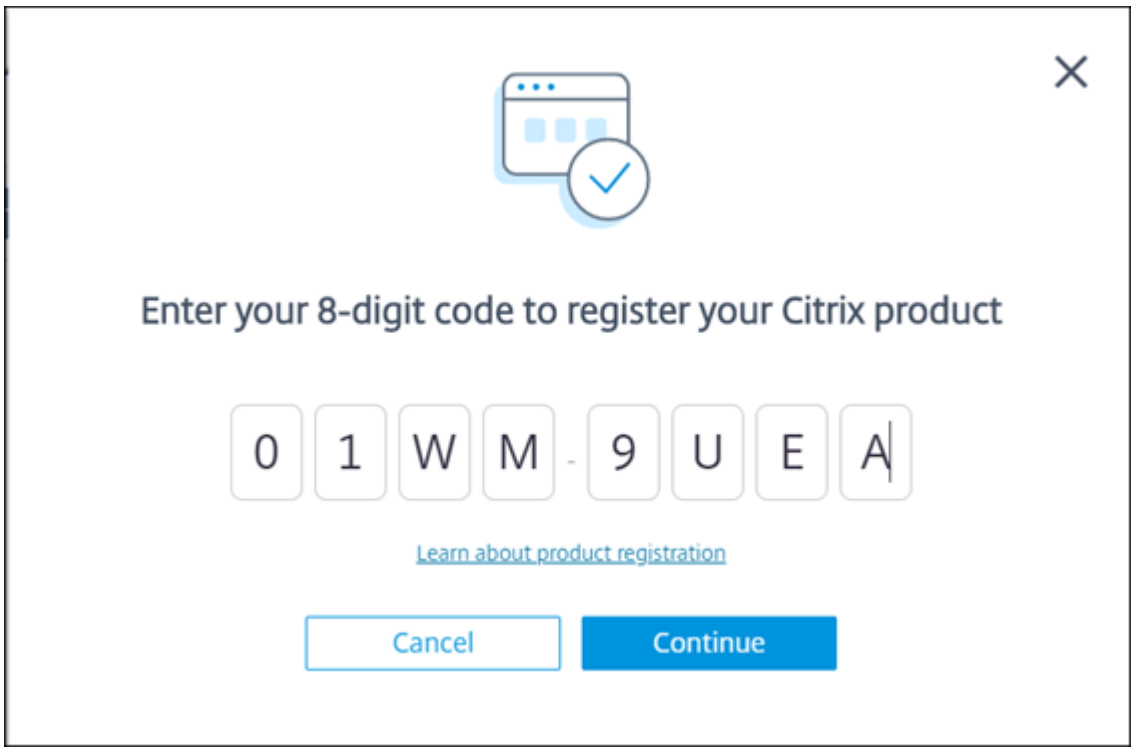

 

6. Viene generato un codice di registrazione univoco a 8 cifre da utilizzare per registrare questo sito con Citrix Cloud.

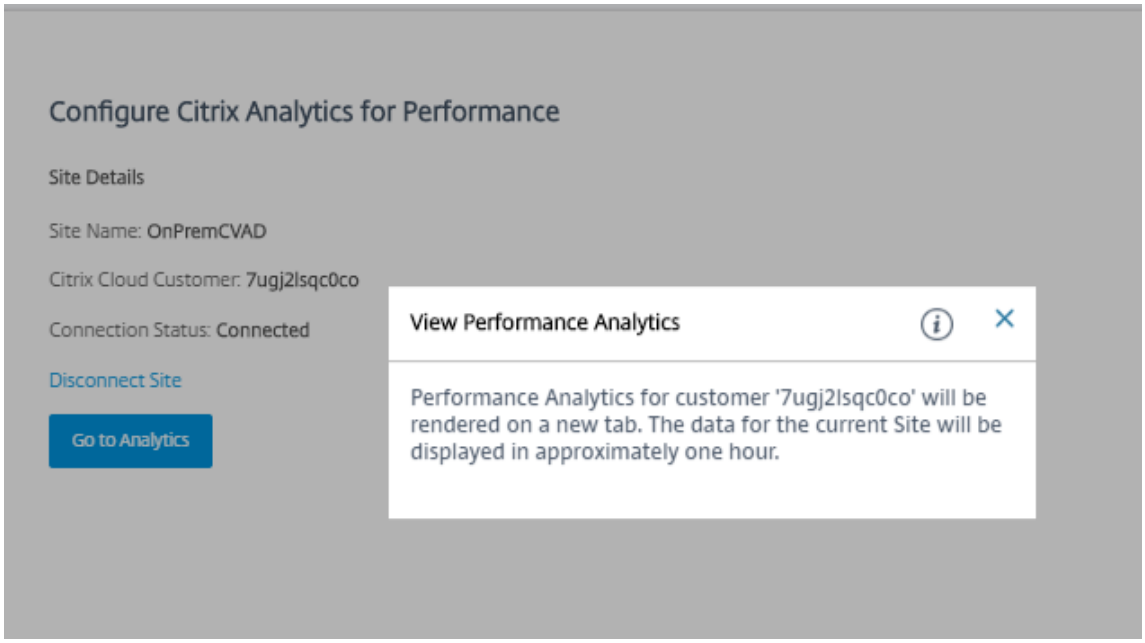



7. Fare clic su **Copy Code** (Copia codice) per copiare il codice e quindi fare clic su **Register on Citrix Cloud** (Registra su Citrix Cloud).
8. Si verrà reindirizzati all'URL di registrazione in Citrix Cloud. Accedere con le credenziali Citrix Cloud e selezionare il cliente.
9. Incollare il codice di registrazione copiato nella pagina Product Registrations (Registrazioni prodotto) in Citrix Cloud. Fare clic su **Continua** per effettuare la registrazione. Controllare i dettagli della registrazione e fare clic su **Register** (Registra).

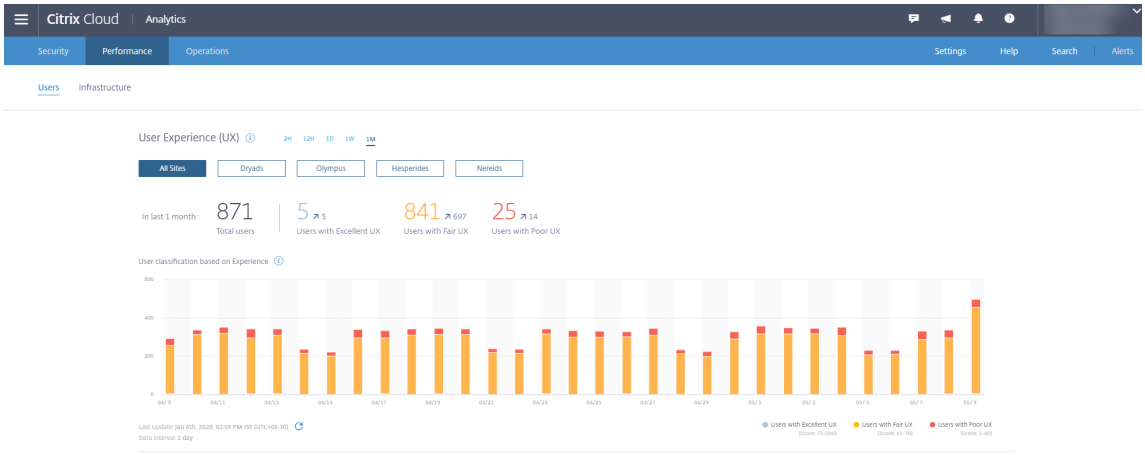



10. Il sito locale si registra con Citrix Cloud. Ora, da **Director**, fare clic su **Go to Analytics** (Vai ad Analytics) nella scheda **Analytics** (Analisi).




11. Performance Analytics viene aperto in una nuova scheda del browser.




Se la sessione Citrix Cloud è scaduta, si potrebbe essere reindirizzati alla pagina di accesso Citrix.com o My Citrix account (Il mio account Citrix).

12. Per registrare più siti con Performance Analytics, ripetere i passaggi di configurazione precedenti per ciascun sito da Director. Le metriche per tutti i siti configurati vengono visualizzate nella dashboard di Performance Analytics.

    Nel caso in cui sia in esecuzione più di un'istanza di Director per sito, eseguire la configurazione da una qualsiasi istanza di Director. Tutte le altre istanze di Director collegate al sito vengono aggiornate al successivo aggiornamento dopo il processo di configurazione.

13. Per disconnettere il sito da Citrix Cloud, fare clic su **Disconnetti sito**. Questa opzione elimina la configurazione esistente.

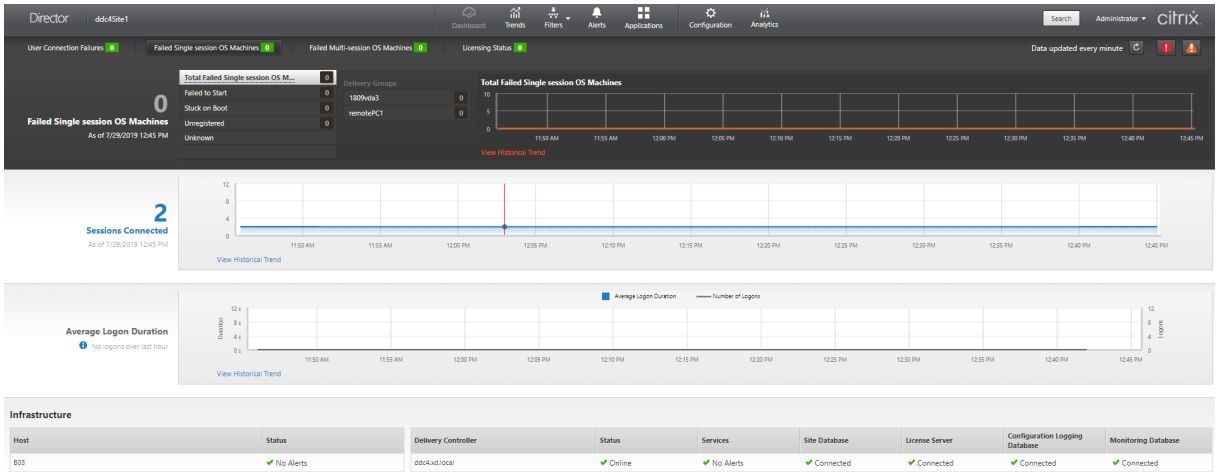
    > **Note:**
    >
    > La prima volta che si configura un sito, gli eventi del sito potrebbero richiedere tempo (circa un'ora) per essere elaborati, causando un ritardo nella visualizzazione delle metriche nella dashboard di Performance Analytics. Successivamente, gli eventi si aggiornano a intervalli regolari.
    >
    > Dopo la disconnessione, la trasmissione dei dati dal vecchio account continua per qualche tempo fino a quando non vengono trasmessi gli eventi del nuovo account. Per circa un'ora dopo l'interruzione della trasmissione dei dati, le analisi relative al vecchio account rimangono visualizzate nella dashboard di Performance Analytics.
    >
    > Alla scadenza del diritto di utilizzo del servizio Citrix Analytics, è necessario fino a un giorno per interrompere l'invio delle metriche del sito a Performance Analytics.

# Analisi del sito

January 7, 2024

Con l'autorizzazione di amministratore completa, quando si apre Director la dashboard fornisce una posizione centralizzata per monitorare lo stato e l'utilizzo di un sito.




Se al momento non ci sono errori e non si sono verificati errori negli ultimi 60 minuti, i pannelli rimangono compressi. In caso di errori, viene visualizzato automaticamente il pannello dell'errore specifico.

> **Nota:**
>
> A seconda della licenza dell'organizzazione e dei privilegi di amministratore, alcune opzioni o funzionalità potrebbero non essere disponibili.

## Pannelli della dashboard di Director

### User Connection Failures (Errori di connessione utente)

Errori di connessione negli ultimi 60 minuti. Fare clic sulle categorie accanto al numero totale per visualizzare le metriche per quel tipo di errore. Nella tabella adiacente, tale numero viene suddiviso per gruppi di consegna. Gli errori di connessione includono errori causati dal raggiungimento dei limiti dell'applicazione. Per ulteriori informazioni sui limiti delle applicazioni, vedere Applicazioni.

**Failed Single-session OS Machines (Macchine con sistema operativo a sessione singola che presentano errori) o Failed Multi-session OS Machines (Macchine con sistema operativo multisessione che presentano errori)**

Errori totali negli ultimi 60 minuti suddivisi per gruppi di consegna. Errori suddivisi per tipo, tra cui avvio non riuscito, blocco all'avvio e mancata registrazione. Per le macchine con sistema operativo multisessione, gli errori includono anche le macchine che raggiungono il carico massimo.

**Licensing Status (Stato della licenza)**

Gli avvisi del Licence Server visualizzano gli avvisi inviati dal License Server e le azioni necessarie per risolverli. È richiesto License Server versione 11.12.1 o successiva. Gli avvisi dei Delivery Controller visualizzano i dettagli dello stato della licenza rilevato dal controller e vengono inviati dal controller. È necessario un controller per XenApp 7.6 o XenDesktop 7.6 o versioni successive. È possibile impostare la soglia per gli avvisi in Studio. Lo stato della licenza visualizzato in **Delivery Controllers** (Delivery Controller) > **Details** (Dettagli) > **Product Editions** (Edizioni prodotto) > **PLT** indica **Premium** e non **Platinum**.

**Grace State (Stato di tolleranza)**

Director mostra uno dei seguenti stati di tolleranza. Queste informazioni vengono recuperate dal Delivery Controller.

1. **Not Active** (Non attivo): non è presente alcun periodo di tolleranza. Si applicano i normali limiti della licenza.
2. **Out of Box Grace** (Tolleranza iniziale): 10 connessioni per i primi 30 giorni dopo una nuova installazione quando si punta a un server delle licenze senza licenze.
3. **Supplemental Grace** (Tolleranza supplementare): quando tutte le licenze vengono consumate, è previsto un periodo di tolleranza di 15 giorni per la continuità aziendale fino all'aggiunta di nuove licenze o alla riduzione del consumo. Sono consentite connessioni illimitate durante il periodo di tolleranza supplementare. Gli utenti non sono interessati. Gli avvisi mostrati in Director non possono essere ignorati fino alla scadenza o alla reimpostazione del periodo di tolleranza supplementare.
4. **Emergency Grace** (Tolleranza di emergenza): entra in vigore quando il server delle licenze è irraggiungibile o le informazioni sulla licenza non possono essere recuperate durante il brokering di una connessione. La tolleranza di emergenza è valida per 30 giorni. Gli utenti non sono interessati. Gli errori mostrati in Director non possono essere ignorati finché il server delle licenze non è raggiungibile.

5. **Grace Expired** (Tolleranza scaduta): la tolleranza di emergenza o il periodo di tolleranza supplementare è scaduto.

Per ulteriori informazioni, vedere Scoperto della licenza e Periodo di tolleranza supplementare.

#### Sessions Connected (Sessioni connesse)

Sessioni connesse per tutti i gruppi di consegna negli ultimi 60 minuti.

#### Average Logon Duration (Durata media dell'accesso)

Dati di accesso per gli ultimi 60 minuti. Il numero elevato a sinistra è la durata media dell'accesso nel corso dell'ora. I dati di accesso per VDA precedenti a XenDesktop 7.0 non sono inclusi in questa media. Per ulteriori informazioni, vedere Diagnosticare i problemi di accesso degli utenti.

#### Infrastructure (Infrastruttura)

Elenca l'infrastruttura del sito: host e controller. Per l'infrastruttura di Citrix Hypervisor o VMware, è possibile visualizzare gli avvisi sulle prestazioni. Ad esempio, è possibile configurare XenCenter per generare avvisi sulle prestazioni quando CPU, I/O di rete o utilizzo di I/O su disco superano una soglia specificata su un server gestito o una macchina virtuale. Per impostazione predefinita, l'intervallo di ripetizione dell'avviso è di 60 minuti, ma è possibile configurarlo. Per i dettagli, vedere la sezione XenCenter Performance Alerts (Avvisi sulle prestazioni di XenCenter) nella documentazione del prodotto Citrix Hypervisor.

> **Nota:**
>
> Se non viene visualizzata alcuna icona per una determinata metrica, questo indica che tale metrica non è supportata dal tipo di host in uso. Ad esempio, non sono disponibili informazioni sullo stato per gli host System Center Virtual Machine Manager (SCVMM), AWS e CloudStack.

Continuare la risoluzione dei problemi utilizzando queste opzioni (che sono documentate nelle sezioni seguenti):

- Controllare l'alimentazione della macchina dell'utente
- Prevent connections to machines (Impedisci le connessioni alle macchine)

### Monitorare le sessioni

Se una sessione viene disconnessa, è ancora attiva e le relative applicazioni continuano a essere eseguite, ma il dispositivo utente non comunica più con il server.

| Azione | Descrizione |
| --- | --- |
| Visualizzare la macchina o la sessione di un utente attualmente connesso | Dalle viste Activity Manager (Gestione attività) e User Details (Dettagli utente), visualizzare la macchina o la sessione attualmente connessa dell'utente e un elenco di tutte le macchine e le sessioni a cui l'utente ha accesso. Per accedere a questo elenco, fare clic sull'icona del commutatore di sessione nella barra del titolo dell'utente. Per ulteriori informazioni, vedere Ripristinare le sessioni. |
| Visualizzare il numero totale di sessioni connesse in tutti i gruppi di consegna | Dalla dashboard, nel riquadro **Sessions Connected** (Sessioni connesse), visualizzare il numero totale di sessioni connesse in tutti i gruppi di consegna negli ultimi 60 minuti. Quindi, fare clic sul numero totale elevato, che apre la vista Filters (Filtri), in cui è possibile visualizzare i dati della sessione sotto forma di grafici in base ai gruppi di consegna e agli intervalli selezionati e all'utilizzo nei gruppi di consegna. |
| Terminare le sessioni inattive | La vista Sessions Filters (Filtri sessioni) visualizza i dati relativi a tutte le sessioni attive. Filtrare le sessioni in base all'utente associato, al gruppo di consegna, allo stato della sessione e al tempo di inattività superiore a un periodo di soglia. Dall'elenco filtrato, selezionare le sessioni da scollegare o disconnettere. Per ulteriori informazioni, vedere Risolvere i problemi relativi alle applicazioni. |
| Visualizzare i dati per un periodo di tempo più lungo | Nella vista Trends (Tendenze), selezionare la scheda **Sessions** (Sessioni) per eseguire il drill down dei dati di utilizzo più specifici per le sessioni connesse e disconnesse per un periodo di tempo più lungo (ovvero i totali delle sessioni precedenti agli ultimi 60 minuti). Per visualizzare queste informazioni, fare clic su **View historical trends** (Visualizza tendenze storiche). |

> **Nota:**
>
> Se il dispositivo utente esegue un Virtual Delivery Agent (VDA) legacy, ad esempio un VDA precedente alla versione 7 o un VDA Linux, Director non è in grado di visualizzare informazioni complete sulla sessione. Visualizza invece un messaggio che indica che le informazioni non sono disponibili.

**Limitazione delle regole di assegnazione del desktop** Web Studio consente l'assegnazione di più regole di assegnazione del desktop (DAR) per utenti o gruppi di utenti diversi a un singolo VDA nel gruppo di consegna. StoreFront visualizza il desktop assegnato con il **Display Name** (Nome visualizzato) corrispondente in base al DAR dell'utente che ha effettuato l'accesso. Tuttavia, Director non supporta le DAR e visualizza il desktop assegnato utilizzando il nome del gruppo di consegna indipendentemente dall'utente connesso. Di conseguenza, non è possibile mappare un desktop specifico a una macchina in Director.

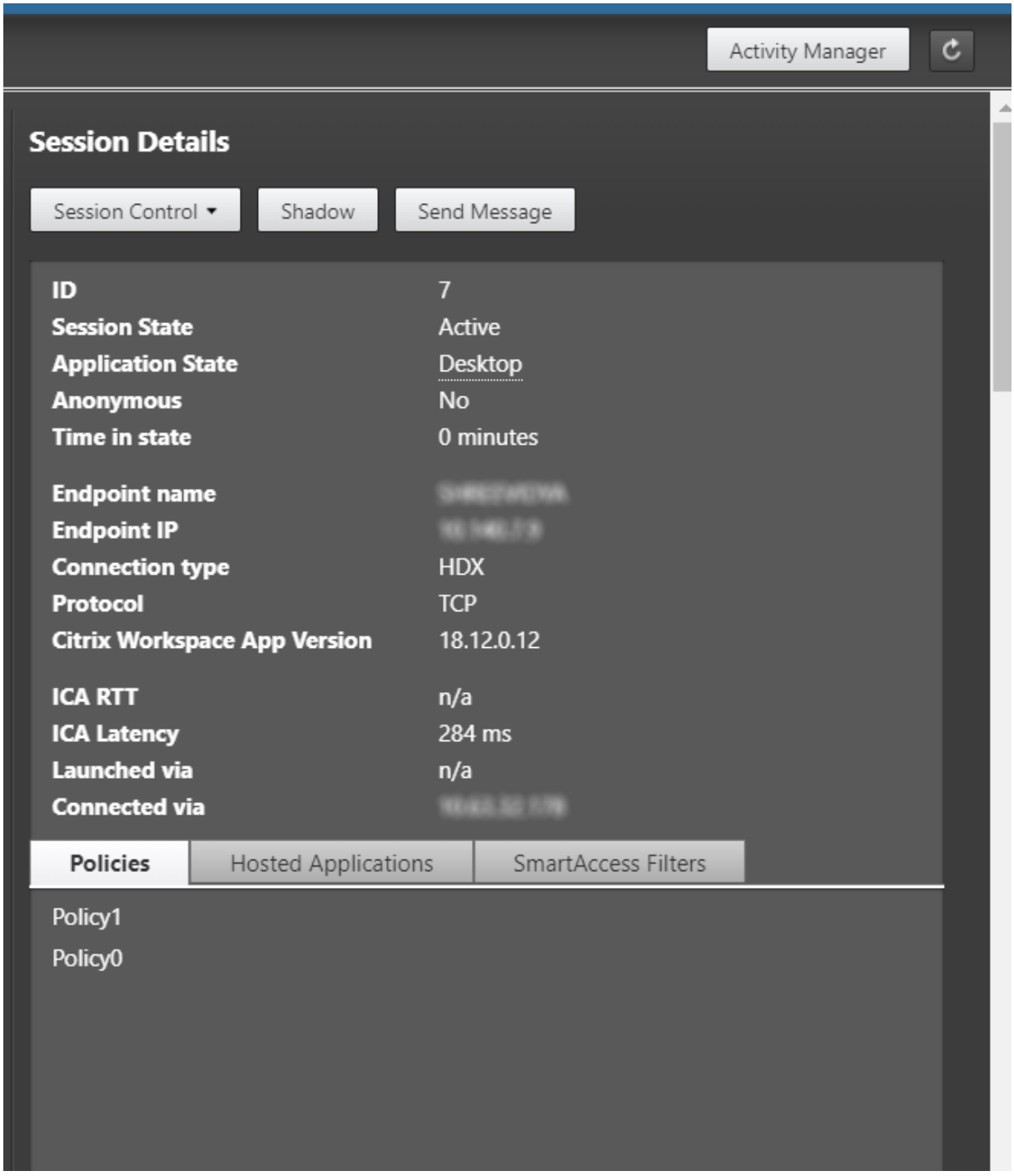
È possibile mappare il desktop assegnato visualizzato in StoreFront al nome del gruppo di consegna visualizzato in Director utilizzando il seguente comando PowerShell:

```
Get-BrokerDesktopGroup | Where-Object { $_.Uid -eq (Get-BrokerAssignmentPolicyRule).DesktopGroupUid } | Where-Object { $_.PublishedName -eq "" } | Select-Object -Property Name, Uid
```

### Protocollo di trasporto della sessione

Visualizzare il protocollo di trasporto in uso per il tipo di connessione HDX per la sessione corrente nel pannello **Session Details** (Dettagli sessione). Queste informazioni sono disponibili per le sessioni avviate sui VDA versione 7.13 o successiva.




- Per il tipo di connessione **HDX**:
  - Il protocollo viene visualizzato come **UDP** se viene utilizzato EDT per la connessione HDX.
  - Il protocollo viene visualizzato come **TCP** se viene utilizzato TCP per la connessione HDX.
- Per il tipo di connessione **RDP**, il protocollo viene visualizzato come **n/a** (n/d).

Quando è configurato il trasporto adattivo, il protocollo di trasporto della sessione passa dinamica-

mente da EDT (su UDP) a TCP e viceversa, in base alle condizioni di rete. Se la sessione HDX non può essere stabilita utilizzando EDT, ritorna al protocollo TCP.

Per ulteriori informazioni sulla configurazione del trasporto adattivo, vedere Trasporto adattivo.

## Esportare i report

È possibile esportare i dati delle tendenze per generare rapporti regolari di utilizzo e gestione della capacità. L'esportazione supporta i formati di report PDF, Excel e CSV. I report in formato PDF ed Excel contengono tendenze rappresentate come grafici e tabelle. I report in formato CSV contengono dati tabulari che possono essere elaborati per generare viste o possono essere archiviati.

Per esportare un report:

1. Andare alla scheda **Trends** (Tendenze).
2. Impostare i criteri del filtro e il periodo di tempo e fare clic su **Apply** (Applica). Il grafico e la tabella delle tendenze vengono popolati con dati.
3. Fare clic su **Export** (Esporta) e immettere il nome e il formato del report.

Director genera il report in base ai criteri del filtro selezionati. Se si modificano i criteri del filtro, fare clic su **Apply** (Applica) prima di fare clic su **Export** (Esporta).

> **Nota:**
>
> L'esportazione di una grande quantità di dati provoca un aumento significativo del consumo di memoria e CPU sul server di Director, sul Delivery Controller e sui server SQL. Il numero supportato di operazioni di esportazione simultanee e la quantità di dati che è possibile esportare sono impostati su limiti predefiniti per ottenere prestazioni ottimali per l'esportazione.

### Limiti di esportazione supportati

I report PDF ed Excel esportati contengono grafici completi per i criteri del filtro selezionati. Tuttavia, i dati tabulari in tutti i formati di report vengono troncati oltre i limiti predefiniti per il numero di righe o record nella tabella. Il numero predefinito di record supportati è definito in base al formato del report.

È possibile modificare il limite predefinito configurando le impostazioni dell'applicazione Director in Internet Information Services (IIS).

| Formato del report | Numero predefinito di record supportati | Campi nelle impostazioni dell'applicazione Director | Numero massimo di record supportati |
|---|---|---|---|
| PDF | 500 | UI.ExportPdfDrilldownLimit | 5000 |
| Excel | 100.000 | UI.ExportExcelDrilldownLimit | 100.000 |
| CSV | 100.000 (10.000.000 nella scheda **Sessions** [Sessioni]) | UI.ExportCsvDrilldownLimit | 10,000 |

Per modificare il limite del numero di record che è possibile esportare:

1. Aprire la console di IIS Manager.
2. Andare al sito Web di Director sotto il sito Web predefinito.
3. Fare doppio clic su **Application Settings** (Impostazioni applicazione).
4. Modificare o aggiungere un'impostazione per i campi UI.ExportPdfDrilldownLimit, UI.ExportExcelDrilldownL o UI.ExportCsvDrilldownLimit, come richiesto.

L'aggiunta di questi valori dei campi in Application Settings (Impostazioni applicazione) sostituisce i valori predefiniti.

> **Avviso:**
>
> L'impostazione di valori dei campi superiori al numero massimo di record supportati può influire sulle prestazioni di esportazione e non è supportata.

#### Gestione degli errori

Questa sezione fornisce informazioni sulla gestione degli errori che potrebbero verificarsi durante l'operazione di esportazione.

- **Director has timed out** (Timeout di Director)

Questo errore può verificarsi a causa di problemi di rete o di utilizzo elevato delle risorse sul server di Director o con il servizio di monitoraggio.

La durata di timeout predefinita è di 100 secondi. Per aumentare la durata del timeout del servizio Director, impostare il valore del **campo Connector.DataServiceContext.Timeout in** Director Application Settings (Impostazioni dell'applicazione Director) in Internet Information Services (IIS):

1. Aprire la console di IIS Manager.
2. Andare al sito Web di Director sotto il sito Web predefinito.

3. Fare doppio clic su **Application Settings** (Impostazioni applicazione).
4. Modificare il valore **Connector.DataServiceContext.Timeout**.

- **Monitor has timed out** (Timeout del monitor)

Questo errore può verificarsi a causa di problemi di rete o di utilizzo elevato delle risorse con il servizio di monitoraggio o sul server SQL.

Per aumentare la durata del timeout del servizio di monitoraggio, eseguire i seguenti comandi PowerShell sul Delivery Controller:

```
asnp Citrix.*
Get-MonitorConfiguration
Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <timeout value>
```

- **Max concurrent Export or Preview operations ongoing** (Limite massimo di operazioni simultanee di esportazione o anteprima in corso)

Director supporta un'istanza di esportazione o anteprima. Se viene visualizzato l'errore **Max concurrent Export or Preview operations ongoing** (Limite massimo di operazioni simultanee di esportazione o anteprima in corso), riprovare la successiva operazione di esportazione in un secondo momento.

È possibile aumentare il numero di operazioni simultanee di esportazione o anteprima, tuttavia ciò può influire sulle prestazioni di Director e non è supportato:

1. Aprire la console di IIS Manager.
2. Andare al sito Web di Director sotto il sito Web predefinito.
3. Fare doppio clic su **Application Settings** (Impostazioni applicazione).
4. Modificare il valore **UI.ConcurrentExportLimit**.

- **Insufficient disk space in Director** (Spazio su disco insufficiente in Director)

Ogni operazione di esportazione richiede un massimo di 2 GB di spazio su disco rigido nella cartella Temp di Windows. Riprovare l'esportazione dopo aver liberato dello spazio o dopo aver aggiunto più spazio su disco rigido sul server di Director.

### Aggiornamenti rapidi per il monitor

Per visualizzare gli aggiornamenti rapidi installati su una specifica macchina VDA (fisica o VM), scegliere la vista **Machine Details** (Dettagli macchina).

### Controllare gli stati di alimentazione della macchina utente

Per controllare lo stato delle macchine selezionate in Director, utilizzare le opzioni Power Control (Controllo dell'alimentazione). Queste opzioni sono disponibili per le macchine con sistema operativo a sessione singola, ma potrebbero non essere disponibili per le macchine con sistema operativo multi-sessione.

> **Nota:**
>
> Questa funzionalità non è disponibile per macchine fisiche o macchine che utilizzano Remote PC Access (Accesso remoto PC).

| Comando | Funzione |
| --- | --- |
| **Restart (Riavvia)** | Esegue un arresto ordinato della VM e tutti i processi in esecuzione vengono arrestati singolarmente prima di riavviare la VM. Ad esempio, selezionare le macchine che appaiono in Director come "Failed to start"(Impossibile eseguire l'avvio) e utilizzare questo comando per riavviarle. |
| **Force Restart (Forza riavvio)** | Riavvia la VM senza prima eseguire alcuna procedura di arresto. Questo comando equivale a scollegare un server fisico dalla corrente, quindi a ricollegarlo e riaccenderlo. |
| **Shut Down (Arresta)** | Esegue un arresto ordinato della VM. Tutti i processi in esecuzione vengono interrotti singolarmente. |
| **Force Shutdown (Imponi arresto)** | Spegne la VM senza prima eseguire alcuna procedura di arresto. Questo comando equivale a scollegare un server fisico dalla corrente. Potrebbe non sempre arrestare tutti i processi in esecuzione e se si spegne una VM in questo modo si rischia di perdere dati. |

| Comando | Funzione |
| --- | --- |
| **Suspend (Sospendi)** | Sospende una VM in esecuzione nello stato corrente e memorizza tale stato in un file nel repository di archiviazione predefinito. Questa opzione consente di spegnere il server host della VM e successivamente, dopo il riavvio, riattivare la VM, riportandola allo stato di esecuzione originale. |
| **Resume (Riprendi)** | Riprende una VM sospesa e ripristina lo stato di esecuzione originale. |
| **Start (Avvia)** | Avvia una VM quando è spenta (chiamato anche avvio a freddo). |

Se le azioni di controllo dell'alimentazione non vanno a buon fine, passare il mouse sopra l'avviso e viene visualizzato un messaggio a comparsa con i dettagli dell'errore.

### Prevent connections to machines (Impedisci le connessioni alle macchine)

Utilizzare la modalità di manutenzione per impedire temporaneamente nuove connessioni mentre l'amministratore appropriato esegue attività di manutenzione sull'immagine.

Quando si abilita la modalità di manutenzione sulle macchine, non sono consentite nuove connessioni fino a quando non viene disabilitata. Se gli utenti sono attualmente connessi, la modalità di manutenzione ha effetto non appena tutti gli utenti vengono disconnessi. Per gli utenti che non si disconnettono, inviare un messaggio che li informa che le macchine verranno spente in un determinato momento e utilizzare i controlli di alimentazione per forzare l'arresto delle macchine.

1. Selezionare la macchina, ad esempio dalla vista User Details (Dettagli utente), o un gruppo di macchine nella vista Filters (Filtri).
2. Selezionare **Maintenance Mode** (Modalità di manutenzione) e attivare l'opzione.

Se un utente tenta di connettersi a un desktop assegnato mentre è in modalità di manutenzione, viene visualizzato un messaggio che indica che il desktop non è disponibile. Non è possibile stabilire nuove connessioni fino a quando non si disabilita la modalità di manutenzione.

### Analisi delle applicazioni

La scheda **Applications** (Applicazioni) visualizza le analisi basate sulle applicazioni in un'unica vista consolidata per facilitare l'analisi e la gestione efficienti delle prestazioni delle applicazioni. È possibile ottenere importanti dettagli approfonditi sulle informazioni sullo stato e sull'utilizzo di tutte le

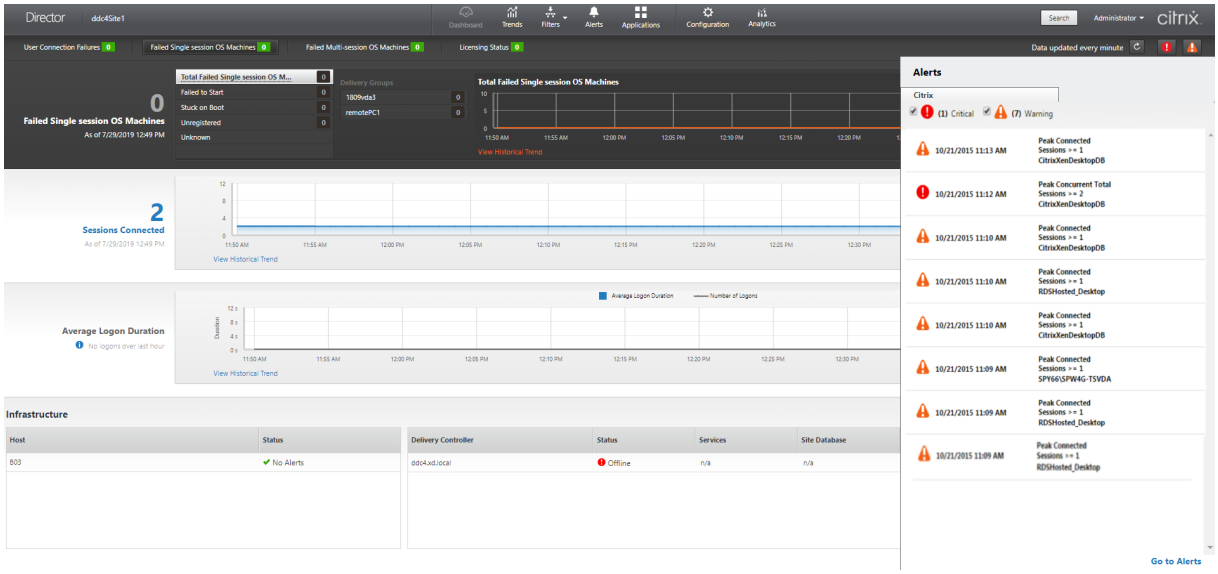
 

applicazioni pubblicate sul sito. Questa scheda mostra metriche come i risultati del probe, il numero di istanze per applicazione e gli errori e i guasti associati alle applicazioni pubblicate. Per ulteriori informazioni, vedere la sezione Analisi delle applicazioni in **Risolvere i problemi relativi alle applicazioni**.

## Avvisi e notifiche

January 10, 2024

Gli avvisi vengono visualizzati in Director nella dashboard e in altre viste di alto livello con simboli di avvertimento e avviso critico. Gli avvisi sono disponibili per i siti con licenza **Premium**. Gli avvisi si aggiornano automaticamente ogni minuto; è inoltre possibile aggiornarli su richiesta.



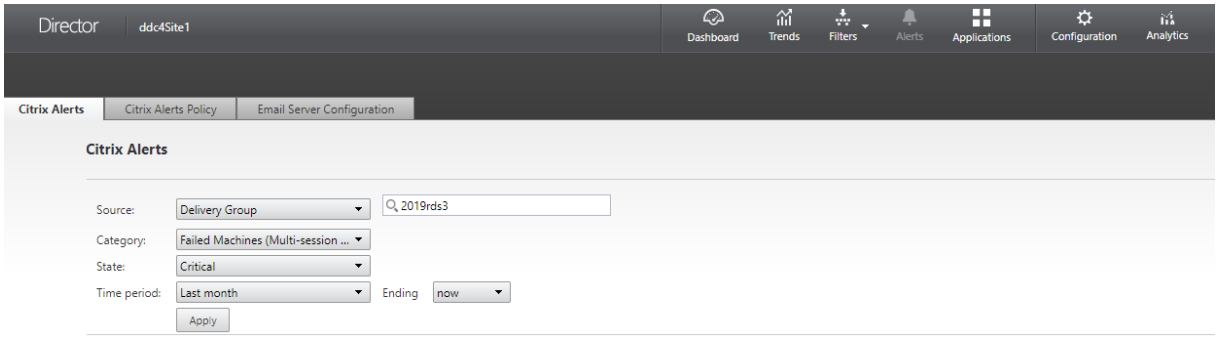

Un avviso di avvertimento (triangolo ambrato) indica che la soglia di avvertimento di una condizione è stata raggiunta o superata.

Un avviso critico (cerchio rosso) indica che la soglia critica di una condizione è stata raggiunta o superata.

È possibile visualizzare informazioni più dettagliate sugli avvisi selezionando un avviso dalla barra laterale, facendo clic sul collegamento **Go to Alerts** (Vai agli avvisi) nella parte inferiore della barra laterale o selezionando **Alerts** (Avvisi) nella parte superiore della pagina di Director.

Nella vista Alerts (Avvisi), è possibile filtrare ed esportare avvisi. Ad esempio, è possibile filtrare le macchine con sistema operativo multisessione che presentano problemi per un gruppo di consegna specifico nell'ultimo mese o tutti gli avvisi per un utente specifico. Per ulteriori informazioni, vedere Esportare i report.




## Avvisi Citrix

Gli avvisi Citrix sono avvisi monitorati in Director che provengono dai componenti Citrix. È possibile configurare gli avvisi Citrix in Director in **Alerts** (Avvisi) > **Citrix Alerts Policy** (Criterio per gli avvisi Citrix). Come parte della configurazione, è possibile impostare notifiche da inviare via e-mail a individui e gruppi quando gli avvisi superano le soglie impostate. Per ulteriori informazioni sulla configurazione di Citrix Alerts, vedere Creare criteri per gli avvisi.

> **Nota:**
>
> Assicurarsi che il firewall, il proxy o Microsoft Exchange Server non blocchino gli avvisi e-mail.

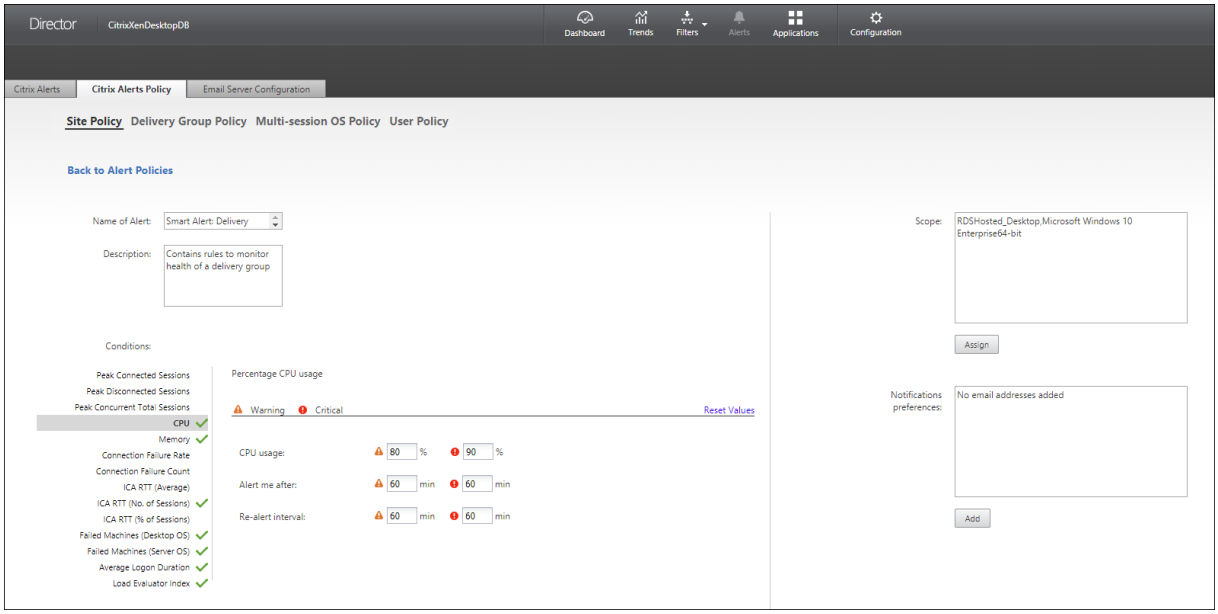
## Criteri intelligenti per gli avvisi

È disponibile un set di criteri incorporati per gli avvisi con valori di soglia predefiniti per i gruppi di consegna e l'ambito del VDA con sistema operativo multisessione. Questa funzionalità richiede Delivery Controller versione 7.18 o successive. È possibile modificare i parametri di soglia dei criteri incorporati per gli avvisi in **Alerts** (Avvisi) > **Citrix Alerts Policy** (Criterio per gli avvisi Citrix).
Questi criteri vengono creati quando è presente almeno un target per gli avvisi: un gruppo di consegna o un VDA con sistema operativo multisessione definito nel sito. Inoltre, questi avvisi incorporati vengono aggiunti automaticamente a un nuovo gruppo di consegna o a un VDA con sistema operativo multisessione.

Nel caso in cui vengano aggiornati Director e il sito, i criteri per gli avvisi della precedente istanza di Director vengono trasferiti. I criteri incorporati per gli avvisi vengono creati solo se non esistono regole di avviso corrispondenti nel database di monitoraggio.

Per i valori di soglia dei criteri per gli avvisi incorporati, vedere la sezione Condizioni dei criteri per gli avvisi.



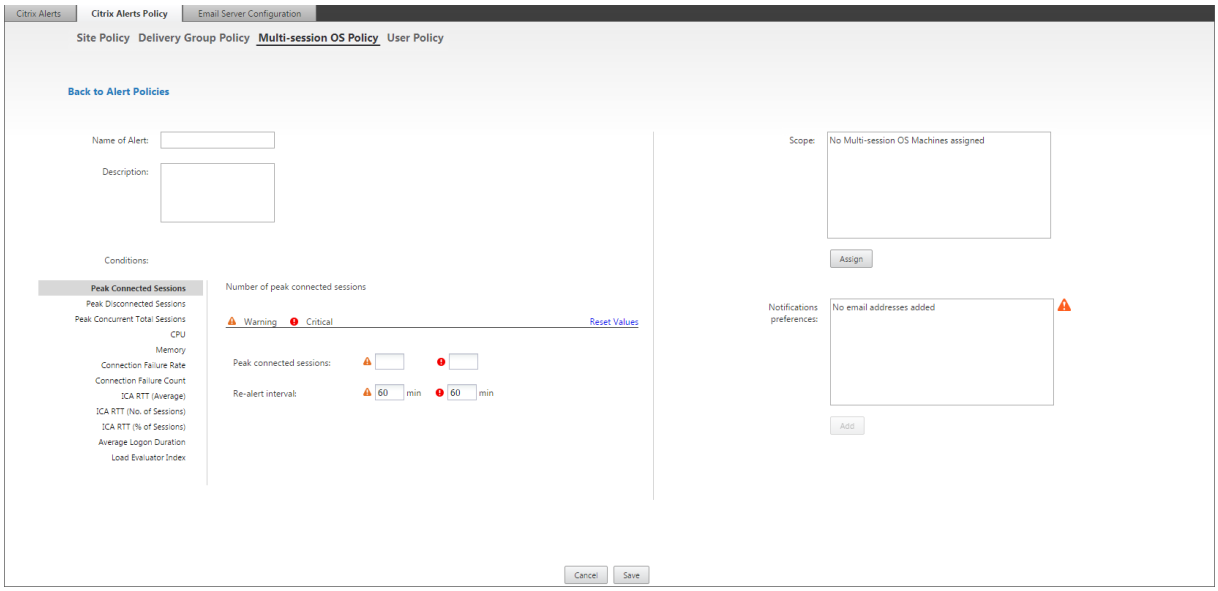

## Avvisi SCOM

Gli avvisi SCOM visualizzano informazioni sugli avvisi di Microsoft System Center 2012 Operations Manager (SCOM) per fornire un'indicazione più completa dello stato e delle prestazioni del centro dati all'interno di Director. Per ulteriori informazioni, vedere la sezione Configurare l'integrazione degli avvisi SCOM .

Il numero di avvisi visualizzato accanto alle icone di avviso prima di espandere la barra laterale è la somma combinata degli avvisi Citrix e SCOM.

## Creare criteri per gli avvisi




Per creare un nuovo criterio per gli avvisi, ad esempio per generare un avviso quando viene soddisfatta una serie specifica di criteri di conteggio delle sessioni:

1. Andare ad **Alerts** (Avvisi) > **Citrix Alerts Policy** (Criterio per gli avvisi Citrix) e selezionare, ad esempio, Multi-session OS Policy (Criterio del sistema operativo multisessione).
2. Fare clic su **Create**.
3. Assegnare un nome al criterio e descriverlo, quindi impostare le condizioni che devono essere soddisfatte per l'attivazione dell'avviso. Ad esempio, specificare i conteggi Warning (Avvertimento) e Critical (Critico) per Peak Connected Sessions (Sessioni di picco connesse), Peak Disconnected Sessions (Sessioni di picco disconnesse) e Peak Concurrent Total Sessions (Sessioni di picco simultanee totali). I valori di avvertimento non devono essere superiori ai valori di avviso critico. Per ulteriori informazioni, vedere Condizioni dei criteri per gli avvisi.
4. Impostare l'intervallo Re-alert (Visualizza nuovamente avviso). Se le condizioni per l'avviso sono ancora soddisfatte, l'avviso viene riattivato a questo intervallo di tempo e viene generata una notifica via e-mail, se impostata nel criterio di avviso. Un avviso ignorato non genera una notifica via e-mail all'intervallo di riavviso.
5. Impostare il campo Scope (Ambito). Ad esempio, impostare un gruppo di consegna specifico.
6. In Notification preferences (Preferenze di notifica), specificare chi deve essere avvisato via e-mail quando viene attivato l'avviso. È necessario specificare un server e-mail nella scheda **Email Server Configuration** (Configurazione server e-mail) per impostare le preferenze di notifica e-mail in Alerts Policies (Criteri per gli avvisi).
7. Fare clic su **Salva**.

La creazione di un criterio con 20 o più gruppi di consegna definiti in Scope (Ambito) potrebbe richiedere circa 30 secondi per completare la configurazione. Durante questo periodo viene

visualizzata una rotellina.

La creazione di più di 50 criteri per un massimo di 20 gruppi di consegna univoci (1000 target di gruppi di consegna in totale) potrebbe comportare un aumento del tempo di risposta (oltre 5 secondi).

Lo spostamento di una macchina contenente sessioni attive da un gruppo di consegna a un altro potrebbe causare avvisi errati del gruppo di consegna definiti utilizzando i parametri della macchina.

> **Nota:**
> dopo aver eliminato un criterio di avviso, potrebbero essere necessari fino a 30 minuti prima che le notifiche di avviso generate dalla politica si interrompano.

## Condizioni dei criteri per gli avvisi

Di seguito sono riportate le categorie di avvisi, le azioni consigliate per mitigare l'avviso e le condizioni dei criteri incorporate, se definite. I criteri incorporati per gli avvisi sono definiti per intervalli di avviso e riavviso di 60 minuti.

#### Peak Connected Sessions (Sessioni di picco connesse)

- Controllare la vista Director Session Trends (Tendenze della sessione di Director) per verificare se sono presenti sessioni di picco connesse.
- Verificare che vi sia capacità sufficiente per supportare il carico della sessione.
- Aggiungere nuove macchine, se necessario.

#### Peak Disconnected Sessions (Sessioni di picco disconnesse)

- Controllare la vista Director Session Trends (Tendenze della sessione di Director) per verificare se sono presenti sessioni di picco disconnesse.
- Verificare che vi sia capacità sufficiente per supportare il carico della sessione.
- Aggiungere nuove macchine, se necessario.
- Disconnettere le sessioni disconnesse, se necessario.

#### Peak Concurrent Total Sessions (Sessioni di picco simultanee totali)

- Controllare la vista Director Session Trends (Tendenze della sessione di Director) per verificare se sono presenti sessioni di picco simultanee.
- Verificare che vi sia capacità sufficiente per supportare il carico della sessione.
- Aggiungere nuove macchine, se necessario.
- Disconnettere le sessioni disconnesse, se necessario.

#### CPU

La percentuale di utilizzo della CPU indica il consumo complessivo della CPU sul VDA, incluso quello dei processi. È possibile ottenere maggiori informazioni sull'utilizzo della CPU da parte dei singoli processi dalla pagina **Machine details** (Dettagli macchina) del VDA corrispondente.

- Andare a **Machine Details (Dettagli macchina) > View Historical Utilization (Visualizza utilizzo storico) > Top 10 Processes (Primi 10 processi)** e identificare i processi che consumano CPU. Assicurarsi che il criterio di monitoraggio dei processi sia abilitato per avviare la raccolta delle statistiche sull'utilizzo delle risorse a livello di processo.
- Terminare il processo, se necessario.
- L'interruzione del processo causa la perdita dei dati non salvati.
- Se tutto funziona come previsto, aggiungere altre risorse CPU in futuro.

  > **Nota:**
  >
  > L'impostazione dei criteri **Enable resource monitoring** (Abilita il monitoraggio delle risorse) è consentita per impostazione predefinita per il monitoraggio dei contatori delle prestazioni della CPU e della memoria su macchine con VDA. Se questa impostazione dei criteri è disabilitata, gli avvisi con condizioni relative alla CPU e alla memoria non vengono attivati. Per ulteriori informazioni, vedere Impostazioni dei criteri di monitoraggio.

  **Condizioni dei criteri intelligenti:**

  - **Scope** (Ambito): gruppo di consegna, ambito del sistema operativo multisessione
  - **Threshold values** (Valori soglia): Warning (Avvertimento) - 80%, Critical (Avviso critico) - 90%

#### Memory (Memoria)

La percentuale di utilizzo della memoria indica il consumo complessivo di memoria sul VDA, incluso quello dei processi. È possibile ottenere maggiori informazioni sull'utilizzo della memoria da parte dei singoli processi dalla pagina **Machine details** (Dettagli macchina) del VDA corrispondente.

- Andare a **Machine Details (Dettagli macchina) > View Historical Utilization (Visualizza utilizzo storico) > Top 10 Processes (Primi 10 processi)** e identificare i processi che consumano memoria. Assicurarsi che il criterio di monitoraggio dei processi sia abilitato per avviare la raccolta delle statistiche sull'utilizzo delle risorse a livello di processo.
- Terminare il processo, se necessario.
- L'interruzione del processo causa la perdita dei dati non salvati.
- Se tutto funziona come previsto, aggiungere ulteriore memoria in futuro.

> **Nota:**
>
> L'impostazione dei criteri **Enable resource monitoring** (Abilita monitoraggio delle risorse) è consentita per impostazione predefinita per il monitoraggio dei contatori delle prestazioni della CPU e della memoria sulle macchine con VDA. Se questa impostazione dei criteri è disabilitata, gli avvisi con condizioni relative alla CPU e alla memoria non vengono attivati. Per ulteriori informazioni, vedere Impostazioni dei criteri di monitoraggio.

**Condizioni dei criteri intelligenti:**

- **Scope** (Ambito): gruppo di consegna, ambito del sistema operativo multisessione
- **Threshold values** (Valori soglia): Warning (Avvertimento) - 80%, Critical (Avviso critico) - 90%

#### Connection Failure Rate (Frequenza dei problemi di connessione)

Percentuale di problemi di connessione nell'ultima ora.

- Calcolata in base al totale delle connessioni non riuscite rispetto al numero totale di tentativi di connessione.
- Controllare la vista Director Connection Failures Trend (Tendenze degli errori di connessione di Director) per visualizzare gli eventi registrati dal log di configurazione.
- Determinare se le applicazioni o i desktop sono raggiungibili.

#### Connection Failure Count (Conteggio degli errori di connessione)

Numero di problemi di connessione nell'ultima ora.

- Controllare la vista Director Connection Failures Trend (Tendenze degli errori di connessione di Director) per visualizzare gli eventi registrati dal log di configurazione.
- Determinare se le applicazioni o i desktop sono raggiungibili.

#### ICA RTT (Average) (Tempo di round trip ICA [media])

Tempo medio di round trip ICA.

- Controllare Citrix ADM per i dettagli del tempo di round trip ICA, per determinare la causa principale. Per ulteriori informazioni, vedere la documentazione di Citrix ADM.
- Se Citrix ADM non è disponibile, controllare la vista Director User Details (Dettagli utente di Director) per il tempo di round trip ICA e la latenza e per determinare se si tratta di un problema di rete o di un problema delle applicazioni o dei desktop.

#### ICA RTT (No. of Sessions) (Tempo di round trip ICA [numero di sessioni])

Numero di sessioni che superano la soglia per il tempo di round trip ICA.

- Controllare Citrix ADM per visualizzare il numero di sessioni con tempo di round trip ICA elevato. Per ulteriori informazioni, vedere la documentazione di Citrix ADM.
- Se Citrix ADM non è disponibile, collaborare con il team di rete per determinare la causa principale.

  **Condizioni dei criteri intelligenti:**

  - **Scope** (Ambito): gruppo di consegna, ambito del sistema operativo multisessione
  - **Threshold values** (Valori soglia): Warning (Avvertimento): 300 ms per 5 o più sessioni, Critical (Avviso critico): 400 ms per 10 o più sessioni

#### ICA RTT (% of Sessions) (Tempo di round trip ICA [% delle sessioni])

Percentuale di sessioni che superano il tempo medio di round trip ICA.

- Controllare Citrix ADM per visualizzare il numero di sessioni con tempo di round trip ICA elevato. Per ulteriori informazioni, vedere la documentazione di Citrix ADM.
- Se Citrix ADM non è disponibile, collaborare con il team di rete per determinare la causa principale.

#### ICA RTT (User) (Tempo di round trip ICA [utente])

Tempo di round trip ICA applicato alle sessioni avviate dall'utente specificato. L'avviso viene attivato se il tempo di round trip ICA è maggiore della soglia in almeno una sessione.

#### Failed Machines (Single-session OS) (Macchine che presentano problemi [sistema operativo a sessione singola])

Numero di macchine con sistema operativo a sessione singola che presentano problemi. Gli errori possono verificarsi per vari motivi, come mostrato nella dashboard di Director e nelle viste Filters (Filtri).

- Eseguire la diagnostica Citrix Scout per determinare la causa principale.

  **Condizioni dei criteri intelligenti:**

  - **Scope** (Ambito): gruppo di consegna, ambito del sistema operativo multisessione
  - **Threshold values** (Valori soglia): Warning (Avvertimento) - 1, Critial (Avviso critico) - 2

**Failed Machines (Multi-session OS) (Macchine che presentano problemi [sistema operativo multisessione])**

Numero di macchine con sistema operativo multisessione che presentano problemi. Gli errori possono verificarsi per vari motivi, come mostrato nella dashboard di Director e nelle viste Filters (Filtri).

- Eseguire la diagnostica Citrix Scout per determinare la causa principale.

  **Condizioni dei criteri intelligenti:**

  - **Scope** (Ambito): gruppo di consegna, ambito del sistema operativo multisessione
  - **Threshold values** (Valori soglia): Warning (Avvertimento) - 1, Critial (Avviso critico) - 2

**Computer con errori (in %)**

Percentuale di computer con sistema operativo a sessione singola e multisessione che hanno riportato errori in un gruppo di consegna calcolata in base al numero di macchine con errore. Questa condizione di avviso consente di configurare le soglie di avviso in termini di percentuale di macchine con errori all'interno di un gruppo di consegna e viene calcolata ogni 30 secondi.
Gli errori possono verificarsi per vari motivi, come mostrato nella dashboard di Director e nelle viste Filters (Filtri). Eseguire la diagnostica Citrix Scout per determinare la causa principale. Per ulteriori informazioni, vedere Risoluzione dei problemi degli utenti.

**Average Logon Duration (Durata media dell'accesso)**

Durata media dell'accesso per gli accessi avvenuti nell'ultima ora.

- Controllare la dashboard di Director per ottenere metriche aggiornate sulla durata dell'accesso. Un numero elevato di utenti che effettuano l'accesso in un breve periodo di tempo può aumentare la durata dell'accesso.
- Controllare la linea di base e la ripartizione degli accessi per restringere la causa. Per ulteriori informazioni, vedere Diagnosticare i problemi di accesso degli utenti

  **Condizioni dei criteri intelligenti:**

  - **Scope** (Ambito): gruppo di consegna, ambito del sistema operativo multisessione
  - **Threshold values** (Valori soglia): Warning (Avvertimento) - 45 secondi, Critical (Avviso critico) - 60 secondi

**Logon Duration (User) (Durata dell'accesso [utente])**

Durata dell'accesso per gli accessi dell'utente specificato che si sono verificati nell'ultima ora.

#### Load Evaluator Index (Indice di valutazione del carico)

Valore dell'indice di valutazione del carico negli ultimi 5 minuti.

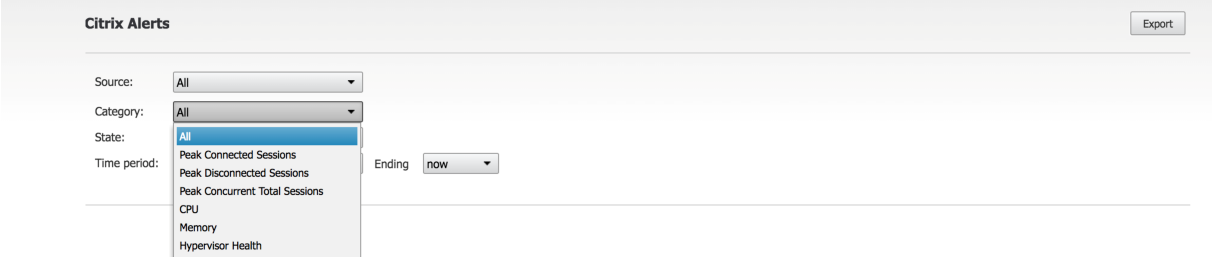
- Controllare Director per verificare la presenza di macchine con sistema operativo multisessione che potrebbero avere un carico di picco (carico massimo). Visualizzare sia la dashboard (errori) che il report Trends Load Evaluator Index (Indice delle tendenze per la valutazione del carico).

  **Condizioni dei criteri intelligenti:**

  - **Scope** (Ambito): gruppo di consegna, ambito del sistema operativo multisessione
  - **Threshold values** (Valori soglia): Warning (Avvertimento) - 80%, Critical (Avviso critico) - 90%

### Monitoraggio degli avvisi di Hypervisor

Director visualizza avvisi per monitorare lo stato dell'hypervisor. Gli avvisi di Citrix Hypervisor e VMware vSphere aiutano a monitorare i parametri e gli stati dell'Hypervisor. Viene monitorato anche lo stato della connessione all'hypervisor per fornire un avviso se il cluster o il pool di host viene riavviato o non è disponibile.

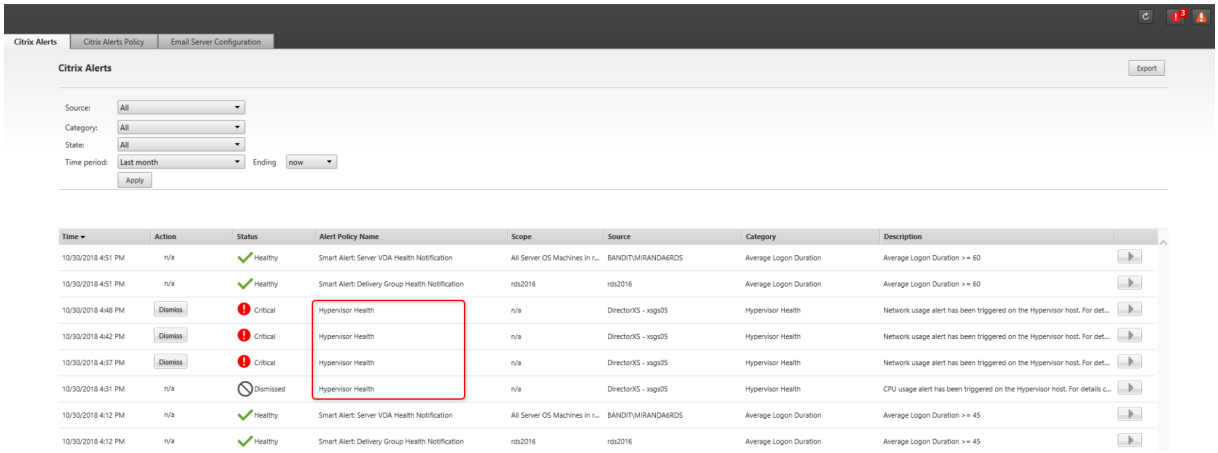



Per ricevere avvisi per l'hypervisor, assicurarsi che venga creata una connessione di hosting in Web Studio. Per ulteriori informazioni, vedere Connessioni e risorse. Solo queste connessioni sono monitorate per gli avvisi dell'hypervisor.

Questi avvisi vengono visualizzati una volta raggiunte o superate le soglie. Gli avvisi di Hypervisor possono essere:

- Critical (Avviso critico): soglia critica del criterio di allarme dell'hypervisor raggiunta o superata
- Warning (Avvertimento): soglia di avvertimento del criterio di allarme dell'hypervisor raggiunta o superata
- Dismissed (Ignorato): avviso non più visualizzato come avviso attivo




Questa funzionalità richiede Delivery Controller versione 7 1811 o successive. Se si utilizza una versione precedente di Director con siti 7 1811 o successivi, viene visualizzato solo il conteggio degli avvisi dell'hypervisor. Per visualizzare gli avvisi, è necessario aggiornare Director.

Nella tabella seguente vengono descritti i vari parametri e stati degli avvisi di Hypervisor.

| Avviso | Hypervisor supportati | Attivato da | Condizione | Configurazione |
|---|---|---|---|---|
| CPU usage (Utilizzo della CPU) | Citrix Hypervisor, VMware vSphere | Hypervisor | Soglia di avviso di utilizzo della CPU raggiunta o superata | Le soglie di avviso devono essere configurate in Hypervisor. |
| Memory usage (Utilizzo della memoria) | Citrix Hypervisor, VMware vSphere | Hypervisor | Soglia di avviso di utilizzo della memoria raggiunta o superata | Le soglie di avviso devono essere configurate in Hypervisor. |
| Network usage (Utilizzo della rete) | Citrix Hypervisor, VMware vSphere | Hypervisor | Soglia di avviso di utilizzo della rete raggiunta o superata | Le soglie di avviso devono essere configurate in Hypervisor. |
| Disk usage (Utilizzo del disco) | VMware vSphere | Hypervisor | Soglia di avviso di utilizzo del disco raggiunta o superata | Le soglie di avviso devono essere configurate in Hypervisor. |

| Avviso | Hypervisor supportati | Attivato da | Condizione | Configurazione |
|---|---|---|---|---|
| Host connection or power state (Connessione host o stato di alimentazione) | VMware vSphere | Hypervisor | L'host di Hypervisor è stato riavviato o non è disponibile | Gli avvisi sono predefiniti in VMware vSphere. Non sono necessarie configurazioni aggiuntive. |
| Hypervisor connection unavailable (Connessione all'Hypervisor non disponibile) | Citrix Hypervisor, VMware vSphere | Delivery Controller | La connessione all'hypervisor (pool o cluster) viene persa, interrotta o riavviata. Questo avviso viene generato ogni ora finché la connessione non è disponibile. | Gli avvisi sono predefiniti nel Delivery Controller. Non sono necessarie configurazioni aggiuntive. |

> **Nota:**
>
> Per ulteriori informazioni sulla configurazione degli avvisi, vedere Avvisi di Citrix XenCenter o consultare la documentazione di Avvisi di VMware vCenter.

La preferenza per le notifiche e-mail può essere configurata in **Citrix Alerts Policy (Criteri per gli avvisi Citrix) > Site Policy (Criterio del sito) > Hypervisor Health (Stato dell'Hypervisor)**. Le condizioni di soglia per i criteri di avviso di Hypervisor possono essere configurate, modificate, disabilitate o eliminate solo dall'hypervisor e non da Director. Tuttavia, in Director è possibile modificare le preferenze e-mail e ignorare un avviso. È possibile disabilitare l'avviso se il proprio ruolo non prevede il monitoraggio dell'infrastruttura.

> **Importante:**
>
> - Gli avvisi attivati da Hypervisor vengono recuperati e visualizzati in Director. Tuttavia, i cambiamenti nel ciclo di vita/stato degli avvisi di Hypervisor non si riflettono in Director.
> - Gli avvisi integri o ignorati o disabilitati nella console di Hypervisor continueranno a essere visualizzati in Director e dovranno essere ignorati esplicitamente.
> - Gli avvisi che vengono ignorati in Director non vengono automaticamente ignorati nella

> console di Hypervisor.

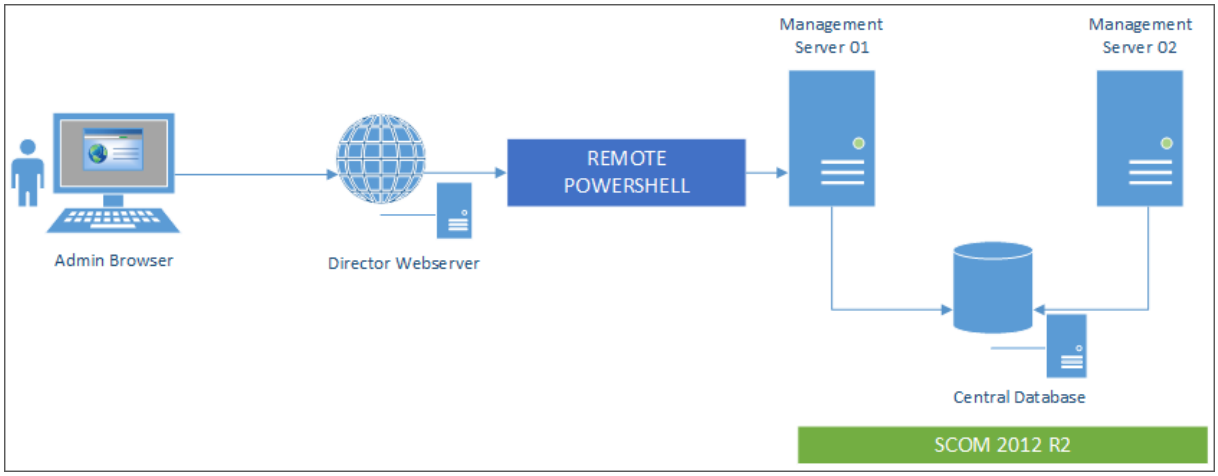
### Configurare l'integrazione degli avvisi SCOM

L'integrazione di SCOM con Director consente di visualizzare le informazioni di avviso di SCOM sulla dashboard e in altre viste di alto livello in Director.

Gli avvisi SCOM vengono visualizzati sullo schermo insieme agli avvisi Citrix. È possibile accedere agli avvisi SCOM ed eseguirne il drill down dalla scheda SCOM nella barra laterale.

È possibile visualizzare gli avvisi precedenti dell'ultimo mese, nonché ordinare, filtrare ed esportare le informazioni filtrate nei formati di report CSV, Excel e PDF. Per ulteriori informazioni, vedere Esportare i report.

L'integrazione di SCOM utilizza sessioni remote di PowerShell 3.0 o versioni successive per eseguire query sui dati di SCOM Management Server e mantiene una connessione persistente allo spazio di esecuzione nella sessione Director dell'utente. Director e il server SCOM devono avere la stessa versione di PowerShell.




I requisiti per l'integrazione di SCOM sono:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0 o versione successiva (la versione di PowerShell su Director e sul server SCOM devono corrispondere)
- CPU quad core con 16 GB di RAM (consigliata)
- Deve essere configurato un server di gestione principale per SCOM nel file web.config di Director. È possibile farlo utilizzando lo strumento DirectorConfig.

Citrix consiglia di configurare l'account amministratore di Director come ruolo SCOM Operator (Operatore SCOM), in modo che le informazioni complete degli avvisi possano essere recuperate in Di-

rector. Se ciò non fosse possibile, configurare un account amministratore SCOM nel file web.config utilizzando lo strumento DirectorConfig.

Citrix consiglia inoltre di non configurare più di 10 amministratori di Director per il server di gestione SCOM, per garantire prestazioni ottimali.

Sul server di Director:

1. Digitare **Enable-PSRemoting** per abilitare la comunicazione remota di PowerShell.
2. Aggiungere SCOM Management Server (Server di gestione SCOM) all'elenco TrustedHosts. Aprire un prompt di PowerShell ed eseguire i seguenti comandi:
   - Ottenere l'elenco attuale di TrustedHosts

     Get-Item WSMAN:\localhost\Client\TrustedHosts
   - Aggiungere il nome di dominio completo del server di gestione SCOM all'elenco di TrustedHosts. <Old Values> (Valori precedenti) rappresenta l'insieme esistente di voci restituite dal cmdlet Get-Item.

     Set-Item WSMAN:localhostClientTrustedHosts -Value "<FQDN SCOM Management Server>,<Old Values>"
3. Configurare SCOM utilizzando lo strumento DirectorConfig.

   C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom

Sul server di gestione SCOM:

1. Assegnare gli amministratori di Director a un ruolo amministratore SCOM.
   a) Aprire la console di gestione SCOM e andare ad **Administration** (Amministrazione) > **Security** (Sicurezza) > **User Roles** (Ruoli utente).
   b) In User Roles (Ruoli utente), è possibile creare un nuovo ruolo utente o modificarne uno esistente. Esistono quattro categorie di ruoli operatore SCOM che definiscono la natura dell'accesso ai dati SCOM. Ad esempio, un ruolo di sola lettura non vede il riquadro Administration (Amministrazione) e non è in grado di rilevare o gestire regole, macchine o account. Un ruolo Operator (Operatore) è un ruolo amministratore completo.

      **Nota:**

      Le seguenti operazioni non sono disponibili se l'amministratore di Director è assegnato a un ruolo diverso da Operator (Operatore):

      - Se sono configurati più server di gestione e il server di gestione principale non è disponibile, l'amministratore di Director non può connettersi al server di gestione secondario. Il server di gestione principale è il server configurato nel file

> web.config di Director, ovvero lo stesso server specificato con lo strumento DirectorConfig nel passaggio 3 precedente. I server di gestione secondari sono server di gestione peer del server principale.
> - Durante il filtraggio degli avvisi, l'amministratore di Director non può cercare l'origine degli avvisi. Questa operazione richiede un'autorizzazione a livello di operatore.

c) Per modificare qualsiasi ruolo utente, fare clic con il pulsante destro del mouse sul ruolo, quindi fare clic su **Properties** (Proprietà).

d) Nella finestra di dialogo User Role Properties (Proprietà ruolo utente), è possibile aggiungere o rimuovere gli amministratori di Director dal ruolo utente specificato.

2. Aggiungere gli amministratori di Director al gruppo Remote Management Users (Utenti di gestione remota) sul server di gestione SCOM. Questo consente agli amministratori di Director di stabilire una connessione remota PowerShell.
3. Digitare **Enable-PSRemoting** per abilitare la comunicazione remota di PowerShell.
4. Impostare i limiti delle proprietà WS-Management:

a) Modificare MaxConcurrentUsers:

Nell'interfaccia della riga di comando:

"'winrm set winrm/config/winrs @{MaxConcurrentUsers = "20"}

```
In PS:

```Set -Item WSMan:\localhost\Shell\MaxConcurrentUsers 20<!--
   NeedCopy-->
```

b) Modificare MaxShellsPerUser:

Nell'interfaccia della riga di comando:

```
winrm set winrm/config/winrs @{ MaxShellsPerUser="20"} <!--
NeedCopy-->
```

In PS:

"'Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20

```
1.  Modificare MaxMemoryPerShellMB:

    Nell'interfaccia della riga di comando:

    ```winrm set winrm/config/winrs @{
 MaxMemoryPerShellMB="1024" }
 <!--NeedCopy-->
```

```
1 In PS:
```

```
Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024<!--
NeedCopy-->
```

5. Per garantire che l'integrazione di SCOM funzioni in ambienti con domini misti, impostare la seguente voce del Registro di sistema.

Percorso: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Chiave: LocalAccountTokenFilterPolicy

Tipo: DWord

Valore: 1

**Attenzione:** la modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Una volta configurata l'integrazione di SCOM, potrebbe essere visualizzato il messaggio "Cannot get the latest SCOM alerts. View the Director server event logs for more information"(Impossibile ottenere gli avvisi SCOM più recenti. Visualizzare i log eventi del server di Director per ulteriori informazioni). I log eventi del server aiutano a identificare e correggere il problema. Le cause possono includere:

- Perdita di connettività di rete sulla macchina di Director o SCOM.
- Il servizio SCOM non è disponibile o è troppo occupato per rispondere.
- Autorizzazione non riuscita a causa di una modifica delle autorizzazioni per l'utente configurato.
- Errore in Director durante l'elaborazione dei dati SCOM.
- Mancata corrispondenza della versione di PowerShell tra Director e il server SCOM.

## Filtrare i dati per risolvere i problemi

April 3, 2024

Quando si fa clic sui numeri nella Dashboard o si seleziona un filtro predefinito dal menu Filters, si apre la vista Filters in cui sono visualizzati i dati in base al tipo di macchina o guasto selezionato.

I filtri predefiniti non possono essere modificati, ma è possibile salvare un filtro predefinito come filtro personalizzato e modificarlo. Inoltre, è possibile creare viste filtrate personalizzate di macchine, connessioni, sessioni e istanze delle applicazioni in tutti i gruppi di consegna.

1. Selezionare una vista:

   - **Machines** (Macchine). Selezionare Single-session OS Machines (Macchine con sistema operativo a sessione singola) o Multi-session OS Machines (Macchine con sistema operativo multisessione). Queste viste mostrano il numero di macchine configurate. La scheda Multi-session OS Machines (Macchine con sistema operativo multisessione) include anche l'indice di valutazione del carico, che indica la distribuzione dei contatori delle prestazioni e le descrizioni dei comandi del conteggio delle sessioni se si passa il mouse sul collegamento.
   - **Sessions** (Sessioni). È inoltre possibile visualizzare il conteggio delle sessioni dalla vista Sessions (Sessioni). Utilizzare le misurazioni del tempo di inattività per identificare le sessioni inattive oltre un periodo di soglia. Fare clic sull'**utente associato** per aprire l'Activity Manager per l'utente. Facendo clic sul nome dell'**endpoint** si apre l'Activity Manager relativo all'endpoint. Facendo clic su **View Details** (Visualizza dettagli), si apre rispettivamente la pagina **User Details** (Dettagli utente) o **Endpoint Details** (Dettagli endpoint). Per ulteriori informazioni, vedere Dettagli utente.
   - **Connections** (Connessioni). Filtrare le connessioni in base a diversi periodi di tempo, inclusi gli ultimi 60 minuti, le ultime 24 ore o gli ultimi 7 giorni.
   - **Application Instances** (Istanze dell'applicazione). Questa vista visualizza le proprietà di tutte le istanze delle applicazioni sui VDA del server e del sistema operativo a sessione singola. Le misurazioni del tempo di inattività della sessione sono disponibili per le istanze delle applicazioni sui VDA con sistema operativo multisessione.

   > **Nota:**
   >
   > Se sono state avviate sessioni desktop su VDA installati su un computer Windows 10 1809, in Activity Manager (Gestione attività) in Director è possibile che Microsoft Edge e Office vengano visualizzati come applicazioni in esecuzione attiva, mentre sono in esecuzione solo in background.

2. Per **Filter by** (Filtra per), selezionare i criteri.
3. Utilizzare le schede aggiuntive per ogni vista, se necessario, per completare il filtro.
4. Selezionare colonne aggiuntive, se necessario, per continuare con la risoluzione dei problemi.
5. Salvare il filtro e assegnarvi un nome.
6. Per accedere ai filtri da più server Director, archiviare i filtri in una cartella condivisa accessibile da tali server:

   - La cartella condivisa deve disporre delle autorizzazioni di modifica per gli account sul server Director.
   - I server Director devono essere configurati per accedere alla cartella condivisa. Per procedere con la configurazione, eseguire **IIS Manager**. In **Sites (Siti) > Default Web Site**

**(Sito Web predefinito) > Director\ > Application Settings (Impostazioni applicazione)**, modificare l'impostazione **Service.UserSettingsPath** per riflettere il percorso UNC della cartella condivisa.

7. Per aprire il filtro in un secondo momento, dal menu **Filters** (Filtri) selezionare il tipo di filtro (macchine, sessioni, connessioni o istanze dell'applicazione), quindi selezionare il filtro salvato.
8. Fare clic su **Export** (Esporta) per esportare i dati in file in formato CSV. È possibile esportare fino a 100.000 record di dati. Questa funzionalità è disponibile in Delivery Controller versione 1808 e successive.
9. Se necessario, per le viste **Machines** (Macchine) o **Connections** (Connessioni), utilizzare i controlli di alimentazione per tutte le macchine selezionate nell'elenco filtrato. Per la vista Sessions (Sessioni), utilizzare i controlli di sessione o l'opzione per inviare messaggi.
10. Nelle viste **Machines** (Macchine) e **Connections** (Connessioni), fare clic su **Failure Reason** (Motivo dell'errore) di una macchina che presenta problemi o di una connessione non riuscita per ottenere una descrizione dettagliata dell'errore e delle azioni consigliate per risolverlo. I motivi degli errori e le azioni consigliate per gli errori delle macchine e delle connessioni sono disponibili nella Cause di errori e risoluzione dei problemi di Citrix Director.
11. Nella vista **Machines** (Macchine), fare clic sul collegamento del nome di una macchina per accedere alla pagina **Machine Details** (Dettagli macchina) corrispondente. Questa pagina visualizza i dettagli della macchina, fornisce controlli di alimentazione, visualizza la CPU, la memoria, il monitoraggio del disco e i grafici sul monitoraggio della GPU. Inoltre, fare clic su **View Historical Utilization** (Visualizza utilizzo storico) per visualizzare le tendenze di utilizzo delle risorse per la macchina. Per ulteriori informazioni, vedere Risolvere i problemi relativi alle macchine.
12. Nella vista **Application Instances** (Istanze applicazione), ordinare o filtrare in base al **tempo di inattività** superiore a un periodo di soglia. Selezionare le istanze dell'applicazione inattive da terminare. Lo scollegamento o la disconnessione di un'istanza dell'applicazione termina tutte le istanze dell'applicazione attive nella stessa sessione. Per ulteriori informazioni, vedere Risolvere i problemi relativi alle applicazioni. La pagina dei filtri Application Instances (Istanze delle applicazioni) e le misurazioni del tempo di inattività nelle pagine dei filtri Sessions (Sessioni) sono disponibili se la versione di Director, dei Delivery Controller e dei VDA corrisponde a 7.13 o successiva.

> **Nota:**
> Web Studio consente l'assegnazione di più regole di assegnazione del desktop (DAR) per diversi utenti o gruppi di utenti a un singolo VDA nel gruppo di consegna. StoreFront visualizza il desktop assegnato con il Display Name (Nome visualizzato) corrispondente in base al DAR dell'utente che ha effettuato l'accesso. Tuttavia, Director non supporta le DAR e visualizza il desktop assegnato utilizzando il nome del gruppo di consegna indipendentemente dall'utente connesso. Di

> conseguenza, non è possibile mappare un desktop specifico a una macchina in Director. Per mappare il desktop assegnato visualizzato in StoreFront al nome del gruppo di consegna visualizzato in Director, utilizzare il seguente comando PowerShell:

```
Get-BrokerDesktopGroup | Where-Object {
  $\_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $\_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```

## Monitorare le tendenze storiche di un sito

January 7, 2024

La vista Trends (Tendenze) accede alle informazioni sulle tendenze storiche di ciascun sito per i seguenti parametri:

- sessioni
- errori di connessione
- errori della macchina
- prestazioni di accesso
- valutazione del carico
- gestione della capacità
- utilizzo della macchina
- utilizzo delle risorse
- analisi della rete per ogni sito.

Per individuare queste informazioni, fare clic sul menu **Trends** (Tendenze).

La funzione di drill down con zoom avanti consente di spostarsi tra i grafici delle tendenze selezionando un periodo di tempo (facendo clic su un punto dati nel grafico) ed eseguendo il drill down per visualizzare i dettagli associati alla tendenza. Questa funzionalità consente di comprendere meglio i dettagli di chi o cosa è influenzato.

Per modificare l'ambito predefinito di ciascun grafico, applicare un filtro diverso ai dati.

Selezionare un periodo di tempo per il quale si ha bisogno di informazioni storiche sulle tendenze. La disponibilità del periodo di tempo dipende dalla distribuzione di Director, come segue:

- I report sulle tendenze fino all'ultimo anno (365 giorni) sono disponibili nei siti con licenza Premium.

- I report sulle tendenze fino all'ultimo mese (31 giorni) sono disponibili nei siti con licenza Advanced.
- I report sulle tendenze fino agli ultimi 7 giorni sono disponibili nei siti con licenze diverse da Premium e Advanced.

> **Nota:**
>
> - In tutte le distribuzioni di Director, le informazioni sulle sessioni, gli errori e le tendenze delle prestazioni di accesso sono disponibili come grafici e tabelle quando il periodo di tempo è impostato su Last month (**Ending now**) (Ultimo mese [che sta per concludersi]) o un periodo più limitato. Per il periodo di tempo impostato come Last month (Ultimo mese) con una data di fine personalizzata o come Last year (Ultimo anno), le informazioni sulle tendenze sono disponibili come grafici e non come tabelle.
> - I valori di conservazione per la pulitura del servizio di monitoraggio controllano la disponibilità dei dati sulle tendenze. I valori predefiniti sono disponibili in Granularità e conservazione dei dati. I clienti di siti con licenza Premium possono modificare la conservazione per la pulitura sul numero di giorni di conservazione desiderato.
> - I seguenti parametri in IIS Manager controllano l'intervallo di date di fine personalizzate disponibili per la selezione. Tuttavia, la disponibilità dei dati per le date selezionate dipende dall'impostazione di conservazione per la pulitura per la metrica specifica da misurare.

| Parametro | Valori predefiniti |
|---|---|
| UI.TrendsLast2HoursRange | 3 |
| UI.TrendsLast24HoursRange | 32 |
| UI.TrendsLast7DaysRange | 32 |
| UI.TrendsLastMonthRange | 365 |

### Tendenze disponibili

**View trends for sessions** (Visualizza tendenze per le sessioni): dalla scheda **Sessions** (Sessioni), selezionare il gruppo di consegna e il periodo di tempo per visualizzare informazioni più dettagliate sul conteggio delle sessioni simultanee.

La colonna **Session Auto Reconnect** (Riconnessione automatica sessione) visualizza il numero di riconnessioni automatiche in una sessione. La riconnessione automatica è abilitata quando sono in vigore i criteri Session Reliability (Affidabilità della sessione) o Auto Client Reconnect (Riconnessione automatica client). Quando si verifica un'interruzione della rete sull'endpoint, entrano in vigore i seguenti criteri:

- Session Reliability (Affidabilità della sessione) entra in vigore (per impostazione predefinita per 3 minuti) quando l'app Citrix Receiver o Citrix Workspace tenta di connettersi al VDA.
- Auto Client Reconnect (Riconnessione automatica client) entra in vigore tra 3 e 5 minuti quando il client tenta di connettersi al VDA.

Entrambe le riconnessioni vengono acquisite e visualizzate all'utente. Queste informazioni possono richiedere un tempo massimo di 5 minuti per apparire nell'interfaccia utente di Director dopo che si è verificata la riconnessione.

Le informazioni di riconnessione automatica consentono di visualizzare le connessioni di rete che presentano interruzioni e risolverne i problemi. Analizzano anche le reti che hanno un'esperienza senza interruzioni. È possibile visualizzare il numero di riconnessioni per un gruppo di consegna o un periodo di tempo specifico selezionato in Filters (Filtri). Il drill down fornisce informazioni aggiuntive come l'affidabilità della sessione o la riconnessione automatica del client, i timestamp, l'IP dell'endpoint e il nome dell'endpoint della macchina su cui è installata l'app Workspace.

Per impostazione predefinita, i log vengono ordinati in base ai timestamp degli eventi in ordine decrescente. Questa funzionalità è disponibile per l'app Citrix Workspace per Windows, l'app Citrix Workspace per Mac, Citrix Receiver per Windows e Citrix Receiver per Mac. Questa funzionalità richiede Delivery Controller versione 7 1906 o successiva e VDA 1906 o versioni successive.

Per ulteriori informazioni sulle riconnessioni delle sessioni, vedere Sessions.

Per ulteriori informazioni sui criteri, vedere Impostazioni dei criteri di riconnessione automatica del client e Impostazioni dei criteri di affidabilità delle sessioni.

A volte, i dati di riconnessione automatica potrebbero non essere visualizzati in Director per i seguenti motivi:

- L'app Workspace non invia i dati di riconnessione automatica al VDA.
- Il VDA non invia i dati al servizio di monitoraggio.
- I Delivery Controller scartano i payload VDA perché potrebbero non avere le sessioni corrispondenti.

> **Nota:**
>
> Talvolta, l'indirizzo IP del client potrebbe non essere ottenuto correttamente se sono impostati determinati criteri di Citrix Gateway.

**View trends for connection failures** (Visualizza tendenze per errori di connessione): dalla scheda Failures (Errori), selezionare la connessione, il tipo di macchina, il tipo di errore, il gruppo di consegna e il periodo di tempo per visualizzare un grafico contenente informazioni più dettagliate sugli errori di connessione utente nel sito.

**View trends for machine failures** (Visualizza tendenze per gli errori delle macchine): dalla scheda **Single-session OS Machine Failures** (Errori delle macchine con sistema operativo a sessione sin-

gola) o dalla scheda Multi-session OS Machines (Macchine con sistema operativo multisessione), selezionare il tipo di errore, il gruppo di consegna e il periodo di tempo per visualizzare un grafico contenente informazioni più dettagliate sugli errori delle macchine nel sito.

**View trends for logon performance** (Visualizza tendenze per le prestazioni di accesso): dalla scheda **Logon Performance**(Prestazioni di accesso), selezionare il gruppo di consegna e il periodo di tempo per visualizzare un grafico contenente informazioni più dettagliate sulla durata dei tempi di accesso degli utenti nel sito e se il numero di accessi influisce sulle prestazioni. Questa vista mostra anche la durata media delle fasi di accesso, come la durata del brokering e l'ora di avvio della VM.
Questi dati sono specificamente riferiti agli accessi utente e non includono gli utenti che tentano di riconnettersi da sessioni disconnesse.
La tabella sotto il grafico mostra Logon Duration by User Session (Durata dell'accesso per sessione utente). È possibile scegliere le colonne da visualizzare e ordinare il report in base a una qualsiasi delle colonne.
Per ulteriori informazioni, vedere Diagnosticare i problemi di accesso degli utenti.

**View trends for load evaluation** (Visualizza tendenze per la valutazione del carico): dalla scheda **Load Evaluator Index** (Indice di valutazione del carico), visualizzare un grafico contenente informazioni più dettagliate sul carico distribuito tra le macchine con sistema operativo multisessione. Le opzioni di filtro per questo grafico includono il gruppo di consegna o la macchina con sistema operativo multisessione in un gruppo di consegna, la macchina con sistema operativo multisessione (disponibile solo se è stata selezionata la macchina con sistema operativo multisessione in un gruppo di consegna) e l'intervallo.

**View hosted applications usage** (Visualizza utilizzo delle applicazioni ospitate): la disponibilità di questa funzionalità dipende dalla licenza dell'organizzazione.
Dalla scheda **Capacity Management** (Gestione capacità), selezionare la scheda **Hosted Applications Usage** (Utilizzo delle applicazioni ospitate). Selezionare il gruppo di consegna e il periodo di tempo per visualizzare un grafico che mostra il picco di utilizzo simultaneo e una tabella che visualizza l'utilizzo in base all'applicazione. Dalla tabella Application Based Usage (Utilizzo basato sull'applicazione), è possibile scegliere un'applicazione specifica per visualizzare i dettagli e un elenco di utenti che utilizzano o hanno utilizzato l'applicazione.

**View Single-session and Multi-session OS usage** (Visualizza utilizzo del sistema operativo a sessione singola e multisessione): la vista Trends (Tendenze) mostra l'utilizzo del sistema operativo a sessione singola per sito e per gruppo di consegna. Quando si seleziona **Site** (Sito), viene visualizzato l'utilizzo per gruppo di consegna. Quando si seleziona Delivery Group (Gruppo di consegna), viene visualizzato l'utilizzo per utente.
La vista Trends (Tendenze) mostra anche l'utilizzo del sistema operativo multisessione per sito, per gruppo di consegna e per macchina. Quando si seleziona **Site** (Sito), viene visualizzato l'utilizzo per gruppo di consegna. Quando si seleziona Delivery Group (Gruppo di consegna), viene visualizzato l'utilizzo per macchina e per utente. Quando si seleziona Machine (Macchina), viene visualizzato l'

utilizzo per utente.

**View virtual machine usage** (Visualizza utilizzo della macchina virtuale): dalla scheda **Machine Usage** (Utilizzo macchina), selezionare **Single-session OS Machines (Macchine con sistema operativo a sessione singola) o Multi-session OS Machines (Macchine con sistema operativo multisessione)** per ottenere una visualizzazione in tempo reale dell'utilizzo della VM, che consente di valutare rapidamente le esigenze di capacità del sito.
Single-session OS availability (Disponibilità del sistema operativo a sessione singola): visualizza lo stato corrente delle macchine con sistema operativo a sessione singola (VDI) in base alla disponibilità per l'intero sito o per un gruppo di consegna specifico.
Multi-session OS availability (Disponibilità del sistema operativo multisessione): visualizza lo stato corrente delle macchine con sistema operativo multisessione in base alla disponibilità per l'intero sito o per un gruppo di consegna specifico.

> **Nota:**
> Il numero di macchine visualizzate in Available Counter (Contatore disponibile) include le macchine in modalità di manutenzione.

**View resource utilization** (Visualizza utilizzo delle risorse): dalla scheda **Resource Utilization** (Utilizzo delle risorse), selezionare **Single-session OS Machines (Macchine con sistema operativo a sessione singola) o Multi-session OS Machines (Macchine con sistema operativo multisessione)** per ottenere informazioni dettagliate sui dati delle tendenze storiche per l'utilizzo di CPU e memoria, nonché su IOPS e sulla latenza del disco per ogni macchina VDI, per una migliore pianificazione della capacità.
Questa funzionalità richiede Delivery Controller e VDA **versione 7.11** o successiva.
I grafici mostrano i dati relativi alla CPU media, alla memoria media, agli IOPS medi, alla latenza del disco e alle sessioni di picco simultanee. È possibile eseguire il drill down sulla macchina e visualizzare dati e grafici per i primi 10 processi che consumano CPU.

Filtrare in base al gruppo di consegna e al periodo di tempo. I grafici della CPU, dell'utilizzo della memoria e delle sessioni di picco simultanee sono disponibili per le ultime 2 ore, le ultime 24 ore, gli ultimi 7 giorni, l'ultimo mese e l'ultimo anno. I grafici sugli IOPS e la latenza del disco medi sono disponibili per le ultime 24 ore, l'ultimo mese e l'ultimo anno.

> **Nota:**
>
> - L'impostazione dei criteri di monitoraggio **Enable Process Monitoring** (Abilita monitoraggio processo) deve essere impostata su **Allowed** (Consentito) per raccogliere e visualizzare i dati nella tabella Top 10 Processes (Primi 10 processi) della pagina Historic Machine Utilization (Utilizzo storico della macchina). Il criterio è impostato su **Prohibited** (Non consentito) per impostazione predefinita. Tutti i dati di utilizzo delle risorse vengono raccolti per impostazione predefinita. Questa opzione può essere disabilitata utilizzando l'impostazione

> dei criteri **Enable Resource Monitoring** (Abilita monitoraggio delle risorse). La tabella sotto i grafici mostra i dati di utilizzo delle risorse per ogni macchina. Per ulteriori informazioni, vedere Impostazioni dei criteri di monitoraggio.
> - L'IOPS medio mostra le medie giornaliere. L'IOPS di picco è calcolato come la più alta delle medie IOPS per l'intervallo di tempo selezionato (una media IOPS è la media oraria degli IOPS raccolti nel corso di un'ora sul VDA).
> - Il drill-down della macchina elenca i processi con un utilizzo medio della CPU o un utilizzo medio della memoria superiore all'1%; ciò potrebbe significare che a volte vengono elencati meno di 10 processi.

**View network analysis data** (Visualizza dati di analisi di rete): la disponibilità di questa funzionalità dipende dalla licenza dell'organizzazione e dalle autorizzazioni dell'amministratore. Questa funzionalità richiede Delivery Controller **versione 7.11** o successiva.

Dalla scheda **Network** (Rete), monitorare l'analisi della rete, che fornisce una visualizzazione contestuale di utenti, applicazioni e desktop della rete. Con questa funzionalità, Director fornisce analisi avanzate del traffico ICA nella distribuzione tramite i report HDX Insight di Citrix ADM. Per ulteriori informazioni, vedere Configurare l'analisi di rete.

**View application failures** (Visualizza errori dell'applicazione): nella scheda **Application Failures** (Errori applicazione) vengono visualizzati gli errori associati alle applicazioni pubblicate sui VDA.

Questa funzionalità richiede Delivery Controller e VDA **versione 7.15** o successiva. Sono supportati i VDA con sistema operativo a sessione singola che eseguono Windows Vista e versioni successive e i VDA con sistema operativo multisessione che eseguono Windows Server 2008 e versioni successive. Per ulteriori informazioni, vedere Monitoraggio storico degli errori delle applicazioni.

Per impostazione predefinita, vengono visualizzati solo gli errori delle applicazioni dei VDA con sistema operativo multisessione. È possibile impostare il monitoraggio degli errori delle applicazioni utilizzando i criteri di monitoraggio. Per ulteriori informazioni, vedere Impostazioni dei criteri di monitoraggio.

**View probe results** (Visualizza risultati del probe): la scheda **Probe Results** (Risultati del probe) visualizza i risultati del probe per le applicazioni e i desktop configurati per il probe nella pagina Configuration (Configurazione). Qui viene registrata la fase di avvio durante la quale si è verificato l'errore.

Per ulteriori informazioni, vedere Probe delle applicazioni e dei desktop.

**Create customized reports** (Crea report personalizzati): la scheda Custom Reports (Report personalizzati) fornisce un'interfaccia utente per la generazione di report personalizzati contenenti dati storici e in tempo reale del database Monitoring (Monitoraggio) in formato tabulare.

Questa funzionalità richiede Delivery Controller **versione 7.12** o successiva.

Dall'elenco delle query Custom Report (Report personalizzato) salvate in precedenza, è possibile fare clic su **Run and download** (Esegui e scarica) per esportare il report in formato CSV, fare clic su **Copy**

**OData** (Copia OData) per copiare e condividere la query OData corrispondente oppure fare clic su **Edit** (Modifica) per modificare la query.
È possibile creare una nuova query Custom Report (Report personalizzato) basata su macchine, connessioni, sessioni o istanze dell'applicazione. Specificare le condizioni di filtro in base a campi come macchina, gruppo di consegna o periodo di tempo. Specificare le colonne aggiuntive richieste nel report personalizzato. L'anteprima visualizza un campione dei dati del report. Il salvataggio della query Custom Report (Report personalizzato) la aggiunge all'elenco delle query salvate.

È possibile creare una query Custom Report (Report personalizzato) basata su una query OData copiata. Per farlo, selezionare l'opzione OData Query (Query OData) e incollare la query OData copiata. È possibile salvare la query risultante per eseguirla in un secondo momento.

> **Nota:**
> I nomi delle colonne nel report Preview (Anteprima) ed Export (Esporta) generati utilizzando le query OData non sono tradotti, ma vengono visualizzati in inglese.

Le icone a forma di bandierina sul grafico indicano eventi o azioni significativi per l'intervallo di tempo specifico. Passare il mouse sulla bandierina e fare clic per elencare eventi o azioni.

> **Nota:**
>
> - I dati di accesso alla connessione HDX non vengono raccolti per le versioni di VDA precedenti alla 7. Per i VDA precedenti, i dati del grafico vengono visualizzati come 0.
> - I gruppi di consegna eliminati in Citrix Studio sono disponibili per la selezione nei filtri Trends (Tendenze) di Director finché i dati correlati non vengono eliminati. Se si seleziona un gruppo di consegna eliminato, vengono visualizzati grafici per i dati disponibili fino alla conservazione. Tuttavia, le tabelle non mostrano dati.
> - Lo spostamento di una macchina contenente sessioni attive da un gruppo di consegna a un altro fa sì che le tabelle **Resource Utilization (Utilizzo delle risorse) e Load Evaluator Index (Indice di valutazione del carico)** del nuovo gruppo di consegna visualizzino le metriche consolidate dei gruppi di consegna vecchi e nuovi.

## Monitoraggio di macchine gestite dalla scalabilità automatica

January 7, 2024

La scalabilità automatica è una funzionalità di gestione dell'alimentazione che consente la gestione proattiva dell'alimentazione di tutte le macchine con sistema operativo multisessione e a sessione singola registrate in un gruppo di consegna. È possibile configurare Autoscale per un gruppo di consegna selezionato in Web Studio. Per ulteriori informazioni, vedere Autoscale.

È possibile monitorare le metriche chiave delle macchine abilitate ad Autoscale utilizzando Director.

### Utilizzo della macchina

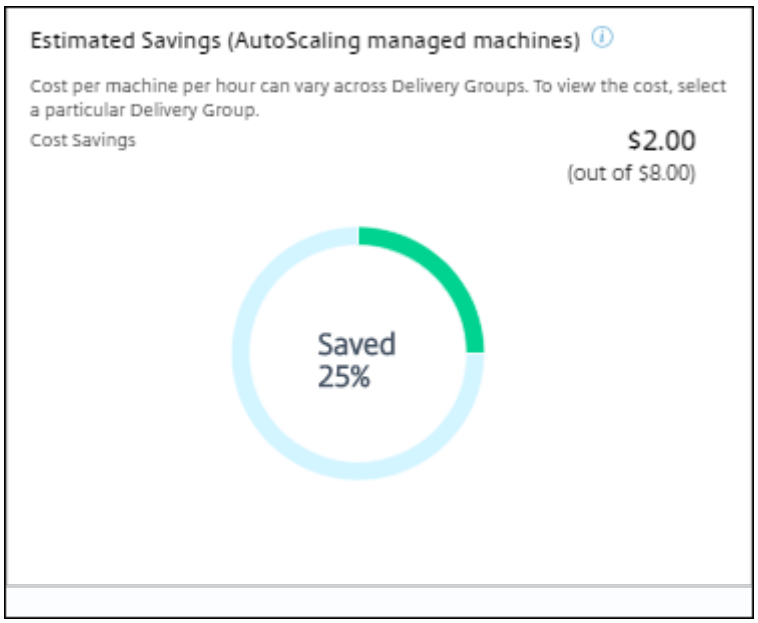
La pagina **Machine Usage** (Utilizzo macchina) visualizza il numero di macchine con sistema operativo multisessione e sessione singola abilitate per la scalabilità automatica che sono accese per un gruppo di consegna e un periodo di tempo selezionati. Questa metrica indica l'utilizzo effettivo delle macchine incluse nel gruppo di consegna.
Dalla scheda **Single session OS Machines** (Macchine con sistema operativo a sessione singola) o dalla scheda **Multi-session OS Machines** (Macchine con sistema operativo multisessione), selezionare il gruppo di consegna e il periodo di tempo.

Il grafico illustra le seguenti metriche:

- **Machines On**: il numero di macchine abilitate alla scalabilità automatica che sono accese
- **Machines Registered**: il numero di macchine con sistema operativo multisessione o a sessione singola registrate
- **Machines under Maintenance**: il numero di macchine con sistema operativo multisessione o a sessione singola con modalità di manutenzione attivata

### Risparmio stimato

La pagina **Machine Usage** visualizza anche i risparmi sui costi stimati ottenuti abilitando la scalabilità automatica nel gruppo di consegna selezionato.



Il risparmio stimato viene calcolato come percentuale di risparmi per macchina all'ora (in dollari USA) come configurato in **Manage** > **Autoscale**. Per ulteriori informazioni sulla configurazione dei risparmi per macchina, vedere Autoscale.

Quando si selezionano tutti i gruppi di consegna, viene visualizzato il valore medio del risparmio stimato in tutti i gruppi di consegna.

La stima del risparmio aiuta gli amministratori a consolidare l'infrastruttura esistente e pianificare la capacità per ottenere il massimo risparmio e utilizzo.

### Notifiche di avviso per macchine e sessioni

La dashboard di Director visualizza le notifiche di avviso di cui è possibile effettuare un ulteriore drill-down. I dettagli dell'avviso vengono visualizzati nella pagina **Alerts**.

- Per creare un criterio di avviso in un gruppo di consegna, passare ad **Alerts** > **Citrix Alerts Policy** > **Delivery Group Policy**.
- Qui è possibile impostare le seguenti soglie di avvertenza e soglie critiche:
  - macchine con errori (sistema operativo a sessione singola) e macchine con errori (sistema operativo multisessione);
  - sessioni connesse di picco, sessioni disconnesse di picco e sessioni totali concorrenti di picco nel gruppo di consegna.
- Vengono generati avvisi quando la metrica corrispondente all'interno del gruppo di consegna raggiunge la soglia.

Per maggiori dettagli sulle condizioni dei criteri di avviso e sulla creazione di nuovi criteri di avviso, vedere Avvisi e notifiche.

### Stato della macchina

- In **Filters** > **Machines** è visualizzato lo stato di alimentazione di tutte le macchine in un formato tabellare. È possibile filtrare indicando un gruppo di consegna specifico.
- In **Filters** > **Sessions** è visualizzato il filtro in base al nome della macchina per vedere le sessioni a essa associate e il loro stato in tempo reale.
- In **Trends** > **Sessions**, selezionare il gruppo di consegna e il periodo di tempo per visualizzare l'andamento delle sessioni e le metriche associate.

Per ulteriori informazioni, vedere Filtrare i dati per risolvere i problemi.

### Tendenze di valutazione del carico

Nella pagina **Trends** > **Load Evaluator Index** (Indice di valutazione del carico) è visualizzato un grafico con informazioni dettagliate sul carico distribuito tra le macchine con sistema operativo multisessione. Le opzioni di filtro per questo grafico includono il gruppo di consegna o la macchina con sistema operativo multisessione in un gruppo di consegna, la macchina con sistema operativo multisessione (disponibile solo se è stata selezionata la macchina con sistema operativo multisessione in un gruppo di consegna) e l'intervallo. L'indice di valutazione del carico viene visualizzato sotto forma di percentuali di CPU, memoria, disco o sessioni totali e viene visualizzato rispetto al numero di utenti connessi nell'ultimo intervallo.

## Risolvere i problemi relativi alle distribuzioni

January 7, 2024

In qualità di amministratore dell'help desk, è possibile cercare l'utente che segnala un problema e visualizzare i dettagli delle sessioni o delle applicazioni associate a tale utente. Analogamente, è possibile cercare macchine o endpoint in cui vengono segnalati problemi. È possibile risolvere rapidamente i problemi monitorando le metriche rilevanti ed eseguendo azioni appropriate.

Le azioni disponibili includono:

- Chiudere un'applicazione o un processo che non risponde
- Operazioni di shadowing sul computer dell'utente
- Scollegare una sessione che non risponde
- Riavviare il computer
- Mettere la macchina in modalità di manutenzione
- Reimpostare il profilo utente

## Risolvere i problemi relativi alle applicazioni

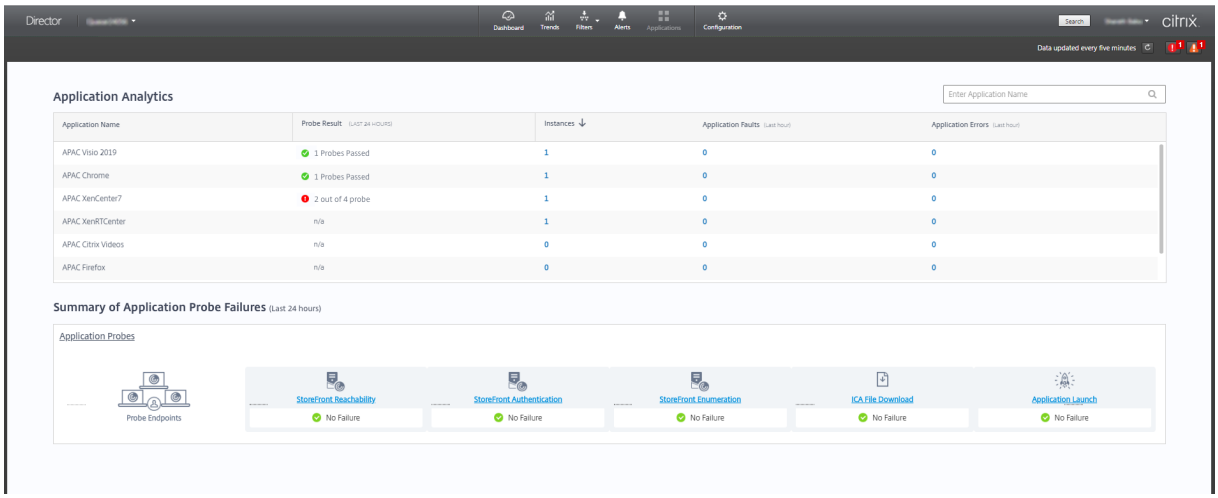
January 7, 2024

### Analisi delle applicazioni

La vista **Applications** (Applicazioni) visualizza le analisi basate sulle applicazioni in un'unica vista consolidata per facilitare l'analisi e la gestione efficienti delle prestazioni delle applicazioni. È possibile

ottenere importanti dettagli approfonditi sulle informazioni sullo stato e sull'utilizzo di tutte le applicazioni pubblicate sul sito. La vista predefinita aiuta a identificare le applicazioni più frequentemente eseguite.
Questa funzionalità richiede Delivery Controller versione 7.16 o successiva e VDA versione 7.15 o successiva.




La colonna **Probe Result** (Risultato del probe) visualizza il risultato dell'esecuzione del probe delle applicazioni nelle ultime 24 ore. Fare clic sul collegamento dei risultati del probe per visualizzare ulteriori dettagli nella pagina **Trends** (Tendenze) > **Application Probe Results** (Risultati del probe delle applicazioni). Per ulteriori dettagli su come configurare i probe delle applicazioni e dei desktop, vedere Probe delle applicazioni e dei desktop.

La colonna **Instances** (Istanze) visualizza l'utilizzo delle applicazioni. Indica il numero di istanze delle applicazioni attualmente in esecuzione (istanze connesse e disconnesse). Per risolvere ulteriormente i problemi, fare clic sul campo **Instances** (Istanze) per visualizzare la pagina dei filtri **Application Instances** (Istanze dell'applicazione) corrispondente. Qui è possibile selezionare le istanze dell'applicazione da scollegare o disconnettere.

> **Nota:**
>
> Per gli amministratori di ambiti personalizzati, Director non visualizza le istanze delle applicazioni create in gruppi di applicazioni. Per visualizzare tutte le istanze dell'applicazione, è necessario essere un amministratore completo. Per ulteriori informazioni, vedere l'articolo CTX256001 del Knowledge Center.

Monitorare lo stato delle applicazioni pubblicate nel sito con le colonne **Application Faults** (Problemi delle applicazioni) e **Application Errors** (Errori delle applicazioni). Queste colonne visualizzano il numero aggregato di problemi ed errori che si sono verificati durante l'avvio dell'applicazione corrispondente nell'ultima ora. Fare clic sul campo **Application Faults** (Problemi delle applicazioni) o **Application Errors** (Errori delle applicazioni) per visualizzare i dettagli degli errori nella pagina

**Trends** (Tendenze) > **Application Failures** (Errori delle applicazioni) corrispondente all'applicazione selezionata.

Le impostazioni dei criteri degli errori delle applicazioni regolano la disponibilità e la visualizzazione di problemi ed errori. Per ulteriori informazioni sui criteri e su come modificarli, vedere Criteri per il monitoraggio degli errori delle applicazioni in **Impostazioni dei criteri di monitoraggio**.

## Monitoraggio delle applicazioni in tempo reale

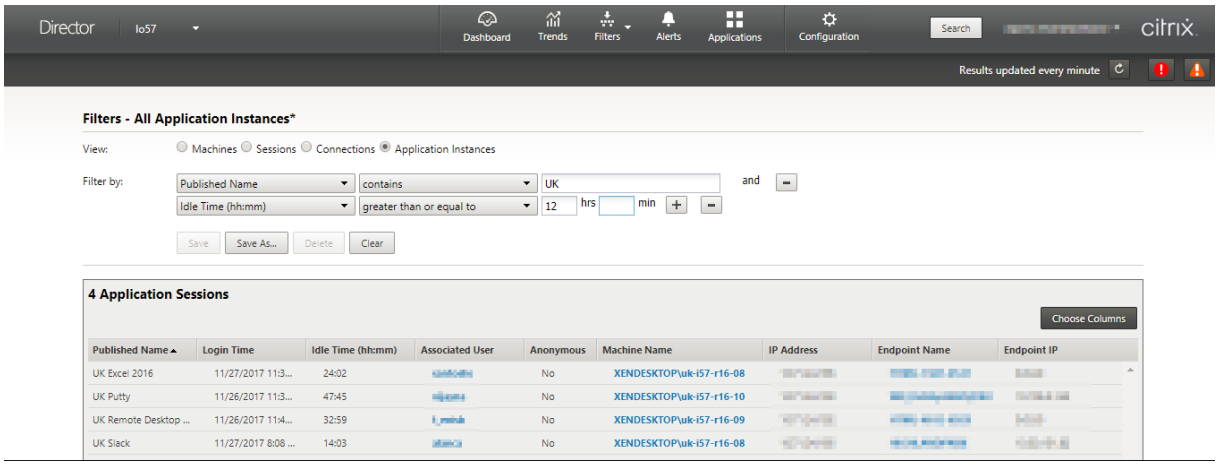
È possibile risolvere i problemi delle applicazioni e delle sessioni utilizzando la metrica relativa al tempo di inattività per identificare le istanze inattive oltre un limite di tempo specifico.

I casi d'uso tipici per la risoluzione dei problemi basati sulle applicazioni sono nel settore sanitario, dove i dipendenti condividono le licenze delle applicazioni. In questo caso è necessario terminare le sessioni inattive e le istanze delle applicazioni per ripulire l'ambiente Citrix Virtual Apps and Desktops, per riconfigurare server con prestazioni insoddisfacenti o per gestire e aggiornare le applicazioni.

La pagina dei filtri **Application Instances** (Istanze delle applicazioni) elenca tutte le istanze delle applicazioni sui VDA del server e con sistema operativo a sessione singola. Le misurazioni del tempo di inattività associate vengono visualizzate per le istanze delle applicazioni sui VDA con sistema operativo multisessione che sono rimasti inattivi per almeno 10 minuti.

> **Nota:**
> Le metriche Application Instances (Istanze delle applicazioni) sono disponibili sui siti di tutte le edizioni con licenza.

Utilizzare queste informazioni per identificare le istanze delle applicazioni inattive oltre un determinato periodo di tempo e per scollegarle o disconnetterle, a seconda dei casi. A tale scopo, selezionare **Filters (Filtri) > Application Instances (Istanze delle applicazioni)** e selezionare un filtro pre-salvato oppure scegliere **All Application Instances** (Tutte le istanze delle applicazioni) e creare un filtro personalizzato.

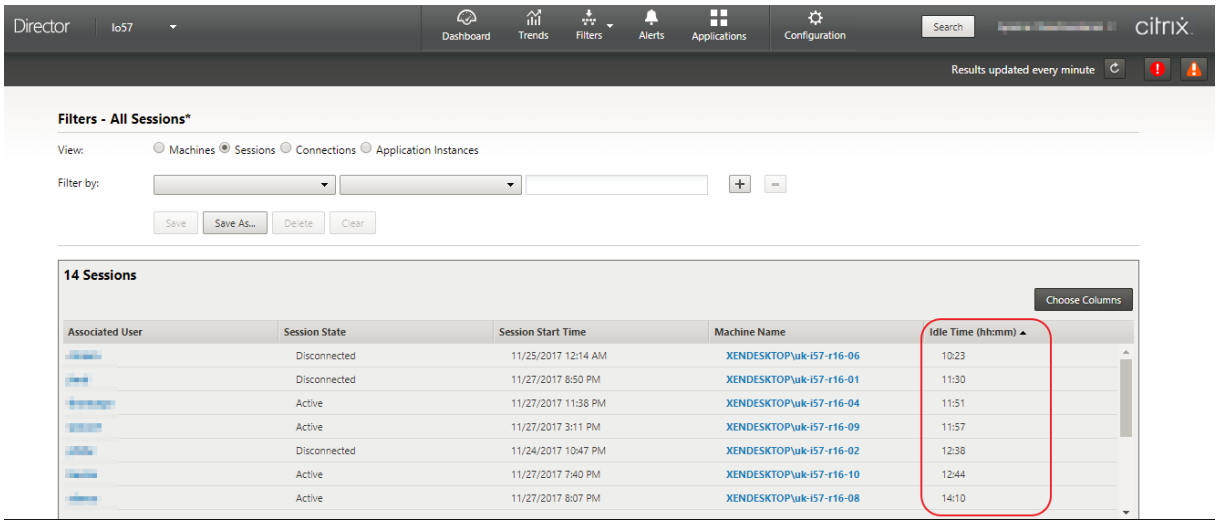


Un esempio di filtro è il seguente. Come criteri **Filter by** (Filtra per), scegliere **Published Name** (Nome pubblicato) dell'applicazione e **Idle Time** (Tempo di inattività). Quindi, impostare **Idle Time** (Tempo di inattività) su un valore **maggiore o uguale a** un limite di tempo specifico e salvare il filtro per riutilizzarlo. Dall'elenco filtrato, selezionare le istanze dell'applicazione. Selezionare l'opzione per inviare messaggi o scegliere **Logoff** (Scollega) o **Disconnect** (Disconnetti) dal menu a discesa **Session Control** (Controllo sessione) per terminare le istanze.

> **Nota:**
> Lo scollegamento o la disconnessione di un'istanza di un'applicazione scollega o disconnette la sessione corrente, terminando così tutte le istanze dell'applicazione appartenenti alla stessa sessione.

È possibile identificare le sessioni inattive dalla pagina dei filtri **Sessions** (Sessioni) utilizzando lo stato della sessione e la metrica relativa al tempo di inattività della sessione. Ordinare in base alla colonna **Idle Time** (Tempo di inattività) o definire un filtro per identificare le sessioni che sono inattive oltre un limite di tempo specifico. Il tempo di inattività è elencato per le sessioni sui VDA con sistema operativo multisessione che sono rimasti inattivi per almeno 10 minuti.




Il **tempo di inattività** viene visualizzato come **N/A** (N/D) quando la sessione o l'istanza dell'applicazione

- non è rimasta inattiva per più di 10 minuti,
- viene avviata su un VDA con sistema operativo a sessione singola oppure
- viene avviata su un VDA versione 7.12 o precedente.

### Monitoraggio storico degli errori delle applicazioni

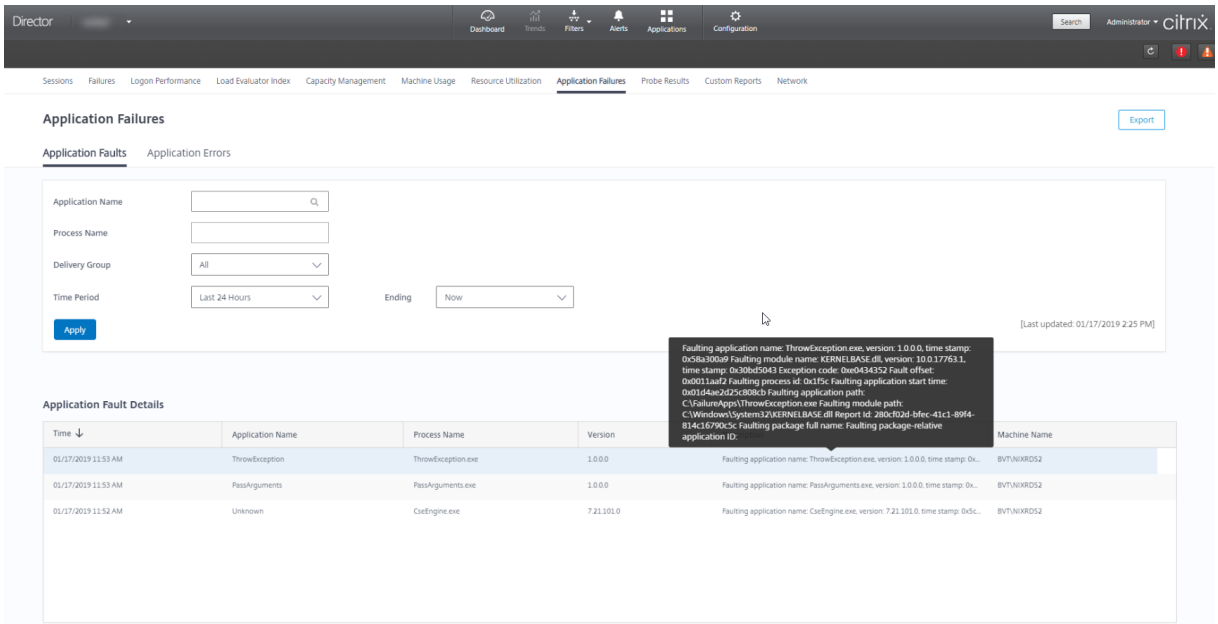
La scheda **Trends** (Tendenze) -> **Application Failures** (Errori delle applicazioni) visualizza gli errori associati alle applicazioni pubblicate sui VDA.

Le tendenze relative agli errori delle applicazioni sono disponibili per le ultime 2 ore, le ultime 24 ore, gli ultimi 7 giorni e l'ultimo mese per i siti con licenze Premium e Advanced. Sono disponibili per le ultime 2 ore, le ultime 24 ore e gli ultimi 7 giorni per gli altri tipi di licenze. Gli errori delle applicazioni registrati in Event Viewer (Visualizzatore eventi) con origine "Application errors"(Errori delle applicazioni) vengono monitorati. Fare clic su **Export** (Esporta) per generare report in formato CSV, Excel o PDF.

Le impostazioni di conservazione per la pulizia per il monitoraggio degli errori delle applicazioni, GroomApplicationErrorsRetentionDays e GroomApplicationFaultsRetentionDays, sono impostate su un giorno per impostazione predefinita per i siti con licenze Premium e non Premium. È possibile modificare questa impostazione utilizzando il comando PowerShell:

```
PowerShell command Set-MonitorConfiguration -\<setting name\> \<value
\> <!--NeedCopy-->
```




Gli errori vengono visualizzati come **Application Faults** (Problemi delle applicazioni) o **Application Errors** (Errori delle applicazioni) in base alla gravità. La scheda Application Faults (Problemi delle applicazioni) visualizza gli errori associati alla perdita di funzionalità o dati. La scheda Application Errors (Errori delle applicazioni) indica problemi che non sono immediatamente rilevanti e che indicano condizioni che potrebbero causare problemi futuri.

È possibile filtrare gli errori in base a **Published Application Name** (Nome dell'applicazione pubblicata), **Process Name** (Nome del processo) o **Delivery Group** (Gruppo di consegna) e **Time Period** (Periodo di tempo). La tabella mostra il codice del problema o dell'errore e una breve descrizione dell'errore. La descrizione dettagliata dell'errore viene visualizzata come una descrizione comando.

> **Nota:**
> Il nome dell'applicazione pubblicata viene visualizzato come "Unknown"(Sconosciuto) quando non è possibile derivare il nome dell'applicazione corrispondente. Questo si verifica in genere quando un'applicazione avviata presenta problemi in una sessione desktop o quando presenta problemi a causa di un'eccezione non gestita causata da un file eseguibile dipendente.

Per impostazione predefinita, vengono monitorati solo gli errori delle applicazioni ospitate su VDA con sistema operativo multisessione. È possibile modificare le impostazioni di monitoraggio tramite i criteri di gruppo di monitoraggio: Enable monitoring of application failures (Abilita il monitoraggio degli errori delle applicazioni), Enable monitoring of application failures on Single-session OS VDAs (Abilita il monitoraggio degli errori delle applicazioni sui VDA con sistema operativo a sessione singola) e List of applications excluded from failure monitoring (Elenco delle applicazioni escluse dal monitoraggio degli errori). Per ulteriori informazioni, vedere Criteri per il monitoraggio degli errori delle applicazioni nelle impostazioni dei criteri di monitoraggio.

La pagina **Trends** (Tendenze) **> Application Probe Results** (Risultati del probe delle applicazioni) visualizza i risultati dell'esecuzione del probe delle applicazioni nel sito per le ultime 24 ore e gli ultimi 7 giorni. Per ulteriori dettagli su come configurare i probe delle applicazioni, vedere Probe delle applicazioni.

## Risolvere i problemi relativi alle macchine

April 3, 2024

> **Nota:**
>
> **Citrix Health Assistant** è uno strumento per risolvere i problemi di configurazione nei VDA non registrati. Lo strumento automatizza diversi controlli dello stato per identificare le possibili cause principali degli errori di registrazione dei VDA e dei problemi relativi all'avvio della sessione e alla configurazione del reindirizzamento del fuso orario. L'articolo del Knowledge Center Citrix Health Assistant - Risolvere i problemi relativi alla registrazione dei VDA e all'avvio della sessione contiene le istruzioni per il download e l'uso dello strumento **Citrix Health Assistant**.

La vista **Filters (Filtri) > Machines (Macchine)** nella console di Director visualizza le macchine configurate nel sito. La scheda Multi-session OS Machines (Macchine con sistema operativo multisessione) include l'indice di valutazione del carico, che indica la distribuzione dei contatori delle prestazioni e le descrizioni dei comandi del conteggio delle sessioni se si passa il mouse sul collegamento.

Fare clic sulla colonna **Failure Reason** (Motivo dell'errore) di una macchina che presenta un problema per ottenere una descrizione dettagliata dell'errore e delle azioni consigliate per risolverlo. I motivi

degli errori e le azioni consigliate per gli errori delle macchine e delle connessioni sono disponibili in Cause di errori e risoluzione dei problemi di Citrix Director.

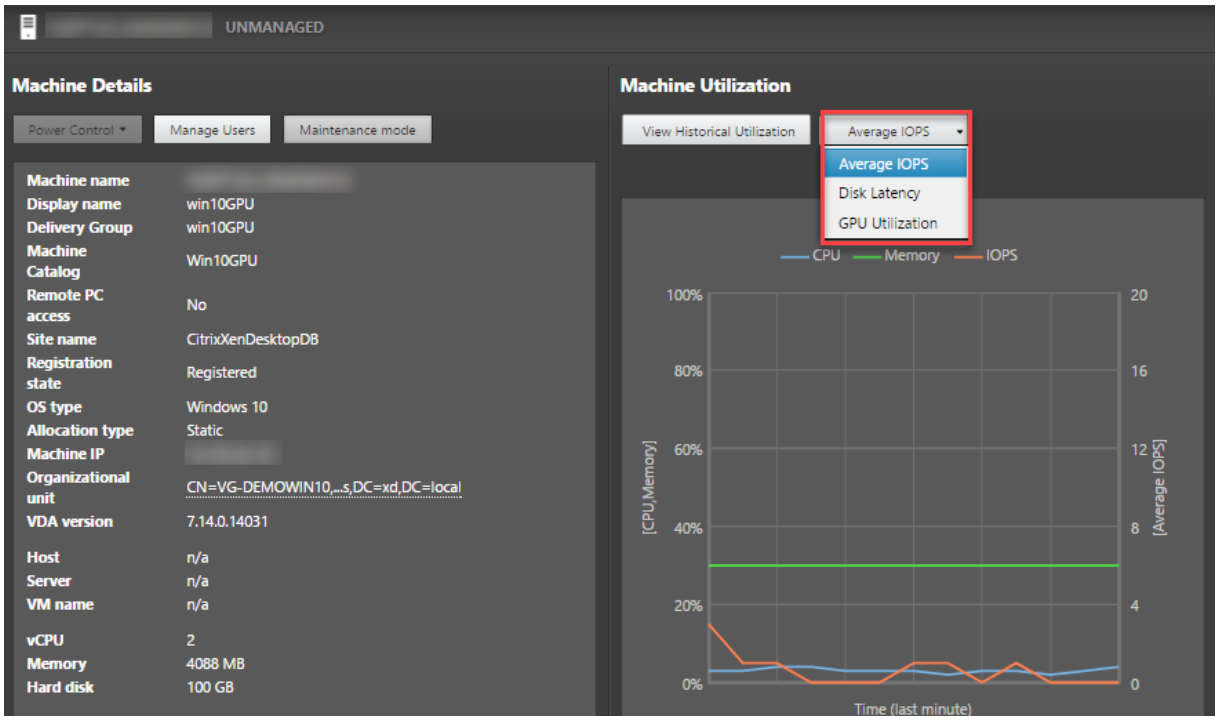
Fare clic sul collegamento del nome della macchina per andare alla pagina **Machine Details** (Dettagli macchina).

La pagina Machine Details (Dettagli macchina) elenca i dettagli della macchina, i dettagli dell'infrastruttura e i dettagli degli aggiornamenti rapidi applicati alla macchina.

### Utilizzo delle risorse in tempo reale basato sulla macchina

Il pannello **Machine Utilization** (Utilizzo macchina) visualizza grafici che mostrano l'utilizzo in tempo reale di CPU e memoria. Inoltre, i grafici relativi al monitoraggio del disco e della GPU sono disponibili per i siti con Delivery Controller e VDA versioni **7.14** o successive.

I grafici di monitoraggio del disco, gli IOPS medi e la latenza del disco sono importanti misurazioni delle prestazioni che consentono di monitorare e risolvere i problemi relativi ai dischi dei VDA. Il grafico Average IOPS (IOPS medi) visualizza il numero medio di letture e scritture su un disco. Selezionare **Disk Latency** (Latenza del disco) per visualizzare un grafico del ritardo tra una richiesta di dati e il relativo ritorno dal disco, misurato in millisecondi.



### Utilizzo della GPU

Selezionare **GPU Utilization** (Utilizzo della GPU) per visualizzare la percentuale di utilizzo della GPU, della memoria della GPU, del codificatore e del decodificatore per risolvere i problemi relativi alla GPU sui VDA con sistema operativo multisessione o a sessione singola.

**Versioni di GPU supportate:**

- GPU NVIDIA Tesla M60 con Display Driver versione 369.17 o successiva. Per ulteriori informazioni, vedere NVIDIA vGPU Software.
- CPU AMD Radeon Instinct MI25 GPUs e AMD EPYC 7V12(Rome). Per ulteriori informazioni, vedere AMD Drivers and Support.

**Driver:**

Sui VDA devono essere installati i driver o le estensioni appropriati.

- Per le GPU NVIDIA, installare i driver GRID manualmente o tramite estensioni. Per ulteriori informazioni, vedere NVIDIA vGPU Software.
  - Si noti che per NVIDIA sono supportati solo i driver GRID. I driver CUDA non funzionano con la serie NVadsA10 v5 e non sono supportati.
  - Per un processo di esempio di installazione dei driver GPU Nvidia Grid tramite estensioni su macchine basate su Azure, vedere Driver NVIDIA GRID. Estensione del driver GPU NVIDIA - VM Windows di Azure - Macchine virtuali di Azure.
  - Per un processo di esempio di installazione manuale dei driver GPU Nvidia Grid, vedere Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines.
- Per le GPU AMD, installare i driver grafici AMD manualmente o tramite estensioni. Per ulteriori informazioni, vedere AMD Drivers and Support.
  - Per un processo di esempio dell'installazione dei driver GPU AMD tramite estensioni su macchine basate su Azure, vedere AMD GPU Driver Extension - Azure Windows VMs - Macchine virtuali di Azure.
  - Per un processo di esempio dell'installazione manuale dei driver GPU AMD su macchine Azure, vedere Install AMD GPU drivers on N-series VMs running Windows.

**Note d'uso:**

- I grafici di utilizzo della GPU sono disponibili solo per i VDA che eseguono Windows a 64 bit.
- Sui VDA deve essere abilitato HDX 3D Pro per fornire l'accelerazione della GPU. Per ulteriori informazioni, vedere Accelerazione GPU per sistema operativo Windows a sessione singola e Accelerazione GPU per sistema operativo multisessione Windows.
- Quando un VDA accede a più di una GPU, il grafico di utilizzo visualizza la media delle metriche della GPU raccolte dalle singole GPU. Le metriche della GPU vengono raccolte per l'intero VDA e non per i singoli processi.

- Per AMD, l'utilizzo di encoder e decoder non è supportato separatamente. Qualsiasi carico di lavoro di codifica/decodifica che utilizza la GPU verrà segnalato come carico 3D generale sull'utilizzo della GPU.
- Assicurarsi di installare la WMI NVIDIA durante l'installazione. Questa finestra è disponibile solo durante l'installazione manuale.
- Se i driver sono installati ma Director non rileva la GPU
  - Controllare Task Manager (Gestione attività). Se i driver sono installati correttamente, la GPU dovrebbe essere visualizzata in Task Manager.
  - Controllare se la macchina è registrata. A volte può trascorrere del tempo prima che sia rilevata la presenza online delle macchine.
- Se l'utilizzo della GPU non mostra alcuna attività in Director, assicurarsi che il carico di lavoro in esecuzione utilizzi la GPU. Per i carichi di lavoro grafici, questo può essere abilitato da Impostazioni > Sistema > Schermo > Impostazioni grafiche > scegliere l'app di cui impostare le preferenze. Assicurarsi di attivare le prestazioni elevate. A volte, Windows utilizza per impostazione predefinita la CPU per i carichi di lavoro grafici quando questa è impostata sui valori predefiniti del sistema o sul risparmio energetico, in base ad altre impostazioni.
- I dati vengono aggiornati ogni minuto e la visualizzazione dei dati inizia entro un minuto dalla selezione di **GPU Utilization**.

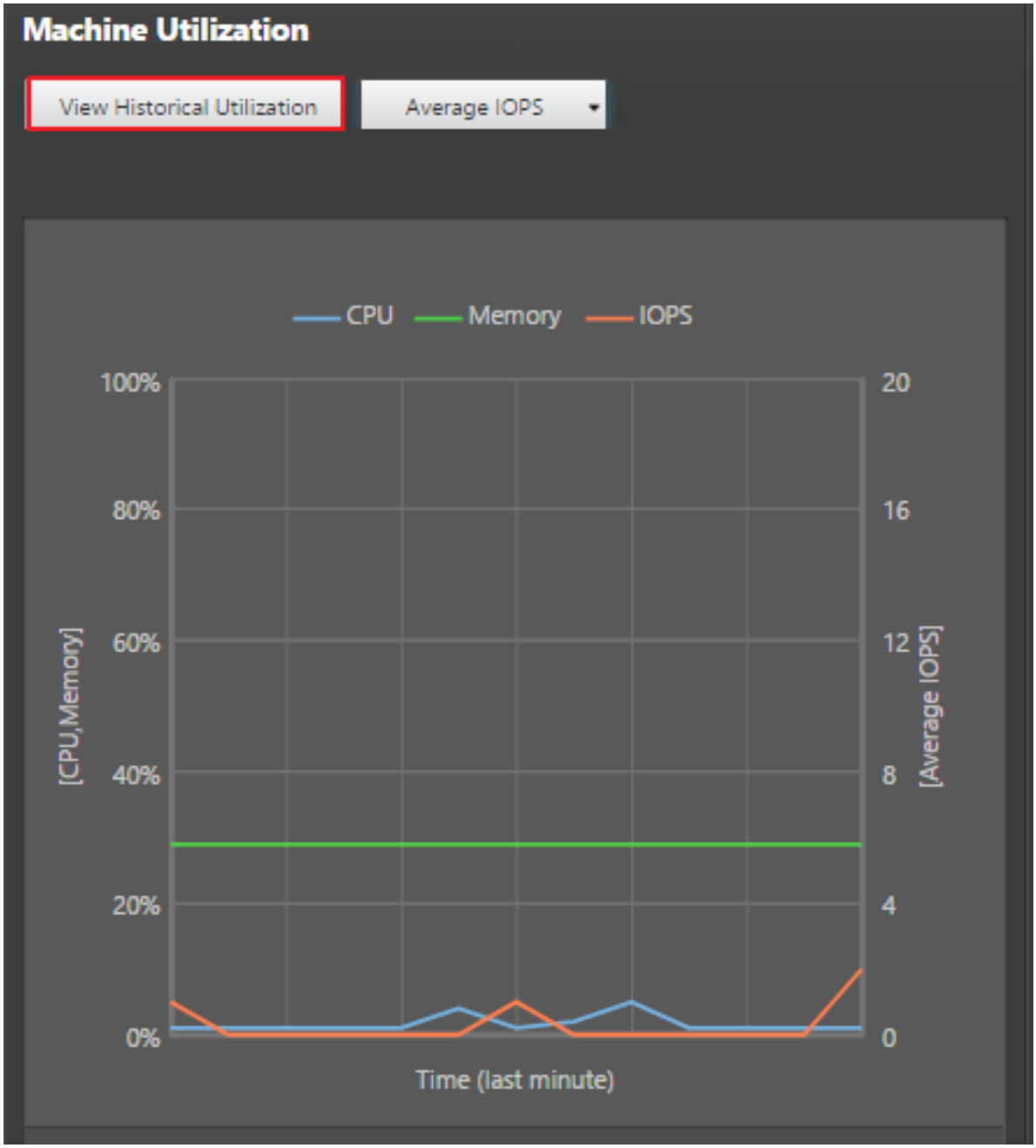
### Utilizzo storico delle risorse basato sulla macchina

Nel pannello **Machine Utilization** (Utilizzo macchina), fare clic su **View Historical Utilization** (Visualizza utilizzo storico) per visualizzare l'utilizzo storico delle risorse sulla macchina selezionata.
I grafici di utilizzo includono contatori critici delle prestazioni di CPU, memoria, sessioni simultanee di picco, IOPS medio e latenza del disco.

> **Nota:**
>
> L'impostazione dei criteri di monitoraggio **Enable Process Monitoring**(Abilita monitoraggio processo) deve essere impostata su Allowed (Consentito) per raccogliere e visualizzare i dati nella tabella Top 10 Processes (Primi 10 processi) della pagina Historic Machine Utilization (Utilizzo storico della macchina). La raccolta è vietata per impostazione predefinita.

I dati relativi all'utilizzo della CPU e della memoria, agli IOPS medi e alla latenza del disco vengono raccolti per impostazione predefinita. È possibile disabilitare la raccolta utilizzando l'impostazione dei criteri **Enable Resource Monitoring** (Abilita monitoraggio delle risorse).



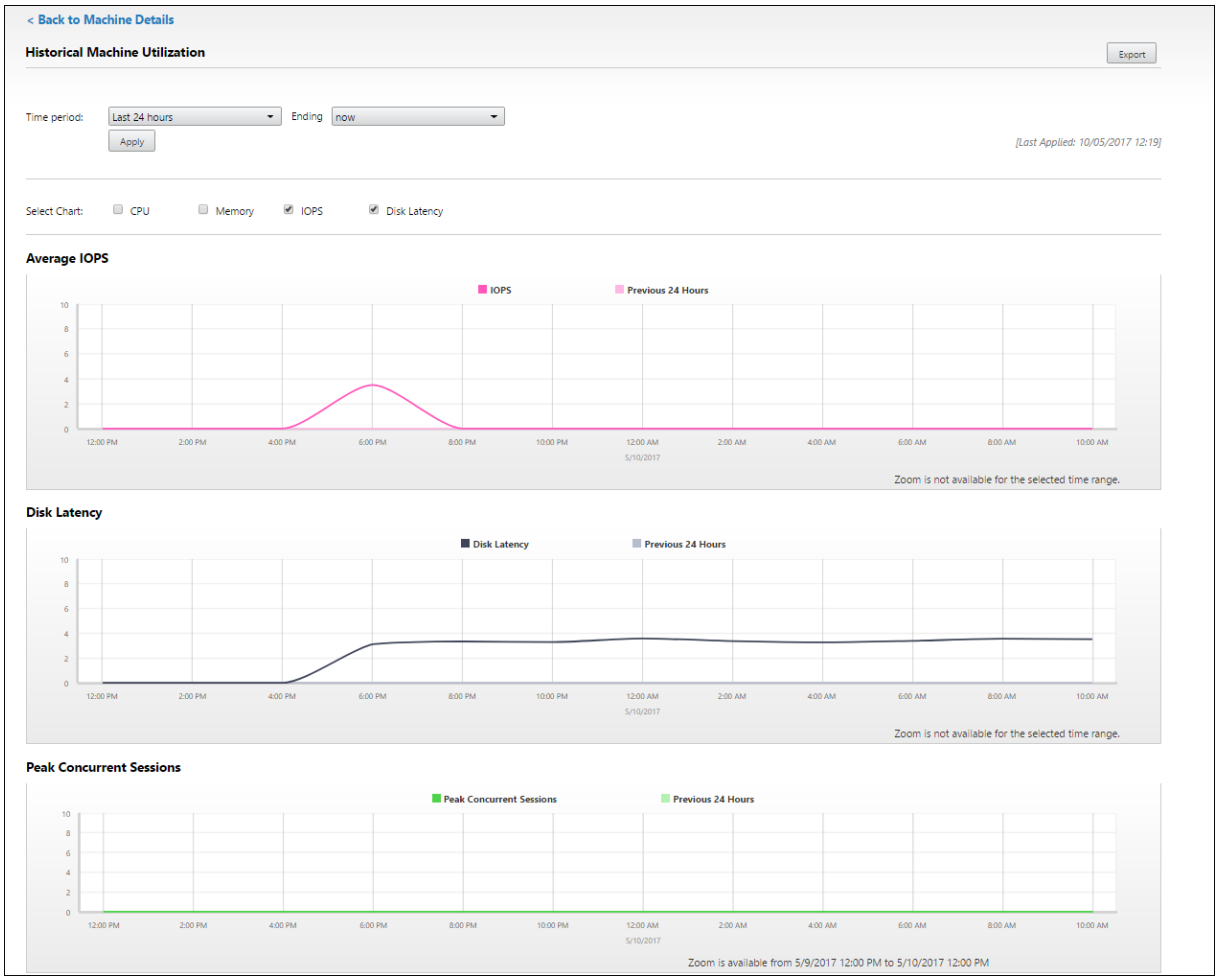

1. Dal pannello **Machine Utilization** (Utilizzo macchina) nella vista **Machine Details** (Dettagli macchina), selezionare **View Historical Utilization** (Visualizza utilizzo storico).
2. Nella pagina **Historical Machine Utilization** (Utilizzo storico della macchina), impostare **Time Period** (Periodo di tempo) per visualizzare l'utilizzo nelle ultime 2 ore, nelle ultime 24 ore, negli ultimi 7 giorni, nell'ultimo mese o nell'ultimo anno.

> **Nota:**
>
> I dati medi di utilizzo degli IOPS e della latenza del disco sono disponibili solo per le ultime

> 24 ore, l'ultimo mese e l'anno corrente. L'ora di fine personalizzata non è supportata.

3. Fare clic su **Apply** (Applica) e selezionare i grafici richiesti.
4. Passare il mouse sulle diverse sezioni del grafico per visualizzare ulteriori informazioni per il periodo di tempo selezionato.




Ad esempio, se si seleziona **Last 2 hours** (Ultime 2 ore), il periodo di base sono le 2 ore precedenti l'intervallo di tempo selezionato. Visualizzare le tendenze della CPU, della memoria e della sessione nelle ultime 2 ore e all'ora di base. Se si seleziona **Last month** (Ultimo mese), il periodo di base è il mese precedente. Selezionare questa opzione per visualizzare gli IOPS e la latenza del disco medi nell'ultimo mese e all'ora di base.

1. Fare clic su **Export** (Esporta) per esportare i dati di utilizzo delle risorse per il periodo selezionato. Per ulteriori informazioni, vedere la sezione Esportare i report nella sezione di monitoraggio delle distribuzioni.
2. Sotto i grafici, la tabella elenca i primi 10 processi in base all'utilizzo della CPU o della memoria. È possibile ordinare i dati in base a una qualsiasi delle colonne, che mostrano Application Name

(Nome applicazione), User Name (Nome utente), Session ID (ID sessione), Average CPU (CPU media), Peak CPU (CPU di picco), Average Memory (Memoria media) e Peak Memory (Memoria di picco) nell'intervallo di tempo selezionato. Le colonne IOPS e Disk Latency (Latenza del disco) non possono essere ordinate.

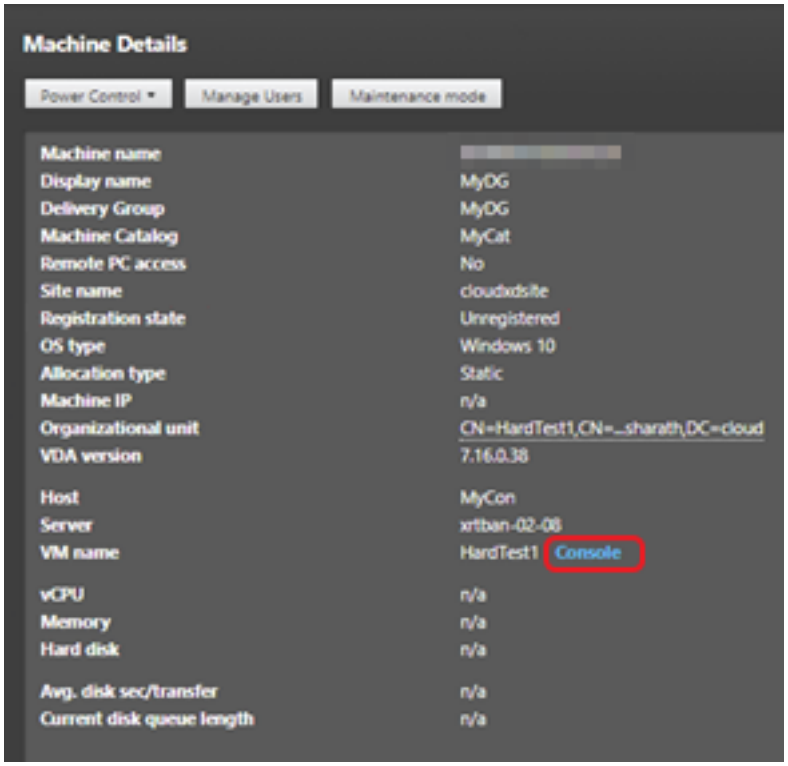
> **Nota:**
>
> L'ID di sessione per i processi di sistema viene visualizzato come "0000".

3. Per visualizzare la tendenza storica sul consumo di risorse di un determinato processo, eseguire il drill down di uno dei primi 10 processi.

### Accesso alla console della macchina

È possibile accedere alle console delle macchine con sistema operativo a sessione singola e multisessione ospitati su XenServer versione 7.3 e successive direttamente da Director. In questo modo non è necessario che XenCenter risolva i problemi sui VDA ospitati da XenServer. Per rendere disponibile questa funzionalità:

- È richiesto Delivery Controller versione 7.16 o successiva.
- La versione dell'istanza di XenServer che ospita la macchina deve corrispondere a 7.3 o successiva e deve essere accessibile dall'interfaccia utente di Director.



Per risolvere i problemi di una macchina, fare clic sul collegamento **Console** nel pannello Machine Details (Dettagli macchina) corrispondente. Dopo l'autenticazione delle credenziali host fornite, la console della macchina si apre in una scheda separata utilizzando noVNC, un client VNC basato sul Web. Ora si ha accesso alla console con tastiera e mouse.

> **Nota:**
>
> - Questa funzionalità non è supportata su Internet Explorer 11.
> - Se il puntatore del mouse sulla console della macchina non è allineato, vedere la procedura di risoluzione del problema in CTX230727.
> - Director avvia l'accesso alla console in una nuova scheda, assicurando che le impostazioni del browser consentano le finestre a comparsa.
> - Per motivi di sicurezza, Citrix consiglia di installare certificati SSL sul browser.

### Stato licenza Servizi Desktop remoto Microsoft

È possibile visualizzare lo stato della licenza Servizi Desktop remoto Microsoft nel pannello Machine Details (Dettagli macchina) nella pagina **Machine Details** (Dettagli macchina) e nella pagina **User Details** (Dettagli utente) per macchine con sistema operativo multisessione.


Viene visualizzato uno dei seguenti messaggi:

- License available (Licenza disponibile)
- Not configured properly (warning) (Non configurato correttamente [avviso])
- License error (error) (Errore di licenza [errore])
- Incompatible VDA version (error) (Versione VDA incompatibile [errore])

> **Nota:**
>
> Lo stato di integrità della licenza Servizi Desktop remoto per le macchine sottoposte a periodo di tolleranza con licenza valida visualizza un messaggio **License available** (Licenza disponibile) in

> verde. Rinnovare la licenza prima della scadenza.

Per i messaggi di avviso e di errore, passare il mouse sull'icona delle informazioni per visualizzare informazioni aggiuntive come indicato nella tabella seguente.

| Tipo di messaggio | Messaggi in Director |
|---|---|
| Errore | Disponibile per VDA versione 7.16 e successive. |
| Errore | Non sono consentite nuove connessioni RDS. |
| Errore | La licenza Servizi Desktop remoto ha superato il periodo di tolleranza. |
| Errore | Un License Server non è configurato per il livello di sistema operativo richiesto con il tipo di licenza Accesso client per dispositivo. |
| Errore | Il License Server configurato non è compatibile con il livello del sistema operativo host di Servizi Desktop remoto con il tipo di licenza Accesso client per dispositivo. |
| Avviso | Terminal Server personale non è un tipo di licenza Servizi Desktop remoto valido in una distribuzione Citrix Virtual Apps and Desktops. |
| Avviso | Desktop remoto per amministrazione non è un tipo di licenza valido in una distribuzione Citrix Virtual Apps and Desktops. |
| Avviso | Un tipo di licenza Servizi Desktop remoto non è configurato. |
| Avviso | Il controller di dominio o License Server non è raggiungibile con il tipo di licenza Servizi Desktop remoto Accesso client per utente. |
| Avviso | Con il tipo di licenza Accesso client per dispositivo, la licenza del dispositivo client non può essere determinata poiché il server delle licenze per il livello di sistema operativo richiesto non è raggiungibile. |

> **Nota:**
>
> Questa funzionalità è applicabile solo per CAL (licenza di accesso client) di Servizi Desktop remoto Microsoft.

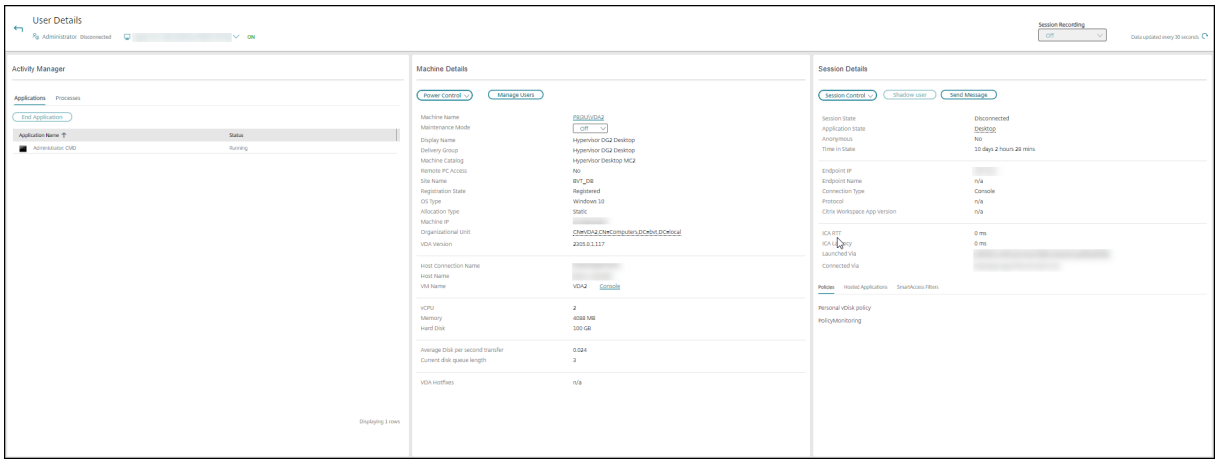
 

# Risolvere i problemi dell'utente

January 7, 2024

Utilizzare la vista **Help Desk** (Helpdesk) di Director (pagina**Activity Manager** [Gestione attività]) per visualizzare le informazioni sull'utente o la sessione:


Facendo clic su **View Details** dall'Activity Manager relativa a un utente, si apre la pagina **User Details** (Dettagli utente).
Facendo clic su **Dettagli utente** dall'Activity Manager di un endpoint, si apre la pagina **Endpoint Details** (Dettagli dell'endpoint).




Se l'utente ha avviato più sessioni, il selettore di sessione aiuta a selezionare una sessione.


Scegliere una sessione per visualizzarne i dettagli.

- È possibile controllare dettagli sulla sessione, l'esperienza di accesso dell'utente, l'avvio della sessione, la connessione e le applicazioni.
- È possibile oscurare la macchina dell'utente.
- Registrare la sessione ICA.
- Risolvere il problema con le azioni consigliate nella tabella seguente e, se necessario, segnalare il problema all'amministratore appropriato.

### Suggerimenti per la risoluzione dei problemi

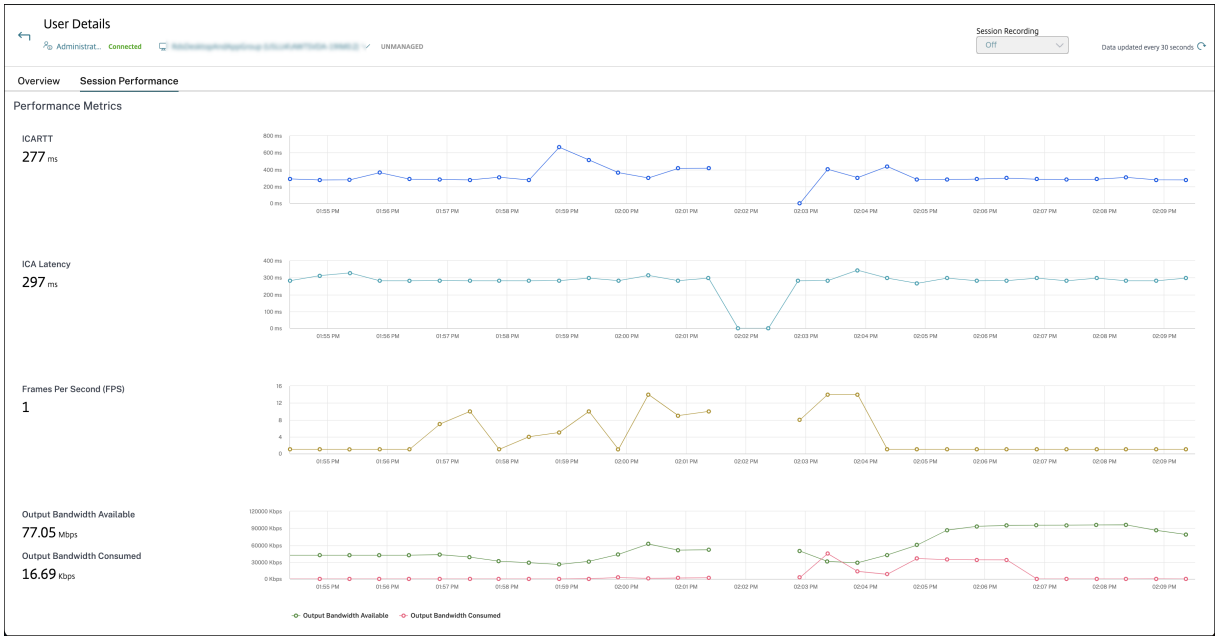
| Problema dell'utente | Suggerimenti |
|---|---|
| L'accesso richiede molto tempo o non riesce in modo intermittente o ripetuto | Diagnosticare i problemi di accesso utente |
| L'avvio della sessione richiede molto tempo o non riesce in modo intermittente o ripetuto | Diagnosticare i problemi di avvio |
| L'applicazione è lenta o non risponde | Risolvere gli errori delle applicazioni |
| Connessione non riuscita | Ripristinare le connessioni desktop |
| La sessione è lenta o non risponde | Ripristinare le sessioni |
| Registrare le sessioni | Registrare le sessioni |
| Il video è lento o di scarsa qualità | Eseguire report sui sistemi di canale HDX |

> **Nota:**
> Per assicurarsi che la macchina non sia in modalità di manutenzione, dalla vista User Details (Dettagli utente) esaminare il riquadro Machine details (Dettagli macchina).

### Tendenze per le metriche delle prestazioni delle sessioni

La scheda **Session Performance** (Prestazioni della sessione) ha migliorato i flussi di lavoro per la risoluzione dei problemi, a partire dalla capacità di correlare le metriche in tempo reale per identificare i problemi all'interno delle sessioni utente. Le tendenze delle metriche di sessione quali ICARTT (Tempo di round trip ICA), ICA Latency (Latenza ICA), Frames Per Second (Fotogrammi per secondo), Output Bandwidth Available (Larghezza di banda in uscita disponibile) e Output Bandwidth Consumed (Larghezza di banda in uscita consumata) aiutano a indicare come queste metriche si sono comportate nel tempo.




> **Nota:**
> il grafico viene tracciato solo per la durata di tempo in cui la sessione è connessa.

**ICARTT**: ICARTT è l'intervallo di tempo tra l'azione di un utente e la risposta grafica visualizzata sul suo schermo.

**ICA Latency**: la latenza ICA è fondamentalmente la latenza della rete. Questo parametro indica se la rete è lenta.

**Frames Per Second**: i fotogrammi al secondo sono una metrica importante che indica la reattività della sessione.

**Output Bandwidth Available**: la larghezza di banda in uscita disponibile è una misura della larghezza di banda totale disponibile per trasmettere dati dal VDA all'endpoint.

**Output Bandwidth Consumed**: la larghezza di banda in uscita consumata indica la quantità effettiva di dati trasmessi dal VDA all'endpoint per visualizzare le sessioni agli utenti.

L'analisi della larghezza di banda in uscita disponibile e della larghezza di banda in uscita consumata aiuta a verificare se è disponibile una larghezza di banda sufficiente per servire le sessioni e a rilevare se una sessione soffre di una larghezza di banda insufficiente.

Questa funzionalità consente di unire più metriche di prestazione in un'unica visualizzazione e riduce il tempo medio per la risoluzione dei problemi di esperienza della sessione.

## Suggerimenti di ricerca

Quando si digita il nome dell'utente in un campo di ricerca, Director cerca gli utenti in Active Directory per gli utenti di tutti i siti configurati per supportare Director.

Quando si digita il nome di una macchina multiutente in un campo di ricerca, Director visualizza i dettagli della macchina per la macchina specificata.

Quando si digita il nome di un endpoint in un campo di ricerca, Director utilizza le sessioni non autenticate (anonime) e autenticate connesse a un endpoint specifico, il che consente la risoluzione dei problemi delle sessioni non autenticate. Assicurarsi che i nomi degli endpoint siano univoci per abilitare la risoluzione dei problemi delle sessioni non autenticate.

I risultati di ricerca includono anche utenti che attualmente non utilizzano una macchina o non sono assegnati a una macchina.

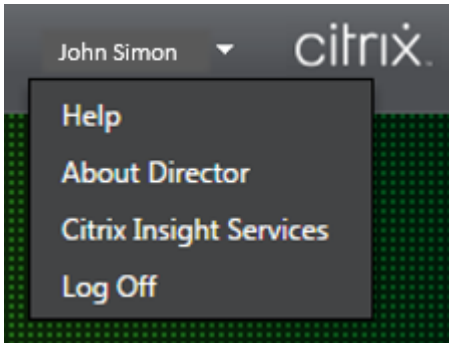
- Le ricerche non fanno distinzione tra maiuscole e minuscole.
- Le voci parziali generano un elenco di possibili corrispondenze.
- Dopo aver digitato alcune lettere di un nome in due parti (nome utente, cognome e nome o nome visualizzato) separate da uno spazio, i risultati includono corrispondenze per entrambe le stringhe. Ad esempio, se si digita jo rob, i risultati potrebbero includere stringhe come "John Robertson"o "Robert, Jones".

Per tornare alla pagina di destinazione, fare clic sul **logo di Director**.

## Accedere a Citrix Insight Services

È possibile accedere a Citrix Insight Services (CIS) dall'elenco a discesa **User** (Utente) in Director per accedere a ulteriori informazioni diagnostiche. I dati disponibili in CIS provengono da fonti che comprendono Call Home e Citrix Scout.




**Caricare le informazioni sulla risoluzione dei problemi per il team del supporto tecnico Citrix**

Eseguire Citrix Scout da un singolo Delivery Controller o VDA per acquisire punti dati chiave e tracce Citrix Diagnostics Facility (CDF) per risolvere i problemi dei computer selezionati. Scout offre la possibilità di caricare in modo sicuro i dati sulla piattaforma CIS per assistere il supporto tecnico Citrix nella risoluzione dei problemi. Il supporto tecnico Citrix utilizza la piattaforma CIS per ridurre il tempo necessario per risolvere i problemi segnalati dai clienti.

Scout viene installato con i componenti di Citrix Virtual Apps and Desktops. A seconda della versione di Windows, Scout viene visualizzato nel menu Start di Windows o nella schermata iniziale quando si installa Citrix Virtual Apps and Desktops o se ne esegue l'aggiornamento.

Per avviare Scout, dal menu Start o dalla schermata iniziale selezionare Citrix > Citrix Scout.

Per informazioni sull'utilizzo e la configurazione di Scout e le domande frequenti, consultare CTX130147.

## Diagnosticare i problemi di avvio

January 7, 2024

Oltre alle fasi del processo di accesso menzionate nella sezione Diagnosticare i problemi di accesso degli utenti, Director visualizza la durata di avvio della sessione. Questa è suddivisa nella durata Workspace App Session Startup (Avvio della sessione dell'app Workspace) e VDA Session Startup (Avvio della sessione VDA) nella pagina **User Details** (Dettagli utente) e nelle pagine **Machine Details** (Dettagli macchina). Queste due durate contengono inoltre singole fasi di cui vengono visualizzate le durate dell'avvio. Questi dati aiutano a comprendere e risolvere i problemi di durata elevata dell'avvio delle sessioni. Inoltre, la durata di ogni fase coinvolta nell'avvio della sessione aiuta a risolvere i problemi associati alle singole fasi. Ad esempio, se il tempo di mappatura dell'unità è elevato, è possibile verificare se tutte le unità valide sono mappate correttamente nell'oggetto Criteri di gruppo o nello

script. Questa funzionalità è disponibile su Delivery Controller versione 7 1906 e successive e VDA 1903 e versioni successive.

### Prerequisiti

Assicurarsi che siano soddisfatti i seguenti prerequisiti perché vengano visualizzati i dati relativi alla durata dell'avvio delle sessioni:

- Delivery Controller 7 1906 o versioni successive.
- VDA 1903 o versioni successive.
- Il servizio Citrix End User Experience Monitoring (EUEM) deve essere in esecuzione sul VDA.

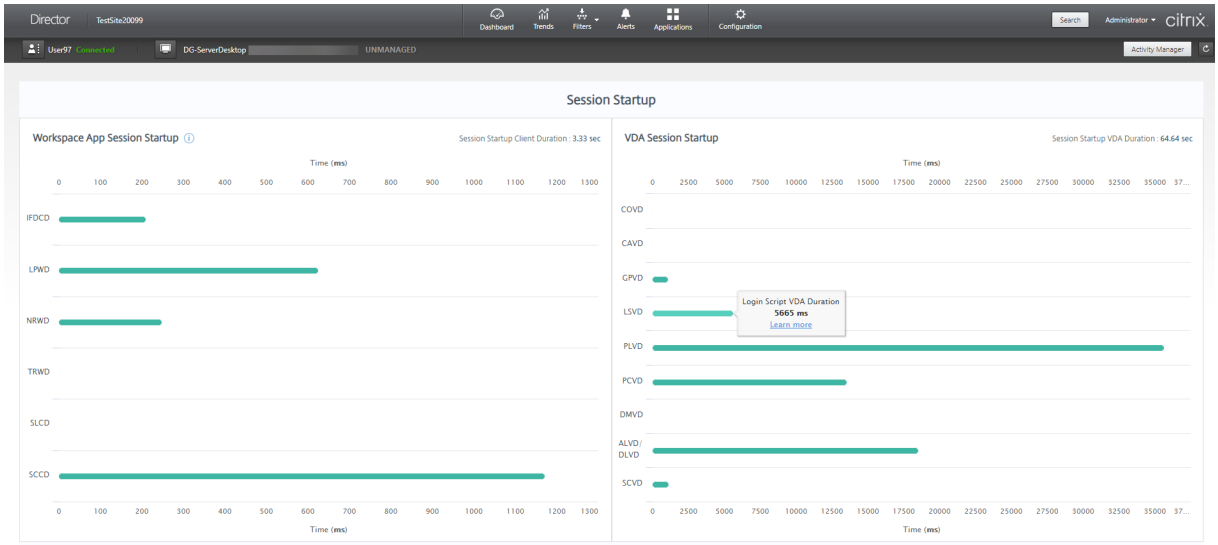
### Limiti

Le seguenti limitazioni si applicano quando Director visualizza i dati relativi alla durata dell'avvio delle sessioni.

- La durata dell'avvio delle sessioni è disponibile solo per le sessioni HDX.
- Per gli avvii delle sessioni da iOS e Android OS, è disponibile solo la durata dell'avvio VDA.
- IFDCD è disponibile solo quando viene rilevata l'app Workspace durante l'avvio da un browser.
- Per gli avvii delle sessioni da macOS, IFDCD è disponibile solo per l'app Workspace 1902 o versioni successive.
- Per gli avvii delle sessioni dal sistema operativo Windows, IFDCD è disponibile per l'app Workspace 1902 e versioni successive. Per le versioni precedenti, IFDCD viene visualizzato solo per gli avvii di app dal browser con l'app Workspace rilevata.

> **Note:**
>
> - Se si riscontrano problemi di visualizzazione della durata di avvio delle sessioni dopo aver soddisfatto i prerequisiti, visualizzare i log del server Director e del VDA come descritto in CTX130320.
>
>  Per le sessioni condivise (più applicazioni avviate nella stessa sessione), vengono visualizzate le metriche di avvio dell'app Workspace per la connessione più recente o l'avvio dell'applicazione più recente.
> - Alcune metriche in VDA Session Startup (Avvio della sessione VDA) non sono applicabili alle riconnessioni. In questi casi, viene visualizzato un messaggio.




## Fasi di avvio delle sessioni dell'app Workspace

### Session Startup Client Duration (SSCD) (Durata del client di avvio della sessione [SSCD])

Quando questa metrica è alta, indica un problema lato client che causa lunghi tempi di avvio. Esaminare le metriche successive per determinare la probabile causa principale del problema. SSCD inizia il più vicino possibile all'ora della richiesta (clic del mouse). Termina quando è stata stabilita la connessione ICA tra il dispositivo client e il VDA. Nel caso di una sessione condivisa, questa durata è molto inferiore, poiché gran parte dei costi di configurazione associati alla creazione di una nuova connessione al server non vengono sostenuti. Al livello successivo, sono disponibili diverse metriche dettagliate.

### ICA File Download Duration (IFDCD) (Durata del download del file ICA [IFDCD])

Questo è il tempo necessario perché il client esegua il download del file ICA dal server. Il processo generale è il seguente:

1. L'utente fa clic su una risorsa (applicazione o desktop) nell'applicazione Workspace.
2. Una richiesta dell'utente viene inviata allo StoreFront tramite Citrix Gateway (se configurato), che invia la richiesta al Delivery Controller.
3. Il Delivery Controller trova una macchina disponibile per la richiesta e invia le informazioni sulla macchina e altri dettagli a StoreFront. Inoltre, StoreFront richiede e riceve un ticket una tantum dalla Secure Ticket Authority.
4. StoreFront genera un file ICA e lo invia all'utente tramite Citrix Gateway (se configurato).

IFDCD rappresenta il tempo necessario per il processo completo (passaggi 1-4). La durata IFDCD interrompe il conteggio quando il client riceve il file ICA.

LPWD è il componente StoreFront del processo.

Se il valore IFDCD è alto (ma LPWD è normale), l'elaborazione sul lato server dell'avvio è riuscita, ma si sono verificati dei problemi di comunicazione tra il dispositivo client e StoreFront. Questo deriva da problemi di rete tra le due macchine. In questo modo è possibile risolvere prima i problemi di rete potenziali.

#### Launch Page Web Server Duration (LPWD) (Durata del server Web della pagina di avvio [LPWD])

Questo è il tempo necessario per elaborare la pagina di avvio (launch.aspx) su StoreFront. Se il valore LPWD è alto, potrebbe esserci un collo di bottiglia su StoreFront.

Le possibili cause includono:

- Carico elevato su StoreFront. Cercare di identificare la causa del rallentamento controllando i log di Internet Information Services (IIS) e gli strumenti di monitoraggio, Gestione attività, Monitoraggio prestazioni e così via.
- StoreFront sta riscontrando problemi di comunicazione con altri componenti come il Delivery Controller. Controllare se la connessione di rete tra StoreFront e Delivery Controller è lenta o alcuni Delivery Controller sono inattivi o sovraccarichi.

#### Name Resolution Web Server Duration (NRWD) (Durata del server Web con risoluzione dei nomi [NRWD])

Questo è il tempo impiegato dal Delivery Controller per risolvere il nome di un'applicazione pubblicata/desktop in un indirizzo IP della macchina VDA.

Quando questa metrica è alta, indica che il Delivery Controller sta impiegando molto tempo per risolvere il nome di un'applicazione pubblicata in un indirizzo IP.

Le possibili cause includono un problema del client, problemi con il Delivery Controller, come il sovraccarico del Delivery Controller, o un problema con il collegamento di rete tra i due.

#### Ticket Response Web Server Duration (TRWD) (Durata del server Web di risposta del ticket [TRWD])

Questa durata indica il tempo necessario per ottenere un ticket (se necessario) dal server Secure Ticket Authority (STA) o dal Delivery Controller. Quando questa durata è elevata, indica che il server STA o il Delivery Controller sono sovraccarichi.

#### Session Look-up Client Duration (SLCD) (Durata del client di ricerca della sessione [SLCD])

Questa durata rappresenta il tempo necessario per interrogare ogni sessione per ospitare l'applicazione pubblicata richiesta. Il controllo viene eseguito sul client per determinare se una sessione esistente può gestire la richiesta di avvio dell'applicazione. Il metodo utilizzato dipende dal fatto che la sessione sia nuova o condivisa.

#### Session Creation Client Duration (SCCD) (Durata del client di creazione della sessione [SCCD])

Questa durata rappresenta il tempo necessario per creare una sessione, dal momento in cui wfica32.exe (o un file equivalente simile) viene avviato al momento in cui viene stabilita la connessione.

### Fasi di avvio della sessione VDA

#### Session Startup VDA Duration (SSVD) (Durata del VDA di avvio della sessione [SSVD])

Questa durata è la metrica di avvio della connessione lato server di alto livello che include il tempo impiegato dal VDA per eseguire l'intera operazione di avvio. Quando questa metrica è alta, indica che è presente un problema del VDA che aumenta i tempi di avvio della sessione. Questo include il tempo impiegato sul VDA per eseguire l'intera operazione di avvio.

#### Credentials Obtention VDA Duration (COVD) (Durata del VDA per l'ottenimento delle credenziali [COVD])

Il tempo impiegato dal VDA per ottenere le credenziali utente.

Questa durata può aumentare artificialmente se un utente non riesce a fornire le credenziali in modo tempestivo. Pertanto, non è inclusa nella durata di avvio del VDA. È probabile che questa durata sia significativa solo se viene utilizzato l'accesso manuale e viene visualizzata la finestra di dialogo delle credenziali lato server (o se viene visualizzata una nota legale prima dell'inizio dell'accesso).

#### Credentials Authentication VDA Duration (CAVD) (Durata del VDA per l'autenticazione delle credenziali [CAVD])

Questo è il tempo impiegato dal VDA per autenticare le credenziali dell'utente confrontandole con il provider di autenticazione. Può trattarsi di Kerberos, Active Directory o SSPI (Security Support Provider Interface).

**Group Policy VDA Duration (GPVD) (Durata del VDA per i Criteri di gruppo [GPVD])**

Questa durata è il tempo necessario per applicare gli oggetti Criteri di gruppo durante l'accesso.

**Login Script Execution VDA Duration (LSVD) (Durata del VDA di esecuzione dello script di accesso [LSVD])**

Questo è il tempo impiegato dal VDA per eseguire gli script di accesso dell'utente.

Prendere in considerazione la possibilità di rendere asincroni gli script di accesso dell'utente o del gruppo. Prendere in considerazione l'ottimizzazione di eventuali script di compatibilità delle applicazioni o utilizzare variabili d'ambiente.

**Profile Load VDA Duration (PLVD) (Durata del VDA per il caricamento del profilo [PLVD])**

Questo è il tempo impiegato dal VDA per caricare il profilo dell'utente.

Se questa durata è elevata, esaminare la configurazione User Profile (Profilo utente). Le dimensioni e la posizione del profilo mobile contribuiscono a rallentare gli avvii delle sessioni. Quando un utente accede a una sessione in cui sono abilitati i profili mobili e le Home directory di Servizi terminal, il contenuto e l'accesso del profilo mobile a tale cartella vengono mappati durante l'accesso. Questo richiede risorse aggiuntive. A volte, questo può consumare una quantità significativa dell'utilizzo della CPU. Prendere in considerazione l'utilizzo delle **Home directory di Servizi terminal** con cartelle personali reindirizzate per mitigare questo problema. In generale, è consigliabile utilizzare Citrix Profile Management per gestire i profili utente negli ambienti Citrix. Se si utilizza Citrix Profile Management e i tempi di accesso sono lenti, verificare se il software antivirus blocca lo strumento Citrix Profile Management.

**Printer Creation VDA Duration (PCVD) (Durata del VDA per la creazione della stampante [PCVD])**

Questo è il tempo impiegato dal VDA per mappare in modo sincrono le stampanti client dell'utente. Se la configurazione è impostata per eseguire la creazione della stampante in modo asincrono, il valore non viene registrato per PCVD in quanto non influisce sul completamento dell'avvio della sessione.

Il tempo eccessivo impiegato per la mappatura delle stampanti è spesso il risultato delle impostazioni dei criteri di creazione automatica delle stampanti. Il numero di stampanti aggiunte localmente sui dispositivi client degli utenti e la configurazione di stampa possono influire direttamente sugli orari di inizio della sessione. All'avvio di una sessione, Citrix Virtual Apps and Desktops deve creare tutte le stampanti mappate localmente sul dispositivo client. Prendere in considerazione la riconfigurazione dei criteri di stampa per ridurre il numero di stampanti create, in particolare quando gli utenti hanno

molte stampanti locali. A tale scopo, modificare il criterio Printer Auto creation (Creazione automatica delle stampanti) nel Delivery Controller e in Citrix Virtual Apps and Desktops.

#### Drive Mapping VDA Duration (DMVD) (Durata del VDA per la mappatura unità [DMVD])

Questo è il tempo impiegato dal VDA per mappare le unità client, i dispositivi e le porte dell'utente.

Assicurarsi che i criteri di base includano impostazioni per disabilitare i canali virtuali inutilizzati. Ad esempio, la mappatura delle porte audio o COM, per ottimizzare il protocollo ICA e migliorare le prestazioni complessive della sessione.

#### Application/Desktop Launch VDA Duration (ALVD/DLVD) (Durata del VDA per l'avvio di applicazioni/desktop [ALVD/DLVD])

Questa fase è una combinazione della durata di Userinit e Shell. Quando un utente accede a una macchina Windows, winlogon esegue userinit.exe. Usernit.exe esegue script di accesso, ristabilisce le connessioni di rete e quindi avvia Explorer.exe. Userinit rappresenta la durata tra l'avvio di userinit.exe e l'avvio dell'interfaccia utente per il desktop virtuale o l'applicazione. La durata di Shell è il tempo che intercorre tra l'inizializzazione dell'interfaccia utente e il momento in cui l'utente riceve il controllo della tastiera e del mouse.

#### Session Creation VDA Duration (SCVD) (Durata del VDA per la creazione di sessioni [SCVD])

Questa durata include eventuali ritardi vari nel tempo di creazione della sessione sul VDA.

## Diagnosticare i problemi di accesso utente

January 7, 2024

Utilizzare i dati Logon Duration (Durata dell'accesso) per risolvere i problemi di accesso degli utenti.

La durata dell'accesso viene misurata solo per le connessioni iniziali a un desktop o un'app che utilizzano HDX. Questi dati non includono utenti che tentano di connettersi con Remote Desktop Protocol o riconnettersi da sessioni disconnesse. In particolare, la durata dell'accesso non viene misurata quando un utente si connette inizialmente utilizzando un protocollo non HDX e si ricollega utilizzando HDX.

Nella vista User Details (Dettagli utente), la durata viene visualizzata come valore numerico. Al di sotto di questo numero, viene visualizzata l'ora in cui si è verificato l'accesso e un grafico delle fasi del processo di accesso.

Man mano che gli utenti accedono a Citrix Virtual Apps and Desktops, il servizio di monitoraggio tiene traccia delle fasi del processo di accesso. Le fasi iniziano dal momento in cui l'utente si connette dall' app Citrix Workspace al momento in cui il desktop è pronto per l'uso.

Il numero elevato a sinistra è il tempo di accesso totale. Viene calcolato combinando il tempo impiegato per stabilire la connessione e ottenere un desktop dal Delivery Controller con il tempo impiegato per l'autenticazione e l'accesso a un desktop virtuale. Le informazioni sulla durata sono presentate in secondi (o frazioni di secondi).

### Prerequisiti

Assicurarsi che siano soddisfatti i seguenti prerequisiti per la visualizzazione dei dati e dei drill-down relativi alla durata degli accessi:

1. Installare **Citrix User Profile Manager** e **Citrix User Profile Manager WMI Plugin** sul VDA.
2. Assicurarsi che il servizio Citrix Profile Management sia in esecuzione.
3. Per i siti XenApp e XenDesktop 7.15 e versioni precedenti, disabilitare l'impostazione dell' oggetto Criteri di gruppo **Non elaborare l'elenco di esecuzione precedente**.
4. L'opzione Controlla traccia processo deve essere abilitata per il drill-down della sessione interattiva.
5. Per il drill-down dell'oggetto Criteri di gruppo, aumentare le dimensioni dei log operativi di Criteri di gruppo.

> **Note:**
>
> - La durata dell'accesso è supportata solo sulla shell predefinita di Windows (explorer.exe) e non su shell personalizzate.
> - La durata dell'accesso per Remote PC Access (Accesso remoto PC) è disponibile solo quando **Citrix User Profile Manager** e **Citrix User Profile Manager WMI Plugin** sono installati come componenti aggiuntivi durante l'installazione di Remote PC Access (Accesso remoto PC). Per ulteriori informazioni, vedere il passaggio 4 in Considerazioni sulla configurazione e sulla sequenza di Remote PC Access (Accesso remoto PC).

### Procedura per risolvere i problemi di accesso degli utenti

1. Dalla vista **User Details** (Dettagli utente), risolvere il problema dello stato di accesso utilizzando il riquadro Logon Duration (Durata dell'accesso).
    - Se l'utente sta effettuando l'accesso, la vista riflette il processo di accesso.
    - Se l'utente ha effettuato l'accesso, il riquadro Logon Duration (Durata dell'accesso) visualizza il tempo necessario per l'accesso alla sessione corrente.

2. Esaminare le fasi del processo di accesso.

## Fasi del processo di accesso

### Brokering

Tempo necessario per decidere quale desktop assegnare all'utente.

### VM start (Avvio VM)

Se la sessione richiede l'avvio di una macchina, l'avvio della VM è il tempo necessario per avviare la macchina virtuale.

### HDX connection (Connessione HDX)

Tempo necessario per completare i passaggi necessari per configurare la connessione HDX dal client alla macchina virtuale.

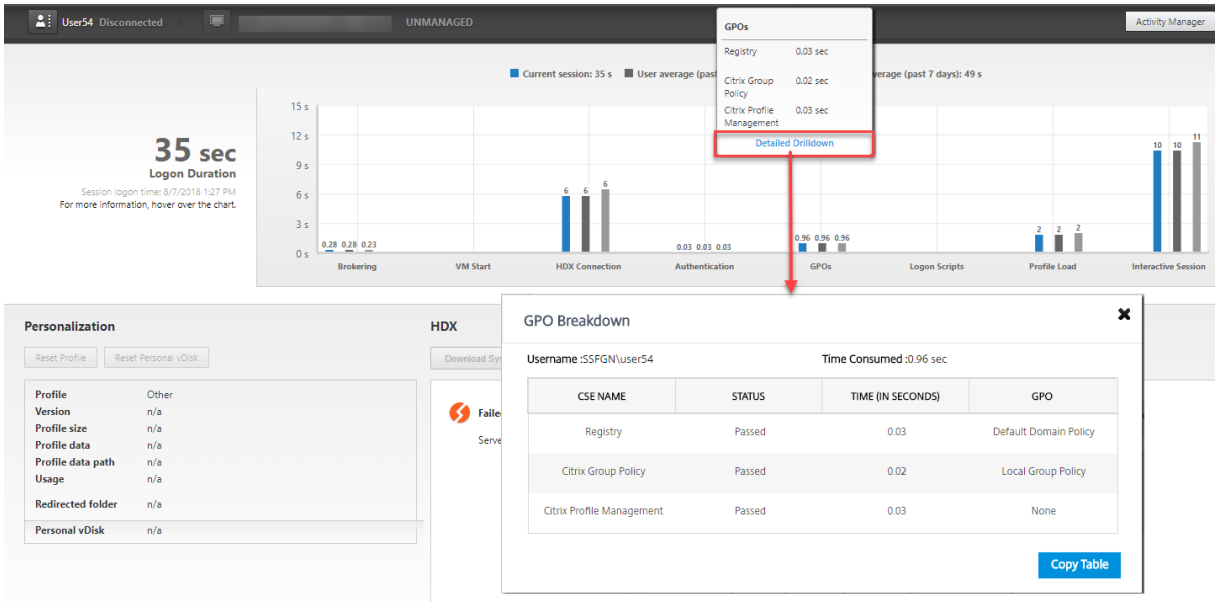
### Autenticazione

Tempo necessario per completare l'autenticazione alla sessione remota.

### GPOs (Oggetti Criteri di gruppo)

Se le impostazioni di Criteri di gruppo sono abilitate sulle macchine virtuali, questo è il tempo necessario per applicare gli oggetti Criteri di gruppo durante l'accesso. Il drill-down del tempo impiegato per applicare ogni criterio in base alle CSE (estensioni lato client) è disponibile come descrizione comando quando si passa il mouse sulla barra degli oggetti Criteri di gruppo.




Fare clic su **Espansione dettagliata** per visualizzare una tabella con lo stato dei criteri e il nome dell'oggetto Criteri di gruppo corrispondente. Le durate temporali nel drill-down rappresentano solo il tempo di elaborazione delle CSE e non si sommano al tempo totale dell'oggetto Criteri di gruppo. È possibile copiare la tabella del drill-down per ulteriori risoluzioni dei problemi o per utilizzarla nei report. Il tempo degli oggetti Criteri di gruppo per i criteri viene recuperato dai log del Visualizzatore eventi. I log possono essere sovrascritti a seconda della memoria allocata per i log operativi (la dimensione predefinita è 4 MB). Per ulteriori informazioni sull'aumento delle dimensioni del registro per i registri operativi, vedere l'articolo di Microsoft TechNet Configuring the Event Logs.

### Logon scripts (Script di accesso)

Se gli script di accesso sono configurati per la sessione, questo è il tempo necessario per la loro esecuzione.

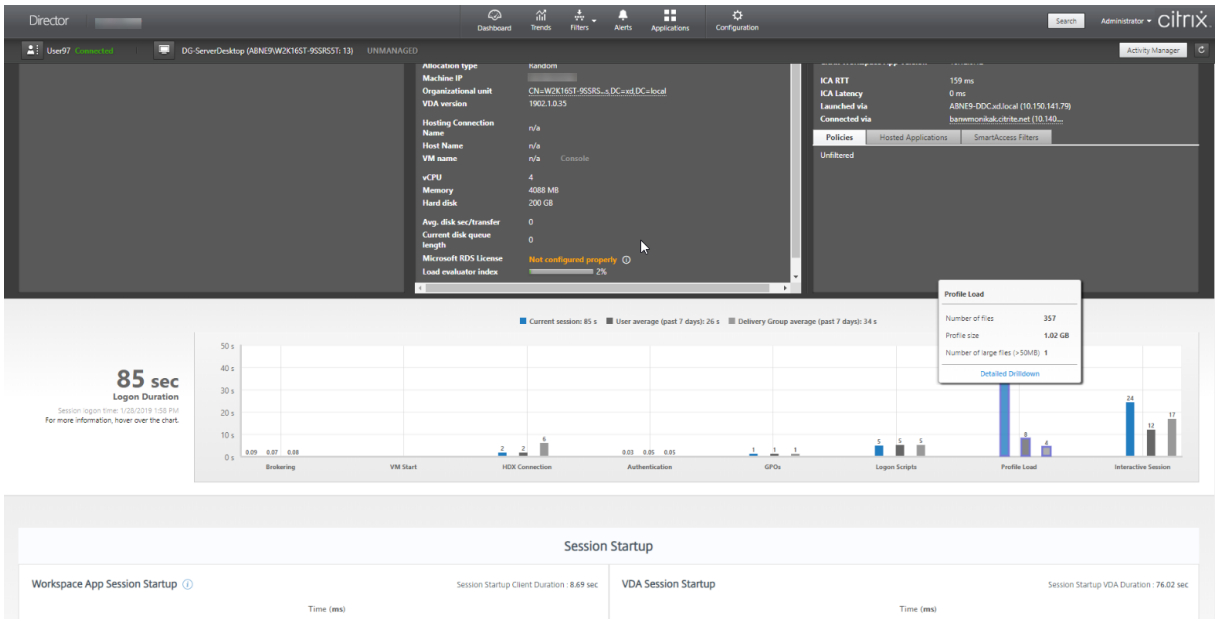
### Profile load (Caricamento del profilo)

Se le impostazioni del profilo sono configurate per l'utente o la macchina virtuale, questo è il tempo necessario per il caricamento del profilo.

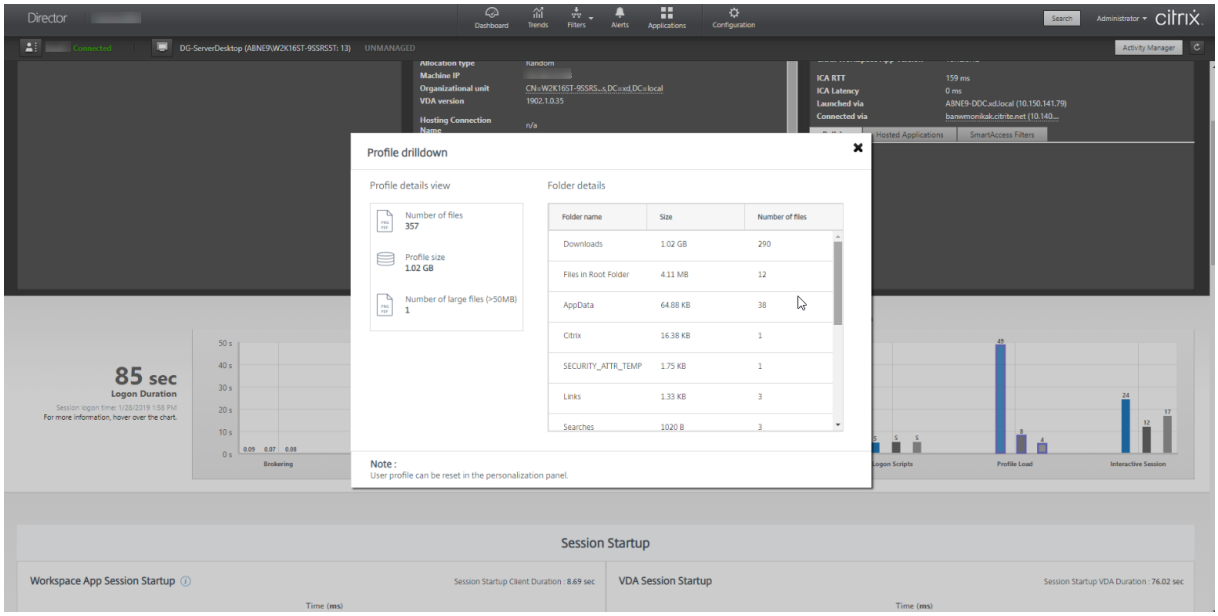
Se Citrix Profile Management è configurato, la barra Profile Load (Caricamento profilo) include il tempo impiegato da Citrix Profile Management per elaborare i profili utente. Queste informazioni aiutano gli amministratori a risolvere i problemi relativi alla durata elevata dell'elaborazione dei profili. Quando Profile Management è configurato, la barra Profile Load (Caricamento profilo) visualizza una durata maggiore. L'aumento è causato da questo miglioramento e non causa un degrado delle prestazioni. Questo miglioramento è disponibile sui VDA 1903 o versioni successive.

Se si passa il mouse sulla barra Profile Load (Caricamento profilo), viene visualizzata una descrizione comando che mostra i dettagli del profilo utente per la sessione corrente.




Fare clic su **Detailed Drilldown** (Drill-down dettagliato) per eseguire il drill-down di ogni singola cartella nella cartella principale del profilo (ad esempio, C:/Users/username), le relative dimensioni e il numero di file (inclusi i file all'interno delle cartelle nidificate).




Il drill-down del profilo è disponibile sui Delivery Controller versione 7 1811 o successive e i VDA 1811 o versioni successive. Utilizzando le informazioni di drill-down del profilo, è possibile risolvere i problemi relativi a un tempo di caricamento del profilo elevato. È possibile effettuare le seguenti operazioni:

- Reimpostare il profilo utente
- Ottimizzare il profilo rimuovendo file di grandi dimensioni indesiderati
- Ridurre il numero di file per ridurre il carico di rete
- Usare lo streaming dei profili

Per impostazione predefinita, tutte le cartelle nella radice del profilo vengono visualizzate nel drill-down. Per nascondere la visibilità delle cartelle, modificare il seguente valore del Registro di sistema sulla macchina VDA:

> **Avviso:**
>
> L'aggiunta e la modifica non corrette del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non garantisce che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

1. Sul VDA, aggiungere un nuovo valore del Registro di sistema **ProfileFoldersNameHidden** in HKEY_LOCAL_MACHINE\Software\Citrix\Director\
2. Impostare il valore su 1. Questo valore deve essere un valore DWORD (32 bit). La visibilità dei nomi delle cartelle ora è disabilitata.
3. Per rendere nuovamente visibili i nomi delle cartelle, impostare il valore su 0.

> **Nota:**
> È possibile utilizzare i comandi dell'oggetto Criteri di gruppo o PowerShell per applicare la modifica del valore del Registro di sistema su più macchine. Per ulteriori informazioni sull'utilizzo di un oggetto Criteri di gruppo per distribuire le modifiche del Registro di sistema, vedere il blog.

#### Informazioni aggiuntive

- Il drill-down del profilo non considera le cartelle reindirizzate.
- I file NTUser.dat nella cartella principale potrebbero non essere visibili agli utenti finali. Tuttavia, sono inclusi nel drill-down del profilo e visualizzati nell'elenco dei file nella **cartella principale**.
- Alcuni file nascosti nella cartella AppData non sono inclusi nel drill-down del profilo.
- Il numero di file e i dati relativi alle dimensioni del profilo potrebbero non corrispondere ai dati nel riquadro Personalization (Personalizzazione) a causa di alcune limitazioni di Windows.

#### Interactive Session (Sessione interattiva)

Questo è il tempo necessario per "trasferire"il controllo della tastiera e del mouse all'utente dopo il caricamento del profilo utente. Normalmente è la durata più lunga di tutte le fasi del processo di accesso e viene calcolata come **Interactive Session duration (Durata della sessione interattiva)**

**= Desktop Ready Event Timestamp (Data e ora evento Desktop pronto) (EventId 1000 su VDA) - User Profile Loaded Event Timestamp (Data e ora evento Profilo utente caricato) (EventId 2 su VDA)**. La sessione interattiva è composta da tre sottofasi: Pre-userinit, Userinit e Shell. Passare il mouse su Interactive Session (Sessione interattiva) per visualizzare una descrizione comando che mostra quanto segue:

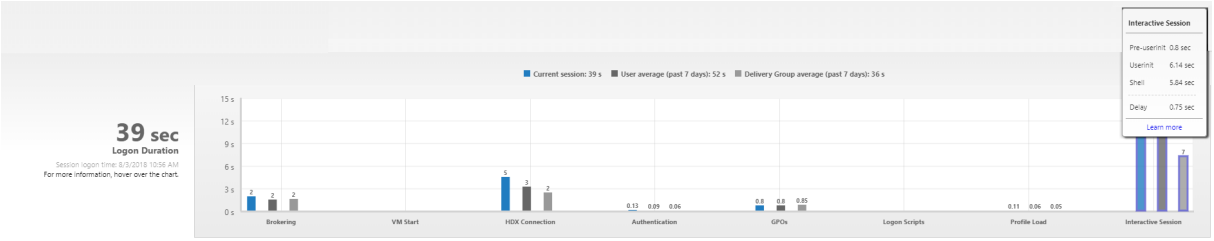
- sottofasi
- tempo impiegato per ogni sottofase
- ritardo totale cumulativo tra queste sottofasi

> **Nota:**
>
> Questa funzionalità è disponibile sui VDA 1811 e versioni successive. Se sono state avviate sessioni su siti precedenti a 7.18 e successivamente è stato eseguito l'aggiornamento a 7.18 o versioni successive, viene visualizzato un messaggio "Drilldown unavailable due to server error" (Drill-down non disponibile a causa di un errore del server). Tuttavia, se sono state avviate le sessioni dopo l'aggiornamento, non viene visualizzato alcun messaggio di errore.

Per visualizzare la durata di ogni sottofase, abilitare Controlla traccia processo sulla VM (VDA). Quando l'opzione Controlla traccia processo è disabilitata (impostazione predefinita), vengono visualizzate la durata di Pre-userinit e la durata combinata di Userinit e Shell. È possibile abilitare Controlla traccia processo tramite un oggetto Criteri di gruppo (GPO) come segue:

1. Creare un oggetto Criteri di gruppo e modificarlo utilizzando l'Editor oggetti Criteri di gruppo.
2. Andare a **Configurazione computer > Impostazioni di Windows > Impostazioni di sicurezza > Criteri locali > Criteri di controllo**.
3. Nel riquadro di destra, fare doppio clic su **Controlla traccia processo**.
4. Selezionare **Operazione riuscita** e fare clic su OK.
5. Applicare questo oggetto Criteri di gruppo ai VDA o al gruppo richiesti.

Per ulteriori informazioni sul tracciamento del processo di verifica e sull'abilitazione o disabilitazione del processo, vedere Controlla traccia processo nella documentazione Microsoft.




Riquadro Logon Duration (Durata dell'accesso) nella vista User Details (Dettagli utente).

- **Interactive Session —Pre-userinit** (Sessione interattiva - Pre-userinit): il segmento di Interactive Session (Sessione interattiva) che si sovrappone a oggetti Criteri di gruppo e script. Questa sottofase può essere ridotta ottimizzando gli oggetti Criteri di gruppo e gli script.

- **Interactive Session** —**Userinit** (Sessione interattiva - Userinit): quando un utente accede a una macchina Windows, Winlogon esegue userinit.exe. Userinit.exe esegue gli script di accesso, ristabilisce le connessioni di rete e quindi avvia Explorer.exe, l'interfaccia utente di Windows. Questa sottofase di Interactive Session (Sessione interattiva) rappresenta la durata tra l'avvio di Userinit.exe e l'avvio dell'interfaccia utente per il desktop virtuale o l'applicazione.
- **Interactive Session** —**Shell** (Sessione interattiva - Shell): nella fase precedente, Userinit avvia l'inizializzazione dell'interfaccia utente di Windows. La sottofase Shell acquisisce la durata tra l'inizializzazione dell'interfaccia utente e il momento in cui l'utente riceve il controllo della tastiera e del mouse.
- **Delay** (Ritardo): si tratta del ritardo temporale cumulativo tra le sottofasi **Pre-userinit e Userinit** e le sottofasi **Userinit e Shell**.

Il tempo di accesso totale non è una somma esatta di queste fasi. Ad esempio, alcune fasi si verificano in parallelo e, in alcune fasi, si verifica una maggiore elaborazione che può comportare una durata dell'accesso più lunga della somma.
Il tempo di accesso totale non include il tempo di inattività ICA, ovvero il tempo tra il download del file ICA e l'avvio del file ICA per un'applicazione.
Per abilitare l'apertura automatica del file ICA all'avvio dell'applicazione, configurare il browser per l'avvio automatico del file ICA al momento del download di un file ICA. Per ulteriori informazioni, vedere CTX804493.

> **Nota:**
> Il grafico Logon Duration (Durata dell'accesso) mostra le fasi di accesso in secondi. Tutti i valori di durata inferiore a un secondo vengono visualizzati come valori secondari. I valori superiori a un secondo sono arrotondati al mezzo secondo più vicino (0,5 s). Il grafico è stato progettato per mostrare il valore dell'asse y più alto come 200 secondi. Qualsiasi valore superiore a 200 secondi viene mostrato con il valore effettivo visualizzato sopra la barra.

### Suggerimenti per la risoluzione dei problemi

Per identificare valori insoliti o imprevisti nel grafico, confrontare il tempo impiegato in ogni fase della sessione corrente con la durata media per questo utente negli ultimi sette giorni e la durata media per tutti gli utenti di questo gruppo di consegna per gli ultimi sette giorni.

Segnalare i problemi secondo necessità. Ad esempio, se l'avvio della VM è lento, potrebbe trattarsi di un problema dell'hypervisor, quindi occorre segnalarlo all'amministratore dell'hypervisor. Oppure, se il tempo di brokering è lento, è possibile segnalare il problema all'amministratore del sito per verificare il bilanciamento del carico sul Delivery Controller.

Esaminare le differenze insolite, tra cui:

- Barre di accesso mancanti (correnti)

- Notevoli discrepanze tra la durata corrente e la durata media di questo utente. Le cause includono:
  - È stata installata una nuova applicazione.
  - Si è verificato un aggiornamento del sistema operativo.
  - Sono state apportate modifiche alla configurazione.
  - Le dimensioni del profilo dell'utente sono elevate. In questo caso, il caricamento del profilo è elevato.
- Notevoli discrepanze tra il log dell'utente per quanto riguarda i numeri (durata corrente e media) e la durata media del gruppo di consegna.

Se necessario, fare clic su **Restart** (Riavvia) per osservare il processo di accesso dell'utente al fine di risolvere i problemi, ad esempio VM Start (Avvio VM) o Brokering.

## Shadowing degli utenti

January 7, 2024

Da Director, utilizzare la funzionalità di shadowing degli utenti per visualizzare la macchina virtuale o la sessione di un utente o lavorarci direttamente. È possibile utilizzare la funzionalità di shadowing sia sui VDA Windows che Linux. L'utente deve essere connesso alla macchina di cui si desidera fare lo shadowing. Verificarlo controllando il nome della macchina elencato nella barra del titolo dell'utente.

Director avvia lo shadowing in una nuova scheda. Aggiornare le impostazioni del browser per consentire i popup dall'URL di Director.

Accedere alla funzionalità di shadowing dalla vista **User Details** (Dettagli utente). Selezionare la sessione utente e fare clic su **Shadow** (Avvia shadowing) nella vista Activity Manager (Gestione attività) o nel riquadro Session Details (Dettagli sessione).

### Shadowing di VDA Linux

Lo shadowing è disponibile per i VDA Linux versione 7.16 o successive con le distribuzioni Linux RHEL7.3 o Ubuntu versione 16.04.

> **Nota:**
>
> - Il VDA deve essere accessibile dall'interfaccia utente di Director perché lo shadowing funzioni. Pertanto, lo shadowing è possibile solo per i VDA Linux nella stessa intranet del client di Director.

> - Director utilizza il nome di dominio completo per connettersi al VDA Linux di destinazione. Assicurarsi che il client di Director sia in grado di risolvere il nome di dominio completo del VDA Linux.
> - Sul VDA devono essere installati i pacchetti python websockify e x11vnc.
> - La connessione noVNC al VDA utilizza il protocollo WebSocket. Per impostazione predefinita, viene utilizzato il protocollo WebSocket **ws://**. Per motivi di sicurezza, Citrix consiglia di utilizzare il protocollo **wss://** sicuro. Installare i certificati SSL su ciascun client Director e VDA Linux.

Seguire le istruzioni riportate in Shadowing delle sessioni per configurare il VDA per lo shadowing.

1. Dopo aver fatto clic su **Shadow** (Avvia shadowing), la connessione di shadowing viene inizializzata e sul dispositivo utente viene visualizzato un prompt di conferma.
2. Chiedere all'utente di fare clic su **Yes** (Sì) per avviare la condivisione della macchina o della sessione.
3. L'amministratore può solo visualizzare la sessione di cui viene eseguito lo shadowing.

### Shadowing dei VDA Windows

Lo shadowing delle sessioni di VDA Windows viene eseguito utilizzando l'Assistenza remota di Windows. Abilitare la funzionalità **User Windows Remote Assistance** (Assistenza remota di Windows per l'utente) durante l'installazione del VDA. Per ulteriori informazioni, vedere Abilitare o disabilitare funzionalità.

1. Dopo aver fatto clic su **Shadow** (Avvia shadowing), la connessione di shadowing viene inizializzata e una finestra di dialogo richiede di aprire o salvare il file richiesta di supporto .msrc.
2. Aprire il file richiesta di supporto con Remote Assistance Viewer, se non è già selezionato per impostazione predefinita. Sul dispositivo dell'utente viene visualizzato un messaggio di conferma.
3. Chiedere all'utente di fare clic su **Yes** (Sì) per avviare la condivisione della macchina o della sessione.
4. Per un maggiore controllo, chiedere all'utente di condividere il controllo della tastiera e del mouse.

#### Ottimizzare i browser Microsoft Internet Explorer per lo shadowing

Configurare il browser Microsoft Internet Explorer in modo che apra automaticamente il file Microsoft Remote Assistance (.msra) scaricato con il client di Assistenza remota.

A tale scopo, è necessario abilitare l'impostazione Richiesta di conferma automatica per download di file nell'editor Criteri di gruppo:

Configurazione computer > Modelli amministrativi > Componenti di Windows > Internet Explorer > Pannello di controllo Internet > Scheda Sicurezza > Area Internet > Richiesta di conferma automatica per download di file.

Per impostazione predefinita, questa opzione è abilitata per i siti nell'area Intranet locale. Se il sito di Director non si trova nell'area Intranet locale, prendere in considerazione l'aggiunta manuale del sito a quest'area.

## Inviare messaggi agli utenti

January 7, 2024

Da Director, inviare un messaggio a un utente connesso a una o più macchine. Utilizzare questa funzionalità per inviare avvisi immediati sulle azioni amministrative, come la manutenzione imminente del desktop, le disconnessioni e i riavvii delle macchine e il ripristino dei profili.

1. Nella vista Activity Manager (Gestione attività), selezionare l'utente e fare clic su Dettagli.
2. Nella vista User Details (Dettagli utente), individuare il riquadro Session Details (Dettagli sessione) e fare clic su Send Message (Invia messaggio).
3. Digitare le informazioni sul messaggio nei campi Subject (Oggetto) e Message (Messaggio) e fare clic su Invia.

Se il messaggio viene inviato correttamente, viene visualizzato un messaggio di conferma in Director. Il messaggio viene visualizzato nella macchina dell'utente.

Se il messaggio non viene inviato correttamente, viene visualizzato un messaggio di errore in Director. Risolvere il problema in base al messaggio di errore. Al termine, digitare di nuovo il testo dell'oggetto e del messaggio e fare clic nuovamente clic su **Try** (Prova).

## Risolvere gli errori delle applicazioni

January 7, 2024

Nella vista **Activity Manager** (Gestione attività), fare clic sulla scheda Applications (Applicazioni). È possibile visualizzare tutte le applicazioni su tutte le macchine a cui l'utente ha accesso, incluse le applicazioni locali e ospitate per la macchina attualmente connessa, e lo stato di ciascuna.

> **Nota:**
>
> Se la scheda Applications è disattivata, contattare un amministratore che dispone dell'autoriz-

> zazione per abilitare la scheda.

L'elenco include solo le applicazioni avviate all'interno della sessione.

Per le macchine con sistema operativo multisessione e le macchine con sistema operativo a sessione singola, le applicazioni sono elencate per ogni sessione disconnessa. Se l'utente non è connesso, non viene visualizzata alcuna applicazione.

| Azione | Descrizione |
| --- | --- |
| Terminare l'applicazione che non risponde | Scegliere l'applicazione che non risponde e fare clic su End Application (Termina applicazione). Una volta terminata l'applicazione, chiedere all'utente di avviarla di nuovo. |
| Terminare i processi che non rispondono | Se si dispone dell'autorizzazione richiesta, fare clic sulla scheda Processes (Processi). Selezionare un processo correlato all'applicazione o che utilizza una quantità elevata di risorse della CPU o memoria e fare clic su End Process (Termina processo). Tuttavia, se non si dispone dell'autorizzazione necessaria per terminare il processo, il tentativo di terminare un processo non riesce. |
| Riavviare la macchina dell'utente | Solo per le macchine con sistema operativo a sessione singola, per la sessione selezionata fare clic su Restart (Riavvia). In alternativa, dalla vista Machine Details (Dettagli macchina), utilizzare i controlli di alimentazione per riavviare o spegnere la macchina. Chiedere all'utente di effettuare nuovamente l'accesso in modo da poter ricontrollare l'applicazione. Per le macchine con sistema operativo multisessione, l'opzione di riavvio non è disponibile. In questo caso, disconnettersi dall'utente e lasciare che l'utente acceda di nuovo. |

| Azione | Descrizione |
| --- | --- |
| Mettere la macchina in modalità di manutenzione | Se l'immagine della macchina necessita di manutenzione, ad esempio una patch o altri aggiornamenti, mettere la macchina in modalità di manutenzione. Dalla vista Machine Details (Dettagli macchina), fare clic su Details (Dettagli) e attivare l'opzione Maintenance Mode (Modalità di manutenzione). Fare una segnalazione all'amministratore appropriato. |

## Ripristinare le connessioni desktop

January 7, 2024

Da Director, controllare lo stato della connessione dell'utente per la macchina corrente nella barra del titolo dell'utente.

Utilizzare questa funzionalità per inviare avvisi immediati sulle azioni amministrative, come la manutenzione imminente del desktop, le disconnessioni e i riavvii delle macchine e i ripristini dei profili.

| Azione | Descrizione |
| --- | --- |
| Assicurarsi che la macchina non sia in modalità di manutenzione | Nella pagina User Details (Dettagli utente), assicurarsi che la modalità di manutenzione sia disattivata. |
| Riavviare la macchina dell'utente | Selezionare la macchina e fare clic su **Restart** (Riavvia). Utilizzare questa opzione se la macchina dell'utente non risponde o non è in grado di connettersi. Ad esempio, quando la macchina utilizza una quantità insolitamente elevata di risorse della CPU, il che può rendere la CPU inutilizzabile. |

## Ripristinare le sessioni

January 7, 2024

Se una sessione viene disconnessa, è ancora attiva e le relative applicazioni continuano a essere eseguite, ma il dispositivo utente non comunica più con il server.

Nella vista User Details (Dettagli utente), risolvere i problemi relativi alla sessione nel riquadro **Session Details** (Dettagli sessione). È possibile visualizzare i dettagli della sessione corrente, indicati dall'ID della sessione.

| Azione | Descrizione |
|---|---|
| Terminare le applicazioni o i processi che non rispondono | Fare clic sulla scheda **Applications** (Applicazioni). Selezionare le applicazioni che non rispondono e fare clic su **End Application** (Termina applicazione). Analogamente, selezionare gli eventuali processi corrispondente che non rispondono e fare clic su **End Process** (Termina processo). Inoltre, terminare i processi che consumano una quantità insolitamente elevata di memoria o risorse della CPU, il che può rendere inutilizzabile la CPU. |
| Disconnettere la sessione di Windows | Fare clic su **Session Control** (Controllo sessione) e quindi selezionare **Disconnect** (Disconnetti). Questa opzione è disponibile solo per macchine con sistema operativo multisessione con broker. Per le sessioni senza broker, l'opzione è disabilitata. |
| Disconnettersi dalla sessione dell'utente | Fare clic su **Session Control** (Controllo sessione), quindi selezionare **Log Off** (Esci). |

Per testare la sessione, l'utente può tentare di riaccedervi. È inoltre possibile ricorrere allo shadowing dell'utente per monitorare più da vicino questa sessione.

## Eseguire report sui sistemi di canale HDX

January 7, 2024

Nella vista **User Details** (Dettagli utente), controllare lo stato dei canali HDX sulla macchina dell'utente nel riquadro **HDX**. Questo riquadro è disponibile solo se la macchina dell'utente è collegata utilizzando HDX.

Se viene visualizzato un messaggio che indica che le informazioni non sono attualmente disponibili, attendere un minuto per l'aggiornamento della pagina oppure selezionare il pulsante **Refresh** (Aggiorna). L'aggiornamento dei dati HDX richiede un po'più tempo rispetto ad altri dati.

Fare clic su un'icona di errore o di avviso per ulteriori informazioni.

> Suggerimento:
>
> È possibile visualizzare informazioni sugli altri canali nella stessa finestra di dialogo facendo clic sulle frecce sinistra e destra nell'angolo sinistro della barra del titolo.

I report di sistema del canale HDX vengono utilizzati principalmente dal supporto Citrix per ulteriori risoluzioni dei problemi.

1. Nel riquadro HDX, fare clic su Download System Report (Scarica report di sistema).
2. È possibile visualizzare o salvare il file .xml del report.
    - Per visualizzare il file.xml, fare clic su Open (Apri). Il file .xml viene visualizzato nella stessa finestra dell'applicazione Director.
    - Per salvare il file.xml, fare clic su Save (Salva). Viene visualizzata la finestra Save As (Salva con nome), che richiede un percorso sulla macchina di Director in cui scaricare il file.

## Reimpostare un profilo utente

January 7, 2024

> **ATTENZIONE:**
>
> Quando un profilo viene reimpostato, le cartelle e i file dell'utente vengono salvati e copiati nel nuovo profilo. Tuttavia, manca la maggior parte dei dati del profilo utente (ad esempio, il Registro di sistema viene reimpostato e le impostazioni dell'applicazione potrebbero essere state eliminate).

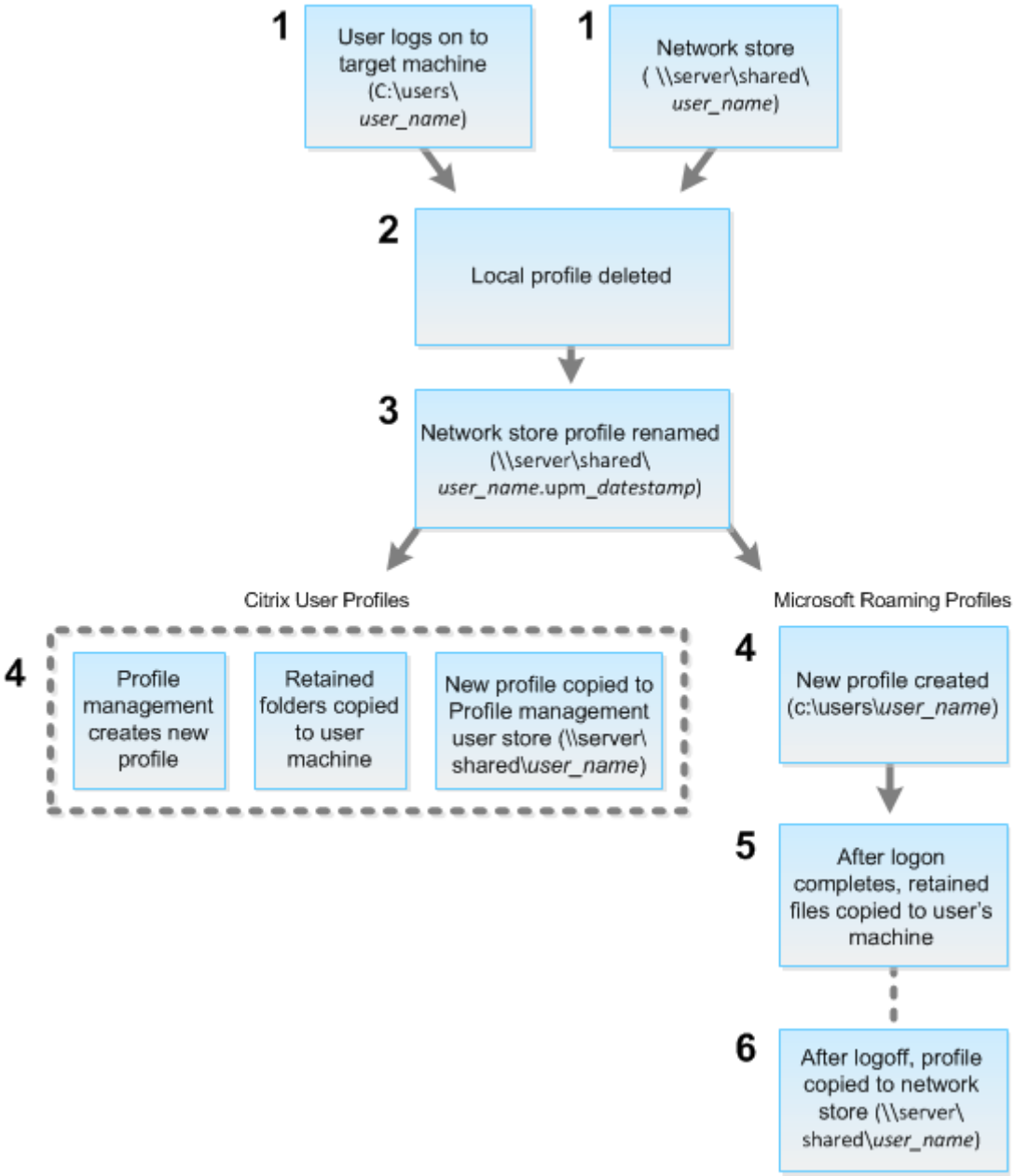
A partire da Profile Management 2106, la funzione di ripristino è disponibile per la soluzione di profili utente basata su contenitore di profili Citrix Management.

### Come vengono elaborati i profili ripristinati

È possibile reimpostare qualsiasi profilo utente Citrix o profilo mobile Microsoft. Dopo che l'utente si disconnette e si seleziona il comando reset (in Director o utilizzando l'SDK di PowerShell), Director identifica innanzitutto il profilo utente in uso ed emette un comando reset appropriato. Director riceve le informazioni tramite Profile Management, incluse informazioni sulle dimensioni, sul tipo e sui tempi di accesso del profilo.

Questo diagramma illustra il processo successivo all'accesso dell'utente, quando viene reimpostato un profilo utente.



Il comando reset emesso da Director specifica il tipo di profilo. Il servizio Profile Management tenta quindi di reimpostare un profilo di quel tipo e cerca la condivisione di rete appropriata (archivio utente). Se l'utente viene elaborato da Profile Management, ma riceve un comando di profilo mobile, il comando viene rifiutato (o viceversa).

1. Se è presente un profilo locale, viene eliminato.
2. Il profilo di rete viene rinominato.
3. L'azione successiva dipende dal tipo di profilo in fase di reimpostazione: un profilo utente Citrix o un profilo mobile Microsoft.

   Per i profili utente Citrix, il nuovo profilo viene creato utilizzando le regole di importazione di Profile Management. Le cartelle vengono copiate nuovamente nel profilo di rete e l'utente può accedere normalmente. Se per il ripristino viene utilizzato un profilo mobile, le eventuali impostazioni del Registro di sistema nel profilo mobile vengono mantenute nel profilo di ripristino. È possibile configurare Profile Management in modo che un profilo del modello sostituisca il profilo mobile, se necessario.

   Per i profili mobili Microsoft, Windows crea un profilo e, quando l'utente effettua l'accesso, le cartelle vengono copiate nuovamente nel dispositivo dell'utente. Quando l'utente si disconnette di nuovo, il nuovo profilo viene copiato nell'archivio di rete.

### Per ripristinare un profilo utente in Director

Se si utilizza Citrix Virtual Desktops (Desktop VDA), effettuare le seguenti operazioni:

1. Da **Director**, cercare l'utente di cui si desidera reimpostare il profilo e selezionare la sessione di questo utente.
2. Fare clic su **Reset Profile** (Reimposta profilo).
3. Chiedere all'utente di disconnettersi da tutte le sessioni.
4. Chiedere all'utente di accedere di nuovo.
   Le cartelle e i file salvati dal profilo dell'utente vengono copiati nel nuovo profilo.

Se si utilizza Citrix Virtual Desktops (Server VDA), è necessario effettuare l'accesso per eseguire il ripristino del profilo. L'utente deve quindi disconnettersi e accedere nuovamente per completare il ripristino del profilo.

> **Importante:**
>
> Se l'utente dispone di profili su più piattaforme (ad esempio Windows 8 e Windows 7), chiedere all'utente di accedere prima allo stesso desktop o alla stessa app segnalati dall'utente come problema. Questa azione di accesso assicura che venga ripristinato il profilo corretto. Se il profilo è un profilo utente Citrix, è già reimpostato quando viene visualizzato il desktop dell'utente. Se

> il profilo è un profilo mobile Microsoft, il ripristino della cartella potrebbe essere ancora in corso per un breve periodo. L'utente deve rimanere connesso fino al completamento del ripristino.

Se il profilo non viene ripristinato correttamente (ad esempio, l'utente non è in grado di accedere nuovamente alla macchina o mancano alcuni file), è necessario ripristinare manualmente il profilo originale.

Notare quanto segue:

- Se l'archivio utenti è abilitato come soluzione per i profili utente, il nuovo profilo contiene le seguenti cartelle personali del profilo utente originale:
  - Desktop
  - Cookie
  - Preferiti
  - Documenti
  - Immagini
  - Musica
  - Video
- Se il contenitore di profili di Citrix Management è abilitato come soluzione completa per i profili utente, il nuovo profilo non contiene le cartelle personali precedenti.
- In Windows 8 e versioni successive, i cookie non vengono copiati quando i profili vengono reimpostati.

### Per ripristinare manualmente un profilo dopo un ripristino non riuscito

1. Chiedere all'utente di disconnettersi da tutte le sessioni.
2. Eliminare il profilo locale, se ne esiste uno.
3. Individuare la cartella archiviata nella condivisione di rete contenente la data e l'ora aggiunte al nome della cartella, la cartella con estensione .upm_datestamp.
4. Eliminare il nome del profilo corrente, ossia quello senza l'estensione upm_datestamp.
5. Rinominare la cartella archiviata utilizzando il nome del profilo originale, ossia rimuovere l'estensione di data e ora. Il profilo è stato restituito allo stato originale di pre-ripristino.

### Per reimpostare un profilo utilizzando l'SDK di PowerShell

È possibile reimpostare un profilo utilizzando l'SDK Broker PowerShell.

#### New-BrokerMachineCommand

Crea un comando che viene messo in coda per la consegna a un utente, una sessione o una macchina specifici. Per ulteriori informazioni su questo cmdlet, vedere https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/.

#### Esempi

Per ulteriori informazioni su come utilizzare i cmdlet PowerShell per reimpostare un profilo, vedere gli esempi seguenti:

Reimpostare un profilo di Profile Management

- Supponiamo di voler reimpostare il profilo per user1. Utilizzare il comando PowerShell New-BrokerMachineCommand. Ad esempio:

  ```
  New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile"-DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1
  ```

> **Importante:**
>
> `CommandData $byteArray` deve essere nel seguente formato: `<SID>[,<backup path>]`. Se non si fornisce il percorso di backup, Profile Management genera una cartella di backup denominata in base alla data e all'ora correnti.

Reimpostare un profilo mobile Windows

- Supponiamo di voler reimpostare il profilo di roaming per user1. Utilizzare il comando PowerShell New-BrokerMachineCommand. Ad esempio:

  ```
  New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile"-DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1
  ```

## Registrare le sessioni

January 7, 2024

È possibile registrare le sessioni ICA utilizzando i controlli Session Recording (Registrazione sessione) dalla schermata **User Details** (Dettagli utente) e **Machine Details** (Dettagli macchina) in Director. Questa funzionalità è disponibile per i clienti dei siti **Premium**.

### Registrazione della sessione basata sui criteri

Per configurare Session Recording (Registrazione sessione) in Director utilizzando lo strumento DirectorConfig, vedere la sezione **Configure Director to use the Session Recording Server** (Configurare Director per utilizzare il server di registrazione delle sessioni) in Configure session recording policies. I controlli Session Recording (Registrazione sessione) sono disponibili in Director solo se l'utente connesso dispone dell'autorizzazione per modificare i criteri di registrazione della sessione. Questa autorizzazione può essere impostata nella console Session Recording Authorization (Autorizzazione per la registrazione della sessione) come descritto in Authorize users.

> **Nota:**
> Le modifiche apportate alle impostazioni Session Recording (Registrazione sessione) tramite Director o la console Session Recording Policy (Criteri di registrazione della sessione) hanno effetto a partire dalla successiva sessione ICA.

### Controlli Session Recording (Registrazione sessione) in Director

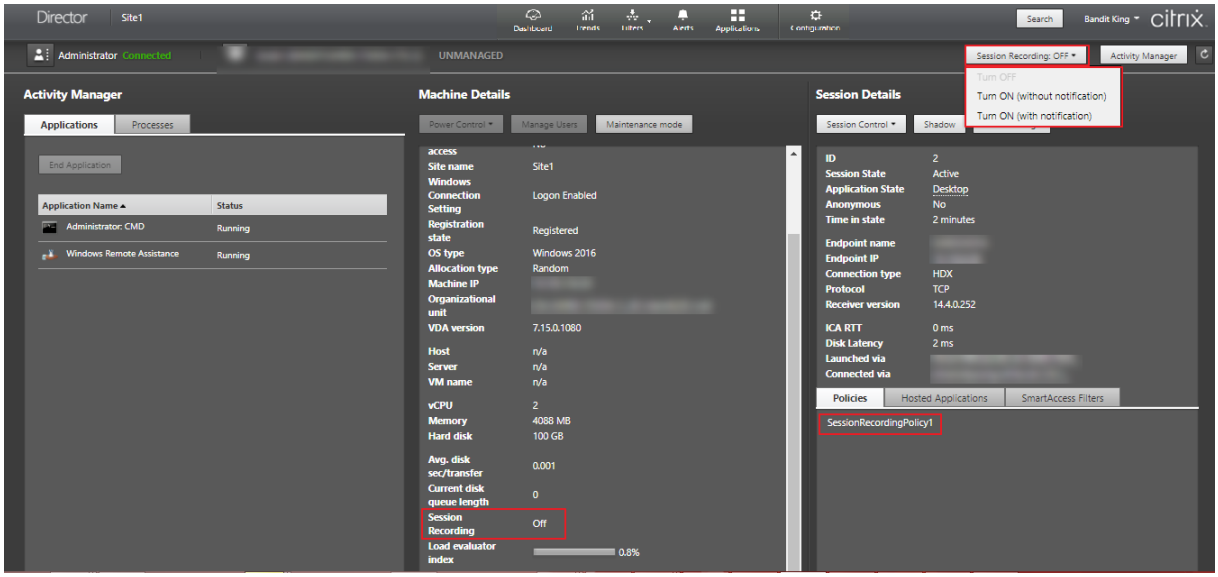
È possibile abilitare Session Recording (Registrazione sessione) per un utente specifico in **Activity Manager** (Gestione attività) o nella schermata **User Details** (Dettagli utente). Le sessioni successive vengono registrate per l'utente specifico su tutti i server supportati.

È possibile effettuare le seguenti operazioni:

- Turn ON (with notification) (Attiva [con notifica]): la sessione successiva viene registrata e l'utente riceve una notifica che la sessione verrà registrata al momento dell'accesso alla sessione ICA.
- Turn ON (without notification) (Attiva [senza notifica]): la sessione successiva viene registrata e la sessione viene registrata senza avvisare l'utente.
- Turn OFF (Disattiva): disabilita la registrazione delle sessioni per l'utente.

Il riquadro **Policies** (Criteri) visualizza il nome del criterio Session Recording (Registrazione sessione) attivo.




Il riquadro **Machine Details** (Dettagli macchina) visualizza lo stato del criterio Session Recording (Registrazione sessione) per la macchina.

## Matrice di compatibilità delle funzionalità

January 7, 2024

Citrix Director 7 2203 è compatibile con:

- Citrix Virtual Apps and Desktops 7 2112 e versioni successive
- Citrix Virtual Apps and Desktops 7 1912 LTSR

All'interno di ciascun sito, sebbene sia possibile utilizzare Director con versioni precedenti di Delivery Controller, tutte le funzionalità dell'ultima versione di Director potrebbero non essere disponibili. Citrix consiglia di utilizzare la stessa versione per Director, Delivery Controller e VDA.

> **Nota:**
>
> Dopo aver aggiornato un Delivery Controller, viene richiesto di aggiornare il sito all'apertura di Studio. Per ulteriori informazioni, consultare la sezione **Sequenza di aggiornamento** in Aggiornare una distribuzione.

La prima volta che si effettua l'accesso dopo un aggiornamento di Director, viene eseguito un controllo della versione sui siti configurati. Se un sito sta eseguendo una versione del Controller precedente a quella di Director, viene visualizzato un messaggio sulla console di Director, che consiglia l'aggiornamento del sito. Inoltre, finché la versione del sito è più vecchia di quella di Director, rimane visualizzata una nota nella dashboard di Director che indica questa mancata corrispondenza.

> **Nota:**
>
> Le versioni precedenti di Citrix Director non visualizzano i criteri applicati alle sessioni utente in esecuzione su versioni dei VDA recenti. Citrix Director 1912 e versioni precedenti non visualizzano i criteri applicati alle sessioni utente in esecuzione su VDA versioni 2003 e successive. Utilizzare Citrix Director versioni 2003 e successive per visualizzare tali criteri.

Di seguito sono elencate le funzionalità specifiche di Director con la versione minima di Delivery Controller (DC), VDA e altri componenti dipendenti richiesti insieme alla versione della licenza.

| Versione di Director | Funzionalità | Dipendenze - versione minima richiesta | Versione |
|---|---|---|---|
| 2305 | Supporta l'autenticazione tramite Citrix Gateway | Nessuna | Tutte |
| 2305 | Gestione di Autoscale in Director | Nessuna | Tutte |
| 2303 | Avviso di macchine con errori | DC 7 2303 | Premium |
| 2203 | Supporto TLS 1.3 | - | Tutte |
| 2212 | Utilizzo della GPU in tempo reale disponibile per le GPU AMD | DC 7.14 e VDA 7.14 con Windows a 64 bit e HDX 3D Pro abilitati | Tutte |
| 2212 | Pianificazione avanzata del probe | DC 7 1906 e Citrix Probe Agent 2209 | Premium |
| 1909 | Configurazione di siti locali con Citrix Analytics for Performance | DC 7 1906 e VDA 1906 | Tutte |
| 1906 | Riconnessione automatica della sessione | DC 7 1906 e VDA 1906 | Tutte |
| 1906 | Durata dell'avvio della sessione | DC 7 1906 e VDA 1903 | Tutte |

| Versione di Director | Funzionalità | Dipendenze - versione minima richiesta | Versione |
|---|---|---|---|
| 1906 | Probe dei desktop | DC 7 1906 e Citrix Probe Agent 1903 | Premium |
| 7.9 e versioni successive | Durata di Profile Management Citrix nel caricamento del profilo | VDA 1903 | Tutte |
| 1811 | Drill-down del profilo | DC 7 1811 e VDA 1811 | Tutte |
| 1811 | Monitoraggio degli avvisi di Hypervisor | DC 7 1811 | Premium |
| 1811 | Probe delle applicazioni | DC 7 1811 e Citrix Application Probe Agent 1811 | Premium |
| 1811 | Stato licenza Servizi Desktop remoto Microsoft | DC 7 1811 e VDA 7.16 | Tutte |
| 1811 | Visualizzazione dei dati RTOP chiave | DC 7 1811 e VDA 1808 | Premium |
| 1808 | Esportazione dei dati dei filtri | DC 7 1808 | Tutte |
| 1808 | Drill-down della sessione interattiva | DC 7 1808 e VDA 1808 | Tutte |
| 1808 | Drill-down dell'oggetto Criteri di gruppo | DC 7 1808 e VDA 1808 | Tutte |
| 1808 | Dati cronologici della macchina disponibili utilizzando l'API OData | DC 7 1808 | Tutte |
| 7.18 | Probe delle applicazioni | DC 7.18 | Premium (precedentemente Platinum) |
| 7.18 | Criteri intelligenti per gli avvisi | DC 7.18 | Premium (precedentemente Platinum) |

| Versione di Director | Funzionalità | Dipendenze - versione minima richiesta | Versione |
|---|---|---|---|
| 7.18 | Link Health Assistant | Nessuna | Tutte |
| 7.18 | Drill-down della sessione interattiva | Nessuna | Tutte |
| 7.17 | Autenticazione smart card PIV | Nessuna | Tutte |
| 7.16 | Analisi delle applicazioni | DC 7.16 e VDA 7.15 | Tutte |
| 7.16 | API OData V.4 | DC 7.16 | Tutte |
| 7.16 | Shadowing degli utenti di VDA Linux | VDA 7.16 | Tutte |
| 7.16 | Supporto dei gruppi locali di dominio | Nessuna | Tutte |
| 7.16 | Accesso alla console della macchina | DC 7.16 | Tutte |
| 7.15 | Monitoraggio degli errori delle applicazioni | DC 7.15 e VDA 7.15 | Tutte |
| 7.14 | Risoluzione dei problemi incentrata sulle applicazioni | DC 7.13 e VDA 7.13 | Tutte |
| 7.14 | Monitoraggio disco | DC 7.14 e VDA 7.14 | Tutte |
| 7.14 | Monitoraggio GPU | DC 7.14 e VDA 7.14 | Tutte |
| 7.13 | Protocollo di trasporto nel riquadro Session Details (Dettagli sessione) | DC 7.x e VDA 7.13 | Tutte |
| 7.12 | Descrizioni in linguaggio accessibile degli errori di connessione e delle macchine | DC 7.12 e VDA 7.x | Tutte |

| Versione di Director | Funzionalità | Dipendenze - versione minima richiesta | Versione |
|---|---|---|---|
| 7.12 | Maggiore disponibilità dei dati storici nella versione Enterprise | DC 7.12 e VDA 7.x | Enterprise |
| 7.12 | Reporting personalizzato | DC 7.12 e VDA 7.x | Premium (precedentemente Platinum) |
| 7.11 | Report sull'utilizzo delle risorse | DC 7.11 e VDA 7.11 | Tutte |
| 7.11 | Avvisi estesi per condizioni legate a CPU, memoria e tempo di round trip ICA | DC 7.11 e VDA 7.11 | Premium (precedentemente Platinum) |
| 7.11 | Miglioramenti dell'esportazione di report | DC 7.11 e VDA 7.x | Tutte |
| 7.11 | Integrazione con Citrix ADM | DC 7.11, VDA 7.x e MAS versione 11.1 Build 49.16 | Premium (precedentemente Platinum) |
| 7.9 | Suddivisione della durata dell'accesso | DC 7.9 e VDA 7.x | Tutte |
| 7.7 | Monitoraggio e avvisi proattivi | DC 7.7 e VDA 7.x | Premium (precedentemente Platinum) |
| 7.7 | Integrazione SCOM | DC 7.7, VDA 7.x, SCOM 2012 R2 e PowerShell 3.0 | Premium (precedentemente Platinum) |
| 7.7 | Integrazione con autenticazione Windows | DC 7.x e VDA 7.x | Tutte |
| 7.7 | Utilizzo del sistema operativo a sessione singola e multisessione | DC 7.7 e VDA 7.x | Premium (precedentemente Platinum) |

| Versione di Director | Funzionalità | Dipendenze - versione minima richiesta | Versione |
|---|---|---|---|
| 7.6.300 | Supporto del canale virtuale Framehawk | DC 7.6 e VDA 7.6 | Tutte |
| 7.6.200 | Integrazione della registrazione della sessione | DC 7.6 e VDA 7.x | Premium (precedentemente Platinum) |
| 7 | Integrazione di HDX Insight | DC 7.6, VDA 7.x e Citrix ADM | Premium (precedentemente Platinum) |

## Granularità e conservazione dei dati

January 7, 2024

### Aggregazione dei valori dei dati

Il servizio di monitoraggio raccoglie vari dati, tra cui l'utilizzo della sessione utente, i dettagli sulle prestazioni di accesso dell'utente, i dettagli del bilanciamento del carico della sessione e le informazioni relative alla connessione e ai guasti della macchina. I dati vengono aggregati in modo diverso a seconda della categoria. Comprendere l'aggregazione dei valori dei dati presentati utilizzando le API del metodo OData è fondamentale per l'interpretazione dei dati. Ad esempio:

- Per un determinato periodo di tempo si verificano errori relativi alle sessioni connesse e alle macchine. Pertanto, sono espressi come valori massimi in un periodo di tempo.
- LogOn Duration (Durata dell'accesso) è una misura della durata del tempo, quindi viene espressa come media in un periodo di tempo.
- LogOn Count (Conteggio degli accessi) e Connection Failures (Errori di connessione) sono conteggi di occorrenze in un determinato periodo di tempo, pertanto vengono espressi come somme nell'arco di un periodo di tempo.

### Valutazione simultanea dei dati

Le sessioni devono essere sovrapposte per essere considerate simultanee. Tuttavia, quando l'intervallo di tempo è di 1 minuto, tutte le sessioni in quel minuto (che si sovrappongano o meno) sono con-

siderate simultanee. La dimensione dell'intervallo è così piccola che il sovraccarico delle prestazioni correlato al calcolo della precisione non ha sostanzialmente valore. Se le sessioni si verificano nella stessa ora, ma non nello stesso minuto, non vengono considerate sovrapposte.

### Correlazione delle tabelle di riepilogo con dati non elaborati

Il modello di dati rappresenta le metriche in due modi diversi:

- Le tabelle di riepilogo rappresentano viste aggregate delle metriche in granularità al minuto, ora e giorno.
- I dati non elaborati rappresentano singoli eventi o lo stato corrente individuati nella sessione, nella connessione, nell'applicazione e in altri oggetti.

Quando si tenta di correlare i dati tra le chiamate API o all'interno del modello di dati stesso, è importante comprendere i seguenti concetti e limitazioni:

- **Nessun dato di riepilogo per intervalli parziali.** I riepiloghi delle metriche sono progettati per soddisfare le esigenze delle tendenze storiche per lunghi periodi di tempo. Queste metriche vengono aggregate nella tabella di riepilogo per intervalli completi. Non ci sono dati di riepilogo per un intervallo parziale all'inizio (dati più vecchi disponibili) della raccolta dati né alla fine. Quando si visualizzano aggregazioni di un giorno (Interval=1440), ciò significa che i primi e i più recenti giorni incompleti non hanno dati. Sebbene possano esistere dati non elaborati per questi intervalli parziali, non vengono mai riassunti. È possibile determinare il primo e l'ultimo intervallo di aggregazione per una particolare granularità dei dati estraendo il valore SummaryDate minimo e massimo da una determinata tabella di riepilogo. La colonna SummaryDate (Data riepilogo) rappresenta l'inizio dell'intervallo. La colonna Granularity (Granularità) rappresenta la lunghezza dell'intervallo per i dati aggregati.
- **Correlazione in base al tempo.** Le metriche vengono aggregate nella tabella di riepilogo per intervalli completi come descritto nella sezione precedente. Possono essere utilizzati per le tendenze storiche, ma gli eventi non elaborati potrebbero essere più attuali nello stato di quanto è stato riassunto per l'analisi delle tendenze. Qualsiasi confronto temporale tra riepilogo e dati non elaborati deve considerare che non vi sono dati di riepilogo per intervalli parziali che potrebbero verificarsi o per l'inizio e la fine del periodo di tempo.
- **Eventi mancati e latenti.** Le metriche aggregate nella tabella di riepilogo potrebbero risultare leggermente imprecise se gli eventi non vengono rilevati o sono latenti nel periodo di aggregazione. Sebbene il servizio di monitoraggio cerchi di mantenere uno stato corrente accurato, non torna indietro nel tempo per rielaborare l'aggregazione nelle tabelle di riepilogo per eventi mancanti o latenti.
- **Alta disponibilità della connessione.** Durante l'alta disponibilità della connessione, ci saranno lacune nel conteggio dei dati di riepilogo delle connessioni correnti, ma le istanze di sessione saranno ancora in esecuzione nei dati non elaborati.

- **Periodi di conservazione dei dati.** I dati nelle tabelle di riepilogo vengono conservati in una pianificazione di pulizia diversa dalla pianificazione per i dati non elaborati relativi agli eventi. I dati potrebbero essere mancanti perché sono stati eliminati dal riepilogo o dalle tabelle non elaborate. Anche i periodi di conservazione potrebbero differire a seconda delle diverse granularità dei dati di riepilogo. I dati con granularità inferiore (minuti) vengono puliti più rapidamente rispetto ai dati con granularità più elevata (giorni). Se i dati mancano da una granularità a causa della pulizia, si potrebbero trovare in una granularità più elevata. Poiché le chiamate API restituiscono solo la granularità specifica richiesta, se non si ricevono dati per una granularità non significa che i dati non esistano per una granularità superiore per lo stesso periodo di tempo.
- **Fusi orari.** Le metriche vengono memorizzate con timestamp UTC. Le tabelle di riepilogo sono aggregate in base ai limiti di un'ora del fuso orario. Per i fusi orari che non utilizzano limiti di un'ora, potrebbe esserci qualche discrepanza riguardo a dove i dati sono aggregati.

### Granularità e conservazione

La granularità dei dati aggregati recuperati da Director è una funzione dell'intervallo temporale (T) richiesto. Le regole sono le seguenti:

- 0 < T <= 1 ora - utilizza granularità al minuto
- 0 < T <= 30 giorni - utilizza granularità all'ora
- T > 31 giorni - utilizza granularità al giorno

I dati richiesti che non provengono da dati aggregati provengono dalle informazioni non elaborate sulla sessione e sulla connessione. Questi dati tendono a crescere rapidamente e quindi hanno le proprie impostazioni di pulizia. La pulizia garantisce che solo i dati rilevanti siano conservati a lungo termine. La pulizia garantisce prestazioni migliori pur mantenendo la granularità richiesta per la creazione di report. I clienti dei siti con licenza Premium possono modificare la conservazione della pulizia scegliendo il numero desiderato di giorni di conservazione, altrimenti viene utilizzato il valore predefinito. Se si fosse verificata una perdita di connettività con il database del sito, il Servizio di monitoraggio utilizza i giorni di conservazione predefiniti per il diritto di uso Premium come specificato nella tabella seguente.

Per accedere alle impostazioni, eseguire i seguenti comandi PowerShell sul Delivery Controller:

```
asnp Citrix.*
 Get-MonitorConfiguration
 Set-MonitorConfiguration -<setting name> <value>
<!--NeedCopy-->
```

| | Nome impostazione | Pulizia interessata | Valore predefinito Premium (giorni) | Valore predefinito non Premium (giorni) |
|---|---|---|---|---|
| 1 | GroomSessionsRetentionDays (Giorni di conservazione della pulizia delle sessioni) | SessionRetentionDays (Conservazione dei record sulla sessione e la connessione dopo il termine della sessione | 90 | 7 |
| 2 | GroomFailuresRetentionDays (Giorni di conservazione della pulizia degli errori) | MachineFailureLog (Log degli errori macchina) e ConnectionFailureLog (Log degli errori di connessione) | 90 | 7 |
| 3 | GroomLoadIndexesRetentionDays (Giorni di conservazione della pulizia degli indici di caricamento) | LoadIndex (Indice di caricamento) | 90 | 7 |

| | Nome impostazione | Pulizia interessata | Valore predefinito Premium (giorni) | Valore predefinito non Premium (giorni) |
|---|---|---|---|---|
| 4 | GroomDeletedRetentionDays (Giorni di conservazione della pulizia degli elementi eliminati) | Entità Machine (Macchina), Catalog (Catalogo), DesktopGroup (Gruppo desktop) e Hypervisor con stato del ciclo di vita "Deleted" (Eliminato). Questa impostazione elimina anche tutti i record Session (Sessione), SessionDetail (Dettagli sessione), Summary (Riepilogo), Failure (Errore) o LoadIndex (Indice di caricamento) correlati | 90 | 7 |

| | | Nome impostazione | Pulizia interessata | Valore predefinito Premium (giorni) | Valore predefinito non Premium (giorni) |
|---|---|---|---|---|---|
| | 5 | GroomSummariesRetentionDays (Giorni di conservazione della pulizia dei riepiloghi) | SRetentionDaysDesktopGroup-Summary (Riepilogo dei gruppi desktop), FailureLog-Summary (Riepilogo dei log degli errori) e LoadIndex-Summary (Riepilogo degli indici di caricamento). Dati aggregati: granularità giornaliera | 90 | 7 |
| | 6 | GroomMachineHotfixLogRetentionDays (Giorni di conservazione della pulizia dei log degli hotfix delle macchine) | Hotfix applicati alle macchine con VDA e Controller | 90 | 90 |
| | 7 | GroomMinuteRetentionDays (Giorni di conservazione della pulizia dei minuti) | Dati aggregati - granularità al minuto | 3 | 3 |

| | | Nome impostazione | Pulizia interessata | Valore predefinito Premium (giorni) | Valore predefinito non Premium (giorni) |
|---|---|---|---|---|---|
| | 8 | GroomHourlyRetentionDays (Giorni di conservazione della pulizia delle ore) | Dati aggregati - granularità oraria | 32 | 7 |
| | 9 | GroomApplicationInstanceRetentionDays (Giorni di conservazione della pulizia delle istanze delle applicazioni) | Cronologia dell'istanza dell'applicazione | 90 | 0 |
| | 10 | GroomNotificationLogRetentionDays (Giorni di conservazione della pulizia dei log delle notifiche) | Record di log delle notifiche | 90 | 90 |
| | 11 | GroomResourceUsageRawDataRetentionDays (Giorni di conservazione della pulizia dei dati non elaborati sull'utilizzo delle risorse) | Dati sull'utilizzo delle risorse - dati non elaborati | 1 | 1 |
| | 12 | GroomResourceUsageMinuteDataRetentionDays (Giorni di conservazione della pulizia dei dati sui minuti di utilizzo delle risorse) | Dati di riepilogo dell'utilizzo delle risorse - granularità al minuto | 7 | 7 |

| | Nome impostazione | Pulizia interessata | Valore predefinito Premium (giorni) | Valore predefinito non Premium (giorni) |
|---|---|---|---|---|
| 13 | GroomResourceUsageHourDataRetentionDays (Giorni di conservazione della pulizia dei dati delle ore di utilizzo delle risorse) | Dati di riepilogo dell'utilizzo delle risorse - granularità all'ora | 30 | 7 |
| 14 | GroomResourceUsageDayDataRetentionDays (Giorni di conservazione della pulizia dei dati dei giorni di utilizzo delle risorse) | Dati di riepilogo dell'utilizzo delle risorse - granularità al giorno | 90 | 7 |
| 15 | GroomProcessUsageRawDataRetentionDays (Giorni di conservazione della pulizia dei dati non elaborati di utilizzo dei processi) | Dati di pulizia dei processi - dati non elaborati | 1 | 1 |
| 16 | GroomProcessUsageMinuteDataRetentionDays (Giorni di conservazione della pulizia dei dati dei minuti di utilizzo dei processi) | Dati di pulizia dei processi - granularità al minuto | 3 | 3 |

| | Nome impostazione | Pulizia interessata | Valore predefinito Premium (giorni) | Valore predefinito non Premium (giorni) |
|---|---|---|---|---|
| 17 | GroomProcessUsageHourDataRetentionDays (Giorni di conservazione della pulizia delle ore di utilizzo dei processi) | Dati di utilizzo dei processi - granularità all'ora | 7 | 7 |
| 18 | GroomProcessUsageDayDataRetentionDays (Giorni di conservazione della pulizia dei giorni di utilizzo dei processi) | Dati di utilizzo dei processi - granularità al giorno | 30 | 7 |
| 19 | GroomSessionMetricsDataRetentionDays (Giorni di conservazione della pulizia dei dati delle metriche delle sessioni) | Dati delle metriche delle sessioni | 1 | 1 |
| 20 | GroomMachineMetricsDataRetentionDays (Giorni di conservazione della pulizia dei dati delle metriche delle macchine) | Dati delle metriche delle macchine | 3 | 3 |

| | Nome impostazione | Pulizia interessata | Valore predefinito Premium (giorni) | Valore predefinito non Premium (giorni) |
|---|---|---|---|---|
| 21 | GroomMachineMetricDaySummaryDataRetentionDays (Giorni di conservazione della pulizia dei dati di riepilogo dei giorni delle metriche delle macchine) | Dati di riepilogo delle metriche delle macchine | 90 | 7 |
| 22 | GroomApplicationErrorsRetentionDays (Giorni di conservazione della pulizia degli errori delle applicazioni) | Dati degli errori delle applicazioni | 1 | 1 |
| 23 | GroomApplicationFaultsRetentionDays (Giorni di conservazione della pulizia dei problemi delle applicazioni) | Dati dei problemi delle applicazioni | 1 | 1 |

> **Attenzione:**
>
> La modifica dei valori nel database del servizio di monitoraggio richiede il riavvio del servizio perché i nuovi valori abbiano effetto. Si consiglia di apportare modifiche al database del servizio di monitoraggio solo sotto la direzione di Citrix Support.

Le impostazioni GroomProcessUsageRawDataRetentionDays, GroomResourceUsageRawDataRetentionDays e GroomSessionMetricsDataRetentionDays sono limitate ai valori predefiniti di 1, mentre GroomProcessUsageMinuteDataRetentionDays è limitata al valore predefinito di 3. I comandi PowerShell per impostare questi valori sono stati disabilitati, poiché i dati di utilizzo dei processi tendono a crescere rapidamente.
Inoltre, le impostazioni di conservazione basate sulla licenza sono le seguenti:

- **Siti con licenza Premium**: la conservazione della pulizia di tutte le impostazioni è limitata a 1000 giorni (Citrix consiglia 365 giorni).
- **Siti con licenza avanzata**: la conservazione della pulizia per tutte le impostazioni è limitata a 31 giorni.
- **Tutti gli altri siti**: la conservazione della pulizia per tutte le impostazioni è limitata a 7 giorni.

**Eccezioni:**

- GroomApplicationInstanceRetentionDays può essere impostata solo nei siti con licenza Premium.
- GroomApplicationErrorsRetentionDays e GroomApplicationFaultsRetentionDays sono limitate a 31 giorni nei siti con licenza Premium.

La conservazione dei dati per lunghi periodi ha le seguenti implicazioni sulle dimensioni della tabella:

- **Dati orari.** Se i dati orari possono rimanere nel database per un massimo di due anni, un sito di 1000 gruppi di consegna può causare la crescita del database come segue:

  1000 gruppi di consegna x 24 ore al giorno x 365 giorni all'anno x 2 anni = 17.520.000 righe di dati. L'impatto sulle prestazioni di una quantità così elevata di dati nelle tabelle di aggregazione è significativo. Poiché i dati della dashboard sono ricavati da questa tabella, i requisiti relativi al server del database potrebbero essere notevoli. Una quantità eccessiva di dati potrebbe avere un impatto significativo sulle prestazioni.

- **Dati di sessioni ed eventi.** Dati raccolti ogni volta che viene avviata una sessione e viene effettuata una connessione/riconnessione. Per un sito di grandi dimensioni (100.000 utenti), questi dati crescono rapidamente. Ad esempio, due anni di queste tabelle raccoglierebbero più di un TB di dati, richiedendo un database di livello aziendale di fascia alta.

## Cause di errori e risoluzione dei problemi di Citrix Director

January 7, 2024

Le tabelle seguenti descrivono le varie categorie di errori, i motivi e le azioni da intraprendere per risolvere i problemi. Per ulteriori informazioni, vedere Enumerazioni, codici di errore e descrizioni.

### Errori di connessione

| Categoria | Motivo | Problema | Azione |
| --- | --- | --- | --- |
| N/A | [0] Unknown. Questo codice di errore non è mappato. | Il servizio di monitoraggio non è in grado di determinare il motivo dell'errore di avvio o connessione segnalato dalle informazioni condivise dal servizio Broker. | Raccogliere i log CDF sul controller e contattare il supporto Citrix. |
| [0] None | [1] None | Nessuna | N/A |
| [2] MachineFailure | [2] SessionPreparation | Richiesta di preparazione della sessione dal Delivery Controller al VDA non riuscita. Possibili cause: problemi di comunicazione tra il controller e il VDA, problemi riscontrati dal servizio Broker durante la creazione di una richiesta di preparazione o problemi di rete che determinano la mancata accettazione della richiesta da parte del VDA. | Per problemi comuni che causano problemi di comunicazione tra il controller e il VDA, vedere la procedura di risoluzione dei problemi elencati nell'articolo del Knowledge Center, Risoluzione dei problemi relativi alla registrazione di Virtual Delivery Agent con i Delivery Controller in Citrix Virtual Apps and Desktops. |
| [2] MachineFailure | [3] RegistrationTimeout | Il VDA era acceso, ma si è verificato un timeout durante il tentativo di registrazione con il Delivery Controller. | Verificare che il servizio Broker Citrix sia in esecuzione sul Delivery Controller e che il servizio Desktop sia in esecuzione sul VDA. Se sono stati interrotti, avviarli. |

| Categoria | Motivo | Problema | Azione |
| --- | --- | --- | --- |
| [1] ClientConnection-Failure | [4] ConnectionTimeout | Il client non si è connesso al VDA dopo che il VDA è stato preparato per l'avvio della sessione. Il brokering della sessione è stato eseguito correttamente, ma si è verificato un timeout durante l'attesa che il client si connettesse al VDA. Possibili cause: impostazioni del firewall, interruzioni di rete o impostazioni che impediscono le connessioni remote. | Controllare la console di Director per verificare se il client ha attualmente una connessione attiva, il che significa che nessun utente ha subito conseguenze. Se non è presente alcuna sessione, esaminare i log eventi sul client e sul VDA per verificare la presenza di eventuali errori. Risolvere eventuali problemi di connettività di rete tra il client e il VDA. |
| [4] NoLicensesAvailable | [5] Licensing | La richiesta di licenza non è riuscita. Possibili cause: numero insufficiente di licenze o il server delle licenze è rimasto inattivo per più di 30 giorni. | Verificare che il server delle licenze sia online e raggiungibile. Risolvere eventuali problemi relativi alla connettività di rete del server delle licenze o riavviare il server delle licenze in caso di errato funzionamento. Verificare che ci siano licenze sufficienti nell'ambiente e assegnarne altre se necessario. |

| Categoria | Motivo | Problema | Azione |
| --- | --- | --- | --- |
| [1] ClientConnection-Failure | [6] Ticketing | Si è verificato un errore durante la creazione di ticket, il che indica che la connessione client al VDA non corrisponde alla richiesta di cui è stato eseguito il brokering. Un ticket di richiesta di avvio viene preparato dal Broker e consegnato nel file ICA. Quando l'utente tenta di avviare una sessione, il VDA convalida il ticket di avvio nel file ICA con il Broker. Possibili cause: il file ICA è danneggiato o l'utente sta tentando di stabilire una connessione non autorizzata. | Verificare che l'utente abbia accesso all'applicazione o al desktop in base ai gruppi di utenti definiti nei gruppi di consegna. Chiedere all'utente di riavviare l'applicazione o il desktop per determinare se si tratta di un problema temporaneo. Se il problema si verifica di nuovo, esaminare i log eventi del dispositivo client per rilevare eventuali errori. Verificare che il VDA a cui l'utente sta tentando di connettersi sia registrato. Se non è registrato, rivedere i log eventi sul VDA e risolvere eventuali problemi di registrazione. |
| [1] ClientConnection-Failure | [7] Other | Una sessione è stata segnalata come terminata dal VDA dopo che il client ha inizialmente contattato il VDA ma prima che completasse la sequenza di connessione. | Verificare se la sessione non è stata terminata dall'utente prima dell'avvio. Provare a riavviare la sessione, se il problema persiste, raccogliere i log CDF e contattare il supporto Citrix. |

| Categoria | Motivo | Problema | Azione |
| --- | --- | --- | --- |
| [1] ClientConnection-Failure | [8] GeneralFail | La sessione non è stata avviata. Possibili cause: è stato richiesto un avvio di cui è stato eseguito il brokering mentre il Broker si stava ancora avviando o inizializzando, oppure si è verificato un errore interno durante la fase di brokering di un avvio. | Verificare che il servizio Broker Citrix sia in esecuzione e riprovare ad avviare la sessione. |
| [5] Configuration | [9] MaintenanceMode | Il VDA, o il gruppo di consegna a cui appartiene il VDA, è configurato in modalità di manutenzione. | Determinare se la modalità di manutenzione è necessaria. Disabilitare la modalità di manutenzione sul gruppo di consegna o sulla macchina in questione se non è necessaria e chiedere all'utente di tentare di riconnettersi. |
| [5] Configuration | [10] ApplicationDisabled | Gli utenti finali non possono accedere all'applicazione perché è stata disabilitata dall'amministratore. | Se l'applicazione è destinata a essere disponibile per l'uso in produzione, abilitarla e chiedere all'utente di riconnettersi. |

| Categoria | Motivo | Problema | Azione |
| --- | --- | --- | --- |
| [4] NoLicensesAvailable | [11] LicenseFeature Refused | La funzionalità utilizzata non è coperta dalle licenze esistenti. | Contattare un rappresentante commerciale Citrix per confermare le funzionalità coperte dalla versione e dal tipo di licenza Citrix Virtual Apps and Desktops esistenti. |
| [3] NoCapacityAvailable | [13] SessionLimitReached | Tutti i VDA sono in uso e non è disponibile capacità per ospitare altre sessioni. Possibili cause: tutti i VDA sono in uso (per i VDA con sistema operativo a sessione singola) oppure tutti i VDA hanno raggiunto il numero massimo di sessioni simultanee configurate consentito (per i VDA con sistema operativo multisessione). | Verificare se sono presenti VDA in modalità di manutenzione. Disabilitare la modalità di manutenzione se non è necessaria, per liberare più capacità. È consigliabile aumentare il valore di **Maximum Number of Sessions** (Numero massimo di sessioni) nell'impostazione dei criteri Citrix per consentire più sessioni per i VDA del server. Prendere in considerazione l'aggiunta di altri VDA con sistema operativo multisessione. Prendere in considerazione l'aggiunta di altri VDA con sistema operativo a sessione singola. |

| Categoria | Motivo | Problema | Azione |
| --- | --- | --- | --- |
| [5] Configuration | [14] DisallowedProtocol | I protocolli ICA e RDP non sono consentiti. | Eseguire il comando PowerShell **Get-BrokerAccessPolicyRule** sul Delivery Controller e verificare che il valore **AllowedProtocols** (Protocolli consentiti) disponga di tutti i protocolli desiderati. Questo problema si verifica solo in caso di errata configurazione. |
| [5] Configuration | [15] ResourceUnavailable | L'applicazione o il desktop a cui l'utente sta tentando di connettersi non è disponibile. L'applicazione o il desktop potrebbe non esistere o non sono disponibili VDA per l'esecuzione. Possibili cause: l'applicazione o il desktop non sono stati pubblicati o i VDA che ospitano l'applicazione o il desktop hanno raggiunto il carico massimo oppure l'applicazione o il desktop sono configurati in modalità di manutenzione. | Verificare che l'applicazione o il desktop siano ancora pubblicati e che i VDA non siano in modalità di manutenzione. Determinare se i VDA con sistema operativo multisessione sono a pieno carico. In tal caso, eseguire il provisioning di più VDA con sistema operativo multisessione. Verificare che siano disponibili VDA con sistema operativo a sessione singola per le connessioni. Se necessario, eseguire il provisioning di più VDA con sistema operativo a sessione singola. |

| Categoria | Motivo | Problema | Azione |
| --- | --- | --- | --- |
| [5] Configuration | [16] ActiveSessionReconnectDisabled | La sessione ICA è attiva e connessa a un endpoint diverso. Tuttavia, poiché l'opzione **Active Session Reconnection** (Riconnessione della sessione attiva) è disabilitata, il client non può connettersi alla sessione attiva. | Sul Delivery Controller, verificare che l'opzione **Active Session Reconnection** (Riconnessione della sessione attiva) sia abilitata. Verificare che il valore di **DisableActiveSessionReconnect** nel Registro di sistema, in **HKEY_LOCAL_MACHINE\Software** sia impostato su 0. |
| [2] MachineFailure | [17] NoSessionToReconnect | Il client ha tentato di riconnettersi a una sessione specifica, ma la sessione è stata terminata. | Riprovare la riconnessione del controllo dell'area di lavoro. |

| Categoria | Motivo | Problema | Azione |
| --- | --- | --- | --- |
| [2] MachineFailure | [18] SpinUpFailed | Il VDA non può essere acceso per l'avvio della sessione. Si tratta di un problema segnalato dall' hypervisor. | Se la macchina è ancora spenta, provare ad avviarla da Citrix Studio. Se l' operazione non riesce, esaminare la connettività e le autorizzazioni dell' hypervisor. Se il VDA è una macchina con provisioning PVS, verificare nella console PVS che la macchina sia in esecuzione. In caso contrario, verificare che alla macchina sia assegnato un Personal vDisk, accedere all' hypervisor per reimpostare la VM. |
| [2] MachineFailure | [19] Refused | Il Delivery Controller invia una richiesta al VDA per prepararsi a una connessione da parte di un utente finale, ma il VDA rifiuta attivamente questa richiesta. | Verificare tramite ping che il Delivery Controller e il VDA possano comunicare correttamente. In caso contrario, risolvere eventuali problemi di firewall o di routing di rete. |

| Categoria | Motivo | Problema | Azione |
| --- | --- | --- | --- |
| [2] MachineFailure | [20] ConfigurationSet Failure | Il Delivery Controller non ha inviato al VDA i dati di configurazione richiesti, come le impostazioni dei criteri e le informazioni sulla sessione, durante l'avvio della sessione. Possibili cause: problemi di comunicazione tra il controller e il VDA, problemi riscontrati dal servizio Broker durante la creazione di una richiesta di impostazione della configurazione o problemi di rete che determinano la mancata accettazione della richiesta da parte del VDA. | - |
| [3] NoCapacityAvailable | [21] MaxTotalInstance-sExceeded | È stato raggiunto il numero massimo di istanze di un'applicazione. Non è possibile aprire istanze aggiuntive dell'applicazione sul VDA. Questo problema è correlato alla funzionalità dei limiti dell'applicazione. | Prendere in considerazione l'aumento dell'impostazione dell'applicazione **Limit the number of instances running at the same time** (Limita il numero di istanze in esecuzione contemporaneamente) su un valore più elevato, se la licenza lo consente. |

| Categoria | Motivo | Problema | Azione |
| --- | --- | --- | --- |
| [3] NoCapacityAvailable | [22] MaxPerUserInstancesExceeded | L'utente sta tentando di aprire più istanze di un'applicazione, ma l'applicazione è configurata per consentire solo una singola istanza dell'applicazione per utente. Questo problema è correlato alla funzionalità dei limiti dell'applicazione. | Per impostazione predefinita, è consentita solo un'istanza dell'applicazione per utente. Se sono necessarie più istanze per utente, prendere in considerazione la possibilità di deselezionare l'impostazione **Limit to one instance per user** (Limita a un'istanza per utente) nelle impostazioni dell'applicazione. |
| [1] ClientConnectionFailure | [23] Communication error | Il Delivery Controller ha tentato di inviare informazioni al VDA, ad esempio una richiesta di preparazione per una connessione, ma si è verificato un errore durante il tentativo di comunicazione. Ciò può essere causato da interruzioni della rete. | Se è già avviato, riavviare il servizio Desktop sul VDA per riavviare il processo di registrazione e verificare che il VDA si registri correttamente. Verificare che i Delivery Controller configurati per il VDA siano accurati tramite i dettagli nel log eventi dell'applicazione. |

| Categoria | Motivo | Problema | Azione |
| --- | --- | --- | --- |
| [3] NoCapacityAvailable | [100] NoMachineAvailable Il servizio di monitoraggio converte [12] NoDesktopAvailable in questo codice di errore. | Il VDA assegnato per avviare la sessione è in uno stato non valido o non è disponibile. Possibili cause: lo stato di alimentazione del VDA è sconosciuto o non disponibile, il VDA non è stato riavviato dall'ultima sessione dell'utente, la condivisione della sessione è disabilitata mentre la sessione corrente richiede che sia abilitata oppure il VDA è stato rimosso dal gruppo di consegna o dal sito. | Verificare che il VDA si trovi in un gruppo di consegna. In caso contrario, aggiungerlo al gruppo di consegna appropriato. Verificare che vi siano sufficienti VDA registrati e pronti per poter avviare il desktop condiviso pubblicato o l'applicazione richiesta dall'utente. Verificare che l'hypervisor che ospita il VDA non sia in modalità di manutenzione. |

| Categoria | Motivo | Problema | Azione |
| --- | --- | --- | --- |
| [2] MachineFailure | [101] MachineNotFunctional. Il servizio di monitoraggio converte [12] NoDesktopAvailable in questo codice di errore. | Il VDA non è operativo. Possibili cause: il VDA è stato rimosso dal gruppo di consegna, il VDA non è registrato, lo stato di alimentazione del VDA non è disponibile o il VDA sta riscontrando problemi interni. | Verificare che il VDA si trovi in un gruppo di consegna. In caso contrario, aggiungerlo al gruppo di consegna appropriato. Verificare che il VDA venga visualizzato come acceso in Citrix Studio. Se lo stato di alimentazione è sconosciuto per più macchine, risolvere eventuali problemi relativi alla connettività all'hypervisor o agli errori dell'host. Verificare che l'hypervisor che ospita il VDA non sia in modalità di manutenzione. Riavviare il VDA una volta risolti questi problemi. |

### Tipo di guasto della macchina

| Codice di errore | ID codice di errore | Problema | Azione |
| --- | --- | --- | --- |
| Unknown (Sconosciuto) | - | - | - |
| Unregistered (Non registrato) | 3 | - | - |

| Codice di errore | ID codice di errore | Problema | Azione |
|---|---|---|---|
| MaxCapacity (rappresentato come Max Load su Director) | 4 | La macchina sta segnalando se stessa alla massima capacità, ossia Max Load Index | Assicurarsi che tutti gli hypervisor siano accesi. Aggiungere altre macchine ai Delivery Group interessati aggiungendo più capacità all'hypervisor o aggiungendo altri hypervisor. |
| StuckOnBoot (Blocco all'avvio) | 2 | La VM non ha completato la sequenza di avvio e non comunica con l'hypervisor. | Assicurarsi che la VM sia stata avviata correttamente sull'hypervisor. Controllare la presenza di altri messaggi sulla VM, ad esempio problemi del sistema operativo. Assicurarsi che gli strumenti dell'hypervisor siano installati sulla VM. Assicurarsi che il VDA sia installato sulla VM. |
| FailedToStart (Impossibile avviare) | 1 | La VM ha riscontrato problemi durante il tentativo di avviare l'hypervisor. | Controllare i log dell'hypervisor. |
| Nessuna | 0 | - | - |

**Motivo della cancellazione della registrazione della macchina (applicabile quando il tipo di errore è Unregistered [Non registrato] o Unknown [Sconosciuto])**

| Codice di errore | ID codice di errore | Problema | Azione |
|---|---|---|---|
| AgentShutdown (Spegnimento dell'agente) | 0 | Il VDA ha sperimentato un arresto normale. | Accendere il VDA se non si prevede che sia spento, in base ai criteri di gestione dell'alimentazione esistenti. Esaminare eventuali errori nei log eventi. |
| AgentSuspended (Agente sospeso) | 1 | Il VDA è in modalità di ibernazione o sospensione. | Far uscire il VDA dalla modalità di ibernazione. Prendere in considerazione la disabilitazione dell'ibernazione per i VDA Citrix Virtual Apps and Desktops tramite le impostazioni di alimentazione. |
| IncompatibleVersion (Versione incompatibile) | 100 | Il VDA non può comunicare con il Delivery Controller a causa di una mancata corrispondenza nelle versioni del protocollo Citrix. | Allineare le versioni del VDA e del Delivery Controller. |

| Codice di errore | ID codice di errore | Problema | Azione |
| --- | --- | --- | --- |
| AgentAddressResolutionFailed (Risoluzione dell'indirizzo agente non riuscita) | 101 | Il Delivery Controller non è stato in grado di risolvere l'indirizzo IP del VDA. | Verificare che l'account della macchina VDA esista in AD. In caso contrario, crearlo. Verificare che il nome e l'indirizzo IP del VDA nel DNS siano accurati. In caso contrario, correggerli. Se il problema è diffuso, convalidare le impostazioni DNS sui Delivery Controller. Verificare la risoluzione DNS dal controller eseguendo il comando`nslookup`. |
| | 101 | Il Delivery Controller non è stato in grado di risolvere l'indirizzo IP del VDA. | Verificare che l'account della macchina VDA esista in AD. In caso contrario, crearlo. Verificare che il nome e l'indirizzo IP del VDA nel DNS siano accurati. In caso contrario, correggerli. |

| Codice di errore | ID codice di errore | Problema | Azione |
| --- | --- | --- | --- |
| AgentNotContactable (Agente non contattabile) | 102 | Si è verificato un problema di comunicazione tra il Delivery Controller e il VDA. | Utilizzare un comando ping per verificare che il Delivery Controller e il VDA siano in grado di comunicare correttamente. In caso contrario, risolvere eventuali problemi del firewall o di rete. Per i problemi comuni che causano problemi di comunicazione tra il controller e il VDA, vedere la procedura di risoluzione dei problemi elencati nell'articolo del Knowledge Center, Risoluzione dei problemi relativi alla registrazione di Virtual Delivery Agent con i Delivery Controller in Citrix Virtual Apps and Desktops (CTX136668). |

| Codice di errore | ID codice di errore | Problema | Azione |
|---|---|---|---|
| | 102 | Si è verificato un problema di comunicazione tra il Delivery Controller e il VDA. | Per i problemi comuni che causano problemi di comunicazione tra il controller e il VDA, vedere la procedura di risoluzione dei problemi elencati nell'articolo del Knowledge Center, Risoluzione dei problemi relativi alla registrazione di Virtual Delivery Agent con i Delivery Controller in Citrix Virtual Apps and Desktops (CTX136668). Contattare il supporto Citrix. |
| AgentWrongActiveDirectoryOU (UO di Active Directory dell'agente errata) | 103 | Si è verificato un errore di configurazione del rilevamento di Active Directory. L'unità organizzativa specifica del sito (dove le informazioni del controller del sito sono memorizzate in AD) configurata nel Registro di sistema del VDA è per un sito diverso. | Assicurarsi che la configurazione di Active Directory sia corretta o controllare le impostazioni del Registro di sistema. |
| EmptyRegistrationRequest (Richiesta di registrazione vuota) | 104 | La richiesta di registrazione inviata dal VDA al Directory Controller era vuota. Ciò può essere dovuto a un'installazione del software VDA corrotta. | Riavviare il servizio Desktop sul VDA per riavviare il processo di registrazione e verificare che il VDA si registri correttamente tramite il log eventi dell'applicazione. |

| Codice di errore | ID codice di errore | Problema | Azione |
|---|---|---|---|
| MissingRegistrationCapabilities (Funzionalità di registrazione mancanti) | 105 | La versione del VDA non è compatibile con il Delivery Controller. | Aggiornare il VDA o rimuovere il VDA e quindi reinstallarlo. |
| MissingAgentVersion (Versione agente mancante) | 106 | La versione del VDA non è compatibile con il Delivery Controller. | Reinstallare il software VDA se il problema riguarda tutte le macchine. |
| InconsistentRegistrationCapabilities (Funzionalità di registrazione incoerenti) | 107 | Il VDA non è in grado di comunicare le proprie funzionalità al Broker. Ciò può essere dovuto all'incompatibilità tra le versioni del VDA e del Delivery Controller. Le funzionalità di registrazione, che cambiano con ogni versione, sono espresse in un modo che non corrisponde alla richiesta di registrazione. | Allineare le versioni del VDA e del Delivery Controller. |
| NotLicensedForFeature (Funzionalità non concessa in licenza) | 108 | La funzionalità che si sta cercando di utilizzare non è concessa in licenza. | Controllare la versione delle licenze Citrix oppure rimuovere il VDA e quindi reinstallarlo. |
| | 108 | La funzionalità che si sta cercando di utilizzare non è concessa in licenza. | Contattare il supporto Citrix. |
| UnsupportedCredentialSecurity version (Versione della sicurezza delle credenziali non supportata) | 109 | Il VDA e il Delivery Controller non utilizzano lo stesso meccanismo di crittografia. | Allineare le versioni del VDA e del Delivery Controller. |

| Codice di errore | ID codice di errore | Problema | Azione |
| --- | --- | --- | --- |
| InvalidRegistrationRequest (Richiesta di registrazione non valida) | 110 | Il VDA ha inviato una richiesta di registrazione al Broker, ma il contenuto della richiesta è danneggiato o non è valido. | Per i problemi comuni che causano problemi di comunicazione tra il controller e il VDA, vedere la procedura di risoluzione dei problemi elencati nell'articolo del Knowledge Center, Risoluzione dei problemi relativi alla registrazione di Virtual Delivery Agent con i Delivery Controller in Citrix Virtual Apps and Desktops (CTX136668). |
| SingleMultiSessionMismatch (Mancata corrispondenza multisessione singola) | 111 | Il tipo di sistema operativo del VDA non è compatibile con il catalogo delle macchine o il gruppo di consegna. | Aggiungere il VDA al tipo di catalogo delle macchine o al gruppo di consegna corretto contenente macchine con lo stesso sistema operativo. |
| FunctionalLevelTooLowForCatalog (Livello funzionale troppo basso per il catalogo) | 112 | Il catalogo delle macchine è impostato su un livello funzionale VDA superiore rispetto alla versione di VDA installata. | Verificare che il livello funzionale del catalogo delle macchine del VDA corrisponda a quello del VDA. Aggiornare il catalogo delle macchine o eseguirne il downgrade in modo che corrisponda a quello del VDA. |

| Codice di errore | ID codice di errore | Problema | Azione |
| --- | --- | --- | --- |
| FunctionalLevelTooLowForDesktopGroup (Livello funzionale troppo basso per il gruppo desktop) | 112 | Il gruppo di consegna è impostato su un livello funzionale del VDA superiore rispetto alla versione di VDA installata. | Verificare che il livello funzionale del gruppo di consegna del VDA corrisponda a quello del VDA. Aggiornare il catalogo delle macchine o eseguirne il downgrade in modo che corrisponda a quello del VDA. |
| PowerOff (Spegnimento) | 200 | Il VDA non si è chiuso correttamente. | Se il VDA deve essere acceso, provare ad avviare il VDA da Citrix Studio e verificare che si avvii e si registri correttamente. Risolvere gli eventuali problemi di avvio o registrazione. Esaminare i log eventi sul VDA una volta eseguito il backup per determinare la causa principale dello spegnimento. |
| AgentRejectedSettingsUpdate (Aggiornamento delle impostazioni rifiutato dall'agente) | 203 | Impostazioni come i criteri Citrix sono state modificate o aggiornate, ma si è verificato un errore nell'invio degli aggiornamenti al VDA. Ciò può verificarsi se gli aggiornamenti non sono compatibili con la versione del VDA installata. | Se necessario, aggiornare il VDA. Controllare se gli aggiornamenti applicati sono supportati con la versione del VDA. |

| Codice di errore | ID codice di errore | Problema | Azione |
| --- | --- | --- | --- |
| SessionPrepareFailure (Errore di preparazione della sessione) | 206 | Il Broker non ha completato un controllo delle sessioni in esecuzione sul VDA. | Se il problema è diffuso, riavviare il servizio Broker Citrix sul Delivery Controller. |
| | 206 | Il Broker non ha completato un controllo delle sessioni in esecuzione sul VDA. | Contattare il supporto Citrix. |
| ContactLost (Perdita di contatto) | 207 | Il Delivery Controller ha perso la connessione con il VDA. Ciò può essere causato da interruzioni di rete. | Verificare che il servizio Broker Citrix sia in esecuzione sul Delivery Controller e che il servizio Desktop sia in esecuzione sul VDA. Se sono stati interrotti, avviarli. Se è già avviato, riavviare il servizio Desktop sul VDA per riavviare il processo di registrazione e verificare che il VDA si registri correttamente. Verificare che i Delivery Controller configurati per il VDA siano accurati tramite i dettagli nel log eventi dell'applicazione. Utilizzare un comando ping per verificare che il Delivery Controller e il VDA siano in grado di comunicare correttamente. In caso contrario, risolvere eventuali problemi del firewall o di rete. |

| Codice di errore | ID codice di errore | Problema | Azione |
| --- | --- | --- | --- |
| | 207 | Il Delivery Controller ha perso la connessione con il VDA. Ciò può essere causato da interruzioni di rete. | Verificare che il servizio Desktop sia in esecuzione sul VDA. Se è interrotto, avviarlo. |
| BrokerRegistrationLimitReached (Limite di registrazione del Broker raggiunto) | 201 | Il Delivery Controller ha raggiunto il numero massimo configurato di VDA a cui è consentito di registrarsi contemporaneamente. Per impostazione predefinita, il Delivery Controller consente 10.000 registrazioni VDA simultanee. | Prendere in considerazione l'aggiunta di Delivery Controller al sito o la creazione di un sito. È inoltre possibile aumentare il numero di VDA autorizzati a registrarsi contemporaneamente con il Delivery Controller tramite la chiave del Registro di sistema **HKEY_LOCAL_MACHINE\Software** Per ulteriori informazioni, vedere l'articolo del Knowledge Center Chiavi del Registro di sistema utilizzate da Citrix Virtual Apps and Desktops (CTX117446). L'aumento di questo numero potrebbe richiedere più risorse di CPU e memoria per il controller. |

| Codice di errore | ID codice di errore | Problema | Azione |
| --- | --- | --- | --- |
| SettingsCreationFailure (Errore di creazione delle impostazioni) | 208 | Il Broker non ha creato una serie di impostazioni e configurazioni da inviare al VDA. Se il Broker non è in grado di raccogliere i dati, la registrazione non riesce e il VDA non viene registrato. | Controllare i log eventi sul Delivery Controller per verificare la presenza di eventuali errori. Riavviare il servizio Broker se i log non indicano un problema specifico. Una volta riavviato il servizio Broker, riavviare il servizio Desktop sui VDA interessati e verificare che si registrino correttamente. |
| | 208 | Il Broker non ha creato una serie di impostazioni e configurazioni da inviare al VDA. Se il Broker non è in grado di raccogliere i dati, la registrazione non riesce e il VDA non viene registrato. | Riavviare il servizio Desktop sui VDA interessati e verificare che si registrino correttamente. Contattare il supporto Citrix. |

| Codice di errore | ID codice di errore | Problema | Azione |
|---|---|---|---|
| SendSettingsFailure (Errore di invio delle impostazioni) | 204 | Il Broker non ha inviato impostazioni e dati di configurazione al VDA. Se il Broker è in grado di raccogliere i dati ma non è in grado di inviarli, la registrazione non riesce. | Se è limitato a un singolo VDA, riavviare il servizio Desktop sul VDA per forzare una nuova registrazione e verificare che il VDA si registri correttamente tramite il log eventi dell'applicazione. Risolvere eventuali errori riscontrati. Per i problemi comuni che causano problemi di comunicazione tra il controller e il VDA, vedere la procedura di risoluzione dei problemi elencati nell'articolo del Knowledge Center, Risoluzione dei problemi relativi alla registrazione di Virtual Delivery Agent con i Delivery Controller in Citrix Virtual Apps and Desktops (CTX136668). |
| AgentRequested (Agente richiesto) | 2 | Si è verificato un errore sconosciuto. | Contattare il supporto Citrix. |
| DesktopRestart (Riavvio del desktop) | 201 | Si è verificato un errore sconosciuto. | Contattare il supporto Citrix. |
| DesktopRemoved (Desktop rimosso) | 202 | Si è verificato un errore sconosciuto. | Contattare il supporto Citrix. |
| SessionAuditFailure (Errore di controllo della sessione) | 205 | Si è verificato un errore sconosciuto. | Contattare il supporto Citrix. |
| UnknownError (Errore sconosciuto) | 300 | Si è verificato un errore sconosciuto. | Contattare il supporto Citrix. |

| Codice di errore | ID codice di errore | Problema | Azione |
|---|---|---|---|
| RegistrationStateMismatch (Mancata corrispondenza dello stato di registrazione) | 302 | Si è verificato un errore sconosciuto. | Contattare il supporto Citrix. |
| Unknown (Sconosciuto) | - | Si è verificato un errore sconosciuto. | Contattare il supporto Citrix. |

## Avvisi di terze parti

January 7, 2024

Questa versione di Citrix Virtual Apps and Desktops potrebbe includere software di terze parti concessi in licenza in base ai termini definiti nei seguenti documenti:

- Avvisi di terze parti per Citrix Virtual Apps and Desktops (download del PDF)
- Non-Commercial Software Disclosures For FlexNet Publisher 2017 (11.15.0.0) (download del PDF)
- Supplemento alla documentazione di FlexNet Publisher, software open source di terze parti utilizzato in FlexNet Publisher 11.15.0 (download del PDF)

## SDK e API

January 7, 2024

Con questa versione sono disponibili diversi SDK e API. Per accedere agli SDK e alle API, andare a Creare qualsiasi cosa con Citrix. Da lì, selezionare **Citrix Workspace** per accedere alle informazioni di programmazione per Citrix Virtual Apps and Desktops e ai relativi componenti.

> **Nota:**
>
> Citrix Virtual Apps and Desktops SDK e Citrix Group Policy SDK possono essere installati come modulo o snap-in. Diversi SDK componenti (come Citrix Licensing, Citrix Provisioning e StoreFront) vengono installati utilizzando solo uno snap-in.

Questo prodotto supporta le versioni di PowerShell dalla 3 alla 5.

### Citrix Virtual Apps and Desktops SDK

Questo SDK viene installato automaticamente come modulo PowerShell quando si installa un Delivery Controller o Studio. Ciò consente di utilizzare i cmdlet di questo SDK senza dover aggiungere snap-in. Se si sceglie di installare questo SDK come snap-in, le istruzioni sono fornite di seguito.

#### Autorizzazioni

È necessario eseguire la shell o lo script utilizzando un'identità con diritti di amministrazione Citrix. Sebbene i membri del gruppo di amministratori locali sul controller abbiano automaticamente privilegi amministrativi completi per consentire l'installazione di Citrix Virtual Apps o Citrix Virtual Desktops, Citrix consiglia di creare amministratori Citrix con i diritti appropriati per le normali attività, anziché utilizzare l'account degli amministratori locali.

#### Accedere ai cmdlet ed eseguirli

1. Avviare una shell in PowerShell: aprire Studio, selezionare la scheda **PowerShell** e quindi fare clic su **Launch PowerShell** (Avvia PowerShell).
2. Per utilizzare i cmdlet SDK all'interno degi script, impostare il criterio di esecuzione in PowerShell. Per ulteriori informazioni sui criteri di esecuzione di PowerShell, vedere la documentazione Microsoft.
3. Se si desidera utilizzare lo snap-in (anziché il modulo), aggiungere lo snap-in utilizzando il cmdlet `Add-PSSnapin` (o `asnp`).

   V1 e V2 indicano la versione dello snap-in. Gli snap-in di XenDesktop 5 corrispondono alla versione 1. Citrix Virtual Apps and Desktops e le versioni precedenti di XenDesktop 7 corrispondono alla versione 2. Ad esempio, per installare lo snap-in Citrix Virtual Apps and Desktops, digitare `Add-PSSnapin Citrix.ADIdentity.Admin.V2`. Per importare tutti i cmdlet, digitare: `Add-PSSnapin Citrix.*.Admin.V*`

È ora possibile utilizzare i cmdlet e i file della guida.

- Per accedere ai file della guida per questo SDK, selezionare il prodotto o il componente nell'elenco Categories (Categorie), quindi selezionare **Citrix Virtual Apps and Desktops SDK** (SDK Citrix Virtual Apps and Desktops).
- Per informazioni su PowerShell, vedere Ambiente di script integrato di Windows PowerShell (ISE).

### SDK Group Policy

L'SDK Citrix Group Policy consente di visualizzare e configurare le impostazioni e i filtri dei Criteri di gruppo. Questa SDK utilizza un provider PowerShell per creare un'unità virtuale corrispondente alle impostazioni e ai filtri della macchina e dell'utente. Il provider viene visualizzato come estensione di `New-PSDrive`.

Per utilizzare l'SDK Group Policy, è necessario installare l'SDK di Studio o Citrix Virtual Apps and Desktops.

Il provider Citrix Group Policy PowerShell è disponibile come modulo o come snap-in.

- Per utilizzare il modulo, non è necessaria alcuna operazione aggiuntiva.
- Per aggiungere lo snap-in, digitare `Add-PSSnapin citrix.common.grouppolicy`.

Per accedere alla guida, digitare: `help New-PSDrive -path localgpo:/`.

Per creare un'unità virtuale e caricarla con le impostazioni, digitare `New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>`, dove la stringa Controller è il nome di dominio completo di un controller nel sito a cui si desidera connettersi e caricare le impostazioni.

### API REST di Citrix Virtual Apps and Desktops

Con le API REST di Citrix Virtual Apps and Desktops, è possibile automatizzare la gestione delle risorse all'interno di una distribuzione di Citrix Virtual Apps and Desktops.

Le API REST di Citrix Virtual Apps and Desktops sono disponibili all'indirizzo https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis. Le API non applicabili a Citrix Virtual Apps and Desktops sono contrassegnate di conseguenza. Seguire le indicazioni riportate qui per configurare l'accesso al servizio API e utilizzare le API per gestire e ottimizzare le risorse.

### Monitor Service OData

L'API Monitor consente l'accesso ai dati del servizio di monitoraggio utilizzando la versione 3 o 4 dell'API OData. È possibile creare dashboard di monitoraggio e reportistica personalizzate in base ai dati interrogati dai dati del servizio di monitoraggio. OData V.4 si basa sull'API Web ASP.NET e supporta le query di aggregazione.

Per ulteriori informazioni, vedere l'API Monitor Service OData.