シトリックス バーチャル アプリケーションズ アンド デスクトップ™ 7 2311

リリースについて

このCitrix Virtual Apps and Desktopsリリースには、Windows Virtual Delivery Agent (VDA) の新しいバージョンと、いくつかのコアコンポーネントの新しいバージョンが含まれています。次のことができます。

- **サイトのインストールまたはアップグレード**: このリリースの ISO を使用して、コアコンポーネントと VDA をインストールまたはアップグレードします。最新バージョンにインストールまたはアップグレードすることで、最新の機能を使用できます。
- **既存のサイトでのVDAのインストールまたはアップグレード**: 展開が既にあり、コアコンポーネントをアップグレードする準備ができていない場合でも、新しいVDAをインストール（またはアップグレード）することで、最新のHDX™機能のいくつかを引き続き使用できます。VDAのみをアップグレードすることは、非本番環境で機能強化をテストしたい場合に役立ちます。

  VDAをこのバージョン（バージョン7.9以降）にアップグレードした後、マシンカタログの機能レベルを更新する必要はありません。7.9（またはそれ以降）の値はデフォルトの機能レベルのままであり、このリリースで有効です。詳しくは、「VDAのバージョンと機能レベル」を参照してください。

インストールとアップグレードの手順：

- 新しいサイトを構築する場合は、「インストールと構成」の順序に従ってください。
- サイトをアップグレードする場合は、「展開のアップグレード」を参照してください。

シトリックス バーチャル アプリケーションズ アンド デスクトップ 7 2311

HDX Direct (プレビュー)

新しい機能強化により、HDX Directは、直接通信が可能な場合、内部および外部のクライアントデバイスがセッションホストと安全な直接接続を確立できるようになりました。詳細については、「HDX Direct」を参照してください。

構成ログへのメタデータ関連付けのサポート

この機能強化により、高レベルの操作で`name-value`ペアを関連付けることで、構成ログにメタデータを添付できるようになりました。詳しくは、「構成ログへのメタデータ関連付け」を参照してください。

オンプレミス向けCitrix Secure Private Access™

オンプレミス向けCitrix Secure Private Accessは、Citrix Virtual Apps and Desktops 2311リリースの一部として一般提供されるようになりました。オンプレミス向けSecure Private Accessソリューションには、Secure Private Accessサービスと同様のルックアンドフィールを持つフルサービスの管理コンソールUIが含まれています。詳細については、「オンプレミス向けCitrix Secure Private Access – 一般提供」を参照してください。

Citrix Hypervisor™がXenServer®にブランド変更

最新のリブランディング戦略に沿って、**Citrix Hypervisor** のすべてのインスタンスを **XenServer®** に更新しました。

Citrix Virtual Apps and DesktopsでのOracle Cloud Infrastructure (OCI) プロビジョニング済みマシンの登録のサポート

Universalまたはオンプレミス期間ライセンスのお客様は、OCIを介してプロビジョニングされた仮想マシンをCitrix Virtual Apps and Desktopsに登録できるようになりました。この機能強化により、Citrixテクノロジーを利用して、これらのVMへのシームレスで安全なアクセスが可能になります。OCIを介してプロビジョニングされたマシンに対しては、Machine Creation Service (MCS) またはCitrix Provisioning™のサポートは提供されません。

AzureからCitrix Virtual Apps and Desktopsコントロールプレーンを実行

現在、Delivery Controllers、StudioなどのCitrix Virtual Apps and Desktopsコントロールプレーンインフラストラクチャをから実行できます。

Citrix Virtual Apps and Desktops 2209以前のWindowsデスクトップおよびアプリケーションのアイコンをデフォルトアイコンに変更するPowerShellスクリプト

バージョン2209でのCitrix Virtual Apps and Desktopsアーキテクチャの変更後、Windowsデスクトップおよびこのリリースより前に展開されたアプリケーションのデフォルトアイコンは、汎用PCデスクトップアイコンに変更されました。この変更は、デフォルトアイコンを指しているデスクトップおよびアプリケーションにのみ適用されます。アイコンをWindowsアプリケーションのデフォルトアイコンに戻したい場合は、Remote PowerShell SDKを使用して次のスクリプトを実

行してください: `Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0`。

双方向URLリダイレクトを含む強化されたサーバー側ポリシー

現在、サーバー側ポリシーコントロールを使用して双方向URLリダイレクトを管理できます。

詳細については、「双方向コンテンツリダイレクトポリシー設定」を参照してください。

仮想配信エージェント (VDAs) 2311

VDAインストーラーの機能強化

以下の機能強化が、`VDAServerSetup_xxxx.exe`、`VDAWorkstationSetup_xxxx.exe`、および `VDAWorkstationCoreSetup_xxxx.exe` インストーラーに導入されました。

- 新しく追加された引数: `/enable_hdx_tls_dtls` および `/websockettoken`
- 除外するオプション: Citrix App Protection Component、Citrix HyperV Filter Driver、および Citrix Personalization for the App-V - VDAコンポーネント

詳細については、「VDAのインストール用コマンドラインオプション」を参照してください。

適応型リフレッシュレート

新しいスケーラビリティの改善により、HDXは仮想モニターのリフレッシュレートを、設定されたターゲットFPSポリシーに一致させるようになりました。詳細については、「適応型リフレッシュレート」を参照してください。

AMD Radeon PRO V620を搭載したNGads Azure SKUのサポート

AMD Radeon PRO V620を搭載したNGads Azure SKUがサポートされるようになりました。これにより、AzureでGPUアクセラレーション対応のSKUを選択する際の選択肢が増えました。

AOMedia Video 1 (AV1) エンコーディングのサポート

AV1ビデオコーデックは、以下のグラフィックモードでサポートされるようになりました。

- **アクティブに変化する領域の場合**
- **画面全体の場合**

以下のGPUがサポートされています。

- NVIDIA Ada LovelaceベースのGPU

- Intel ARCまたはIntel Data Center GPU Flexシリーズ GPU

新しいAV1ビデオコーデックにより、H.264およびH.265と比較して、優れた画像圧縮、より良い画質、および低い帯域幅の使用量を体験できるようになりました。詳細については、「AV1」を参照してください。

グラフィックのロストトレラントモードのサポート

ロストトレラントモードは、パケット損失が検出されたときにセッションがインタラクティブな状態を維持するように徹底的に再設計されました。

詳細については、「ロストトレラントモード」を参照してください。

Auto-tagsを作成するためのPowerShellコマンド（プレビュー）

この機能を使用すると、PowerShellコマンドを使用してタグを自動的に作成できます。詳細については、「自動タグ」を参照してください。

Rendezvous V2プロトコルがデフォルト

Rendezvousは引き続きデフォルトで無効になっています。Rendezvousが有効になっている場合、デフォルトでV1ではなくV2を使用します。詳細については、「Rendezvousバージョンの構成」を参照してください。

Universal Print ServerでのTLS 1.3のサポート

Universal Print ServerはTLS 1.3をサポートするようになり、これにより、すべてのレガシー暗号スイートの削除、ハンドシェイクプロセスの短縮、TLSプロトコルバージョンネゴシエーションメカニズムの更新などを含む、全体的なセキュリティ体制が強化されます。

詳細については、「Universal Print Serverでのトランスポート層セキュリティ（TLS）」を参照してください。

仮想チャネル許可リストのログ記録の機能強化

仮想チャネル許可リストのログに新しい構成オプションが追加され、ログレベルとスロットリング期間を設定して、生成されるイベントの量を管理できるようになりました。詳細については、「仮想チャネル許可リストのログ記録の機能強化」を参照してください。

仮想IPおよび仮想ループバック

仮想IPと仮想ループバックは、Windows Server 2019およびWindows Server 2022でサポートされるようになりました。詳細については、「仮想IPと仮想ループバック」を参照してください。

サイト上のすべてのデリバリーグループで電源管理されたデスクトップVDAの再利用を有効にするPowerShellコマンド

以前は、ローカルホストキャッシュイベント中に、プールされたデリバリーグループ（MCSまたはCitrix Provisioningによって作成されたもの）内の電源管理されたデスクトップVDAへのアクセスを有効にするには、デリバリーグループごとに`ReuseMachinesWithoutShutdownInOutage` PowerShellコマンドを実行する必要がありました。現在、環境で作成された新しいデリバリーグループの`ReuseMachinesWithoutShutdownInOutage`のデフォルト値を変更できます。詳細については、アプリケーションとデスクトップを参照してください。

Windows Virtual Desktops AgentでのWebカメラリダイレクトに対するMedia Foundation Transforms（MFT）のサポート

Windows Virtual Desktops AgentでWebカメラリダイレクトのオプションとしてMFTを選択できるようになりました。MFTを使用すると、メディアデータ処理が簡素化されます。

詳しくは、「Microsoftドキュメント」を参照してください。

インターネットおよびURLフィルタリング用のプロキシを備えたVDA環境（プレビュー）

インターネット接続とWebフィルタリングにプロキシを使用している場合でも、VDAアップグレードサービスを使用してVDAを更新できるようになりました。ポリシーで構成されたプロキシは、レジストリで構成されたプロキシよりも優先されます。詳しくは、「VDAのインストール」を参照してください。また、プロキシでホワイトリストに登録する必要があるURLのリストも参照してください。

EDTの輻輳制御の強化

EDTの輻輳制御アルゴリズムが更新され、困難なネットワークでの応答性とパフォーマンスが最適化されました。

USB診断ツール

VDA上のコマンドラインツールで、Citrix管理者がクライアントで発生するUSBデバイスリダイレクトの問題を迅速に診断および解決するのに役立ちます。このユーティリティツールは、ICAセッション内でリダイレクトに失敗するクライアントに接続されたUSBデバイスに関連する構成の問題を解決するために必要な重要な情報を収集します。詳細については、USB診断ツールを参照してください。

登録に連続して失敗したVDAマシンはSin Binに移動

VDA登録プロセスを改善するため、登録に2回連続で失敗したマシンは、3分間「Sin Bin」と呼ばれる隔離バケットに入れられます。マシンがSin Binにある場合、Citrix Virtual Apps and Desktopsは登録要求を拒否します。

> **注:**
>
> 以下のエラーの場合、マシンは最初の発生後すぐにシンビンに移動されます。
>
> - DALWorkerFunctionalLevelTooLowForCatalogException
> - DALWorkerFunctionalLevelTooLowForDesktopGroupException
> - DALSingleMultiSessionMismatchException
> - DALWorkerPoweredOffDuringRegistrationException

App-V、MSIX、およびMSIX app attachのパッケージ化されたアプリケーションをシングルセッションおよび共有デスクトップVDAで公開する

シングルセッションおよび共有デスクトップVDAで、App-V、MSIX、MSIX app attachなどのパッケージ化されたアプリケーションにアクセスできるようになりました。この機能強化により、サインイン時にパッケージ化されたアプリケーションをすぐに使用できるようになります。この機能により、パッケージ化されたアプリケーションの起動が高速化され、ローカルにインストールされたアプリケーションにアクセスするのと同様の体験を提供することで、ユーザーエクスペリエンスが大幅に向上します。詳細については、「シングルセッションまたは共有デスクトップVDAでパッケージ化されたアプリケーションを公開する」を参照してください。

ウェブスタジオ

セキュリティ保護されたデフォルト設定の表示

この機能は、デフォルト設定とともにセキュリティ保護されたデフォルト設定を表示します。セキュリティ保護されたデフォルト設定が有効になっている場合、VDAインストール中にポリシー設定の優先順位は次のように影響を受けます。

- カスタマイズされた設定が最も高い優先順位になります

- セキュリティ保護されたデフォルト設定が2番目に高い優先順位になります
- デフォルト設定が最も低い優先順位になります

たとえば、デフォルト設定はセキュリティ保護されたデフォルト設定によって上書きされる場合があります。詳細については、「ポリシー設定」を参照してください。

複数サイト管理のサポート

この機能強化により、サイト管理を一元化するための統合されたWeb Studioコンソールが提供されます。同じWeb Studioから複数のサイトを効率的に管理できるようになり、このタスクに関連する課題が大幅に改善されます。統合されたWeb Studioを使用する利点は次のとおりです。

- **管理の簡素化** - サイト間の切り替えがシームレスに行えます。
- **効率的なヘルプデスク運用** - さまざまなサイトのユーザーをサポートする際に、タイムリーで効果的な対応を保証します。

詳しくは、「複数のサイト管理を有効にする」を参照してください。

デリバリーグループレベルでの負荷分散方法の構成のサポート

この機能により、デリバリーグループレベルで**垂直負荷分散方法**を選択できます。この機能を使用すると、次のマシンが起動される前に、各マシンが最大負荷インデックスに合わせられます。この機能により、各マシンの利用率が最大化され、パブリッククラウドでのコスト削減が実現されます。この機能は、マシンの負荷分散戦略を管理する上で、より高い柔軟性を提供します。

デリバリーグループを構成して、サイトレベルで設定された負荷分散方法を採用するか、垂直または水平負荷分散方法を選択してサイトレベルの設定を上書きすることができます。詳しくは、「負荷分散」を参照してください。

空のコンピューターカタログの作成のサポート

VMをすぐに作成せずに、コンピューターカタログを作成できるようになりました。この機能を使用すると、バックエンドホストが完全に準備されるか、VMプロビジョニングが完了するまでVMの作成を延期できるため、カタログ作成の柔軟性が向上します。詳しくは、「コンピューターカタログの作成」を参照してください。

リソースのネットワーク変更のサポート

Web Studioで、ホスト接続に関連付けられているリソースのネットワークを変更できるようになりました。リソースが使用中の場合、リソースからネットワークの関連付けを解除することはできません。詳しくは、「ネットワークの編集」を参照してください。

PowerShellログ

Web Studioで、日々のUIアクションに対応するPowerShellコマンドを表示できるようになりました。この機能は、学習目的で基盤となるPowerShellコマンドに関する洞察を得るのに役立ちます。PowerShellログを表示するには、**Logging > PowerShell**に移動します。詳しくは、「構成ログ」を参照してください。

MCSプロビジョニングされたコンピューターカタログ

孤立したAzureリソースの検出。 この機能により、Azure展開内の孤立したリソースを検出できるようになり、効率的なリソース管理が可能になります。孤立したリソースが特定された後、さらなるアクションを実行して、生産性の向上とコスト削減を実現できます。詳しくは、「展開内の孤立したAzureリソースを検出する」を参照してください。

AWSおよびGCP VMのコンピュータープロファイルサポート。 MCSを使用してAWSまたはGCP VMをプロビジョニングする際、既存のVMをコンピュータープロファイルとして選択できるようになり、VMが選択したVMから設定を継承できるようになります。

- GCP VMの場合、継承される設定には、ディスク暗号化セットID、マシンサイズ、ストレージタイプ、ゾーンが含まれます。
- AWS VMの場合、継承される設定はステージによって異なります。
  - カタログ作成時：マシン仕様、マシンサイズ、テナンシータイプ、セキュリティグループ、NICの数
  - カタログ編集時：マシン仕様、マシンサイズ、セキュリティグループ。

詳細については、「マシンカタログの作成」を参照してください。

さまざまなAzureマシンプロパティの更新をサポート。 Machine Creation Services™ (MCS) でプロビジョニングされたAzureマシンカタログを管理する際に、以下のプロパティ設定を更新できるようになりました。

- ストレージの種類
- 専用ホストグループ
- アジュール コンピュート ギャラリー設定
- ライトバックキャッシュ（WBC）設定（例：**ディスクキャッシュサイズ、メモリキャッシュサイズ、ストレージコスト削減の有効化**）

これらの設定のいずれかを更新すると、Web Studioは関連する設定を自動的に識別し、自動同期を提供するか、関連する設定を再選択するよう求めるプロンプトメッセージを表示します。この機

能により、関連する設定全体で一貫した変更が保証され、潜在的な構成エラーが防止されます。詳細については、「カタログの編集」を参照してください。

マシンプロファイルを使用したさまざまなAzureマシンプロパティの更新をサポート。 MCSでプロビジョニングされたAzureマシンカタログの場合、マシンプロファイルを介して、より広範囲のプロパティ設定を更新できるようになりました。これには以下が含まれます。

- マシンサイズ
- ライセンスの種類
- 可用性ゾーン
- 専用ホストグループID

マシンプロファイルを更新すると、Web Studioは現在の設定と新しい設定を比較します。違いがある場合は、どちらを適用するか確認を求められます。この設計により、VM設定の更新が透過的かつ効率的に行われます。

VMシャットダウン時にストレージディスクをStandard HDDにダウングレードするオプション。 Azureカタログを作成または更新する際に、**ディスク設定**ページで新しいオプション**ストレージコストの節約を有効にする**が利用可能になりました。このオプションは、VMがシャットダウンしたときに、ストレージディスクとライトバックキャッシュディスクをStandard HDDにダウングレードすることで、ストレージコストを節約します。VMは再起動時に元の設定に戻ります。詳しくは、「Microsoft Azureカタログの作成」を参照してください。

マシンプロファイルの*ホストでの暗号化*プロパティに基づいてマシンサイズをフィルタリングする機能（Azure VM固有）。 Azureマシンカタログの作成または管理中に*ホストでの暗号化*が有効になっているマシンプロファイルを選択すると、この機能をサポートするマシンサイズのみが表示されます。

Hybrid Azure AD参加済みマシンカタログの証明書有効期限警告のサポート。 Web Studioは、Hybrid Azure AD参加済みマシンカタログのユーザー証明書の有効期限について、1か月前に警告を提供するようになりました。この機能強化は、証明書の有効期限切れによるサービス中断のリスクを軽減することを目的としています。詳細と推奨されるアクションを表示するには、**マシンカタログ**ノードに移動し、マシンカタログを選択して、**トラブルシューティング**タブをクリックします。

Citrixサイトデータベースからのみ VM レコードを削除するオプション。 到達不能なハイパーバイザーが原因でカタログとVMの削除が失敗した場合、VMレコードをCitrixサイトデータベースからのみ削除し、VMをホスト上にそのまま残すオプションを選択できるようになりました。詳しくは、「カタログの削除」を参照してください。

電源サイクル中にVMとシステムディスクを保持する単一オプション。 Azureで既存のVMを起動する方が、新しいVMを起動するよりも高速になり、電源サイクル間でVMを保持する方が効率的な選択肢となりました。この変更に対応して、**電源サイクル間でVMを保持する**と**電源サイクル中にシステムディスクを保持する**というオプションを、単一のオプション**電源サイクル中にVMとシステムディスクを保持する**に統合しました。これは、システムディスクを保持することでVMの再起動時間を短縮するためにこのオプションを選択すると、VMも保持されることを意味します。

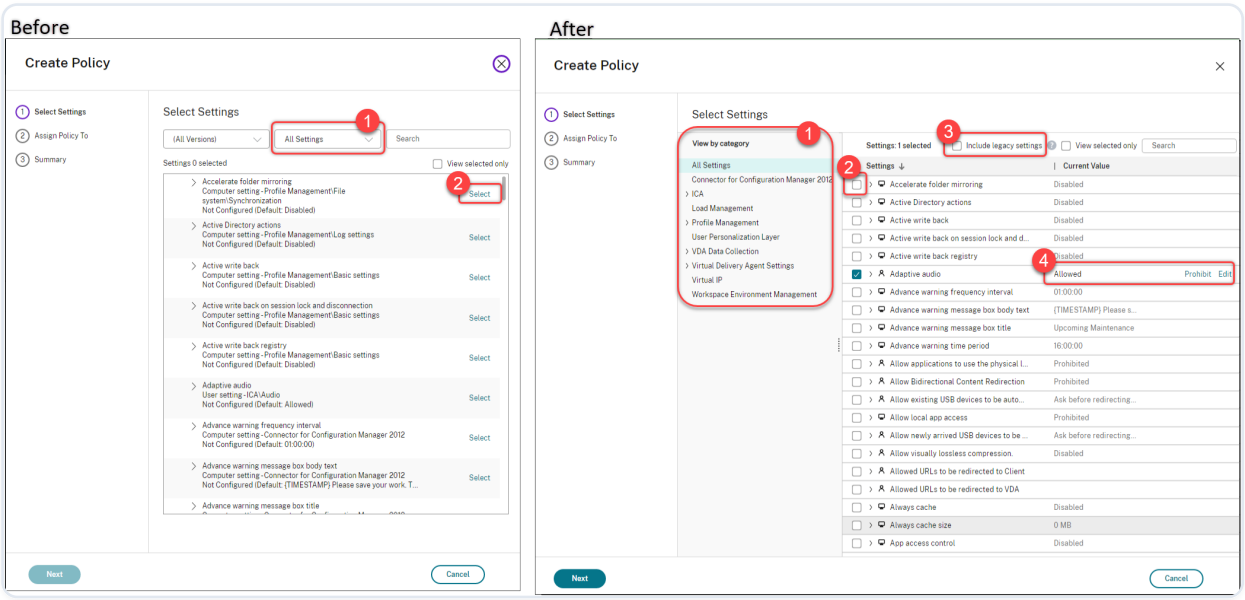
ポリシー関連

新しいポリシー検証。 追加のポリシー検証が追加されました。その結果、無効なポリシー設定が存在する場合、ポリシーを有効にしたり、インプレースアップグレードを実行したりすると、ポリシーデータが失われる可能性があります。Web Studio以外の方法でポリシーを作成または編集する場合は、最新バージョンのSDKとスナップインを使用することをお勧めします。詳しくは、「CTX666304」を参照してください。

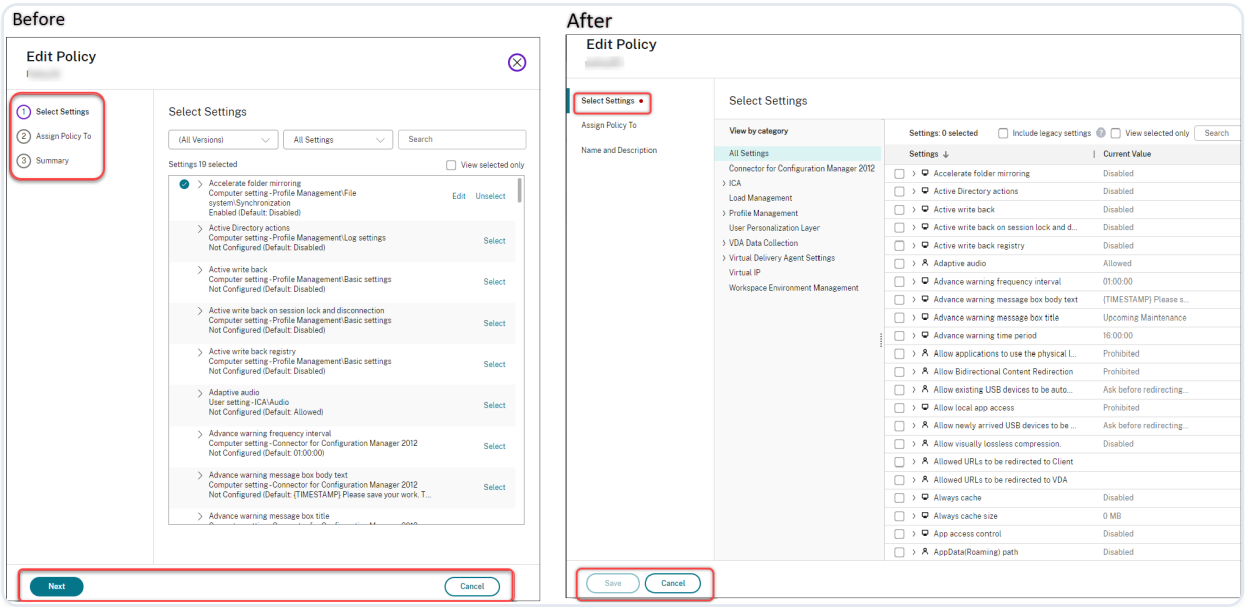
ポリシーセット。 **Web Studio > ポリシー**で、ポリシーセットを使用してポリシーをグループ化し、ロールベースのアクセスを簡素化できるようになりました。その後、ポリシーセットにスコープとデリバリーグループを割り当てることで、承認された管理者のみが関連するユーザーとマシンに適用されるポリシーを管理できるようになります。詳しくは、「ポリシーセット」を参照してください。

ユーザーエクスペリエンスの向上。 ユーザーエクスペリエンスを向上させ、ポリシー管理をより効率的にするために、**ポリシー**ノードに以下の改善を実装しました。

- **ポリシーの作成**および**テンプレートの作成**アクションの新しいUIデザイン:
    - ポリシー設定の展開可能なフォルダービュー。**設定の選択**ページでは、すべての設定がカテゴリ別に展開可能なツリービューで表示され、設定を見つけやすくなっています。
    - 設定を選択するには、**選択**ボタンを使用する代わりに、チェックボックスをクリックするだけです。
    - レガシー設定はデフォルトで非表示になり、最も関連性の高い設定のみが表示されます。レガシー設定が必要な場合は、**レガシー設定を含める**を選択してください。
    - ブール設定の横にアクションボタンが追加され、設定リストでその値を直接変更できるようになりました。



- **ポリシーの編集**アクションの新しいUIデザイン:
  - ナビゲーションメニューが順序なしリストに更新されました。リスト内の各項目には、そのページに**保存**ボタンが含まれるようになりました。この新しいデザインにより、ナビゲーションメニューのすべての項目を移動することなく、項目に加えられた変更を保存できます。これらの改善により、ポリシー管理がより効率的かつ合理化されます。
  - ナビゲーション項目の横に赤い点が表示され、設定エラーを示します。



- ドラッグしてポリシーの優先順位を変更します。優先順位リストで、ポリシーを目的の位置にドラッグすることで、その優先順位を変更できるようになりました。

ポリシーの作成/編集設定ページでのVDAバージョンサポート ポリシーの設定を構成する際、以下のカテゴリで設定を表示するオプションが利用可能になりました。

- **すべての設定。** すべてのVDAバージョンに適用可能なすべての設定を表示します。

- **現在の設定のみ。** 現在のVDAバージョンに固有の設定を表示します。
- **レガシー設定のみ。** 非推奨のVDAバージョンにのみ適用可能な設定を表示します。

強化された検索機能

検索機能を刷新し、フィルターとのインタラクションを含めることで、より良いユーザーエクスペリエンスを提供します。以下の機能が追加されました:

- **保存されたフィルターセットの削除**: **フィルターセットの管理**に移動することなく、検索メニュー内で保存されたフィルターセットを簡単に削除できるようになりました。
- **AND/OR演算子の更新**: **すべてに一致 (AND演算子)** および **いずれかに一致 (OR演算子)** オプションがフィルターパネルで利用可能になり、フィルターアイコンをワンクリックでアクセスできます。
- **簡素化された条件選択**: フィルターパネルで複数の条件を直接指定できるようになりました。
- **よりクリーンなインターフェイス**: **フィルターのピン留め**機能は削除され、UIの煩雑さが軽減され、検索エクスペリエンスがより直感的になりました。
- **クイックフィルター追加**: フィルターを適用した後、プラス記号を使用して、もう1つのフィルターをすばやく追加できるようになりました。

これらの機能強化は、**マシンカタログ**、**デリバリーグループ**、**アプリケーショングループ**、および**アプリケーション**などの他のノードにも拡張されました。

詳細については、「Studioでの検索の使用」を参照してください。

検索ノードのデータキャッシュ

検索ノードのデータキャッシュを導入しました。 この機能強化により、検索のパフォーマンスが向上し、通常のタスクを容易にするユースケースを以下に示します。

- 検索結果が初めて取得された後の迅速な表示。
- 検索ノードから移動して戻った後もページネーション結果を保持します。

Azure Germanyオプションを削除しました

Microsoft Cloud DeutschlandがOctober 29, 2021に閉鎖されたことに伴い、ホスト接続作成ページからAzure Germanyオプションを削除しました。

Web Studioを使用したCitrix Provisioningカタログ作成のサポート

Citrix Provisioningカタログを作成するには、Citrix Virtual Apps and Desktopsセットアップウィザードを使用する必要がありました。この機能により、Web StudioとPowerShellを使用してCitrix Provisioningカタログを作成できるようになりました。

この実装により、以下の利点が得られます。

- MCSとCitrix Provisioningカタログの両方を管理するための単一の統合コンソール。
- ID管理ソリューション、オンデマンドプロビジョニングなど、Citrix Provisioningカタログの新機能があります。

現在、この機能はAzureワークロードでのみ利用可能です。詳細については、Citrix StudioでCitrix Provisioningカタログを作成する を参照してください。

Citrix ディレクター

ユーザーインターフェイスの改善

Citrix Directorのユーザーインターフェイスが、モダンなルックアンドフィールに刷新されました。新しく改善されたユーザーインターフェイスは、より簡単なナビゲーションと優れたデータ表現を提供します。改善されたエクスペリエンスは直感的で、Citrixセッションの監視とトラブルシューティングに必要なデータを容易に理解できるように設計されています。

ライブセッションと録画セッションを再生する

Citrix Directorは、Session Recordingサービスを使用して記録された、記録済みおよびライブのユーザーセッションの再生をサポートするようになりました。再生から、ユーザーが遭遇したセッション関連の問題を迅速に理解できます。この機能により、Directorコンソール内でセッション関連のメトリックとともに記録にすぐにアクセスできます。これにより、記録で発見された問題とパフォーマンスメトリックを関連付けるのに役立ちます。複数のセッション記録サーバーで記録を検索したり、記録を表示するためにサードパーティ製アプリを探したりする必要がなくなります。

この機能には以下が必要です。

- VDAおよびSession Recordingサーバーはバージョン2308以降であること。
- Delivery Controller™およびDirectorはバージョン2311以降であること。

Directorは記録を一元的なリポジトリに保存し、**Session Selector**モーダルに表示します。**Sessions with recordings**リンクは、過去24時間または過去2日間にアクティブだったセッション

の記録を表示します。記録は、Citrix Session Recording再生サーバーを使用して新しいタブで再生されます。

詳細については、セッションの録画 を参照してください。

エンドツーエンドのネットワークホップビュー

エンドツーエンドのネットワークホップビューは、Citrix Directorにおけるトラブルシューティングワークフローを強化するための次のステップです。**User Details** > **Session Performance** > **Session Topology**セクションでは、接続されたHDXセッションのエンドツーエンドのネットワークホップビューを視覚的に表現します。セッション内パスは、セッションパスに関与するコンポーネントとそのメタデータ、コンポーネント間のリンク、およびVDAで公開されているアプリケーションを理解するのに役立ちます。セッショントポロジは、データフローを把握し、パフォーマンスの問題を引き起こしている可能性のある特定のホップを特定するのに役立ちます。

さらに、セッションが接続状態にある場合、ICA LatencyおよびICA RTTの測定値が表示されます。詳細については、エンドツーエンドのネットワークホップビュー を参照してください。

最適な画面解像度

Citrix Directorを表示するための推奨される最適な画面解像度は1440 x 1024に更新されました。Directorのシステム要件の詳細については、「システム要件」を参照してください。

MS Teamsの最適化

Directorは、Microsoft Teamsが最適化されているかどうかを表示します。これは、**ユーザーの詳細**ページ > **セッションの詳細**パネルで確認できます。この情報は、VDAバージョン2311以降で利用可能です。Directorは、Microsoft Teamsが公開アプリケーションとして、または公開デスクトップ内で実行されている場合にのみ、Microsoft Teamsの最適化ステータスを表示します。この機能強化により、チケット解決にかかる時間が短縮され、トラブルシューティング中に管理者が重要なメトリックを把握するのに役立ちます。詳細については、「ユーザーの問題のトラブルシューティング」を参照してください。

プローブの概要の機能強化

プローブ > **概要**ページで、プローブメトリックとプローブ失敗ステージの概要が利用可能になりました。プローブメトリックには、スケジュール済み、失敗、スキップ、成功した実行の数が表示されます。失敗ステージのグラフィカル表示は、ほとんどの失敗が発生したステージを分析するのに役立ちます。この情報は、プローブ結果のトラブルシューティングを迅速に行うのに役立ちます。詳細については、「アプリケーションとデスクトップのプローブ」の記事を参照してください。

「セッションログオン期間」ビューの刷新

ユーザーの詳細ページの新しい**セッションログオン**タブには、ログオン期間フェーズの視覚化が強化されています。新しい表示では、個々のログオンフェーズの重複が示されます。また、個々のフェーズの説明と、GPOおよびプロファイル詳細のサブフェーズ測定へのドリルダウンも提供されます。この視覚化は、ログオン期間に関連する問題を理解し、簡単にトラブルシューティングするのに役立ちます。詳細については、「ユーザーログオンの問題の診断」を参照してください。

動的セッション記録

セッションを再確立することなく、**ユーザーの詳細**画面のセッションレコーディングコントロールを使用して、現在アクティブなセッションを記録できるようになりました。この機能により、ユーザーが直面するセッションエクスペリエンス関連の問題のトラブルシューティングが迅速かつ効果的に行えます。これは、再現が困難な問題をデバッグするのに役立ちます。

動的セッション録画について詳しくは、セッション録画サービスの記事を参照してください。

マシン作成サービス (MCS)

プレビュー機能

休止状態対応VMのサポート（プレビュー）。Azure環境では、Web StudioおよびPowerShellコマンドを使用して、休止状態をサポートするMCSマシンカタログを作成できます。この機能を使用すると、セッションがしばらくアイドル状態になったときにVMを一時停止し、ユーザーが再度サインインしたときにVMの以前の状態に再接続できます。詳細については、「休止状態対応VMの作成（プレビュー）」を参照してください。

Citrix管理のHPE Moonshotプラグインのサポート（プレビュー）。以前は、Hewlett Packard Enterprise (HPE) が保守するHPE管理のMoonshotプラグイン（HPE Moonshot Machine Manager）を使用して、HPE Moonshotシャーシで電源管理アクションを実行していました。このプラグインはレガシーAPIに基づいており、MCSインフラストラクチャプロジェクトを困難にしていました。この機能により、Citrix管理のHPE Moonshotプラグイン（HPE Moonshot）が導入されました。このプラグインを使用すると、HPE Moonshotシャーシへの接続を作成し、カタログを作成し、Web StudioおよびPowerShellコマンドを使用してカタログ内のマシンの電源を管理できます。詳細については、以下を参照してください。

- HPE Moonshot仮想化環境（プレビュー）
- 「HPE Moonshot への接続 (プレビュー)」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections/connection-hpe-moonshot.html)

- 「HPE Moonshot マシンカタログの作成 (プレビュー)」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-hpe-moonshot.html)
- 「HPE Moonshot カタログの管理 (プレビュー)」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage/manage-machine-catalog-hpe-moonshot.html)

AWS 関連

マシンプロファイルソースからVMへのタグのコピーのサポート。この機能を使用すると、マシンプロファイルで指定されたNIC、およびディスク（IDディスク、ライトバックキャッシュディスク、OSディスク）のタグを、MCSマシンカタログで新しく作成されたVMにコピーできます。これらのタグは、任意のマシンプロファイルソース（AWS EC2インスタンスまたはAWS起動テンプレートバージョン）で指定できます。この機能は、永続および非永続マシンカタログとVMに適用されます。

詳しくは、VM上のタグをコピーするを参照してください。

CitrixからVMレコードを削除する際のタグの削除。以前は、`Remove-ProvVM`と`Remove-ProvScheme` PowerShellコマンドは、`ForgetVM`パラメーターを使用して、CitrixデータベースからVMとマシンカタログを削除していました。しかし、これらのコマンドはMCSによって作成されたタグを削除しませんでした。すべてのリソースから完全に削除されなかったVMとマシンカタログを個別に管理する必要がありました。

この機能を使用すると、次のことができます。

- `Remove-ProvVM`と`ForgetVM`パラメーターを使用して、マシンカタログから単一のVMまたはVMのリストからVMとMCS作成タグを削除します。
- `Remove-ProvScheme`と`ForgetVM`パラメーターを使用して、Citrixデータベースからマシンカタログを削除し、マシンカタログからリソースを削除します。

この実装は、以下の点で役立ちます。

- リークしたリソースの特定
- 不要なリソースを維持するための追加コストの削減

この機能は、永続VMにのみ適用されます。詳しくは、タグの削除を参照してください。

マシンプロファイルのサポート。AWSでMachine Creation Services (MCS) を使用してマシンをプロビジョニングするカタログを作成する際、EC2インスタンス（VM）または起動テンプレートバージョンからハードウェアプロパティをキャプチャし、それらをプロビジョニングされたマシンに適用するために、マシンプロファイルを使用できるようになりました。キャプチャされるプロパティには、例えば、EBSボリュームプロパティ、インスタンスタイプ、EBS最適化、およびそ

の他のサポートされているAWS構成が含まれます。カタログを編集する際、プロビジョニングされたマシンのマシンプロファイルは、別のVMまたは起動テンプレートを提供することで変更できます。詳しくは、マシンプロファイルを使用してカタログを作成するを参照してください。

インスタンスのフィルタリングのサポート。以前は、AWS EC2インスタンスをMCSマシンカタログを作成するためのマシンプロファイル入力として使用すると、無効なマシンプロファイル入力（たとえば、マスターイメージと互換性のない特定のプロパティ値を持つマシンプロファイル入力）が原因で、カタログが適切に作成されなかったり、正しく機能しなかったりすることがありました。この機能を使用すると、有効なマシンプロファイルVMとして使用できるAWS EC2インスタンスを一覧表示できます。これを行うには、`Get-HypInventoryItem`コマンドを使用します。詳細については、「VMインスタンスのフィルタリング」を参照してください。

インスタンスの休止状態のサポート。AWSインスタンスを起動し、必要に応じて使用し、その後休止状態にできるようになりました。休止プロセスでは、インスタンスのインメモリ状態と、そのプライベートIPアドレスおよびエラスティックIPアドレスが保存され、中断したところから正確に再開できます。休止状態をサポートするVMの作成の詳細については、「インスタンスの休止状態」を参照してください。

Azure関連

マシンプロファイルからの診断設定のキャプチャのサポート。Azure環境では、MCSは、MCSマシンカタログの作成または更新時、あるいは既存のVMの更新時に、マシンプロファイルからVMおよびNICの診断設定をキャプチャすることをサポートするようになりました。したがって、この実装により、診断データは、詳細な分析と視覚化のために、Log AnalyticsワークスペースやEvent Hubsなどの指定されたAzure宛先エンドポイントにシームレスに送信できます。詳細については、「マシンプロファイルからVMおよびNICの診断設定をキャプチャする」を参照してください。

MCSでのスポットVMの使用に対するAzureのサポート。AzureスポットVMを使用すると、Azureの未使用のコンピューティング容量を大幅なコスト削減で活用できます。ただし、その強制排除ポリシーのため、AzureスポットVMは一部の重要でないアプリケーションやデスクトップにのみ適しています。

この機能を使用すると、マシンプロファイル（VMまたはテンプレート仕様）を使用して、AzureスポットVMのMCSマシンカタログを作成できます。既存のカタログを更新して、新しく作成されたVMとしてAzureスポットVMを使用したり、標準のAzure VMに切り替えたりできます。既存のVMをAzureスポットVMに更新することもできます。詳細については、「AzureスポットVMを使用してカタログを作成する」を参照してください。

マシンプロファイルに関連付けられたホストでの暗号化情報を取得する。Azure環境では、この機能により、PowerShellコマンドを使用して、マシンプロファイル入力（VMまたはテンプレート仕

様）に対してホストでの暗号化が有効になっているかどうかを知ることができるようになりました。詳細については、「マシンプロファイルからホストでの暗号化情報を取得する」を参照してください。

マスターイメージのディスク暗号化セットID（DES ID）を使用して、カタログVMのすべてのディスクを暗号化する。Azure環境では、以前はMCSマシンカタログのディスク暗号化セットID（DES ID）はマシンプロファイルまたはカスタムプロパティから派生していました。この機能により、マシンカタログはマスターイメージからDES IDを派生させて、カタログ内のVMのすべてのディスクを暗号化することもできます。

顧客管理の暗号化キーが有効なPVSカタログの作成をサポート。 Azure環境では、Web StudioおよびPowerShellコマンドを使用して、顧客管理の暗号化キー (CMEK) が有効なPVSカタログを作成できるようになりました。詳細については、「顧客管理の暗号化キーが有効なカタログを作成する」を参照してください。

MCSはPVSカタログ作成用のリソースグループを作成する。Web Studioを使用してPVSカタログを作成する際に、既存のリソースグループを選択しない場合、MCSはカタログ作成用のリソースグループを自動的に作成します。PVSカタログの作成の詳細については、「Citrix Provisioningカタログを作成する」を参照してください。

バックアップVMサイズの構成のサポート。パブリッククラウドでは、特定のVMサイズの容量が不足することがあります。また、AzureスポットVMを使用している場合、Azureの容量要件に基づいてVMはいつでも強制排除されます。Azureの容量不足やスポットVMの電源投入失敗といった場合、MCSはバックアップVMサイズにフォールバックするようになりました。カスタムプロパティ `BackupVmConfiguration` を使用して、バックアップVMサイズのリストを提供できます。MCSは、リストで指定された順序でバックアップVMサイズにフォールバックしようとします。提供されたすべてのバックアップVMサイズにフォールバックできない場合、エラーメッセージが表示されます。

この機能は、マシンプロファイルを使用するカタログでのみサポートされており、永続的および非永続的なMCSマシンカタログの両方に適用できます。この機能は現在、Azure環境でのみサポートされています。

詳細については、「バックアップVMサイズを構成する」を参照してください。

すべてのリソースにタグをコピーする機能。 この機能により、Azure環境では、マシンプロファイルで指定されたタグを、新しいVMまたはマシンカタログ内の既存のVMの複数のNICやディスク (OSディスク、IDディスク、ライトバックキャッシュディスクなど) のすべてのリソースにコピーできるようになりました。

マシンプロファイルのソースは、VM または ARM テンプレート仕様にすることができます。詳細については、「すべてのリソースにタグをコピーする」を参照してください。

Azure Monitor Agent を使用したカタログ VM のプロビジョニングのサポート。Azure Monitor Agent (AMA) は、監視データを収集し、Azure Monitor に配信します。この機能により、MCS マシンカタログ VM (永続的および非永続的) を、AMA を拡張機能としてインストールしてプロビジョニングできます。この実装により、監視データ内の VM を一意に識別することで監視が可能になります。AMA の詳細については、「Azure Monitor Agent の概要」を参照してください。

現在、MCS はこの機能に対してマシンプロファイルワークフローのみをサポートしています。

AMA が有効なマシンカタログ VM のプロビジョニングの詳細については、「Azure Monitor Agent がインストールされたカタログ VM のプロビジョニング」を参照してください。

マシンカタログの管理

マシンカタログの異なるバージョンの管理に対する MCS のサポート。この機能を使用すると、PowerShell コマンドを使用してマシンカタログの構成バージョンを管理できます。`Set-ProvScheme` を使用した構成の変更ごとに、新しい構成バージョンが作成されます。次のことができます。

- バージョンの一覧を表示する
- 以前のバージョンを使用してマシンカタログを更新する
- VM で使用されていないバージョンを手動で削除する
- マシンカタログが保持する最大バージョン数を変更する

詳細については、「マシンカタログのバージョンを管理する」を参照してください。

AWS 環境で、マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換するサポート。AWS 環境では、VM または起動テンプレートをマシンプロファイルの入力として使用して、マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換できるようになりました。カタログに追加された新しい VM は、マシンプロファイルからプロパティ値を取得します。詳細については、「マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換する」を参照してください。

アクティブなコンピューターアカウントの ID 情報の修復。この機能を使用すると、ID 関連の問題があるアクティブなコンピューターアカウントの ID 情報をリセットできます。マシンパスワードと信頼キーのみをリセットするか、ID ディスクのすべての構成をリセットするかを選択できます。この実装は、永続的および非永続的な両方のマシンカタログに適用できます。現在、この機能

は Azure および VMware 仮想化環境でのみサポートされています。詳細については、「アクティブなコンピューターアカウントの ID 情報を修復する」を参照してください。

AWS で MCS によって作成されたマシンカタログ内の永続 VM の OS ディスクをリセットする機能。AWS 環境では、PowerShell コマンド `Reset-ProvVMDisk` を使用して、MCS によって作成されたマシンカタログ内の永続 VM の OS ディスクをリセットできるようになりました。この機能は、OS ディスクのリセットプロセスを自動化します。たとえば、MCS を使用して作成された永続的な開発デスクトップカタログの VM を初期状態にリセットするのに役立ちます。

PowerShell コマンドを使用して OS ディスクをリセットする方法の詳細については、「OS ディスクのリセット」を参照してください。

孤立したリソースのリストを取得する

MCSによって作成されたものの、MCSによって追跡されなくなった孤立したリソースのリストを取得できます。これは現在、Azure環境に適用されます。リストを取得するには、PowerShellコマンドを使用できます。接続を使用してフィルタリングできます。詳細については、「孤立したリソースのリストを取得する」を参照してください。

MCSによるメモリおよびディスクキャッシュサイズの変更機能

この機能により、新しいマシンカタログを作成することなく、PowerShellコマンドを使用してライトバックキャッシュ（MCSIOが有効な場合）のメモリおよびディスクキャッシュサイズを変更できるようになりました。この実装は、ビジネスニーズに適した最適化されたキャッシュ構成を持つことに役立ちます。この機能は以下に適用されます。

- GCPおよびMicrosoft Azure環境、および
- MCSIOが有効な非永続カタログ

詳細については、「既存のマシンカタログのキャッシュ構成を変更する」を参照してください。

VMwareにおけるVMのストレージ移行のサポート

この機能により、VMware環境で、既存のVMのディスクストレージを古いストレージから新しいストレージに移動できます。移行中、MCSは電源管理、OSディスクのリセットなどのVM機能を保持します。新しいディスクストレージサービスを使用して、新しいVMをマシンカタログに追加することもできます。これを行うには、PowerShellコマンド`Move-ProvVMDisk`を使用します。詳細については、「VMのストレージ移行」を参照してください。

マシンプロファイルに対するSCVMMのサポート

この機能により、System Center Virtual Machine Manager (SCVMM) 環境でマシンプロファイルを使用してMCSマシンカタログを作成および更新できるようになりました。ネストされた仮想化とvTPMを有効にすることもできます。詳細については、「マシンプロファイルを使用してカタログを作成する」を参照してください。

ハイブリッドAzure AD参加済みマシンIDのユーザー証明書を修復する

この機能により、ハイブリッドAzure AD参加済みマシンIDのユーザー証明書が破損または期限切れになった場合、PowerShellコマンドを使用して修復できます。詳細については、「ハイブリッドAzure Active Directory参加済みカタログを作成する」を参照してください。

ハイブリッドAzure AD参加済みマシンカタログのユーザー証明書の有効期限に関する情報を取得するには、`Get-ProvScheme`コマンドを実行します。

SCCMの重複GUID問題の解決策

MCSを使用して複数のVMを作成した後、System Center Configuration Manager (SCCM) は、GUIDが重複しているため、コンソールに1つのVMしか表示しませんでした。この問題は、イメージ準備にステップを追加することで解決されました。このステップは、マスターイメージ内の既存の証明書とGUID情報を削除します。このステップはデフォルトで有効になっています。

プロファイル管理

新機能については、独自のドキュメントにある新機能の記事を参照してください。

リナックス VDA

新機能については、独自のドキュメントにある新機能の記事を参照してください。

セッション録画

新機能については、独自のドキュメントにある新機能の記事を参照してください。

ワークスペース環境管理™

新機能については、独自のドキュメントにある新機能の記事を参照してください。

シトリックス プロビジョニング

新機能については、独自のドキュメントにある新機能の記事を参照してください。

フェデレーション認証サービス

新機能については、独自のドキュメントにある新機能の記事を参照してください。

シトリックス バーチャル アプリケーションズ アンド デスクトップ™ 7 2311

リリースについて

このCitrix Virtual Apps and Desktopsリリースには、Windows Virtual Delivery Agent (VDA) の新しいバージョンと、いくつかのコアコンポーネントの新しいバージョンが含まれています。次のことができます。

- **サイトのインストールまたはアップグレード**: このリリースの ISO を使用して、コアコンポーネントと VDA をインストールまたはアップグレードします。最新バージョンにインストールまたはアップグレードすることで、最新の機能を使用できます。
- **既存のサイトでのVDAのインストールまたはアップグレード**: 展開が既にあり、コアコンポーネントをアップグレードする準備ができていない場合でも、新しいVDAをインストール（またはアップグレード）することで、最新のHDX™機能のいくつかを引き続き使用できます。VDAのみをアップグレードすることは、非本番環境で機能強化をテストしたい場合に役立ちます。

  VDAをこのバージョン（バージョン7.9以降）にアップグレードした後、マシンカタログの機能レベルを更新する必要はありません。7.9（またはそれ以降）の値はデフォルトの機能レベルのままであり、このリリースで有効です。詳しくは、「VDAのバージョンと機能レベル」を参照してください。

インストールとアップグレードの手順：

- 新しいサイトを構築する場合は、「インストールと構成」の順序に従ってください。
- サイトをアップグレードする場合は、「展開のアップグレード」を参照してください。

シトリックス バーチャル アプリケーションズ アンド デスクトップ 7 2311

HDX Direct (プレビュー)

新しい機能強化により、HDX Directは、直接通信が可能な場合、内部および外部のクライアントデバイスがセッションホストと安全な直接接続を確立できるようになりました。詳細については、「HDX Direct」を参照してください。

構成ログへのメタデータ関連付けのサポート

この機能強化により、高レベルの操作で`name-value`ペアを関連付けることで、構成ログにメタデータを添付できるようになりました。詳しくは、「構成ログへのメタデータ関連付け」を参照してください。

オンプレミス向けCitrix Secure Private Access™

オンプレミス向けCitrix Secure Private Accessは、Citrix Virtual Apps and Desktops 2311リリースの一部として一般提供されるようになりました。オンプレミス向けSecure Private Accessソリューションには、Secure Private Accessサービスと同様のルックアンドフィールを持つフルサービスの管理コンソールUIが含まれています。詳細については、「オンプレミス向けCitrix Secure Private Access – 一般提供」を参照してください。

Citrix Hypervisor™がXenServer®にブランド変更

最新のリブランディング戦略に沿って、**Citrix Hypervisor** のすべてのインスタンスを **XenServer®** に更新しました。

Citrix Virtual Apps and DesktopsでのOracle Cloud Infrastructure (OCI) プロビジョニング済みマシンの登録のサポート

Universalまたはオンプレミス期間ライセンスのお客様は、OCIを介してプロビジョニングされた仮想マシンをCitrix Virtual Apps and Desktopsに登録できるようになりました。この機能強化により、Citrixテクノロジーを利用して、これらのVMへのシームレスで安全なアクセスが可能になります。OCIを介してプロビジョニングされたマシンに対しては、Machine Creation Service (MCS) またはCitrix Provisioning™のサポートは提供されません。

AzureからCitrix Virtual Apps and Desktopsコントロールプレーンを実行

現在、Delivery Controllers、StudioなどのCitrix Virtual Apps and Desktopsコントロールプレーンインフラストラクチャをから実行できます。

Citrix Virtual Apps and Desktops 2209以前のWindowsデスクトップおよびアプリケーションのアイコンをデフォルトアイコンに変更するPowerShellスクリプト

バージョン2209でのCitrix Virtual Apps and Desktopsアーキテクチャの変更後、Windowsデスクトップおよびこのリリースより前に展開されたアプリケーションのデフォルトアイコンは、汎用PCデスクトップアイコンに変更されました。この変更は、デフォルトアイコンを指しているデスクトップおよびアプリケーションにのみ適用されます。アイコンをWindowsアプリケーションのデフォルトアイコンに戻したい場合は、Remote PowerShell SDKを使用して次のスクリプトを実

行してください: `Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0`。

双方向URLリダイレクトを含む強化されたサーバー側ポリシー

現在、サーバー側ポリシーコントロールを使用して双方向URLリダイレクトを管理できます。

詳細については、「双方向コンテンツリダイレクトポリシー設定」を参照してください。

仮想配信エージェント (VDAs) 2311

VDAインストーラーの機能強化

以下の機能強化が、`VDAServerSetup_xxxx.exe`、`VDAWorkstationSetup_xxxx.exe`、および `VDAWorkstationCoreSetup_xxxx.exe` インストーラーに導入されました。

- 新しく追加された引数: `/enable_hdx_tls_dtls` および `/websockettoken`
- 除外するオプション: Citrix App Protection Component、Citrix HyperV Filter Driver、および Citrix Personalization for the App-V - VDAコンポーネント

詳細については、「VDAのインストール用コマンドラインオプション」を参照してください。

適応型リフレッシュレート

新しいスケーラビリティの改善により、HDXは仮想モニターのリフレッシュレートを、設定されたターゲットFPSポリシーに一致させるようになりました。詳細については、「適応型リフレッシュレート」を参照してください。

AMD Radeon PRO V620を搭載したNGads Azure SKUのサポート

AMD Radeon PRO V620を搭載したNGads Azure SKUがサポートされるようになりました。これにより、AzureでGPUアクセラレーション対応のSKUを選択する際の選択肢が増えました。

AOMedia Video 1 (AV1) エンコーディングのサポート

AV1ビデオコーデックは、以下のグラフィックモードでサポートされるようになりました。

- **アクティブに変化する領域の場合**
- **画面全体の場合**

以下のGPUがサポートされています。

- NVIDIA Ada LovelaceベースのGPU

- Intel ARCまたはIntel Data Center GPU Flexシリーズ GPU

新しいAV1ビデオコーデックにより、H.264およびH.265と比較して、優れた画像圧縮、より良い画質、および低い帯域幅の使用量を体験できるようになりました。詳細については、「AV1」を参照してください。

グラフィックのロストトレラントモードのサポート

ロストトレラントモードは、パケット損失が検出されたときにセッションがインタラクティブな状態を維持するように徹底的に再設計されました。

詳細については、「ロストトレラントモード」を参照してください。

Auto-tagsを作成するためのPowerShellコマンド（プレビュー）

この機能を使用すると、PowerShellコマンドを使用してタグを自動的に作成できます。詳細については、「自動タグ」を参照してください。

Rendezvous V2プロトコルがデフォルト

Rendezvousは引き続きデフォルトで無効になっています。Rendezvousが有効になっている場合、デフォルトでV1ではなくV2を使用します。詳細については、「Rendezvousバージョンの構成」を参照してください。

Universal Print ServerでのTLS 1.3のサポート

Universal Print ServerはTLS 1.3をサポートするようになり、これにより、すべてのレガシー暗号スイートの削除、ハンドシェイクプロセスの短縮、TLSプロトコルバージョンネゴシエーションメカニズムの更新などを含む、全体的なセキュリティ体制が強化されます。

詳細については、「Universal Print Serverでのトランスポート層セキュリティ（TLS）」を参照してください。

仮想チャネル許可リストのログ記録の機能強化

仮想チャネル許可リストのログに新しい構成オプションが追加され、ログレベルとスロットリング期間を設定して、生成されるイベントの量を管理できるようになりました。詳細については、「仮想チャネル許可リストのログ記録の機能強化」を参照してください。

仮想IPおよび仮想ループバック

仮想IPと仮想ループバックは、Windows Server 2019およびWindows Server 2022でサポートされるようになりました。詳細については、「仮想IPと仮想ループバック」を参照してください。

サイト上のすべてのデリバリーグループで電源管理されたデスクトップVDAの再利用を有効にするPowerShellコマンド

以前は、ローカルホストキャッシュイベント中に、プールされたデリバリーグループ（MCSまたはCitrix Provisioningによって作成されたもの）内の電源管理されたデスクトップVDAへのアクセスを有効にするには、デリバリーグループごとに`ReuseMachinesWithoutShutdownInOutage` PowerShellコマンドを実行する必要がありました。現在、環境で作成された新しいデリバリーグループの`ReuseMachinesWithoutShutdownInOutage`のデフォルト値を変更できます。詳細については、アプリケーションとデスクトップを参照してください。

Windows Virtual Desktops AgentでのWebカメラリダイレクトに対するMedia Foundation Transforms（MFT）のサポート

Windows Virtual Desktops AgentでWebカメラリダイレクトのオプションとしてMFTを選択できるようになりました。MFTを使用すると、メディアデータ処理が簡素化されます。

詳しくは、「Microsoftドキュメント」を参照してください。

インターネットおよびURLフィルタリング用のプロキシを備えたVDA環境（プレビュー）

インターネット接続とWebフィルタリングにプロキシを使用している場合でも、VDAアップグレードサービスを使用してVDAを更新できるようになりました。ポリシーで構成されたプロキシは、レジストリで構成されたプロキシよりも優先されます。詳しくは、「VDAのインストール」を参照してください。また、プロキシでホワイトリストに登録する必要があるURLのリストも参照してください。

EDTの輻輳制御の強化

EDTの輻輳制御アルゴリズムが更新され、困難なネットワークでの応答性とパフォーマンスが最適化されました。

USB診断ツール

VDA上のコマンドラインツールで、Citrix管理者がクライアントで発生するUSBデバイスリダイレクトの問題を迅速に診断および解決するのに役立ちます。このユーティリティツールは、ICAセッション内でリダイレクトに失敗するクライアントに接続されたUSBデバイスに関連する構成の問題を解決するために必要な重要な情報を収集します。詳細については、USB診断ツールを参照してください。

登録に連続して失敗したVDAマシンはSin Binに移動

VDA登録プロセスを改善するため、登録に2回連続で失敗したマシンは、3分間「Sin Bin」と呼ばれる隔離バケットに入れられます。マシンがSin Binにある場合、Citrix Virtual Apps and Desktopsは登録要求を拒否します。

> **注:**
>
> 以下のエラーの場合、マシンは最初の発生後すぐにシンビンに移動されます。
>
> - DALWorkerFunctionalLevelTooLowForCatalogException
> - DALWorkerFunctionalLevelTooLowForDesktopGroupException
> - DALSingleMultiSessionMismatchException
> - DALWorkerPoweredOffDuringRegistrationException

App-V、MSIX、およびMSIX app attachのパッケージ化されたアプリケーションをシングルセッションおよび共有デスクトップVDAで公開する

シングルセッションおよび共有デスクトップVDAで、App-V、MSIX、MSIX app attachなどのパッケージ化されたアプリケーションにアクセスできるようになりました。この機能強化により、サインイン時にパッケージ化されたアプリケーションをすぐに使用できるようになります。この機能により、パッケージ化されたアプリケーションの起動が高速化され、ローカルにインストールされたアプリケーションにアクセスするのと同様の体験を提供することで、ユーザーエクスペリエンスが大幅に向上します。詳細については、「シングルセッションまたは共有デスクトップVDAでパッケージ化されたアプリケーションを公開する」を参照してください。

ウェブスタジオ

セキュリティ保護されたデフォルト設定の表示

この機能は、デフォルト設定とともにセキュリティ保護されたデフォルト設定を表示します。セキュリティ保護されたデフォルト設定が有効になっている場合、VDAインストール中にポリシー設定の優先順位は次のように影響を受けます。

- カスタマイズされた設定が最も高い優先順位になります

- セキュリティ保護されたデフォルト設定が2番目に高い優先順位になります
- デフォルト設定が最も低い優先順位になります

たとえば、デフォルト設定はセキュリティ保護されたデフォルト設定によって上書きされる場合があります。詳細については、「ポリシー設定」を参照してください。

複数サイト管理のサポート

この機能強化により、サイト管理を一元化するための統合されたWeb Studioコンソールが提供されます。同じWeb Studioから複数のサイトを効率的に管理できるようになり、このタスクに関連する課題が大幅に改善されます。統合されたWeb Studioを使用する利点は次のとおりです。

- **管理の簡素化** - サイト間の切り替えがシームレスに行えます。
- **効率的なヘルプデスク運用** - さまざまなサイトのユーザーをサポートする際に、タイムリーで効果的な対応を保証します。

詳しくは、「複数のサイト管理を有効にする」を参照してください。

デリバリーグループレベルでの負荷分散方法の構成のサポート

この機能により、デリバリーグループレベルで**垂直負荷分散方法**を選択できます。この機能を使用すると、次のマシンが起動される前に、各マシンが最大負荷インデックスに合わせられます。この機能により、各マシンの利用率が最大化され、パブリッククラウドでのコスト削減が実現されます。この機能は、マシンの負荷分散戦略を管理する上で、より高い柔軟性を提供します。

デリバリーグループを構成して、サイトレベルで設定された負荷分散方法を採用するか、垂直または水平負荷分散方法を選択してサイトレベルの設定を上書きすることができます。詳しくは、「負荷分散」を参照してください。

空のコンピューターカタログの作成のサポート

VMをすぐに作成せずに、コンピューターカタログを作成できるようになりました。この機能を使用すると、バックエンドホストが完全に準備されるか、VMプロビジョニングが完了するまでVMの作成を延期できるため、カタログ作成の柔軟性が向上します。詳しくは、「コンピューターカタログの作成」を参照してください。

リソースのネットワーク変更のサポート

Web Studioで、ホスト接続に関連付けられているリソースのネットワークを変更できるようになりました。リソースが使用中の場合、リソースからネットワークの関連付けを解除することはできません。詳しくは、「ネットワークの編集」を参照してください。

PowerShellログ

Web Studioで、日々のUIアクションに対応するPowerShellコマンドを表示できるようになりました。この機能は、学習目的で基盤となるPowerShellコマンドに関する洞察を得るのに役立ちます。PowerShellログを表示するには、**Logging > PowerShell**に移動します。詳しくは、「構成ログ」を参照してください。

MCSプロビジョニングされたコンピューターカタログ

孤立したAzureリソースの検出。 この機能により、Azure展開内の孤立したリソースを検出できるようになり、効率的なリソース管理が可能になります。孤立したリソースが特定された後、さらなるアクションを実行して、生産性の向上とコスト削減を実現できます。詳しくは、「展開内の孤立したAzureリソースを検出する」を参照してください。

AWSおよびGCP VMのコンピュータープロファイルサポート。 MCSを使用してAWSまたはGCP VMをプロビジョニングする際、既存のVMをコンピュータープロファイルとして選択できるようになり、VMが選択したVMから設定を継承できるようになります。

- GCP VMの場合、継承される設定には、ディスク暗号化セットID、マシンサイズ、ストレージタイプ、ゾーンが含まれます。
- AWS VMの場合、継承される設定はステージによって異なります。
  - カタログ作成時：マシン仕様、マシンサイズ、テナンシータイプ、セキュリティグループ、NICの数
  - カタログ編集時：マシン仕様、マシンサイズ、セキュリティグループ。

詳細については、「マシンカタログの作成」を参照してください。

さまざまなAzureマシンプロパティの更新をサポート。 Machine Creation Services™ (MCS) でプロビジョニングされたAzureマシンカタログを管理する際に、以下のプロパティ設定を更新できるようになりました。

- ストレージの種類
- 専用ホストグループ
- アジュール コンピュート ギャラリー設定
- ライトバックキャッシュ（WBC）設定（例：**ディスクキャッシュサイズ、メモリキャッシュサイズ、ストレージコスト削減の有効化**）

これらの設定のいずれかを更新すると、Web Studioは関連する設定を自動的に識別し、自動同期を提供するか、関連する設定を再選択するよう求めるプロンプトメッセージを表示します。この機

能により、関連する設定全体で一貫した変更が保証され、潜在的な構成エラーが防止されます。詳細については、「カタログの編集」を参照してください。

マシンプロファイルを使用したさまざまなAzureマシンプロパティの更新をサポート。 MCSでプロビジョニングされたAzureマシンカタログの場合、マシンプロファイルを介して、より広範囲のプロパティ設定を更新できるようになりました。これには以下が含まれます。

- マシンサイズ
- ライセンスの種類
- 可用性ゾーン
- 専用ホストグループID

マシンプロファイルを更新すると、Web Studioは現在の設定と新しい設定を比較します。違いがある場合は、どちらを適用するか確認を求められます。この設計により、VM設定の更新が透過的かつ効率的に行われます。

VMシャットダウン時にストレージディスクをStandard HDDにダウングレードするオプション。 Azureカタログを作成または更新する際に、**ディスク設定**ページで新しいオプション**ストレージコストの節約を有効にする**が利用可能になりました。このオプションは、VMがシャットダウンしたときに、ストレージディスクとライトバックキャッシュディスクをStandard HDDにダウングレードすることで、ストレージコストを節約します。VMは再起動時に元の設定に戻ります。詳しくは、「Microsoft Azureカタログの作成」を参照してください。

マシンプロファイルの*ホストでの暗号化*プロパティに基づいてマシンサイズをフィルタリングする機能（Azure VM固有）。 Azureマシンカタログの作成または管理中に*ホストでの暗号化*が有効になっているマシンプロファイルを選択すると、この機能をサポートするマシンサイズのみが表示されます。

Hybrid Azure AD参加済みマシンカタログの証明書有効期限警告のサポート。 Web Studioは、Hybrid Azure AD参加済みマシンカタログのユーザー証明書の有効期限について、1か月前に警告を提供するようになりました。この機能強化は、証明書の有効期限切れによるサービス中断のリスクを軽減することを目的としています。詳細と推奨されるアクションを表示するには、**マシンカタログ**ノードに移動し、マシンカタログを選択して、**トラブルシューティング**タブをクリックします。

Citrixサイトデータベースからのみ VM レコードを削除するオプション。 到達不能なハイパーバイザーが原因でカタログとVMの削除が失敗した場合、VMレコードをCitrixサイトデータベースからのみ削除し、VMをホスト上にそのまま残すオプションを選択できるようになりました。詳しくは、「カタログの削除」を参照してください。

電源サイクル中にVMとシステムディスクを保持する単一オプション。 Azureで既存のVMを起動する方が、新しいVMを起動するよりも高速になり、電源サイクル間でVMを保持する方が効率的な選択肢となりました。この変更に対応して、**電源サイクル間でVMを保持する**と**電源サイクル中にシステムディスクを保持する**というオプションを、単一のオプション**電源サイクル中にVMとシステムディスクを保持する**に統合しました。これは、システムディスクを保持することでVMの再起動時間を短縮するためにこのオプションを選択すると、VMも保持されることを意味します。

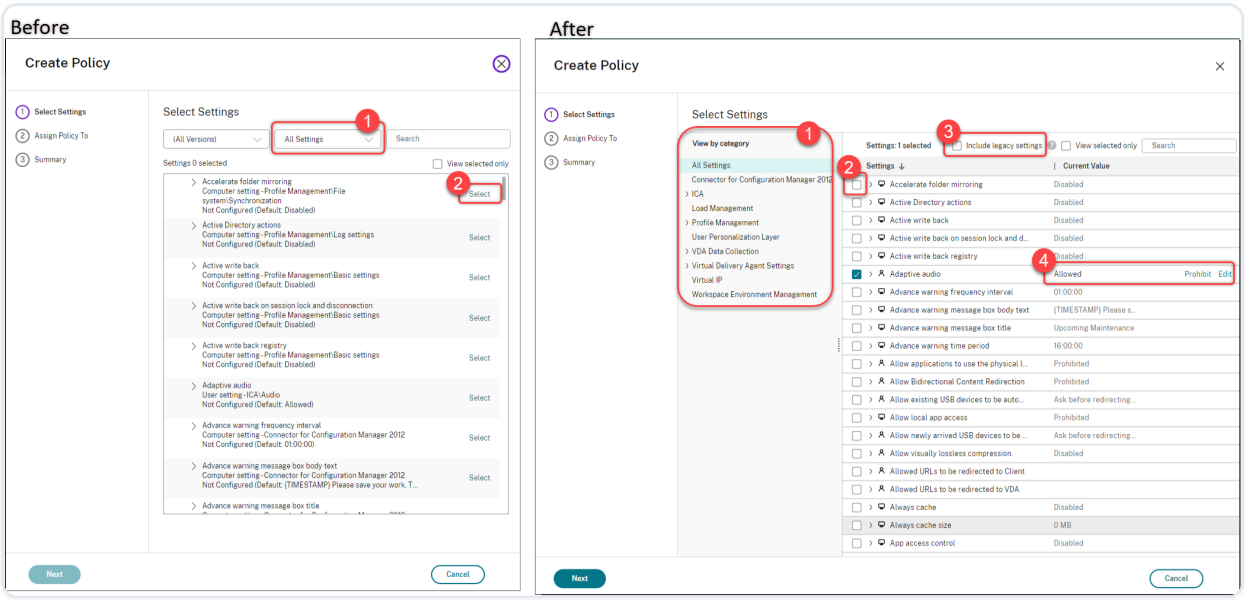
ポリシー関連

新しいポリシー検証。 追加のポリシー検証が追加されました。その結果、無効なポリシー設定が存在する場合、ポリシーを有効にしたり、インプレースアップグレードを実行したりすると、ポリシーデータが失われる可能性があります。Web Studio以外の方法でポリシーを作成または編集する場合は、最新バージョンのSDKとスナップインを使用することをお勧めします。詳しくは、「CTX666304」を参照してください。

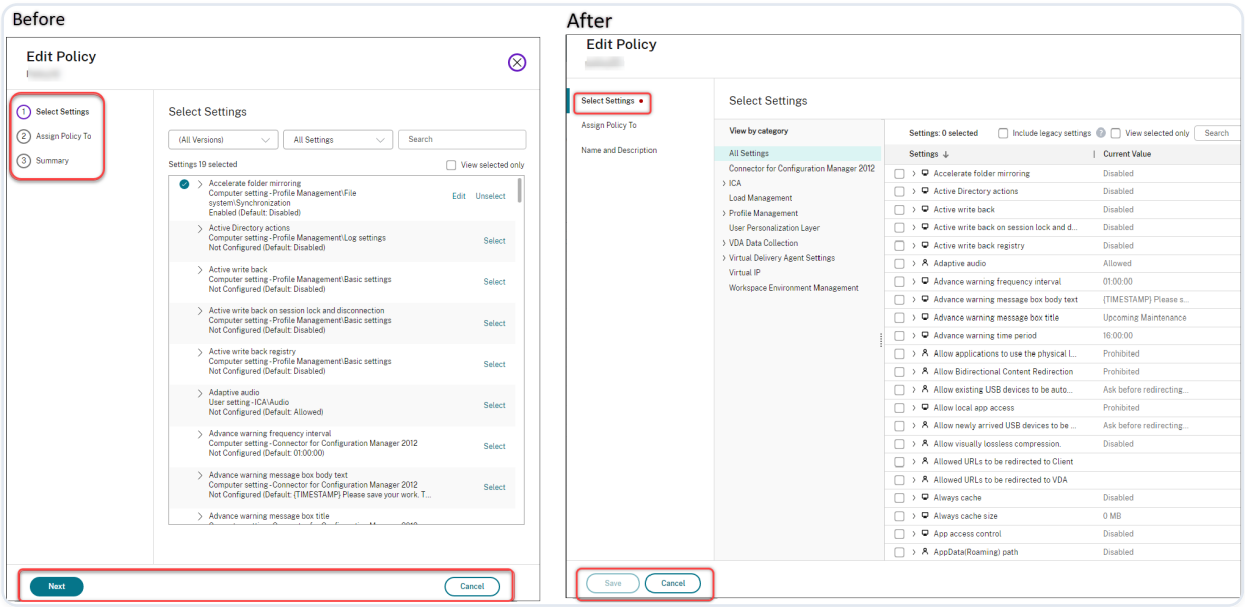
ポリシーセット。 **Web Studio > ポリシー**で、ポリシーセットを使用してポリシーをグループ化し、ロールベースのアクセスを簡素化できるようになりました。その後、ポリシーセットにスコープとデリバリーグループを割り当てることで、承認された管理者のみが関連するユーザーとマシンに適用されるポリシーを管理できるようになります。詳しくは、「ポリシーセット」を参照してください。

ユーザーエクスペリエンスの向上。 ユーザーエクスペリエンスを向上させ、ポリシー管理をより効率的にするために、**ポリシー**ノードに以下の改善を実装しました。

- **ポリシーの作成**および**テンプレートの作成**アクションの新しいUIデザイン:
    - ポリシー設定の展開可能なフォルダービュー。**設定の選択**ページでは、すべての設定がカテゴリ別に展開可能なツリービューで表示され、設定を見つけやすくなっています。
    - 設定を選択するには、**選択**ボタンを使用する代わりに、チェックボックスをクリックするだけです。
    - レガシー設定はデフォルトで非表示になり、最も関連性の高い設定のみが表示されます。レガシー設定が必要な場合は、**レガシー設定を含める**を選択してください。
    - ブール設定の横にアクションボタンが追加され、設定リストでその値を直接変更できるようになりました。



- **ポリシーの編集**アクションの新しいUIデザイン:
  - ナビゲーションメニューが順序なしリストに更新されました。リスト内の各項目には、そのページに**保存**ボタンが含まれるようになりました。この新しいデザインにより、ナビゲーションメニューのすべての項目を移動することなく、項目に加えられた変更を保存できます。これらの改善により、ポリシー管理がより効率的かつ合理化されます。
  - ナビゲーション項目の横に赤い点が表示され、設定エラーを示します。



- ドラッグしてポリシーの優先順位を変更します。優先順位リストで、ポリシーを目的の位置にドラッグすることで、その優先順位を変更できるようになりました。

ポリシーの作成/編集設定ページでのVDAバージョンサポート ポリシーの設定を構成する際、以下のカテゴリで設定を表示するオプションが利用可能になりました。

- **すべての設定。** すべてのVDAバージョンに適用可能なすべての設定を表示します。

- **現在の設定のみ。** 現在のVDAバージョンに固有の設定を表示します。
- **レガシー設定のみ。** 非推奨のVDAバージョンにのみ適用可能な設定を表示します。

強化された検索機能

検索機能を刷新し、フィルターとのインタラクションを含めることで、より良いユーザーエクスペリエンスを提供します。以下の機能が追加されました:

- **保存されたフィルターセットの削除**: **フィルターセットの管理**に移動することなく、検索メニュー内で保存されたフィルターセットを簡単に削除できるようになりました。
- **AND/OR演算子の更新**: **すべてに一致 (AND演算子)** および **いずれかに一致 (OR演算子)** オプションがフィルターパネルで利用可能になり、フィルターアイコンをワンクリックでアクセスできます。
- **簡素化された条件選択**: フィルターパネルで複数の条件を直接指定できるようになりました。
- **よりクリーンなインターフェイス**: **フィルターのピン留め**機能は削除され、UIの煩雑さが軽減され、検索エクスペリエンスがより直感的になりました。
- **クイックフィルター追加**: フィルターを適用した後、プラス記号を使用して、もう1つのフィルターをすばやく追加できるようになりました。

これらの機能強化は、**マシンカタログ**、**デリバリーグループ**、**アプリケーショングループ**、および**アプリケーション**などの他のノードにも拡張されました。

詳細については、「Studioでの検索の使用」を参照してください。

検索ノードのデータキャッシュ

検索ノードのデータキャッシュを導入しました。 この機能強化により、検索のパフォーマンスが向上し、通常のタスクを容易にするユースケースを以下に示します。

- 検索結果が初めて取得された後の迅速な表示。
- 検索ノードから移動して戻った後もページネーション結果を保持します。

Azure Germanyオプションを削除しました

Microsoft Cloud DeutschlandがOctober 29, 2021に閉鎖されたことに伴い、ホスト接続作成ページからAzure Germanyオプションを削除しました。

Web Studioを使用したCitrix Provisioningカタログ作成のサポート

Citrix Provisioningカタログを作成するには、Citrix Virtual Apps and Desktopsセットアップウィザードを使用する必要がありました。この機能により、Web StudioとPowerShellを使用してCitrix Provisioningカタログを作成できるようになりました。

この実装により、以下の利点が得られます。

- MCSとCitrix Provisioningカタログの両方を管理するための単一の統合コンソール。
- ID管理ソリューション、オンデマンドプロビジョニングなど、Citrix Provisioningカタログの新機能があります。

現在、この機能はAzureワークロードでのみ利用可能です。詳細については、Citrix StudioでCitrix Provisioningカタログを作成する を参照してください。

Citrix ディレクター

ユーザーインターフェイスの改善

Citrix Directorのユーザーインターフェイスが、モダンなルックアンドフィールに刷新されました。新しく改善されたユーザーインターフェイスは、より簡単なナビゲーションと優れたデータ表現を提供します。改善されたエクスペリエンスは直感的で、Citrixセッションの監視とトラブルシューティングに必要なデータを容易に理解できるように設計されています。

ライブセッションと録画セッションを再生する

Citrix Directorは、Session Recordingサービスを使用して記録された、記録済みおよびライブのユーザーセッションの再生をサポートするようになりました。再生から、ユーザーが遭遇したセッション関連の問題を迅速に理解できます。この機能により、Directorコンソール内でセッション関連のメトリックとともに記録にすぐにアクセスできます。これにより、記録で発見された問題とパフォーマンスメトリックを関連付けるのに役立ちます。複数のセッション記録サーバーで記録を検索したり、記録を表示するためにサードパーティ製アプリを探したりする必要がなくなります。

この機能には以下が必要です。

- VDAおよびSession Recordingサーバーはバージョン2308以降であること。
- Delivery Controller™およびDirectorはバージョン2311以降であること。

Directorは記録を一元的なリポジトリに保存し、**Session Selector**モーダルに表示します。**Sessions with recordings**リンクは、過去24時間または過去2日間にアクティブだったセッション

の記録を表示します。記録は、Citrix Session Recording再生サーバーを使用して新しいタブで再生されます。

詳細については、セッションの録画 を参照してください。

エンドツーエンドのネットワークホップビュー

エンドツーエンドのネットワークホップビューは、Citrix Directorにおけるトラブルシューティングワークフローを強化するための次のステップです。**User Details** > **Session Performance** > **Session Topology**セクションでは、接続されたHDXセッションのエンドツーエンドのネットワークホップビューを視覚的に表現します。セッション内パスは、セッションパスに関与するコンポーネントとそのメタデータ、コンポーネント間のリンク、およびVDAで公開されているアプリケーションを理解するのに役立ちます。セッショントポロジは、データフローを把握し、パフォーマンスの問題を引き起こしている可能性のある特定のホップを特定するのに役立ちます。

さらに、セッションが接続状態にある場合、ICA LatencyおよびICA RTTの測定値が表示されます。詳細については、エンドツーエンドのネットワークホップビュー を参照してください。

最適な画面解像度

Citrix Directorを表示するための推奨される最適な画面解像度は1440 x 1024に更新されました。Directorのシステム要件の詳細については、「システム要件」を参照してください。

MS Teamsの最適化

Directorは、Microsoft Teamsが最適化されているかどうかを表示します。これは、**ユーザーの詳細**ページ > **セッションの詳細**パネルで確認できます。この情報は、VDAバージョン2311以降で利用可能です。Directorは、Microsoft Teamsが公開アプリケーションとして、または公開デスクトップ内で実行されている場合にのみ、Microsoft Teamsの最適化ステータスを表示します。この機能強化により、チケット解決にかかる時間が短縮され、トラブルシューティング中に管理者が重要なメトリックを把握するのに役立ちます。詳細については、「ユーザーの問題のトラブルシューティング」を参照してください。

プローブの概要の機能強化

プローブ > **概要**ページで、プローブメトリックとプローブ失敗ステージの概要が利用可能になりました。プローブメトリックには、スケジュール済み、失敗、スキップ、成功した実行の数が表示されます。失敗ステージのグラフィカル表示は、ほとんどの失敗が発生したステージを分析するのに役立ちます。この情報は、プローブ結果のトラブルシューティングを迅速に行うのに役立ちます。詳細については、「アプリケーションとデスクトップのプローブ」の記事を参照してください。

「セッションログオン期間」ビューの刷新

ユーザーの詳細ページの新しい**セッションログオン**タブには、ログオン期間フェーズの視覚化が強化されています。新しい表示では、個々のログオンフェーズの重複が示されます。また、個々のフェーズの説明と、GPOおよびプロファイル詳細のサブフェーズ測定へのドリルダウンも提供されます。この視覚化は、ログオン期間に関連する問題を理解し、簡単にトラブルシューティングするのに役立ちます。詳細については、「ユーザーログオンの問題の診断」を参照してください。

動的セッション記録

セッションを再確立することなく、**ユーザーの詳細**画面のセッションレコーディングコントロールを使用して、現在アクティブなセッションを記録できるようになりました。この機能により、ユーザーが直面するセッションエクスペリエンス関連の問題のトラブルシューティングが迅速かつ効果的に行えます。これは、再現が困難な問題をデバッグするのに役立ちます。

動的セッション録画について詳しくは、セッション録画サービスの記事を参照してください。

マシン作成サービス (MCS)

プレビュー機能

休止状態対応VMのサポート（プレビュー）。Azure環境では、Web StudioおよびPowerShellコマンドを使用して、休止状態をサポートするMCSマシンカタログを作成できます。この機能を使用すると、セッションがしばらくアイドル状態になったときにVMを一時停止し、ユーザーが再度サインインしたときにVMの以前の状態に再接続できます。詳細については、「休止状態対応VMの作成（プレビュー）」を参照してください。

Citrix管理のHPE Moonshotプラグインのサポート（プレビュー）。以前は、Hewlett Packard Enterprise (HPE) が保守するHPE管理のMoonshotプラグイン（HPE Moonshot Machine Manager）を使用して、HPE Moonshotシャーシで電源管理アクションを実行していました。このプラグインはレガシーAPIに基づいており、MCSインフラストラクチャプロジェクトを困難にしていました。この機能により、Citrix管理のHPE Moonshotプラグイン（HPE Moonshot）が導入されました。このプラグインを使用すると、HPE Moonshotシャーシへの接続を作成し、カタログを作成し、Web StudioおよびPowerShellコマンドを使用してカタログ内のマシンの電源を管理できます。詳細については、以下を参照してください。

- HPE Moonshot仮想化環境（プレビュー）
- 「HPE Moonshot への接続 (プレビュー)」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections/connection-hpe-moonshot.html)

- 「HPE Moonshot マシンカタログの作成 (プレビュー)」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-hpe-moonshot.html)
- 「HPE Moonshot カタログの管理 (プレビュー)」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage/manage-machine-catalog-hpe-moonshot.html)

AWS 関連

マシンプロファイルソースからVMへのタグのコピーのサポート。この機能を使用すると、マシンプロファイルで指定されたNIC、およびディスク（IDディスク、ライトバックキャッシュディスク、OSディスク）のタグを、MCSマシンカタログで新しく作成されたVMにコピーできます。これらのタグは、任意のマシンプロファイルソース（AWS EC2インスタンスまたはAWS起動テンプレートバージョン）で指定できます。この機能は、永続および非永続マシンカタログとVMに適用されます。

詳しくは、VM上のタグをコピーするを参照してください。

CitrixからVMレコードを削除する際のタグの削除。以前は、`Remove-ProvVM`と`Remove-ProvScheme` PowerShellコマンドは、`ForgetVM`パラメーターを使用して、Citrixデータベースから VMとマシンカタログを削除していました。しかし、これらのコマンドはMCSによって作成されたタグを削除しませんでした。すべてのリソースから完全に削除されなかったVMとマシンカタログを個別に管理する必要がありました。

この機能を使用すると、次のことができます。

- `Remove-ProvVM`と`ForgetVM`パラメーターを使用して、マシンカタログから単一のVMまたはVMのリストからVMとMCS作成タグを削除します。
- `Remove-ProvScheme`と`ForgetVM`パラメーターを使用して、Citrixデータベースからマシンカタログを削除し、マシンカタログからリソースを削除します。

この実装は、以下の点で役立ちます。

- リークしたリソースの特定
- 不要なリソースを維持するための追加コストの削減

この機能は、永続VMにのみ適用されます。詳しくは、タグの削除を参照してください。

マシンプロファイルのサポート。AWSでMachine Creation Services (MCS) を使用してマシンをプロビジョニングするカタログを作成する際、EC2インスタンス（VM）または起動テンプレートバージョンからハードウェアプロパティをキャプチャし、それらをプロビジョニングされたマシンに適用するために、マシンプロファイルを使用できるようになりました。キャプチャされるプロパティには、例えば、EBSボリュームプロパティ、インスタンスタイプ、EBS最適化、およびそ

の他のサポートされているAWS構成が含まれます。カタログを編集する際、プロビジョニングされたマシンのマシンプロファイルは、別のVMまたは起動テンプレートを提供することで変更できます。詳しくは、マシンプロファイルを使用してカタログを作成するを参照してください。

インスタンスのフィルタリングのサポート。以前は、AWS EC2インスタンスをMCSマシンカタログを作成するためのマシンプロファイル入力として使用すると、無効なマシンプロファイル入力（たとえば、マスターイメージと互換性のない特定のプロパティ値を持つマシンプロファイル入力）が原因で、カタログが適切に作成されなかったり、正しく機能しなかったりすることがありました。この機能を使用すると、有効なマシンプロファイルVMとして使用できるAWS EC2インスタンスを一覧表示できます。これを行うには、`Get-HypInventoryItem`コマンドを使用します。詳細については、「VMインスタンスのフィルタリング」を参照してください。

インスタンスの休止状態のサポート。AWSインスタンスを起動し、必要に応じて使用し、その後休止状態にできるようになりました。休止プロセスでは、インスタンスのインメモリ状態と、そのプライベートIPアドレスおよびエラスティックIPアドレスが保存され、中断したところから正確に再開できます。休止状態をサポートするVMの作成の詳細については、「インスタンスの休止状態」を参照してください。

Azure関連

マシンプロファイルからの診断設定のキャプチャのサポート。Azure環境では、MCSは、MCSマシンカタログの作成または更新時、あるいは既存のVMの更新時に、マシンプロファイルからVMおよびNICの診断設定をキャプチャすることをサポートするようになりました。したがって、この実装により、診断データは、詳細な分析と視覚化のために、Log AnalyticsワークスペースやEvent Hubsなどの指定されたAzure宛先エンドポイントにシームレスに送信できます。詳細については、「マシンプロファイルからVMおよびNICの診断設定をキャプチャする」を参照してください。

MCSでのスポットVMの使用に対するAzureのサポート。AzureスポットVMを使用すると、Azureの未使用のコンピューティング容量を大幅なコスト削減で活用できます。ただし、その強制排除ポリシーのため、AzureスポットVMは一部の重要でないアプリケーションやデスクトップにのみ適しています。

この機能を使用すると、マシンプロファイル（VMまたはテンプレート仕様）を使用して、AzureスポットVMのMCSマシンカタログを作成できます。既存のカタログを更新して、新しく作成されたVMとしてAzureスポットVMを使用したり、標準のAzure VMに切り替えたりできます。既存のVMをAzureスポットVMに更新することもできます。詳細については、「AzureスポットVMを使用してカタログを作成する」を参照してください。

マシンプロファイルに関連付けられたホストでの暗号化情報を取得する。Azure環境では、この機能により、PowerShellコマンドを使用して、マシンプロファイル入力（VMまたはテンプレート仕

様）に対してホストでの暗号化が有効になっているかどうかを知ることができるようになりました。詳細については、「マシンプロファイルからホストでの暗号化情報を取得する」を参照してください。

マスターイメージのディスク暗号化セットID（DES ID）を使用して、カタログVMのすべてのディスクを暗号化する。Azure環境では、以前はMCSマシンカタログのディスク暗号化セットID（DES ID）はマシンプロファイルまたはカスタムプロパティから派生していました。この機能により、マシンカタログはマスターイメージからDES IDを派生させて、カタログ内のVMのすべてのディスクを暗号化することもできます。

顧客管理の暗号化キーが有効なPVSカタログの作成をサポート。 Azure環境では、Web StudioおよびPowerShellコマンドを使用して、顧客管理の暗号化キー (CMEK) が有効なPVSカタログを作成できるようになりました。詳細については、「顧客管理の暗号化キーが有効なカタログを作成する」を参照してください。

MCSはPVSカタログ作成用のリソースグループを作成する。Web Studioを使用してPVSカタログを作成する際に、既存のリソースグループを選択しない場合、MCSはカタログ作成用のリソースグループを自動的に作成します。PVSカタログの作成の詳細については、「Citrix Provisioningカタログを作成する」を参照してください。

バックアップVMサイズの構成のサポート。パブリッククラウドでは、特定のVMサイズの容量が不足することがあります。また、AzureスポットVMを使用している場合、Azureの容量要件に基づいてVMはいつでも強制排除されます。Azureの容量不足やスポットVMの電源投入失敗といった場合、MCSはバックアップVMサイズにフォールバックするようになりました。カスタムプロパティ `BackupVmConfiguration` を使用して、バックアップVMサイズのリストを提供できます。MCSは、リストで指定された順序でバックアップVMサイズにフォールバックしようとします。提供されたすべてのバックアップVMサイズにフォールバックできない場合、エラーメッセージが表示されます。

この機能は、マシンプロファイルを使用するカタログでのみサポートされており、永続的および非永続的なMCSマシンカタログの両方に適用できます。この機能は現在、Azure環境でのみサポートされています。

詳細については、「バックアップVMサイズを構成する」を参照してください。

すべてのリソースにタグをコピーする機能。 この機能により、Azure環境では、マシンプロファイルで指定されたタグを、新しいVMまたはマシンカタログ内の既存のVMの複数のNICやディスク (OSディスク、IDディスク、ライトバックキャッシュディスクなど) のすべてのリソースにコピーできるようになりました。

マシンプロファイルのソースは、VM または ARM テンプレート仕様にすることができます。詳細については、「すべてのリソースにタグをコピーする」を参照してください。

Azure Monitor Agent を使用したカタログ VM のプロビジョニングのサポート。Azure Monitor Agent (AMA) は、監視データを収集し、Azure Monitor に配信します。この機能により、MCS マシンカタログ VM (永続的および非永続的) を、AMA を拡張機能としてインストールしてプロビジョニングできます。この実装により、監視データ内の VM を一意に識別することで監視が可能になります。AMA の詳細については、「Azure Monitor Agent の概要」を参照してください。

現在、MCS はこの機能に対してマシンプロファイルワークフローのみをサポートしています。

AMA が有効なマシンカタログ VM のプロビジョニングの詳細については、「Azure Monitor Agent がインストールされたカタログ VM のプロビジョニング」を参照してください。

マシンカタログの管理

マシンカタログの異なるバージョンの管理に対する MCS のサポート。この機能を使用すると、PowerShell コマンドを使用してマシンカタログの構成バージョンを管理できます。`Set-ProvScheme` を使用した構成の変更ごとに、新しい構成バージョンが作成されます。次のことができます。

- バージョンの一覧を表示する
- 以前のバージョンを使用してマシンカタログを更新する
- VM で使用されていないバージョンを手動で削除する
- マシンカタログが保持する最大バージョン数を変更する

詳細については、「マシンカタログのバージョンを管理する」を参照してください。

AWS 環境で、マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換するサポート。AWS 環境では、VM または起動テンプレートをマシンプロファイルの入力として使用して、マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換できるようになりました。カタログに追加された新しい VM は、マシンプロファイルからプロパティ値を取得します。詳細については、「マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換する」を参照してください。

アクティブなコンピューターアカウントの ID 情報の修復。この機能を使用すると、ID 関連の問題があるアクティブなコンピューターアカウントの ID 情報をリセットできます。マシンパスワードと信頼キーのみをリセットするか、ID ディスクのすべての構成をリセットするかを選択できます。この実装は、永続的および非永続的な両方のマシンカタログに適用できます。現在、この機能

は Azure および VMware 仮想化環境でのみサポートされています。詳細については、「アクティブなコンピューターアカウントの ID 情報を修復する」を参照してください。

AWS で MCS によって作成されたマシンカタログ内の永続 VM の OS ディスクをリセットする機能。AWS 環境では、PowerShell コマンド `Reset-ProvVMDisk` を使用して、MCS によって作成されたマシンカタログ内の永続 VM の OS ディスクをリセットできるようになりました。この機能は、OS ディスクのリセットプロセスを自動化します。たとえば、MCS を使用して作成された永続的な開発デスクトップカタログの VM を初期状態にリセットするのに役立ちます。

PowerShell コマンドを使用して OS ディスクをリセットする方法の詳細については、「OS ディスクのリセット」を参照してください。

孤立したリソースのリストを取得する

MCSによって作成されたものの、MCSによって追跡されなくなった孤立したリソースのリストを取得できます。これは現在、Azure環境に適用されます。リストを取得するには、PowerShellコマンドを使用できます。接続を使用してフィルタリングできます。詳細については、「孤立したリソースのリストを取得する」を参照してください。

MCSによるメモリおよびディスクキャッシュサイズの変更機能

この機能により、新しいマシンカタログを作成することなく、PowerShellコマンドを使用してライトバックキャッシュ（MCSIOが有効な場合）のメモリおよびディスクキャッシュサイズを変更できるようになりました。この実装は、ビジネスニーズに適した最適化されたキャッシュ構成を持つことに役立ちます。この機能は以下に適用されます。

- GCPおよびMicrosoft Azure環境、および
- MCSIOが有効な非永続カタログ

詳細については、「既存のマシンカタログのキャッシュ構成を変更する」を参照してください。

VMwareにおけるVMのストレージ移行のサポート

この機能により、VMware環境で、既存のVMのディスクストレージを古いストレージから新しいストレージに移動できます。移行中、MCSは電源管理、OSディスクのリセットなどのVM機能を保持します。新しいディスクストレージサービスを使用して、新しいVMをマシンカタログに追加することもできます。これを行うには、PowerShellコマンド`Move-ProvVMDisk`を使用します。詳細については、「VMのストレージ移行」を参照してください。

マシンプロファイルに対するSCVMMのサポート

この機能により、System Center Virtual Machine Manager (SCVMM) 環境でマシンプロファイルを使用してMCSマシンカタログを作成および更新できるようになりました。ネストされた仮想化とvTPMを有効にすることもできます。詳細については、「マシンプロファイルを使用してカタログを作成する」を参照してください。

ハイブリッドAzure AD参加済みマシンIDのユーザー証明書を修復する

この機能により、ハイブリッドAzure AD参加済みマシンIDのユーザー証明書が破損または期限切れになった場合、PowerShellコマンドを使用して修復できます。詳細については、「ハイブリッドAzure Active Directory参加済みカタログを作成する」を参照してください。

ハイブリッドAzure AD参加済みマシンカタログのユーザー証明書の有効期限に関する情報を取得するには、`Get-ProvScheme`コマンドを実行します。

SCCMの重複GUID問題の解決策

MCSを使用して複数のVMを作成した後、System Center Configuration Manager (SCCM) は、GUIDが重複しているため、コンソールに1つのVMしか表示しませんでした。この問題は、イメージ準備にステップを追加することで解決されました。このステップは、マスターイメージ内の既存の証明書とGUID情報を削除します。このステップはデフォルトで有効になっています。

プロファイル管理

新機能については、独自のドキュメントにある新機能の記事を参照してください。

リナックス VDA

新機能については、独自のドキュメントにある新機能の記事を参照してください。

セッション録画

新機能については、独自のドキュメントにある新機能の記事を参照してください。

ワークスペース環境管理™

新機能については、独自のドキュメントにある新機能の記事を参照してください。

シトリックス プロビジョニング

新機能については、独自のドキュメントにある新機能の記事を参照してください。

フェデレーション認証サービス

新機能については、独自のドキュメントにある新機能の記事を参照してください。

修正された問題

Citrix Virtual Apps and Desktops™ 2311 には、以下の修正された問題が含まれています。

全般

- Citrix Workspace™ アプリからVDAに渡される際、オーディオデバイスの名前が32文字に切り詰められます。その結果、一部のアプリではクライアントセッションでデバイスが認識されない場合があります。
- ブラウザコンテンツリダイレクトされたサイトにアクセスした後、ユーザーセッションからサインアウトすると、エラーメッセージが表示される場合があります。回避策として、エラーメッセージを無視してください。
- クライアントへの位置情報アクセスを有効にするために使用されるポリシー「**Allow applications to use the physical location of the client device**」が機能しません。
- Automated Configuration Tool (ACT) を使用してオンプレミス環境からクラウド環境に移行すると、移行完了後、**Manage Autoscale** インターフェイスの **User Logoff Notifications** データが **Send logoff reminders without forcing user logoff** に変更されます。この問題を解決するには、Automated Configuration for Virtual Apps and Desktops からACTの最新バージョンをダウンロードしてください。

Citrixポリシー

- **Citrix Group Policy Modelling Wizard** でユーザーを選択し、**Skip to the final page of the wizard without collecting additional data** オプションを選択すると、**Summary** ページに次のエラーメッセージが表示される場合があります。

  値はnullにできません。パラメーター名キー

- プロファイルのリセット後、フォルダーリダイレクトが断続的に失敗する場合があります。

デリバリーコントローラー™

- 特定のCitrix XMLパフォーマンスカウンターがパフォーマンスモニターグラフに追加されない場合があります。
- パスワードフィールドが空の場合、公開されたリソースの列挙に失敗する場合があります。

グラフィック

- ダブルホップセッションでWebカメラが期待どおりに動作しません。この問題は、仮想デスクトップセッション内から仮想デスクトップまたはアプリケーションを起動するために、次のいずれかのクライアントを使用した場合に発生します。
  - Windows版 Citrix Workspaceアプリ
  - Linux向け Citrix Workspace アプリ
  - Mac向けCitrix Workspaceアプリ
- Windows Virtual Desktop Agent上の一部のアプリケーションで、Webカメラのリダイレクトが失敗する場合があります。
- ポリシー「ドラッグ中のウィンドウコンテンツの表示」を「禁止」に設定しても、ESXiおよびHyper-Vでは機能しません。
- セッション中にALT+TABキーを押すと、**Graphics Status Indicator**がアプリとして表示されます。このアプリをクリックすると、ボタンのない灰色のウィンドウが表示されます。そのため、ウィンドウを適切に閉じることができません。ALT+F4で閉じると、**Graphics Status Indicator**は閉じられ、セッション中は利用できなくなります。

HDX USBデバイス

- クライアントUSBデバイスの自動リダイレクトがオンになっている場合でも、Bloomberg Keyboard 5 Biometric Moduleが自動的に接続できない場合があります。

マシン作成サービス™

- Delivery ControllerとリモートPowerShellのバージョンに互換性がない場合、ForgetVMパラメーターを指定したPowerShellコマンドRemove-ProvVMが正しく機能しない可能性があります。これは、Delivery ControllerとリモートPowerShellのバージョンが両方とも2212より前であるか、または2212以降である必要があることを意味します。たとえば、Delivery Controllerのバージョンが2212より新しく、リモートPowerShellのバージョンが2212より古い場合、ForgetVMパラメーターを指定したRemove-ProvVMコマンドは期待どおりに機能しません。回避策として、最新のDelivery Controllerバージョンで動作するように最新のPowerShellバージョンをダウンロードしてください。

メタインストーラー

- Citrix Virtual Apps and Desktopsをバージョン1912 LTSRからバージョン2305または2203 LTSRにアップグレードしようとすると、次のエラーメッセージが表示されて失敗する場合があります: サポートされていない構成が検出されました。

ユニバーサル プリント サーバー

サーバー

- Universal Print Serverに接続されているプリンターが、印刷中にセッションに表示されない場合があります。この問題は、Universal Print Serverでhttpd.confファイルが変更されたときに発生します。
- Citrix Universal™ Print Serverを使用してファイルを印刷しているときに、Print Spoolerサービスが予期せず終了する場合があります。
- プリンターのセキュリティ権限から**Everyone**グループを削除すると、Citrix Universal Print Serverが期待どおりに機能しない場合があります。

クライアント

- Knowledge Centerの記事CTX140208に記載されているとおりにインストールされたHP Color LaserJet 2800 Series PSドライバーが、VDAのアップグレード中にアンインストールされる場合があります。

シングルセッションOS用VDA

インストール、アンインストール、アップグレード

- VDAをバージョン2203 LTSR CU3にアップグレードした後、カスタムICA®ファイルを使用してアプリケーションを起動しようとすると失敗する場合があります。

キーボード

- VDAをバージョン2305またはバージョン2203 LTSR CU3にアップグレードした後、ショートカットキーの組み合わせが正しく機能しない場合があります。たとえば、Word文書で選択した単語に対して**Ctrl+Shift+K**キーを押すと大文字になります。しかし、**K**キーを離してもう一度押しても、変更は元に戻りません。

印刷

- 初回起動時にローカルプリンターがセッションにリダイレクトされない場合があります。ただし、2回目以降の起動時にはローカルプリンターがリダイレクトされます。

- macOS Sonomaを実行しているMac版Citrix Workspaceアプリを使用してローカルプリンター経由でファイルを印刷しようとすると、次のエラーメッセージが表示されて失敗する場合があります。

  エラー: プリンターがアクティブ化されていません。エラーコード -41

- Citrix Universal Printer Driver (UPD) を使用してファイルを印刷しようとすると、印刷されたファイルに誤った画像が表示されることがあります。この問題は、VDA をバージョン 7.15.5000 からバージョン 1912.1000 にアップグレードし、ヘビーウェイト圧縮を有効にした場合に発生します。
- Universal Print Server ポリシーが有効になっている VDA を再起動すると、Universal Print Server の負荷分散が開始されない場合があります。

セッション/接続

- この修正により、トースト通知がシームレスセッションに表示される場合があります。この修正を機能させるには、shellbridge を有効にする必要があります。ただし、この修正には以下の視覚的な制限があります。
  - トースト通知の周囲に黒い背景が表示されます。
  - トースト通知がローカルタスクバーの一部を覆います。
- スマートカードを使用して Citrix Virtual Apps and Desktops バージョン 2203 LTSR CU2 の VDA セッションに再接続しようとすると、**ようこそ**画面で停止したままになることがあります。
- IPv6 が有効になっている場合、VDA が断続的に登録解除されることがあります。
- バージョン 2203 LTSR CU2 を実行し、Microsoft Defender Application Control がインストールされている VDA に接続するセッションを開始すると、数秒間グレーの画面が表示されることがあります。
- Delivery Controller で Browser Content Redirection (BCR) プロキシ構成ポリシーを「Direct」に設定すると、エンドポイントまたはネットワークからの遅延により、BCR Webページが部分的にしか読み込まれない場合があります。

スマートカード

- VDA からログオフすると、CtxSvcHost (CtxSmartCardSvc) が予期せず終了する場合があります。

システム例外

- バージョン 2203 LTSR CU2 から CU3 にアップグレードされた VDA で、picadm.sys に致命的な例外が発生し、ブルースクリーンが表示されることがあります。

ユーザーエクスペリエンス

- テキストと画像にコピーオプションを使用してコンテンツをコピーしたり、書式設定されたコンテンツをコピーしたりすると、機能しない場合があります。
- 公開されたMicrosoft Visioまたはデスクトップ上のVisioアプリからユーザーデバイス上のアプリにコンテンツをコピーすると、失敗する場合があります。

ユーザーインターフェイス

- Windows Serverバージョン2019以前では、VDAがマウスイベントをエンドポイントに送信できず、アプリケーションでグラフィックまたはマウスの問題が発生する場合があります。
- 非英語オペレーティングシステムで**Citrix HDX 3D Pro Warning**ダイアログに表示されるメッセージが破損して表示される場合があります。

マルチセッションOS用VDA

インストール、アンインストール、アップグレード

- VDAをバージョン2203 LTSR CU3にアップグレードした後、カスタムICAファイルでアプリケーションを起動しようとすると失敗する場合があります。

印刷

- 初回起動時にローカルプリンターがセッションにリダイレクトされない場合があります。ただし、それ以降の起動時にはローカルプリンターはリダイレクトされます。
- macOS Sonomaを実行しているMac版Citrix Workspaceアプリを使用してローカルプリンター経由でファイルを印刷しようとすると、次のエラーメッセージが表示されて失敗する場合があります。

  エラー: プリンターがアクティブ化されていません。エラーコード -41

- Citrix Universal Printer Driver (UPD) を使用してファイルを印刷しようとすると、印刷されたファイルに誤った画像が表示されることがあります。この問題は、VDAをバージョン7.15.5000からバージョン1912.1000にアップグレードし、**heavyweight compression**を有効にした場合に発生します。

- Universal Print Serverポリシーが有効なVDAを再起動すると、Universal Print Serverの負荷分散が開始されない場合があります。

セッション/接続

- Citrix Virtual Apps and Desktops バージョン 2203 LTSR CU2 でスマートカードを使用して VDA セッションに再接続しようとすると、ようこそ画面で停止したままになることがあります。
- shellbridge が有効になっている場合、ウィンドウの **X** アイコンをクリックしてもセッションからログオフできないことがあります。
- IPv6 が有効になっている場合、VDA が断続的に登録解除されることがあります。
- Delivery Controller で Browser Content Redirection (BCR) プロキシ構成ポリシーを Direct に設定した後、エンドポイントまたはネットワークの遅延により、BCR の Web ページが部分的にしか読み込まれないことがあります。

スマートカード

- VDAからログオフすると、CtxSvcHost (CtxSmartCardSvc) が予期せず終了する場合があります。

システム例外

- バージョン 2203 LTSR CU2 から CU3 にアップグレードされた VDA で、picadm.sys に致命的な例外が発生し、ブルースクリーンが表示されることがあります。
- VDA を 1912 LTSR CU5 から CU6 にアップグレードすると、Wdica.sys に致命的な例外が発生し、バグチェックコード 0x000000CE を伴うブルースクリーンが表示されます。

ユーザーエクスペリエンス

- 「テキストと画像にコピー」オプションを使用してコンテンツをコピーしたり、書式設定されたコンテンツをコピーしたりすると、失敗することがあります。
- 公開された Microsoft Visio またはデスクトップ上の Visio アプリからユーザーデバイス上のアプリにコンテンツをコピーすると、失敗することがあります。
- ドラッグアンドドロップポリシーが有効になっている場合、公開アプリケーションのドラッグまたはサイズ変更の試行が失敗する可能性があります。

仮想デスクトップコンポーネント - その他

- VDAをバージョン2203にアップグレードした後、デュアル管理者モードでネットワーク共有から開かれた公開App-Vアプリケーションが起動に失敗する場合があります。

プロファイル管理

- (/ja-jp/profile-management/current-release/whats-new/fixed-issues.html)は、このリリースでの更新に関する具体的な情報を提供します。

リナックス ブイディーエー

- (/ja-jp/linux-virtual-delivery-agent/current-release/whats-new/fixed-issues.html)は、このリリースでの更新に関する具体的な情報を提供します。

セッション録画

- (/ja-jp/session-recording/current-release/whats-new/fixed-issues.html)は、このリリースでの更新に関する具体的な情報を提供します。

ワークスペース環境管理™

- (/ja-jp/workspace-environment-management/current-release/fixed-issues.html)は、このリリースでの更新に関する具体的な情報を提供します。

シトリックス プロビジョニング™

- (/ja-jp/provisioning/current-release/whats-new/fixed-issues.html)は、このリリースでの更新に関する具体的な情報を提供します。

フェデレーション認証サービス

- (/ja-jp/federated-authentication-service/current-release/whats-new/fixed-issues.html)は、このリリースでの更新に関する具体的な情報を提供します。

既知の問題

注

- 既知の問題に回避策がある場合は、問題の説明の後に記載されています。
- レジストリエントリの変更を推奨する回避策には、次の警告が適用されます。

> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になる深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤っ

> た使用によって生じる問題を解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

全般

- VDAをアップグレードする前にCitrix Files for Windowsおよび/またはCitrix Files for Officeがインストールされている場合、これらのコンポーネントはアップグレードプロセス中にアンインストールされます。これを解決するには、VDAのアップグレードが完了した後でコンポーネントを再インストールしてください。
- アプリバーを起動し、Citrix Workspace™ app for WindowsでConnection Centerメニューを開くと、アプリバーはそれをホストするサーバーの下に表示されません。
- Citrix Workspace app for Windowsを使用し、アプリバーを垂直位置で起動すると、バーがスタートメニューまたはシステムクロックトレイを覆います。
- ユーザーがホスト上で既にフォーカスされているコンボボックスを選択すると、コンボボックスが正しく表示されない場合があります。回避策として、別のUI要素を選択してからコンボボックスを選択してください。
- Windows 10からWindows 11へのインプレースOSアップグレードを実行した後、Citrix Desktop Serviceが起動に失敗する場合があります。この問題を解決するには、マシンを再起動してください。
- Windows Server 2022、Windows 10 Enterprise multi-session、およびWindows 11 Enterprise multi-sessionを実行しているセッションホストでは、マルチセッションVDAのセッション制限設定が拒否されます。

  回避策として、GPOを通じてRDSセッション時間制限を構成できます。
- 管理者権限でアプリケーションを実行している場合、FIDO2に関連付けられたWindowsセキュリティダイアログボックスはICA®セッションウィンドウの前面に表示されません。 昇格されたプロセスとして実行されている場合、WindowsセキュリティダイアログボックスがICAセッションウィンドウの背後に隠れるのは、オペレーティングシステムの設計によるものです。
- クライアントからICAセッションへの100MBを超えるデータのクリップボードのコピーと貼り付けが失敗する場合があります。大容量バッファのコピーはサポートされていません。
- Webカメラのリダイレクトの場合、RDPクライアントからセカンドホップへの接続はサポートされていません。
- Windows VDAを使用している場合、日本語キーボードから韓国語キーボードに切り替える際にキーボードマッピングエラーが発生する可能性があります。

- 以下のように環境が構成されているデスクトップセッションで画像をスキャンする際に、画像がスキャンされないことがあります。この問題は断続的に発生します。
  - スキャナードライバーおよびイメージングアプリケーションのインストール
  - DDCでUSBリダイレクトポリシーが有効化されている
  - 環境設定:
    - DDC: Win2k19 + 7.33CU4 の組み合わせ
    - VDA: Win2k19/Win2k16+ 7.40.0.191
    - クライアント: Win10x64 22H2 + CWA 24.1.0.597
- 一部のシナリオで、クライアントIPポリシーフィルターを使用すると、ポリシーの評価に使用されるIPアドレスが正しくありません。
- Microsoft Teamsチャットからの画面共有はサポートされていません。

ポリシー

- Citrix Virtual Apps and Desktopsの以前のバージョンから2311または2402 LTSRにアップグレードする場合、Policy設定に無効なデータ値が存在すると、ポリシーデータが失われる可能性があります。この問題と関連する回避策の詳細については、CTX666304を参照してください。

スタジオ

- 「すべて」のスコープを持たないカスタム管理者は、デフォルトのポリシーセットからポリシーを編集または削除できません。 回避策として、カスタム管理者がアクセスできるスコープをデフォルトポリシーに追加します。

グラフィック

- Theora圧縮を使用して64ビットのWebカメラアプリでビデオプレビューを開始すると、セッションがクラッシュする可能性があります。
- Windows 11 バージョン 22H2 で、セッション内で Windows Media Player ウィンドウを移動すると、ビデオの下半分のみが表示されます。回避策として、 **> > > >** を選択します。
- Skype for desktopアプリで、リモートデスクトップに接続されている余分なWebカメラに気づく場合があります。これらの余分なWebカメラのプレビューはブロックされ、セキュリティ上の理由から黒い画面が表示されることがあります。余分なWebカメラは無視し、エンドポイント用のWebカメラを引き続き使用できます。

マシン作成サービス™

- AWSでホストされているVMware環境では、マスターイメージでvTPMが有効になっている場合、MCSマシンカタログの作成が失敗します。この問題は、すべてのCitrix Virtual Apps and Desktopsバージョンに影響し、VMware環境の問題が原因です。サポートについては、VMwareサポートにお問い合わせください。

ウェブスタジオ

- 展開で *Citrix Studio* と *Web Studio* の両方を使用している場合、*Citrix Studio* でアプリケーションフォルダを作成しても、そのフォルダにアプリケーションを追加しないと、その空のフォルダが *Web Studio* に表示されないという問題が発生する可能性があります。
- Web Studio を使用して Azure へのホスティング接続を作成する際に、 ページで をクリックし、 をクリックすると、エラーが発生する場合があります。この問題を解決するには、ブラウザでサードパーティの Cookie を許可してください。

印刷

- 仮想デスクトップで選択されたUniversal Print Serverプリンターは、コントロールパネルの**デバイスとプリンター**ウィンドウに表示されません。ただし、ユーザーがアプリケーションで作業している場合、それらのプリンターを使用できます。この問題はWindows 10でのみ発生します。詳細については、CTX213540を参照してください。
- 印刷ダイアログウィンドウでデフォルトプリンターが正しくマークされない場合があります。この問題は、デフォルトプリンターに送信される印刷ジョブには影響しません。
- Universal Print ServerへのSSL接続が有効になっている場合、ロードバランスされたネットワークプリンターからの印刷ジョブの一部が失敗することがあります。これは、印刷ジョブが次々と高速に実行された場合に発生します。

サードパーティの問題

- Chrome は、Web ページのツールバー、タブ、メニュー、およびボタンに対してのみ UI オートメーションをサポートしています。この Chrome の問題により、タッチデバイス上の Chrome ブラウザでは自動キーボード表示機能が動作しない場合があります。回避策として、`chrome --force-renderer-accessibility` を実行するか、新しいブラウザタブを開いて `chrome://accessibility` と入力し、特定のページまたはすべてのページで **Native accessibility API** のサポートを有効にすることができます。さらに、シームレスアプリを公開する際に、`--force-renderer-accessibility` スイッチを使用して Chrome を公開できます。

- セッションホストに FsLogix 2201 HF1 がインストールされている場合、セッションの起動時に黒い画面が表示されることがあります。この問題に対処するには、FsLogix を新しいバージョンにアップグレードする必要があります。

プロファイル管理

- Profile Management 2311 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

リナックス VDA

- Linux VDA 2311 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

セッション録画

- Session Recording 2311 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

ワークスペース エンバイロメント マネジメント™

- Workspace Environment Management 2311 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

シトリックス プロビジョニング™

- Citrix Provisioning 2311 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

フェデレーション認証サービス

- Federated Authentication Service 2311 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

廃止予定

この記事のお知らせは、段階的に廃止されるプラットフォーム、Citrix製品、および機能について事前に通知し、お客様がタイムリーなビジネス上の意思決定を行えるようにすることを目的としています。Citrixは、いつそれらが廃止されるかを決定するために、顧客の使用状況とフィードバックを監視しています。お知らせは、その後のリリースで変更される可能性があり、すべての非推奨の機能や機能が含まれていない場合があります。製品ライフサイクルサポートの詳細については、製品ライフサイクルサポートポリシーの記事を参照してください。Long Term Service

Release (LTSR) サービスオプションについては、`<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX205549>`を参照してください。

廃止予定と削除

次の表は、非推奨または削除されたプラットフォーム、Citrix®製品、および機能を示しています。**太字**の日付は、このリリースでの変更を示します。

非推奨

非推奨の項目はすぐに削除されません。Citrixは引き続きそれらをサポートしますが、将来のリリースで削除されます。

項目	非推奨が発表されたバージョン	代替
ターゲット最小フレームレートポリシー	2311	ターゲット最小フレームレートを変更するには、**グラフィックスステータスインジケーター**を使用します。
システムセンターコンフィギュレーションマネージャー用 Citrixコネクタ 3.1 のサポート	2311	イメージまたはアプリケーションの更新を手動で行います。
カタログが作成されたリージョンとは異なるリージョンでマスターイメージを使用するためのサポート	2311	マスターイメージを目的のリージョンにレプリケートするには、Azure Compute Galleryを使用します。
HDX™ Graphics ディスプレイメモリ制限設定	2311	クライアントの表示レイアウトが完全に収容されるように、必要な最小限のメモリが割り当てられます。
HDX Graphicsでのプログレッシブモードのサポート	2311	Thinwireを使用します。プログレッシブモードを参照してください。
Internet Explorer 11でのブラウザコンテンツリダイレクトのサポート	2311	Google Chromeベースのブラウザコンテンツリダイレクトを使用します。

項目	非推奨が発表されたバージョン	代替
AWSボリュームワーカーのサポートを削除しました	2311	Direct disk upload and downloadを使用します。Direct disk upload and downloadを参照してください。
BrokerでのSQL Server 2016のサポート	2308	最新バージョンを使用してください。詳細については、「システム要件」を参照してください。
DirectorでのXenApp 5.xのサポート	2308	---
DirectorでのXenApp 6.xのサポート	2308	---
Directorでのアラート用SCOMパック	2308	---
Directorでのプラグインのサポート	2308	---
WebRTC SDP形式 (プランB)のサポート	2308	Citrix Workspace™ アプリをサポートされているバージョンにアップグレードしてください。
Microsoft Teams最適化におけるシングルウィンドウモードのサポート	2308	Citrix Workspaceアプリをマルチウィンドウモードをサポートするバージョンにアップグレードしてください。詳細については、機能マトリックスとバージョンサポートを参照してください。
AWS環境で使用される `AwsCaptureInstanceProperties` のサポート	2308	マシンプロファイルを使用してください。マシンプロファイルを使用してカタログを作成するを参照してください。

項目	非推奨が発表されたバージョン	代替
`Schedule-ProvVMUpdate` PowerShellコマンド	2305	`Set-ProvVMUpdateTimeWindow` を使用してください。
`Request-ProvVMUpdate` PowerShellコマンド	2305	`Set-ProvVMUpdateTimeWindow` を `-StartsNow` および `-DurationInMinutes -1` パラメーターとともに使用してください。
`Cancel-ProvVMUpdate` PowerShell コマンド	2305	`Clear-ProvVMUpdateTimeWindow` を使用します。
`New-ProvScheme` コマンドで使用される `DedicatedTenancy` パラメーター	2303	`TenancyType` パラメーターを使用します。
ライセンスサーバー VPX	2206	---
Azure 環境で VM をプロビジョニングするためのアンマネージドディスク。	2206	マネージドディスクを使用。
ホストからクライアントへの (URL) リダイレクト	2203	双方向コンテンツリダイレクト。
クラウドおよびオンプレミス環境で使用される4つのAWS固有コマンドのサポート: `Revoke-HypSecurityGroupIngress`、`Revoke-HypSecurityGroupEgress`、`Grant-Hypsecuritygroupegress`、および `Grant-`	2203	---

項目	非推奨が発表されたバージョン	代替
`HypSecurityGroupIngress`。		
VDAメタインストーラーからのCitrix Files for WindowsおよびCitrix Files for Outlook。	2203	スタンドアロンインストーラーを使用してください。
VDAメタインストーラーからのWEMエージェントコンポーネント。	2203	---
Remote PC Access用のSCCM統合型Wake on LANオプション。	2012	スタンドアロンWake on LAN機能を使用してください。
XenAppおよびXenDesktop、Provisioning Services、StoreFront用のCitrix SCOM Management Pack。監視可能な製品バージョンについては、Citrix SCOM Management Packsのドキュメントを参照してください。	1912	展開の監視と管理にはDirectorを使用してください。SCOMのEOLと代替策の詳細については、https://support.citrix.com/article/CTX266943を参照してください。
モビリティ SDK / モバイル SDK (旧Citrix Labsより)	7.16	モバイルエクスペリエンスポリシー設定、およびホスト型デスクトップ/アプリのネイティブエクスペリエンスに置き換えられました。

削除

削除された項目は、Citrix Virtual Apps and Desktopsから削除されたか、サポートされなくなりました。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
Citrix StudioでのPVSインポー	1912 LTSR	2311	以下のいずれかの方法でCitrix

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
トウィザードのサポート			Provisioning™ マシンをプロビジョニングします。 • Citrix Provisioning Console を使用してマシンをプロビジョニングし、Citrix Provisioning Devices Export Wizardを使用して Citrix Virtual Apps and Desktopsにエクスポートします。Export Devices Wizardで詳細を確認してください。 • Web Studio を使用して Citrix Provisioningカタログ

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
			を作成します。Create Citrix Provisioning catalogs in Citrix Studioで詳細を確認してください。
HDX Graphics FullScreen + テキスト最適化	2311	2311	
HDX 3D ProでのNVIDIA Frame Buffer Capture (NVFBC) のサポート	2308	2311	Desktop Duplication API (DDAPI) を使用します。
vGPU 11以前、およびドライバーバージョン466.77以前のNVIDIA GPUハードウェアエンコード (NVENC)。	2305	2305	現在サポートされているNVIDIAドライバーを使用してください: vGPU 13以降、バージョン471.41以降。
VDAメタインストーラーからのCitrix Supportability Tools (SupportabilityTool_x64 .msi)。	---	2212	---

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
Citrix License Administration Console (Windows License Server 11.16.3 build 30000に最後に含まれ、Windows License Server v11.16.6 build 31000で削除されました)。	2003	2006	Citrix Licensing Managerを使用してください。
Windows 10 バージョン 1709以前での Citrix Indirect Display Driver (IDD) グラフィックアダプターのサポート。	2003	2003	Citrix Virtual Apps and Desktops 7 1912 LTSR VDAを使用してください。
GRID 9以前のディスプレイドライバーを使用したNVIDIA GPU (NVENC) によるハードウェアエンコーディング。	2003	2003	Citrix Virtual Apps and Desktops 7 2003以降のVDAでGRID 10ディスプレイドライバーを使用するか、Citrix Virtual Apps and Desktops 7 1912 LTSR VDAを使用します。
セルフサービスパスワードリ	2003	2006	---

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
セット (SSPR) 機能。			
VDAおよびコアサーバーコンポーネント向けのMicrosoft .NET Frameworkバージョン4.8より前のバージョンに対するサポート。Delivery Controller、Studio、Director、StoreFrontが含まれます。	1912	2003	.NET Frameworkバージョン4.8にアップグレードします。
Windowsサーバー 2012 R2 上の VDA。	1912	2003	サポートされているオペレーティングシステムにVDAをインストールします。
Citrix Virtual Apps and Desktops Premium edition の AppDNA® アプリケーション移行コンポーネント。	1909	2003	---
32ビット (x86) マシンへのStudioのインストール。	1909	2003	サポートされているx64オペレーティングシステムにインス

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
			トールしてください。
シームレスアプリケーションにおけるExcelフックのサポート。これは、Microsoft Excel 2010の各ワークブックに対して個別のタスクバーアイコンを作成するために使用されていました。	1909	1909	---
Windows Server 2012 R2 (サービスパックを含む) 上のコアサーバーコンポーネント。含まれるもの: Delivery Controller™、Studio、およびDirector。	1906	2003	より新しいサポート対象のオペレーティングシステムにインストールします。
Microsoft SQL Server バージョン 2008 R2、2012、2014 (すべてのサービスパックとエディションを含む) 上のサイト構成、構成ログ、および監	1906	2003	サポートされているMicrosoft SQL Serverバージョンにデータベースをインストールします。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
視データベースのサポート。			
x86プラットフォーム上のWindows 10でのVDAのサポート。	1906	1909*	サポートされているx64オペレーティングシステムにVDAをインストールします。*この機能は、Citrix Virtual Apps and Desktops 7 1912 LTSRでは引き続きサポートされています。
Citrix Virtual Apps and Desktopsインストールメディアからの Citrix Smart Tools Agentの削除。	1903	1906	---
StoreFront内の以下のサポート終了製品に対するDelivery Controllerオプションの削除: VDI-in-a-Box、および XenMobile (9.0以前)。	1903	1903	---
Red Hat Enterprise Linux/CentOS 7.5でのLinux	1903	1903	Red Hat Enterprise Linuxの新しいバージョンに Linux VDAをイ

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
VDAのサポート。			ンストールします。
Citrix Virtual Apps and Desktops（旧XenAppおよびXenDesktop）とCitrix Receiver、およびWorkspace Hub間のTLS 1.0およびTLS 1.1プロトコルに対するStoreFrontのサポート。	7.17	2203	Citrix ReceiverをTLS 1.2プロトコルをサポートするCitrix Workspaceアプリにアップグレードします。Citrix Workspaceアプリの詳細については、https://docs.citrix.com/ja-jp/citrix-workspace-appを参照してください。
ポリシー設定「インボックスプリンタードライバーの自動インストール」に対するVDAのサポート。	7.16	2311	なし。このポリシー設定は、以前のOS（Windows 7、Windows Server 2012 R2以前）上のVDAでのみサポートされます。
Desktop Applianceサイト上のデスクトップにユーザーがアクセスするためのStoreFrontのサポート	1811	1912	ドメインに参加していないユースケースには、Desktop Lockを使用してください。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
Framehawkディスプレイリモートテクノロジーのサポート	1811	1903	adaptive transportを有効にしてThinwireを使用してください。
すべてのCitrix Virtual Apps and Desktops（およびXenAppおよびXenDesktop）バージョンにおけるCitrix Smart Scaleのサポート。この機能は31 May 2019にサポート終了となります。	1808	1906	電源管理機能の向上のために、Citrix Cloud上のVirtual Apps and Desktops Serviceの使用を検討してください。
Citrix StoreFront、Citrix VDA、Citrix Studio、Citrix Director、およびCitrix Delivery Controllerによる Microsoft .NET Frameworkバージョン4.5.1、4.5.2、4.6、4.6.1、4.6.2、および4.7のサポート。	7.18	1808	.NET Frameworkバージョン4.7.1以降にアップグレードしてください。（インストーラーは、まだインストールされていない場合、.NET Framework 4.7.1を自動的にインストールします。）
Red Hat Enterprise	7.18	1808	Red Hat Enterprise

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
Linux 7.3 上の Linux VDA のサポート。			Linux の新しいバージョンに Linux VDA をインストールします。
SUSE Linux Enterprise Server 11 Service Pack 4 における Linux VDA のサポート。	7.16	7.16	サポートされているSUSEバージョンにLinux VDAをインストールします。
VDA 上の Citrix WDDM ドライバーのサポート	7.16	7.16	Citrix WDDM ドライバーは、VDA とともにインストールされなくなりました。
Windows 10 バージョン 1511 (Threshold 2) およびそれ以前の Windows シングルセッション OS リリース (Windows 8.x および Windows 7 を含む) 上の VDA (<https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-	7.15 LTSR (および 7.12)	7.16	Windows 10の最小バージョン 1607 (Redstone 1) 以降の半期チャネルにシングルセッション OS VDAをインストールします。1607 LTSB を使用している場合は、7.15 VDAを推奨します。CTX224843を参照してください。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
users/> を参照)。			
Windows Server 2008 R2 およびWindows Server 2012 (サービスパックを含む) 上のVDA	7.15 LTSR (および7.12)	7.16	サポートされているオペレーティングシステムにVDAをインストールします。
デスクトップコンポジションリダイレクト (以前はDirectXコマンドリモート処理として知られていた) (DCR)	7.15 LTSR	7.16	Thinwireを使用します。
Citrix Receiver for Webクラシックエクスペリエンス (「緑の吹き出し」ユーザーインターフェイス)	7.15 LTSR (およびStoreFront 3.12)	1903	Citrix Receiver for Web統合エクスペリエンス。
Windows Server 2012およびWindows Server 2008 R2 (サービスパックを含む) 上のコアコンポーネント。含まれるもの: Delivery Controller、Studio、Director、StoreFront、	7.15 LTSR	7.18	サポートされているオペレーティングシステムにコンポーネントをインストールします。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
License Server、Universal Print Server。			
Windows Server 2012およびWindows Server 2008 R2（Service Packを含む）でのセルフサービスパスワードリセット（SSPR）機能	7.15 LTSR	7.18	より新しいサポートされているオペレーティングシステムにインストールします。
Windows 7、Windows 8、およびWindows 8.1（Service Packを含む）でのStudio	7.15 LTSR	7.18	サポートされているオペレーティングシステムにStudioをインストールします。
Flashリダイレクト	7.15 LTSR	1912	ビデオコンテンツをHTML5ビデオとして作成します。管理対象コンテンツにはHTML5ビデオリダイレクトを、公開Webサイトにはブラウザコンテンツリダイレクトを使用します。詳細については、Flashリダイレクトのサポート終了の注記を参

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
			照してください。
StoreFrontとのCitrix Online統合（Goto製品）	7.14 (およびStoreFront 3.11)	StoreFront 3.12	---
VDAインストール中に作成され、VDAマシンのローカル管理者グループに追加されたユーザーアカウントCtxAppVCOMAdminは、作成されなくなりました。基盤となる「COM」メカニズムも削除されました。	7.14	7.14	WindowsサービスCtxAppVServiceは同じ機能を実行します。これは自動的にインストールおよび構成され、ユーザーによる操作は不要です。
Windows Server 2008 32ビット版でのUniversal Print Server UpsServer コンポーネントのサポート	7.14	7.14	より新しいサポート対象のオペレーティングシステムにインストールしてください。
Internet Explorer 8 でのストアフロントおよび ウェブ用Receiver	7.13	7.13	---
Citrix App-Vコンポーネントのインストールを	7.13	7.13	コマンドラインインストールオプション /

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
防止するためのVDAコマンドラインインストールオプション / no_appv			exclude "Citrix Personalization for App-V – VDA" を使用します。
フルプロダクトインストーラーは、新規インストール時にCitrix.Common.Commandsスナップインをインストールしなくなり、既存のインストールをアップグレードする際に自動的に削除します。	7.13	7.13	Citrix.Common.Commandsスナップインによって提供されていた一部のPowerShellコマンドは、XenApp 6.5 SDKで引き続き利用できます。
*-CtxIconコマンドレットによって提供されていた、アイコンデータを操作する部分的な機能。	7.13	7.13	現在はBroker Serviceの*-BrokerIconコマンドレットによって提供されています。
レガシーThinwireモード	7.12	7.16	Thinwireを使用してください。Windows Server 2008 R2でレガシーThinwireモードを使用している場合は、Windows Server 2012 R2またはWindows Server 2016に

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
			移行し、Thinwireを使用してください。
StoreFront 2.0、2.1、2.5、および2.5.2からのインプレースアップグレード	7.13	7.16	これらのバージョンのいずれかから、サポートされている新しいバージョンにアップグレードし、その後XenAppおよびXenDesktop 7.16にアップグレードしてください。
XenDesktop 5.6または5.6 FP1からのインプレースアップグレード	7.12	7.16	XenDesktop 5.6または5.6 FP1の展開を現在のXenDesktopバージョンに移行してください。これを行うには、まずXenDesktop 7.6 LTSR（最新のCUを含む）にアップグレードし、次に最新のCitrix Virtual Desktops（旧XenDesktop）リリースまたはLTSRバージョンにアップグレードしてください。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
32ビット（x86）マシンへのDelivery Controller、Director、StoreFront、またはLicense Serverのインストール。	7.12	7.16	サポートされているx64オペレーティングシステムにインストールしてください。
接続リース	7.12	7.16	ローカルホストキャッシュを使用してください。
Windows XPで使用されていたXenDesktop 5.6。Windows XPへのVDAインストールはサポートされていません。	7.12	7.16	サポートされているオペレーティングシステムにVDAをインストールしてください。
CloudPlatform接続のサポート	7.12	2003	別のサポートされているハイパーバイザーまたはクラウドサービスを使用してください。
Azure Classic（Azure Service Managementとしても知られています）接続のサポート	7.12	2003	Citrix Cloud上のVirtual Apps and Desktopsサービスの使用を検討してください。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
AppDisks機能（およびそれをサポートするStudioへのAppDNA統合）	7.13	2003	Citrix App Layeringを使用してください。
パーソナル vディスク機能	7.15	2006†	Citrix App Layeringユーザーレイヤーまたはユーザーパーソナライゼーションレイヤーテクノロジーを使用してください。

† Citrix Virtual Apps and Desktops 7 2003では、Personal vDiskドライバーはVDAインストーラーから削除されました。Citrix Virtual Apps and Desktops 7 2006では、Personal vDiskドライバーのワークフローはStudioから削除されました。

システム要件

はじめに

このドキュメントのシステム要件は、この製品バージョンがリリースされた時点でのものです。更新は定期的に行われます。ここに記載されていないコンポーネント（ホストシステム、Citrix Workspace™アプリ、Citrix Provisioning™など）のシステム要件は、それぞれのドキュメントに記載されています。

インストールを開始する前に、インストール準備を確認してください。

特に記載がない限り、コンポーネントインストーラーは、必要なバージョンがマシンで検出されない場合、ソフトウェアの前提条件（.NETおよびC++パッケージなど）を自動的に展開します。Citrix®インストールメディアには、これらの前提ソフトウェアの一部も含まれています。

インストールメディアには、いくつかのサードパーティ製コンポーネントが含まれています。Citrixソフトウェアを使用する前に、サードパーティからのセキュリティ更新プログラムを確認し、インストールしてください。

Windows Serverにインストールできるコンポーネントおよび機能の場合、特に記載がない限り、Nano Serverのインストールはサポートされていません。Server Coreは、Delivery ControllerおよびDirectorのみでサポートされています。

ハードウェア要件

RAMとディスク容量の値は、製品イメージ、オペレーティングシステム、およびマシン上のその他のソフトウェアの要件に追加されるものです。パフォーマンスは構成によって異なります。構成には、使用する機能、ユーザー数、およびその他の要因が含まれます。最小要件のみを使用すると、パフォーマンスが低下する可能性があります。

次の表に、コアコンポーネントの最小要件を示します。

コンポーネント	最小
すべてのコアコンポーネントとStoreFront™を1台のサーバーにインストール（評価用のみ、本番環境への展開は不可）	5 GB RAM

コンポーネント	最小
すべてのコアコンポーネントとStoreFrontを1台のサーバーにインストール（テスト展開または小規模な本番環境用）	12 GB RAM
Delivery Controller™ (ローカルホストキャッシュにはより多くのディスク容量が必要です)	5 GB RAM、800 MB ハードディスク
スタジオ	1 GB RAM、100 MB ハードディスク
ディレクター	2 GB RAM、200 MB ハードディスク
StoreFront	2 GB RAM、ディスクの推奨事項については、StoreFront のドキュメントを参照してください
ライセンスサーバー	8 GB RAM。ディスクの推奨事項については、ライセンスのドキュメントを参照してください

デスクトップとアプリケーションを提供するVMのサイジング

ハードウェア製品の複雑で動的な性質、および各展開に固有のニーズがあるため、具体的な推奨事項を提供することはできません。一般的に、Citrix Virtual Apps™ VMのサイジングは、ユーザーのワークロードではなくハードウェアに基づいています。例外はRAMです。より多くのRAMを消費するアプリケーションには、より多くのRAMが必要です。

詳細については、以下を参照してください。

- Citrix Tech Zoneには、サイジングに関するガイダンスが含まれています。
- 「Citrix Virtual Apps and Desktops Single Server Scalability」(/ja-jp/tech-zone/design/design-decisions/single-server-scalability.html)では、単一の物理ホストでサポートできるユーザー数またはVM数について説明しています。

マイクロソフト ビジュアル C++

Delivery Controller、Virtual Delivery Agent (VDA)、またはUniversal Print Serverをインストールすると、CitrixインストーラーはMicrosoft Visual C++ 2015–2022 Redistributableを自動的にインストールします。

- マシンにそのランタイムの以前のバージョン（2015-2019など）が含まれている場合、Citrixインストーラーがそれをアップグレードします。
- マシンに2015年より前のバージョンが含まれている場合、Citrixは新しいバージョンを並行してインストールします。

デリバリーコントローラー

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー コア 2022
- ウィンドウズ サーバー 2022
- Windows Server 2019、StandardおよびDatacenter Edition、およびServer Coreオプション付き
- Windows Server 2016、StandardおよびDatacenterエディション、Server Coreオプション付き

要件:

- Microsoft .NET Framework 4.8（またはそれ以降のバージョン）がまだインストールされていない場合、自動的にインストールされます。
- Windows PowerShell 3.0、4.0、または5.0。
- Microsoft Visual C++ 2015–2019 再頒布可能パッケージ。

データベース

サイト構成、構成ログ、および監視データベースでサポートされているMicrosoft SQL Serverのバージョン：

- SQL Server 2022、Express、Standard、およびEnterprise エディション。
- SQL Server 2019、Express、Standard、およびEnterprise エディション。
- SQL Server 2017、Express、Standard、および Enterprise エディション。
    - 新規インストールの場合：既存のサポートされているSQL Serverインストールが検出されない場合、デフォルトで、Controllerのインストール時に累積更新プログラム16が適用されたSQL Server Express 2017がインストールされます。
    - アップグレードの場合、既存のSQL Server Expressバージョンはアップグレードされません。
- SQL Server 2016 SP2、Express、Standard、および Enterprise エディション。

次のデータベース高可用性ソリューションがサポートされています（SQL Server Expressはスタンドアロンモードのみをサポートするため、これを除く）：

- SQL Server AlwaysOn フェールオーバークラスターインスタンス
- SQL Server AlwaysOn 可用性グループ（基本可用性グループを含む）
- SQL Server データベースミラーリング

コントローラーとSQL Serverサイトデータベース間の接続には、Windows認証が必要です。

ローカルホストキャッシュに関する考慮事項: Microsoft SQL Server Express LocalDBは、ローカルホストキャッシュがスタンドアロンで使用するSQL Server Expressの機能です。ローカルホストキャッシュは、SQL Server Express LocalDB以外のSQL Server Expressのコンポーネントを必要としません。

- Controllerをインストールする際、ローカルホストキャッシュ機能で使用するために、累積更新プログラム15が適用されたMicrosoft SQL Server Express LocalDB 2019がインストールされます。(このインストールは、サイトデータベース用のデフォルトのSQL Server Expressインストールとは別です。)
- コントローラーをアップグレードしても、既存のMicrosoft SQL Server Express LocalDBバージョンは自動的にアップグレードされません。交換要件と手順については、「SQL Server Express LocalDB の交換」を参照してください。

その他のデータベース情報:

- データベース
- CTX114501 には、現在サポートされているデータベースが一覧表示されています。
- データベースのサイジングに関するガイダンス
- ローカルホストキャッシュ

ウェブスタジオ

> **注:**
>
> - Citrix Virtual Apps and Desktops™ の展開は、Web Studio (Web ベース) と Citrix Studio (Windows ベース) の 2 つの管理コンソールを使用して管理できます。この記事では Web Studio のみを取り上げます。Citrix Studio の詳細については、Citrix Virtual Apps and Desktops 7 2212 以前の同等の記事を参照してください。

- Web Studio は、オンプレミスの Citrix Virtual Apps and Desktops 展開を構成および管理できる Web ベースの管理コンソールです。ユーザーエクスペリエンスの向上を目的として設計されており、Windows ベースの管理コンソールである Citrix Studio よりも一般的に応答が高速です。「Web Studio のインストール」を参照してください。

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー Core 2022
- ウィンドウズ サーバー 2022
- Windows Server 2019、Standard および Datacenter エディション、および Server Core オプション
- Windows Server 2016、Standard および Datacenter エディション、および Server Core オプション

シトリックス ディレクター

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー コア 2022
- ウィンドウズ サーバー 2022
- Windows Server 2019、StandardおよびDatacenter Edition、およびServer Coreオプション
- Windows Server 2016、StandardおよびDatacenterエディション、Server Coreオプション付き

要件:

- Microsoft .NET Framework 4.8（またはそれ以降のバージョン）がまだインストールされていない場合、自動的にインストールされます。
- Microsoft Internet Information Services (IIS) 7.0およびASP.NET 2.0。IISサーバーの役割に静的コンテンツの役割サービスがインストールされていることを確認してください。このソフトウェアがまだインストールされていない場合は、Windows Serverのインストールメディアを求められ、そのソフトウェアがインストールされます。
- Citrix Directorがインストールされているマシンでイベントログを表示するには、Microsoft .NET Framework 2.0をインストールする必要があります。

シトリックス プロファイル管理:

- Directorでユーザープロファイルの詳細を表示するには、Citrix Profile ManagementとCitrix Profile Management WMI Plug-inがVDAにインストールされており（インストールウィザードの**追加コンポーネント**ページ）、Citrix Profile Management Serviceが実行されていることを確認してください。

System Center オペレーションズマネージャー (SCOM) 統合の要件:

- System Center 2012 R2 オペレーションズマネージャー

Directorを表示するためのサポートされているブラウザー:

- Internet Explorer 11。Internet Explorer の互換モードはサポートされていません。Director にアクセスするには、推奨されるブラウザ設定を使用してください。Internet Explorer をインストールする際は、推奨されるセキュリティ設定と互換性設定を使用するデフォルトを受け入れてください。すでにブラウザをインストールしていて、推奨設定を使用しないことを選択した場合は、**ツール > インターネットオプション > 詳細設定 > リセット** に移動し、指示に従ってください。
- マイクロソフト エッジ。
- ファイアフォックス ESR (延長サポート版)。
- クローム.

Directorを表示するための推奨される最適な画面解像度は1440 x 1024です。

シングルセッションOS用Virtual Delivery Agent (VDA)

サポートされているオペレーティングシステム:

- ウィンドウズ 11
- Windows 10 (x64のみ)、現在メインストリームサポート中のすべてのバージョン。
  - エディションのサポートについては、Knowledge Center の記事 CTX224843 を参照してください。
  - バージョン 1709 の Citrix 既知の問題については、Knowledge Center の記事 CTX229052 を参照してください。

要件:

- Microsoft .NET Framework 4.8 (またはそれ以降のバージョン) がまだインストールされていない場合、自動的にインストールされます。
- Microsoft Visual C++ 2015–2019 再頒布可能パッケージ。

Remote PC Access は、物理オフィスPCにインストールするこの VDA を使用します。この VDA は、Windows 11 および Windows 10 上の Citrix Virtual Desktops™ Remote PC Access のセキュアブートをサポートしています。

いくつかのマルチメディアアクセラレーション機能（HDX MediaStream Windows Media Redirectionなど）を使用するには、VDAをインストールするマシンにMicrosoft Media Foundationがインストールされている必要があります。マシンにMedia Foundationがインストールされていない場合、マルチメディアアクセラレーション機能はインストールされず、動作しません。Citrixソフトウェアのインストール後にマシンからMedia Foundationを削除しないでください。削除すると、ユーザーはマシンにログオンできなくなります。ほとんどのサポートされているWindowsシングルセッションOSエディションでは、Media Foundationのサポートはすでにインストールされており、削除できません。ただし、Nエディションには特定のメディア関連テクノロジーが含まれていません。そのソフトウェアはMicrosoftまたはサードパーティから入手できます。詳細については、「インストール準備」を参照してください。

Linux VDAの詳細については、「Linux Virtual Delivery Agent」の記事を参照してください。

Server VDI機能を使用するには、コマンドラインインターフェイスを使用して、サポートされているWindows ServerマシンにWindowsシングルセッションOS用VDAをインストールできます。ガイダンスについては、Server VDIを参照してください。

Windows 7マシンへのVDAのインストールについては、以前のオペレーティングシステムを参照してください。

マルチセッションOS用Virtual Delivery Agent (VDA)

サポートされているオペレーティングシステム:

- Windows 11 (Citrix DaaS™でのみサポート)
- Windows 10 (x64のみ、Citrix DaaSでのみサポート)、現在メインストリームサポート中のすべてのバージョン。
- ウィンドウズ サーバー 2022
- Windows Server 2019、StandardおよびDatacenterエディション
- Windows Server 2016、Standard、および Datacenter エディション

インストーラーは以下の要件を自動的に展開します。これらはCitrixインストールメディアの**Support**フォルダーにもあります。

- Microsoft .NET Framework 4.8 がまだインストールされていない場合（またはそれ以降のバージョンがインストールされていない場合）、自動的にインストールされます。

- Microsoft Visual C++ 2015–2019 再頒布可能パッケージ。

リモートデスクトップサービス役割サービスがまだインストールおよび有効化されていない場合、インストーラーは自動的にそれらをインストールして有効化します。

いくつかのマルチメディアアクセラレーション機能（HDX MediaStream Windows Media Redirectionなど）を使用するには、VDAをインストールするマシンにMicrosoft Media Foundationがインストールされている必要があります。マシンにMedia Foundationがインストールされていない場合、マルチメディアアクセラレーション機能はインストールされず、動作しません。Citrixソフトウェアのインストール後にマシンからMedia Foundationを削除しないでください。削除すると、ユーザーはマシンにログオンできなくなります。ほとんどのWindows Serverバージョンでは、Media Foundation機能はサーバーマネージャーを通じてインストールされます。詳しくは、「インストール準備」を参照してください。

VDAにMedia Foundationが存在しない場合、以下のマルチメディア機能は動作しません。

- Windows Media リダイレクト
- HTML5 ビデオ リダイレクト
- HDX™ RealTime ウェブカメラ リダイレクト

Linux VDAについては、「Linux Virtual Delivery Agent」の記事を参照してください。

Windows Server 2008 R2マシンにVDAをインストールする方法については、以前のオペレーティングシステムを参照してください。

ホスト / 仮想化リソース

以下のホスト/仮想化リソース（アルファベット順）がサポートされています。該当する場合、*major.minor*バージョンとそのバージョンへの更新がサポートされます。Knowledge Centerの記事「CTX131239」には、現在のバージョン情報と既知の問題へのリンクが含まれています。

一部の機能は、すべてのホストプラットフォームまたはすべてのプラットフォームバージョンでサポートされていない場合があります。詳細については、機能のドキュメントを参照してください。

Remote PC AccessのWake on LAN機能には、Microsoft System Center Configuration Manager 2012以降が必要です。

サポートされているハイパーバイザー:

- **ゼンサーバー（旧シトリックス ハイパーバイザー™）**

  CTX131239には、現在のバージョン情報と既知の問題へのリンクが含まれています。

詳しくは、「XenServer仮想化環境」を参照してください。

- **マイクロソフト システム センター バーチャル マシン マネージャー**

  サポートされているSystem Center Virtual Machine Managerのバージョンに登録できるHyper-Vのすべてのバージョンが含まれます。

  CTX131239には、現在のバージョン情報と既知の問題へのリンクが含まれています。

  詳しくは、「Microsoft System Center Virtual Machine Manager仮想化環境」を参照してください。

- **Nutanix アクロポリス**

  CTX131239には、現在のバージョン情報と既知の問題へのリンクが含まれています。

  詳しくは、「Nutanix仮想化環境」を参照してください。

- **ヴイエムウェア vスフィア (vセンター + ESXi)**

  vSphere vCenter Linked Mode操作はサポートされていません。

  CTX131239には、現在のバージョン情報と既知の問題へのリンクが含まれています。

  詳しくは、「VMware仮想化環境」を参照してください。

サポートされているパブリッククラウドホスト：

- **アマゾン ウェブサービス (AWS)**

  AWSを使用して仮想マシンをプロビジョニングする方法については、「Amazon Web Services仮想化環境」を参照してください。

- **Google Cloud Platform** 詳しくは、「Google Cloud Platform仮想化環境」および「Google CloudでのCitrix DaaSの概要」を参照してください。

- **Microsoft Azure リソース マネージャー**

  仮想マシンのプロビジョニングにMicrosoft Azure Resource Managerを使用する方法については、「Microsoft Azure Resource Manager仮想化環境」を参照してください。

- **Nutanix クラウドおよびパートナーソリューション**

  Nutanixクラウドおよびパートナーソリューションの使用方法については、「Nutanixクラウドおよびパートナーソリューション」を参照してください。

- **VMware クラウドおよびパートナーソリューション**

VMwareクラウドおよびパートナーソリューションの使用方法については、「VMwareクラウドおよびパートナーソリューション」を参照してください。

展開にパブリッククラウドホスト接続を追加する場合は、次の点を考慮してください。

- ハイブリッド権限ライセンスが必要です。ハイブリッド権限ライセンスについては、「ハイブリッド権限による移行とアップグレード (TTU)」を参照してください。ライセンスの追加については、「サイトの作成」を参照してください。
- 情報源はCitrix DaaSドキュメントを参照するよう案内しています。Citrix DaaS製品のパブリッククラウドホストに精通している場合でも、オンプレミス版にはいくつかの違いがあります。
  - Citrix DaaSでは、管理インターフェイスはFull Configurationとして知られています。オンプレミスのCitrix Virtual Apps and Desktopsでは、管理インターフェイスはWeb Studioとして知られています。
  - Citrix DaaSへの更新は、約4週間ごとに展開されます。そのため、Citrix DaaSで利用可能な特定の機能がオンプレミス版では利用できない場合があります。

Active Directoryの機能レベル

Active Directoryフォレストおよびドメインでサポートされている機能レベルは次のとおりです。

- ウィンドウズ サーバー 2025
- Windows サーバー 2016
- ウィンドウズ サーバー 2012 R2
- Windows サーバー 2012
- Windows サーバー 2008 R2
- ウィンドウズ サーバー 2008

注記：

Citrix Virtual Apps and Desktopsサイトをアップグレードする前に、個々の機能の要件を確認してください。新しい機能やVDAには、特定の最小Active Directory機能レベルが必要となる場合があるためです。

HDX

オーディオ

Multi-Stream ICA® 用のUDPオーディオは、Citrix Workspaceアプリ for WindowsおよびCitrix Workspaceアプリ for Linux 13でサポートされています。

エコーキャンセルは、Citrix Workspaceアプリ for Windowsでサポートされています。

特定のHDX機能のサポートと要件を参照してください。HDX機能とCitrix Workspaceアプリの詳細については、機能マトリックスを参照してください。

HDX Windows Media の配信

Windows Mediaクライアント側コンテンツフェッチ、Windows Mediaリダイレクト、およびリアルタイムWindows Mediaマルチメディアトランスコーディングでは、Citrix Workspaceアプリ for Windows、Citrix Workspaceアプリ for iOS、およびCitrix Workspaceアプリ for Linuxがサポートされています。

Windows 8デバイスでWindows Mediaクライアント側コンテンツフェッチを使用するには、Citrix Multimedia Redirectorをデフォルトプログラムとして設定します。**コントロールパネル > プログラム > 既定のプログラム > 既定のプログラムを設定**で、**Citrix Multimedia Redirector**を選択し、**このプログラムを既定として設定**または**このプログラムの既定を選択**をクリックします。GPUトランスコーディングには、Compute Capability 1.1以降のNVIDIA CUDA対応GPUが必要です。`<https://developer.nvidia.com/cuda/cuda-gpus>`を参照してください。

HDX スリーディー プロ

Windows シングルセッション OS 用 VDA は、実行時に GPU ハードウェアの存在を検出します。

アプリケーションをホストする物理マシンまたは仮想マシンは、GPU パススルーまたは仮想 GPU (vGPU) を使用できます。

- GPU パススルーは以下で利用できます。
  - XenServer®
  - ニュータニックス AHV
  - VMware vSphere および VMware ESX (ここでは仮想ダイレクトグラフィックスアクセラレーション (vDGA) と呼ばれます)
  - Windows Server 2016 の Microsoft Hyper-V (ここではディスクリートデバイス割り当て (DDA) と呼ばれます)。

- vGPU は以下で利用できます。
  - XenServer
  - ニュータニックス AHV
  - ヴイエムウェア ブイスフィア

`<https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/2311/graphics/hdx-3d-pro>` を参照してください。

Citrix は、ホストコンピューターに少なくとも 4 GB の RAM と、2.3 GHz 以上のクロック速度を持つ 4 つの仮想 CPU を搭載することを推奨します。

グラフィック処理ユニット (GPU):

- NVIDIA GRID API を使用した仮想グラフィックスアクセラレーションの場合、NVIDIA Virtual GPU (vGPU) ソフトウェアバージョン 13 以降でサポートされているすべての NVIDIA GRID GPU とともに HDX 3D Pro を使用できます。`<https://docs.nvidia.com/grid/index.html>` を参照してください。 サポートされているハイパーバイザーとハードウェアの詳細なリストについては、NVIDIA vGPU ソフトウェア ドキュメントを参照してください。
- 仮想グラフィックアクセラレーションは、Intel Xeon Processor E3ファミリーのデータセンターグラフィックプラットフォームおよびIntelデータセンターGPU Flexシリーズでサポートされています。詳細については、GPU Flex seriesを参照してください。
- AMD GPUは、AMDのmxGPU仮想化でサポートされています。サポートされているハードウェアの詳細については、AMD documentationを参照してください。

ユーザーデバイス:

- Citrixは、ハードウェアリソースに応じて最大8台の4Kモニターをサポートします。使用するGPUによっては、この最大値に他のハードウェア制限がある場合があります。
- Citrixでは、ユーザーデバイスに少なくとも4GBのRAMと1.6GHz以上のクロック速度を持つCPUを搭載することを推奨しています。最適なパフォーマンスを得るには、ユーザーデバイスに少なくとも8GBのRAMと3GHz以上のクロック速度を持つデュアルコアCPUを搭載することを推奨します。
- マルチモニターアクセスの場合、Citrixはクアッドコアcpuを搭載したユーザーデバイスを推奨します。
- Citrix Workspaceアプリがインストールされている必要があります。

詳細については、HDX 3D Pro articlesおよびwww.citrix.com/xenapp/3dを参照してください。

ユニバーサル プリント サーバー

Universal Print Serverは、クライアントコンポーネントとサーバーコンポーネントで構成されています。UpsClientコンポーネントはVDAインストールに含まれています。ユーザーセッションでCitrix Universal™ Print Driverを使用してプロビジョニングしたい共有プリンターが存在する各プリントサーバーに、UpsServerコンポーネントをインストールします。

UpsServerコンポーネントは以下でサポートされています。

- Windows サーバー 2022
- Windows サーバー 2019
- ウィンドウズ サーバー 2016

要件:

- Microsoft Visual C++ 2015–2019 再頒布可能パッケージ
- マイクロソフト .NET Framework 4.8（最低限）

マルチセッションOS用VDAの場合、印刷操作中のユーザー認証には、Universal Print ServerがVDAと同じドメインに参加している必要があります。

スタンドアロンのクライアントおよびサーバーコンポーネントパッケージもダウンロードできます。

詳しくは、「プリンターのプロビジョニング」を参照してください。

その他

Citrix License Server 11.17.2以降のみがサポートされています。詳しくは、「ライセンス」を参照してください。

このリリースでCitrix Provisioning (旧Provisioning Services) を使用する場合、バージョン7.xはXenAppおよびXenDesktop 7.xのライフサイクルとCitrix Virtual Apps and Desktopsのライフサイクルによってカバーされます。バージョン互換性の詳細については、「製品マトリックス」を参照してください。

サポートされているStoreFrontのバージョンについては、「StoreFrontのシステム要件」を参照してください。

Citrixポリシー情報をサイト構成データベースではなくActive Directoryに保存する場合、Microsoft Group Policy Management Console (GPMC) が必要です。
`CitrixGroupPolicyManagement_x64.msi`を個別にインストールする場合 (たとえば、Citrix

Virtual Apps and Desktopsのコアコンポーネントがインストールされていないマシンにインストールする場合)、そのマシンにはVisual Studio 2015ランタイムがインストールされている必要があります。詳しくは、Microsoftのドキュメントを参照してください。

GPMCを使用してドメインGPOを編集する場合は、Delivery Controllerを含むすべてのマシンで(Windows Server Managerの) グループポリシー管理機能を有効にしてください。

複数のNICがサポートされています。

デフォルトでは、現在のVDAをインストールしても、Windows向けCitrix Workspaceアプリはインストールされません。詳しくは、「Windows向けCitrix Workspaceアプリのドキュメント」を参照してください。

その機能でサポートされているブラウザー情報については、「ローカルアプリアクセス」を参照してください。

このバージョンのCitrix Virtual Apps and Desktopsには、最低でもHDX RealTime Connector 2.9 LTSRが必要です。詳しくは、「HDX RealTime Optimization Packのドキュメント」を参照してください。

この製品は PowerShell バージョン 3 から 5 までをサポートしています。

技術概要

Citrix Virtual Apps and Desktops™ は、IT部門が仮想マシン、アプリケーション、ライセンス、セキュリティを制御できるようにしつつ、あらゆるデバイスからどこからでもアクセスできるようにする仮想化ソリューションです。

Citrix Virtual Apps and Desktops は、以下を可能にします:

- エンドユーザーが、デバイスのオペレーティングシステムやインターフェイスに依存せずにアプリケーションとデスクトップを実行すること。
- 管理者が、ネットワークを管理し、選択されたデバイスから、またはすべてのデバイスからアクセスを制御すること。
- 管理者が、単一のデータセンターからネットワーク全体を管理すること。

Citrix Virtual Apps and Desktops は、FlexCast Management Architecture (FMA) と呼ばれる統合アーキテクチャを共有しています。FMAの主な機能は、単一のサイトから複数のバージョンのCitrix Virtual AppsまたはCitrix Virtual Desktops™を実行できること、および統合されたプロビジョニングです。

主要コンポーネント

この記事は、Citrix Virtual Apps and Desktops を初めて使用する方に最も役立ちます。現在、6.x以前のXenAppファーム、またはXenDesktop 5.6以前のサイトをお持ちの場合は、7.xでの変更点 も参照してください。

この図は、一般的な展開（サイトと呼ばれます）における主要コンポーネントを示しています。

一般的な展開における主要コンポーネント(/en-us/citrix-virtual-apps-desktops/2311/media/components-new-op.png)

デリバリーコントローラー™

Delivery Controller は、サイトの中心的な管理コンポーネントです。各サイトには1つ以上のDelivery Controllerがあります。これはデータセンター内の少なくとも1つのサーバーにインストールされます。サイトの信頼性と可用性を確保するために、複数のサーバーにControllerをインス

トールしてください。展開にハイパーバイザーまたはその他のサービスが含まれている場合、Controllerサービスはそれと通信して以下を行います:

- アプリケーションとデスクトップを配布する
- ユーザーアクセスを認証および管理する
- ユーザーとデスクトップおよびアプリケーション間の接続を仲介する
- ユーザー接続を最適化する
- 接続の負荷を分散する

Controller の Broker Service は、どのユーザーがどこにログオンしているか、ユーザーがどのようなセッションリソースを持っているか、既存のアプリケーションに再接続する必要があるかどうかを追跡します。Broker Service は PowerShell コマンドレットを実行し、TCP ポート 80 を介して VDA 上のブローカーエージェントと通信します。TCP ポート 443 を使用するオプションはありません。

Monitor Service は履歴データを収集し、監視データベースに格納します。このサービスは TCP ポート 80 または 443 を使用します。

Controller サービスからのデータは、サイトデータベースに保存されます。

Controller は、需要と管理構成に基づいてデスクトップの状態を管理し、起動および停止します。

データベース

各サイトには、構成情報とセッション情報を保存するために、少なくとも1つの Microsoft SQL Server データベースが必要です。このデータベースには、Controller を構成するサービスによって収集および管理されるデータが保存されます。データベースはデータセンター内にインストールし、Controller への永続的な接続があることを確認してください。

サイトは構成ログデータベースと監視データベースも使用します。デフォルトでは、これらのデータベースはサイトデータベースと同じ場所にインストールされますが、これを変更できます。

仮想デリバリーエージェント (VDA)

VDA は、ユーザーが利用できるようにするサイト内の各物理マシンまたは仮想マシンにインストールされます。これらのマシンはアプリケーションまたはデスクトップを提供します。VDA は、マシンが Controller に登録できるようにし、それによってマシンとそれがホストするリソースをユーザーが利用できるようにします。VDA は、マシンとユーザーデバイス間の接続を確立および管理します。VDA はまた、ユーザーまたはセッションに Citrix® ライセンスが利用可能であることを確認し、セッション用に構成されたポリシーを適用します。

VDA は、VDA 内のブローカーエージェントを介して、Controller 内の Broker Service にセッション情報を通信します。ブローカーエージェントは複数のプラグインをホストし、リアルタイムデータを収集します。TCP ポート 80 を介して Controller と通信します。

「VDA」という言葉は、エージェントとそれがインストールされているマシンを指すためによく使われます。

VDA は、シングルセッションおよびマルチセッションの Windows オペレーティングシステムで利用できます。マルチセッション Windows オペレーティングシステム用の VDA は、複数のユーザーが同時にサーバーに接続できるようにします。シングルセッション Windows オペレーティングシステム用の VDA は、一度に1人のユーザーのみがデスクトップに接続できるようにします。(/ja-jp/linux-virtual-delivery-agent/current-release.html) Linux VDA も利用可能です。

シトリックス ストアフロント™

StoreFrontは、ユーザーを認証し、ユーザーがアクセスするデスクトップとアプリケーションのストアを管理します。これは、エンタープライズアプリケーションストアをホストでき、ユーザーが利用できるデスクトップやアプリケーションへのセルフサービスアクセスを提供します。また、ユーザーのアプリケーションサブスクリプション、ショートカット名、その他のデータを追跡します。これにより、ユーザーは複数のデバイスで一貫したエクスペリエンスを得ることができます。

Citrix Workspace™ アプリ

ユーザーデバイスやその他のエンドポイント（仮想デスクトップなど）にインストールされたCitrix Workspaceアプリは、ドキュメント、アプリケーション、デスクトップへの迅速で安全なセルフサービスアクセスをユーザーに提供します。Citrix Workspaceアプリは、Windows、Web、およびSoftware as a Service (SaaS) アプリケーションへのオンデマンドアクセスを提供します。デバイス固有のCitrix Workspaceアプリソフトウェアをインストールできないデバイスの場合、Citrix Workspaceアプリ for HTML5は、HTML5互換のWebブラウザを介した接続を提供します。

スタジオ

Citrix Virtual Apps and Desktopsの展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この製品ドキュメントでは、Web Studioのみを扱います。Citrix Studioの詳細については、「Citrix Virtual Apps and Desktops 7 2212以前」を参照してください。

ウェブスタジオ

Web Studioは、オンプレミスのCitrix Virtual Apps and Desktops展開を構成および管理できるWebベースの管理コンソールです。ユーザーエクスペリエンスの向上を目的として設計されており、Windowsベースの管理コンソールであるCitrix Studioよりも一般的に応答が高速です。「Web Studioのインストール」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-core/install-web-studio.html)を参照してください。

シトリックス スタジオ

Citrix Studioは、Citrix Virtual Apps and Desktopsの展開を構成および管理する管理コンソールです。Citrix Studioは、アプリケーションとデスクトップの配信を管理するための個別の管理コンソールを不要にします。Citrix Studioには、環境設定、アプリケーションとデスクトップをホストするワークロードの作成、およびユーザーへのアプリケーションとデスクトップの割り当てをガイドするウィザードが用意されています。また、Studioを使用して、サイトのCitrixライセンスを割り当てて追跡することもできます。

Citrix Studioは、Controller内のBroker Serviceから表示する情報を取得し、TCPポート80を介して通信します。

Citrix Director (シトリックス ディレクター)

Directorは、ITサポートチームとヘルプデスクチームが環境を監視し、システムに重大な影響を与える前に問題をトラブルシューティングし、エンドユーザーのサポートタスクを実行できるようにするWebベースのツールです。1つのDirector展開を使用して、複数のCitrix Virtual AppsまたはCitrix Virtual Desktopsサイトに接続して監視できます。

Directorには以下が表示されます。

- コントローラー内のブローカーサービスからのリアルタイムセッションデータ。これには、ブローカーサービスがVDA内のブローカーエージェントから取得するデータが含まれます。
- コントローラー内のモニターサービスからの履歴サイトデータ。

Director は、Citrix Gateway デバイスによって取得された ICA® のパフォーマンスデータとヒューリスティックデータを使用して、データから分析を構築し、それを管理者に提示します。

Windowsリモートアシスタンスを使用して、Directorを介してユーザーのセッションを表示および操作することもできます。

Citrix ライセンスサーバー

ライセンスサーバーは、Citrix製品ライセンスを管理します。コントローラーと通信して各ユーザーセッションのライセンスを管理し、Studioと通信してライセンスファイルを割り当てます。サイトには、ライセンスファイルを保存および管理するために少なくとも1つのライセンスサーバーが必要です。

ハイパーバイザーまたはその他のサービス

ハイパーバイザーまたはその他のサービスは、サイト内の仮想マシンをホストします。これらは、アプリケーションとデスクトップをホストするために使用するVM、および Citrix Virtual Apps and Desktops コンポーネントをホストするために使用するVMです。ハイパーバイザーは、ハイパーバイザーの実行と仮想マシンのホストに完全に特化したホストコンピューターにインストールされます。

Citrix Virtual Apps and Desktops は、さまざまなハイパーバイザーやその他のサービスをサポートしています。

多くの展開でハイパーバイザーが必要ですが、リモート PC アクセスを提供するためにハイパーバイザーは必要ありません。また、Provisioning Services (PVS) を使用して VM をプロビジョニングする場合も、ハイパーバイザーは必要ありません。

追加コンポーネント

以下のコンポーネントも、Citrix Virtual Apps and Desktops の展開に含めることができます。詳細については、各ドキュメントを参照してください。

シトリックス プロビジョニング™

Citrix Provisioning (旧 Provisioning Services) は、一部のエディションで利用可能なオプションコンポーネントです。仮想マシンのプロビジョニングにおいて、MCS の代替手段を提供します。MCS がマスターイメージのコピーを作成するのに対し、PVS はマスターイメージをユーザーデバイスにストリーミングします。PVS はこれを行うためにハイパーバイザーを必要としないため、物理マシンをホストするために使用できます。PVS は Controller と通信して、ユーザーにリソースを提供します。

Citrix ゲートウェイ

ユーザーが企業ファイアウォールの外部から接続する場合、Citrix Virtual Apps and Desktops は Citrix Gateway (旧 Access Gateway および NetScaler® Gateway) テクノロジーを使用して、TLS でこれらの接続を保護できます。Citrix Gateway または VPX 仮想アプライアンスは、非武装地帯

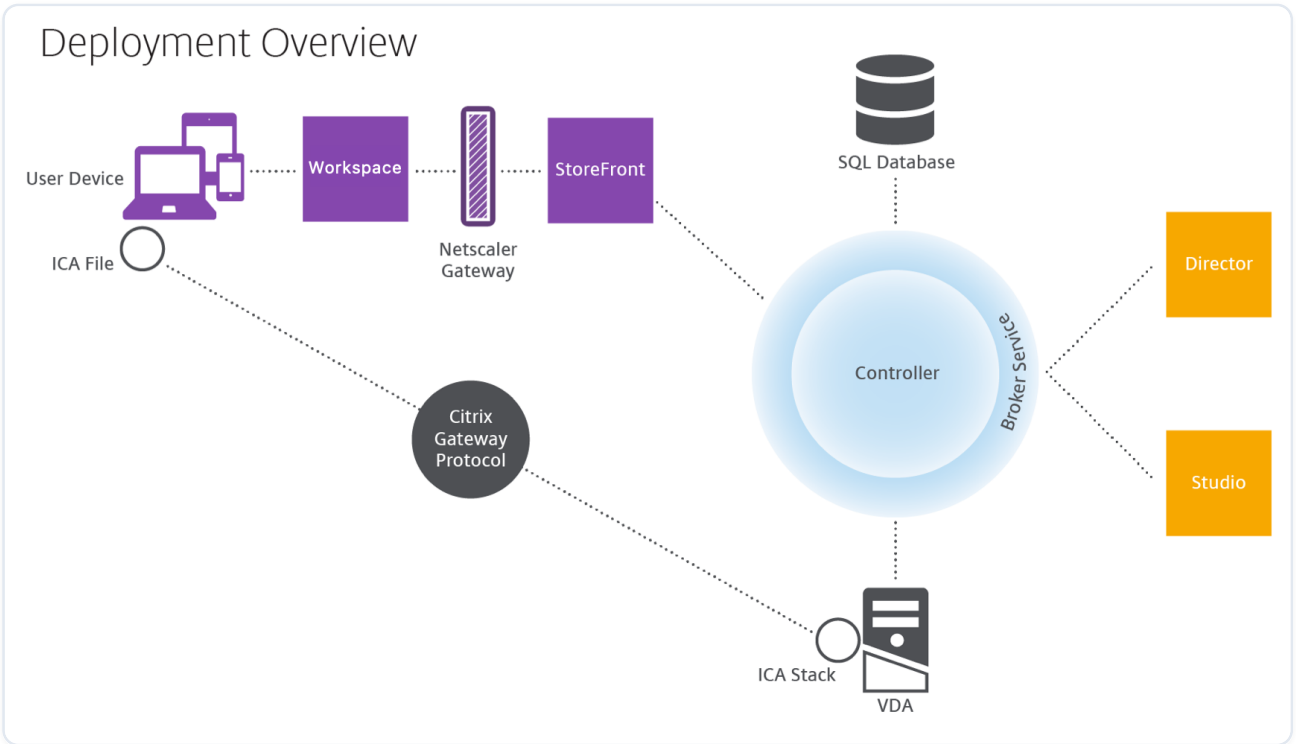
(DMZ) に展開される SSL VPN アプライアンスです。これは、企業ファイアウォールを介した単一の安全なアクセスポイントを提供します。

シトリックス SD-WAN™

仮想デスクトップが支店などのリモートロケーションのユーザーに配信される展開では、Citrix SD-WANテクノロジーを使用してパフォーマンスを最適化できます。リピーターはWAN全体のパフォーマンスを高速化します。ネットワークにリピーターがある場合、支店のユーザーはWAN経由でLANのようなパフォーマンスを体験できます。Citrix SD-WANはユーザーエクスペリエンスのさまざまな部分に優先順位を付けることができるため、たとえば、ネットワーク経由で大きなファイルや印刷ジョブが送信されたときに、支店でのユーザーエクスペリエンスが低下することはありません。HDX™ WAN最適化は、トークン化された圧縮とデータ重複排除を提供し、帯域幅要件を劇的に削減し、パフォーマンスを向上させます。

典型的な展開の仕組み

サイトは、スケーラビリティ、高可用性、フェールオーバーを可能にし、設計上安全なソリューションを提供する専用の役割を持つマシンで構成されます。サイトは、VDA がインストールされたサーバーとデスクトップマシン、およびアクセスを管理する Delivery Controller で構成されます。



VDAを使用すると、ユーザーはデスクトップやアプリケーションに接続できます。ほとんどの配信方法ではデータセンターの仮想マシンにインストールされますが、リモートPCアクセス用に物理PCにインストールすることもできます。

Controller は、リソース、アプリケーション、デスクトップを管理し、ユーザー接続を最適化およびバランス調整する独立した Windows サービスで構成されています。各サイトには 1 つ以上の Controller があります。セッションは遅延、帯域幅、ネットワークの信頼性の影響を受けるため、可能であればすべての Controller を同じ LAN 上に配置してください。

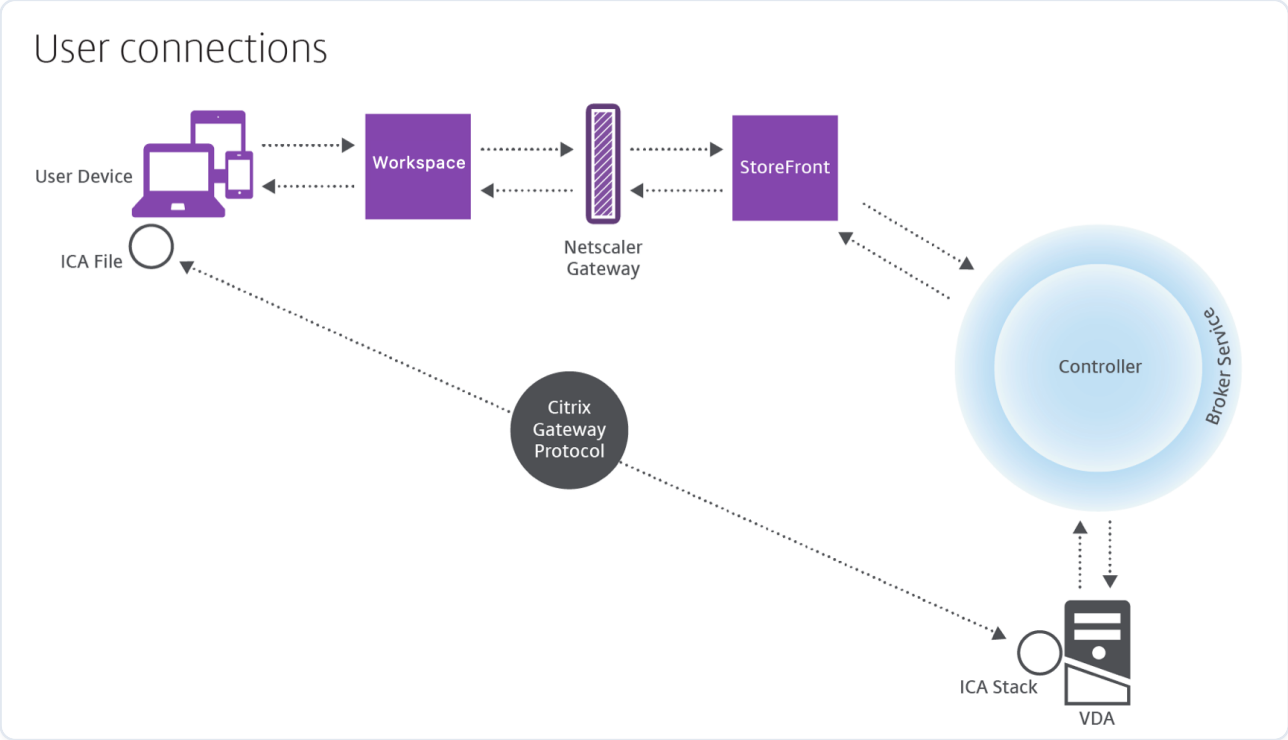
ユーザーがControllerに直接アクセスすることはありません。VDAはユーザーとController間の仲介役として機能します。ユーザーがStoreFrontを使用してログオンすると、資格情報はController上のBroker Serviceに渡されます。その後、Broker Serviceは、設定されたポリシーに基づいてプロファイルと利用可能なリソースを取得します。

ユーザー接続の処理方法

セッションを開始するには、ユーザーは自分のデバイスにインストールされているCitrix Workspaceアプリ、またはStoreFront Webサイトのいずれかを介して接続します。

ユーザーは、必要な物理または仮想デスクトップ、あるいは仮想アプリケーションを選択します。

ユーザーの資格情報は、この経路を介してControllerにアクセスし、ControllerはBroker Serviceと通信して必要なリソースを決定します。Citrixは、Citrix Workspaceアプリから送信される資格情報を暗号化するために、管理者がStoreFrontにSSL証明書を配置することを推奨します。



Broker Serviceは、ユーザーがアクセスを許可されているデスクトップとアプリケーションを決定します。

資格情報が検証されると、利用可能なアプリケーションまたはデスクトップに関する情報が、StoreFront-Citrix Workspaceアプリの経路を介してユーザーに返送されます。ユーザーがこのリストからアプリケーションまたはデスクトップを選択すると、その情報は経路を介してControllerに戻されます。その後、Controllerは特定のアプリケーションまたはデスクトップをホストする適切なVDAを決定します。

コントローラーは、ユーザーの資格情報を含むメッセージをVDAに送信し、その後、ユーザーと接続に関するすべてのデータをVDAに送信します。VDAは接続を受け入れ、同じ経路を通じてCitrix Workspaceアプリに情報を送り返します。必要なパラメーターのセットはStoreFrontで収集されます。これらのパラメーターは、Citrix WorkspaceアプリとStoreFrontのプロトコル会話の一部として、または独立コンピューティングアーキテクチャ (ICA) ファイルに変換されてダウンロードされるかのいずれかの方法で、Citrix Workspaceアプリに送信されます。サイトが適切に設定されていれば、このプロセス全体を通じて資格情報は暗号化されたままになります。

ICAファイルはユーザーのデバイスにコピーされ、デバイスとVDA上で実行されているICAスタックとの間に直接接続を確立します。この接続は、管理インフラストラクチャ（Citrix Workspaceアプリ、StoreFront、およびコントローラー）をバイパスします。

Citrix WorkspaceアプリとVDA間の接続には、Citrix Gatewayプロトコル (CGP) が使用されます。接続が失われた場合、セッションの信頼性機能により、ユーザーは管理インフラストラクチャを介して再起動することなく、VDAに再接続できます。セッションの信頼性は、Citrixポリシーで有効または無効にできます。

クライアントがVDAに接続した後、VDAはユーザーがログオンしたことをコントローラーに通知します。その後、コントローラーはこの情報をサイトデータベースに送信し、監視データベースへのデータログを開始します。

データアクセスが機能する仕組み

すべてのCitrix Virtual Apps and Desktopsセッションは、IT部門がStudioまたはDirectorを介してアクセスできるデータを生成します。Studioを使用すると、管理者はBroker Agentからリアルタイムデータにアクセスしてサイトを管理します。Directorは、同じデータに加えて、監視データベースに保存されている履歴データにもアクセスします。また、ヘルプデスクのサポートとトラブルシューティングのために、NetScaler GatewayからHDXデータにもアクセスします。

展開におけるデータアクセス(/en-us/citrix-virtual-apps-desktops/2311/media/data-access.png)

コントローラー内では、Broker Serviceがリアルタイムデータを提供するマシンのすべてのセッションのセッションデータを報告します。Monitor Serviceもリアルタイムデータを追跡し、それを履歴データとして監視データベースに保存します。

StudioはBroker Serviceとのみ通信します。リアルタイムデータのみにアクセスします。DirectorはBroker Service（Broker Agent内のプラグインを介して）と通信し、サイトデータベースにアクセスします。

DirectorはCitrix Gatewayにもアクセスして、HDXデータに関する情報を取得できます。

デスクトップとアプリケーションの配信

アプリケーションとデスクトップを配信するマシンは、マシンカタログを使用して設定します。次に、利用可能にするアプリケーションとデスクトップ（カタログ内のマシンを使用）と、それらにアクセスできるユーザーを指定するデリバリーグループを作成します。オプションで、その後アプリケーショングループを作成して、アプリケーションのコレクションを管理できます。

マシンカタログ

マシンカタログは、単一のエンティティとして管理する仮想マシンまたは物理マシンのコレクションです。これらのマシンと、それらに含まれるアプリケーションまたは仮想デスクトップは、ユーザーに提供するリソースです。カタログ内のすべてのマシンには、同じオペレーティングシステムとVDAがインストールされています。また、同じアプリケーションまたは仮想デスクトップも含まれています。

通常、マスターイメージを作成し、それを使用してカタログ内に同一のVMを作成します。VMの場合、そのカタログ内のマシンのプロビジョニング方法として、Citrixツール（Citrix ProvisioningまたはMCS）またはその他のツールを指定できます。あるいは、既存の独自のイメージを使用することもできます。その場合、ターゲットデバイスは個別に管理するか、サードパーティの電子ソフトウェア配布 (ESD) ツールを使用して一括で管理する必要があります。

有効なマシンタイプは次のとおりです。

- **マルチセッションOS:** マルチセッションオペレーティングシステムを搭載した仮想マシンまたは物理マシン。Citrix Virtual Apps公開アプリ（サーバーベースのホスト型アプリケーションとも呼ばれる）およびCitrix Virtual Apps公開デスクトップ（サーバーホスト型デスクトップとも呼ばれる）の配信に使用されます。これらのマシンには、一度に複数のユーザーが接続できます。
- **シングルセッションOS:** シングルセッションオペレーティングシステムを搭載した仮想マシンまたは物理マシン。VDIデスクトップ（オプションでパーソナライズ可能なシングルセッションOSを実行するデスクトップ）、VMホスト型アプリ（シングルセッションOSからのアプリケーション）、およびホスト型物理デスクトップの配信に使用されます。これらのデスクトップには、一度に1人のユーザーのみが接続できます。

- **Remote PC Access:** リモートユーザーがCitrix Workspaceアプリを実行している任意のデバイスから物理的なオフィスPCにアクセスできるようにします。オフィスPCはCitrix Virtual Desktops展開を通じて管理され、ユーザーデバイスを許可リストで指定する必要があります。

詳しくは、「Citrix Virtual Apps and Desktopsイメージ管理」および「マシンカタログの作成」を参照してください。

デリバリーグループ

デリバリーグループは、どのユーザーがどのアプリケーション、デスクトップ、またはその両方にどのマシンでアクセスできるかを指定します。デリバリーグループには、マシンカタログのマシンと、サイトにアクセスできるActive Directoryユーザーが含まれます。Active Directoryグループとデリバリーグループは、同様の要件を持つユーザーをグループ化する方法であるため、Active Directoryグループによってユーザーをデリバリーグループに割り当てることができます。

各デリバリーグループには複数のカタログのマシンを含めることができ、各カタログは複数のデリバリーグループにマシンを提供できます。ただし、個々のマシンは一度に1つのデリバリーグループにのみ属することができます。

デリバリーグループ内のユーザーがアクセスできるリソースを定義します。たとえば、異なるアプリケーションを異なるユーザーに配信するには、すべてのアプリケーションを1つのカタログのマスターイメージにインストールし、そのカタログに十分な数のマシンを作成して、複数のデリバリーグループに分散させることができます。その後、各デリバリーグループを構成して、マシンにインストールされているアプリケーションの異なるサブセットを配信できます。

詳しくは、「デリバリーグループの作成」を参照してください。

アプリケーショングループ

アプリケーショングループは、より多くのデリバリーグループを使用するよりも、アプリケーション管理とリソース制御の利点を提供します。タグ制限機能を使用すると、既存のマシンを複数の公開タスクに利用できるため、展開とより多くのマシンの管理にかかるコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。アプリケーショングループは、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングする場合にも役立ちます。

詳しくは、「アプリケーショングループの作成」を参照してください。

詳細情報

- シトリックス バーチャル アプリケーションズ アンド デスクトップス の図

- ネットワークポート
- データベース
- サポートされているハイパーバイザーおよびその他のサービス

データベース

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

Citrix Virtual AppsまたはCitrix Virtual Desktops™サイトでは、次の3つのSQL Serverデータベースを使用します。

- **サイト：** （サイト構成とも呼ばれる）実行中のサイト構成、現在のセッション状態、および接続情報を保存します。
- **ログ：** （構成ログとも呼ばれる）サイト構成の変更と管理アクティビティに関する情報を保存します。このデータベースは、構成ログ機能が有効になっている場合（デフォルト = 有効）に使用されます。
- **監視：** Directorが使用するデータ（セッション情報や接続情報など）を保存します。

各Delivery Controllerはサイトデータベースと通信します。Controllerとデータベース間ではWindows認証が必要です。Controllerは、サイト内の他のControllerに影響を与えることなく、プラグを抜いたり電源を切ったりできます。ただし、これはサイトデータベースが単一障害点となることを意味します。データベースサーバーが故障した場合、既存の接続はユーザーがログオフまたは切断するまで機能し続けます。サイトデータベースが利用できなくなった場合の接続動作については、「ローカルホストキャッシュ」を参照してください。

Citrixは、データベースに関して以下を推奨します。

- **定期的にバックアップする。** データベースサーバーが故障した場合にバックアップから復元できるように、データベースを定期的にバックアップしてください。各データベースのバックアップ戦略は異なる場合があります。詳細については、CTX135207を参照してください。ただし、これは現在サポートされておらず、お客様が利用できないCitrixXenDesktopDBを参照していることに注意してください。

- **サイト、監視、およびログのSQL Serverデータベースを定期的にバックアップおよび復元する。** SQL Serverデータベースに関する具体的な情報については、「SQL Serverデータベースの完全バックアップと差分バックアップの作成」を参照してください。

サイトに複数のゾーンが含まれている場合は、プライマリゾーンに常にサイトデータベースが含まれていることを確認してください。すべてのゾーンのControllerがそのデータベースと通信します。

高可用性

自動フェールオーバーを確実にするために考慮すべき高可用性ソリューションがいくつかあります。

- **AlwaysOn可用性グループ（基本可用性グループを含む）：** SQL Server 2012で導入されたこのエンタープライズレベルの高可用性および災害復旧ソリューションにより、1つ以上のデータベースの可用性を最大化できます。AlwaysOn可用性グループでは、SQL ServerインスタンスがWindows Server Failover Clustering（WSFC）ノードに存在する必要があります。詳細については、「SQL ServerでのWindows Serverフェールオーバークラスタリング」を参照してください。
- **SQL Server データベースミラーリング:** データベースをミラーリングすると、アクティブなデータベースサーバーが失われた場合でも、自動フェールオーバープロセスが数秒で発生するため、ユーザーは通常影響を受けません。この方法は、各データベースサーバーで完全なSQL Serverライセンスが必要となるため、他のソリューションよりも高価です。ミラーリング環境ではSQL Server Expressエディションを使用できません。
- **SQLクラスタリング:** Microsoft SQLクラスタリングテクノロジーを使用すると、障害が発生した別のサーバーのタスクと責任を1つのサーバーが自動的に引き継ぐことができます。ただし、このソリューションのセットアップはより複雑であり、自動フェールオーバープロセスは通常、SQLミラーリングなどの代替手段よりも遅くなります。
- **ハイパーバイザーの高可用性機能を使用する:** この方法では、データベースを仮想マシンとして展開し、ハイパーバイザーの高可用性機能を使用します。このソリューションは、既存のハイパーバイザーソフトウェアを使用し、SQL Server Expressエディションも使用できるため、ミラーリングよりも安価です。ただし、データベース用に新しいマシンが起動するのに時間がかかる場合があり、ユーザーへのサービスが中断される可能性があるため、自動フェールオーバープロセスは遅くなります。

ローカルホストキャッシュ機能は、SQL Serverの高可用性ベストプラクティスを補完します。ローカルホストキャッシュを使用すると、サイトデータベースが利用できない場合でも、ユー

ザーはアプリケーションやデスクトップに接続および再接続できます。詳細については、「ローカルホストキャッシュ」を参照してください。

サイト内のすべてのControllerが失敗した場合、VDAを高可用性モードで動作するように構成できます。これにより、ユーザーはデスクトップやアプリケーションへのアクセスを継続できます。高可用性モードでは、VDAはControllerによって仲介される接続ではなく、ユーザーからの直接ICA接続を受け入れます。この機能は、すべてのControllerとの通信が失敗するまれな場合にのみ使用してください。この機能は、他の高可用性ソリューションの代替ではありません。詳細については、「CTX 127564」を参照してください。

SQLクラスタリングまたはSQLミラーリングのインストールで、ノードにControllerをインストールすることはサポートされていません。

データベースソフトウェアのインストール

デフォルトでは、そのサーバーで別のSQL Serverインスタンスが検出されない場合、最初のDelivery Controller™をインストールするときにSQL Server Expressエディションがインストールされます。このデフォルトのアクションは、概念実証またはパイロット展開には通常十分です。ただし、SQL Server ExpressはMicrosoftの高可用性機能をサポートしていません。

デフォルトのインストールでは、デフォルトのWindowsサービスアカウントと権限が使用されます。これらのデフォルトの詳細（sysadminロールへのWindowsサービスアカウントの追加を含む）については、Microsoftのドキュメントを参照してください。この構成では、Controllerはネットワークサービスアカウントを使用します。Controllerには、追加のSQL Serverロールや権限は必要ありません。

必要に応じて、データベースインスタンスの**インスタンスを非表示**を選択できます。Web Studioでデータベースのアドレスを構成するときは、インスタンス名ではなく、インスタンスの静的ポート番号を入力してください。SQL Serverデータベースエンジンのインスタンスを非表示にする方法の詳細については、Microsoftのドキュメントを参照してください。

ほとんどの運用環境の展開、およびMicrosoftの高可用性機能を使用するすべての展開では、サポートされているSQL Serverの非Expressエディションのみを使用することをお勧めします。SQL Serverは、最初のControllerがインストールされているサーバー以外のマシンにインストールしてください。システム要件に、サポートされているSQL Serverのバージョンが記載されています。データベースは1台以上のマシンに配置できます。

サイトを作成する前に、SQL Serverソフトウェアがインストールされていることを確認してください。データベースを作成する必要はありませんが、作成する場合は空である必要があります。Microsoftの高可用性テクノロジーの構成も推奨されます。

Windows Updateを使用してSQL Serverを最新の状態に保ちます。

サイト作成ウィザードからデータベースをセットアップする

サイト作成ウィザードの**データベース**ページで、データベース名とアドレス（場所）を指定します。（データベースアドレス形式を参照）。DirectorがMonitor Serviceを照会する際の潜在的なエラーを避けるため、監視データベースの名前に空白を使用しないでください。

「**データベース**」ページでは、データベースを設定するための2つのオプション（自動設定とスクリプトの使用）が提供されます。通常、必要なデータベース権限（Web Studioユーザーおよび Citrix管理者）がある場合は、自動オプションを使用できます。（「データベース設定に必要な権限」を参照してください。）

サイト作成後、構成ログおよび監視データベースの場所を後で変更できます。「データベースの場所の変更」を参照してください。

サイトをミラーデータベースを使用するように構成するには、以下を完了してから、自動またはスクリプトによるセットアップ手順に進みます。

1. SQL Server ソフトウェアを2台のサーバー (AとB) にインストールします。
2. サーバーAで、プリンシパルとして使用するデータベースを作成します。サーバーAのデータベースをバックアップし、サーバーBにコピーします。
3. サーバーBで、バックアップファイルを復元します。
4. サーバーAでミラーリングを開始します。

サイト作成後にミラーリングを確認するには、PowerShellコマンドレット`get-configdbconnection`を実行して、接続文字列にフェールオーバーパートナーがミラーに設定されていることを確認します。

後でミラーデータベース環境でDelivery Controllerを追加、移動、または削除する場合は、「Delivery Controller」を参照してください。

自動セットアップ

必要なデータベース権限がある場合は、サイト作成ウィザードの**データベース**ページで、**Studioからデータベースを作成およびセットアップ**を選択します。その後、プライマリデータベースの名前とアドレスを指定します。

指定したアドレスにデータベースが存在する場合、それは空である必要があります。指定したアドレスにデータベースが存在しない場合、データベースが見つからないことが通知され、データ

ベースを作成するかどうかを尋ねられます。その操作を確定すると、Web Studioは自動的にデータベースを作成し、プライマリおよびレプリカデータベースの初期化スクリプトを適用します。

スクリプトによるセットアップ

必要なデータベース権限がない場合は、データベース管理者など、権限を持つ人に支援を依頼してください。手順は次のとおりです。

1. サイト作成ウィザードの**データベース**ページで、**手動でセットアップするためのスクリプトを生成**を選択します。この操作により、サイト、監視、ログデータベースという、以下のプライマリおよびレプリカデータベースのそれぞれについて、次の3種類のスクリプトが生成されます。

   - *「SysAdmin」という名前を含むスクリプト*。データベースとDelivery Controllerのログインを作成するスクリプトです。これらのタスクにはsecurityadmin権限が必要です。
   - *「DbOwner」という名前を含むスクリプト*。データベースにユーザーロールを作成し、ログインを追加し、データベーススキーマを作成するスクリプトです。これらのタスクには`db_owner`権限が必要です。
   - *「Mixed」という名前を含むスクリプト*。必要な権限に関係なく、すべてのタスクを1つのスクリプトにまとめたものです。

   スクリプトの保存場所を指定できます。

   > **注:**
   >
   > エンタープライズ環境では、データベースのセットアップには、異なる役割（権限）を持つ異なるチームによって処理される可能性のあるスクリプトが含まれます。`securityadmin`または`db_owner`。該当する場合、まず`securityadmin`ロールを持つ管理者によって「SysAdmin」スクリプトが実行され、次に`db_owner`権限を持つ管理者によって「DbOwner」スクリプトが実行されます。これらのスクリプトを生成するには、PowerShellを使用することもできます。詳細については、「Preferred database rights scripts」を参照してください。

2. これらのスクリプトをデータベース管理者に渡します。この時点でサイト作成ウィザードは自動的に停止します。後で戻ってサイト作成を続行する際に、プロンプトが表示されます。

データベース管理者は、データベースを作成します。各データベースは、次の特性を持つ必要があります。

- `_CI_AS_KS`で終わる照合順序を使用します。`_100_CI_AS_KS`で終わる照合順序を使用することをお勧めします。
- 最適なパフォーマンスを得るには、SQL ServerのRead-Committed Snapshotを有効にします。詳細については、「CTX 137161」を参照してください。
- 該当する場合、高可用性機能が構成されていること。
- ミラーリングを構成するには、まずデータベースを完全復旧モデルを使用するように設定します（シンプルモデルがデフォルトです）。プリンシパルデータベースをファイルにバックアップし、ミラーサーバーにコピーします。次に、ミラーサーバーでバックアップファイルを復元します。最後に、プリンシパルサーバーでミラーリングを開始します。

データベース管理者は、SQLCMD コマンドラインユーティリティまたは SQLCMD モードの SQL Server Management Studio を使用して、次の操作を実行します。

- 高可用性SQL Serverデータベースインスタンス（高可用性が構成されている場合）で、`xxx_Replica.sql`スクリプトをそれぞれ実行します。
- プリンシパルSQL Serverデータベースインスタンスで、`xxx\_Principal.sql`スクリプトをそれぞれ実行します。

SQLCMD の詳細については、Microsoft のドキュメントを参照してください。

すべてのスクリプトが正常に完了すると、データベース管理者は Citrix 管理者に3つの主要なデータベースアドレスを提供します。

Web Studio はサイト作成の続行を促します。**データベース**ページに戻ります。アドレスを入力してください。データベースをホストしているサーバーのいずれかに接続できない場合、エラーメッセージが表示されます。

データベース設定に必要な権限

データベースを作成および初期化する（またはデータベースの場所を変更する）には、ローカル管理者であり、ドメインユーザーである必要があります。また、特定の SQL Server 権限も必要です。以下の権限は、明示的に構成するか、Active Directory グループメンバーシップによって取得できます。Web Studio のユーザー資格情報にこれらの権限が含まれていない場合、SQL Server のユーザー資格情報の入力を求められます。

操作	目的	サーバーロール	データベースロール
データベースの作成	適切な空のデータベースを作成する	`dbcreator`	

操作	目的	サーバーロール	データベースロール
スキーマの作成	すべてのサービス固有のスキーマを作成し、最初の Controller をサイトに追加する	`securityadmin` *	`db_owner`
コントローラーを追加	サイトにコントローラー（最初のコントローラー以外）を追加	`securityadmin` *	`db_owner`
コントローラー（ミラーサーバー）を追加	ミラーデータベースのミラーロールにあるデータベースサーバーにコントローラーログインを追加	`securityadmin` *	
コントローラーを削除	サイトからコントローラーを削除	**	`db_owner`
スキーマを更新	スキーマの更新またはホットフィックスを適用		`db_owner`

* 技術的にはより制限的ですが、実際には、`securityadmin` サーバーロールは `sysadmin` サーバーロールと同等として扱うことができます。

** コントローラーがサイトから削除されても、データベースサーバーへのコントローラーログオンは削除されません。これは、同じマシン上のこのCitrix製品以外のサービスで使用されているログオンが誤って削除されるのを避けるためです。ログオンが不要になった場合は、手動で削除する必要があります。この操作には、`securityadmin` サーバーロールのメンバーシップが必要です。

これらの操作を実行するためにWeb Studioを使用する場合、Web Studioユーザーは、明示的に適切なサーバーロールのメンバーであるデータベースサーバーアカウントを持っているか、またはそうであるアカウントの資格情報を提供できる必要があります。

優先データベース権限スクリプト

エンタープライズ環境では、データベースのセットアップには、異なる役割（権限）を持つ異なるチームによって処理される必要があるスクリプトが含まれます。`securityadmin`または`db_owner`。

PowerShellを使用すると、推奨されるデータベース権限を指定できます。デフォルト以外の値を指定すると、個別のスクリプトが作成されます。1つのスクリプトには`securityadmin`ロールが必要なタスクが含まれます。もう1つのスクリプトは`db_owner`権限のみを必要とし、データベース管理者に連絡することなく、Citrix管理者が実行できます。

`get-*DBSchema`コマンドレットでは、`-DatabaseRights`オプションには次の有効な値があります。

- `SA`: データベースとDelivery Controllerのログインを作成するスクリプトを生成します。これらのタスクには`securityadmin`権限が必要です。
- `DBO`: データベースにユーザーロールを作成し、ログインを追加し、データベーススキーマを作成するスクリプトを生成します。これらのタスクには`db_owner`権限が必要です。
- `Mixed`: (デフォルト) 必要な権限に関係なく、すべてのタスクを1つのスクリプトにまとめます。

詳細については、コマンドレットのヘルプを参照してください。

データベースアドレス形式

データベースアドレスは、次のいずれかの形式で指定できます。

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

AlwaysOn可用性グループの場合は、場所フィールドにグループのリスナーを指定します。

データベースの場所を変更する

サイトを作成した後、構成ログデータベースと監視データベースの場所を変更できます。(サイトデータベースの場所は変更できません。)データベースの場所を変更すると、次のようになります。

- 以前のデータベースのデータは、新しいデータベースにインポートされません。
- ログを取得する際、両方のデータベースからログを集計することはできません。

- 新しいデータベースの最初のログエントリは、データベースの変更が発生したことを示しますが、以前のデータベースは特定されません。

強制ログが有効になっている場合、構成ログデータベースの場所を変更することはできません。

データベースの場所を変更するには：

1. データベースを配置するサーバーに、サポートされているバージョンのMicrosoft SQL Serverがインストールされていることを確認します。必要に応じて高可用性機能をセットアップします。
2. Web Studioにサインインし、左側のペインで**設定**を選択します。
3. **データベース**タイルを見つけ、**編集**を選択します。
4. **データベースの管理**ページで、新しい場所を指定するデータベースを選択し、アクションバーで**データベースの変更**を選択します。
5. 新しい場所とデータベース名を指定します。
6. Web Studioにデータベースを作成させたい場合で、適切な権限がある場合は、**完了**をクリックします。プロンプトが表示されたら**完了**をクリックすると、Web Studioが自動的にデータベースを作成します。Web Studioは、あなたの資格情報を使用してデータベースにアクセスしようとします。失敗した場合は、データベースユーザーの資格情報の入力を求められます。その後、Web Studioはデータベーススキーマをデータベースにアップロードします。資格情報は、データベース作成期間中のみ保持されます。
7. Web Studioでデータベースを作成したくない場合、または十分な権限がない場合は、**データベーススクリプトの生成**をクリックします。生成されたスクリプトには、必要に応じてデータベースとミラーデータベースを手動で作成するための手順が含まれています。スキーマをアップロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

詳細情報

- データベースサイジングツール。
- サイトデータベースのサイジングと、SQL Serverの高可用性ソリューションを使用する場合の接続文字列の構成。

配信方法

Citrix Virtual Apps and Desktops™ は、さまざまな配信方法を提供します。1つの配信方法だけでは、すべての要件を満たせない可能性があります。

はじめに

適切なアプリケーション配信方法を選択することで、スケーラビリティ、管理性、ユーザーエクスペリエンスの向上に役立ちます。

- **インストール済みアプリ:** アプリケーションはベースデスクトップイメージの一部です。インストールプロセスには、レジストリの変更に加えて、イメージドライブにコピーされるdll、exe、その他のファイルが含まれます。詳細については、「マシンカタログの作成」を参照してください。
- **ストリーミングアプリ (Microsoft App-V):** アプリケーションはプロファイルされ、オンデマンドでネットワーク経由でデスクトップに配信されます。アプリケーションファイルとレジストリ設定は、仮想デスクトップ上のコンテナに配置され、ベースオペレーティングシステムおよび相互から分離されます。この分離により、互換性の問題に対処できます。詳細については、「App-Vアプリケーションの展開と配信」を参照してください。
- **レイヤー化されたアプリ (Citrix App Layering):** 各レイヤーには、単一のアプリケーション、エージェント、またはオペレーティングシステムが含まれています。1つのOSレイヤー、1つのプラットフォームレイヤー (VDA、Citrix Provisioningエージェント)、および多数のアプリケーションレイヤーを統合することで、管理者は新しい展開可能なイメージを簡単に作成できます。OS、エージェント、およびアプリケーションが単一のレイヤーに存在するため、レイヤー化により継続的なメンテナンスが簡素化されます。レイヤーを更新すると、そのレイヤーを含むすべての展開済みイメージが更新されます。詳細については、「Citrix App Layering」を参照してください。
- **ホスト型Windowsアプリ:** マルチユーザーのCitrix Virtual Appsホストにインストールされ、デスクトップではなくアプリケーションとして展開されるアプリケーション。ユーザーはVDIデスクトップまたはエンドポイントデバイスからホスト型Windowsアプリにシームレスにアクセスでき、アプリがリモートで実行されているという事実を隠します。詳細については、「デリバリーグループの作成」を参照してください。
- **ローカルアプリ:** エンドポイントデバイスに展開されたアプリケーション。アプリケーションはエンドポイントで実行されますが、そのインターフェイスはユーザーのホスト型VDIセッション内に表示されます。詳細については、「ローカルアプリアクセスとURLリダイレクト」を参照してください。

デスクトップの場合、公開デスクトップまたはVDIデスクトップを検討してください。

Citrix Virtual Apps™ の公開アプリとデスクトップ

マルチセッションOSマシンを使用して、Citrix Virtual Apps and Desktops公開アプリと公開デスクトップを配信します。

ユースケース:

- 多数のユーザーへのアプリケーション配信コストを最小限に抑えながら、安全で高精細なユーザーエクスペリエンスを提供するために、安価なサーバーベースの配信を希望する場合。
- ユーザーが明確に定義されたタスクを実行し、アプリケーションのパーソナライズやオフラインアクセスを必要としない場合。ユーザーには、コールセンターオペレーターや小売業の従業員などのタスクワーカー、またはワークステーションを共有するユーザーが含まれます。
- アプリケーションの種類: 任意のアプリケーション。

利点と考慮事項:

- データセンター内で管理可能でスケーラブルなソリューション。
- 最も費用対効果の高いアプリケーション配信ソリューション。
- ホストされたアプリケーションは一元的に管理され、ユーザーはアプリケーションを変更できません。これにより、一貫性があり、安全で、信頼性の高いユーザーエクスペリエンスが提供されます。
- ユーザーはアプリケーションにアクセスするためにオンラインである必要があります。

ユーザーエクスペリエンス:

- ユーザーは、StoreFront™、**スタート**メニュー、または提供されたURLから1つ以上のアプリケーションを要求します。
- アプリケーションは仮想的に配信され、ユーザーデバイス上で高解像度でシームレスに表示されます。
- プロファイル設定に応じて、ユーザーのアプリケーションセッションが終了すると、ユーザーの変更は保存されます。そうでない場合、変更は削除されます。

アプリケーションの処理、ホスト、および配信:

- アプリケーションの処理は、ユーザーデバイスではなく、ホスティングマシンで行われます。ホスティングマシンは物理マシンまたは仮想マシンです。
- アプリケーションとデスクトップは、マルチセッションOSマシン上に存在します。
- マシンはマシンカタログを通じて利用可能になります。
- マシンカタログからのマシンは、同じアプリケーションセットをユーザーグループに配信するデリバリーグループに編成されます。
- マルチセッションOSマシンは、デスクトップまたはアプリケーション、あるいはその両方をホストするデリバリーグループをサポートします。

セッション管理と割り当て:

- マルチセッションOSマシンは、単一のマシンから複数のセッションを実行し、複数のアプリケーションとデスクトップを、同時に接続された複数のユーザーに提供します。各ユーザーは、ホストされているすべてのアプリケーションを実行するために、単一のセッションを必要とします。

  たとえば、ユーザーがログオンしてアプリケーションを要求すると、そのマシン上の1つのセッションは他のユーザーには利用できなくなります。2人目のユーザーがログオンし、そのマシンがホストするアプリケーションを要求すると、同じマシン上の2番目のセッションも利用できなくなります。両方のユーザーがさらにアプリケーションを要求しても、ユーザーは同じセッションを使用して複数のアプリケーションを実行できるため、追加のセッションは必要ありません。さらに2人のユーザーがログオンしてデスクトップを要求し、同じマシンで2つのセッションが利用可能な場合、その単一のマシンは4つの異なるユーザーをホストするために4つのセッションを使用していることになります。
- ユーザーが割り当てられているデリバリーグループ内で、最も負荷の低いサーバー上のマシンが選択されます。セッションが利用可能なマシンは、ユーザーがログオンしたときに、アプリケーションをユーザーに提供するためにランダムに割り当てられます。

VMホスト型アプリ

シングルセッションOSマシンを使用してVMホスト型アプリケーションを配信する

ユースケース:

- 安全で、一元管理を提供し、ホストサーバーあたり多数のユーザーをサポートするクライアントベースのアプリケーション配信ソリューションを求めています。それらのユーザーに、高解像度でシームレスに表示されるアプリケーションを提供したいと考えています。
- ユーザーは、社内ユーザー、外部請負業者、サードパーティの共同作業者、およびその他の暫定的なチームメンバーです。ユーザーはホスト型アプリケーションへのオフラインアクセスを必要としません。
- アプリケーションの種類: 他のアプリケーションとうまく連携しない可能性のあるアプリケーションや、Microsoft .NET Frameworkのようにオペレーティングシステムと相互作用する可能性のあるアプリケーション。これらの種類のアプリケーションは、仮想マシンでのホスティングに最適です。

利点と考慮事項:

- マスターイメージ上のアプリケーションとデスクトップは、データセンター内のマシンで安全に管理、ホスト、実行され、より費用対効果の高いアプリケーション配信ソリューションを提供します。
- ログオン時に、ユーザーは同じアプリケーションをホストするように構成されたデリバリーグループ内のマシンにランダムに割り当てられます。また、ユーザーがログオンするたびに、単一のマシンを単一のユーザーに割り当ててアプリケーションを配信するように静的に割り当てることもできます。静的に割り当てられたマシンでは、ユーザーは仮想マシンに独自のアプリケーションをインストールして管理できます。
- シングルセッションOSマシンでは、複数のセッションの実行はサポートされていません。そのため、各ユーザーはログオン時にデリバリーグループ内の単一のマシンを消費し、ユーザーはアプリケーションにアクセスするためにオンラインである必要があります。
- この方法により、アプリケーション処理用のサーバーリソースの量が増加し、ユーザーデータ用のストレージの量が増加する可能性があります。

ユーザーエクスペリエンス：

- マルチセッションOSマシンで共有アプリケーションをホストする場合と同様の、シームレスなアプリケーションエクスペリエンス。

アプリケーションの処理、ホスト、および配信：

- マルチセッションOSマシンと同じですが、仮想シングルセッションOSマシンである点が異なります。

セッション管理と割り当て：

- シングルセッションOSマシンは、単一のマシンから単一のデスクトップセッションを実行します。アプリケーションのみにアクセスする場合、オペレーティングシステムは各アプリケーションを新しいセッションとして認識するため、単一ユーザーは複数のアプリケーションを使用できます（単一のアプリケーションに限定されません）。
- デリバリーグループ内で、ユーザーがログオンすると、静的に割り当てられたマシン（ユーザーがログオンするたびに同じマシン）にアクセスするか、セッションの可用性に基づいて選択されるランダムに割り当てられたマシンにアクセスできます。

VDIデスクトップ

シングルセッションOSマシンを使用して、Citrix Virtual Apps and Desktops VDIデスクトップを配信します。

VDIデスクトップは仮想マシンでホストされ、各ユーザーにデスクトップオペレーティングシステムを提供します。

VDIデスクトップは公開デスクトップよりも多くのリソースを必要としますが、それらにインストールされているアプリケーションがサーバーベースのオペレーティングシステムをサポートする必要はありません。また、選択するVDIデスクトップの種類によっては、これらのデスクトップを個々のユーザーに割り当てることができます。これにより、ユーザーは高度なパーソナライゼーションが可能になります。

VDIデスクトップ用のマシンカタログを作成するときは、次のいずれかの種類のデスクトップを作成します。

- **ランダム非永続デスクトップ（プール型VDIデスクトップとも呼ばれる）：** ユーザーがこれらのデスクトップのいずれかにログオンするたびに、そのユーザーはデスクトップのプールから選択されたデスクトップに接続します。このプールは単一のマスターイメージに基づいています。デスクトップへのすべての変更は、マシンが再起動すると失われます。
- **静的非永続デスクトップ：** 最初のログオン時に、ユーザーはデスクトップのプールからデスクトップを割り当てられます。（プール内の各マシンは単一のマスターイメージに基づいています。）最初の使用後、ユーザーがデスクトップを使用するためにログオンするたびに、そのユーザーは最初の使用時に割り当てられた同じデスクトップに接続します。デスクトップへのすべての変更は、マシンが再起動すると失われます。
- **静的永続デスクトップ:** 他の種類のVDIデスクトップとは異なり、ユーザーはこれらのデスクトップを完全にパーソナライズできます。初回ログオン時に、ユーザーはデスクトッププールからデスクトップを割り当てられます。そのユーザーによる以降のログオンは、初回使用時に割り当てられた同じデスクトップに接続します。デスクトップへの変更は、マシンの再起動後も保持されます。

リモートPCアクセス

Remote PC Accessは、Citrix Virtual Apps and Desktopsの機能で、組織が従業員に企業リソースへのリモートアクセスを安全かつ容易に許可できるようにします。Citrixプラットフォームは、ユーザーが物理的なオフィスPCにアクセスできるようにすることで、この安全なアクセスを可能にします。ユーザーがオフィスPCにアクセスできれば、業務に必要なすべてのアプリケーション、データ、リソースにアクセスできます。Remote PC Accessは、テレワークに対応するための他のツールの導入や提供の必要性を排除します。例えば、仮想デスクトップやアプリケーション、およびそれらに関連するインフラストラクチャなどです。

Remote PC Accessは、仮想デスクトップとアプリケーションを提供するCitrix Virtual Apps and Desktopsと同じコンポーネントを使用します。その結果、Remote PC Accessの展開と構成の要件

およびプロセスは、仮想リソースを提供するためのCitrix Virtual Apps and Desktopsの展開に必要なものと同じです。この統一性により、一貫性のある統合された管理エクスペリエンスが提供されます。ユーザーは、Citrix HDX™を使用してオフィスPCセッションを配信することで、最高のユーザーエクスペリエンスを得られます。

詳細については、Remote PC Accessを参照してください。

ネットワークポート

完全なネットワークポート情報は、Citrix Technologies で使用される通信ポートに記載されています。

Citrix®コンポーネントがインストールされると、オペレーティングシステムのホストファイアウォールも、デフォルトで、デフォルトのネットワークポートに合わせて更新されます。

ポート情報が必要になる場合があります。

- 規制遵守のため。
- Citrix Virtual Apps and Desktops™コンポーネントと他のCitrix製品またはコンポーネントの間にネットワークファイアウォールがある場合、そのファイアウォールを適切に構成できるようにするため。
- オペレーティングシステムのホストファイアウォールではなく、マルウェア対策パッケージに付属しているものなど、サードパーティのホストファイアウォールを使用する場合。
- これらのコンポーネントのホストファイアウォール（通常はWindowsファイアウォールサービス）の構成を変更する場合。
- コンポーネント機能を再構成して別のポートまたはポート範囲を使用し、その後、構成で使用されていないポートを無効にするかブロックする場合。

一部のポートは、Internet Assigned Numbers Authority (IANA) に登録されています。これらの割り当てに関する詳細は、`<http://www.iana.org/assignments/port-numbers>`で確認できます。ただし、IANAが保持する記述情報は、必ずしも今日の使用状況を反映しているわけではありません。

また、VDA および Delivery Controller™ 上のオペレーティングシステムは、独自の用途のために受信ポートを必要とします。詳細については、Microsoft Windows のドキュメントを参照してください。

HDX™

> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターの使用は、お客様ご自身の責任で行ってください。編集する前に、必ずレジストリをバックアップしてください。

> Citrix HDXは、あらゆるデバイスで、あらゆるネットワーク経由で、集中管理されたアプリケーションとデスクトップのユーザーに高精細なエクスペリエンスを提供する幅広いテクノロジーのセットを表します。

仮想チャネル(/en-us/citrix-virtual-apps-desktops/2311/media/hdx-vir-channels.png)

HDXは、次の3つの技術原則に基づいて設計されています。

- インテリジェントリダイレクト
- 適応型圧縮
- データ重複排除

これらをさまざまな組み合わせで適用することで、ITおよびユーザーエクスペリエンスを最適化し、帯域幅の消費を削減し、ホスティングサーバーあたりのユーザー密度を向上させます。

- **インテリジェントリダイレクト** - インテリジェントリダイレクトは、画面アクティビティ、アプリケーションコマンド、エンドポイントデバイス、ネットワークおよびサーバーの機能を検査し、アプリケーションまたはデスクトップアクティビティをどこでどのようにレンダリングするかを即座に決定します。レンダリングは、エンドポイントデバイスまたはホスティングサーバーのいずれかで実行できます。
- **適応型圧縮** - 適応型圧縮により、リッチなマルチメディアディスプレイを低帯域幅のネットワーク接続で配信できます。HDXはまず、入力、デバイス、ディスプレイの種類（テキスト、ビデオ、音声、マルチメディア）など、いくつかの変数を評価します。最適な圧縮コーデックと、CPUおよびGPU使用率の最適な比率を選択します。その後、各固有のユーザーと状況に基づいてインテリジェントに適応します。このインテリジェントな適応は、ユーザーごと、またはセッションごとに行われます。

  適応型圧縮(/en-us/citrix-virtual-apps-desktops/2311/media/hdx-adaptive-compression.png)
- **データ重複排除** - ネットワークトラフィックの重複排除は、クライアントとサーバー間で送信される集約データを削減します。これは、ビットマップグラフィック、ドキュメント、印刷

ジョブ、ストリーミングメディアなど、一般的にアクセスされるデータ内の繰り返されるパターンを利用することで実現されます。これらのパターンをキャッシュすることで、変更のみがネットワーク経由で送信され、重複するトラフィックが排除されます。HDXはまた、マルチメディアストリームのマルチキャストもサポートしており、ソースからの単一の送信が、各ユーザーへの1対1の接続ではなく、1つの場所で複数のサブスクライバーによって視聴されます。

詳細については、高精細なユーザーワークスペースで生産性を向上させるを参照してください。

デバイス上での動作

HDXは、ユーザーエクスペリエンスを向上および最適化するために、ユーザーデバイスのコンピューティング能力を利用します。HDXテクノロジーにより、ユーザーは仮想デスクトップまたはアプリケーションでマルチメディアコンテンツをスムーズかつシームレスに体験できます。ワークスペースコントロールにより、ユーザーは仮想デスクトップとアプリケーションを一時停止し、作業を中断した時点から別のデバイスで再開できます。

ネットワーク上

HDXは、低帯域幅および高遅延のWAN接続を含むあらゆるネットワーク上で最高のパフォーマンスを提供するために、高度な最適化および高速化機能を組み込んでいます。

HDXの機能は、環境の変化に適応します。これらの機能は、パフォーマンスと帯域幅のバランスを取ります。デスクトップまたはアプリケーションが社内ネットワーク上でローカルにアクセスされるか、企業ファイアウォールの外部からリモートでアクセスされるかにかかわらず、各ユーザーシナリオに最適なテクノロジーを適用します。

データセンター内

HDXは、クライアントデバイスの機能に関係なく、サーバーの処理能力とスケーラビリティを使用して、高度なグラフィックパフォーマンスを提供します。

Citrix Directorが提供するHDXチャネル監視は、ユーザーデバイス上の接続されたHDXチャネルのステータスを表示します。

HDX インサイト

HDX Insightは、NetScaler® Network InspectorとPerformance ManagerをDirectorと統合したものです。ICAトラフィックに関するデータを取得し、リアルタイムおよび履歴の詳細をダッシュボードビューで提供します。このデータには、クライアント側およびサーバー側のICAセッション遅

延、ICAチャネルの帯域幅使用量、および各セッションのICAラウンドトリップタイム値が含まれます。

NetScalerでHDX Insight仮想チャネルを使用して、必要なすべてのデータポイントを非圧縮形式で移動できます。この機能を無効にすると、NetScalerデバイスは、さまざまな仮想チャネルに分散されたICA®トラフィックを復号化および解凍します。単一の仮想チャネルを使用すると、複雑さが軽減され、スケーラビリティが向上し、費用対効果が高まります。

最小要件:

- シトリックス バーチャル アプリケーションズ アンド デスクトップ™ 7 v1808
- XenAppおよびXenDesktop 7.17
- NetScalerバージョン12.0 Build 57.x
- Citrix Workspace™ アプリ Windows 用 1808
- シトリックス レシーバー Windows版 4.10
- Citrix Workspace アプリ Mac 用 1808
- シトリックス レシーバー Mac版 12.8

HDX Insight仮想チャネルを有効または無効にする

この機能を無効にするには、Citrix NetScaler Application Flowサービスのプロパティを「無効」に設定します。有効にするには、サービスを「自動」に設定します。いずれの場合も、これらのプロパティを変更した後、サーバーマシンを再起動することをお勧めします。デフォルトでは、このサービスは有効（自動）になっています。

Insight仮想チャネルの画像(/en-us/citrix-virtual-apps-desktops/2311/media/hdx-insight-virtual-channel.png)

仮想デスクトップからHDX機能を利用する

- 4つのHDXマルチメディアリダイレクトテクノロジーの1つであるブラウザコンテンツリダイレクトが、HTML5およびWebRTCマルチメディアコンテンツの配信をどのように高速化するかを確認するには：

  a. Chromeブラウザ拡張機能をダウンロードし、仮想デスクトップにインストールします。

  b. ブラウザコンテンツリダイレクトが仮想デスクトップへのマルチメディアコンテンツの配信をどのように高速化するかを体験するには、YouTubeなどのHTML5ビデオを含むWebサイトから、デスクトップでビデオを視聴します。ユーザーはブラウザコンテンツリダイレクトが実行されていることを知りません。ブラウザコンテンツリダイレクトが使用されて

いるかどうかを確認するには、ブラウザウィンドウを素早くドラッグします。ビューポートとユーザーインターフェイスの間に遅延またはフレーム外の表示が見られます。また、Webページを右クリックして、メニューで**About HDX Browser Redirection**を探すこともできます。

- HDXが高品位オーディオを配信する方法を確認するには：

  a. 最大のオーディオ品質を得るためにCitrixクライアントを設定します。詳細については、Citrix Workspaceアプリのドキュメントを参照してください。

  b. デスクトップでデジタルオーディオプレーヤー（iTunesなど）を使用して音楽ファイルを再生します。

HDXは、ほとんどのユーザーに優れたグラフィックとビデオ体験をデフォルトで提供し、設定は不要です。ほとんどのユースケースで最高の体験を提供するCitrixポリシー設定は、デフォルトで有効になっています。

- HDX は、クライアント、プラットフォーム、アプリケーション、ネットワーク帯域幅に基づいて最適な配信方法を自動的に選択し、変化する状況に基づいて自己調整します。
- HDX は、2D および 3D グラフィックとビデオのパフォーマンスを最適化します。
- HDX を使用すると、ユーザーデバイスは、ホストサーバーを介するのではなく、インターネットまたはイントラネット上のソースプロバイダーからマルチメディアファイルを直接ストリーミングできます。このクライアント側コンテンツフェッチの要件が満たされない場合、メディア配信はサーバー側コンテンツフェッチとマルチメディアリダイレクトにフォールバックします。通常、マルチメディアリダイレクト機能ポリシーの調整は必要ありません。
- マルチメディアリダイレクトが利用できない場合、HDX はリッチなサーバーレンダリングビデオコンテンツを仮想デスクトップに配信します。たとえば、`<http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/>` のような高解像度ビデオを含むウェブサイトでビデオを視聴できます。

知っておくと良いこと:

- HDX 機能のサポートおよび要件については、システム要件 の記事を参照してください。特に明記されていない限り、HDX 機能はサポートされている Windows マルチセッション OS および Windows シングルセッション OS マシン、およびリモート PC アクセスデスクトップで利用できます。
- このコンテンツでは、ユーザーエクスペリエンスの最適化、サーバーのスケーラビリティの向上、または帯域幅要件の削減方法について説明します。Citrix ポリシーとポリシー設定の使用方法については、このリリースの Citrix ポリシー ドキュメントを参照してください。

- レジストリの編集を含む手順については、注意して使用してください。レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になる可能性のある深刻な問題が発生する可能性があります。Citrix は、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

自動クライアント再接続とセッションの信頼性

ホストされたアプリケーションやデスクトップにアクセスしているときに、ネットワークの中断が発生する可能性があります。よりスムーズな再接続を体験していただくために、自動クライアント再接続とセッションの信頼性を提供しています。デフォルト設定では、セッションの信頼性が開始され、その後、自動クライアント再接続が続きます。

自動クライアント再接続:

自動クライアント再接続は、クライアントエンジンを再起動して、切断されたセッションに再接続します。自動クライアント再接続は、設定で指定された時間の後にユーザーセッションを閉じ（または切断し）ます。自動クライアント再接続が進行中の場合、システムはアプリケーションおよびデスクトップのネットワーク中断通知をユーザーに次のように送信します。

- **デスクトップ。** セッションウィンドウはグレー表示され、再接続までの時間がカウントダウンタイマーで表示されます。
- **アプリケーション。** セッションウィンドウが閉じ、再接続が試行されるまでの時間を示すカウントダウンタイマーを含むダイアログがユーザーに表示されます。

自動クライアント再接続中、セッションはネットワーク接続を期待して再起動します。自動クライアント再接続が進行中の間、ユーザーはセッションを操作できません。

再接続時、切断されたセッションは保存された接続情報を使用して再接続されます。ユーザーは通常通りアプリケーションやデスクトップを操作できます。

自動クライアント再接続のデフォルト設定：

- 自動クライアント再接続タイムアウト: 120秒
- 自動クライアント再接続: 有効
- 自動クライアント再接続認証: 無効
- 自動クライアント再接続ログ記録: 無効

詳細については、(/ja-jp/citrix-virtual-apps-desktops/2311/policies/reference/ica-policy-settings/auto-client-reconnect-policy-settings.html)のを参照してください。

セッションの信頼性:

セッションの信頼性により、ネットワークの中断時でもICAセッションがシームレスに再接続されます。セッションの信頼性は、設定で指定された時間の経過後にユーザーセッションを閉じます（または切断します）。セッションの信頼性タイムアウト後、自動クライアント再接続設定が有効になり、切断されたセッションへのユーザーの再接続が試行されます。セッションの信頼性が進行中の場合、アプリケーションおよびデスクトップのネットワーク中断通知は次のようにユーザーに送信されます。

- **デスクトップ。** セッションウィンドウが半透明になり、再接続までの時間をカウントダウンタイマーが表示します。
- **アプリケーション。** ウィンドウが半透明になり、通知領域から接続中断のポップアップが表示されます。

セッションの信頼性がアクティブな間、ユーザーはICAセッションを操作できません。ただし、ネットワーク中断直後の数秒間はキーストロークなどのユーザーアクションがバッファリングされ、ネットワークが利用可能になったときに再送信されます。

再接続時、クライアントとサーバーはプロトコル交換の同じ時点から再開します。セッションウィンドウの半透明表示が解除され、アプリケーションには適切な通知領域ポップアップが表示されます。

デフォルトのセッションの信頼性設定

- セッションの信頼性タイムアウト: 180秒
- 再接続UIの不透明度レベル: 80%
- セッションの信頼性接続: 有効
- セッションの信頼性ポート番号: 2598

詳細については、(/ja-jp/citrix-virtual-apps-desktops/2311/policies/reference/ica-policy-settings/session-reliability-policy-settings.html)のを参照してください。

NetScalerと自動クライアント再接続およびセッションの信頼性:

サーバーでマルチストリームおよびマルチポートポリシーが有効になっており、以下の条件のいずれかまたはすべてが当てはまる場合、自動クライアント再接続は機能しません。

- NetScaler Gateway でセッションの信頼性が無効になっています。
- NetScaler アプライアンスでフェールオーバーが発生します。
- NetScaler SD-WAN は NetScaler Gateway とともに使用されます。

HDX アダプティブスループット

HDX アダプティブスループットは、出力バッファーを調整することで、ICA セッションのピークスループットをインテリジェントに微調整します。出力バッファーの数は、初期値として高い値に設定されます。この高い値により、特に高遅延ネットワークにおいて、データがより迅速かつ効率的にクライアントに送信されます。インタラクティブ性の向上、ファイル転送の高速化、ビデオ再生のスムーズ化、フレームレートと解像度の向上により、ユーザーエクスペリエンスが強化されます。

セッションのインタラクティブ性は、ICAセッション内のデータストリームがインタラクティブ性に悪影響を与えていないかを判断するために常に測定されます。そのような状況が発生した場合、セッションに対する大量のデータストリームの影響を軽減し、インタラクティブ性を回復させるためにスループットが低下します。

> **重要:**
>
> HDXアダプティブスループットは、出力バッファの設定方法を、クライアントからVDAにメカニズムを移動させることで変更するため、手動での設定は不要です。

この機能には、以下の要件があります。

- VDA バージョン 1811 以降
- Windows 向け Workspace アプリ 1811 以降

ユーザーデバイスに送信される画質の向上

以下の視覚表示ポリシー設定は、仮想デスクトップからユーザーデバイスに送信される画像の品質を制御します。

- 視覚品質。ユーザーデバイスに表示される画像の視覚品質を制御します: 中、高、常にロスレス、ロスレスにビルド (デフォルト = 中)。デフォルト設定の「中」を使用した場合の実際のビデオ品質は、利用可能な帯域幅によって異なります。
- ターゲットフレームレート。仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を指定します (デフォルト = 30)。CPUが遅いデバイスの場合、低い値を指定するとユーザーエクスペリエンスが向上する可能性があります。サポートされる1秒あたりの最大フレームレートは60です。

- 表示メモリ制限。セッションの最大ビデオバッファサイズをキロバイト単位で指定します (デフォルト = 65536 KB)。より多くの色深度と高い解像度を必要とする接続の場合、制限を増やしてください。必要な最大メモリを計算できます。

> **注:**
>
> **表示メモリ制限**設定は非推奨になりました。この変更により、Citrix は表示メモリを制限しなくなりました。代わりに、クライアントの表示レイアウトが完全に収容されるように、必要な最小限のメモリが割り当てられます。

ビデオ会議のパフォーマンスを向上させる

いくつかの一般的なビデオ会議アプリケーションは、マルチメディアリダイレクトを介した Citrix Virtual Apps and Desktops からの配信向けに最適化されています (例: HDX RealTime Optimization Pack を参照)。最適化されていないアプリケーションの場合、HDX ウェブカメラビデオ圧縮は、セッション中のビデオ会議におけるウェブカメラの帯域幅効率と遅延耐性を向上させます。このテクノロジーは、専用のマルチメディア仮想チャネルを介してウェブカメラトラフィックをストリーミングします。このテクノロジーは、アイソクロナス HDX Plug-n-Play USB リダイレクトサポートと比較して帯域幅の使用量が少なく、WAN 接続でもうまく機能します。

Citrix Workspace アプリのユーザーは、Desktop Viewer のマイクとウェブカメラの設定で を選択することで、デフォルトの動作を上書きできます。ユーザーが HDX ウェブカメラビデオ圧縮から切り替えるのを防ぐには、ICA ポリシー設定 > USB デバイスポリシー設定の下にあるポリシー設定を使用して USB デバイスリダイレクトを無効にします。

HDX ウェブカメラビデオ圧縮では、以下のポリシー設定を有効にする必要があります (すべてデフォルトで有効になっています)。

- クライアントオーディオリダイレクト
- クライアントマイクのリダイレクト
- マルチメディア会議

ウェブカメラがハードウェアエンコーディングをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコーディングを使用します。ハードウェアエンコーディングは、ソフトウェアエンコーディングよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、次のDWORDキー値をレジストリキーに追加します: HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1。

ネットワークトラフィックの優先順位

Quality of Serviceをサポートするルーターを使用して、セッションの複数の接続にわたるネットワークトラフィックに優先順位が割り当てられます。ユーザーデバイスとサーバー間でICAトラフィックを伝送するために、4つのTCPストリームと2つのユーザーデータグラムプロトコル（UDP）ストリームが利用可能です。

- TCPストリーム - リアルタイム、インタラクティブ、バックグラウンド、およびバルク
- UDPストリーム - 音声およびFramehawkディスプレイリモート処理

各仮想チャネルは特定の優先順位に関連付けられ、対応する接続で転送されます。接続に使用されるTCPポート番号に基づいて、チャネルを個別に設定できます。

Windows 10、Windows 8、およびWindows 7マシンにインストールされたVirtual Delivery Agent (VDA) では、マルチチャネルストリーミング接続がサポートされています。ネットワーク管理者と協力して、**Multi-Port Policy**設定で構成されたCommon Gateway Protocol (CGP) ポートがネットワークルーターに正しく割り当てられていることを確認してください。

Quality of Serviceは、複数のセッション信頼性ポートまたはCGPポートが構成されている場合にのみサポートされます。

警告:

この機能を使用する場合は、トランスポートセキュリティを使用してください。Citrixは、Internet Protocol Security (IPsec) またはTransport Layer Security (TLS) の使用を推奨しています。TLS接続は、マルチストリームICAをサポートするNetScaler Gatewayを介して接続する場合にのみサポートされます。社内ネットワークでは、TLSを使用したマルチストリーム接続はサポートされていません。

複数のストリーミング接続に対してQuality of Serviceを設定するには、次のCitrixポリシー設定をポリシーに追加します（詳細については、マルチストリーム接続ポリシー設定を参照してください）。

- マルチポートポリシー - この設定は、複数の接続にわたるICAトラフィックのポートを指定し、ネットワークの優先順位を確立します。
    - CGPデフォルトポート優先順位リストから優先順位を選択します。デフォルトでは、プライマリポート（2598）は高優先順位です。

    - 必要に応じて、CGP port1、CGP port2、CGP port3にさらにCGPポートを入力し、それぞれの優先順位を特定します。各ポートには一意の優先順位が必要です。

  追加のTCPトラフィックを許可するように、VDA上のファイアウォールを明示的に構成します。

- マルチストリームコンピューター設定 - この設定はデフォルトで無効になっています。環境でマルチストリームをサポートするCitrix NetScaler SD-WANを使用している場合、この設定を構成する必要はありません。目的のQuality of Serviceを実現するために、サードパーティ製ルーターまたはレガシーNetScaler SD-WANを使用する場合は、このポリシー設定を構成してください。
- マルチストリームユーザー設定 - この設定はデフォルトで無効になっています。

これらの設定を含むポリシーを有効にするには、ユーザーはログオフしてからネットワークにログオンする必要があります。

リモート言語バーの表示/非表示

言語バーは、アプリケーションセッションで優先入力言語を表示します。この機能が有効になっている場合（デフォルト）、Windows向けCitrix Workspaceアプリの**［高度な設定］>［言語バー］**UIから言語バーを表示または非表示にできます。VDA側のレジストリ設定を使用すると、言語バー機能のクライアント制御を無効にできます。この機能が無効になっている場合、クライアントUI設定は有効にならず、ユーザーごとの現在の設定によって言語バーの状態が決まります。詳しくは、「ユーザーエクスペリエンスの向上」を参照してください。

VDAから言語バー機能のクライアント制御を無効にするには：

1. レジストリエディターで、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWIに移動します。
2. DWORD値キーSeamlessFlagsを作成し、0x40000に設定します。

Unicodeキーボードマッピング

Windows以外のCitrix Receiverは、ローカルキーボードレイアウト（Unicode）を使用します。ユーザーがローカルキーボードレイアウトとサーバーキーボードレイアウト（スキャンコード）を変更した場合、それらが同期せず、出力が正しくない可能性があります。たとえば、User1がローカルキーボードレイアウトを英語からドイツ語に変更します。その後、User1はサーバー側のキーボードをドイツ語に変更します。両方のキーボードレイアウトがドイツ語であっても、同期しない可能性があり、文字出力が正しくない原因となります。

Unicode キーボードレイアウトマッピングを有効または無効にする

デフォルトでは、この機能はVDA側で無効になっています。この機能を有効にするには、VDAでレジストリエディターregeditを使用して機能をオンに切り替えます。次のレジストリキーを追加します。

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前：EnableKlMap

種類: DWORD

値: 1

この機能を無効にするには、**EnableKlMap** を 0 に設定するか、**CtxKlMap** キーを削除します。

Unicode キーボードレイアウトマッピング互換モードを有効にする

デフォルトでは、Unicode キーボードレイアウトマッピングは、サーバー側でキーボードレイアウトを変更したときに、新しい Unicode キーボードレイアウトマップを再読み込みするために一部の Windows API を自動的にフックします。一部のアプリケーションはフックできません。互換性を維持するために、これらのフックできないアプリケーションをサポートするように機能を互換モードに変更できます。次のレジストリキーを追加します。

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: DisableWindowHook

種類: DWORD

値: 1

通常の Unicode キーボードレイアウトマッピングを使用するには、**DisableWindowHook** を 0 に設定します。

Citrix ICA® 仮想チャネル

> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じた問題が解決できることを保証できません。レジストリエディターは、ご自

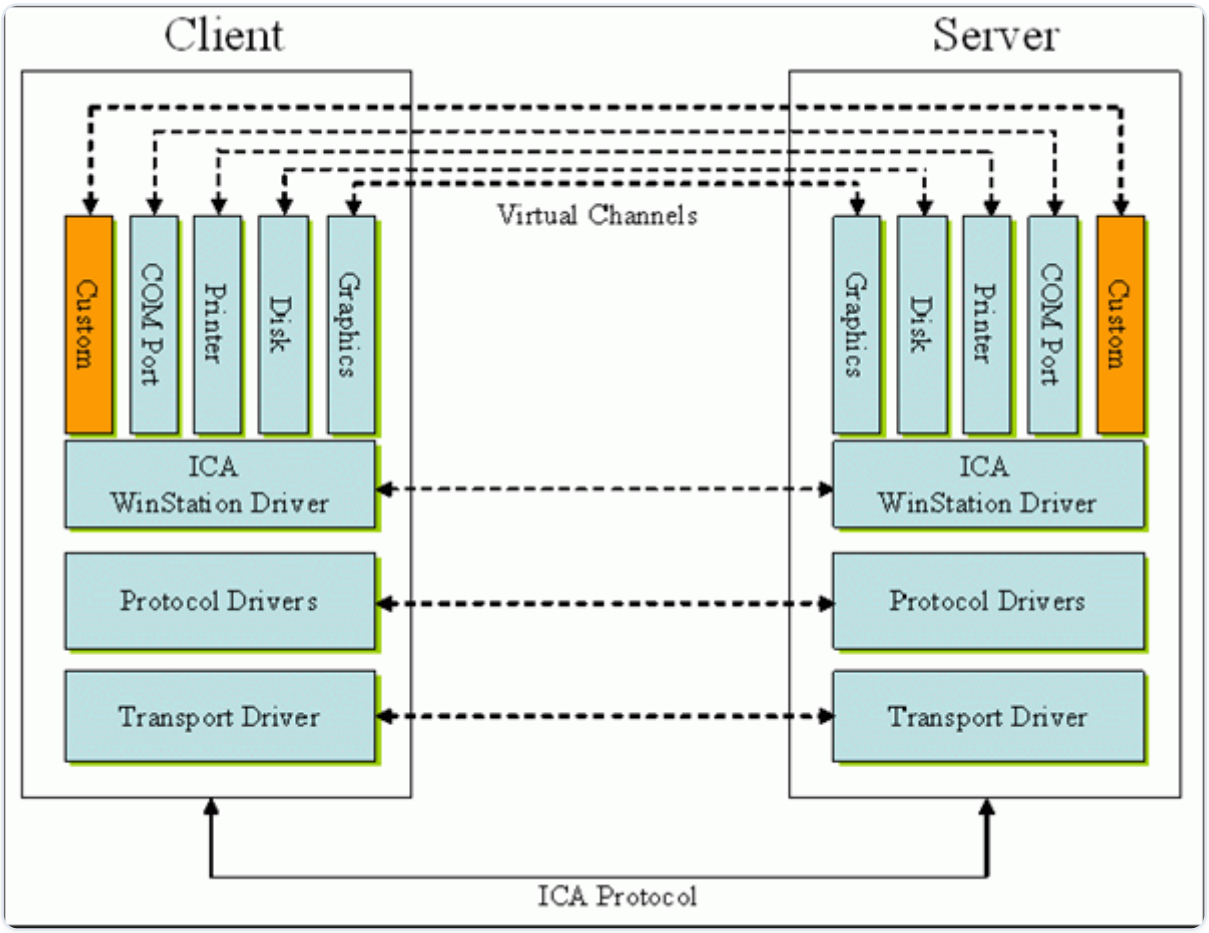
> 身の責任においてご使用ください。編集する前に、必ずレジストリをバックアップしてください。

ICA仮想チャネルとは?

Citrix Workspace™アプリとCitrix Virtual Apps and Desktops™サーバー間の機能と通信の大部分は、仮想チャネルを介して行われます。仮想チャネルは、Citrix Virtual Apps and Desktopsサーバーでのリモートコンピューティングエクスペリエンスに不可欠な部分です。仮想チャネルは次の目的で使用されます。

- オーディオ
- COMポート
- ディスク
- グラフィック
- LPTポート
- プリンタ
- スマートカード
- サードパーティ製のカスタム仮想チャネル
- ビデオ

新しい仮想チャネルは、より多くの機能を提供するために、Citrix Virtual Apps and DesktopsサーバーおよびCitrix Workspaceアプリ製品の新しいバージョンとともにリリースされることがあります。



仮想チャネルは、サーバー側のアプリケーションと通信するクライアント側の仮想ドライバーで構成されます。Citrix Virtual Apps and Desktopsには、さまざまな仮想チャネルが付属しています。これらは、提供されているソフトウェア開発キット (SDK) のいずれかを使用して、顧客やサードパーティベンダーが独自の仮想チャネルを作成できるように設計されています。

仮想チャネルは、さまざまなタスクを安全に実行する方法を提供します。たとえば、クライアント側のデバイスと通信するCitrix Virtual Appsサーバーで実行されているアプリケーションや、クライアント側の環境と通信するアプリケーションなどです。

クライアント側では、仮想チャネルは仮想ドライバーに対応します。各仮想ドライバーは特定の機能を提供します。一部は通常の操作に必要であり、その他はオプションです。仮想ドライバーはプレゼンテーション層プロトコルレベルで動作します。Windows Station（WinStation）プロトコル層によって提供されるチャネルを多重化することにより、いつでも複数のプロトコルをアクティブにできます。

以下の機能は、このレジストリパスの下にあるVirtualDriverレジストリ値に含まれています。

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

または

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0`（64ビット用）

- Thinwire3.0（必須）
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- クリップボード
- ClientComm
- ClientAudio
- LicenseHandler (必須)
- TWI (必須)
- スマートカード
- ICACTL (必須)
- SSPI
- TwainRdr
- ユーザーエクスペリエンス
- Vd3d

> **注:**
>
> レジストリキーからこれらの値の1つ以上を削除することで、特定のクライアント機能を無効にできます。たとえば、クライアントクリップボードを削除したい場合は、**Clipboard**という単語を削除します。

> このリストには、クライアント仮想ドライバーファイルとそれぞれの機能が含まれています。Citrix Virtual AppsおよびWindows用Citrix Workspaceアプリはこれらのファイルを使用します。これらは、汎用USB仮想チャネルで説明されている汎用USBを除き、ダイナミックリンクライブラリ（ユーザーモード）の形式であり、Windowsドライバー（カーネルモード）ではありません。

- vd3dn.dll – デスクトップコンポジションリダイレクトに使用されるDirect3D仮想チャネル
- vdcamN.dll – 双方向オーディオ

- vdcdm30n.dll – クライアントドライブマッピング
- vdcom30N.dll - クライアントCOMポートマッピング
- vdcpm30N.dll – クライアントプリンターマッピング
- vdctln.dll – ICAコントロールチャネル
- vddvc0n.dll – 動的仮想チャネル
- vdeuemn.dll - エンドユーザーエクスペリエンス監視
- vdgusbn.dll – 汎用USB仮想チャネル
- vdkbhook.dll – 透明キーパススルー
- vdlfpn.dll – UDPライクなトランスポートを介したFramehawkディスプレイチャネル
- vdmmn.dll – マルチメディアサポート
- vdmrvc.dll – Mobile Receiver仮想チャネル
- vdmtchn.dll - マルチタッチサポート
- vdscardn.dll – スマートカードサポート
- vdsens.dll – センサー仮想チャネル
- vdspl30n.dll – クライアントUPD
- vdsspin.dll – ケルベロス
- vdtuin.dll – 透明UI
- vdtw30n.dll – クライアント Thinwire
- vdtwin.dll – シームレス
- vdtwn.dll – ツイン

いくつかの仮想チャネルは他のファイルにコンパイルされています。例えば、クリップボードマッピングはwfica32.exeで利用できます。

64ビット互換性

Windows版Citrix Workspaceアプリは64ビット互換です。32ビット用にコンパイルされたほとんどのバイナリと同様に、これらのクライアントファイルには64ビット用にコンパイルされた同等のものがあります。

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll

- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

汎用USB仮想チャネル

汎用USB仮想チャネルの実装では、仮想チャネルドライバーvdgusbn.dllに加えて、2つのカーネルモードドライバーを使用します。

- ctxusbm.sys
- ctxusbr.sys

ICA仮想チャネルの仕組み

仮想チャネルは複数の方法でロードされます。シェル（サーバーの場合はWfShell、ワークステーションの場合はPicaShell）が一部の仮想チャネルをロードします。一部の仮想チャネルはWindowsサービスとしてホストされます。

シェルによってロードされる仮想チャネルモジュール（例）：

- EUEM
- ツイン
- クリップボード
- マルチメディア
- シームレスセッション共有
- タイムゾーン

いくつかはカーネルモードとしてロードされます。例:

- CtxDvcs.sys – ダイナミック仮想チャネル
- Icausbb.sys – 汎用USBリダイレクト
- Picadm.sys – クライアントドライブマッピング

- Picaser.sys – COMポートリダイレクト
- Picapar.sys – LPTポートリダイレクト

サーバー側のグラフィック仮想チャネル

XenApp 7.0およびXenDesktop 7.0以降、`ctxgfx.exe` はワークステーションおよびターミナルサーバーベースのセッションの両方でグラフィック仮想チャネルをホストします。`Ctxgfx` は、対応するドライバー（RDSHの場合は`Icardd.dll`、ワークステーションの場合は`vdod.dll`および`vidd.dll`）と対話するプラットフォーム固有のモジュールをホストします。

XenDesktop® 3D Pro展開の場合、VDA上の対応するGPUにOEMグラフィックドライバーがインストールされます。`Ctxgfx` は、OEMグラフィックドライバーと対話するために特殊なアダプターモジュールをロードします。

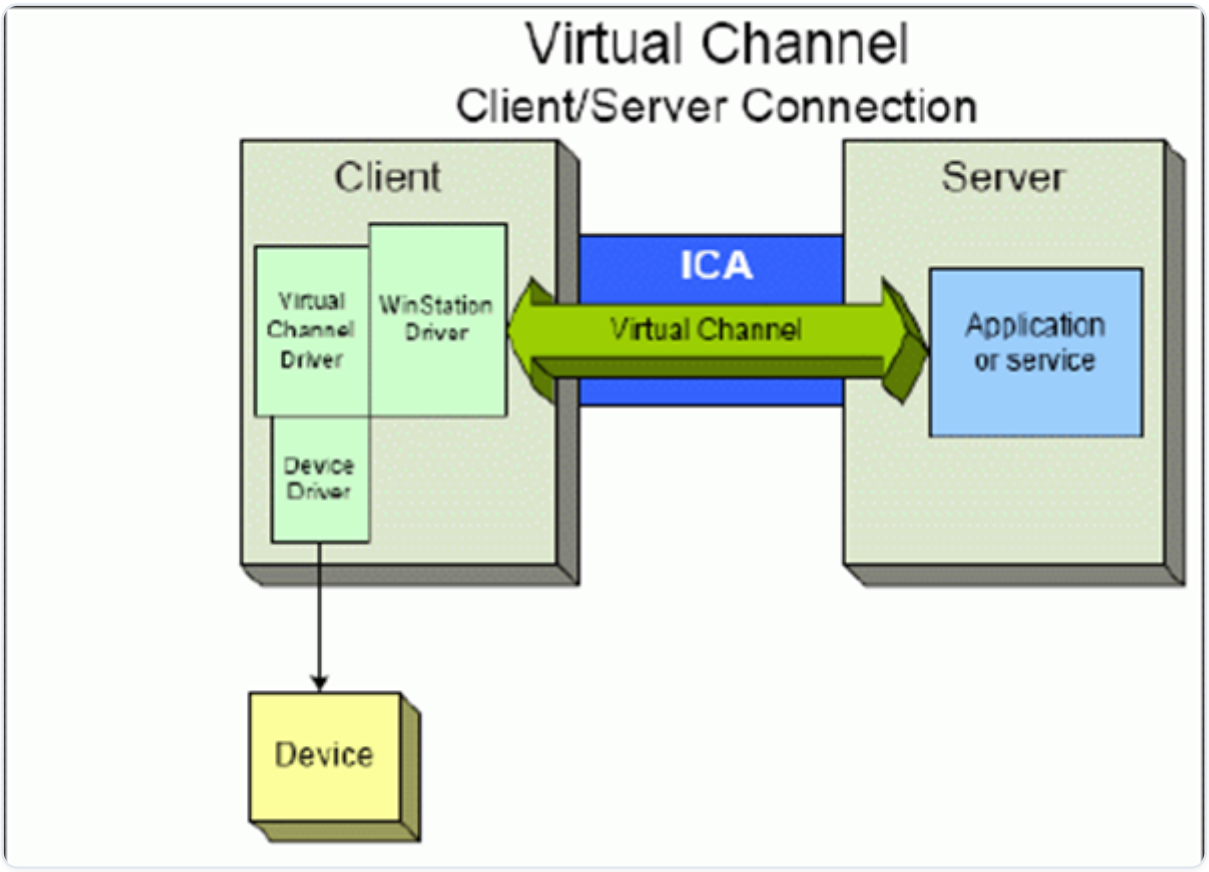
Windowsサービスでの特殊チャネルのホスティング

Citrix Virtual Apps and Desktopsサーバーでは、さまざまなチャネルがWindowsサービスとしてホストされます。このようなホスティングは、セッション内の複数のアプリケーションおよびサーバー上の複数のセッションに対して、1対多のセマンティクスを提供します。このようなサービスの例は次のとおりです。

- Citrixデバイスリダイレクターサービス
- Citrixダイナミック仮想チャネルサービス
- Citrixエンドユーザーエクスペリエンス監視サービス
- Citrix ロケーションおよびセンサー仮想チャネルサービス
- Citrix マルチタッチ リダイレクトサービス
- Citrix 印刷マネージャーサービス
- Citrix スマートカードサービス
- Citrix オーディオ リダイレクトサービス (Citrix Virtual Desktops™ のみ)
- Citrix ICA ステータスチャネルサービス

Citrix Virtual Apps のオーディオ仮想チャネルは、Windows Audio サービスを使用してホストされます。

サーバー側では、すべてのクライアント仮想チャネルが WinStation ドライバー (Wdica.sys) を介してルーティングされます。クライアント側では、wfica32.exe に組み込まれている対応する WinStation ドライバーがクライアント仮想チャネルをポーリングします。この図は、仮想チャネルのクライアント-サーバー接続を示しています。



この概要では、仮想チャネルを使用したクライアント-サーバー間のデータ交換について説明します。

1. クライアントは Citrix Virtual Apps and Desktops サーバーに接続します。クライアントは、サポートする仮想チャネルに関する情報をサーバーに渡します。
2. サーバー側アプリケーションが起動し、仮想チャネルへのハンドルを取得し、必要に応じてチャネルに関する追加情報を問い合わせます。
3. クライアント仮想ドライバーとサーバー側アプリケーションは、次の2つの方法を使用してデータを渡します。

    - サーバーアプリケーションがクライアントに送信するデータを持っている場合、データは直ちにクライアントに送信されます。クライアントがデータを受信すると、WinStation ドライバーは ICA ストリームから仮想チャネルデータを逆多重化し、直ちにクライアント仮想ドライバーに渡します。
    - クライアント仮想ドライバーがサーバーに送信するデータを持っている場合、データは WinStation ドライバーが次にポーリングしたときに送信されます。サーバーがデータを受信すると、仮想チャネルアプリケーションが読み取るまでキューに入れられます。データが受信されたことをサーバー仮想チャネルアプリケーションに通知する方法はありません。

4. サーバー仮想チャネルアプリケーションが完了すると、仮想チャネルを閉じ、割り当てられたリソースを解放します。

Virtual Channel SDK を使用して独自の仮想チャネルを作成する

注：

Citrix SDK は、Citrix Developer ポータル (https://developer.cloud.com) で入手できます。

Virtual Channel SDK を使用して仮想チャネルを作成するには、中程度のプログラミング知識が必要です。この方法を使用して、クライアントとサーバー間の主要な通信パスを提供します。たとえば、セッション内のプロセスで使用するスキャナーなどのデバイスのクライアント側での使用を実装する場合などです。

注：

- Virtual Channel SDK は、仮想チャネルのサーバー側を記述するために WFAPI SDK を必要とします。
- Citrix Virtual Apps and Desktops のセキュリティが強化されたため、ICA セッションで開くことを許可する仮想チャネルを指定する必要があります。詳しくは、「仮想チャネル許可リストポリシー設定」を参照してください。

ICA Client Object SDK を使用して独自の仮想チャネルを作成する

ICA Client Object (ICO) を使用して仮想チャネルを作成する方が、Virtual Channel SDK を使用するよりも簡単です。**CreateChannels** メソッドを使用してプログラムで名前付きオブジェクトを作成することにより、ICO を使用します。

重要：

Citrix Receiver for Windows バージョン 10.00 以降 (および Citrix Workspace apps for Windows) でセキュリティが強化されたため、ICO 仮想チャネルを作成する際には追加の手順を実行する必要があります。

仮想チャネルのパススルー機能

Citrix が提供するほとんどの仮想チャネルは、ICA セッション内 (パススルーセッションとも呼ばれます) で Citrix Workspace app for Windows を使用する場合、変更なしで動作します。クライアントを複数のホップで使用する場合には考慮事項があります。

次の機能は、シングルホップまたはマルチホップで同じように動作します。

- クライアント COM ポートマッピング
- クライアントドライブマッピング
- クライアントプリンターマッピング
- クライアント UPD
- エンドユーザーエクスペリエンス監視
- 汎用 USB
- ケルベロス
- マルチメディアサポート
- スマートカードサポート
- 透過的キーパススルー
- ツイン

レイテンシーの固有の性質、および各ホップで実行される圧縮、解凍、レンダリングなどの要因により、クライアントが経由するホップが増えるごとにパフォーマンスが影響を受ける可能性があります。影響を受ける領域は次のとおりです。

- 双方向オーディオ
- ファイル転送
- 汎用USBリダイレクト
- シームレス
- シンワイヤー

> **重要:**

> 既定では、パススルーセッションで実行されているクライアントのインスタンスによってマップされたクライアントドライブは、接続しているクライアントのクライアントドライブに制限されます。

Citrix Virtual DesktopセッションとCitrix Virtual Appセッション間の仮想チャネルのパススルー機能

Citrixが提供するほとんどの仮想チャネルは、Citrix Virtual Desktopsサーバー上のICAセッション内でCitrix Workspaceアプリ for Windowsを使用する場合（パススルーセッションとも呼ばれます）、変更されずに動作します。

具体的には、Citrix Virtual Desktopsサーバーには、**picaPassthruHook**を実行するVDAフックがあります。このフックにより、クライアントはCPSサーバー上で実行されていると認識し、クライアントを従来のパススルーモードにします。

以下の従来の仮想チャネルとその機能をサポートしています。

- クライアント
- クライアントCOMポートマッピング
- クライアントドライブマッピング
- クライアントプリンターマッピング
- 汎用USB（パフォーマンス上の理由により制限あり）
- マルチメディアサポート
- スマートカードサポート
- SSON
- 透過的なキーパススルー

セキュリティとICA仮想チャネル

使用状況の保護は、仮想チャネルの計画、開発、実装において重要な部分です。このドキュメント全体にわたって、セキュリティの特定の領域に関するいくつかの参照があります。

ベストプラクティス

接続および**再接続**時に仮想チャネルを開きます。ログオフおよび**切断**時に仮想チャネルを閉じます。

仮想チャネル機能を使用するスクリプトを作成する際は、以下のガイドラインを念頭に置いてください。

仮想チャネルの命名:

最大32個の仮想チャネルを作成できます。32個のチャネルのうち17個は、特別な目的のために予約されています。

- 仮想チャネル名は7文字以内である必要があります。
- 最初の3文字はベンダー名に、次の4文字はチャネルタイプに予約されています。たとえば、**CTXAUD**はCitrixオーディオ仮想チャネルを表します。

仮想チャネルは、7文字（またはそれ以下）のASCII名で参照されます。ICAプロトコルの以前のバージョンでは、仮想チャネルには番号が付けられていました。現在、番号はASCII名に基づいて動的に割り当てられるため、実装が容易になっています。内部使用のみを目的として仮想チャネルコードを開発しているユーザーは、既存の仮想チャネルと競合しない任意の7文字の名前を使用できます。数字と大文字および小文字のASCIIのみを使用してください。独自の仮想チャネルを追加する際は、既存の命名規則に従ってください。いくつかの事前定義されたチャネルがあります。事前定義されたチャネルはOEM識別子CTXで始まり、Citrixのみが使用できます。

ダブルホップサポート:

仮想チャネル	ダブルホップはサポートされていますか？
オーディオ	いいえ
ブラウザコンテンツリダイレクション	いいえ
CDM	はい
CEIP	いいえ
クリップボード	はい
コンティニュアム (MRVC)	いいえ
コントロールVC	はい
HTML5 ビデオリダイレクト (v1)	はい
キーボード、マウス	はい
マルチタッチ	いいえ
NSAPVC	いいえ
印刷	はい
SensVC	いいえ
スマートカード	はい

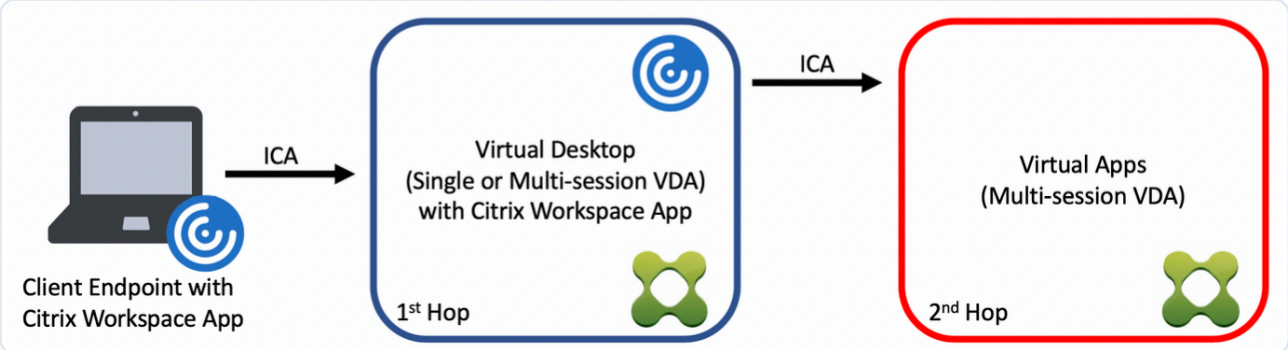
仮想チャネル	ダブルホップはサポートされていますか？
トゥエイン	はい
USB VC	はい
WAYCOMデバイス -K2M (USB VCを使用)	はい
Webカメラビデオ圧縮	はい
Windows Mediaリダイレクト	はい

参照

- ICA 仮想チャネル SDK
- Citrix Developer Networkは、Citrix SDKの使用に関するすべての技術リソースとディスカッションの拠点です。このネットワークでは、SDK、サンプルコードとスクリプト、拡張機能とプラグイン、およびSDKドキュメントにアクセスできます。また、各Citrix SDKに関する技術的な議論が行われるCitrix Developer Networkフォーラムも含まれています。

Citrix Virtual Apps and Desktops™ におけるダブルホップ

Citrix クライアントセッションのコンテキストでは、「ダブルホップ」という用語は、Citrix Virtual Desktop セッション内で実行されている Citrix Virtual App セッションを指します。次の図はダブルホップを示しています。



ダブルホップのシナリオでは、ユーザーがシングルセッションOS VDA (VDIとして知られる) またはマルチセッションOS VDA (公開デスクトップとして知られる) で実行されている Citrix Virtual Desktop に接続すると、それが最初のホップと見なされます。ユーザーが仮想デスクトップに接続した後、ユーザーは Citrix Virtual Apps™ セッションを起動できます。それが2番目のホップと見なされます。

ダブルホップ展開モデルを使用して、さまざまなユースケースをサポートできます。Citrix Virtual Desktop 環境と Citrix Virtual Apps 環境が異なるエンティティによって管理されているケースは、一般的な例の1つです。この方法は、アプリケーションの互換性の問題を解決するのにも効果的です。

システム要件

Citrix Cloud™ サービスを含むすべての Citrix Virtual Apps and Desktops エディションはダブルホップをサポートしています。

最初のホップでは、サポートされているバージョンのシングルセッションまたはマルチセッションOS VDA と Citrix Workspace アプリを使用する必要があります。2番目のホップでは、サポートされているバージョンのマルチセッションOS VDA を使用する必要があります。サポートされているバージョンについては、製品マトリックス ページを参照してください。

最高のパフォーマンスと互換性を得るために、Citrix は、使用中の VDA バージョンと同じかそれ以降のバージョンの Citrix クライアントを使用することを推奨します。

最初のホップが、Citrix Virtual Apps セッションと組み合わされたサードパーティ製 (Citrix 以外) の仮想デスクトップソリューションを含む環境では、サポートは Citrix Virtual Apps 環境に限定されます。サードパーティ製仮想デスクトップに関連する問題 (Citrix Workspace™ アプリの互換性、ハードウェアデバイスのリダイレクト、セッションパフォーマンスなど) が発生した場合、Citrix は限られた範囲で技術サポートを提供できます。トラブルシューティングの一環として、最初のホップに Citrix Virtual Desktop が必要になる場合があります。

ダブルホップにおける HDX™ の展開に関する考慮事項

一般に、ダブルホップの各セッションは一意であり、クライアント/サーバー機能は特定のホップに分離されます。このセクションでは、Citrix 管理者が特に考慮する必要がある領域について説明します。Citrix は、特定の環境構成でユーザーエクスペリエンスとパフォーマンスが適切であることを確認するために、必要な HDX 機能の徹底的なテストを実施することを推奨します。

グラフィック

最初のホップと2番目のホップで、デフォルトのグラフィック設定 (選択的エンコード) を使用します。HDX 3D Pro の場合、Citrix は、グラフィックアクセラレーションを必要とするすべてのアプリケーションを、VDA で利用可能な適切な GPU リソースを使用して最初のホップでローカルに実行することを強く推奨します。

遅延

エンドツーエンドの遅延は、全体的なユーザーエクスペリエンスに影響を与える可能性があります。最初のホップと2番目のホップの間に追加される遅延を考慮してください。これは、ハードウェアデバイスのリダイレクトにおいて特に重要です。

マルチメディア

オーディオおよびビデオコンテンツのサーバー側（セッション内）レンダリングは、最初のホップで最高のパフォーマンスを発揮します。2番目のホップでのビデオ再生は、最初のホップでのデコードと再エンコードを必要とし、その結果、帯域幅とハードウェアリソースの使用率が増加します。オーディオおよびビデオコンテンツは、可能な限り最初のホップに限定する必要があります。

USBデバイスリダイレクト

HDXには、幅広いUSBデバイスタイプをサポートするための汎用および最適化されたリダイレクトモードが含まれています。各ホップで使用されているモードに特に注意し、最良の結果を得るために以下の表を参照してください。汎用および最適化されたリダイレクトモードの詳細については、「汎用USBデバイス」を参照してください。

最初のホップ（VDIまたは公開デスクトップ）	2番目のホップ（仮想アプリ）	サポートに関する注意事項
最適化済み	最適化済み	推奨（デバイスサポートに基づく）。例：USBマスストレージ、TWAINスキャナー、Webカメラ、オーディオ。
汎用	汎用	最適化オプションが利用できないデバイスの場合。
汎用	最適化	技術的には可能ですが、デバイスがサポートされている場合は、両方のホップで最適化モードを使用することをお勧めします。
最適化	汎用	サポートされていません

注:

> USBプロトコルの本質的なチャッティネスのため、ホップをまたぐとパフォーマンスが低下する可能性があります。機能と結果は、特定のデバイスとアプリケーションの要件によって異なります。デバイスリダイレクトのすべての場合において、特にダブルホップシナリオでは、検証テストを強くお勧めします。

サポートの例外

ダブルホップセッションは、以下のものを除き、ほとんどのHDX機能と能力をサポートしています。

- ブラウザコンテンツリダイレクト
- ローカルアプリアクセス
- Skype for Business 向け リアルタイム最適化パック
- Microsoft Teams向け最適化

インストールと構成

展開の各ステップを開始する前に、参照されている記事を確認して、展開中に表示される内容と指定する内容について学習してください。

Citrix Virtual Apps and Desktops を展開するには、次の手順を使用します。

準備

インストール準備 を確認し、必要なタスクをすべて完了してください。

- 概念、機能、以前のリリースとの違い、システム要件、データベースに関する情報の検索場所。
- コアコンポーネントをどこにインストールするかを決定する際の考慮事項。
- 権限とActive Directoryの要件。
- 利用可能なインストーラー、ツール、インターフェイスに関する情報。

コアコンポーネントのインストール

Delivery Controller、Web Studio、Citrix Director、およびCitrix License Server をインストールします。Citrix StoreFront もインストールできます。詳細については、コアコンポーネントのインストール または コマンドラインを使用したインストール を参照してください。

サイトの作成

コアコンポーネントをインストールしてStudioを起動すると、サイトの作成 を求められます。

1つ以上のVirtual Delivery Agent (VDA) をインストールする

Windowsオペレーティングシステムを実行しているマシンにVDAをインストールします。これは、マスターイメージ上でも、各マシンに直接でも可能です。VDAのインストール または コマンドラインを使用したインストール を参照してください。Active Directory を介してVDAをインストールしたい場合は、サンプルスクリプト が提供されています。

Linuxオペレーティングシステムを搭載したマシンについては、Linux Virtual Delivery Agentのガイダンスに従ってください。

Remote PC Access展開の場合、各オフィスPCにシングルセッションOS用VDAをインストールします。コアVDAサービスのみが必要な場合は、スタンドアロンの`VDAWorkstationCoreSetup.exe`インストーラーと既存の電子ソフトウェア配布（ESD）方法を使用してください。（インストールの準備で利用可能なVDAインストーラーについて説明しています。）

オプションコンポーネントのインストール

Citrix Universal Print Serverを使用する予定がある場合は、そのサーバーコンポーネントをプリントサーバーにインストールしてください。コアコンポーネントのインストールまたはコマンドラインを使用したインストールを参照してください。

StoreFrontがSAMLアサーションなどの認証オプションを使用できるようにするには、Citrix Federated Authentication Serviceをインストールします。

エンドユーザーが自分のユーザーアカウントをより詳細に制御できるようにするには、Self-Service Password Resetをインストールします。

必要に応じて、追加のCitrixコンポーネントをCitrix Virtual Apps and Desktops展開に統合します。

- Citrix Provisioningは、マスターイメージをターゲットデバイスにストリーミングしてマシンをプロビジョニングするオプションコンポーネントです。
- Citrix Gatewayは、管理者に対してきめ細かなアプリケーションレベルのポリシーとアクション制御を提供し、アプリケーションとデータへのアクセスを保護するセキュアなアプリケーションアクセスソリューションです。
- Citrix SD-WANは、WANパフォーマンスを最適化するアプライアンスのセットです。

マシンカタログを作成する

Studioでサイトを作成した後、マシンカタログの作成に誘導されます。

カタログには、物理マシンまたは仮想マシン（VM）を含めることができます。仮想マシンはマスターイメージから作成できます。ハイパーバイザーまたはその他のサービスを使用してVMを提供する場合は、まずそのホスト上にマスターイメージを作成します。次に、カタログを作成する際に、VMの作成時に使用されるそのイメージを指定します。

デリバリーグループを作成する

Web Studioで最初のマシンカタログを作成した後、デリバリーグループの作成に誘導されます。

デリバリーグループは、選択したカタログ内のマシンにアクセスできるユーザーと、それらのユーザーが利用できるアプリケーションを指定します。

アプリケーショングループを作成する（オプション）

デリバリーグループを作成した後、オプションでアプリケーショングループを作成できます。アプリケーショングループは、異なるデリバリーグループ間で共有されるアプリケーションや、デリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションのために作成できます。

マシンID

各マシンには、コンピューターアカウントとも呼ばれる一意のマシンIDが必要です。マシンIDは、マシン内でローカルに作成および管理することも、オンプレミスのActive Directory (AD) やAzure ADなどのディレクトリで作成および管理することもできます。Citrix®は、Active Directoryに参加している、Azure Active Directoryに参加している、ハイブリッドAzure Active Directoryに参加している、またはドメインに参加していないマシンで仮想アプリケーションとデスクトップをホストすることをサポートしています。

マシンIDの種類

以下のマシンIDの種類がサポートされています。

マシンIDの種類	説明
AD参加済み	IDはオンプレミスのActive Directoryで作成および管理されます。プロビジョニングされたマシンは、割り当てられたマシンIDを使用してオンプレミスのActive Directoryに参加します。
ハイブリッドAzure AD参加済み	IDはオンプレミスのActive Directoryで作成され、Azure AD Connectを介してAzure ADと同期されます。プロビジョニングされたマシンはオンプレミスのActive Directoryに参加します。その後、マシンはハイブリッドAzure ADに参加します。ハイブリッドAzure AD参加済みVMをインポートする場合、そのVMはCitrix Virtual

マシンIDの種類	説明
	Apps and DesktopsによってActive Directory参加済みVMとして扱われます。
ドメイン非参加	IDはマシン内でローカルに作成および管理されます。Citrix Virtual Apps and DesktopsへのVMのインポートはサポートされていません。

サポートされる構成

各シナリオでサポートされる構成の詳細は以下のとおりです。

サポートされるインフラストラクチャ

マシンID	シトリックス バーチャルアプリおよびデスクトップ™	シトリックス ワークスペース™	シトリックス ストアフロント	シトリックス ゲートウェイ サービス	シトリックス ゲートウェイ
AD参加済み	はい	はい	はい	はい	はい
Azure AD参加済み	いいえ	はい	いいえ	はい	いいえ
ハイブリッド Azure AD 参加済み	はい	はい	はい	はい	はい
ドメイン非参加	はい	はい	いいえ	はい	いいえ

サポートされているワークスペース認証IDプロバイダー

マシンID	アジュール アクティブ ディレクトリ	アクティブ ディレクトリ	ACTIVE DIRECTORYとトークン	オクタ	SAML	シトリックス ゲートウェイ	アダプティブ認証
AD参加済み	はい	はい	はい	はい	はい	はい	はい

マシンID	アジュール アクティブ ディレクトリ	アクティブ ディレクトリ	ACTIVE DIRECTORYとトークン	オクタ	SAML	シトリックス ゲートウェイ	アダプティブ認証
Azure AD参加済み	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
ハイブリッド Azure AD参加済み	はい	はい	はい	はい	はい	はい	はい
ドメイン非参加	はい	はい	はい	はい	はい	はい	はい

Active Directoryに参加済み

認証と承認にはActive Directoryが必要です。Delivery Controllerとの通信の信頼性と機密性を保証するために、Active DirectoryのKerberosインフラストラクチャが使用されます。Kerberosの詳細については、Microsoftのドキュメントを参照してください。

システム要件の記事には、フォレストとドメインでサポートされている機能レベルが記載されています。Policy Modelingを使用するには、ドメインコントローラーがWindows Server 2003からWindows Server 2012 R2で実行されている必要があります。これはドメインの機能レベルには影響しません。

この製品は以下をサポートします。

- **単一のActive Directoryフォレスト内のドメインにユーザーアカウントとコンピューターアカウントが存在する展開。** ユーザーアカウントとコンピューターアカウントは、単一フォレスト内の任意のドメインに存在できます。この種類の展開では、すべてのドメイン機能レベルとフォレスト機能レベルがサポートされます。
- **コントローラーと仮想デスクトップのコンピューターアカウントを含むActive Directoryフォレストとは異なるActive Directoryフォレストにユーザーアカウントが存在する展開。** この種類の展開では、コントローラーと仮想デスクトップのコンピューターアカウントを含むドメインは、ユーザーアカウントを含むドメインを信頼する必要があります。フォレスト信頼または

外部信頼を使用できます。この種類の展開では、すべてのドメイン機能レベルとフォレスト機能レベルがサポートされます。

- **コントローラーのコンピューターアカウントが、仮想デスクトップのコンピューターアカウントを含む1つ以上の追加のActive Directoryフォレストとは異なるActive Directoryフォレストに存在する展開。** この種類の展開では、コントローラーのコンピューターアカウントを含むドメインと、仮想デスクトップのコンピューターアカウントを含むすべてのドメインとの間に双方向の信頼が存在する必要があります。この種類の展開では、コントローラーまたは仮想デスクトップのコンピューターアカウントを含むすべてのドメインが「Windows 2000 native」機能レベル以上である必要があります。すべてのフォレスト機能レベルがサポートされます。
- **書き込み可能なドメインコントローラー。** 読み取り専用ドメインコントローラーはサポートされていません。

オプションで、Virtual Delivery Agents (VDAs) はActive Directoryで公開されている情報を使用して、どのControllerに登録できるかを判断できます（検出）。この方法は主に下位互換性のためにサポートされており、VDAがControllerと同じActive Directoryフォレストにある場合にのみ利用できます。この検出方法の詳細については、Active Directory OUベースの検出およびCTX118976を参照してください。

> **注:**
>
> サイトが構成された後で、Delivery Controller™ のコンピューター名またはドメインメンバーシップを変更しないでください。

複数のActive Directoryフォレスト環境での展開

この情報は、XenDesktop 7.1およびXenApp 7.5の最小バージョンに適用されます。それ以前のバージョンのXenDesktopまたはXenAppには適用されません。

複数のフォレストを持つActive Directory環境で、一方向または双方向の信頼が確立されている場合、名前解決と登録のためにDNSフォワーダーまたは条件付きフォワーダーを使用できます。適切なActive Directoryユーザーがコンピューターアカウントを作成できるようにするには、Delegation of Controlウィザードを使用します。このウィザードの詳細については、Microsoftのドキュメントを参照してください。

フォレスト間に適切なDNSフォワーダーが設定されている場合、DNSインフラストラクチャに逆引きDNSゾーンは必要ありません。

VDAとControllerが別々のフォレストにある場合、Active DirectoryとNetBIOS名が異なっていても、`SupportMultipleForest`キーが必要です。レジストリキーをVDAとDelivery Controllerに追加するには、以下の情報を使用してください。

> **注意:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターの使用は、お客様ご自身の責任において行ってください。編集する前にレジストリをバックアップしてください。

> VDAで、以下を構成します: `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`。

- 名前: `SupportMultipleForest`
- 種類: `REG_DWORD`
- データ: `0x00000001 (1)`

すべてのDelivery Controllerで、以下を構成します: `HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest`。

- 名前: `SupportMultipleForest`
- 種類: `REG_DWORD`
- データ: `0x00000001 (1)`

DNS名前空間がActive Directoryのものと異なる場合、逆引きDNS構成が必要になる場合があります。

Kerberosよりも安全性の低いNTLM認証がVDAで意図せず有効になるのを避けるため、レジストリエントリが追加されました。このエントリは、後方互換性のために引き続き使用できる`SupportMultipleForest`エントリの代わりに使用できます。

VDAで、以下を構成します: `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`。

- 名前: `SupportMultipleForestDdcLookup`

- 種類: `REG_DWORD`
- データ: `0x00000001 (1)`

このレジストリキーは、双方向信頼の複数フォレスト環境でDDCルックアップを実行し、初期登録プロセス中にNTLMベースの認証を削除できるようにします。

セットアップ中に外部信頼が設定されている場合、`ListOfSIDs`レジストリキーが必要です。Active Directory FQDNがDNS FQDNと異なる場合、またはドメインコントローラーを含むドメインのNetBIOS名がActive Directory FQDNと異なる場合、`ListOfSIDs`レジストリキーも必要です。レジストリキーを追加するには、以下の情報を使用します:

VDAの場合、レジストリキー`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs`を見つけます。

- 名前: `ListOfSIDs`
- 種類: `REG_SZ`
- データ: コントローラーのセキュリティ識別子 (SID)。(SIDは`Get-BrokerController`コマンドレットの結果に含まれています。)

外部信頼が設定されている場合、VDAで次の変更を行います:

1. ファイル`Program Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config`を見つけます。
2. ファイルのバックアップコピーを作成します。
3. メモ帳などのテキスト編集プログラムでファイルを開きます。
4. テキスト`allowNtlm="false"`を見つけて、テキストを`allowNtlm="true"`に変更します。
5. ファイルを保存します。

`ListOfSIDs`レジストリキーを追加し、`brokeragent.exe.config`ファイルを編集した後、変更を適用するためにCitrix Desktop Serviceを再起動します。

次の表に、サポートされている信頼の種類を示します。

信頼の種類	推移性	方向	このリリースでサポートされているか
親と子	推移的	双方向	はい
ツリー ルート	推移的	双方向	はい

信頼の種類	推移性	方向	このリリースでサポートされているか
外部	非推移的	一方向または双方向	はい
フォレスト	推移的	一方向または双方向	はい
ショートカット	推移的	一方向または双方向	はい
レルム	推移的または非推移的	一方向または双方向	いいえ

複雑なActive Directory環境の詳細については、「CTX134971」を参照してください。

ドメインに参加していない

この記事では、「システム要件」(/ja-jp/citrix-virtual-apps-desktops/2311/system-requirements.html)セクションに記載されている要件に加えて、Citrix Virtual Apps and Desktops を使用してドメイン非参加カタログを作成するための要件について説明します。

要件

- コントロールプレーン: 「サポートされる構成」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-identities#supported-configurations)を参照
- VDAタイプ: シングルセッション (デスクトップのみ) またはマルチセッション (アプリおよびデスクトップ)
- VDAバージョン: 2311以降
- プロビジョニングタイプ: Machine Creation Services™ (MCS)、永続および非永続
- 割り当てタイプ: 専用およびプール
- ホスティングプラットフォーム: MCSでサポートされるすべてのプラットフォーム
- Rendezvous V2を有効にする必要があります

制限事項

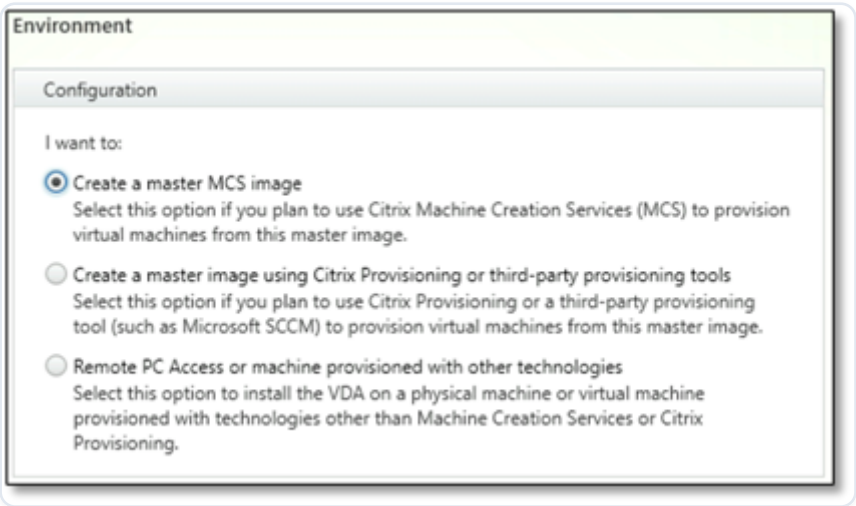
- サービス継続性はサポートされていません。
- マルチセッションのドメインに参加していないVDAを使用する場合、ローカルユーザーのプロファイルデータは保持されず、ログオフ時に削除されます。

VDAのインストールと構成

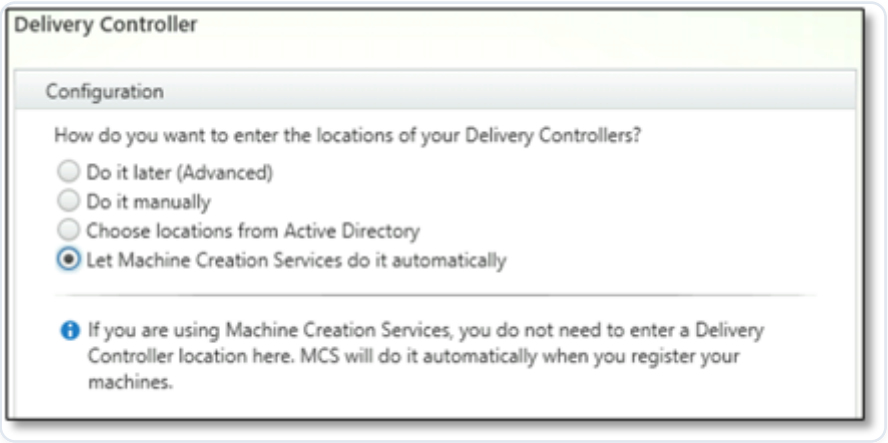
VDAをインストールする手順に従います。

1. インストールウィザードで以下のオプションを選択していることを確認してください。

   - 「環境」ページで、**「マスターMCSイメージを作成」**を選択します。



   - 「Delivery Controller™」ページで、**「Machine Creation Servicesに自動的に実行させる」**を選択します。



次のステップ

リソースの場所とホスティング接続が利用可能になったら、マシンカタログの作成に進みます。ドメインに参加していないマシンカタログの作成に関する詳細については、ドメインに参加していないカタログの作成を参照してください。

インストール準備

Citrix Virtual Apps and Desktops™ の展開は、以下のコンポーネントのインストールから始まります。このプロセスにより、ファイアウォール内のユーザーへのアプリケーションとデスクトップの配信が準備されます。

- 1つ以上のDelivery Controller
- シトリックス ディレクター
- シトリックス ストアフロント™
- シトリックス ライセンス サーバー
- 1つ以上のシトリックス バーチャル デリバリー エージェント (VDA)
- Universal Print Server、Federated Authentication Service、Self-Service Password Resetなどのオプションコンポーネントおよびテクノロジー

ファイアウォール外のユーザー向けには、Citrix Gatewayなどの追加コンポーネントをインストールして構成します。概要については、「Citrix Virtual Apps and DesktopsとCitrix Gatewayの統合」を参照してください。

注:

サーバーOSおよびワークステーションOSで、以下のMicrosoftの前提条件が満たされていることを確認してください。

- Microsoft **Volume Shadow Copy** および **Microsoft Software Shadow Copy Provider** サービスが実行されていること。詳細については、「Volume Shadow Copy Service」を参照してください。
- **MS-Defender** のバージョンは4.18.2105.5より高い必要があります。詳細については、「Microsoft Defender Antivirusのセキュリティインテリジェンスと製品の更新」を参照してください。

展開にWindows Serverワークロードが含まれる場合は、「Microsoft RDSライセンスサーバーを構成する」を参照してください。

製品ISOにあるフルプロダクトインストーラーを使用して、多くのコンポーネントやテクノロジーを展開できます。VDAをインストールするには、スタンドアロンVDAインストーラーを使用できます。スタンドアロンVDAインストーラーは、Citrixダウンロードサイトで入手できます。すべて

のインストーラーは、グラフィカルインターフェイスとコマンドラインインターフェイスを提供します。「インストーラー」を参照してください。

製品ISOには、Active Directory内のマシンにVDAをインストール、アップグレード、または削除するサンプルスクリプトが含まれています。これらのスクリプトは、Machine Creation Services (MCS) およびCitrix Provisioning (旧Provisioning Services) で使用されるイメージを管理するためにも使用できます。詳細については、スクリプトを使用したVDAのインストールを参照してください。

インストール前に確認する情報

- 技術概要: 製品とそのコンポーネントについて理解を深めるため。
- セキュリティ: 展開環境を計画する際。
- 既知の問題: このバージョンで発生する可能性のある問題。
- データベース: システムデータベースとその構成方法について学習します。Controllerのインストール中に、サイトデータベースとして使用するためにSQL Server Expressをインストールできます。ほとんどのデータベース情報は、コアコンポーネントのインストール後にサイトを作成する際に構成します。
- Remote PC Access: ユーザーがオフィスにある物理マシンにリモートでアクセスできるようにする環境を展開する場合。
- 接続とリソース: アプリケーションやデスクトップ用のVMをホストまたはプロビジョニングするためにハイパーバイザーまたはその他のサービスを使用している場合。最初の接続は、サイトを作成する際（コアコンポーネントのインストール後）に構成できます。それまでに仮想化環境をセットアップしてください。
- Microsoft System Center Configuration Manager: アプリケーションとデスクトップへのアクセスを管理するためにConfigMgrを使用している場合、またはRemote PC AccessでWake on LAN機能を使用している場合。
- **パブリッククラウドホスト接続:** ハイブリッドライツライセンスをお持ちの場合、パブリッククラウドへのホスト接続を作成できます。ハイブリッドライツライセンスに関する情報については、ハイブリッドライツの更新を参照してください。パブリッククラウドの資格とこの変更の理由に関する情報については、CTX270373を参照してください。

コンポーネントのインストール場所

サポートされているプラットフォーム、オペレーティングシステム、およびバージョンについては、システム要件を確認してください。コンポーネントの前提条件は、特に記載がない限り自動

的にインストールされます。サポートされているプラットフォームと前提条件については、Citrix StoreFrontおよびCitrix License Serverのドキュメントを参照してください。

コアコンポーネントは、同じサーバーまたは異なるサーバーにインストールできます。

- すべてのコアコンポーネントを1つのサーバーにインストールすることは、評価、テスト、または小規模な本番展開で機能します。
- 将来の拡張に対応するため、コンポーネントを異なるサーバーにインストールすることを検討してください。たとえば、Controllerをインストールしたサーバーとは別のマシンにStudioをインストールすると、サイトをリモートで管理できます。
- ほとんどの運用環境の展開では、コアコンポーネントを別々のサーバーにインストールすることをお勧めします。

  他のサーバーに他のコンポーネントをインストールする前に、Citrix License Serverとライセンスをインストールしてください。
- Server CoreOS（Delivery Controllerなど）にサポートされているコンポーネントをインストールするには、コマンドラインを使用する必要があります。このOSタイプにはグラフィカルインターフェイスがないため、Studioやその他のツールは別の場所にインストールし、それらをControllerサーバーにポイントしてください。

同じサーバーにDelivery Controller™とマルチセッションOS用VDAの両方をインストールできます。インストーラーを起動し、Delivery Controller（およびそのマシンにインストールしたいその他のコアコンポーネント）を選択します。その後、インストーラーを再度起動し、マルチセッションOS用の**Virtual Delivery Agent**を選択します。

各オペレーティングシステムに最新の更新プログラムが適用されていることを確認してください。

すべてのマシンのシステムクロックが同期されていることを確認してください。マシン間の通信を保護するKerberosインフラストラクチャには同期が必要です。

XenServerでは、仮想マシンが登録済みと表示されていても、電源状態が不明と表示される場合があります。この問題を解決するには、レジストリキー`HostTime`の値を編集して、ホストとの時刻同期を無効にします。

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

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

> **ヒント:**

> デフォルト値は`HostTime="UTC"`です。この値をUTC以外のもの（たとえば、`Local`）に変更します。この変更により、ホストとの時刻同期が実質的に無効になります。

> Windows 10シングルセッションマシン向けの最適化ガイダンスは、CTX216252で入手できます。

コンポーネントをインストールしない場所:

- Active Directoryドメインコントローラーには、いかなるコンポーネントもインストールしないでください。
- SQL Serverクラスタリングインストール、SQL Serverミラーリングインストール内のノード、またはHyper-Vを実行しているサーバーにControllerをインストールすることはサポートされていません。

この製品バージョンがサポートしていないWindows OSにVDAをインストールまたはアップグレードしようとすると、オプションを説明する記事へのメッセージが表示されます。

権限とActive Directoryの要件

コンポーネントをインストールするマシンでは、ドメインユーザーであり、ローカル管理者である必要があります。

スタンドアロンVDAインストーラーを使用するには、管理者特権があるか、**管理者として実行**を使用する必要があります。

インストールを開始する前に、Active Directory ドメインを構成してください。

- システム要件には、サポートされているActive Directoryの機能レベルが記載されています。Active Directoryへの参加には、詳細情報が含まれています。
- Active Directoryドメインサービスを実行しているドメインコントローラーが少なくとも1つ必要です。
- ドメインコントローラーには、Citrix Virtual Apps and Desktopsのコンポーネントをインストールしないでください。
- Studioで組織単位名を指定する際に、スラッシュ (/) を使用しないでください。

Citrix License Server のインストールに使用された Windows ユーザーアカウントは、委任管理のフル管理者として自動的に構成されます。

詳細情報:

- セキュリティのベストプラクティス
- 委任管理
- Active Directory構成に関するMicrosoftドキュメント

インストールのガイダンス、考慮事項、およびベストプラクティス

いずれかのコンポーネントのインストール中

- フルプロダクトメディアから Delivery Controller、Studio、License Server、または Director をインストールまたはアップグレードする際に、Citrix インストーラーがマシン上の以前の Windows インストールからの再起動が保留中であることを検出すると、インストーラーは終了/リターンコード 9 で停止します。マシンの再起動を促されます。

  これは Citrix による強制的な再起動ではありません。マシンに以前インストールされた他のコンポーネントが原因です。この状況が発生した場合は、マシンを再起動してから、Citrix インストーラーを再度起動してください。

  コマンドラインインターフェイスを使用する場合、コマンドに `/no_pending_reboot_check` オプションを含めることで、保留中の再起動のチェックを回避できます。
- 通常、コンポーネントに前提条件がある場合、インストーラーはそれらが存在しない場合に展開します。一部の前提条件では、マシンの再起動が必要になる場合があります。
- インストール前、インストール中、インストール後にオブジェクトを作成するときは、各オブジェクトに一意の名前を指定してください。たとえば、ネットワーク、グループ、カタログ、リソースには一意の名前を付けてください。
- コンポーネントが正常にインストールされなかった場合、インストールはエラーメッセージとともに停止します。正常にインストールされたコンポーネントは保持されます。それらを再インストールする必要はありません。
- コンポーネントをインストール（またはアップグレード）すると、Citrix Analytics が自動的に収集されます。デフォルトでは、インストールが完了するとそのデータは自動的にCitrixにアップロードされます。また、コンポーネントをインストールすると、匿名データをアップロードするCitrixカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。

  インストール中に、メンテナンスとトラブルシューティングのための診断情報を収集する他のCitrixテクノロジーに参加することも選択できます。これらのプログラムの詳細については、「Citrix Insight Services」を参照してください。
- Studioをインストール（またはアップグレード）すると、Google Analyticsが自動的に収集され（後でアップロードされ）ます。Studioのインストール後、レジストリキー `HKLM\Software\Citrix\DesktopStudio\GAEnabled` を使用してこの設定を変更できます。

値が**1**の場合は収集とアップロードが有効になり、**0**の場合は収集とアップロードが無効になります。

- VDAのインストールが失敗した場合、MSIアナライザーは失敗したMSIログを解析し、正確なエラーコードを表示します。既知の問題である場合は、アナライザーがCTX記事を提案します。アナライザーは、失敗エラーコードに関する匿名化されたデータも収集します。このデータは、CEIPによって収集された他のデータとともに含まれます。CEIPへの登録を終了すると、収集されたMSIアナライザーデータはCitrixに送信されなくなります。

VDAのインストール中

- Windows向けCitrix Workspace™アプリは利用可能ですが、VDAをインストールする際にはデフォルトではインストールされません。ユーザーまたはご自身で、Citrix Webサイトから Windows向けCitrix Workspaceアプリやその他のCitrix Workspaceアプリをダウンロード、インストール（およびアップグレード）できます。または、StoreFrontサーバーからこれらのCitrix Workspaceアプリを利用可能にすることもできます。StoreFrontのドキュメントを参照してください。
- Microsoft Print Spoolerサービスは有効にする必要があります。このサービスが無効になっている場合、VDAを正常にインストールすることはできません。
- ほとんどのサポートされているWindowsエディションには、Microsoft Media Foundationがすでにインストールされています。マシンにMedia Foundationがない場合（Nエディションなど）、いくつかのマルチメディア機能はインストールされず、動作しません。
  - Windows Mediaリダイレクト
  - HTML5ビデオのリダイレクト
  - HDX™ RealTimeウェブカメラのリダイレクト

  制限を承諾するか、Media Foundationのインストール後にVDAのインストールを終了して後で再起動することができます。グラフィカルインターフェイスでは、この選択肢はメッセージで表示されます。コマンドラインでは、`/no_mediafoundation_ack`オプションを使用して制限を承諾できます。
- VDAをインストールすると、**Direct Access Users**という新しいローカルユーザーグループが自動的に作成されます。シングルセッションOS用VDAでは、このグループはRDP接続にのみ適用されます。マルチセッションOS用VDAでは、このグループはICA®およびRDP接続に適用されます。
- VDAは、通信するための有効なControllerアドレスを持っている必要があります。そうでない場合、セッションを確立できません。Controllerアドレスは、VDAのインストール時または後

で指定できます。これを行う必要があることを忘れないでください。詳細については、VDA登録を参照してください。

VDAインストール後およびインストール中の再起動

VDAインストールの最後に再起動が必要です。その再起動は、デフォルトで自動的に行われます。

VDAをバージョン7.17（またはそれ以降のサポートされているバージョン）にアップグレードする場合、アップグレード中に再起動が発生します。これは回避できません。

VDAのインストール中に必要な再起動の回数を最小限に抑えるには：

- VDAのインストールを開始する前に、サポートされている.NET Frameworkバージョンがインストールされていることを確認してください。
- WindowsマルチセッションOSマシンでは、VDAをインストールする前に、RDSロールサービスをインストールして有効にしてください。

VDAをインストールする前にこれらの前提条件をインストールしない場合：

- グラフィカルインターフェイスまたは`/noreboot`オプションなしでコマンドラインインターフェイスを使用している場合、前提条件のインストール後にマシンは自動的に再起動します。
- `/noreboot`オプションを使用してコマンドラインインターフェイスを使用している場合、再起動を開始する必要があります。

VDAをバージョン7.17以降のサポートされているバージョンにアップグレードする場合、アップグレード中に再起動が発生します。これは回避できません。

インストールまたはアップグレードの失敗時の復元

> **注:**
>
> この機能は、シングルセッションおよびマルチセッションVDAで利用できます。
>
> シングルセッションVDAのインストールまたはアップグレードが失敗し、「障害時の復元」機能が有効になっている場合、マシンはインストールまたはアップグレードが開始される前に設定された復元ポイントに戻されます。

マルチセッションVDAのインストールまたはアップグレードが失敗し、「失敗時の復元」機能が有効になっている場合、マシンはインストールまたはアップグレードが開始される前に実行されたバックアップに戻されます。

この機能が有効な状態でシングルセッションVDAのインストールまたはアップグレードが開始されると、インストーラーは実際のインストールまたはアップグレードを開始する前にシステム復元ポイントを作成します。VDAのインストールまたはアップグレードが失敗した場合、マシンは復元ポイントの状態に戻されます。`%temp%/Citrix`フォルダーには、展開ログと復元に関するその他の情報が含まれています。

この機能を有効にしてマルチセッションVDAのインストールまたはアップグレードを開始すると、インストーラーは実際のインストールまたはアップグレードを開始する前にサーバーバックアップを作成します。VDAのインストールまたはアップグレードが失敗した場合、マシンはバックアップ状態に戻されます。`%temp%/Citrix`フォルダーには、展開ログと復元に関するその他の情報が含まれています。サーバーバックアップの作成にかかる時間は、必要なバックアップのサイズとサーバーで利用可能なリソースの量に基づきます。バックアップは *C:\WindowsImageBackup\servername* に保存されます。

デフォルトでは、この機能は無効になっています。

この機能を有効にする予定がある場合は、GPO設定 (`Computer Configuration > Administrative Templates > System > System Restore`) によってシステム復元が無効になっていないことを確認してください。

> **注:**
>
> このGPO設定は、マルチセッションVDAの復元には適用されません。

> シングルセッションまたはマルチセッションVDAをインストールまたはアップグレードする際にこの機能を有効にするには：

- VDAインストーラーのグラフィカルインターフェイスを使用する場合（**Autostart**または復元オプションやサイレントオプションなしで`XenDesktopVDASetup.exe`コマンドを使用する場合など）は、**Summary**ページで**Enable automatic restore if update fails**チェックボックスをオンにします。

  インストール/アップグレードが正常に完了した場合、復元ポイント/バックアップは使用されませんが、保持されます。
- コマンドラインを使用して、`/enablerestore` または `/enablerestorecleanup` オプションのいずれかで VDA インストーラーを実行します。

- `/enablerestorecleanup`オプションを使用し、インストール/アップグレードが正常に完了した場合、復元ポイント/サーバーバックアップは自動的に削除されます。
- `/enablerestore`オプションを使用し、インストール/アップグレードが正常に完了した場合、復元ポイントは使用されませんが、保持されます。

インストーラー

フルプロダクトインストーラー

ISO に含まれるフルプロダクトインストーラーを使用すると、次のことができます。

- コアコンポーネント（Delivery Controller、Studio、Director、License Server）のインストール、アップグレード、または削除。
- StoreFront のインストールまたはアップグレード。
- シングルセッションまたはマルチセッションオペレーティングシステム用の Windows VDA のインストールまたはアップグレード。
- プリントサーバーに Universal Print Server `UpsServer` コンポーネントをインストールします。
- フェデレーション認証サービス をインストールします。
- Session Recording をインストールします。
- Workspace Environment Management をインストールします。

> **注:**
>
> Workspace Environment Management™ Agent インストーラーはローカライズされていません。英語のみで利用可能です。

1人のユーザー（Web開発など）向けにマルチセッションOSからデスクトップを配信するには、フルプロダクトインストーラーのコマンドラインインターフェイスを使用します。詳細については、「Server VDI」を参照してください。

スタンドアロン VDA インストーラー

スタンドアロンVDAインストーラーは、Citrixダウンロードページで入手できます。（製品インストールメディアからは入手できません。）スタンドアロンVDAインストーラーは、フルプロダクトISOよりもはるかに小さいです。これらは、次のような展開に容易に対応できます。

- ローカルにステージングまたはコピーされた電子ソフトウェア配布 (ESD) パッケージを使用する
- 物理マシンを使用する
- リモートオフィスがある

デフォルトでは、自己解凍型スタンドアロンVDAのファイルは**Temp**フォルダーに抽出されます。フルプロダクトインストーラーを使用する場合よりも、**Temp**フォルダーに抽出する場合の方が、マシンにより多くのディスク容量が必要です。ただし、**Temp**フォルダーに抽出されたファイルは、インストール完了後に自動的に削除されます。または、絶対パスを指定して`/extract`コマンドを使用することもできます。

3つのスタンドアロンVDAインストーラーをダウンロードできます。

VDAServerSetup.exe:

マルチセッションOS用のVDAをインストールします。フルプロダクトインストーラーで利用可能なマルチセッションOS用のVDAオプションをすべてサポートしています。

VDAWorkstationSetup.exe:

シングルセッションOS用のVDAをインストールします。フルプロダクトインストーラーで利用可能なシングルセッションOS用のVDAオプションをすべてサポートしています。

VDAWorkstationCoreSetup.exe:

Remote PC Access展開またはコアVDIインストールに最適化されたシングルセッションOS用のVDAをインストールします。Remote PC Accessは物理マシンを使用します。コアVDIインストールは、イメージとして使用されていないVMです。このような展開のVDA接続に必要なコアサービスのみをインストールします。したがって、フルプロダクトインストーラーまたは`VDAWorkstationSetup.exe`インストーラーで有効なオプションのサブセットのみをサポートします。

このインストーラーは、次の目的で使用されるコンポーネントをインストールまたは含んでいません。

- アップブイ。
- プロファイル管理。Citrix Profile Managementをインストールから除外すると、Citrix Directorの表示に影響します。詳細については、「VDAのインストール」を参照してください。
- マシンIDサービス。
- Citrixサポートツール。

- Windows 用 シトリックス ファイルズ。
- アウトルック用 Citrix Files。

`VDAWorkstationCoreSetup.exe`インストーラーは、Windows向けCitrix Workspaceアプリをインストールまたは含んでいません。

`VDAWorkstationCoreSetup.exe`を使用することは、フルプロダクトインストーラーまたは`VDAWorkstationSetup`インストーラーを使用してシングルセッションOS VDAをインストールし、以下のいずれかを実行することと同じです。

- グラフィカルインターフェイスでは: **環境**ページでRemote PC Accessオプションを選択します。
- コマンドラインインターフェイスでは: `/remotepc`オプションを指定します。
- コマンドラインインターフェイスでは: `/components vda`と、有効な追加コンポーネント名をすべてリストする`/exclude`オプションを指定します。

省略されたコンポーネント/機能は、後でフルプロダクトインストーラーを実行してインストールできます。この操作により、不足しているすべてのコンポーネントをインストールできます。

`VDAWorkstationCoreSetup.exe` インストーラーは、Browser Content Redirection MSI を自動的にインストールします。この自動インストールは、VDA リリース 2003 以降のサポート対象リリースに適用されます。

Citrix インストールリターンコード

インストールログには、コンポーネントインストールの結果が Microsoft の値ではなく、Citrix のリターンコードとして含まれています。

- 0 = 成功
- 1 = 失敗
- 2 = 部分的な成功
- 3 = 部分的な成功と再起動が必要
- 4 = 失敗と再起動が必要
- 5 = ユーザーによってキャンセルされました
- 6 = コマンドライン引数が不足しています
- 7 = 新しいバージョンが見つかりました
- 8 = 成功と再起動が必要

- 9 = ファイルロック再起動
- 10 = 中止
- 11 = メディア失敗
- 12 = ライセンス失敗
- 13 = 事前チェック失敗
- 14 = 再起動保留チェック中止
- -1 = 終了

たとえば、Microsoft System Center Configuration Managerなどのツールを使用する場合、インストールログに終了コード3が含まれていると、スクリプトによるVDAインストールが失敗したように見えることがあります。これは、VDAインストーラーが、ユーザーが開始する必要のある再起動（たとえば、サーバーへのRDSロールの前提条件のインストール後など）を待機している場合に発生する可能性があります。VDAのインストールは、すべての前提条件と選択されたコンポーネントがインストールされ、インストール後にマシンが再起動された場合にのみ成功と見なされます。

あるいは、インストールをCMDスクリプト（Microsoftの終了コードを返す）でラップするか、Configuration Managerパッケージの成功コードを変更することもできます。

Windows Serverワークロード用のMicrosoft RDSライセンスサーバーを構成する

この製品は、Windows 2016などのWindows Serverワークロードを提供する場合に、Windows Serverリモートセッション機能にアクセスします。これには通常、リモートデスクトップサービスクライアントアクセスライセンス (RDS CAL) が必要です。VDAは、RDS CALを要求するためにRDSライセンスサーバーに接続できる必要があります。ライセンスサーバーをインストールしてアクティブ化します。詳細については、Microsoftドキュメント「リモートデスクトップサービスライセンスサーバーをアクティブ化する」を参照してください。概念実証環境では、Microsoftが提供する猶予期間を使用できます。

この方法を使用すると、このサービスにライセンスサーバー設定を適用させることができます。イメージ上のRDSコンソールで、ライセンスサーバーとユーザーごとのモードを構成できます。Microsoftグループポリシー設定を使用してライセンスサーバーを構成することもできます。詳細については、Microsoftドキュメント「クライアントアクセスライセンス (CAL) を使用してRDS展開をライセンスする」を参照してください。

グループポリシー設定を使用してRDSライセンスサーバーを構成するには:

1. 利用可能なマシンにリモートデスクトップサービスライセンスサーバーをインストールします。そのマシンは常に利用可能である必要があります。Citrix製品のワークロードは、このライセンスサーバーに到達できる必要があります。
2. Microsoftグループポリシーを使用して、ライセンスサーバーのアドレスとユーザーごとのライセンスモードを指定します。詳細については、Microsoftドキュメント「RDセッションホストサーバーのリモートデスクトップライセンスモードを指定する」を参照してください。

Windows 10ワークロードには、適切なWindows 10ライセンスのアクティブ化が必要です。Windows 10ワークロードをアクティブ化するには、Microsoftのドキュメントに従うことをお勧めします。

詳細情報

特定のホストタイプのリソースの場所を設定する場合：

- AWSクラウド環境
- XenServer仮想化環境
- Google Cloud環境
- Microsoft Azure Resource Manager クラウド環境(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare/azure.html)
- マイクロソフト システムセンター コンフィギュレーションマネージャー 環境(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare/configmgr.html)
- Microsoft System Center バーチャル マシン マネージャー 仮想化環境(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare/msscvmm.html)
- Nutanix 仮想化環境(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare/nutanix.html)
- Nutanix クラウドおよびパートナーソリューション(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare/nutanix-cloud-patrner-solutions.html)
- VMware 仮想化環境(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare/vmware.html)
- VMware クラウドおよびパートナーソリューション(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare/vmware-cloud-partner-solutions.html)

AWSクラウド環境

この記事では、Citrix Virtual Apps and Desktops で使用できるリソースの場所として AWS アカウントを設定する方法を説明します。このリソースの場所には、概念実証や、複数のアベイラビリ

ティゾーンにリソースを分散させる必要のないその他の展開に最適な、基本的なコンポーネントセットが含まれています。これらのタスクを完了すると、VDA のインストール、マシンのプロビジョニング、マシンカタログの作成、およびデリバリーグループの作成を行うことができます。

この記事のタスクを完了すると、リソースロケーションには次のコンポーネントが含まれます。

- 単一のアベイラビリティゾーン内にパブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド (VPC)。
- VPC のプライベートサブネットに配置され、Active Directory ドメインコントローラーと DNS サーバーの両方として実行されるインスタンス。
- VPC のパブリックサブネットで踏み台ホストとして機能するインスタンス。このインスタンスは、管理目的でプライベートサブネット内のインスタンスへの RDP 接続を開始するために使用されます。リソースロケーションの設定が完了したら、このインスタンスをシャットダウンして、簡単にアクセスできないようにすることができます。VDA インスタンスなど、プライベートサブネット内の他のインスタンスを管理する必要がある場合は、踏み台ホストインスタンスを再起動できます。

タスクの概要

パブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド (VPC) をセットアップします。このタスクを完了すると、AWS はパブリックサブネットに Elastic IP アドレスを持つ NAT ゲートウェイを展開します。このアクションにより、プライベートサブネット内のインスタンスがインターネットにアクセスできるようになります。パブリックサブネット内のインスタンスは受信パブリックトラフィックにアクセスできますが、プライベートサブネット内のインスタンスはアクセスできません。

セキュリティグループを構成します。セキュリティグループは、VPC 内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。また、これらのセキュリティグループを VPC 内の各インスタンスに関連付けます。

DHCPオプションセットを作成します。Amazon VPCでは、DHCPおよびDNSサービスがデフォルトで提供されており、Active Directoryドメインコントローラーでの DNSの構成方法に影響します。AmazonのDHCPは無効にできず、AmazonのDNSはパブリックDNS解決にのみ使用でき、Active Directory名解決には使用できません。DHCPを介してインスタンスに渡されるドメインとネームサーバーを指定するには、DHCPオプションセットを作成します。このセットは、Active Directoryドメインサフィックスを割り当て、VPC内のすべてのインスタンスのDNSサーバーを指定します。インスタンスがドメインに参加したときにホスト（A）および逆引き（PTR）レコード

が自動的に登録されるようにするには、プライベートサブネットに追加する各インスタンスのネットワークアダプタープロパティを構成します。

踏み台ホストとドメインコントローラーをVPCに追加します。踏み台ホストを介して、プライベートサブネット内のインスタンスにログオンし、ドメインを設定してインスタンスをドメインに参加させることができます。

タスク1：VPCをセットアップする

1. AWS マネジメントコンソールから、**VPC** を選択します。
2. VPC ダッシュボードから、**VPC の作成**を選択します。
3. **VPC など**を選択します。
4. 「NATゲートウェイ ($)」の下で、「**1 AZ内**」または「**AZごとに1つ**」を選択します。
5. 「DNSオプション」の下で、「**DNSホスト名を有効にする**」を選択したままにします。
6. 「**VPCを作成**」を選択します。AWSは、パブリックサブネットとプライベートサブネット、インターネットゲートウェイ、ルートテーブル、およびデフォルトのセキュリティグループを作成します。

タスク 2: セキュリティグループの構成

このタスクでは、VPC 用に次のセキュリティグループを作成および構成します:

- パブリックサブネット内のインスタンスに関連付けるパブリックセキュリティグループ。
- プライベートサブネット内のインスタンスに関連付けるプライベートセキュリティグループ。

セキュリティグループを作成するには:

1. VPC ダッシュボードで、「**Security Groups**」を選択します。
2. パブリックセキュリティグループ用のセキュリティグループを作成します。「**Create Security Group**」を選択し、グループの名前タグと説明を入力します。VPC で、以前に作成した VPC を選択します。「**Yes, Create**」を選択します。

パブリックセキュリティグループの構成

1. セキュリティグループのリストから、パブリックセキュリティグループを選択します。
2. **［Inbound Rules］**タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (セッションの信頼性)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. 完了したら、**保存**を選択します。
4. **アウトバウンドルール**タブを選択し、**編集**を選択して、次のルールを作成します。

タイプ	宛先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0

5. 完了したら、**保存**を選択します。

プライベートセキュリティグループを構成する

1. セキュリティグループリストから、プライベートセキュリティグループを選択します。
2. パブリックセキュリティグループからのトラフィックを設定していない場合は、TCPポートを設定する必要があります。**Inbound Rules**タブを選択し、**Edit**を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	パブリックセキュリティグループを選択します。
TCP 53 (DNS)	パブリックセキュリティグループを選択します。
UDP 53 (DNS)	パブリックセキュリティグループを選択します。
80 (HTTP)	「パブリックセキュリティグループ」を選択します。
TCP 135	「パブリックセキュリティグループ」を選択します。
TCP 389	「パブリックセキュリティグループ」を選択します。
UDP 389	「パブリックセキュリティグループ」を選択します。
443 (HTTPS)	「パブリックセキュリティグループ」を選択します。
TCP 1494 (ICA/HDX)	「パブリックセキュリティグループ」を選択します。
TCP 2598 (セッションの信頼性)	「パブリックセキュリティグループ」を選択します。
3389 (RDP)	「パブリックセキュリティグループ」を選択します。
TCP 49152–65535	パブリックセキュリティグループを選択します。

3. 完了したら、 を選択します。
4. タブを選択し、 を選択して次のルールを作成します。

タイプ	宛先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. 完了したら、 を選択します。

タスク 3: インスタンスの起動

次の手順を実行して、2つのEC2インスタンスを作成し、Amazonが生成するデフォルトの管理者パスワードを復号します。

1. AWS管理コンソールから、**EC2**を選択します。
2. EC2ダッシュボードから、**インスタンスの起動**を選択します。
3. Windows Serverマシンイメージとインスタンスタイプを選択します。
4. **［Configure Instance Details］**ページで、インスタンスの名前を入力し、以前に設定したVPCを選択します。
5. **サブネット**で、各インスタンスについて次の選択を行います。
   - Bastionホスト：パブリックサブネットを選択します
   - ドメインコントローラー：プライベートサブネットを選択します
6. **パブリック IP アドレスの自動割り当て**で、各インスタンスに対して以下の選択を行います。
   - 踏み台ホスト：**［Enable］**を選択します。
   - ドメインコントローラー：**［Use default setting］ または ［Disable］**を選択します。
7. **ネットワークインターフェース**で、ドメインコントローラーのプライベートサブネットのIP範囲内のプライマリIPアドレスを入力します。
8. 必要に応じて、**ストレージの追加**ページでディスクサイズを変更します。
9. **インスタンスのタグ付け**ページで、各インスタンスにわかりやすい名前を入力します。

10. 「**セキュリティグループの設定**」ページで、「**既存のセキュリティグループを選択**」を選択し、各インスタンスについて次の選択を行います。
    - バスティオンホスト: パブリックセキュリティグループを選択します。
    - ドメインコントローラー: プライベートセキュリティグループを選択します。
11. 選択内容を確認し、「**起動**」を選択します。
12. 新しいキーペアを作成するか、既存のキーペアを選択します。新しいキーペアを作成する場合は、秘密鍵 (.pem) ファイルをダウンロードし、安全な場所に保管してください。インスタンスのデフォルトの管理者パスワードを取得する際には、秘密鍵を提供する必要があります。
13. 「**インスタンスの起動**」を選択します。「**インスタンスの表示**」を選択して、インスタンスのリストを表示します。新しく起動したインスタンスがすべてのステータスチェックに合格するまで待ってからアクセスしてください。
14. 各インスタンスのデフォルトの管理者パスワードを取得します。
    a. インスタンスリストからインスタンスを選択し、「**接続**」を選択します。
    b. 「**RDPクライアント**」タブに移動し、「**パスワードの取得**」を選択し、プロンプトが表示されたら秘密鍵 (`.pem`) ファイルをアップロードします。
    c. 「**パスワードの復号**」を選択して、人間が読めるパスワードを取得します。AWSはデフォルトのパスワードを表示します。
15. ステップ2から手順を繰り返し、2つのインスタンスを作成します。
    - パブリックサブネットに1つの踏み台ホストインスタンス
    - ドメインコントローラーとして使用するプライベートサブネット内のインスタンスを1つ。

タスク4：DHCPオプションセットを作成する

1. VPCダッシュボードから、「**DHCPオプションセット**」を選択します。
2. 次の情報を入力します。
    - 名前タグ: セットのわかりやすい名前を入力します。
    - ドメイン名: ドメインコントローラーインスタンスを構成するときに使用する完全修飾ドメイン名を入力します。
    - ドメインネームサーバー: ドメインコントローラーインスタンスに割り当てたプライベートIPアドレスと、コンマで区切られた文字列 **AmazonProvidedDNS** を入力します。
    - NTPサーバー: このフィールドは空白のままにします。

- NetBIOSネームサーバー: ドメインコントローラーインスタンスのプライベートIPアドレスを入力します。
- NetBIOSノードタイプ: **2** と入力します。

3. **はい、作成します。** を選択します。
4. 新しいセットをVPCに関連付けます。

   a. VPCダッシュボードから、**Your VPCs** を選択し、以前に設定したVPCを選択します。

   b. **アクション > DHCPオプションセットの編集** を選択します。

   c. プロンプトが表示されたら、作成した新しいセットを選択し、**保存** を選択します。

タスク5：インスタンスを構成する

1. RDPクライアントを使用して、踏み台ホストインスタンスのパブリックIPアドレスに接続します。プロンプトが表示されたら、管理者アカウントの資格情報を入力します。
2. 踏み台ホストインスタンスからリモートデスクトップ接続を起動し、構成するインスタンスのプライベートIPアドレスに接続します。プロンプトが表示されたら、インスタンスの管理者資格情報を入力します。
3. プライベートサブネット内のすべてのインスタンスについて、DNS設定を構成します。

   a. **スタート > コントロールパネル > ネットワークとインターネット > ネットワークと共有センター > アダプターの設定の変更**を選択します。表示されているネットワーク接続をダブルクリックします。

   b. **プロパティ > インターネットプロトコルバージョン4 (TCP/IPv4) > プロパティ**を選択します。

   c. 「**詳細設定 > DNS**」を選択します。次の設定が有効になっていることを確認し、「**OK**」を選択します。

      - この接続のアドレスをDNSに登録する
      - この接続のDNSサフィックスをDNS登録で使用する

4. ドメインコントローラーを構成するには:

   a. Server Manager を使用して、Active Directory ドメインサービス の役割をすべてのデフォルト機能とともに追加します。

   b. インスタンスをドメインコントローラーに昇格させます。昇格中にDNSを有効にし、DHCPオプションセットを作成したときに指定したドメイン名を使用します。プロンプトが表示されたらインスタンスを再起動します。

次のステップ

- コアコンポーネントをインストールする
- VDAのインストール
- サイトを作成する
- AWS での接続の作成と管理については、AWS への接続を参照してください。

詳細情報

- 接続とリソースを作成および管理する
- マシンカタログを作成する

XenServer® 仮想化環境

XenServer は、集中的なワークロード向けに高精細なユーザーエクスペリエンスを保証し、運用管理を簡素化します。

XenServer をセットアップするには、「インストール準備」を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- XenServer で接続を作成および管理するには、「XenServer への接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Google Cloud環境

Citrix Virtual Apps and Desktops™ を使用すると、Google Cloud 上でマシンをプロビジョニングおよび管理できます。

要件

- Citrix Cloud™ アカウント。この記事で説明されている機能は、Citrix Cloud でのみ利用できます。

- Google Cloud プロジェクト。このプロジェクトには、マシンカタログに関連付けられているすべてのコンピューティングリソースが保存されます。既存のプロジェクトでも新規のプロジェクトでもかまいません。
- Google Cloud プロジェクトで4つのAPIを有効にします。詳細については、「Google Cloud APIを有効にする」を参照してください。
- Google Cloud サービスアカウント。サービスアカウントはGoogle Cloudに対して認証を行い、プロジェクトへのアクセスを可能にします。詳細については、「サービスアカウントの構成と更新」を参照してください。
- Googleプライベートアクセスを有効にします。詳細については、「プライベートGoogleアクセスを有効にする」を参照してください。

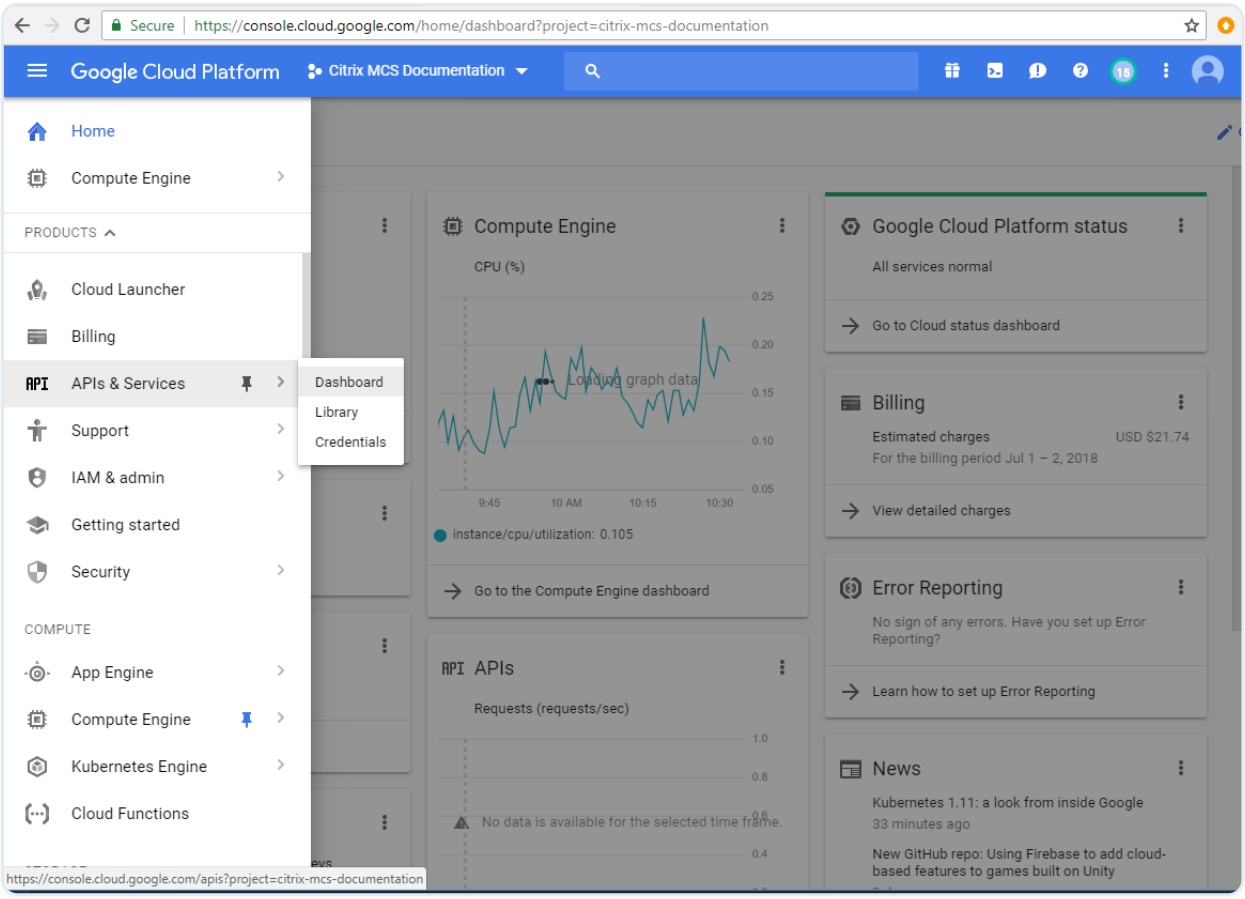
Google Cloud APIを有効にする

Web Studio を介して Google Cloud 機能を使用するには、Google Cloud プロジェクトで次の API を有効にします。

- コンピューティング エンジン API
- Cloud Resource Manager API (クラウド リソース マネージャー API)
- ID およびアクセス管理 (IAM) API
- Cloud Build API (クラウドビルド API)
- クラウドキー管理サービス (KMS)

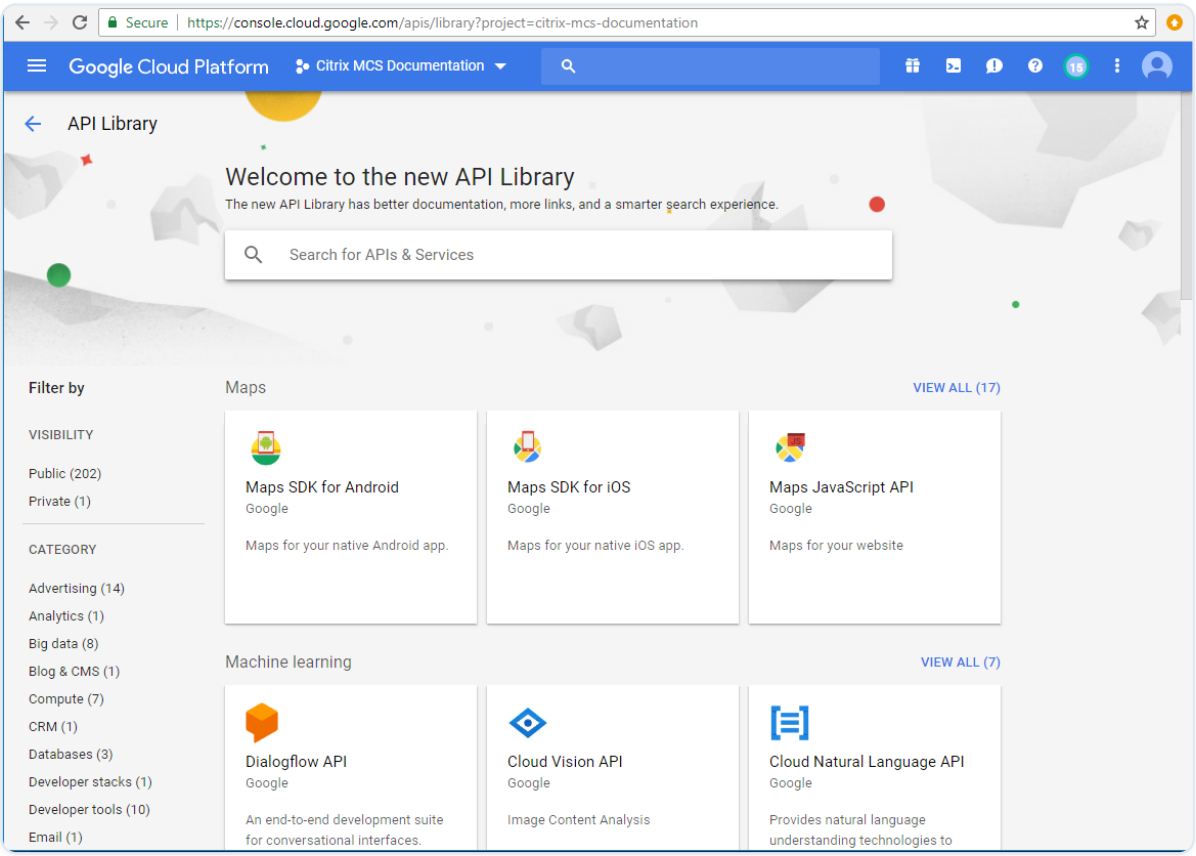
Google Cloudコンソールから、次の手順を実行します。

1. 左上のメニューで、**「APIとサービス」>「ダッシュボード」**を選択します。



2. **ダッシュボード**画面で、Compute Engine APIが有効になっていることを確認します。 有効になっていない場合は、次の手順に従ってください。

   a. 「**APIとサービス > ライブラリ**」に移動します。



b. 検索ボックスに「*Compute Engine*」と入力します。

c. 検索結果から「**Compute Engine API**」を選択します。

d. 「**Compute Engine API**」ページで、「**有効にする**」を選択します。

3. Cloud Resource Manager APIを有効にします。

a. 「**APIとサービス > ライブラリ**」に移動します。

b. 検索ボックスに「*Cloud Resource Manager*」と入力します。

c. 検索結果から「**Cloud Resource Manager API**」を選択します。

d. 「**Cloud Resource Manager API**」ページで、「**有効にする**」を選択します。APIのステータスが表示されます。

4. 同様に、**Identity and Access Management (IAM) API**と**Cloud Build API**を有効にします。

Google Cloud Shell を使用して API を有効にすることもできます。これを行うには、次の手順に従います。

1. Googleコンソールを開き、Cloud Shellをロードします。
2. Cloud Shellで次の4つのコマンドを実行します。

- gcloud サービスを有効にする compute.googleapis.com

- gcloud サービスを有効にする cloudresourcemanager.googleapis.com
- gcloud services iam.googleapis.com を有効にする
- gcloud services cloudbuild.googleapis.com を有効にする

3. Cloud Shellがプロンプトを表示した場合、「**承認**」をクリックします。

サービスアカウントの構成と更新

> **注：**
>
> GCP は、Cloud Build Service のデフォルトの動作とサービスアカウントの使用に関して、April 29, 2024 以降に変更を導入します。詳細については、「Cloud Build Service Account Change」を参照してください。April 29, 2024 より前に Cloud Build API が有効になっている既存の Google プロジェクトは、この変更の影響を受けません。ただし、April 29 以降も既存の Cloud Build Service の動作を維持したい場合は、Cloud Build API を有効にする前に、組織ポリシーを作成または適用して制約の適用を無効にすることができます。その結果、以下のコンテンツは「Before April 29, 2024」と「After April 29, 2024」の2つに分かれています。新しい組織ポリシーを設定する場合は、「Before April 29, 2024」のセクションに従ってください。

April 29, 2024 以前

Citrix Cloudは、Google Cloudプロジェクト内で3つの個別のサービスアカウントを使用します。

- *Citrix Cloud Service Account*：このサービスアカウントにより、Citrix Cloud は Google プロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloud によって生成されたキーを使用して Google Cloud に対して認証を行います。

  このサービスアカウントは、ここに記載されているとおり手動で作成する必要があります。詳細については、「Citrix Cloud Service Account の作成」を参照してください。

  このサービスアカウントはメールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`.
- *Cloud Build Service Account*: このサービスアカウントは、Google Cloud API を有効にするで言及されているすべてのAPIを有効にすると、自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud**コンソールで**IAM と管理 > IAM**に移動し、**Google 提供のロール付与を含める**チェックボックスを選択します。

このサービスアカウントは、**プロジェクトID**と**cloudbuild**という単語で始まるメールアドレスで識別できます。例: `<project-id>@cloudbuild.gserviceaccount.com`

サービスアカウントに以下のロールが付与されていることを確認します。ロールを追加する必要がある場合は、Cloud Build サービスアカウントにロールを追加するに記載されている手順に従ってください。

- Cloud Build サービスアカウント
- Compute Instance 管理者
- サービスアカウントユーザー

- *Cloud Compute Service Account*: このサービスアカウントは、Compute API がアクティブ化されると、Google Cloud によって Google Cloud で作成されたインスタンスに追加されます。このアカウントには、操作を実行するための IAM 基本編集者ロールがあります。ただし、より詳細な制御を行うためにデフォルトの権限を削除する場合は、以下の権限を必要とする**ストレージ管理者**ロールを追加する必要があります。
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

このサービスアカウントは、**プロジェクトID**と**compute**という単語で始まるメールアドレスで識別できます。例: `<project-id>-compute@developer.gserviceaccount.com`.

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービス アカウント**に移動します。
2. **サービス アカウント**ページで、**サービス アカウントを作成**を選択します。
3. **サービス アカウントの作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. **このサービス アカウントにプロジェクトへのアクセス権を付与**ページで、**ロールを選択**ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、**+別のロールを追加**をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービス アカウントに次のロールを付与します。

   - Compute 管理者

- Storage 管理者
- Cloud Build 編集者
- サービス アカウント ユーザー
- クラウド データストア ユーザー
- Cloud KMS 暗号オペレーター

Cloud KMS 暗号化オペレーターには、次の権限が必要です。

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list

> **注:**
>
> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **続行**をクリックします
6. **このサービスアカウントへのユーザーアクセスを許可**ページで、ユーザーまたはグループを追加して、このサービスアカウントでアクションを実行するアクセス権を付与します。
7. **完了**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成したサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを検証します。

考慮事項:

サービスアカウントを作成する際は、以下を考慮してください。

- **このサービスアカウントにプロジェクトへのアクセスを許可**および**このサービスアカウントへのユーザーアクセスを許可**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは**IAMと管理 > IAM**ページに表示されません。

- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加します。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix DaaSで接続を作成するには、Citrix Cloudサービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成する際は、キータイプをJSONに設定してください。そうしないと、Citrix Full Configurationインターフェイスで解析できません。

サービスアカウントキーを作成するには、**IAM と管理 > サービスアカウント**に移動し、Citrix Cloudサービスアカウントのメールアドレスをクリックします。**キー**タブに切り替えて、**キーを追加 > 新しいキーを作成**を選択します。キーのタイプとして**JSON**が選択されていることを確認してください。

> **ヒント:**
>
> Google Cloud コンソールで、**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、Citrix Virtual Apps and Desktops アプリケーションに新しいキーを提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloudコンソールで、**IAM と管理 > IAM**に移動します。
2. **IAM > 権限**ページで、作成したサービスアカウント（メールアドレスで識別可能）を見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの**「project-id」へのアクセスを編集**ページで、**別のロールを追加**を選択して必要なロールをサービスアカウントに1つずつ追加し、**保存**を選択します。

CLOUD BUILD サービスアカウントにロールを追加する

Cloud Build サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM**ページで、**プロジェクト ID**と**cloudbuild**という単語で始まる電子メールアドレスで識別できる Cloud Build サービスアカウントを見つけます。

   例: `<project-id>@cloudbuild.gserviceaccount.com`
3. 鉛筆アイコンを選択して、Cloud Buildアカウントの役割を編集します。
4. 選択したプリンシパルオプションの「**"project-id"へのアクセスを編集**」ページで、**別の役割を追加**を選択して、必要な役割をCloud Buildサービスアカウントに1つずつ追加し、**保存**を選択します。

   > **注:**
   >
   > すべてのAPIを有効にして、役割の完全なリストを取得します。

April 29, 2024 以降

Citrix Cloudは、Google Cloudプロジェクト内で2つの異なるサービスアカウントを使用します。

- *Citrix Cloudサービスアカウント*: このサービスアカウントにより、Citrix CloudはGoogleプロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloudによって生成されたキーを使用してGoogle Cloudに認証します。

  このサービスアカウントは手動で作成する必要があります。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。
- *Cloud Computeサービスアカウント*: このサービスアカウントは、Google Cloud APIを有効にするで言及されているすべてのAPIを有効にすると自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud**コンソールで**IAMと管理 > IAM**に移動し、**Google提供の役割付与を含める**チェックボックスを選択します。このアカウントには、操作を実行するためのIAM基本編集者ロールがあります。ただし、より詳細な制御を行うためにデフォルトの権限を削除した場合、次の権限を必要とする**ストレージ管理者**ロールを追加する必要があります。
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

このサービスアカウントは、**プロジェクトID**と**compute**という単語で始まるメールアドレスで識別できます。例: `<project-id>-compute@developer.gserviceaccount.com.`.

サービスアカウントに次のロールが付与されていることを確認します。

- Cloud Build サービスアカウント
- Compute Instance 管理者
- サービスアカウントユーザー

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービスアカウント**に移動します。
2. **サービスアカウント**ページで、**サービスアカウントを作成**を選択します。
3. **サービスアカウントを作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. **このサービスアカウントにプロジェクトへのアクセス権を付与**ページで、**ロールを選択**ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、**+別のロールを追加**をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントには、以下のロールを付与してください。

   - Compute 管理者
   - Storage管理者
   - Cloud Build編集者
   - サービスアカウントユーザー
   - クラウド データストア ユーザー
   - Cloud KMS 暗号オペレーター

   Cloud KMS 暗号オペレーターには、以下の権限が必要です。

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

> **注：**

> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **CONTINUE**をクリックします。
6. **このサービスアカウントへのユーザーアクセスを許可**ページで、このサービスアカウントでアクションを実行するアクセス権を付与するために、ユーザーまたはグループを追加します。
7. **DONE**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを検証します。

留意事項:

サービスアカウントを作成する際は、以下の点に留意してください。

- **このサービスアカウントにプロジェクトへのアクセスを許可する**および**このサービスアカウントへのユーザーアクセスを許可する**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは、**IAM と管理 > IAM** ページに表示されません。
- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加してください。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUD サービスアカウントキー

Citrix DaaS で接続を作成するには、Citrix Cloud サービスアカウントキーが必要です。キーは資格情報ファイル (.json) に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成する際は、キータイプを JSON に設定してください。そうしないと、Citrix Full Configuration インターフェイスで解析できません。

サービスアカウントキーを作成するには、**IAM と管理 > サービスアカウント**に移動し、Citrix Cloud サービスアカウントのメールアドレスをクリックします。**キー**タブに切り替えて、**キーを追加 > 新しいキーを作成**を選択します。キータイプとして**JSON**を選択してください。

> **ヒント:**

> Google Cloud コンソールの**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存の Google Cloud

> 接続を編集することで、Citrix Virtual Apps and Desktops アプリケーションに新しいキーを提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM > 権限**ページで、メールアドレスで識別できる、作成したサービスアカウントを見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの**「project-id」へのアクセスを編集**ページで、**別のロールを追加**を選択して、必要なロールをサービスアカウントに1つずつ追加し、**保存**を選択します。

CLOUD COMPUTEサービスアカウントにロールを追加する

Cloud Computeサービスアカウントにロールを追加するには：

1. Google Cloudコンソールで、**IAMと管理 > IAM**に移動します。
2. **IAM**ページで、**プロジェクトID**と**compute**という単語で始まるメールアドレスで識別できるCloud Computeサービスアカウントを見つけます。

   例えば、`<project-id>-compute@developer.gserviceaccount.com`
3. 鉛筆アイコンを選択して、Cloud Buildアカウントのロールを編集します。
4. 選択したプリンシパルオプションの**「project-id」へのアクセスを編集ページ**で、**別のロールを追加**を選択して、必要なロールをCloud Buildサービスアカウントに1つずつ追加し、**保存**を選択します。

> **注:**
>
> すべてのAPIを有効にして、ロールの完全なリストを取得します。

ストレージの権限とバケット管理

Citrix Virtual Apps and Desktopsは、Google Cloudサービスのクラウドビルド失敗レポートプロセスを改善します。このサービスは、Google Cloudでビルドを実行します。Citrix Virtual Apps and

Desktopsは、Google Cloudサービスがビルドログ情報をキャプチャする`citrix-mcs-cloud-build-logs-{region}-{5 random characters}`という名前のストレージバケットを作成します。このバケットには、30日後にコンテンツを削除するオプションが設定されています。このプロセスでは、接続に使用されるサービスアカウントに`storage.buckets.update`に設定されたGoogle Cloud権限が必要です。サービスアカウントにこの権限がない場合、Citrix Virtual Apps and Desktopsはエラーを無視し、カタログ作成プロセスを続行します。この権限がないと、ビルドログのサイズが増加し、手動でのクリーンアップが必要になります。

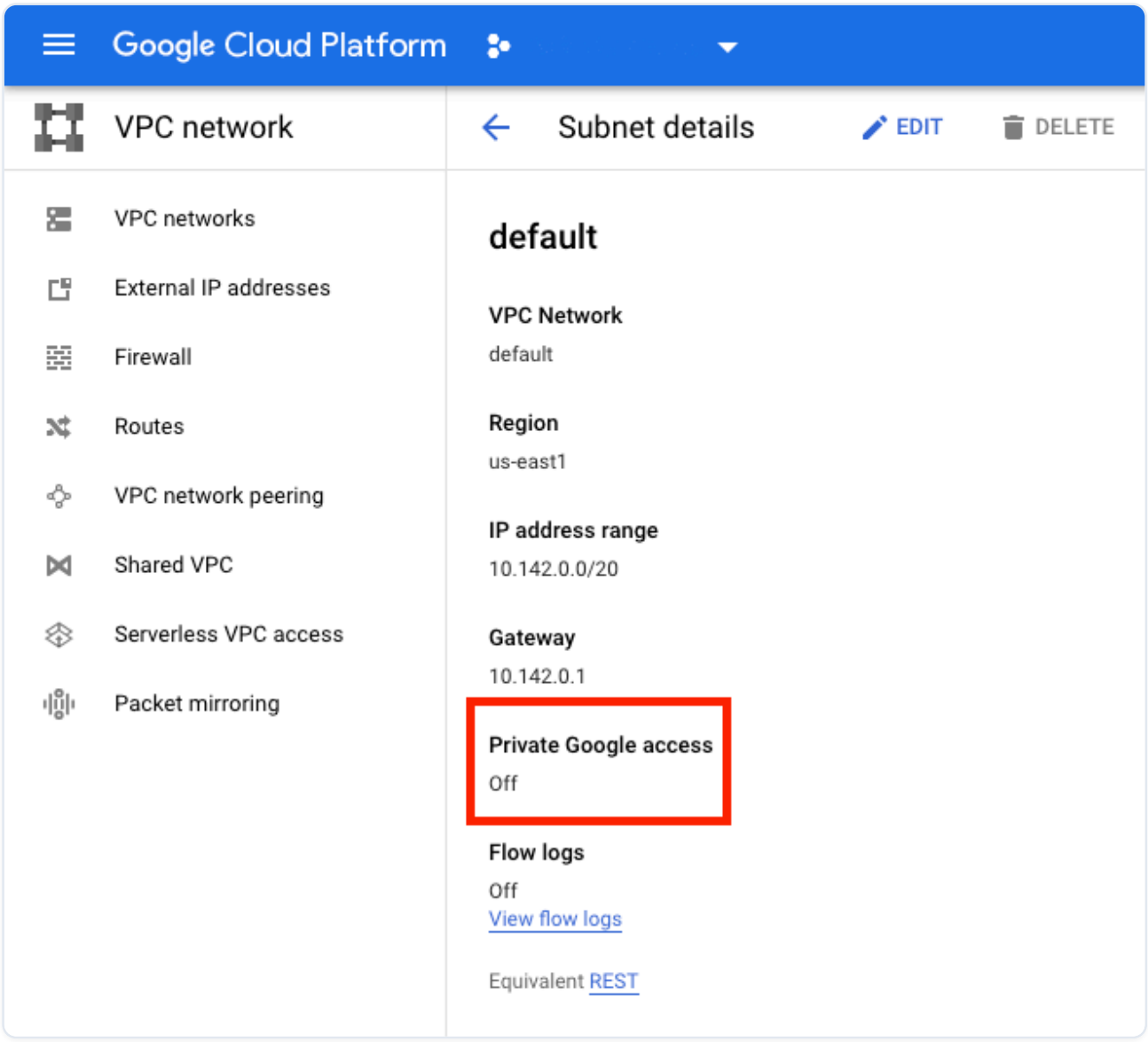
プライベート Google アクセスを有効にする

VMのネットワークインターフェースに外部IPアドレスが割り当てられていない場合、パケットは他の内部IPアドレスの宛先にのみ送信されます。プライベートアクセスを有効にすると、VMはGoogle APIおよび関連サービスで使用される外部IPアドレスのセットに接続します。

> **注:**
>
> プライベートGoogleアクセスが有効になっているかどうかにかかわらず、パブリックIPアドレスを持つVMと持たないVMはすべて、Google Public APIにアクセスできる必要があります。特に、サードパーティのネットワークアプライアンスが環境にインストールされている場合は、その必要があります。

> MCSプロビジョニングのために、サブネット内のVMがパブリックIPアドレスなしでGoogle APIにアクセスできるようにするには：

1. Google Cloudで、**VPC network configuration**にアクセスします。
2. サブネットの詳細画面で、「**Private Googleアクセス**」をオンにします。



詳細については、「プライベートGoogleアクセスの構成」を参照してください。

重要：

ネットワークがVMのインターネットアクセスを防止するように構成されている場合、VMが接続されているサブネットに対してプライベートGoogleアクセスを有効にすることに関連するリスクを、組織が認識し、受け入れることを確認してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成

- Google Cloud 環境での接続の作成と管理については、「Google Cloud 環境への接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

HPE Moonshot 仮想化環境 (プレビュー)

Citrix Virtual Apps and Desktops™ は、Citrix が管理する HPE Moonshot プラグインを介して HPE Moonshot ワークロードを管理します。このプラグインを使用すると、HPE Moonshot シャーシへの接続を作成し、カタログを作成し、カタログ内のマシンの電源管理を行うことができます。

要件

Citrix が管理する HPE Moonshot プラグインを Delivery Controller にインストールします。

> **注:**
>
> - Citrix が管理する HPE Moonshot プラグインと HPE が管理する HPE Moonshot プラグインの両方がインストールされている場合、Delivery Controller は Citrix が管理する HPE Moonshot プラグインを使用します。
> - Citrix が管理する HPE Moonshot プラグインと HPE が管理する HPE Moonshot プラグインの両方がインストールされており、HPE が管理する Moonshot プラグインを使用したい場合は、Citrix が管理する HPE Moonshot プラグインをアンインストールし、`RegisterPlugin` キャッシュを更新してください。

Citrix が管理する HPE Moonshot プラグインをインストールする

Citrix が管理する HPE Moonshot プラグインをインストールするには、次の手順を実行します。

1. `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin`.msi をインストールします。`E:\` は ISO です。
2. PowerShell を管理者として開き、次のコマンドを実行します。

```
C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins.exe
-pluginsroot .\CitrixMachineCreation\v1.0.0.0\
```

3. プラグインの登録が成功したら、**タスクマネージャー**から次のサービスを再起動します。
    a. CitrixBrokerService
    b. CitrixHostService
    c. CitrixMachineCreationService
4. Delivery Controllerにプラグインがインストールされているか確認するには、`Get-HypHypervisorPlugins`を実行します。出力の**DisplayName**フィールドには、**HPE Moonshot**と表示されている必要があります。

Citrix が管理する HPE Moonshot プラグインをアンインストールし、RegisterPlugin キャッシュを更新する

Citrix が管理する HPE Moonshot プラグインと HPE が管理する HPE Moonshot プラグインの両方がインストールされており、HPE が管理する Moonshot プラグインを使用したい場合は、Citrix が管理する HPE Moonshot プラグインをアンインストールし、`RegisterPlugin` キャッシュを更新する必要があります。これを行うには：

1. Citrix管理のHPE Moonshotプラグインをアンインストールします。
2. PowerShellを管理者として開き、次のコマンドを実行します。

```
cd `C:\Program Files\Common Files\Citrix\HCLPlugins\`

C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins.exe
-PluginsRoot ` C:\Program Files\Common
Files\Citrix\HCLPlugins\ManagedMachine\v2.5.0.0\`
```

3. プラグインの登録が成功したら、**タスクマネージャー**から次のサービスを再起動します。
    a. CitrixBrokerService
    b. CitrixHostService
    c. CitrixMachineCreationService
4. Delivery Controllerにプラグインがインストールされているか確認するには、`Get-HypHypervisorPlugins`を実行します。出力の**DisplayName**フィールドには、**HPE Moonshot Machine Manager**と表示されている必要があります。

主な手順

1. HPE 環境をセットアップします。

2. HPE Moonshot シャーシへの接続を作成します。
3. マシンカタログを作成します。

> **注:**
>
> カタログを作成する前に、1 つ以上の HPE Moonshot カートリッジノードがあることを確認し、それらのノードに VDA をインストールしてください。HPE Moonshot シャーシをハイパーバイザー、カートリッジノードを VM と考えることができます。

4. デリバリーグループを作成します。
5. 管理されていない残りの HPE Moonshot ノードを、管理対象のカタログまたはデリバリーグループに移行します。

次のステップ

- コアコンポーネントをインストールする
- VDAをインストールする
- サイトを作成する
- HPE Moonshotで接続を作成および管理するには、HPE Moonshotへの接続を参照してください。

詳細情報

- 接続とリソースを作成および管理する
- マシンカタログを作成する

Microsoft Azure Resource Manager クラウド環境

Microsoft Azure Resource Managerを使用してCitrix Virtual Apps and Desktops™展開環境で仮想マシンをプロビジョニングする場合、以下について理解しておいてください。

- アジュール Active Directory: `<https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/>`
- 同意フレームワーク: `<https://docs.microsoft.com/ja-jp/azure/active-directory/manage-apps/plan-an-application-integration>`
- サービスプリンシパル: `<https://docs.microsoft.com/ja-jp/azure/active-directory/develop/app-objects-and-service-principals/>`

Microsoft Azure Resource Managerを設定するには、インストール準備を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Azure環境で接続を作成および管理するには、Microsoft Azureへの接続を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成
- CTX219211: Microsoft Azure Active Directoryアカウントを設定する
- CTX219243: XenAppおよびXenDesktopにAzureサブスクリプションへのアクセスを許可する
- CTX219271: サイト間VPNを使用してハイブリッドクラウドを展開する

マイクロソフト システム センター コンフィギュレーション マネージャー 環境

Microsoft System Center Configuration Manager (Configuration Manager) を使用してアプリケーションとデスクトップへのアクセスを管理しているサイトでは、次のオプションを使用してその使用を Citrix Virtual Apps and Desktops™ に拡張できます。

- SCCM を使用した VDA のインストール(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-vdas-sccm.html)。
- **Configuration Manager Wake Proxy 機能:** Remote PC Access の Wake on LAN 機能は Configuration Manager でサポートされています。詳細については、「Wake on LAN - SCCM 統合」を参照してください。
- **Citrix Virtual Apps and Desktops のプロパティ:** プロパティ を使用すると、Configuration Manager を介して管理するための Citrix Virtual Desktops™ を識別できます。(一部のバージョンでは、Configuration Manager は Citrix Virtual Apps and Desktops の旧称である XenApp および XenDesktop を使用しています。)

プロパティ

仮想デスクトップを管理するために、Microsoft System Center Configuration Manager でプロパティを使用できます。

Configuration Manager に表示されるブール型プロパティは、true または false ではなく、`1` または `0` として表示されます。

プロパティは、`Root\Citrix\DesktopInformation` 名前空間の `Citrix_virtualDesktopInfo` クラスで利用できます。プロパティ名は、Windows Management Instrumentation (WMI) プロバイダーから取得されます。

プロパティ	説明
`AssignmentType`	IsAssigned の値を設定します。有効な値は、`ClientIP`、`ClientName`、`None`、および `User` です (`IsAssigned` を `True` に設定します)。
`BrokerSiteName`	`HostIdentifier` と同じ値を返します。
`DesktopCatalogName`	デスクトップに関連付けられているマシンカタログ。
`DesktopGroupName`	デスクトップに関連付けられているデリバリーグループ。
`HostIdentifier`	`BrokerSiteName`と同じ値を返します。
`IsAssigned`	デスクトップをユーザーに割り当てる場合は `True`、ランダムなデスクトップの場合は `False`に設定します
`IsMasterImage`	環境に関する決定を可能にします。たとえば、プロビジョニングされたマシンではなく、イメージにアプリケーションをインストールします。有効な値は次のとおりです。イメージとして使用されるVMでは`True`。この値は、インストール時に選択に基づいて設定されるか、そのイメージからプロビジョニングされたVMではクリアされます。
`IsVirtualMachine`	仮想マシンの場合は`True`、物理マシンの場合は`false`。
`OSChangesPersist`	デスクトップオペレーティングシステムイメージが再起動のたびにクリーンな状態にリ

プロパティ	説明
	セットされる場合は`False`。それ以外の場合は`true`。
`PersistentDataLocation`	Configuration Managerが永続データを保存する場所です。これはユーザーがアクセスできません。
`BrokerSiteName`, `DesktopCatalogName`, `DesktopGroupName`, `HostIdentifier`	デスクトップがControllerに登録されるときに決定されます。完全に登録されていないデスクトップの場合、それらはnullです。

プロパティを収集するには、Configuration Managerでハードウェアインベントリを実行します。プロパティを表示するには、Configuration Manager Resource Explorerを使用します。これらの場合、名前にはスペースが含まれるか、プロパティ名とわずかに異なります。たとえば、`BrokerSiteName` は `Broker Site Name` と表示されます。

- Citrix VDA から Citrix WMI プロパティを収集するように Configuration Manager を構成する
- Citrix WMI プロパティを使用してクエリベースのデバイスコレクションを作成する
- Citrix WMI プロパティに基づいてグローバル条件を作成する
- グローバル条件を使用してアプリケーション展開タイプの要件を定義する

Microsoftクラス `CCM_DesktopMachine` の `Root\ccm_vdi` 名前空間にあるMicrosoftプロパティも使用できます。詳細については、Microsoftのドキュメントを参照してください。

マイクロソフト システムセンター バーチャル マシン マネージャー 仮想化環境

仮想マシンを提供する目的で、Microsoft System Center Virtual Machine Manager (VMM) と共に Hyper-V を使用する場合は、このガイダンスに従ってください。

このリリースでは、システム要件に記載されているVMMバージョンがサポートされています。

> **注:**
>
> 混在するHyper-Vクラスター（異なるHyper-Vバージョンを実行しているサーバーを含む）はサポートされていません。

Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™を使用して、以下をプロビジョニングできます。

- 第1世代でサポートされているデスクトップまたはサーバーOSのVM。
- 第2世代でサポートされているデスクトップまたはサーバーOSのVM（セキュアブートのサポートを含む）。

ハイパーバイザーのインストールと構成

重要:

すべてのDelivery Controllerは、VMMサーバーと同じフォレスト内にある必要があります。

1. サーバーにMicrosoft Hyper-VサーバーとVMMをインストールします。
2. すべてのControllerにSystem Center Virtual Machine Managerコンソールをインストールします。コンソールのバージョンは、管理サーバーのバージョンと一致している必要があります。以前のコンソールでも管理サーバーに接続できますが、バージョンが異なる場合、VDAのプロビジョニングは失敗します。
3. 次のアカウント情報を確認します。

   Studioでホストを指定するために使用するアカウントは、関連するHyper-Vマシンに対するVMM管理者またはVMM委任管理者である必要があります。このアカウントがVMMで委任管理者ロールのみを持っている場合、ホスト作成プロセス中にStudioにストレージデータは表示されません。

   Studio統合に使用されるユーザーアカウントは、各Hyper-Vサーバーのadministratorsローカルセキュリティグループのメンバーである必要もあります。この構成は、VMの作成、更新、削除などのVMライフサイクル管理をサポートします。

   Hyper-Vを実行しているサーバーにControllerをインストールすることはサポートされていません。

単一のSCVMMが異なるデータセンター内の複数のクラスターを管理する大規模な展開では、委任管理者のホストグループのスコープを制限できます。

ホストグループのスコープを制限するには、Microsoft System Center Virtual Machine Manager (VMM) コンソールで委任管理者ロールを使用します。

1. **ユーザーロールの作成ウィザード**で、ユーザーロールとしてFabric Administrator (Delegated Administrator) を選択します。
2. **メンバー**で、委任管理者として使用するActive Directoryのユーザーアカウントを追加します。
3. **スコープ**で、委任管理者にアクセスを許可するホストグループを選択します。
4. 委任管理者のユーザー資格情報を使用して、新しい**実行アカウント**を作成します。これらの資格情報を使用して、後でハイパーバイザー接続を作成します。メインの管理者ロールアカウントは使用しないでください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- SCVMMでの接続の作成と管理については、Microsoft System Center Virtual Machine Managerへの接続を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Nutanix仮想化環境

Citrix Virtual Apps and Desktops™展開でNutanix Acropolisを使用して仮想マシンを提供する場合は、このガイダンスに従ってください。セットアッププロセスには、次のタスクが含まれます。

- Citrix Virtual Apps and Desktops 環境に Nutanix プラグインをインストールして登録します。
- Nutanix Acropolis ハイパーバイザーへの接続を作成します。
- Nutanix ハイパーバイザー上に作成したマスターイメージのスナップショットを使用するマシンカタログを作成します。

詳細については、Nutanix サポートポータル で入手できる Nutanix Acropolis MCS プラグインインストールガイドを参照してください。

Nutanixプラグインのインストールと登録

すべての Delivery Controller に Nutanix プラグインをインストールして登録するには、以下の手順を完了します。Citrix Studio を使用して Nutanix への接続を作成します。次に、Nutanix 環境で作成したマスターイメージのスナップショットを使用するマシンカタログを作成します。

ヒント：

Nutanix プラグインをインストールまたは更新する際は、Citrix Host Service、Citrix Broker Service、および Machine Creation Services™ を停止してから再起動することをお勧めします。

Nutanix プラグインのインストールについては、Nutanix ドキュメントサイト を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Nutanix環境で接続を作成および管理するには、Nutanixへの接続を参照してください。

詳細情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Nutanix クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の Nutanix クラウドおよびパートナーソリューションをサポートしています。

- AWS 上のニュータニックス クラウド クラスターズ

AWS 上のニュータニックス クラウド クラスターズ

Citrix Virtual Apps and Desktops は AWS 上の Nutanix Cloud Clusters をサポートしています。Nutanix クラスターは、プライベートクラウドまたは複数のパブリッククラウドでアプリケーションを実行する方法を簡素化します。AWS 上の Nutanix Cloud Clusters の詳細については、「Nutanix Cloud Clusters on AWS Deployment and User Guide」を参照してください。

ヒント:

> このサポートは、Nutanix オンプレミス クラスターと同じ機能を提供します。サポートされるクラスターは、*Prism Element* の単一クラスターのみです。詳細については、こちらを参照してください。

要件

AWS 上で Nutanix クラスターを使用するには、以下が必要です。

- Nutanix アカウント。
- 以下の権限を持つ AWS アカウント:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Nutanix クラスターを作成する

Nutanix Clusterを作成するには：

1. Nutanixアカウントにログインします。
2. **Nutanix cluster**オプションを見つけて、**Launch**をクリックします。**Nutanix Console**が開きます。詳細については、Get Started with Nutanix Cluster on AWSを参照してください。
3. **新しいVPC**を作成することを選択します。

クラスター作成プロセスは、次のエラーで失敗する可能性があります。

- クラスターは指定された時間内に作成できませんでした。クラスターを削除しています。
- ホストNutanix Cluster - ノード `XXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`.
- ホストNutanix Cluster - ノード `XXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info.`.

クラスターの作成に失敗した場合：

- 別のリージョンで再作成してみてください。
- 再試行する前に、Nutanix CloudFormation Stack (CFS) を削除してください。

他のリソースに加えて、Nutanix CFSは以下を作成します：

- *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16 という名前の 1 つの VPC
- 2つのサブネット 10.0.128.0/24 および 10.0.129.0/24

- 1つのインターネットゲートウェイ
- 1つのNATゲートウェイ

クラスターが作成されたら、**Nutanix Prism**のアドレスを取得します。

1. **Nutanix Console**に移動します。
2. コンソールの右上隅で、**Launch Prism Element**リンクにマウスカーソルを合わせ、URLをコピーします。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Nutanixクラウドおよびパートナーソリューションの接続を作成および管理するには、Nutanixクラウドおよびパートナーソリューションへの接続を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

VMware 仮想化環境

仮想マシンを提供するのにVMwareを使用する場合は、このガイダンスに従ってください。

vCenter Serverと適切な管理ツールをインストールします。(vSphere vCenter Linked Mode操作はサポートされていません。)

MCSを使用する予定がある場合は、vCenter ServerのDatastore Browser機能を無効にしないでください(https://kb.vmware.com/s/article/2101567で説明されています)。この機能を無効にすると、MCSは正しく動作しません。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- VMware環境での接続の作成と管理については、「Connection to VMware」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

VMware クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の VMware クラウドおよびパートナーソリューションをサポートしています。

- アジュール VMware ソリューション (AVS)
- グーグル クラウド VMware エンジン
- ヴイエムウェア クラウド オン アマゾン ウェブ サービス (AWS)

Azure VMware Solution (AVS) との統合

Citrix Virtual Apps and Desktop サービスは AVS をサポートしています。AVS は、Azure インフラストラクチャによって作成された vSphere クラスターを含むクラウドインフラストラクチャを提供します。オンプレミス環境で vSphere を使用するのと同じ方法で VDA ワークロードをプロビジョニングするために AVS を使用するには、Citrix Virtual Apps and Desktop サービスを活用してください。

AVS クラスターのセットアップ

Citrix Virtual Apps™ and Desktop サービスで AVS を使用できるようにするには、Azure で以下の手順を実行します。

- ホストクォータを要求する
- Microsoft.AVS リソースプロバイダーを登録する
- ネットワークチェックリスト
- Azure VMware Solution プライベートクラウドを作成する
- Azure VMware Solution プライベートクラウドにアクセスする
- Azure で VMware プライベートクラウドのネットワークを構成する
- Azure VMware Solution の DHCP を構成する
- Azure VMware Solution にネットワークセグメントを追加する
- Azure VMware Solution 環境を確認する

AZURE ENTERPRISE AGREEMENTのお客様のホストクォータを要求する

Azureポータルの**ヘルプとサポート**ページで、**新しいサポートリクエスト**を選択し、次の情報を含めます。

- 問題の種類: 技術
- サブスクリプション: サブスクリプションを選択してください
- サービス: すべてのサービス > Azure VMware Solution
- リソース: 一般的な質問
- 概要: 容量が必要
- 問題の種類: 容量管理の問題
- 問題のサブタイプ: 追加のホストクォータ/容量に関する顧客からの要求

サポートチケットの に、 タブで次の情報を含めます。

- POC または本番環境
- リージョン名
- ホスト数
- その他の詳細

> **注：**

> AVSは最低3台のホストを必要とし、N+1ホストの冗長性を使用することを推奨します。

> サポートチケットの詳細を指定した後、**Review + Create** を選択してAzureにリクエストを送信します。

MICROSOFT.AVS リソースプロバイダーを登録する

ホスト クォータを要求した後、リソース プロバイダーを登録します。

1. Azureポータルにサインインします。
2. Azureポータルメニューで、**すべてのサービス** を選択します。
3. **すべてのサービス** メニューで、サブスクリプションを入力し、**サブスクリプション** を選択します。
4. サブスクリプションリストからサブスクリプションを選択します。
5. **リソースプロバイダー** を選択し、検索バーに **Microsoft.AVS** と入力します。

6. リソースプロバイダーが登録されていない場合は、**登録** を選択します。

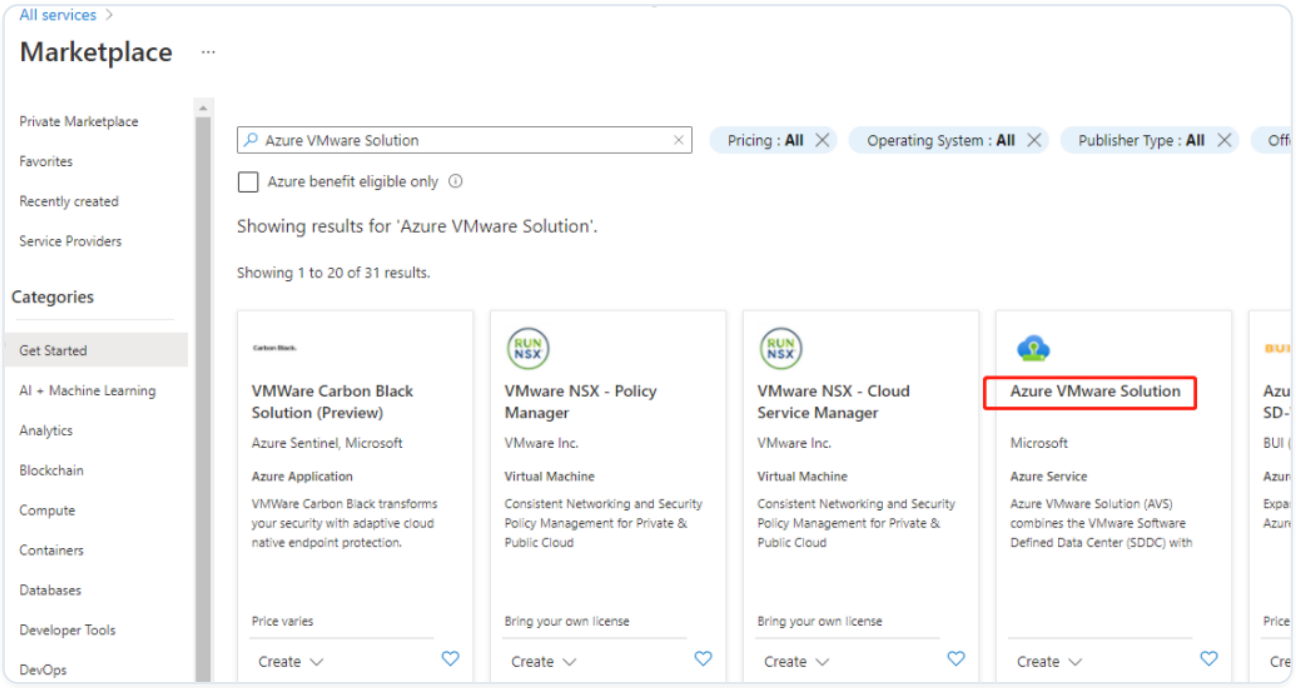
ネットワークに関する考慮事項

AVSは、特定のネットワークアドレス範囲とファイアウォールポートを必要とするネットワークサービスを提供します。詳細については、Azure VMware Solution のネットワーク計画チェックリスト を参照してください。

AZURE VMWARE SOLUTION プライベートクラウドを作成する

環境のネットワーク要件を考慮した後、AVS プライベートクラウドを作成します。

1. Azureポータルにサインインします。
2. **新しいリソースの作成**を選択します。
3. **Marketplace を検索**テキストボックスに「*Azure VMware Solution*」と入力し、リストから **Azure VMware Solution**を選択します。



image

Azure VMware Solutionウィンドウで:

1. **作成**を選択します。
2. タブをクリックします。
3. 以下の表の情報を使用して、フィールドに値を入力します。

フィールド	値
サブスクリプション	展開に使用するサブスクリプションを選択します。Azure サブスクリプション内のすべてのリソースはまとめて請求されます。
リソースグループ	プライベートクラウドのリソースグループを選択します。Azure リソースグループは、Azure リソースがデプロイおよび管理される論理コンテナです。または、プライベートクラウド用に新しいリソースグループを作成することもできます。
場所	east us などの場所を選択します。これは、計画フェーズで定義したリージョンです。
リソース名	Azure VMware Solution プライベートクラウドの名前を指定します。
SKU	AV36 を選択します。
ホスト	プライベートクラウドクラスターに割り当てられたホストの数を表示します。デフォルト値は 3 で、デプロイ後に増減できます。
アドレスブロック	プライベートクラウドの IP アドレスブロックを指定します。CIDR はプライベートクラウド管理ネットワークを表し、vCenter Server や NSX-T Manager などのクラスター管理サービスに使用されます。たとえば、10.175.0.0/22 のように /22 アドレス空間を使用します。このアドレスは一意であり、他の Azure 仮想ネットワークやオンプレミスネットワークと重複しないようにする必要があります。
仮想ネットワーク	Azure VMware Solution ExpressRoute 回線はデプロイ後の手順として確立されるため、このフィールドは空白のままにします。

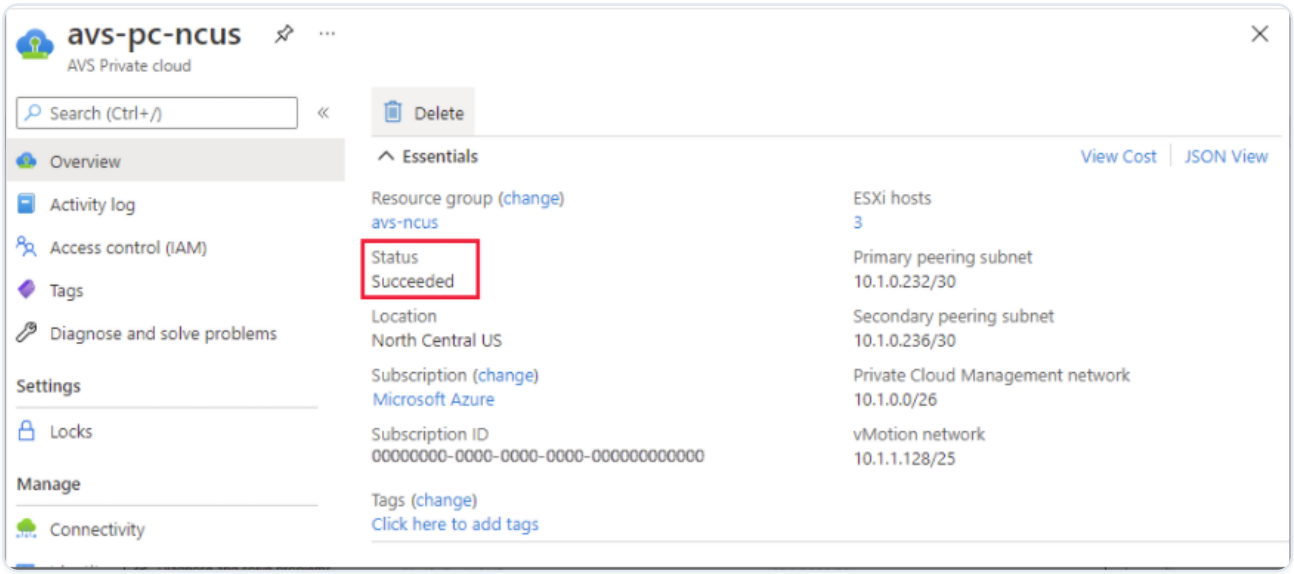
プライベートクラウドの作成画面で、次のようにします。

1. フィールドで、AVS が存在するリージョンを選択します。リソースグループのリージョンは AVS リージョンと同じです。

2. フィールドで、 を選択します。
3. 「**アドレスブロック**」フィールドにIPアドレスを指定します。例: 10.15.0.0/22。
4. 「**確認 + 作成**」を選択します。
5. 情報を確認したら、「**作成**」をクリックします。

Azure ASV プライベートクラウドの作成(/en-us/citrix-virtual-apps-desktops/2311/media/azure-avs-create-private-cloud.png)

> **ヒント:**
>
> プライベートクラウドの作成には3〜4時間かかる場合があります。クラスターに単一ホストを追加するには30〜45分かかる場合があります。
>
> 展開が成功したことを確認します。作成したリソースグループに移動し、プライベートクラウドを選択します。**ステータス**が**成功**になったら、展開は完了です。



AZURE VMWARE SOLUTION プライベートクラウドへのアクセス

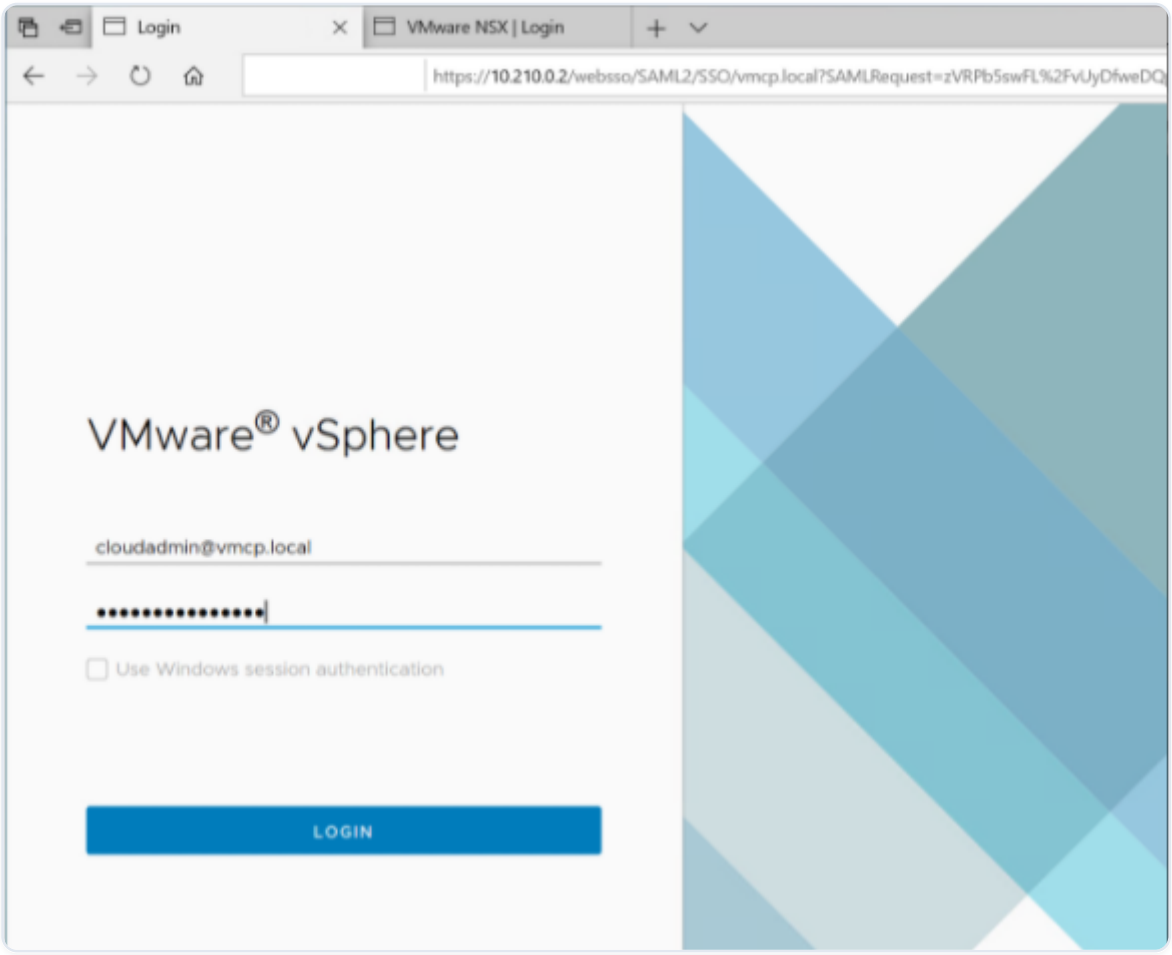
プライベートクラウドを作成したら、Windows VMを作成し、プライベートクラウドのローカルvCenterに接続します。
新しいWindows仮想マシンの作成

1. リソースグループで「**+ Add**」を選択し、「**Microsoft Windows 10/2016/2019**」を検索して選択します。
2. 「**Create**」をクリックします。
3. 必要な情報を入力し、「**Review + Create**」を選択します。

4. 検証が完了したら、仮想マシンの作成プロセスを開始するために**作成**を選択します。

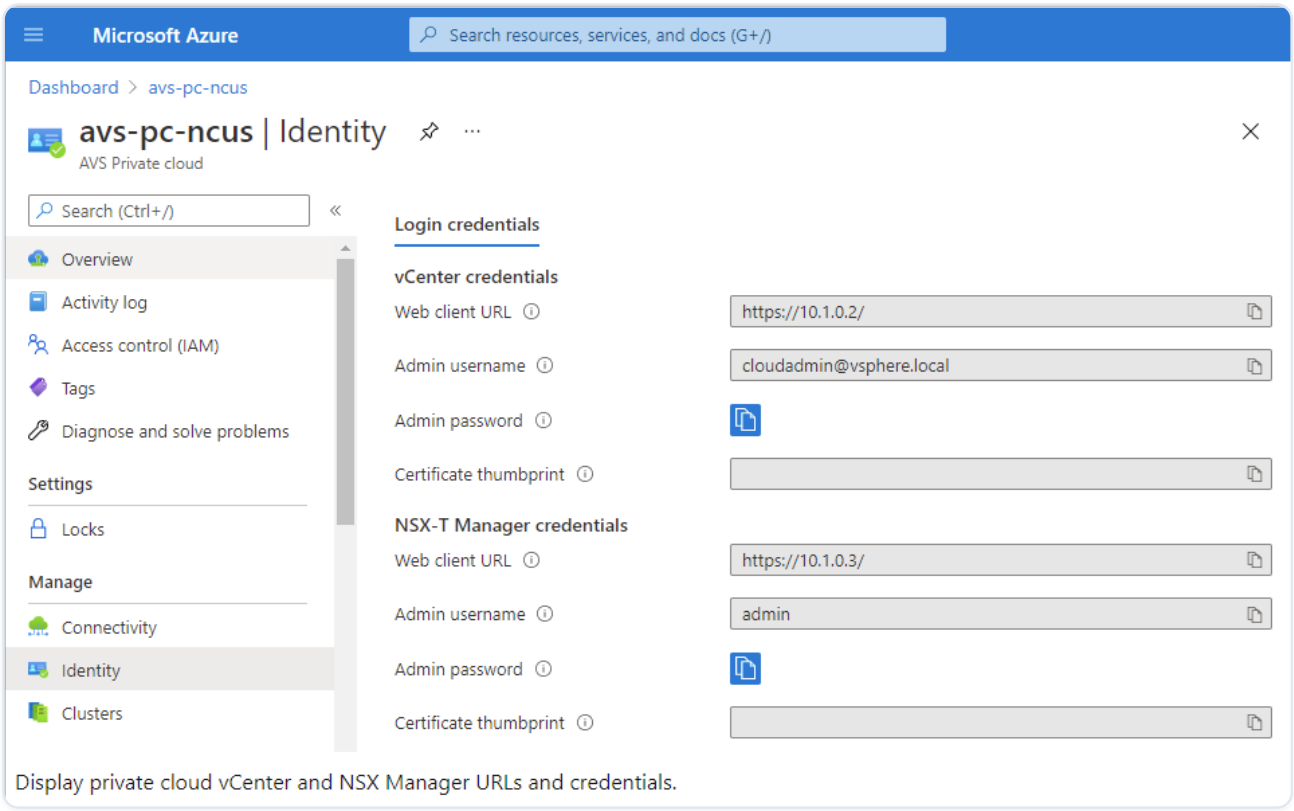
プライベートクラウドのローカルvCenterに接続する

1. クラウド管理者として**VMware vCenter SSO を使用した vSphere Client**にサインインします。



2. Azure ポータルで、プライベートクラウドを選択し、**管理 > ID**を選択します。

プライベートクラウドのvCenterおよびNSX-T ManagerのURLとユーザー資格情報が表示されます。



URLとユーザー資格情報を確認した後：

1. 前の手順で作成したVMに移動し、仮想マシンに接続します。
2. Windows VMでブラウザを開き、2つのブラウザタブでvCenterおよびNSX-T ManagerのURLに移動します。vCenterタブで、前の手順の*cloudadmin@vmcp.local*ユーザー資格情報を入力します。

AZUREでVMWAREプライベートクラウドのネットワークを構成する

ASVプライベートクラウドにアクセスした後、仮想ネットワークとゲートウェイを作成してネットワークを構成します。
仮想ネットワークを作成する

1. Azure ポータルにサインインします。
2. 以前に作成したリソースグループに移動します。
3. 新しいリソースを定義するには、 を選択します。
4. テキストボックスに「*仮想ネットワーク*」と入力します。仮想ネットワークリソースを見つけて選択します。
5. 「**仮想ネットワーク**」ページで、「**作成**」を選択してプライベートクラウドの仮想ネットワークを設定します。
6. 「**仮想ネットワークの作成**」ページで、仮想ネットワークの詳細を入力します。

7. 「**基本**」タブで、仮想ネットワークの名前を入力し、適切なリージョンを選択して、「**次へ：IPアドレス**」をクリックします。
8. 「**IPアドレス**」タブのIPv4アドレス空間で、以前に作成したアドレスを入力します。

> **重要:**

> プライベートクラウドを作成したときに使用したアドレス空間と重複しないアドレスを使用してください。

> アドレス空間を入力した後:

1. 「**+ サブネットの追加**」を選択します。
2. 「**サブネットの追加**」ページで、サブネットに名前と適切なアドレス範囲を割り当てます。
3. 「**追加**」をクリックします。
4. 「**確認 + 作成**」を選択します。
5. 情報を確認し、「**作成**」をクリックします。デプロイが完了すると、仮想ネットワークがリソースグループに表示されます。

仮想ネットワークゲートウェイを作成する
仮想ネットワークを作成した後、仮想ネットワークゲートウェイを作成します。

1. リソースグループで、**+ 追加**を選択して新しいリソースを追加します。
2. **Marketplace を検索**テキストボックスに「*virtual network gateway*」と入力します。仮想ネットワークリソースを見つけて選択します。
3. **仮想ネットワークゲートウェイ**ページで、**作成**をクリックします。
4. **仮想ネットワークゲートウェイの作成**ページの**基本**タブで、フィールドに値を入力します。
5. **確認 + 作成**をクリックします。

Azure ASV セットアップ vCenter(/en-us/citrix-virtual-apps-desktops/2311/media/azure-avs-create-virtual-gateway.png)

仮想ネットワークゲートウェイの構成を確認した後、**作成**をクリックして仮想ネットワークゲートウェイをデプロイします。 デプロイが完了したら、**ExpressRoute**接続をAzure AVSプライベートクラウドを含む仮想ネットワークゲートウェイに接続します。

EXPRESSROUTEを仮想ネットワークゲートウェイに接続する

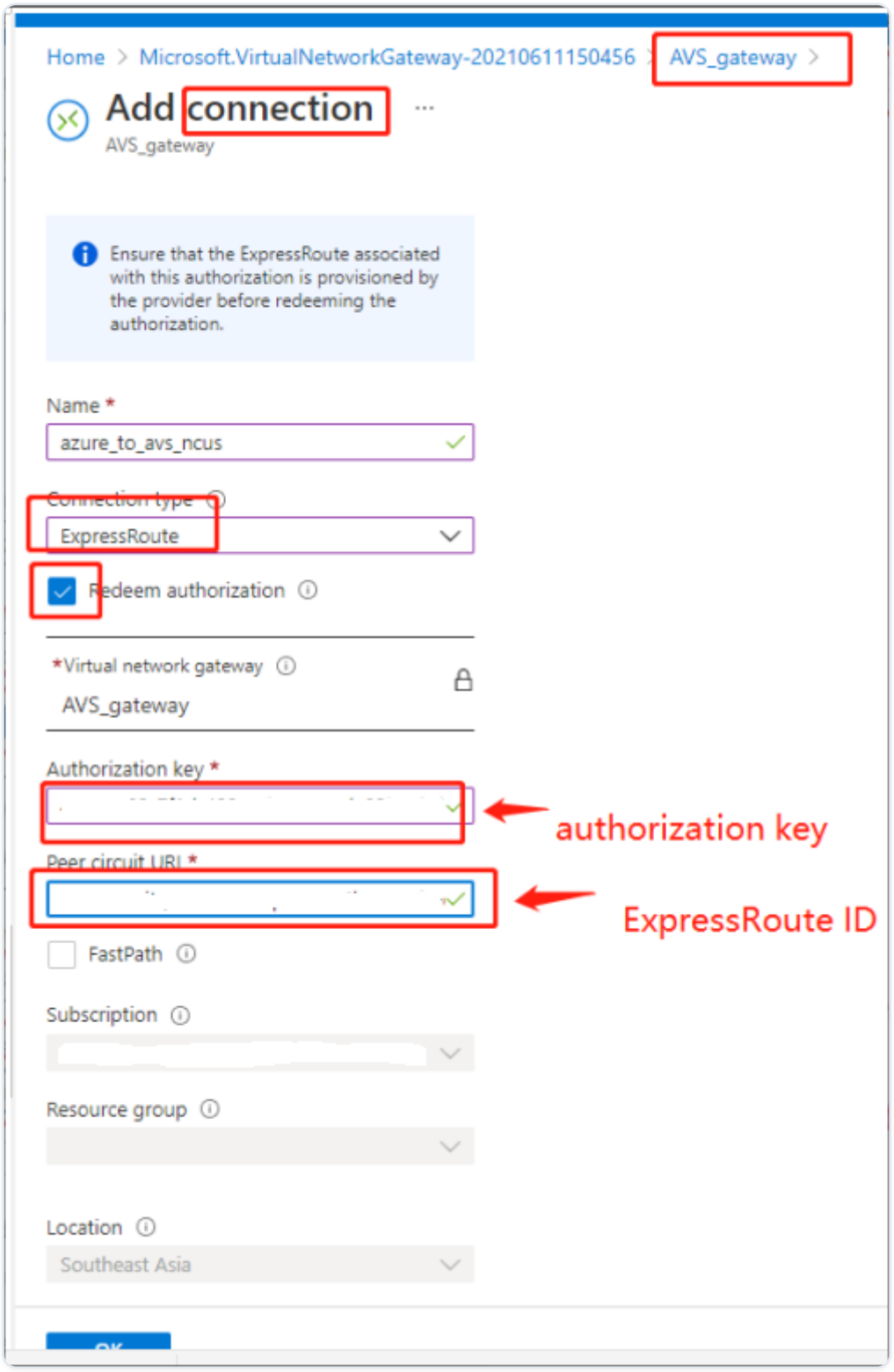
仮想ネットワークゲートウェイをデプロイした後、それとAzure AVSプライベートクラウドの間に接続を追加します。

1. ExpressRoute承認キーを要求します。
2. Azureポータルで、**Azure VMware Solution private cloud**に移動します。「**Manage> Connectivity > ExpressRoute**」を選択し、次に「**+ Request an authorization key**」を選択します。

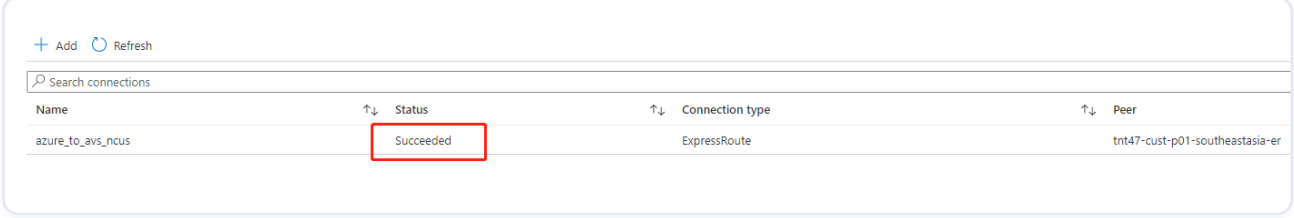
Azure ASV 承認キーの要求(/en-us/citrix-virtual-apps-desktops/2311/media/azure-avs-expressroute.png)

承認キーを要求した後：

1. キーの名前を入力し、**作成**をクリックします。キーの作成には約30秒かかる場合があります。作成されると、新しいキーはプライベートクラウドの承認キーのリストに表示されます。
2. **承認キー**と**ExpressRoute ID**をコピーします。これらはピアリングプロセスを完了するために必要です。承認キーはしばらくすると消えるため、表示されたらすぐにコピーしてください。
3. 使用する**仮想ネットワークゲートウェイ**に移動し、**接続 > + 追加**を選択します。
4. **接続の追加**ページで、フィールドに値を入力し、**OK**を選択します。



ExpressRoute 回線と仮想ネットワーク間の接続が確立されます。



AZURE VMWARE SOLUTION の DHCP を構成する

ExpressRoute を仮想ゲートウェイに接続した後、DHCP を構成します。
NSX-T を使用して DHCP サーバーをホストする
NSX-T Manager で、次の手順を実行します。

1. **ネットワーク > DHCP**を選択し、**サーバーの追加**を選択します。
2. **サーバーの種類**で**DHCP**を選択し、サーバー名と IP アドレスを指定します。
3. **保存**をクリックします。
4. **Tier 1 ゲートウェイ**を選択し、Tier-1 ゲートウェイの縦の省略記号を選択してから、**編集**を選択します。
5. サブネットを追加するには、**IP 割り当てが設定されていません**を選択します。
6. 「**Type**」には「**DHCP Local Server**」を選択します。
7. 「**DHCP Server**」には「**Default DHCP**」を選択し、「**Save**」をクリックします。
8. もう一度「**Save**」をクリックし、「**Close Editing**」を選択します。

Azure ASVでNSX-Tサーバーを追加(/en-us/citrix-virtual-apps-desktops/2311/media/azure-avs-nsx-t-add-server.png)

AZURE VMWARE SOLUTIONでネットワークセグメントを追加する

DHCPを設定したら、ネットワークセグメントを追加します。

ネットワークセグメントを追加するには、NSX-T Managerで、**Networking> Segments** を選択し、**Add Segment** をクリックします。

Azure ASVでNSX-Tセグメントを追加(/en-us/citrix-virtual-apps-desktops/2311/media/azure-avs-nsx-t-add-segment.png)

「**Segments profile**」画面で：

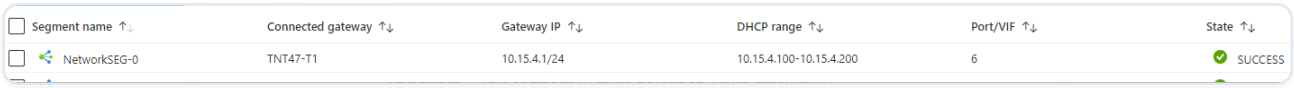
1. セグメントの「**name**」を入力します。
2. 「**Connected Gateway**」として「**Tier-1 Gateway (TNTxx-T1)**」を選択し、「**Type**」は「**Flexible**」のままにします。
3. 事前構成されたオーバーレイ「**Transport Zone(TNTxx-OVERLAY-TZ)**」を選択します。
4. 「**Set Subnets**」をクリックします。

Azure ASVでNSX-Tセグメントプロファイルを追加(/en-us/citrix-virtual-apps-desktops/2311/media/azure-avs-nsx-t-segment-profiles.png)

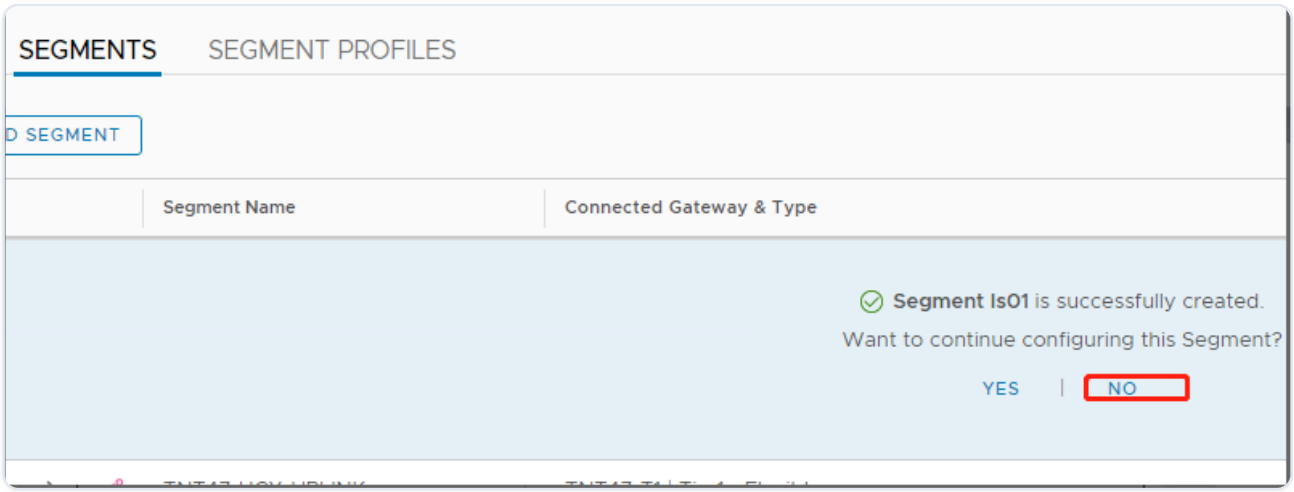
「**Subnets**」セクションで：

1. ゲートウェイIPアドレスを入力します。
2. **Add**を選択します。

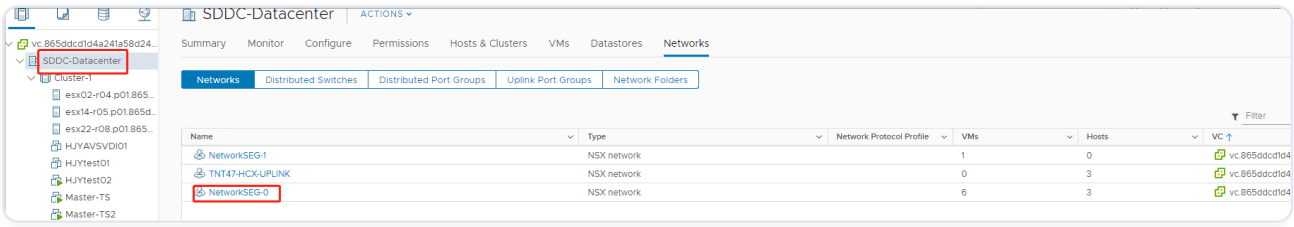
> **重要:**
>
> このセグメントのIPアドレスは、Azureゲートウェイ IPアドレス10.15.0.0/22に属している必要があります。
>
> DHCP範囲はセグメントIPアドレスに属している必要があります。



セグメントの構成を続行するオプションを拒否するには、 を選択します:

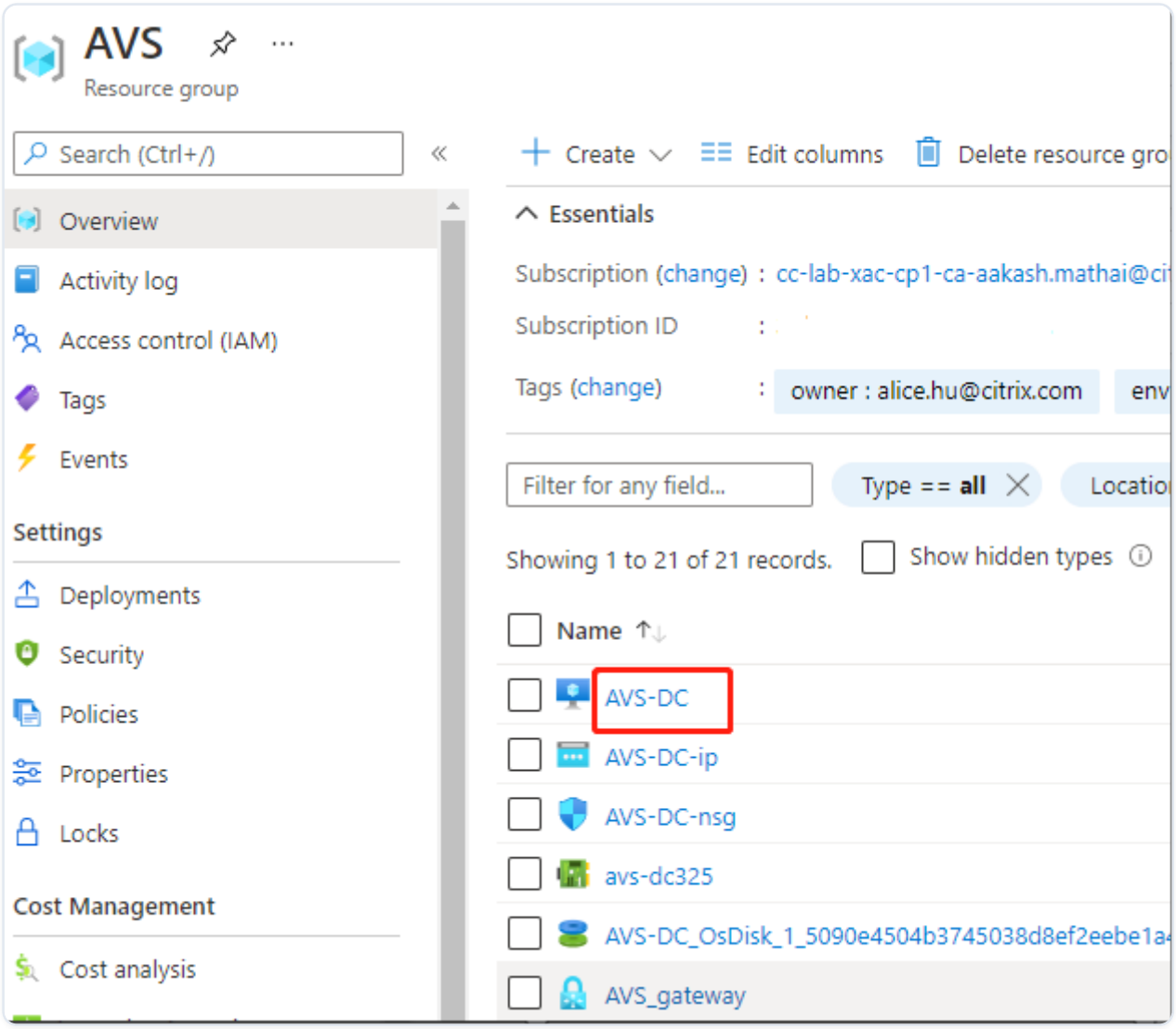


vCenterで、 **>** を選択します:

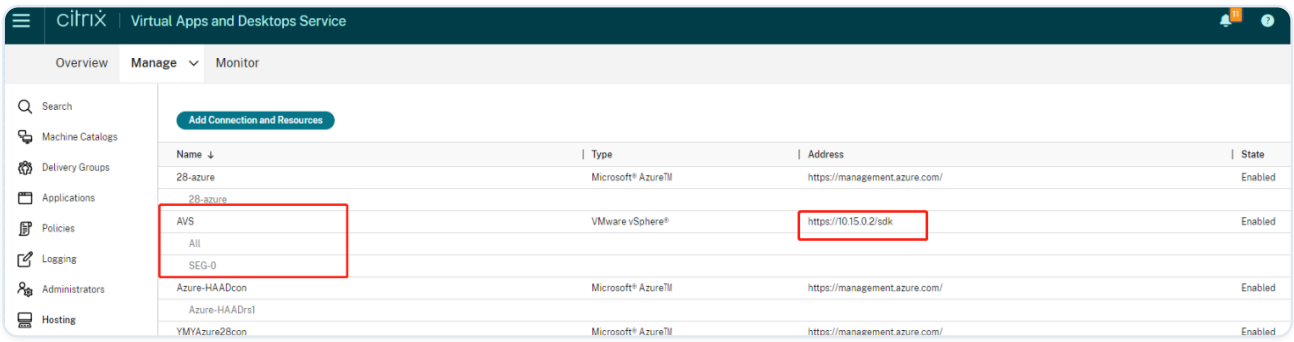


AZURE AVS環境を確認します

Azureリソースグループで直接接続とコネクタを設定します。



vCenterの資格情報で接続を確認します。



グーグル クラウド ヴィエムウェア エンジン

Citrix Virtual Apps and Desktopsを使用すると、VMwareベースのオンプレミスCitrixワークロードをGoogle Cloud VMware Engineに移行できます。

Google Cloud VMware Engineを構成する

以下の手順では、Google Cloud VMware Engineでクラスターを取得してセットアップする方法について説明します。

VMWARE ENGINEポータルにアクセスする

1. **Google Cloud Console**で、ナビゲーションメニューをクリックします。
2. **Compute**セクションで、**VMware Engine**をクリックして、新しいブラウザタブでVMware Engineを開きます。

最初のプライベートクラウドを作成するための要件

Google Cloud VMware Engineへのアクセス、利用可能なVMware Engineノードクォータ、および適切なIAMロールが必要です。プライベートクラウドの作成を続行する前に、以下の要件を準備してください。

1. APIアクセスとノードクォータをリクエストします。詳細については、「APIアクセスとクォータのリクエスト」を参照してください。
2. VMware管理アプライアンスおよびHCX展開ネットワークに使用するアドレス範囲をメモします。詳細については、「ネットワーク要件」を参照してください。
3. VMware Engine Service Admin IAMロールを取得します。

最初のプライベートクラウドを作成する

1. VMware Engineポータルにアクセスします。
2. VMware Engineのホームページで、**プライベートクラウドの作成**をクリックします。ホスティングの場所とハードウェアノードの種類が一覧表示されます。
3. プライベートクラウドのノード数を選択します。少なくとも3つのノードが必要です。
4. VMware管理ネットワークのクラスレスドメイン間ルーティング（CIDR）範囲を入力します。
5. HCX展開ネットワークのCIDR範囲を入力します。

> **重要:**
>
> CIDR範囲は、オンプレミスまたはクラウドのサブネットと重複してはなりません。
> CIDR範囲は/27以上である必要があります。

6. を選択します。
7. 設定を確認します。設定を変更するには、 をクリックします。
8. をクリックして、プライベートクラウドの作成を開始します。

VMware Engineが新しいプライベートクラウドを作成すると、いくつかのVMwareコンポーネントが展開され、プライベートクラウド内のクラスターの初期Autoscale™ポリシーが設定されます。

プライベートクラウドの作成には30分から2時間かかる場合があります。プロビジョニングが完了すると、メールが届きます。

GOOGLE CLOUD VMWARE ENGINE VPNゲートウェイをセットアップする

Google Cloud VMware Engineへの初期接続を確立するには、VPNゲートウェイを使用できます。これはOpenVPNベースのクライアントVPNであり、これを使用してVMware Software Defined Data Center (SDDC) vCenterに接続し、必要な初期構成を行うことができます。

VPNゲートウェイを展開する前に、SDDCが展開されているリージョンの**Edge Services**範囲を構成します。これを行うには：

1. **Google Cloud VMware Engine**ポータルにログオンし、 **>** に移動します。 をクリックします。
2. SDDCが展開されているリージョンを選択し、 と を有効にします。
3. 計画中にメモしたEdge Servicesの範囲を入力し、 をクリックします。これらのサービスを有効にするには10～15分かかります。

   完了すると、エッジサービスは地域設定ページで**有効**と表示されます。これらの設定を有効にすると、パブリックIPがSDDCに割り当てられるようになり、これはVPNゲートウェイを展開するための要件です。

VPNゲートウェイを展開するには：

1. **Google Cloud VMware Engine**ポータルで、**ネットワーク > VPNゲートウェイ**に移動します。**新しいVPNゲートウェイの作成**をクリックします。
2. VPNゲートウェイの名前と、計画中に予約したクライアントサブネットを入力します。**次へ**をクリックします。
3. VPNアクセスを許可するユーザーを選択します。**次へ**をクリックします。
4. VPN経由でアクセス可能にする必要があるネットワークを指定します。**次へ**をクリックします。
5. 概要画面が表示されます。選択内容を確認し、**送信**をクリックしてVPNゲートウェイを作成します。VPNゲートウェイページには、新しいVPNゲートウェイのステータスが**作成中**と表示されます。
6. ステータスが**稼働中**に変わったら、新しいVPNゲートウェイをクリックします。
7. **VPN構成をダウンロード**をクリックして、VPNゲートウェイ用の事前設定済みOpenVPNプロファイルを含むZIPファイルをダウンロードします。UDP/1194およびTCP/443経由で接続するためのプロファイルが利用可能です。好みのものを選択してOpen VPNにインポートし、接続します。

8. **リソース**に移動し、SDDCを選択します。

VPNを接続する

1. VPNゲートウェイの設定を通じて、オンプレミスネットワークとプライベートクラウド間のポイントツーサイト接続を確立します。Google Cloud VMware Engine VPNゲートウェイのセットアップを参照してください。
2. Google Cloud VMware Engine VPNゲートウェイのセットアップでダウンロードしたVPN構成をアップロードします。
3. VPNクライアント（例：OpenVPN Connect）にインポートします。

詳細については、VPNを使用した接続を参照してください。

最初のサブネットを作成する

VMware EngineポータルからNSX-T Managerにアクセスする
サブネットの作成プロセスはNSX-Tで行われ、VMware Engineを介してアクセスします。NSX-T Managerにアクセスするには、次の手順を実行します。

1. **Google Cloud VMware Engine** ポータルにログオンします。
2. メインナビゲーションから、**リソース** に移動します。
3. サブネットを作成するプライベートクラウドに対応する **プライベートクラウド名** をクリックします。
4. プライベートクラウドの詳細ページで、**vSphere Management Network** タブをクリックします。
5. NSX-T Managerに対応する **FQDN** をクリックします。
6. プロンプトが表示されたら、サインイン資格情報を入力します。vIDMを設定し、Active DirectoryなどのIDソースに接続している場合は、代わりにIDソースの資格情報を使用します。

> **注意:**
>
> 生成された資格情報は、プライベートクラウドの詳細ページから取得できます。

サブネットのDHCPサービスを設定する
サブネットを作成する前に、DHCPサービスを設定します。

NSX-T マネージャーで：

1. **ネットワーク > DHCP** に移動します。ネットワークダッシュボードには、DHCPサービスが1つのTier-0と1つのTier-1ゲートウェイを作成することが示されます。
2. DHCPサーバーのプロビジョニングを開始するには、 をクリックします。
3. に を選択し、サーバー名とIPアドレスを指定します。
4. をクリックしてDHCPサービスを作成します。

このDHCPサービスを関連するTier-1ゲートウェイに接続するには、次の手順を実行します。デフォルトのTier-1ゲートウェイは、DHCPサービスによってすでにプロビジョニングされています。

1. を選択し、Tier-1ゲートウェイの縦の省略記号を選択してから、 を選択します。
2. フィールドで、 を選択します。
3. に を選択します。
4. に、作成したDHCPサーバーを選択します。
5. をクリックします。
6. をクリックします。

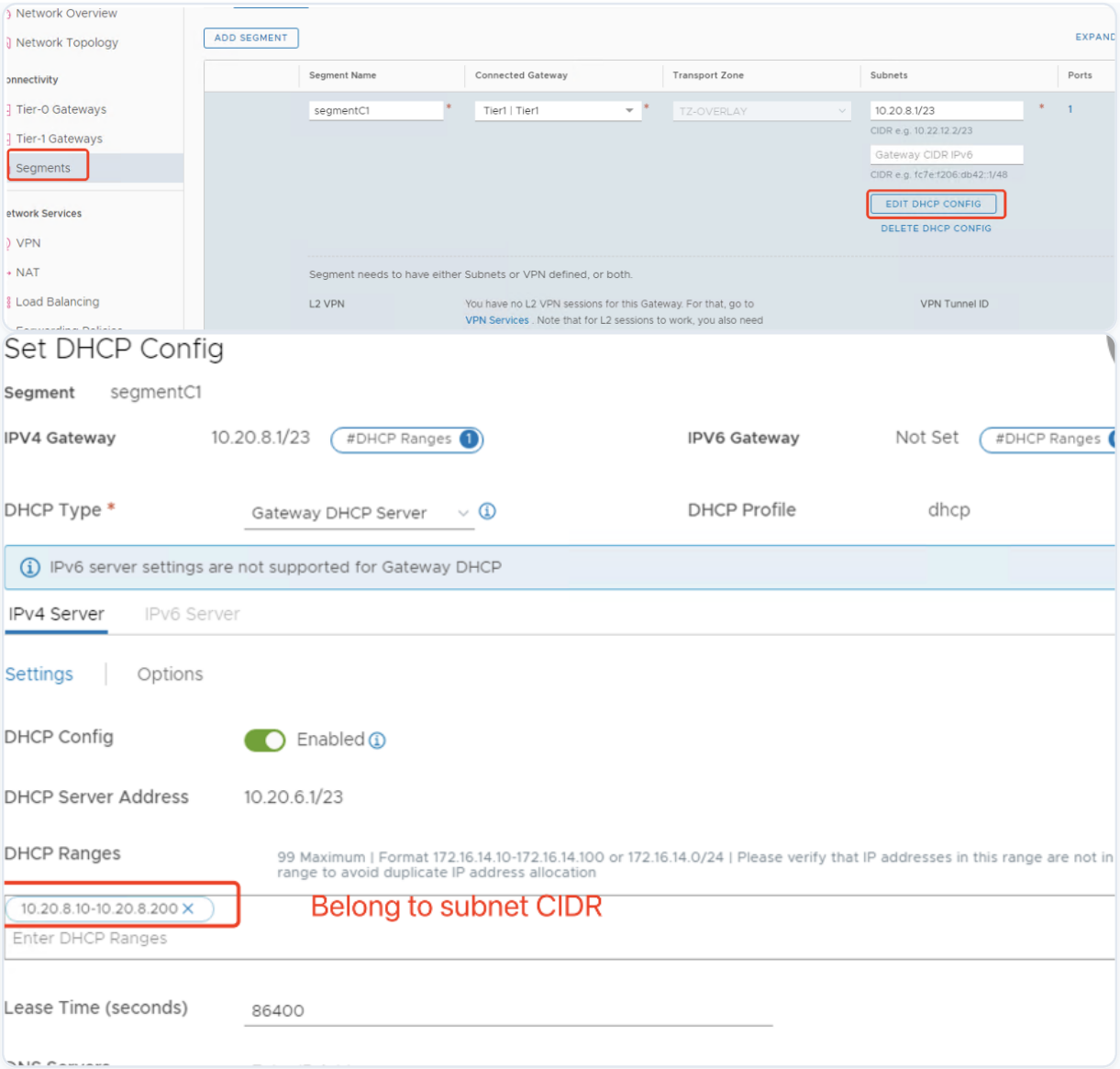
これで、NSX-Tでネットワークセグメントを作成できます。NSX-TでのDHCPの詳細については、VMwareのDHCPに関するドキュメントを参照してください。
NSX-T でネットワークセグメントを作成する
ワークロード VM の場合、プライベートクラウドの NSX-T ネットワークセグメントとしてサブネットを作成します。

1. NSX-T Managerで、 **>** に移動します。
2. をクリックします。
3. セグメントの名前を入力します。
4. **Connected Gateway**として**Tier-1**を選択し、Typeは**Flexible**のままにします。
5. **Set Subnets**をクリックします。
6. **Add Subnets**をクリックします。
7. **Gateway IP/Prefix Length**にサブネット範囲を入力します。サブネット範囲は、最後のオクテットを**.1**として指定します。例: **10.12.2.1/24**。
8. DHCP範囲を指定し、**ADD**をクリックします。
9. 「**Transport Zone**」で、ドロップダウンリストから「**TZ-OVERLAY**」を選択します。
10. **Save**をクリックします。これで、VMの作成時にvCenterでこのネットワークセグメントを選択できるようになります。

特定のリージョンでは、VMware EngineからVPC networkへのプライベートサービスアクセスを使用して、最大100個の一意のルートを設定できます。これには、たとえば、プライベートクラウド管理IPアドレス範囲、NSX-Tワークロードネットワークセグメント、HCXネットワークIPアドレス範囲が含まれます。この制限には、リージョン内のすべてのプライベートクラウドが含まれます。

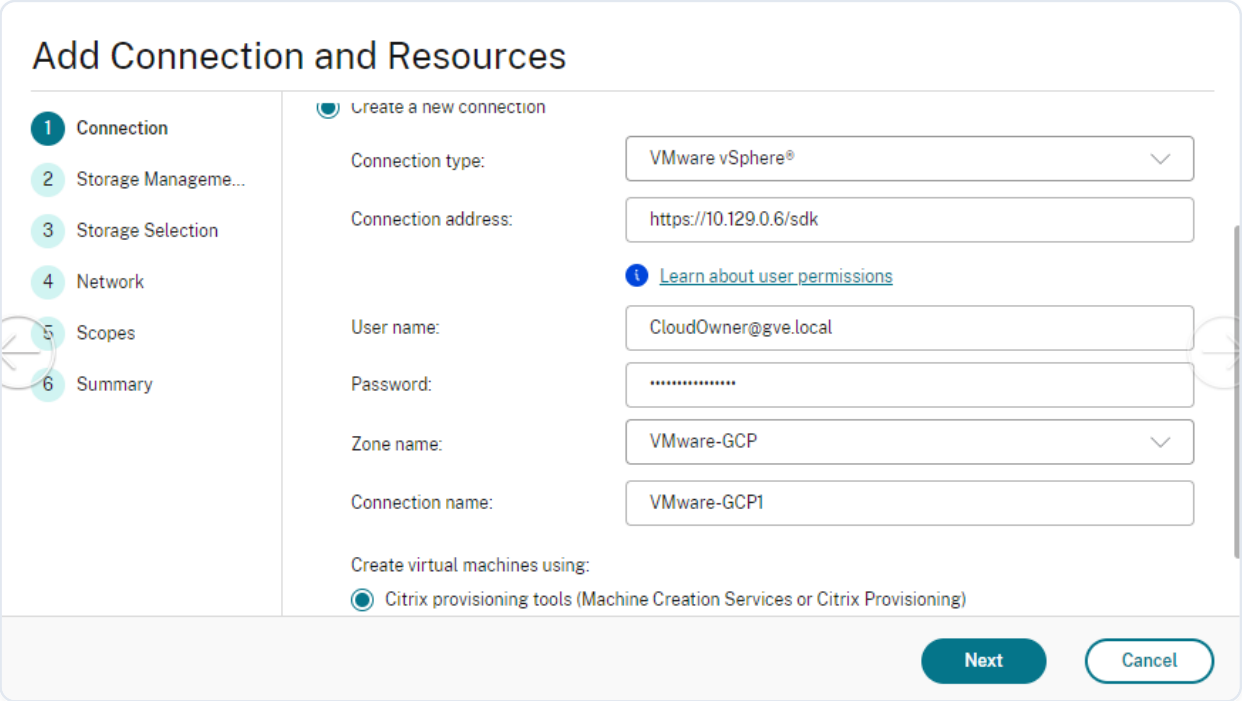
注:

Google Cloudの構成の問題により、DHCP範囲設定を複数回構成する必要があります。したがって、Google Cloudの構成後にDHCP範囲設定を構成するようにしてください。DHCP範囲を構成するには、**EDIT DHCP CONFIG**をクリックします。



CITRIX STUDIOでGOOGLE CLOUD VMWARE接続を作成する

1. vCenterでマシンを作成します。
2. Citrix Studioを起動します。
3. ホスティングノードを選択し、**接続とリソースの追加**をクリックします。
4. **接続**画面で、**新しい接続の作成**を選択し、次の詳細を入力します。



   a. **接続の種類**として**VMware vSphere**を選択します。
   b. **接続アドレス**に、vCenterのプライベートIPアドレスを入力します。
   c. vCenterの資格情報を入力します。
   d. 接続名を入力します。
   e. 仮想マシンを作成するツールを選択します。

5. **ネットワーク**画面で、NSX-Tサーバーで作成されたサブネットを選択します。
6. ウィザードを完了します。

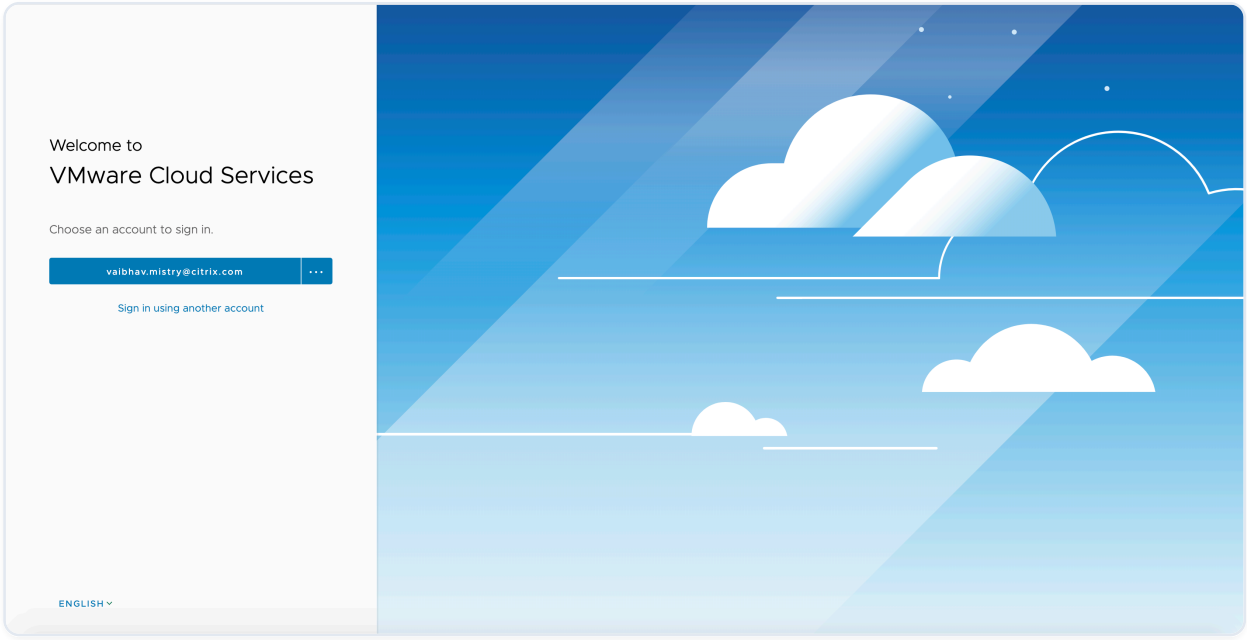
アマゾン ウェブ サービス (AWS) 上の ヴイエムウェア クラウド

Amazon Web Services (AWS) 上のVMware Cloudを使用すると、VMwareベースのオンプレミスCitrixワークロードをAWS Cloudに移行できます。

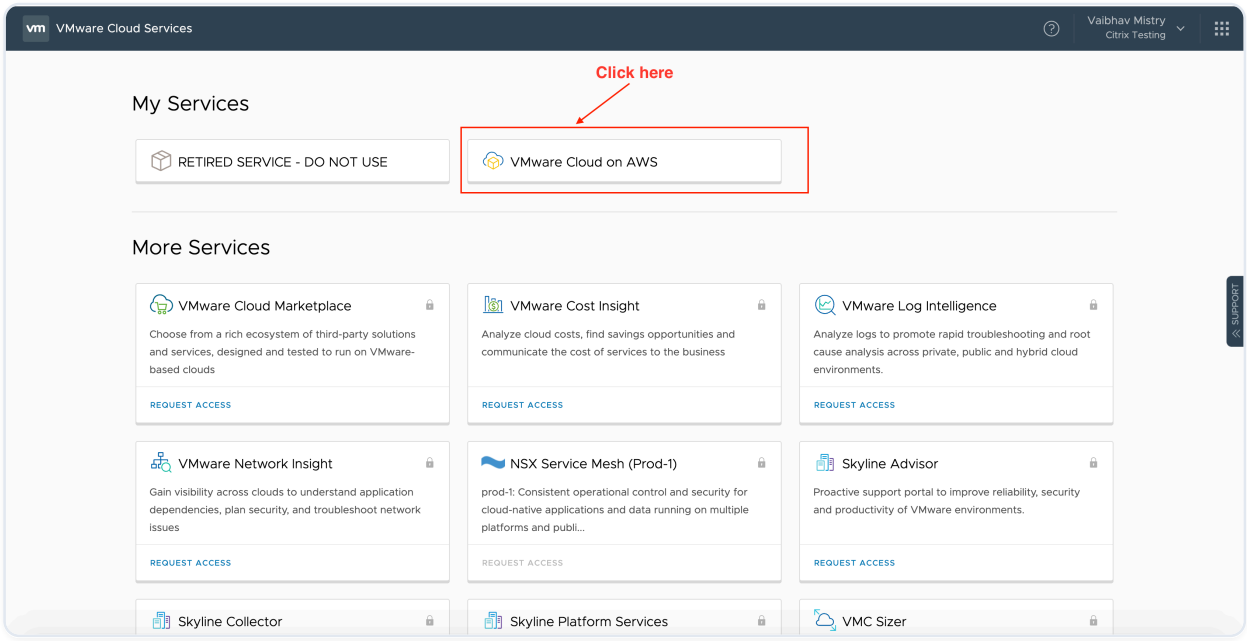
この記事では、AWS上にVMware Cloudをセットアップする手順について説明します。

VMware Cloud環境にアクセスする

1. URL `<https://console.cloud.vmware.com/>`を使用してVMware Cloudサービスにログインします。



2. 「**VMware Cloud on AWS**」をクリックします。「Software-Defined Data Centers (SDDC)」ページが表示されます。



3. **OPEN VCENTER** をクリックし、次に **SHOW CREDENTIALS** をクリックします。後で使用するために資格情報をメモしておきます。

「vCenterを開く」(/en-us/citrix-virtual-apps-desktops/2311/media/vmc-sddc.png)

「資格情報を表示」(/en-us/citrix-virtual-apps-desktops/2311/media/show-credentials-vmc.png)

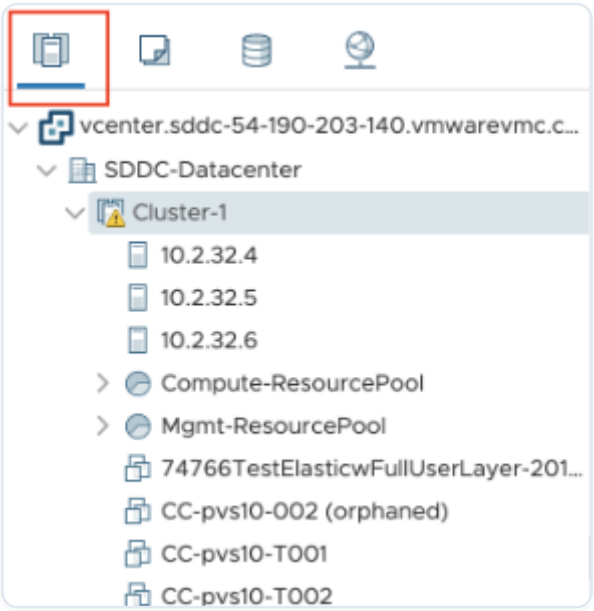
4. Webブラウザを開き、vSphere Web Client の URL を入力します。
5. メモした資格情報を入力し、**Login** をクリックします。vSphere クライアントのWebページは、オンプレミス環境のものと似ています。

   「vSphereクライアントのWebページ」(/en-us/citrix-virtual-apps-desktops/2311/media/vcenter-page.png)

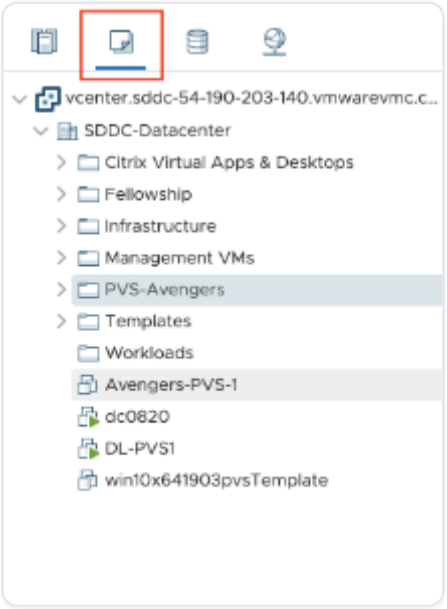
VMwareクラウド環境について

vSphereクライアントのWebページには4つのビューがあります。

- ホストとクラスタビュー: 新しいクラスタを作成することはできませんが、クラウド管理者は複数のリソースプールを作成できます。



- VMとテンプレートビュー: クラウド管理者は多くのフォルダを作成できます。



- ストレージビュー: Citrix Studioでホスティングユニットを追加する際は、**WorkloadDatastore**ストレージを選択してください。Workload Datastoreにのみアクセスできるためです。

  「ストレージビュー」(/en-us/citrix-virtual-apps-desktops/2311/media/storage-view.png)

- ネットワークビュー: VMwareクラウドネットワークと不透明なネットワークでは、アイコンが異なります。

  「ネットワークビュー」(/en-us/citrix-virtual-apps-desktops/2311/media/network-view.png)

クラスターをセットアップした後、接続とリソースを追加するには、VMware仮想化環境を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- 接続の作成と管理については、VMwareクラウドおよびパートナーソリューションへの接続を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

コアコンポーネントをインストールする

> **重要:**

> Citrix は、ライセンスコンプライアンスを含む正当な利益のために、必要に応じて基本的なライセンスデータを収集します。詳細については、「Citrix ライセンスデータ」を参照してください。

> コアコンポーネントは、Citrix Delivery Controller™、Citrix Studio、Web Studio、Citrix Director、および Citrix License Server です。

> **注:**

> Citrix Studio は、オンプレミスの Citrix Virtual Apps and Desktops 展開を構成および管理できる Windows ベースの管理コンソールです。Web Studio は、Citrix Studio の次世代版であり、Citrix Studio と同等の機能を備えた Web ベースの管理コンソールです。Web Studio の詳細については、「Web Studio のインストール」を参照してください。

> (2003 より前のバージョンでは、コアコンポーネントに Citrix StoreFront が含まれていました。**Citrix StoreFront** タイルをクリックするか、インストールメディアで利用可能なコマンドを実行することで、StoreFront をインストールできます。)

インストールを開始する前に、この記事と「インストールの準備」を確認してください。

この記事では、コアコンポーネントのインストール時のインストールウィザードのシーケンスについて説明します。コマンドラインの同等機能が提供されています。詳細については、「コマンドラインを使用したインストール」を参照してください。

ステップ 1. 製品ソフトウェアをダウンロードしてウィザードを起動する

Citrix アカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ のダウンロードページにアクセスします。製品の ISO ファイルをダウンロードします。

ファイルを解凍します。必要に応じて、ISO ファイルを DVD に書き込みます。

コアコンポーネントをインストールするマシンに、ローカル管理者アカウントを使用してログオンします。

DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。

ステップ 2. インストールする製品を選択する

コンポーネントインストーラーの製品選択ページ (/en-us/citrix-virtual-apps-desktops/2311/media/product-selector2-75.png)

インストールする製品（Virtual AppsまたはVirtual Apps and Desktops）の横にある **Start** をクリックします。

（マシンにCitrix Virtual Apps and Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。）

コマンドラインオプション: Citrix Virtual Appsをインストールするには `/xenapp`。このオプションを省略すると、Citrix Virtual Apps and Desktopsがインストールされます。

ステップ 3. インストールするものを選択する

コンポーネントインストーラーのコンポーネント選択ページ (/en-us/citrix-virtual-apps-desktops/2311/media/what-to-install-2.png)

初めて使用する場合は、**Delivery Controller** を選択します。（後のページで、このマシンにインストールする特定のコンポーネントを選択します。）

すでにControllerをインストールしている場合（このマシンまたは別のマシンに）、別のコンポーネントをインストールするには、**Extend Deployment** セクションからそのコンポーネントを選択します。

コマンドラインオプション: `/components`

ステップ 4. ライセンス契約を読んで同意する

コンポーネントインストーラーのライセンス契約ページ (/en-us/citrix-virtual-apps-desktops/2311/media/core-license-75.png)

Licensing Agreement ページで、ライセンス契約を読んだ後、内容を読み、同意したことを示します。次に **Next** をクリックします。

ステップ 5. インストールするコンポーネントとインストール場所を選択する

コンポーネントインストーラーのコアコンポーネントページ (/en-us/citrix-virtual-apps-desktops/2311/media/core-components-75.png)

Core components ページで:

- **場所:** コンポーネントはデフォルトで `C:\Program Files\Citrix` にインストールされます。ほとんどの展開では、デフォルトで問題ありません。別の場所を指定する場合、その場所にはネットワークサービスに対する実行権限が必要です。
- **コンポーネント:** デフォルトでは、すべてのコアコンポーネントのチェックボックスが選択されています。すべてのコアコンポーネントを1つのサーバーにインストールすることは、概念実証、テスト、または小規模な本番展開には問題ありません。大規模な本番環境の場合、CitrixはDirector、StoreFront、およびLicense Serverを別々のサーバーにインストールすること

を推奨します。Secure Private AccessはStoreFrontと一緒にインストールすることをお勧めします。

> **注:**
>
> 複数のサーバーにコンポーネントをインストールする場合は、他のサーバーに他のコンポーネントをインストールする前に、Citrix License Serverとライセンスを最初にインストールしてください。詳細については、Citrix Virtual Apps and Desktopsのライセンスガイドの「自動インストール」セクションを参照してください。

> このマシンに必須のコアコンポーネントをインストールしないことを選択した場合、アイコンで警告が表示されます。この警告は、そのコンポーネントをインストールするように促しますが、必ずしもこのマシンにインストールする必要はありません。

Nextをクリックします。

コマンドラインオプション: `/installdir`、`/components`、`/exclude`

ハードウェアチェック

Delivery Controllerをインストールまたはアップグレードすると、ハードウェアがチェックされます。インストーラーは、マシンに推奨されるRAMの量（5 GB）よりも少ない場合に警告を表示します。これはサイトの安定性に影響を与える可能性があります。詳細については、ハードウェア要件を参照してください。

グラフィカルインターフェイス: ダイアログボックスが表示されます。

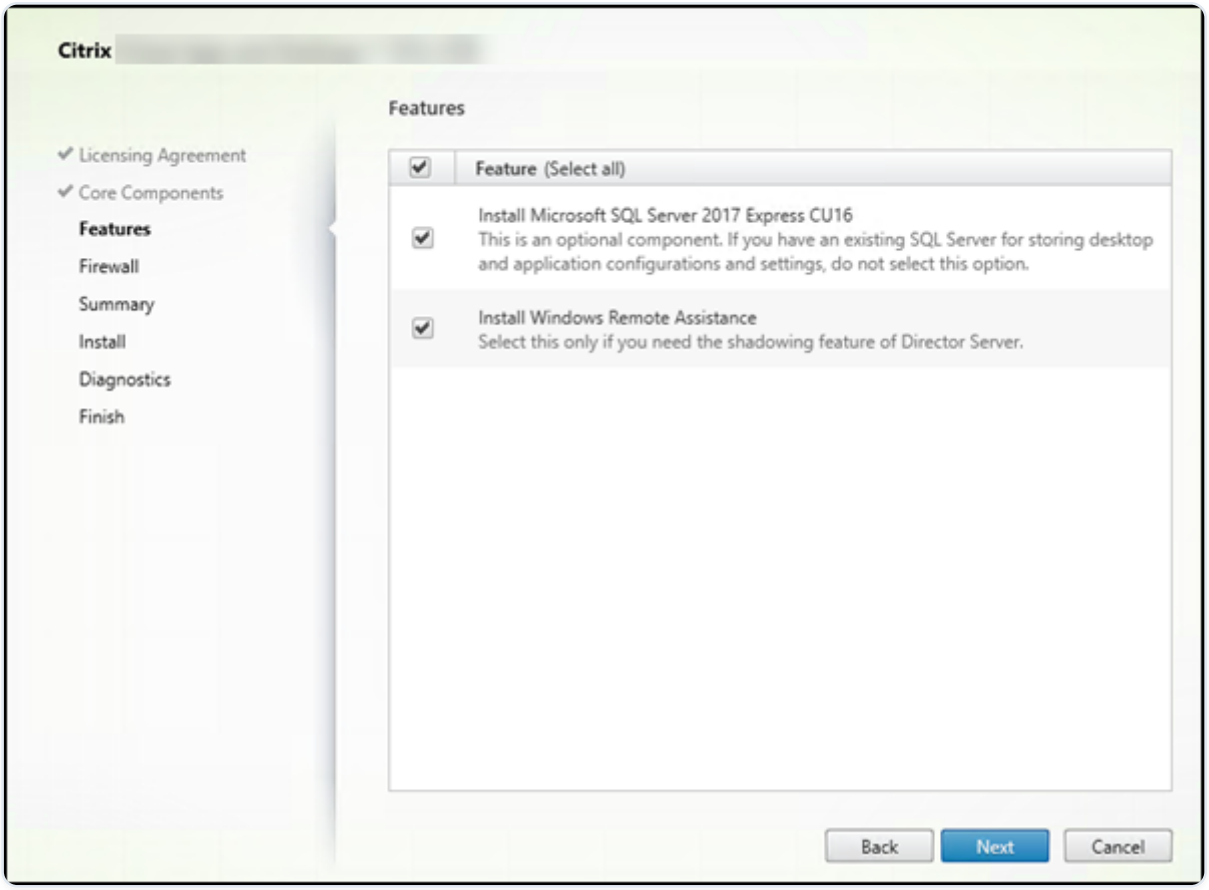
- 推奨: **キャンセル**をクリックしてインストールを停止します。マシンにRAMを追加してから、再度インストールを開始します。
- または、**次へ**をクリックしてインストールを続行します。サイトの安定性に問題が発生する可能性があります。

コマンドラインインターフェイス: インストール/アップグレードが終了します。インストールログには、検出された内容と利用可能なオプションを説明するメッセージが含まれています。

- 推奨: マシンにRAMを追加してから、再度コマンドを実行します。
- または、`/ignore_hw_check_failure`オプションを指定してコマンドを再度実行し、警告を上書きします。サイトの安定性に問題が発生する可能性があります。

アップグレード時には、OS または SQL Server のバージョンがサポートされなくなった場合にも通知されます。詳細については、「展開のアップグレード」を参照してください。

手順 6. 機能の有効化または無効化



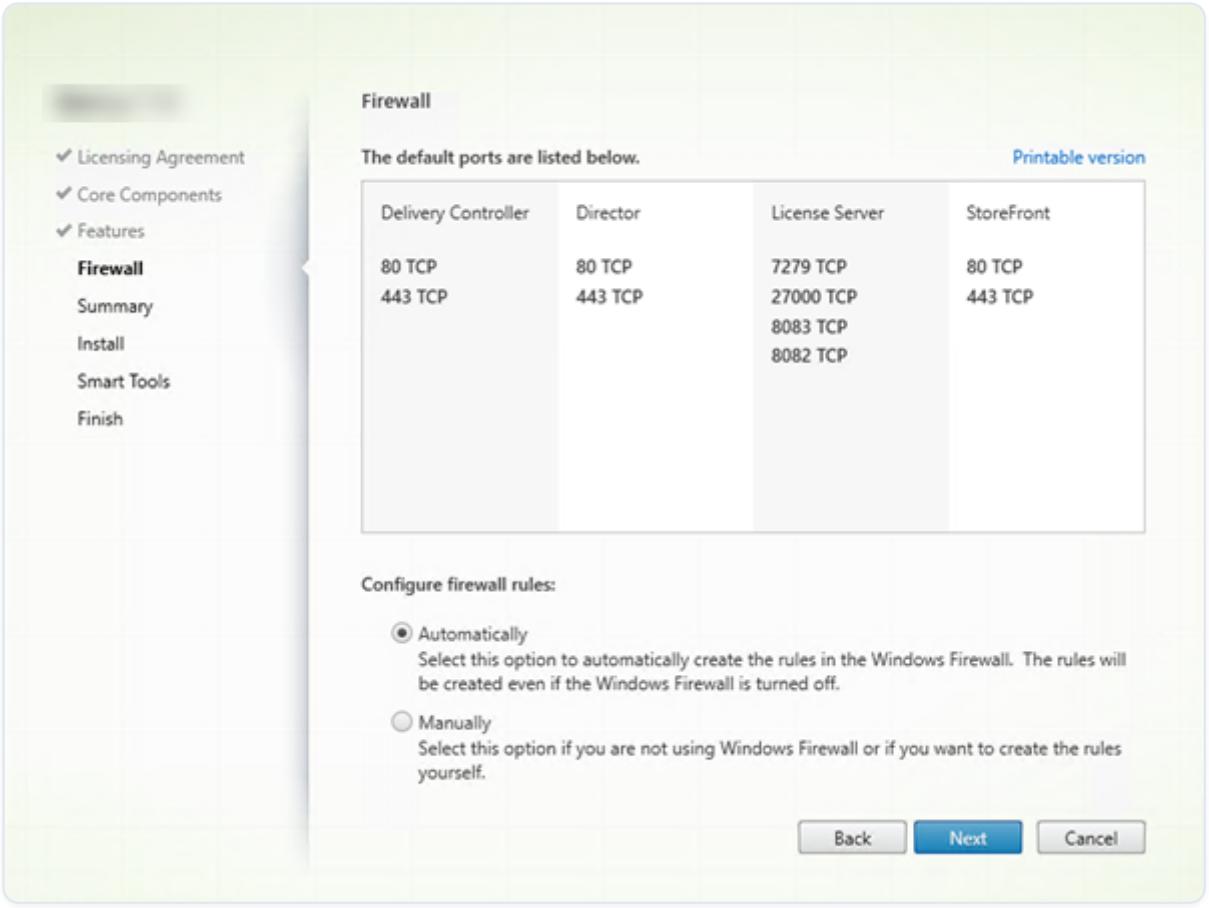
機能ページで：

- サイトデータベースとして使用するためにMicrosoft SQL Server Expressをインストールするかどうかを選択します。デフォルトでは、この選択は有効になっています。Citrix Virtual Apps and Desktopsデータベースに慣れていない場合は、データベースを確認してください。
- Directorをインストールすると、Windowsリモートアシスタンスが自動的にインストールされます。Directorユーザーシャドウイングで使用するために、Windowsリモートアシスタンスでシャドウイングを有効にするかどうかを選択します。シャドウイングを有効にすると、TCPポート3389が開きます。デフォルトでは、この機能は有効になっています。ほとんどの展開では、デフォルト設定で問題ありません。この機能は、Directorをインストールしている場合にのみ表示されます。

Nextをクリックします。

コマンドラインオプション：`/nosql`（インストールを防止するため）、`/no_remote_assistance`（有効化を防止するため）

手順7. Windowsファイアウォールポートを開く



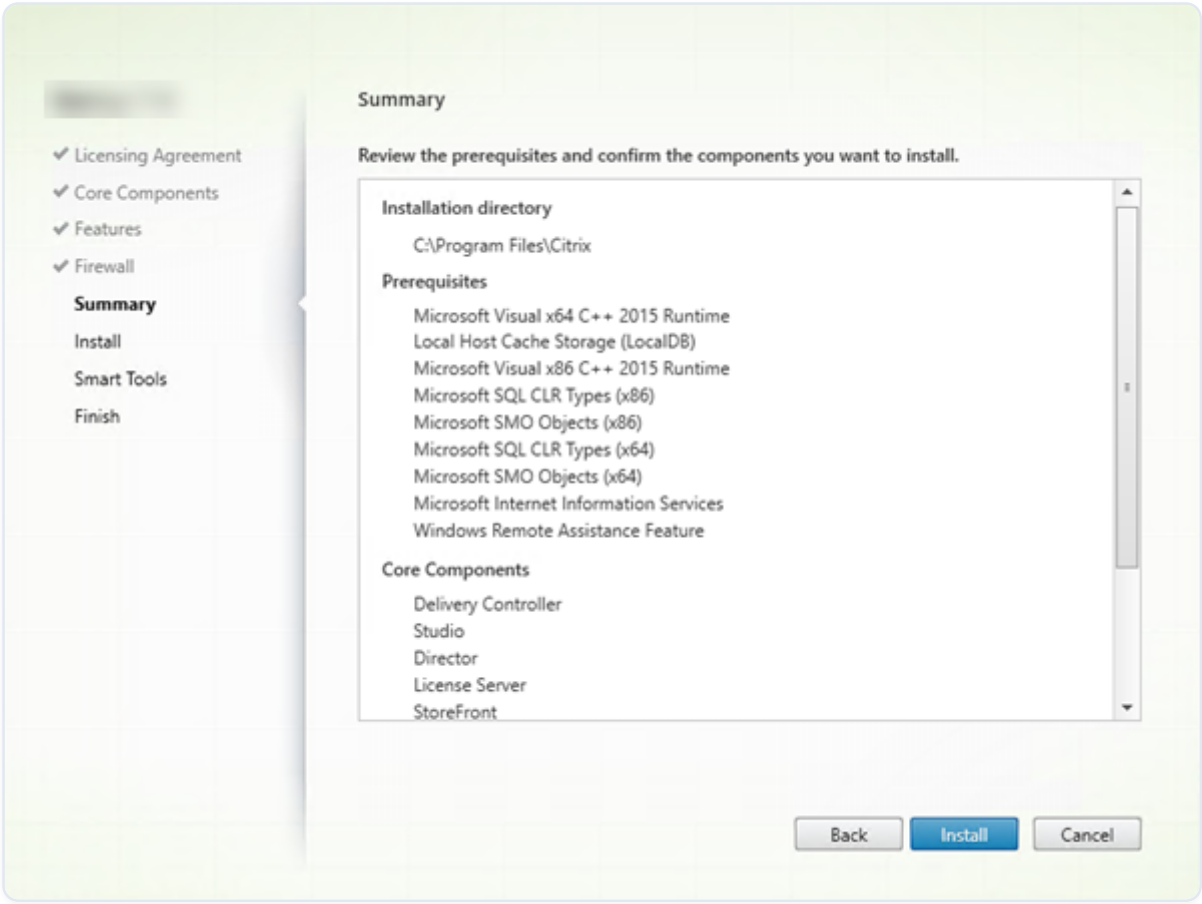
デフォルトでは、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、**ファイアウォール**ページ上のポートは自動的に開かれます。ほとんどの展開では、デフォルト設定で問題ありません。ポート情報については、ネットワークポートを参照してください。

Nextをクリックします。

（このグラフィックは、このマシンにすべてのコアコンポーネントをインストールしたときのポートリストを示しています。この種のインストールは通常、テスト展開のみを対象としています。）

コマンドラインオプション：`/configure_firewall`

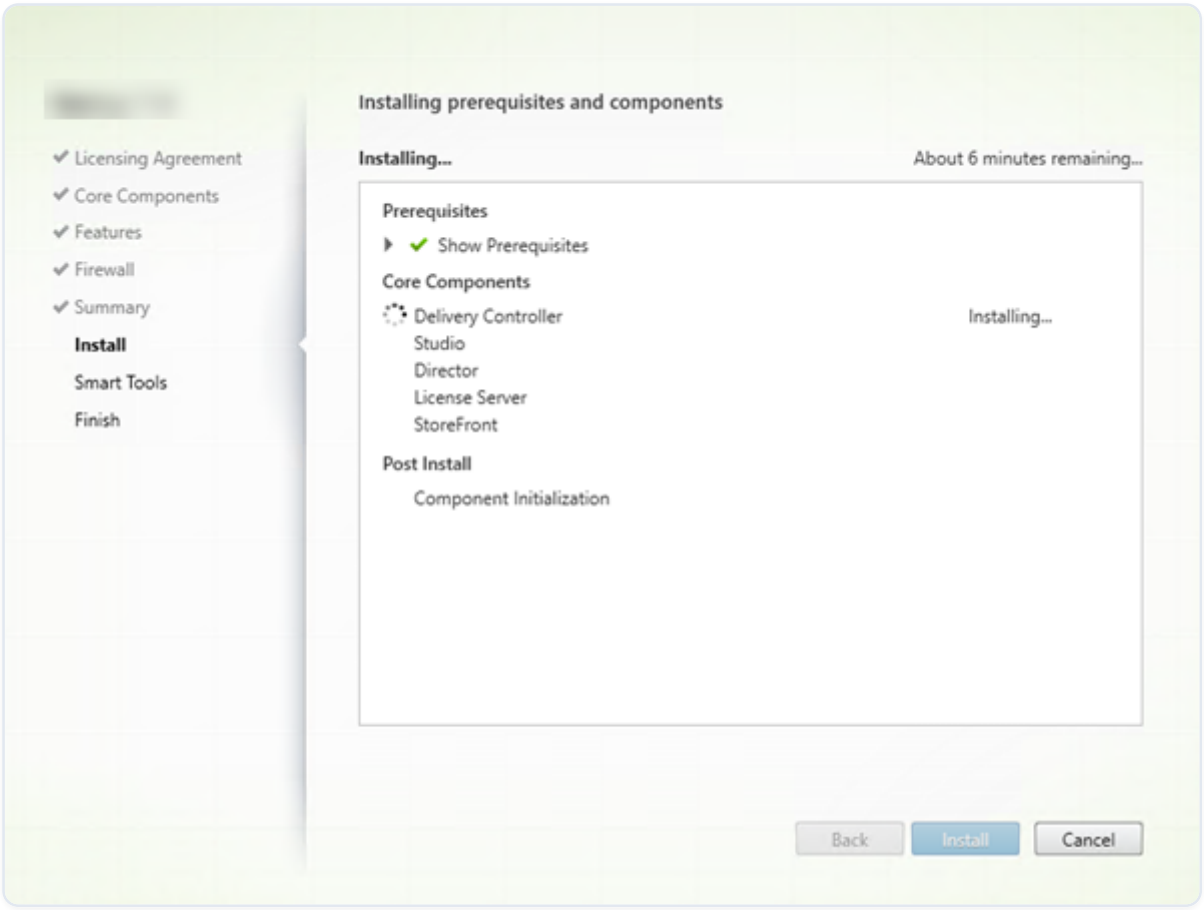
手順8. 前提条件を確認し、インストールを確定する



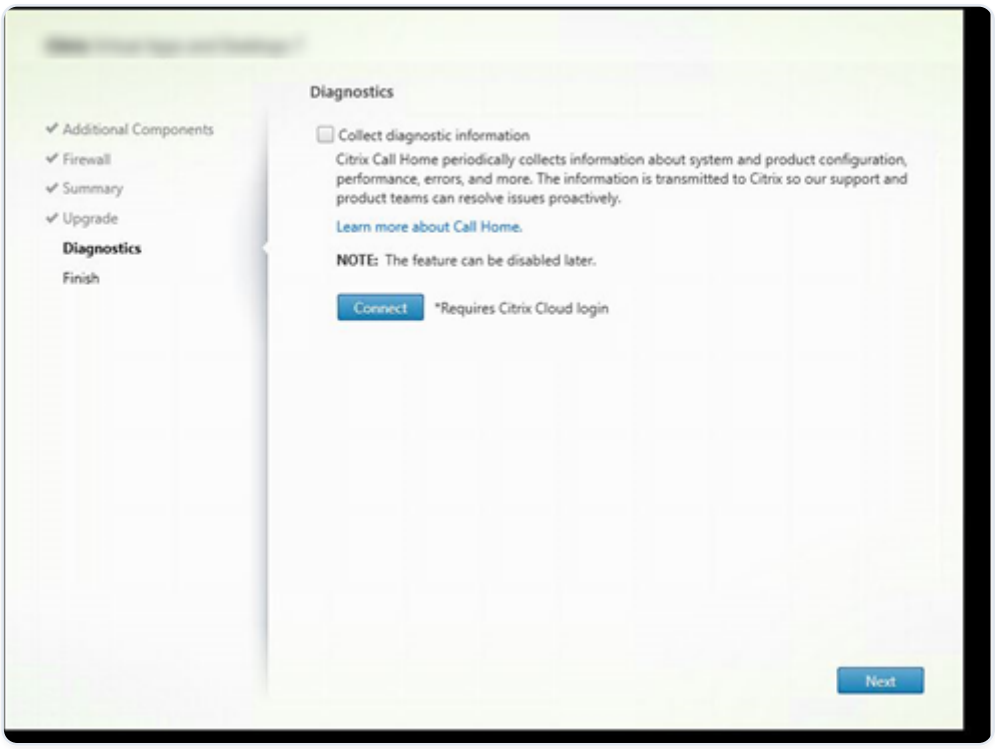
「**概要**」ページには、インストールされるものが表示されます。必要に応じて、「**戻る**」ボタンを使用して以前のウィザードページに戻り、選択を変更してください。

準備ができたら、「**インストール**」をクリックします。

ディスプレイにはインストールの進行状況が表示されます。



ステップ9. 診断情報をCloud Software Groupと共有する



「**診断**」ページで、Citrix Call Homeに参加するかどうかを選択します。

このページは、グラフィカルインターフェイスを使用してDelivery Controllerをインストールするときに表示されます。StoreFrontをインストールする場合（ただしControllerではない場合）、ウィザードはこのページを表示します。その他のコアコンポーネントをインストールする場合（ただしControllerまたはStoreFrontではない場合）、ウィザードはこのページを表示しません。

アップグレード中に、Call Homeがすでに有効になっている場合、またはインストーラーがCitrix Telemetry Serviceに関連するエラーを検出した場合は、このページは表示されません。

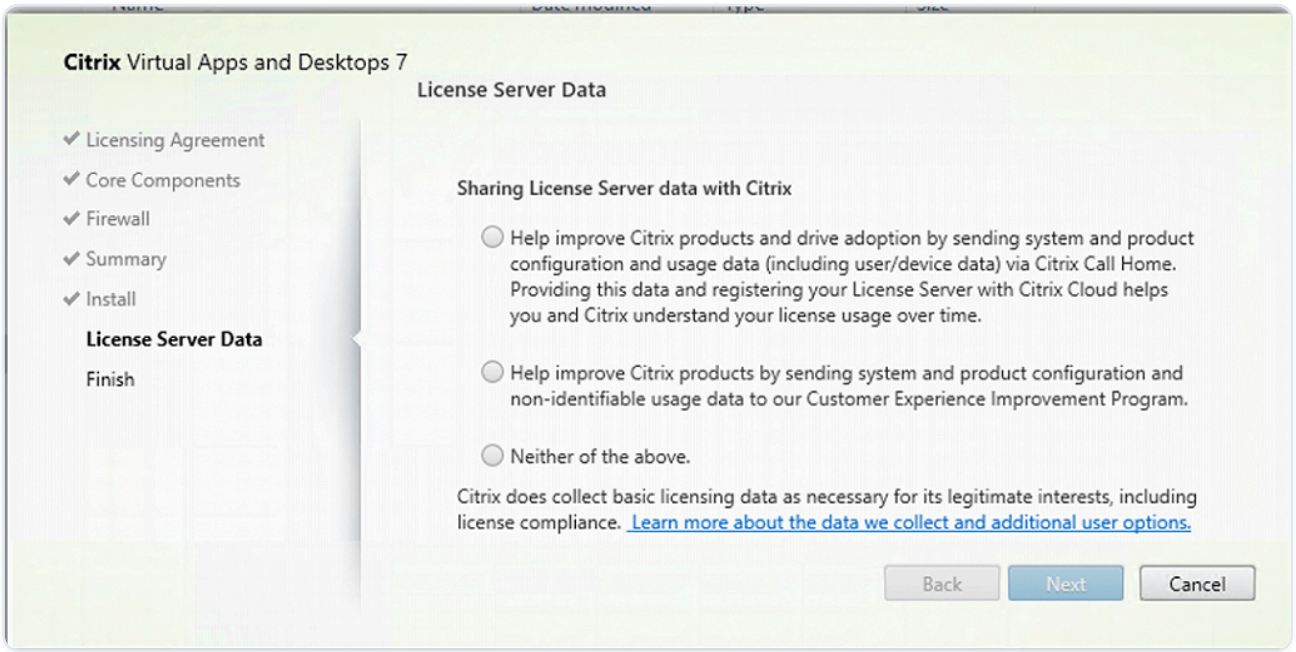
参加することを選択した場合（デフォルト）、「**接続**」をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。登録の選択は、インストール後に変更できます。

資格情報が検証された後（または参加しないことを選択した場合）、「**次へ**」をクリックします。

「**診断**」ページで「**診断情報を収集する**」を最初に選択せずに「**接続**」をクリックすると、「**Citrix Insight Servicesに接続**」ダイアログを閉じた後、「**次へ**」ボタンが無効になります。次のページに進むことはできません。「**次へ**」ボタンを再度有効にするには、「**診断情報を収集する**」を選択し、すぐに選択を解除します。

詳細については、「Call Home」を参照してください。

ステップ10. ライセンスサーバーデータをCloud Software Groupと共有する



「**ライセンスサーバーデータ**」ページでは、お客様にご協力いただくため、Call Homeデータまたはカスタマーエクスペリエンス向上プログラム（CEIP）データのいずれかを共有していただくよ

うお願いしています。さらに、Cloud Software Groupは、正当な利益のために必要に応じて、ライセンスコンプライアンスを含む基本的なライセンスデータの収集も要求します。

ライセンスサーバーデータページは、ライセンスサーバーをインストールしたときに表示されます。

- スタンドアロンとして。
- Delivery Controllerのインストール中に、コアコンポーネントとして。

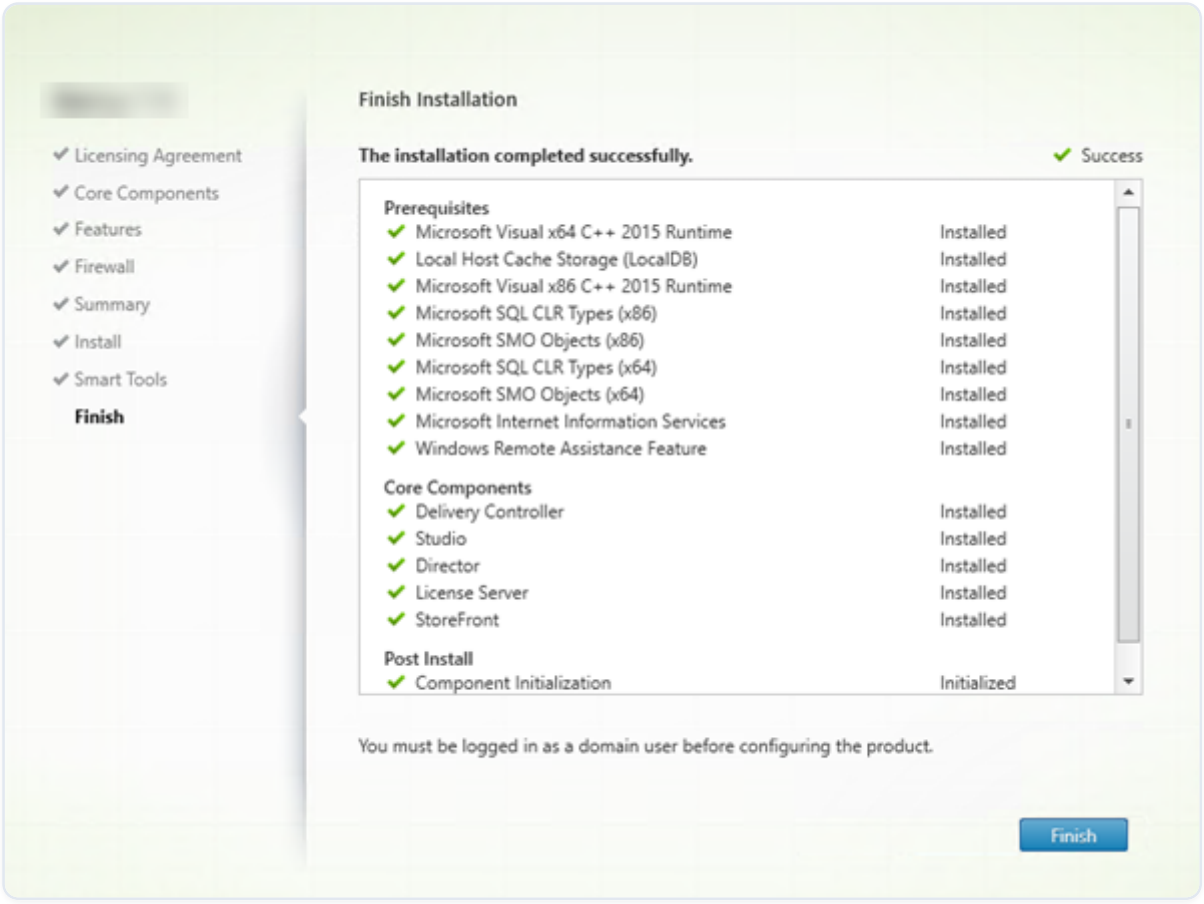
アップグレード中に、`/CITRIX.opt:` ファイルで構成がすでに設定されている場合、このページは表示されません。

ライセンスサーバーは、ライセンスデータ、Call Homeデータ、CEIPデータなど、いくつかの種類のユーザーデータを監視します。Call HomeデータとCEIPデータの収集を有効にするには、参加（オプトイン）を選択する必要があります。

コマンドラインを使用してインストールする際のCall HomeおよびCEIPデータの収集を有効にする方法の詳細については、「コアコンポーネントをインストールするためのコマンドラインオプション」を参照してください。

Cloud Software Groupのライセンスデータ収集の詳細については、「Citrixライセンスデータ収集プログラム」を参照してください。

ステップ11. このインストールを完了する



完了ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントに緑色のチェックマークが表示されます。

完了をクリックします。

ステップ12. 残りのコアコンポーネントを他のマシンにインストールする

すべてのコアコンポーネントを1台のマシンにインストールした場合は、「次のステップ」に進みます。そうでない場合は、他のマシンでインストーラーを実行して他のコンポーネントをインストールします。他のサーバーにControllerを追加でインストールすることもできます。

次のステップ

必要なコンポーネントをすべてインストールした後、Studio を使用してサイトを作成します。

サイトを作成した後、VDA をインストールします。

いつでも、フルプロダクトインストーラーを使用して、以下のコンポーネントで展開を拡張できます。

- **Universal Print Serverサーバーコンポーネント:** プリントサーバーでインストーラーを起動します。

  a. **展開の拡張**セクションで**Universal Print Server**を選択します。

  b. ライセンス契約に同意します。

  c. **ファイアウォール**ページで、デフォルトでは、Windows ファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、TCPポート7229と8080がファイアウォールで開かれます。ポートを手動で開きたい場合は、このデフォルトのアクションを無効にできます。

  コマンドラインからこのコンポーネントをインストールするには、Universal Print Server をインストールするためのコマンドラインオプションを参照してください。

- フェデレーション認証サービス。
- セッション録画。
- ワークスペース環境管理。

コマンドラインを使用したインストール

重要:

- アップグレードする場合で、現在のバージョンがPersonal vDiskまたはAppDisksソフトウェアを使用しているか、インストールされている場合は、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。
- Citrixは、ライセンスコンプライアンスを含む正当な利益のために、必要に応じて基本的なライセンスデータを収集します。詳細については、「Citrixライセンスデータ」を参照してください。

はじめに

この記事は、Windowsオペレーティングシステムを搭載したマシンにコンポーネントをインストールする場合に適用されます。Linuxオペレーティングシステム用VDAについては、「Linux Virtual Delivery Agents」を参照してください。

この記事では、製品のインストールコマンドを発行する方法について説明します。インストールを開始する前に、「インストールの準備」を確認してください。この記事には、利用可能なインストーラーの説明が含まれています。

コマンド実行の進行状況と戻り値を確認するには、元の管理者であるか、**管理者として実行**を使用する必要があります。詳細については、Microsoftのコマンドドキュメントを参照してください。

インストールコマンドを直接使用することに加えて、Active Directory内のマシンにVDAをインストール、アップグレード、または削除するサンプルスクリプトが製品ISOに用意されています。詳細については、「スクリプトを使用したVDAのインストール」を参照してください。

このCitrix Virtual Apps and Desktopsのバージョンでサポートされていないバージョンにインストールまたはアップグレードしようとすると、オプションに関する情報を示すメッセージが表示されます。「以前のオペレーティングシステム」を参照してください。

Citrixがコンポーネントインストールの結果を報告する方法については、「Citrixインストールのリターンコード」を参照してください。

フル製品インストーラーを使用する

フル製品インストーラーのコマンドラインインターフェイスにアクセスするには：

1. Citrixから製品パッケージをダウンロードします。ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。
2. ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
3. コンポーネントをインストールするサーバーに、ローカル管理者アカウントを使用してログオンします。
4. DVDをドライブに挿入するか、ISOファイルをマウントします。
5. メディアの `\x64\XenDesktop Setup` ディレクトリから、適切なコマンドを実行します。

   コアコンポーネントをインストールするには: `XenDesktopServerSetup.exe` を実行します。オプションについては、コアコンポーネントのインストール用コマンドラインオプション を参照してください。

   VDAをインストールするには: `XenDesktopVDASetup.exe` を実行します。オプションについては、VDAのインストール用コマンドラインオプション を参照してください。

   StoreFrontをインストールするには: インストールメディアの `x64 > StoreFront` フォルダーで `CitrixStoreFront-x64.exe` を実行します。

   Universal Print Serverをインストールするには: Universal Print Serverのインストール用コマンドラインオプション のガイダンスに従ってください。

Federated Authentication Serviceをインストールするには： Citrixでは、グラフィカルインターフェイスを使用することをお勧めします。

Session Recordingをインストールするには: Session Recording のガイダンスに従ってください。

Workspace Environment Managementをインストールするには： Workspace Environment Managementのガイダンスに従ってください。

Secure Private Accessをインストールするには： インストールメディアの `x64 > XenDesktop` Setupフォルダーで `XenDesktopSPASetup.exe` を実行します。Secure Private Accessのインストールに関するコマンドラインオプションのガイダンスに従ってください。

コアコンポーネントのインストール用コマンドラインオプション

`XenDesktopServerSetup.exe`コマンドを使用してコアコンポーネントをインストールする場合、以下のパラメーターオプションが有効です。オプションの詳細については、コアコンポーネントのインストールを参照してください。

注:

- コアコンポーネントをインストールするためのコマンドラインオプションを使用している間は、`/exclude`を使用しないでください。
- `/components`を使用して1つのコンポーネントをアップグレードすると、他のコンポーネントもアップグレードされる場合があります。これは、異なるコンポーネント間の潜在的な互換性の問題を回避するためです。
- 1つのコンポーネントのみをアップグレードする場合は、そのコンポーネントの個別のインストーラーを使用してください。展開のアップグレードを参照してください。

- ***/ceipoptin*** *ceipoptin* など.

  Call Homeデータおよびカスタマーエクスペリエンス向上プログラム（CEIP）データの収集を有効にします。有効な値は次のとおりです。

  - `DIAGNOSTIC`: Citrix Licensing が Call Home データを収集できるようにするには、この値を選択します。
  - `ANONYMOUS`: Citrix Licensing が未識別の CEIP データ (ユーザーを特定しないデータ) を収集できるようにするには、この値を選択します。

- `NONE`: Citrix Licensing による CEIP データの収集を無効にするには、この値を選択します。

Call Homeデータの収集について詳しくは、Citrix Licensing Call Homeを参照してください。

CEIPデータの収集について詳しくは、Citrix Licensing Customer Experience Improvement Programを参照してください。

CEIPデータの詳細については、Citrix Licensing CEIP data elementsを参照してください。

License Serverのライセンスデータの詳細については、Citrix Licensing Dataを参照してください。

- **/components** *component* など.

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `CONTROLLER`: コントローラー
  - `DESKTOPSTUDIO`: スタジオ
  - `WEBSTUDIO`: ウェブスタジオ
  - `DESKTOPDIRECTOR`: ディレクター
  - `LICENSESERVER`: Citrix ライセンスサーバー
  - `SECUREPRIVATEACCESS`: セキュア プライベート アクセス

  このオプションを省略すると、すべてのコンポーネントがインストールされます (`/remove`オプションも指定されている場合は、削除されます)。

  (2003年より前のリリースでは、有効な値に`STOREFRONT`が含まれていました。バージョン2003以降では、Use the full-product installerに記載されている専用のStoreFrontインストールコマンドを使用してください)。

- **/configure_firewall**

  Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、インストールされているコンポーネントで使用されるWindowsファイアウォールのすべてのポートを開きます。サードパーティ製ファイアウォールまたはファイアウォールを使用していない場合は、手動でポートを開く必要があります。

- **/ディスエーブルエクスペリエンスメトリクス**

インストール、アップグレード、または削除中に収集された分析データがCitrixに自動的にアップロードされるのを防ぎます。

- **/help** または **/h**

  コマンドのヘルプを表示します。

- **/ignore_hw_check_failure**

  ハードウェアチェックが失敗した場合でも (たとえば、RAM不足のため)、Delivery Controllerのインストールまたはアップグレードを続行できます。詳しくは、Hardware checkを参照してください。

- **/ignore_site_test_failure**

  コントローラーのアップグレード中にのみ有効です。通常、サイトテストの失敗は無視され、アップグレードは続行されます。省略された場合（またはfalseに設定された場合）、サイトテストの失敗があると、アップグレードを実行せずにインストーラーが失敗します。デフォルト = false

  アップグレード中に、サポートされていないSQL Serverバージョンが検出された場合、このオプションは無視されます。詳細については、SQL Serverのバージョンチェックを参照してください。

- **/installdir** *ディレクトリ*

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/logpath** *パス*

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

  Director のインストール時にのみ有効です。Windows リモートアシスタンスを使用するユーザーシャドウイング機能を無効にします。

- **再起動なし**

  インストール後の再起動を防止します。（ほとんどのコアコンポーネントでは、再起動はデフォルトで有効になっていません。）

- **再開しない**

デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume`を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **ノースキューエル**

  コントローラーをインストールするサーバーへのMicrosoft SQL Server Expressのインストールを防止します。このオプションが省略された場合、SQL Server Expressはサイトデータベースとして使用するためにインストールされます。

  このオプションは、ローカルホストキャッシュに使用される SQL Server Express LocalDB のインストールには影響しません。

- **サイレント** または **パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールプロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/リムーブ**

  `/components`オプションで指定されたコアコンポーネントを削除します。

- **/リムーブオール**

  インストールされているすべてのコアコンポーネントを削除します。

- **/センドエクスペリエンスメトリクス**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションを省略した場合（または `/disableexperiencemetrics` が指定されている場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **/テンプディル** *ディレクトリ*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

- **ゼナップ**

  Citrix Virtual Apps をインストールします。このオプションを省略すると、Citrix Virtual Apps and Desktops™ がインストールされます。

コアコンポーネントのインストール例

次のコマンドは、サーバーに Delivery Controller™、Studio、Citrix Licensing、および SQL Server Express をインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall
```

次のコマンドは、サーバーにCitrix Virtual Apps™ Controller、Studio、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall
```

次のコマンドは、サーバーにDelivery Controller、Secure Private Access、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

```
\x64\XenDesktop Setup XenDesktopServerSetup.exe /xenapp /components controller,secureprivateaccess /configure_firewall
```

スタンドアロンVDAインストーラーを使用する

ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。インストールを開始する前に、管理者特権を昇格させるか、**管理者として実行**を使用する必要があります。

1. Citrixから適切なパッケージをダウンロードします。
   - マルチセッションOS Virtual Delivery Agent: `VDAServerSetup_xxxx.exe`
   - シングルセッションOS Virtual Delivery Agent: `VDAWorkstationSetup_xxxx.exe`
   - シングルセッションOS Core Services Virtual Delivery Agent: `VDAWorkstationCoreSetup_xxxx.exe`
2. まずパッケージから既存のディレクトリにファイルを抽出し、その後インストールコマンドを実行するか、単にパッケージを実行します。

   ファイルをインストールする前に抽出するには、絶対パスを指定して`/extract`を使用します（例: `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`）。ディレクトリが存在している必要があります。存在しない場

合、抽出は失敗します。その後、別のコマンドで、この記事に記載されている有効なオプションを使用して、適切なコマンドを実行します。

- `VDAServerSetup_XXXX.exe`の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`を実行します
- `VDAWorkstationCoreSetup_XXXX.exe`の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`を実行します
- `VDAWorkstationSetup_XXXX.exe`の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`を実行します

ダウンロードしたパッケージを実行するには、その名前を実行します: `VDAServerSetup.exe`、`VDAWorkstationSetup.exe`、または`VDAWorkstationCoreSetup.exe`。この記事に記載されている有効なオプションを使用してください。

フル製品インストーラーに慣れている場合：

- スタンドアロンの`VDAServerSetup.exe`または`VDAWorkstationSetup.exe`インストーラーを、名前以外のすべてにおいて`XenDesktopVdaSetup.exe`コマンドであるかのように実行します。
- `VDAWorkstationCoreSetup.exe`インストーラーは、他のインストーラーで利用できるオプションのサブセットをサポートしているため、異なります。

VDA をインストールするためのコマンドラインオプション

以下のオプションは、次のコマンド（インストーラー）のいずれか、または複数で有効です: `VDAServerSetup_xxxx.exe`、`VDAWorkstationSetup_xxxx.exe`、および`VDAWorkstationCoreSetup_xxxx.exe`。

オプションの詳細については、「VDA のインストール」を参照してください。

- **/コンポーネント** *コンポーネント*\[,*コンポーネント*\]

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `VDA`: バーチャル デリバリー エージェント
  - `PLUGINS`: Windows向けCitrix Workspace™アプリ

  VDA と Citrix Workspace app for Windows をインストールするには、`/components vda,plugins` を指定します。

このオプションを省略すると、VDA のみがインストールされます（Citrix Workspace app はインストールされません）。

このオプションは、`VDAWorkstationCoreSetup_xxxx.exe`インストーラーを使用する場合は無効です。そのインストーラーではCitrix Workspace appをインストールできません。

- **/controllers** "*コントローラー* \[*コントローラー*\]"

  VDAが通信できるControllerのFQDNをスペースで区切り、引用符で囲みます。`/site_guid`オプションと`/controllers`オプションの両方を指定しないでください。

- **/エクスペリエンスメトリクス無効化**

  インストール、アップグレード、または削除中に収集された分析データがCitrixに自動的にアップロードされるのを防ぎます。

- **/enable_hdx_ports**

  Windowsファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、VDAおよび有効な機能（Windowsリモートアシスタンスを除く）に必要なポートをWindowsファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、ネットワークポートを参照してください。

  HDX アダプティブトランスポートが使用する UDP ポートを開くには、この`/enable_hdx_ports`オプションに加えて、`/enable_hdx_udp_ports`オプションを指定します。

- **/enable_hdx_udp_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、HDX アダプティブトランスポートが使用する Windows ファイアウォールの UDP ポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

  VDAが使用する追加ポートを開くには、この`/enable_hdx_udp_ports`オプションに加えて、`/enable_hdx_ports`オプションを指定します。

- **/enable_hdx_tls_dtls**

  HDX™ Direct V1用にTCPおよびUDPポート443を開きます。

- **/enable_real_time_transport**

オーディオパケットにUDPを使用するかどうかを有効または無効にします（オーディオ用のRealTime Audio Transport）。この機能を有効にすると、オーディオパフォーマンスが向上する可能性があります。Windowsファイアウォールサービスが検出されたときにUDPポートを自動的に開く場合は、`/enable_hdx_ports`オプションを含めます。

- **/enable_remote_assistance**

  Directorで使用するために、Windowsリモートアシスタンスのシャドウイング機能を有効にします。このオプションを指定すると、Windowsリモートアシスタンスはファイアウォール内の動的ポートを開きます。

- **/enablerestore** または **/enablerestorecleanup**

  （シングルセッションVDAにのみ有効）VDAのインストールまたはアップグレードが失敗した場合に、復元ポイントへの自動復帰を有効にします。

  インストール/アップグレードが正常に完了した場合：

  - `/enablerestorecleanup`は、インストーラーに復元ポイントを削除するよう指示します。
  - `/enablerestore`は、使用されなかった場合でも、インストーラーに復元ポイントを保持するよう指示します。

  詳細については、インストールまたはアップグレードの失敗時の復元を参照してください。

- **/enable_ss_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、画面共有に必要なポートをWindows ファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、手動でファイアウォールを構成する必要があります。

- **/exclude** "*コンポーネント*"\[,"*コンポーネント*"\]

  1つまたは複数のコンマ区切りのオプションコンポーネント（それぞれを引用符で囲む）のインストールを防止します。たとえば、MCSで管理されていないイメージにVDAをインストールまたはアップグレードする場合、Machine Identity Serviceコンポーネントは不要です。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in
Citrix Backup and Restore	Citrix Backup and Restore	Citrix Browser Content Redirection
Citrix Browser Content Redirection	Citrix Browser Content Redirection	Citrix Personalization for App-V - VDA
Citrix MCS IODriver	Citrix MCS IODriver	Citrix Telemetry Service
Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA	Citrix Universal Print Client
Citrix Profile Management	Citrix Profile Management	Citrix Vda Log Capture Service
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in	CSE Component
Citrix Rendezvous V2	Citrix Rendezvous V2	Director VDA Plug-in
Citrix Telemetry Service	Citrix Telemetry Service	Machine Management Provider
Citrix Universal Print Client	Citrix Universal Print Client	VDA Monitor Plug-in
Citrix Vda Log Capture Service	Citrix Vda Log Capture Service	VDA WMI Proxy Plug-in
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent	
CSE Component	CSE Component	
Director VDA Plug-in	Director VDA Plug-in	

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
`Machine Identity Service`	`Machine Identity Service`	
`Machine Management Provider`	`Machine Management Provider`	
`VDA Monitor Plug-in`	`User Personalization Layer`	
`VDA WMI Proxy Plug-in`	`VDA Monitor Plug-in`	
	`VDA WMI Proxy Plug-in`	
`Citrix App Protection Component`	`Citrix App Protection Component`	`Citrix App Protection Component`
`Citrix HyperV Filter Driver`	`Citrix HyperV Filter Driver`	
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`

Citrix Profile Management をインストールから除外すると (`/exclude "Citrix Profile Management"`)、Citrix Director を使用した VDA の監視とトラブルシューティングに影響します。**ユーザーの詳細**ページと**エンドポイント**ページでは、パーソナライゼーションパネルとログオン期間パネルが機能しません。**ダッシュボード**ページと**トレンド**ページでは、平均ログオン期間パネルは、Profile Management がインストールされているマシンのみのデータを表示します。

サードパーティ製のユーザープロファイル管理ソリューションを使用している場合でも、Citrix は Citrix Profile Management Service をインストールして実行することを推奨します。Citrix Profile Management Service を有効にする必要はありません。

`/exclude` と `/includeadditional` の両方を同じコンポーネント名で指定した場合、そのコンポーネントはインストールされません。

このオプションは、`VDAWorkstationCoreSetup.exe` インストーラーを使用する場合は無効です。このインストーラーは、これらの項目の多くを自動的に除外します。

- **/h** または **/help**

  コマンドのヘルプを表示します。

- **/includeadditional** "*コンポーネント*"\[,"*コンポーネント*"\]

  1つ以上のコンマ区切りのオプションコンポーネントのインストールを含めます。各コンポーネントはストレート引用符で囲みます。このオプションは、Remote PC Access展開を作成し、デフォルトで含まれていない他のコンポーネントをインストールする場合に役立ちます。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

  同じコンポーネント名で`/exclude`と`/includeadditional`の両方を指定した場合、そのコンポーネントはインストールされません。

- **/installdir** *ディレクトリ*

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/install_mcsio_driver**

  使用しないでください。代わりに`/includeadditional "Citrix MCS IODriver"`または`/exclude "Citrix MCS IODriver"`を使用してください。

- **/logpath** *パス*

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = 「`%TEMP%\Citrix\XenDesktop Installer`」

  このオプションはグラフィカルインターフェイスでは利用できません。

- **マスターイメージ**

  VDAをVMにインストールする場合にのみ有効です。他のマシンを作成するために使用するイメージとしてVDAをセットアップします。このオプションは`/mastermcsimage`と同等です。

  このオプションは、`VDAWorkstationCoreSetup_xxxx.exe`インストーラーを使用する場合には無効です。

- **マスターMCSイメージ**

  このマシンがMachine Creation Servicesでイメージとして使用されることを指定します。このオプションは`/masterimage`と同等です。

- **マスターPVSイメージ**

  このマシンが、Citrix Provisioning™またはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Managerなど）を使用してVMをプロビジョニングするためのイメージとして使用されることを指定します。

- **WebSocketトークン** *WebSocketToken*

  Web Socket VDAを作成します。WebSocketTokenは、必要なトークン用です。

- **/no_mediafoundation_ack**

  Microsoft Media Foundationがインストールされていないこと、およびいくつかのHDXマルチメディア機能がインストールされず、動作しないことを確認します。このオプションが省略され、Media Foundationがインストールされていない場合、前提条件が満たされていないため、VDAのインストールは終了します。ほとんどのサポートされているWindowsエディションには、Nエディションを除き、Media Foundationがすでにインストールされています。Windowsの機能 > メディア機能を*手動*で有効にした場合、Citrix Meta Installerが探すレジストリキーに値が設定されていない可能性があります。インストールプロセスを開始する前に、`SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-`

`Features\WindowsMediaVersion`レジストリキーをチェックして、値が存在し、空ではないことを確認してください。

- **デスクトップエクスペリエンスなし**

  拡張デスクトップエクスペリエンス機能は利用できなくなりました。このオプション（およびポリシー設定）は、指定されても無視されます。

  マルチセッションOS用VDAをインストールする場合にのみ有効です。拡張デスクトップエクスペリエンス機能の有効化を防止します。この機能は、拡張デスクトップエクスペリエンスCitrixポリシー設定でも制御されます。

- **再起動なし**

  インストール後の再起動を防止します。VDAは再起動するまで使用できません。

- **再開しない**

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume`を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **物理マシン**

  RemotePCインストールの場合、この引数を `/remotepc` と一緒に使用してください。そうしないと、特定のユーザーシナリオでVDAが期待どおりに動作しない可能性があります。

- **ポート番号** *port*

  `/reconfig` オプションが指定されている場合にのみ有効です。VDAとController間の通信を有効にするポート番号です。以前に構成されたポートは、ポート80でない限り無効になります。

- **/proxyconfig** “*アドレスまたはPACファイルのパス*”

  環境でGateway ServiceなどのサービスとRendezvousプロトコルを使用する予定があり、アウトバウンド接続用にネットワークに非透過型プロキシがある場合は、ここでプロキシを指定します。HTTPプロキシのみがサポートされています。Rendezvousプロトコルで使用するプロキシのアドレスまたはPACファイルのパスです。機能の詳細については、Rendezvousプロトコル を参照してください。

  - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
  - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **サイレント** または **パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールおよび構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/再構成**

  `/portnumber`、`/controllers`、または`/enable_hdx_ports`オプションと組み合わせて使用すると、以前に構成されたVDA設定をカスタマイズします。このオプションを`/quiet`オプションと同時に指定しない場合、VDAをカスタマイズするためのグラフィカルインターフェイスが起動します。

- **/リモートPC**

  Remote PC Access展開（シングルセッションOS）またはブローカー接続（マルチセッションOS）でのみ有効です。追加コンポーネントのインストールを除外します（`/exclude`および`/includeadditional`オプションのコンポーネントリストを参照）。

  このオプションは、`VDAWorkstationCoreSetup.exe`インストーラーを使用する場合は無効です。そのインストーラーは、これらのコンポーネントのインストールを自動的に除外します。

  `/remotepc` は `/servervdi` オプションと互換性がありません。

- **/削除**

  `/components`オプションで指定されたコンポーネントを削除します。

- **/remove_appdisk_ack**

  インストールされている場合、VDAインストーラーがAppDisks™ VDAプラグインをアンインストールすることを承認します。

- **/remove_pvd_ack**

  インストールされている場合、VDAインストーラーがPersonal vDiskをアンインストールすることを承認します。

- **/すべて削除**

  VDAを削除します。Citrix Workspaceアプリ（インストールされている場合）は削除しません。

- **/エクスペリエンスメトリックを送信**

インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションが省略された場合（または`/disableexperiencemetrics`オプションが指定された場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **サーバーVDI**

  サポートされているWindowsマルチセッションマシンにシングルセッションOS用VDAをインストールします。Windowsマルチセッションマシンにマルチセッション OS用VDAをインストールする場合は、このオプションを省略してください。

  このオプションを使用する前に、Server VDIを参照してください。

  このオプションは、フルプロダクトVDAインストーラーでのみ使用してください。

- **サイト_GUID** *GUID*

  サイトのActive Directory組織単位（OU）のグローバル一意識別子。これは、検出にActive Directoryを使用している場合に、仮想デスクトップをサイトに関連付けます（自動更新が推奨されるデフォルトの検出方法です）。サイトGUIDは、Studioに表示されるサイトプロパティです。`/site_guid`と`/controllers`の両方のオプションを指定しないでください。

- **一時ディレクトリ** *directory*

  インストール中に一時ファイルを保持するディレクトリ。既定値 = c:\\Windows\\Temp。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **/仮想マシン**

  VDAをVMにインストールする場合にのみ有効です。インストーラーによる物理マシンの検出を上書きします。VMに渡されるBIOS情報により、VMが物理マシンとして表示される場合があるためです。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **/XenDesktopクラウド**

  VDAがCitrix DaaS (Citrix Cloud™) 展開にインストールされていることを示します。

VDAのインストール例

フルプロダクトインストーラーでVDAをインストールする：

次のコマンドは、シングルセッションOS用のVDAとCitrix Workspaceアプリを、VMのデフォルトの場所にインストールします。このVDAはイメージとして使用され、MCSを使用してVMをプロビ

ジョニングします。VDAは、`mydomain`ドメイン内の`Contr-Main`という名前のサーバー上のControllerに最初に登録されます。VDAはユーザーパーソナライゼーションレイヤーとWindowsリモートアシスタンスを使用します。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /
controllers "Contr-Main.mydomain.local" /enable_hdx_ports /includeadditional
"user personalization layer" /mastermcsimage /enable_remote_assistance
```

VDAWorkstationCoreSetupスタンドアロンインストーラーでシングルセッションOS VDAをインストールする：

次のコマンドは、リモートPCアクセスまたはVDI展開で使用するために、シングルセッションOSにコアサービスVDAをインストールします。Citrix Workspaceアプリおよびその他の非コアサービスはインストールされません。Controllerのアドレスが指定され、Windowsファイアウォールサービス内のポートは自動的に開かれます。管理者が再起動を処理します。

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /
enable_hdx_ports /noreboot
```

VDAをカスタマイズする

VDAをインストールした後、いくつかの設定をカスタマイズできます。製品メディアの`\x64\XenDesktop Setup`ディレクトリから、VDAのインストール用コマンドラインオプションで説明されている以下のオプションを1つ以上使用して、`XenDesktopVdaSetup.exe`を実行します。

- `/reconfigure` (VDAをカスタマイズする際に必須)
- `/h` または `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

VDAのトラブルシューティング

- デリバリーグループのStudio表示で、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。

- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを配信できません。

  VDAの登録方法と登録の問題のトラブルシューティングについては、「VDA登録」を参照してください。

Universal Print Serverをインストールするためのコマンドラインオプション

次のオプションは、`XenDesktopPrintServerSetup.exe`コマンドで有効です。

- **/enable_upsserver_port**

このオプションが指定されていない場合、インストーラーはグラフィカルインターフェイスから**ファイアウォール**ページを表示します。インストーラーにWindowsファイアウォールルールを自動的に追加させるには**自動**を選択し、管理者がファイアウォールを手動で構成できるようにするには**手動**を選択します。

プリントサーバーにソフトウェアをインストールした後、「プリンターのプロビジョニング」のガイダンスを使用してUniversal Print Serverを構成します。

Secure Private Accessをインストールするためのコマンドラインオプション

以下のオプションは、以下のコマンド（インストーラー）で有効です:
`XenDesktopSPASetup.exe`

- **/enable_spa_ports**

  Windowsファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、Secure Private Accessに必要なWindowsファイアウォールのポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

- **/NoSQL**

  Secure Private Accessをインストールするサーバーへの Microsoft SQL Server Expressのインストールを防止します。このオプションを省略すると、サイトデータベースとしてSQL Server Expressがインストールされます。

- **/ヘルプ または /h または /?**

  コマンドのヘルプを表示します

- **/再起動しない**

インストール後の再起動を防止します。Secure Private Access は再起動するまで使用できません。

- **/サイレント または /パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールと構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/削除**

  Secure Private Accessを削除します。

オプションの詳細については、「Secure Private Access インストーラー」を参照してください。

詳細情報

Citrix がコンポーネントインストールの結果を報告する方法については、「Citrix インストールリターンコード」を参照してください。

Web Studioのインストール

> **ライセンス要件:**

> Web Studioを使用するには、次のいずれかのライセンスタイプが必要です。

> - Citrix ユニバーサルサブスクリプションライセンス。
> - 年間および期間ベースの小売ライセンス向けCitrixオンプレミスサブスクリプション。
> - Citrix Service Providers (CSP)向けのオンプレミスライセンス。

はじめに

Citrix Studioは、Citrix Virtual Apps and Desktops展開を構成および管理できるWindowsベースの管理コンソールです。Web Studioは、Citrix Studioの次世代版であり、Citrix Studioと完全に同等の機能を備えたWebベースの管理コンソールです。Citrix DaaS Full Configuration interfaceと同じルックアンドフィールで、Web Studioはネイティブのウェブエクスペリエンスを提供することで、管理エクスペリエンスを最新化します。

Web Studioは、Internet Information Service (IIS)がインストールされている任意のWindowsサーバーに展開できます。展開オプションは次の2つです。

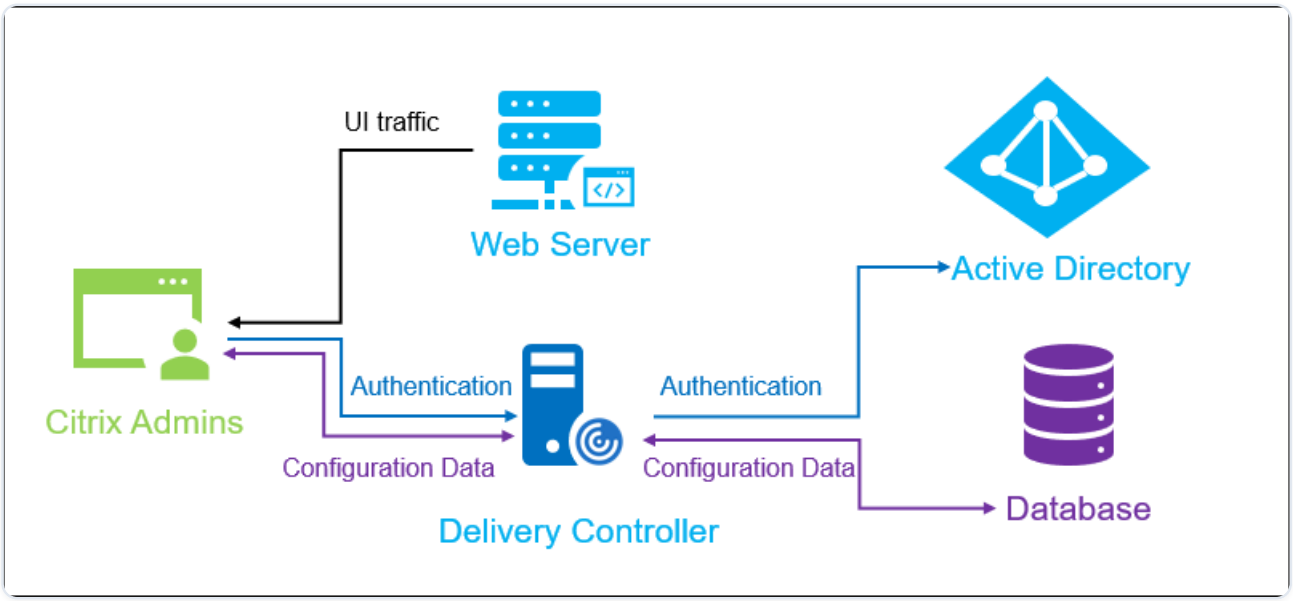
- 専用サーバーにインストールする場合:

  パフォーマンスとスケーラビリティが重要となる大規模な環境では、Web Studioを専用サーバーにインストールすることをお勧めします。このサーバーは、オプションでDirectorもホストできます。

- Delivery Controller™と統合する場合:

  迅速な展開やシンプルな環境では、Web StudioをDelivery Controllerに直接インストールします。このアプローチは、管理オーバーヘッドを最小限に抑えることが優先される小規模な展開に最適です。

次の図は、Web Studioのアーキテクチャを示しています。



Web Studio を稼働させるための一般的なワークフローは次のとおりです。

1. Web Studioをインストールする。
2. サイトをセットアップする。
3. 管理のためにDelivery ControllerをWeb Studioに追加する。
4. Web Studioにログオンする。

Web Studioで利用可能な新機能

新機能の記事を参照してください。

システム要件

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー 2022

- Windows Server 2019、StandardおよびDatacenterエディション、およびServer Coreオプション
- Windows Server 2016、StandardおよびDatacenterエディション、およびServer Coreオプション
- ウィンドウズ 11
- ウィンドウズ 10

サポートされているブラウザー：

- インターネット エクスプローラー 11
  - Internet Explorerでは互換表示モードはサポートされていません。Web Studioにアクセスするには、デフォルト設定を使用してください。
  - Internet Explorerをインストールするときは、推奨されるセキュリティ設定と互換性設定を使用するために、デフォルトを受け入れてください。すでにブラウザーをインストールしていて、推奨設定を使用しないことを選択した場合は、**［ツール］>［インターネットオプション］>［詳細設定］>［リセット］** に移動し、指示に従ってください。
- マイクロソフト エッジ
- Firefox ESR（延長サポート版）
- クローム

Web Studioを表示するための推奨される最適な画面解像度は1440 x 1024です。

前提条件

このWeb Studioリリースは、Citrix Virtual Apps and Desktops™ 2212以降の展開と互換性があります。

2212より前の展開の場合、まず2212にアップグレードしてからWeb Studioをインストールします。

既知の制限事項

Web StudioとCitrix Studioを相互に利用する場合、次の制限事項を考慮してください：Web Studioで作成されたテンプレートはCitrix Studioには表示されず、その逆も同様です。これは、Web StudioがCitrix Studioとは異なるデータベースを使用してテンプレートを保存するためです。回避策として、Web Studioでテンプレートからポリシーを作成し、次にCitrix Studioでこのポリシーからテンプレートを作成してください。その逆も同様です。

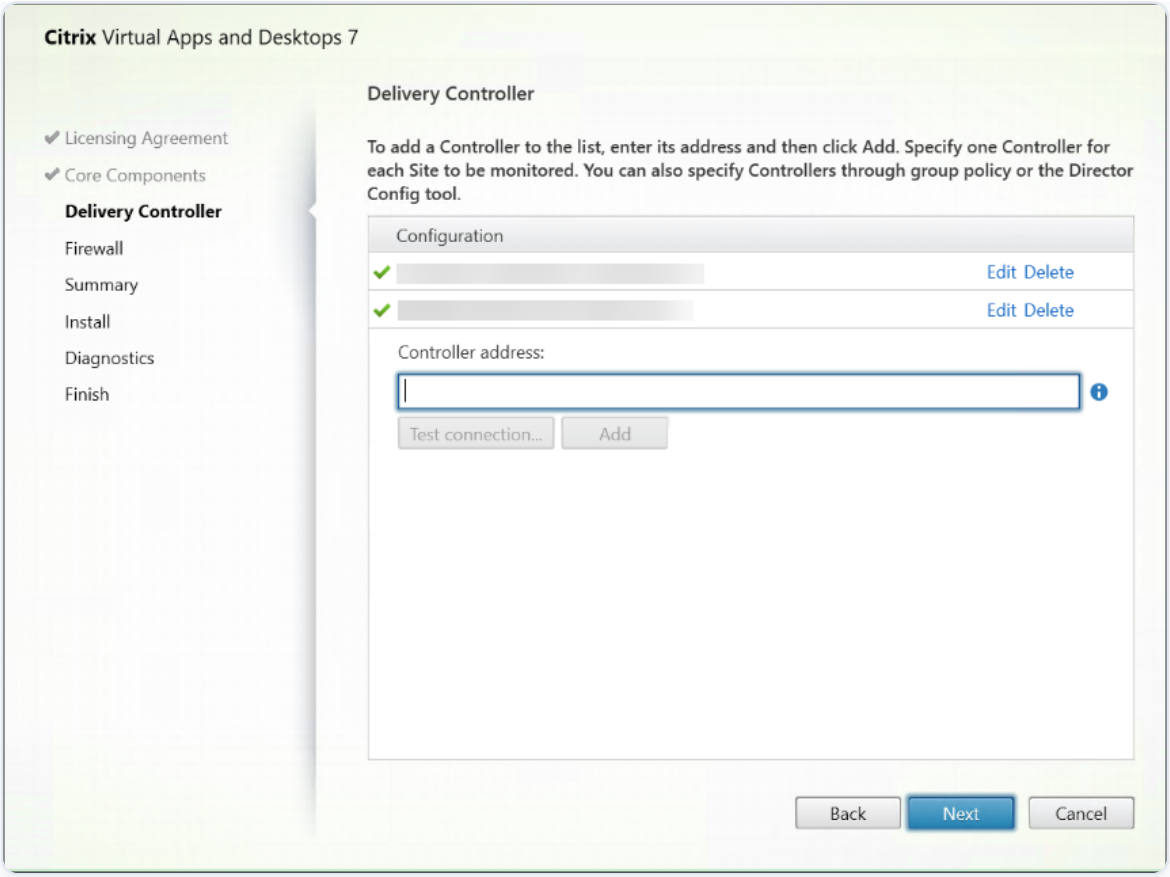
- Web Studioのインストールを成功させるには、Internet Information Services（IIS）Managerでデフォルトのサイト名（**Default Web Site**）を変更しないでください。デフォルトのサイト名を変更すると、インストールが失敗します。

Web Studioのインストール

以下の情報は、コアコンポーネントのインストール のガイダンスを補足するものです。Web Studioをインストールするには：

- Citrix Virtual Apps and Desktops 用の製品版 ISO インストーラーを使用して Web Studio をインストールします。ISO インストーラーは、前提条件を確認し、不足しているコンポーネントをインストールし、Web Studio Web サイトをセットアップし（Delivery Controller のインストールに含まれている場合は Delivery Controller 上に）、基本的な構成を実行します。
- インストール時にWeb Studioが含まれていなかった場合は、インストーラーを使用してWeb Studioを追加します。
- Web Studioのインストール時に、Delivery Controllerのアドレスを入力するよう求められます。

> **注:**
>
> - 複数の Delivery Controller を追加できます。Web Studio はランダムな順序でそれらに接続を試行します。Web Studio が接続しようとしている Delivery Controller に到達できない場合、Web Studio は自動的に他の Delivery Controller にフォールバックします。
> - **コアコンポーネント**で Director が選択され、インストールされている場合、ここで追加する Delivery Controller は Web Studio と Director の両方に使用されます。
> - 外部の公開信頼証明書が構成されておらず、エンタープライズ CA から証明書を要求したくない場合は、Delivery Controller の FQDN を構成するだけで済みます。
> - 外部の公開信頼証明書があり、Delivery Controller のパブリック DNS を構成できる場合は、DNS 名を Delivery Controller アドレスとして入力できます。
> - エンタープライズ CA から証明書を要求でき、個人の DNS を指定できる場合は、個人の DNS を Delivery Controller アドレスとして追加できます。



- ブラウザーとWebサーバー間、およびブラウザーとDelivery Controller間の通信を保護するには、Web StudioをホストするIIS WebサイトとDelivery ControllerでTLS暗号化を有効にする必要があります。Delivery ControllerにTLS証明書が構成されていない場合、インストーラーは、Delivery ControllerのFQDNとlocalhostをDNS名証明書として使用して、自己署名証明書を作成します。TLS証明書が構成されている場合、インストーラーは変更を行いません。TLS暗号化の詳細については、「Web Studio展開の保護（オプション）」を参照してください。
- **完了**ページでは、**Site Manager を起動**チェックボックスがデフォルトで選択されており、Citrix Site Manager が自動的に開きます。後で起動するには、デスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager**を選択します。Web Studio を起動する前に、Citrix Site Manager を使用してサイトを作成するか、既存のサイトに参加する必要があります。詳細については、「サイトのセットアップ」を参照してください。

  Site Manager の起動(/en-us/citrix-virtual-apps-desktops/2311/media/launch-site-manager.png)

注:

コマンドラインを使用して Web Studio をインストールすることもできます。例：`.\XenDesktopServerSetup.exe /components webstudio /controllers`

> `"ddc1.studio.local" /configure_firewall /quiet`。詳細については、「コマンドラインを使用したインストール」を参照してください。

サイトをセットアップする

Citrix Virtual Apps and Desktops 展開（サイトとも呼ばれます）をセットアップするには、Citrix Site Manager ツールを使用します。このツールは、Delivery Controller とともに自動的にインストールされます。

サイトをセットアップするには、次の手順に従います。

1. Delivery Controller で、デスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager** を選択します。
2. Citrix Site Manager で、**Create a site** を選択します。サイトセットアップウィザードが表示されます。
3. サイトを作成し、その設定を次のように構成します。
   - **はじめに**ページで、サイトの名前を入力します。
   - **データベース**ページには、サイト、監視、および構成ログデータベースをセットアップするための選択肢が含まれています。詳しくは、「手順3. データベース」を参照してください。
   - **ライセンス**ページで、License Serverのアドレスを指定し、使用する（インストールする）ライセンスを示します。詳しくは、「手順4. ライセンス」を参照してください。
4. **Summary** ページで、すべての設定を確認し、**Submit** をクリックします。

   このコントローラーの IP アドレスは、サイトに自動的に追加されます。

   > **注:**
   >
   > サイトを作成したユーザーは、そのサイトのフル管理者になります。詳しくは、「委任管理」を参照してください。

サイトの作成後に新しいコントローラーをインストールする場合は、そのコントローラーをサイトに追加する必要があります。詳細な手順は次のとおりです。

1. この新しいControllerでCitrix Site Managerを実行します。
2. **既存のサイトに参加**を選択します。

3. 既にサイトに追加されているControllerのアドレスを入力します。
4. **Submit**をクリックします。

管理のためにDelivery ControllerをWeb Studioに追加する

Studio構成ツールを使用して、管理のためにDelivery ControllerをWeb Studioに追加します。このツールは、Web Studioのインストールフォルダーにあります。

デフォルトでは、このツールは次のデフォルトフォルダーにインストールされます。

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Web Studioで管理したいサイトに対して、次の2つのDelivery Controller (`ddc1.studio.local` および `ddc2.studio.local`) を構成するとします。次のPowerShellコマンドを実行します。

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

> **注:**
>
> - このツールにはコンピューター管理者権限が必要です。
> - IISサーバーのキャッシュ設定により、Delivery Controllerの構成変更がすぐに反映されない場合があります。すぐに反映させるには、Web Studioサーバーに移動し、Internet Information Services (IIS) マネージャーを開き、「スタートページ」>「サイト」>「既定のWebサイト」に移動し、「Webサイトの管理」ペインで「**再起動**」を選択します。
> - サポートされているすべてのパラメーターを表示するには、`StudioConfig.exe --help` を実行します。

Delivery ControllerのプロキシとしてWeb Studioを構成する（オプション）

デフォルトでは、Web Studioコンソールを使用して展開を管理する場合、Webブラウザーを介してWeb StudioサーバーとDelivery Controllerの両方に接続します。Web StudioサーバーをDelivery Controllerのプロキシとして構成するオプションを提供します。その結果、展開を管理する際にはWeb Studioサーバーにのみ接続することになります。

このセクションでは、Web StudioサーバーをDelivery Controllerのプロキシとして構成する方法を説明します。Web StudioとDelivery Controllerは異なるサーバーにインストールされていることを前提としています。

開始する前に、展開に必要なすべてのコアコンポーネントがインストールされていることを確認してください。詳細については、「コアコンポーネントのインストール」を参照してください。

Web Studio のプロキシモードを有効にするには、次の手順に従います。

1. Web Studioサーバーで、Windows PowerShellを管理者として実行します。
2. 次のコマンドを実行します。`fqdn_of_webstudio_machine`はWeb Studioサーバーの FQDN に置き換えてください。

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

Web Studio のプロキシモードを無効にするには、この PowerShell コマンドを実行します。

```
`& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy`
```

注：

ベストプラクティスとして、外部の公開信頼証明書またはエンタープライズ証明機関（CA）からの証明書を使用して、Web Studioの展開を保護することをお勧めします。詳細については、「Web Studio展開の保護」を参照してください。

Web Studio にログオンする

Web Studio の Web サイトは `https://<address of the server hosting Web Studio>/Citrix/Studio` にあります。

Web Studio にログオンするには、デスクトップの メニューを開き、 **>** を選択します。Web Studio のアクセス許可を持つ管理者は、Active Directory ドメインユーザーである必要があります。Web Studio にログオンする際は、次のシナリオを考慮してください。

- サイトのDelivery Controllerをまだ指定していない場合。Delivery Controllerを指定するよう求められ、Web Studioへの一時的なアクセスが提供されます。
- 指定されたDelivery Controllerが現在到達不能な場合、Web Studioにログオンできません。接続をテストして、それらのDelivery Controllerが到達可能であることを確認してください。または、代替のDelivery Controllerを指定して、Web Studioへの一時的なアクセスが提供されるようにします。

次のステップ

1. VDAのインストール
2. Web Studioを使用して、次の方法で仮想アプリとデスクトップをユーザーに配信します。
    a. マシンカタログの作成
    b. デリバリーグループの作成
    c. アプリケーショングループの作成（オプション）

VDAのインストール

> **重要:**
>
> アップグレード中で、現在のバージョンにPersonal vDiskまたはAppDisksソフトウェアがインストールされている場合は、「PvD、AppDisks、およびサポートされていないホストの削除」(/ja-jp/citrix-virtual-apps-desktops/2311/upgrade-migrate/upgrade.html#remove-pvd-appdisks-and-unsupported-hosts)を参照してください。

> Windowsマシンには、マルチセッションOS用VDAとシングルセッションOS用VDAの2種類のVDAがあります。(Linuxマシン用VDAについては、「Linux Virtual Delivery Agent」(/ja-jp/linux-virtual-delivery-agent.html)ドキュメントを参照してください。)

インストールを開始する前に、「インストールの準備」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare.html)を確認し、すべての準備タスクを完了してください。

VDAをインストールする前に、コアコンポーネントをインストールします。VDAをインストールする前にサイトを作成することもできます。

この記事では、VDAをインストールする際のインストールウィザードの順序について説明します。コマンドラインでの同等の操作も提供されています。詳細については、「コマンドラインを使用したインストール」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-command.html)を参照してください。

ステップ1. 製品ソフトウェアをダウンロードし、ウィザードを起動します

フル製品インストーラーを使用している場合:

1. 製品ISOをまだダウンロードしていない場合:

- Citrixアカウントの資格情報を使用してCitrix Virtual Apps and Desktops™ダウンロードページにアクセスします。製品ISOファイルをダウンロードします。
- ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。

2. VDAをインストールするイメージまたはマシンで、ローカル管理者アカウントを使用します。DVDをドライブに挿入するか、ISOファイルをマウントします。インストーラーが自動的に起動しない場合は、マウントされたドライブ上の **AutoSelect** アプリケーションをダブルクリックします。

   インストールウィザードが起動します。

スタンドアロンパッケージを使用している場合:

1. Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktopsのダウンロードページにアクセスします。適切なパッケージをダウンロードしてください。

   - `VDAServerSetup_2308.exe`: マルチセッションOS VDA *バージョン*
   - `VDAWorkstationSetup_2308.exe`: シングルセッションOS VDA *バージョン*
   - `VDAWorkstationCoreSetup_2308.exe`: シングルセッションOSコアサービスVDA *バージョン*

2. パッケージを右クリックし、**管理者として実行**を選択します。

   インストールウィザードが起動します。

ステップ2. インストールする製品を選択する

コンポーネントインストーラーの製品インストールページ(/en-us/citrix-virtual-apps-desktops/2311/media/product-selector2-75.png)

インストールする製品（Citrix Virtual AppsまたはCitrix Virtual Desktops）の横にある**開始**をクリックします。（マシンにCitrix Virtual AppsまたはCitrix Virtual Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。）

コマンドラインオプション: Citrix Virtual Appsをインストールするには`/xenapp`。このオプションを省略すると、Citrix Virtual Desktopsがインストールされます。

ステップ3. VDAを選択する

コンポーネントインストーラーのコンポーネント選択ページ(/en-us/citrix-virtual-apps-desktops/2311/media/what-to-install-2.png)

Virtual Delivery Agentエントリを選択します。インストーラーは、シングルセッションOSまたはマルチセッションOSのどちらで実行されているかを認識しているため、適切なVDAタイプのみを提供します。

たとえば、Windows Server 2019マシンでインストーラーを実行すると、マルチセッションOS用VDAオプションが利用可能になります。シングルセッションOS用VDAオプションは提供されません。

このCitrix Virtual Apps and Desktopsバージョンでサポートされていないオスに Windows VDAをインストール（またはアップグレード）しようとすると、オプションに関する情報に誘導するメッセージが表示されます。

ステップ4. VDAの使用方法を指定する

VDAインストーラーの環境ページ(/en-us/citrix-virtual-apps-desktops/2311/media/vda-ss-environment.png)

「**環境**」ページで、VDAの使用方法を指定し、このマシンをイメージとして使用して、さらに多くのマシンをプロビジョニングするかどうかを示します。

選択したオプションは、Citrix provisioning™ ツールが自動的にインストールされるかどうか（もしあれば）、およびVDAインストーラーの追加コンポーネントページのデフォルト値に影響します。

VDAをインストールすると、いくつかのMSI（プロビジョニング用およびその他）が自動的にインストールされます。これらのインストールを防止する唯一の方法は、コマンドラインインストールで`/exclude`オプションを使用することです。

次のいずれかを選択してください。

- **マスターMCSイメージを作成する:** Machine Creation Services™ を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVDAをVMイメージにインストールします。このオプションはMachine Identity Serviceをインストールします。これがデフォルトのオプションです。

  コマンドラインオプション: `/mastermcsimage` または `/masterimage`

> **重要:**

> インストールメディアまたはISOイメージはローカルにマウントする必要があります。ソフトウェアのインストール目的でネットワークドライブからISOイメージをマウントすることはサポートされていません。

- **Citrix Provisioningまたはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する:** Citrix Provisioningまたはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Managerなど）を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVDAをVMイメージにインストールします。

  コマンドラインオプション: `/masterpvsimage`
- （マルチセッションOSマシンでのみ表示）**サーバーへの仲介接続を有効にする:** 他のマシンをプロビジョニングするためのイメージとして使用されない物理マシンまたは仮想マシンにVDAをインストールするには、このオプションを選択します。

  コマンドラインオプション: `/remotepc`
- （シングルセッションOSマシンでのみ表示）**Remote PC Accessを有効にする:** Remote PC Accessで使用する物理マシンにVDAをインストールするには、このオプションを選択します。

  コマンドラインオプション: `/remotepc`

「**次へ**」をクリックします。

このページは表示されません:

- VDAをアップグレードする場合
- `VDAWorkstationCoreSetup_2308.exe`、`VDAServerSetup_2308.exe`、または`VDAWorkstationSetup_2308.exe`インストーラーを使用している場合

ステップ5. インストールするコンポーネントとインストール場所を選択します

VDAインストーラーのコアコンポーネントページ(/en-us/citrix-virtual-apps-desktops/2311/media/vda-ss-core-components.png)

「**コアコンポーネント**」ページで:

- **場所:** デフォルトでは、コンポーネントは`C:\Program Files\Citrix`にインストールされます。このデフォルトは、ほとんどの展開で問題ありません。別の場所を指定する場合、その場所にはネットワークサービスに対する実行権限が必要です。

- **コンポーネント:** デフォルトでは、Citrix Workspaceアプリ for WindowsはVDAと一緒にインストールされません。`VDAWorkstationCoreSetup.exe`インストーラーを使用している場合、Citrix Workspaceアプリ for Windowsはインストールされないため、このチェックボックスは表示されません。

「**次へ**」をクリックします。

コマンドラインオプション: VDAとCitrix Workspaceアプリ for Windowsをインストールするには、`/installdir`、`/components vda,plugin`

ステップ6. 追加コンポーネントをインストールします

VDAインストーラーの追加コンポーネントページ(/en-us/citrix-virtual-apps-desktops/2311/media/vda-ss-addtnl-components.png)

「**追加コンポーネント**」ページには、VDAとともに他の機能やテクノロジーのインストールを有効または無効にするためのチェックボックスが含まれています。コマンドラインインストールでは、`/exclude`または`/includeadditional`オプションを使用して、利用可能なコンポーネントを明示的に除外または含めることができます。

- **/includeadditional** "*コンポーネント*"\[,"*コンポーネント*"\] ...
- **/exclude** "*コンポーネント*"\[,"*コンポーネント*"\] ...

以下の表は、このページの項目のデフォルト設定を示しています。デフォルト設定は、**環境**ページで選択したオプションによって異なります。

追加コンポーネントページ	環境ページ：「MCSによるマスターイメージ」または「CITRIX PROVISIONINGによるマスターイメージ」が選択されている場合	環境ページ：「サーバーへの仲介接続を有効にする」（マルチセッションOSの場合）または「リモートPCアクセス」（シングルセッションOSの場合）が選択されている場合
Citrix App-V 向けパーソナライゼーション - VDA	選択されていません	選択されていません
ユーザーパーソナライゼーションレイヤー	選択されていません	このユースケースでは無効なため、表示されません。
Citrix プロファイル管理	選択済み	選択されていません
Citrix Profile Management WMI プラグイン	選択済み	未選択

追加コンポーネントページ	環境ページ：「MCSによるマスターイメージ」または「CITRIX PROVISIONINGによるマスターイメージ」が選択されている場合	環境ページ：「サーバーへの仲介接続を有効にする」（マルチセッションOSの場合）または「リモートPCアクセス」（シングルセッションOSの場合）が選択されている場合
Citrix VDA アップグレードエージェント	未選択	未選択
Citrix バックアップおよび復元	未選択	未選択
シトリックス MCS I/Oドライバー	未選択	未選択
シトリックス ランデブー V2	未選択	未選択

このページは、次の場合には表示されません。

- `VDAWorkstationCoreSetup.exe` インストーラーを使用している場合。また、追加コンポーネントのコマンドラインオプションはそのインストーラーでは無効です。
- VDAをアップグレードしており、すべての追加コンポーネントがすでにインストールされている場合。一部の追加コンポーネントがすでにインストールされている場合、このページにはインストールされていないコンポーネントのみが表示されます。

以下のチェックボックスをオンまたはオフにします。（コンポーネントはインストーラーで異なる順序で表示される場合があります。）

- **Citrix Personalization for App-V:** Microsoft App-V パッケージのアプリケーションを使用する場合は、このコンポーネントをインストールします。詳細については、「App-V アプリケーションの展開と配信」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Personalization for App-V – VDA"`、コンポーネントのインストールを防止するには `/exclude "Citrix Personalization for App-V – VDA"`。
- **Citrixユーザーパーソナライゼーションレイヤー:** ユーザーパーソナライゼーションレイヤー用のMSIをインストールします。詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

このコンポーネントは、シングルセッションのWindows 10マシンにVDAをインストールする場合にのみ表示されます。

コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "User Personalization Layer"`、コンポーネントのインストールを防止するには `/exclude "User Personalization Layer"`。

- **Citrix Profile Management:** このコンポーネントは、ユーザープロファイル内のユーザーパーソナライゼーション設定を管理します。詳細については、「Profile Management」を参照してください。

  Citrix Profile Managementをインストールから除外すると、Citrix DirectorでのVDAの監視とトラブルシューティングに影響します。**ユーザー詳細**ページと**エンドポイント**ページでは、**パーソナライゼーション**パネルと**ログオン期間**パネルが機能しません。**ダッシュボード**ページと**トレンド**ページでは、**平均ログオン期間**パネルはProfile Managementがインストールされているマシンのみのデータを表示します。

  サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrixは Citrix Profile Management Serviceをインストールして実行することをお勧めします。Citrix Profile Management Serviceを有効にする必要はありません。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management"`。

- **Citrix Profile Management WMI Plug-in:** このプラグインは、WMI（Windows Management Instrumentation）オブジェクト（プロファイルプロバイダー、プロファイルタイプ、サイズ、ディスク使用量など）でProfile Managementのランタイム情報を提供します。WMIオブジェクトは、Directorにセッション情報を提供します。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management WMI Plug-in"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management WMI Plug-in"`。

- **VDA Upgrade Agent:** Citrix DaaS (旧称 Citrix Virtual Apps and Desktops service) の展開にのみ適用されます。VDA が VDA Upgrade feature に参加できるようにします。この機能を使用すると、管理コンソールから、即時またはスケジュールされた時間にカタログの VDA をアップグレードできます。このエージェントがインストールされていない場合、マシン上で VDA インストーラーを実行して VDA をアップグレードできます。

コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix VDA Upgrade Agent"`、コンポーネントのインストールを防止するには `/exclude "Citrix VDA Upgrade Agent"`。

- **MCSIO write cache for storage optimization:** Citrix MCS IO ドライバーをインストールします。詳しくは、Storage shared by hypervisors および Configure cache for temporary data を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix MCS IODriver"`、コンポーネントのインストールを防止するには `/exclude "Citrix MCS IODriver"`。

- **Proxy Configuration:** 環境でGateway Service、VDA Upgrade ServiceなどでRendezvousプロトコルを使用する予定があり、アウトバウンド接続のためにネットワークに非透過型プロキシがある場合は、このコンポーネントをインストールし、ここでプロキシを指定します。HTTP プロキシのみがサポートされています。

  このコンポーネントをインストールする場合は、**Rendezvous Proxy Configuration** ページでプロキシのアドレスまたはPACファイルのパスを指定します。機能の詳細については、Rendezvous protocol を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Rendezvous V2"`、コンポーネントのインストールを防止するには `/exclude "Citrix Rendezvous V2"`。

- **Citrix Backup and Restore:** VDA のインストールまたはアップグレードが失敗した場合、このコンポーネントはマシンをインストールまたはアップグレード前に作成されたバックアップに戻すことができます。

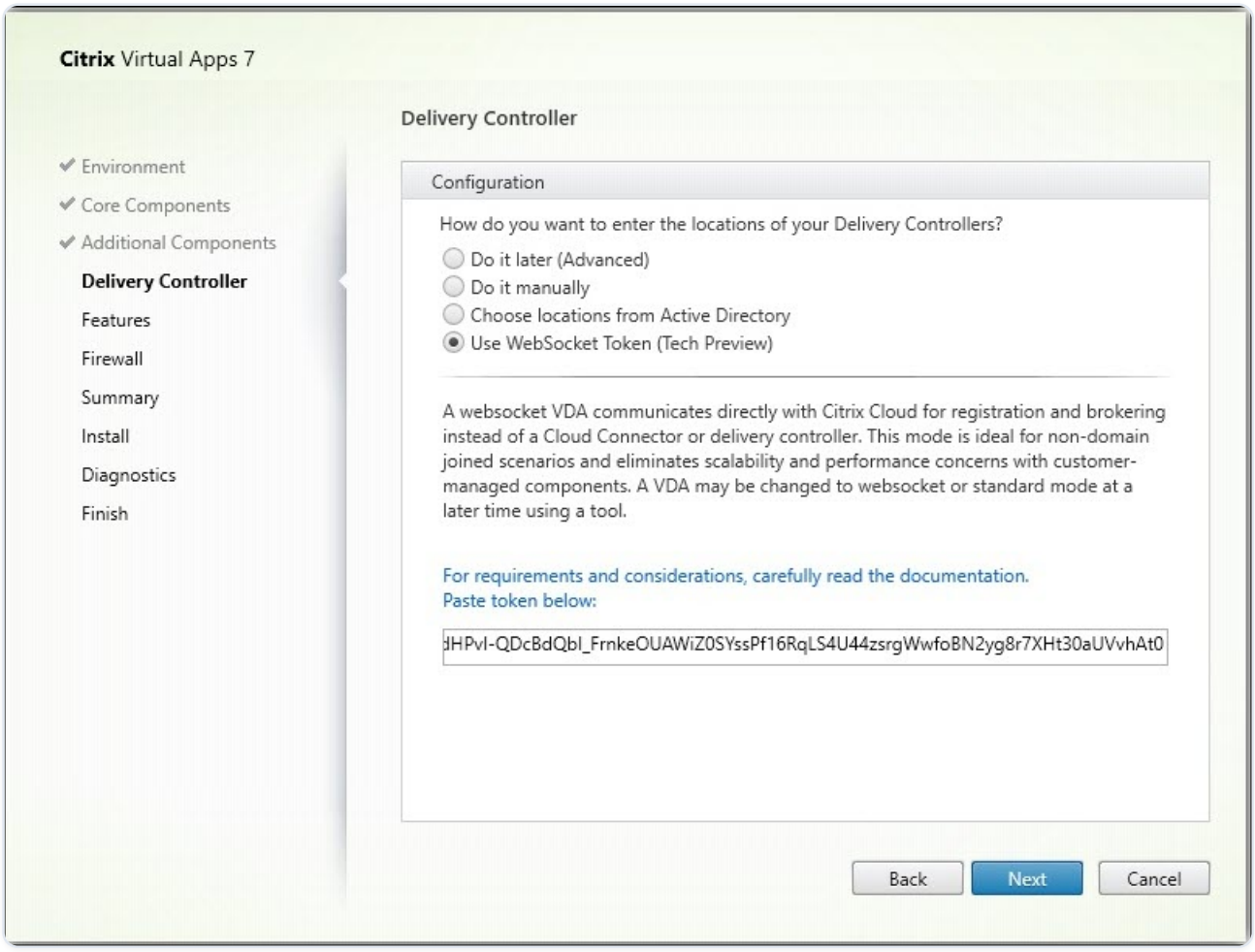
  Prepare to install に記載されている Microsoft の前提条件が満たされていることを確認してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Backup and Restore"`、コンポーネントのインストールを防止するには `/exclude "Citrix Backup and Restore"`。

> **注:**
>
> MCS ストレージ最適化が有効になっている場合、Windows Server またはデスクトップオペレーティングシステムのバックアップまたは復元が失敗する可能性があります。こ

> れを解決するには、メタインストーラーでMCSストレージ最適化オプションを無効にしてください。

Step 7. Delivery Controller™ アドレス



Delivery Controller ページで、インストールされているコントローラーのアドレスを入力する方法を選択します。Citrix では、VDA のインストール中にアドレスを指定することをお勧めします (**手動で実行**)。VDA はこの情報がないとコントローラーに登録できません。VDA が登録できない場合、ユーザーはその VDA 上のアプリケーションやデスクトップにアクセスできません。

- **手動で実行:** (デフォルト) インストールされているControllerのFQDNを入力し、**追加**をクリックします。複数のControllerをインストールしている場合は、それらのアドレスを追加します。
- **後で実行 (詳細設定):** このオプションを選択すると、続行する前に、ウィザードでその操作を実行するかどうかを確認するメッセージが表示されます。後でアドレスを指定するには、インストーラーを再実行するか、Citrixグループポリシーを使用します。ウィザードの**概要**ページでも通知されます。
- **Active Directoryから場所を選択:** マシンがドメインに参加しており、ユーザーがドメインユーザーである場合にのみ有効です。

- **WebSocketトークンを使用 (テクニカルプレビュー):** WebSocket VDAを作成します。WebSocketTokenは、必要なトークン用です。
- **Machine Creation Servicesに自動的に実行させる:** MCSを使用してマシンをプロビジョニングする場合にのみ有効です。

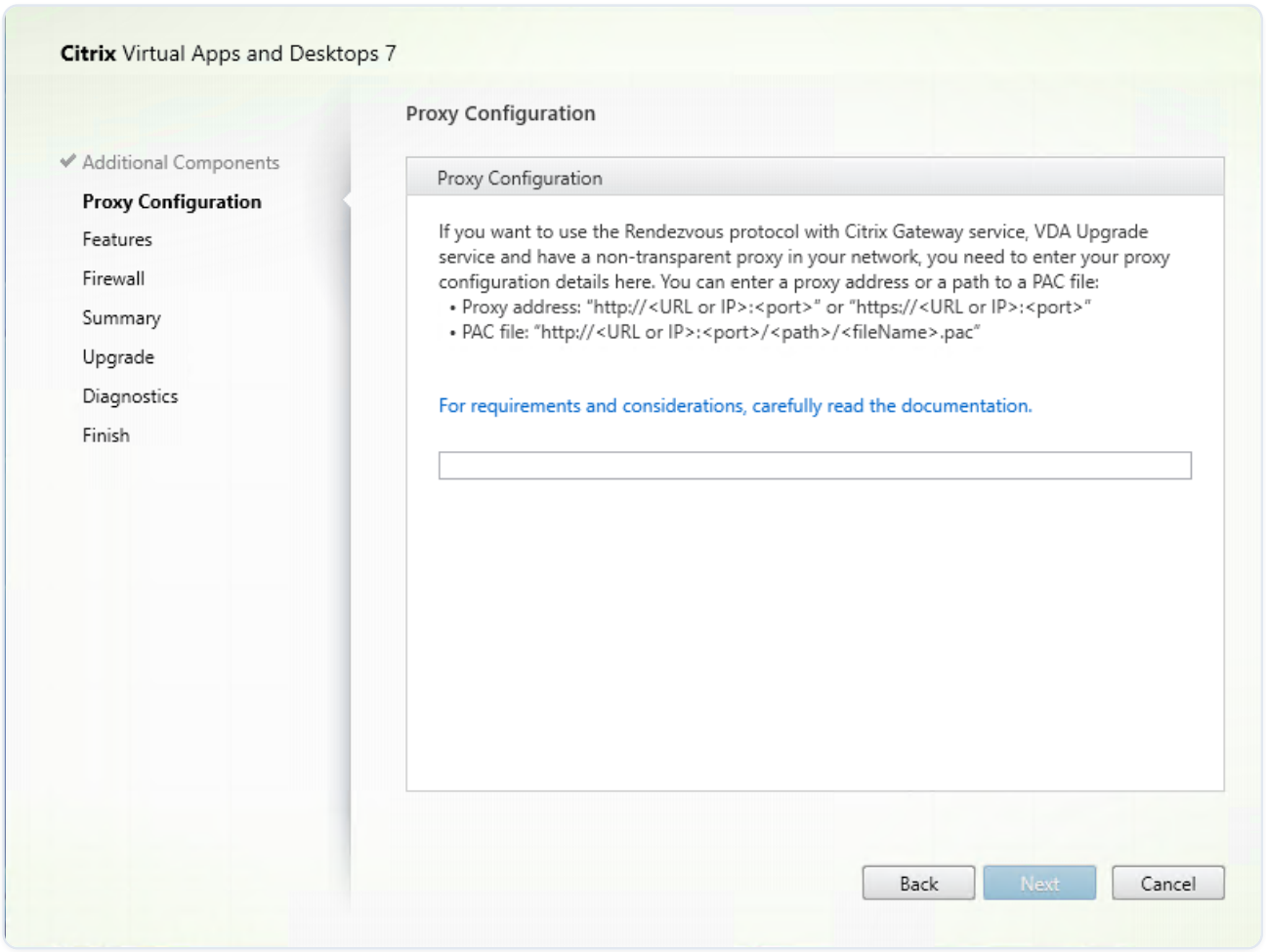
次へをクリックします。**後で実行 (詳細設定)**を選択した場合、後でControllerアドレスを指定することを確認するメッセージが表示されます。

その他の考慮事項:

- アドレスに英数字以外の文字を含めることはできません。
- VDAのインストール中およびグループポリシーでアドレスを指定した場合、ポリシー設定がインストール中に指定された設定よりも優先されます。
- VDAの登録を成功させるには、Controllerとの通信に使用されるファイアウォールポートが開いている必要があります。このアクションは、ウィザードの**ファイアウォール**ページでデフォルトで有効になっています。
- Controllerの場所を指定した後 (VDAのインストール中またはインストール後)、自動更新機能を使用して、Controllerが追加または削除されたときにVDAを更新できます。VDAがControllerを検出して登録する方法について詳しくは、「VDA登録」を参照してください。

コマンドラインオプション: `/controllers`

ステップ8. プロキシ構成



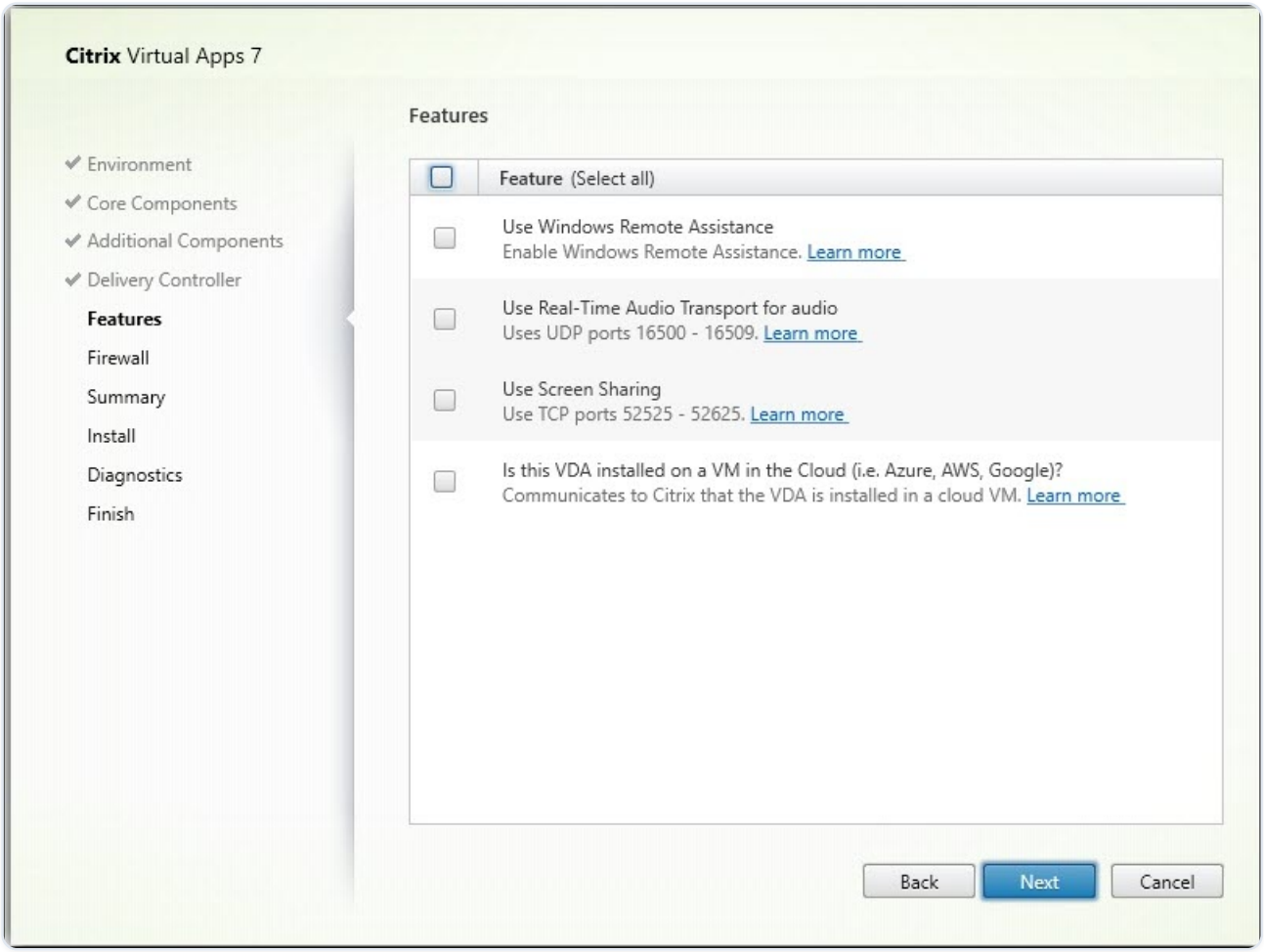
プロキシ構成ページは、**追加コンポーネント**ページで**プロキシ構成**チェックボックスを有効にした場合にのみ表示されます。

1. プロキシソースをプロキシアドレスで指定するか、PACファイルパスで指定するかを選択します。
2. プロキシアドレスまたはPACファイルパスを指定します。
   - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
   - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

接続テストを成功させるには、プロキシポートのファイアウォールが開いている必要があります。プロキシへの接続ができない場合でも、VDAのインストールを続行するかどうかを選択できます。

コマンドラインオプション: `/proxyconfig`

ステップ9. 機能の有効化または無効化



「**機能**」ページで、チェックボックスを使用して、使用したい機能を有効または無効にします。

- **Windows リモートアシスタンスを使用する:** この機能が有効な場合、Windows リモートアシスタンスはDirectorのユーザーシャドウ機能とともに使用されます。Windows リモートアシスタンスは、ファイアウォールで動的ポートを開きます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_remote_assistance`

- **オーディオにリアルタイムオーディオトランスポートを使用する:** ネットワークでVoIPが広く使用されている場合は、この機能を有効にします。この機能は、遅延を減らし、損失の多いネットワークでのオーディオの回復力を向上させます。RTP over UDPトランスポートを使用してオーディオデータを送信できます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_real_time_transport`

- **画面共有を使用する:** 有効にすると、画面共有で使用されるポートがWindowsファイアウォールで開かれます。(デフォルト = 無効)

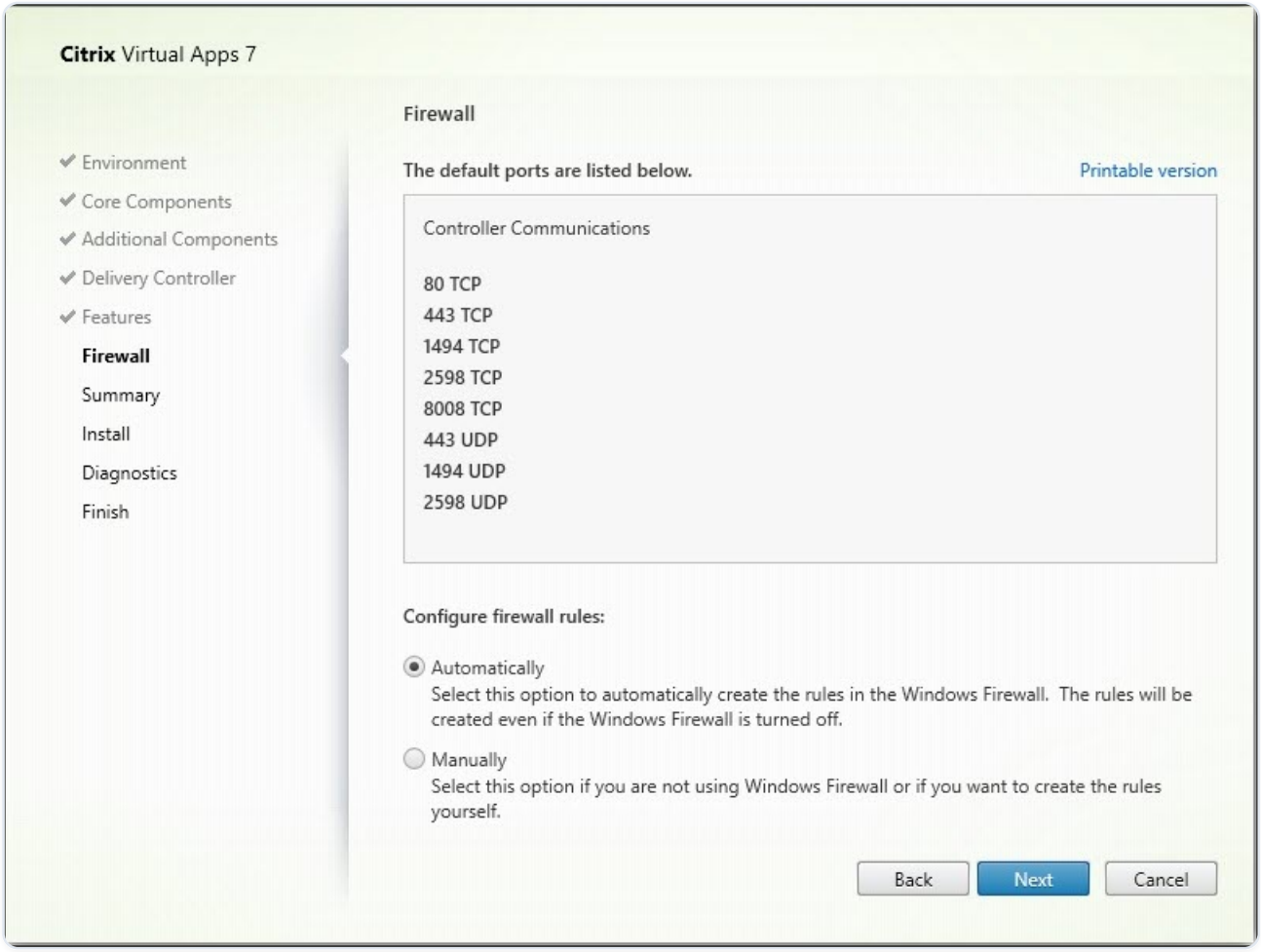
  コマンドラインオプション: `/enable_ss_ports`

- **このVDAはクラウドのVMにインストールされていますか:** この設定は、Citrixがテレメトリ目的でオンプレミスおよびサービス (Citrix Cloud™) VDA展開のリソースの場所を正しく識別するのに役立ちます。この機能は、顧客側の利用には影響しません。展開でCitrix DaaSを使用している場合は、この設定を有効にします (デフォルト = 無効)。

  コマンドラインオプション: `/xendesktopcloud`

Nextをクリックします。

手順10. ファイアウォールポート

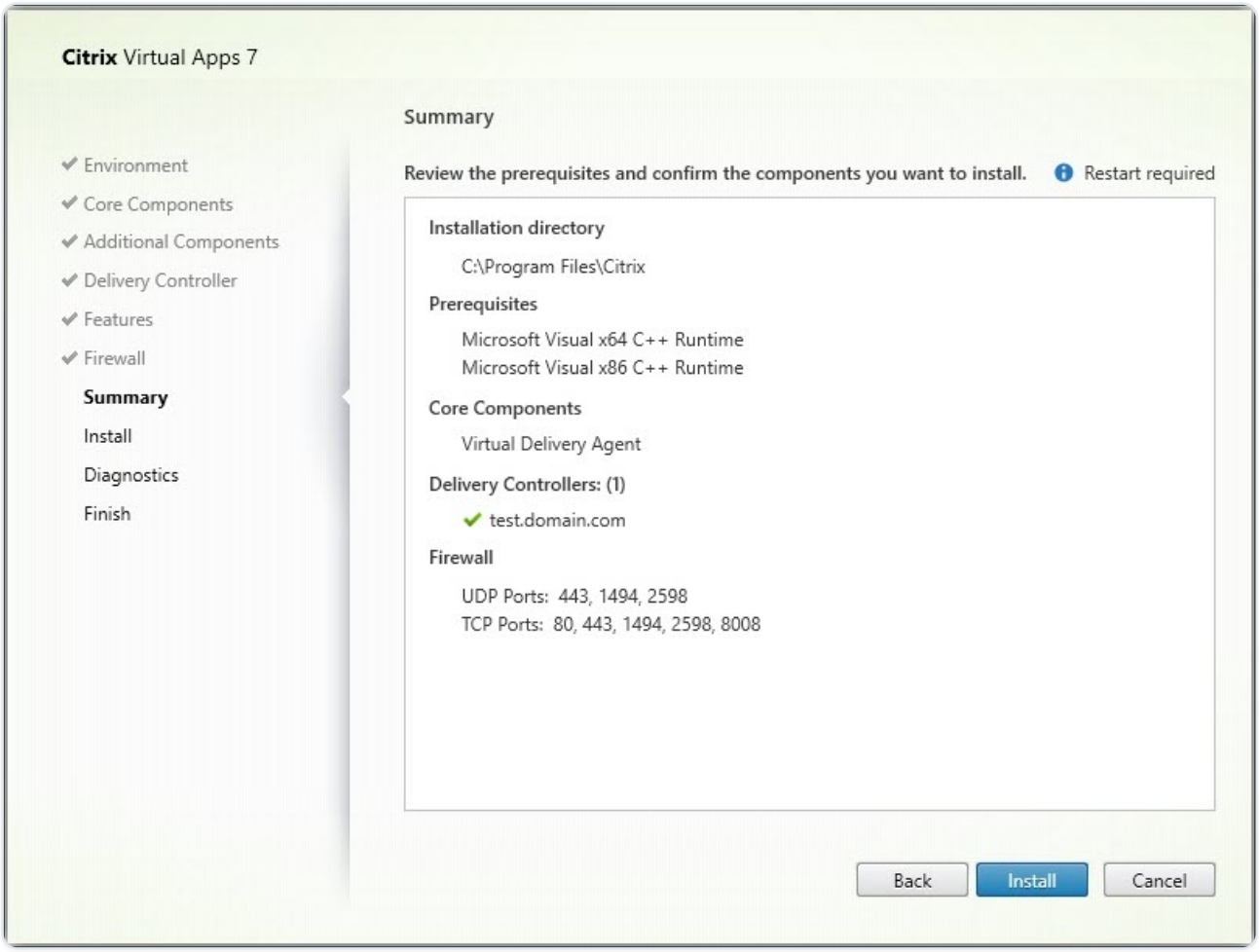


ファイアウォールページでは、デフォルトで、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくてもポートは自動的に開かれます。このデフォルト設定は、ほとんどの展開で問題ありません。ポート情報については、「ネットワークポート」を参照してください。

Nextをクリックします。

コマンドラインオプション: `/enable_hdx_ports`

手順11. 前提条件の確認とインストールの確認



概要ページには、インストールされるものが一覧表示されます。**戻る**ボタンを使用して、以前のウィザードページに戻り、選択を変更します。

準備ができたら、**インストール**をクリックします。

前提条件がまだインストールまたは有効になっていない場合、マシンは1回以上再起動する可能性があります。インストールの準備を参照してください。

手順12. 診断

VDAインストーラーの診断ページ(/en-us/citrix-virtual-apps-desktops/2311/media/vda-ss-diagnostics.png)

「**診断**」ページで、Citrix Call Homeに参加するかどうかを選択します。参加することを選択した場合（デフォルト）、**「接続」**をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。

資格情報が検証された後（または参加しないことを選択した場合）、**「次へ」**をクリックします。

フル製品インストーラーを使用している場合、**診断**ページで最初に**診断情報の収集**を選択せずに**接続**をクリックすると、**Citrix Insight Servicesへの接続**ダイアログを閉じた後、**次へ**ボタンが無効になります。次のページに進むことはできません。**次へ**ボタンを再度有効にするには、**診断情報の収集**を選択し、すぐに選択を解除します。

詳細については、「Call Home」を参照してください。

ステップ13. このインストールを完了する

VDAインストーラーの完了ページ(/en-us/citrix-virtual-apps-desktops/2311/media/vda-ss-finish.png)

完了ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントの緑色のチェックマークが表示されます。

「完了」をクリックします。デフォルトでは、マシンは自動的に再起動します。この自動再起動を無効にすることはできますが、マシンが再起動するまでVDAは使用できません。

次のステップ

必要に応じて、上記のプロシージャを繰り返して、他のマシンまたはイメージにVDAをインストールします。

すべてのVDAをインストールしたら、Studioを起動します。まだサイトを作成していない場合は、Studioが自動的にそのタスクに誘導します。それが完了すると、Studioはマシンカタログとデリバリーグループの作成に誘導します。参照：

- サイトの作成
- マシンカタログの作成
- 「デリバリーグループの作成」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/delivery-groups-create.html)

シトリックス オプティマイザー

Citrix Optimizerは、Citrix管理者がさまざまなコンポーネントを削除および最適化することでVDAを最適化するのに役立つWindows OS用のツールです。

VDA をインストールし、最終的な再起動を完了した後、Citrix Optimizer をダウンロードしてインストールします。CTX224676 を参照してください。CTX 記事には、ダウンロードパッケージと、Citrix Optimizer のインストールおよび使用方法に関する説明が含まれています。

VDAをカスタマイズする

インストール済みの VDA をカスタマイズするには：

1. プログラムの削除または変更を行う Windows 機能から、**Citrix Virtual Delivery Agent** または **Citrix Remote PC Access/VDI Core Services VDA** を選択します。次に右クリックして **変更** を選択します。
2. **Virtual Delivery Agent 設定のカスタマイズ** を選択します。インストーラーが起動したら、以下を変更できます。

   - Controller アドレス
   - Controller に登録するための TCP/IP ポート（デフォルト = 80）
   - Windows ファイアウォールポートを自動的に開くかどうか

トラブルシューティング

- コンポーネントのインストール結果を Citrix がどのように報告するかについては、Citrix インストールリターンコード を参照してください。
- デリバリーグループの Studio 表示で、**詳細** ペインの **インストール済み VDA バージョン** エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンの Windows のプログラムと機能の表示には、実際の VDA バージョンが表示されます。
- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを配信できません。

  VDA 登録方法と登録問題のトラブルシューティング方法については、VDA 登録 を参照してください。

スクリプトを使用してVDAをインストールする

> **注:**
>
> Citrixは、お客様の運用環境に合わせて調整されたスクリプトによって引き起こされる問題について責任を負いません。インストール関連のCitrixの問題については、Citrixサポートポータルを使用して、関連するインストールログとともにテクニカルサポートケースをオープンしてください。

> この記事は、Windowsオペレーティングシステムを搭載したマシンへのVDAのインストールに適用されます。Linuxオペレーティングシステム用VDAの詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

インストールメディアには、Active Directory内のマシンにVirtual Delivery Agent (VDA) をインストール、アップグレード、または削除するサンプルスクリプトが含まれています。これらのスクリプトは、Machine Creation Services™およびCitrix Provisioning (旧Provisioning Services) で使用されるマスターイメージの保守にも使用できます。

必要なアクセス権:

- スクリプトは、VDAインストールコマンドが配置されているネットワーク共有への「Everyone Read」アクセス権を必要とします。インストールコマンドは、フル製品ISOでは `XenDesktopVdaSetup.exe`、スタンドアロンインストーラーでは `VDAWorkstationSetup.exe` または `VDAServerSetup.exe` です。
- ログの詳細は各ローカルマシンに保存されます。レビューと分析のために結果を集中してログに記録するには、スクリプトは適切なネットワーク共有への「Everyone Read and Write」アクセス権を必要とします。

スクリプトの実行結果を確認するには、中央ログ共有を調べます。キャプチャされたログには、スクリプトログ、インストーラーログ、MSIインストールログが含まれます。各インストールまたは削除の試行は、タイムスタンプ付きのフォルダーに記録されます。フォルダーのタイトルは、PASSまたはFAILのプレフィックスで操作結果を示します。標準のディレクトリ検索ツールを使用して、中央ログ共有で失敗したインストールまたは削除を見つけることができます。これらのツールは、ターゲットマシンでローカルに検索する代替手段を提供します。

インストールを開始する前に、インストールの準備のタスクを読み、完了してください。

スクリプトを使用してVDAをインストールまたはアップグレードする

1. インストールメディアの\\Support\\AdDeploy\\からサンプルスクリプト**InstallVDA.bat**を入手します。Citrixは、元のスクリプトをカスタマイズする前にバックアップを作成することをお勧めします。
2. スクリプトを編集します。
    - インストールするVDAのバージョンを指定します: `SET DESIREDVERSION`。たとえば、バージョン7は7.0として指定できます。完全な値は、インストールメディアのProductVersion.txtファイルに記載されています。ただし、完全な一致は必須ではありません。

- インストーラーが呼び出されるネットワーク共有を指定します。レイアウトのルート（ツリーの最上位）を指します。スクリプトの実行時に、適切なバージョンのインストーラー（32ビットまたは64ビット）が自動的に呼び出されます。例: `SET DEPLOYSHARE=\\fileserver1\share1`。
- オプションで、集中ログを保存するためのネットワーク共有の場所を指定します。例: `SET LOGSHARE=\\fileserver1\log1)`。
- コマンドラインを使用したインストールで説明されているように、VDA構成オプションを指定します。`/quiet`および`/noreboot`オプションは、スクリプトにデフォルトで含まれており、必須です: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT`。

3. グループポリシーのスタートアップスクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAをインストールするマシンのみを含める必要があります。そのOU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。サポートされているオペレーティングシステムを持つ各マシンにVDAがインストールされます。

スクリプトを使用してVDAを削除する

1. インストールメディアの\\Support\\AdDeploy\\からサンプルスクリプトUninstallVDA.batを入手します。Citrixは、元のスクリプトをカスタマイズする前にバックアップを作成することをお勧めします。
2. スクリプトを編集します。
   - 削除するVDAのバージョンを指定します: `SET CHECK\_VDA\_VERSION`。たとえば、バージョン7は7.0として指定できます。完全な値は、インストールメディアのProductVersion.txtファイル（7.0.0.3018など）で見つけることができます。ただし、完全一致は必要ありません。
   - オプションで、集中ログを保存するためのネットワーク共有の場所を指定します。
3. グループポリシーのスタートアップスクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAを削除するマシンのみを含める必要があります。OU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。各マシンからVDAが削除されます。

トラブルシューティング

- スクリプトは、スクリプト実行の進行状況を記述する内部ログファイルを生成します。スクリプトは、展開開始から数秒以内に`Kickoff_VDA_Startup_Script`ログを中央ログ共有にコピーします。全体的なプロセスが機能していることを確認できます。このログが期待どおりに中央ログ共有にコピーされない場合は、ローカルマシンを検査してさらにトラブルシューティ

ングを行ってください。スクリプトは、各マシンの`%temp%`フォルダーに2つのデバッグログファイルを配置します。

- `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
- `VDA_Install_ProcessLog_<DateTimeStamp>.log`

スクリプトが次の状態であることを確認するために、これらのログを確認します。

- 期待どおりに実行されている。
- ターゲットオペレーティングシステムを適切に検出する。
- `DEPLOYSHARE`共有の`ROOT`を指すように正しく構成されていること（`AutoSelect.exe`という名前のファイルが含まれています）。
- `DEPLOYSHARE`と`LOG`の両方の共有に対して認証できること。

- Citrixがコンポーネントインストールの結果を報告する方法については、「Citrixインストールリターンコード」を参照してください。
- デリバリーグループのStudio表示では、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを配信できません。

  VDA登録方法と登録の問題のトラブルシューティングについては、「VDA登録」を参照してください。

SCCM を使用した VDA のインストール

> **注：**

> Citrix は、お客様の運用環境に合わせて調整された Microsoft System Center Configuration Manager (SCCM) などのソフトウェア配布ツールを使用して Virtual Delivery Agent (VDA) を展開することによって発生する問題について責任を負いません。インストール関連の Citrix の問題については、Citrix サポートポータル を使用して、関連するインストールログを添えてテクニカルサポートケースをオープンしてください。

概要

Microsoft System Center Configuration Manager (SCCM) または同様のソフトウェア配布ツールを使用して Virtual Delivery Agent (VDA) を正常に展開するには、Citrix® は VDA インストーラーを段階的に使用することをお勧めします。

Citrix は、VDA のインストールまたはアップグレードの一部として VDA クリーンアップユーティリティを使用することをお勧めしません。VDA クリーンアップユーティリティは、VDA インストーラーが以前に失敗した場合の限定的なケースでのみ使用してください。

再起動

VDA のインストール中に必要な再起動の回数は、環境によって異なります。例:

- 保留中の更新や以前のソフトウェアインストールからの再起動のために、再起動が必要になる場合があります。
- 他のプロセスによって以前にロックされていたファイルは更新が必要になる場合があり、追加の再起動を強制します。
- VDA インストーラーの一部のオプションコンポーネント（Citrix Profile Management や Citrix Files など）は、再起動が必要になる場合があります。

SCCMタスクシーケンサーは、必要なすべての再起動を管理します。

タスクシーケンスを定義する

すべての前提条件と再起動を特定したら、SCCM タスクシーケンサーを使用して以下を完了します。

- VDA は、インストールメディアのアクセス可能なコピーから、または VDA スタンドアロンインストーラーのいずれかからインストールできます。
  - `VDAWorkstationSetup_XXXX.exe`
  - `VDAServerSetup_XXXX.exe`
  - `VDAWorkstationCoreSetup_XXXX.exe`

  VDAインストーラーの詳細については、「インストーラー」を参照してください。
- VDAをアップグレードする場合、それがインストールされているマシンは、セッションがない状態でメンテナンスモードである必要があります。
- マシン上でVDAのインストールが初めて実行されるとき、使用されているVDAインストーラーはそのマシンにコピーされます。

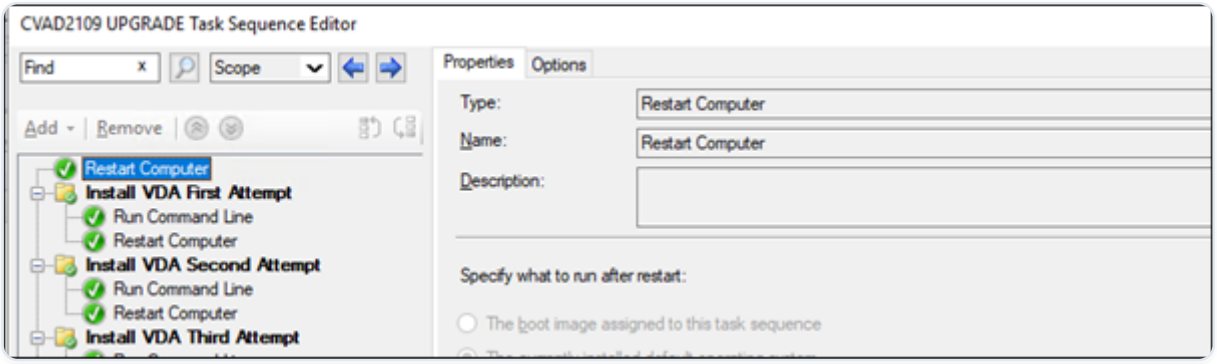
  - `VDAWorkstationCoreSetup_XXXX.exe`以外のVDAインストーラーを使用する場合、VDAインストーラーは`%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`にコピーされます。
  - `VDAWorkstationCoreSetup_XXXX.exe`を使用する場合、VDAインストーラーは`%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe`にコピーされます。`

- VDAインストーラーのディレクトリの場所は、レジストリ`“HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall”``“MetaInstallerInstallLocation”`にも保存されます。
- コマンドラインオプションに`/NOREBOOT`、`/NORESUME`、および`/QUIET`を追加します。
  - `/QUIET`: インストール中にユーザーインターフェイスを表示しないことで、SCCMがインストールプロセスを制御できるようにします。
  - `/NOREBOOT`: VDAインストーラーが自動的に再起動するのを抑制します。SCCMは必要に応じて再起動をトリガーします。
  - `/NORESUME`: 通常、インストール中に再起動が必要な場合、VDAインストーラーは`runonce`レジストリキー(`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`)を設定します。マシンが再起動すると、Windowsはそのキーを使用してVDAインストーラーを起動します。これはSCCMにとって問題です。なぜなら、SCCMはインストールを監視し、終了コードをキャプチャできないからです。

SCCM を使用したインストールシーケンスの例

次の例は、インストールシーケンスを示しています。

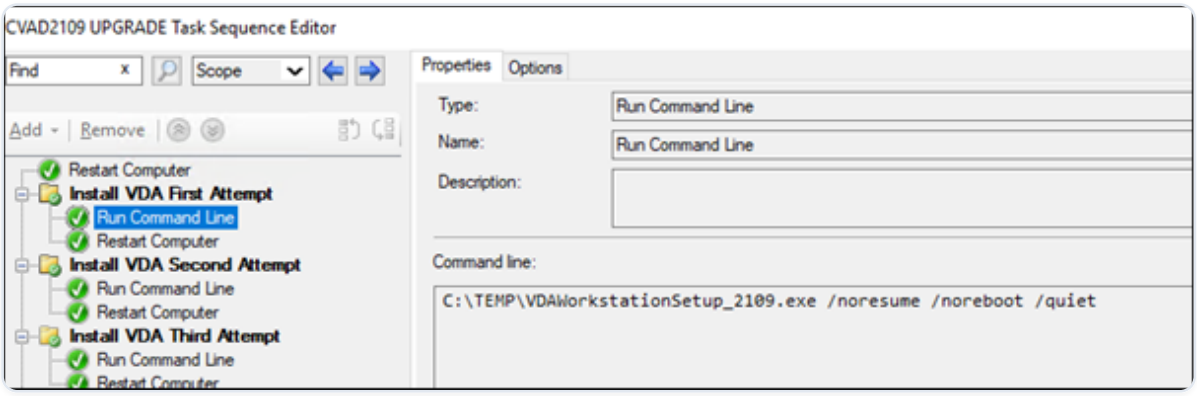
1. **コンピューターの再起動:** マシンを再起動して準備します。



2. **VDAのインストール（初回試行）:** VDAのインストールを開始します。

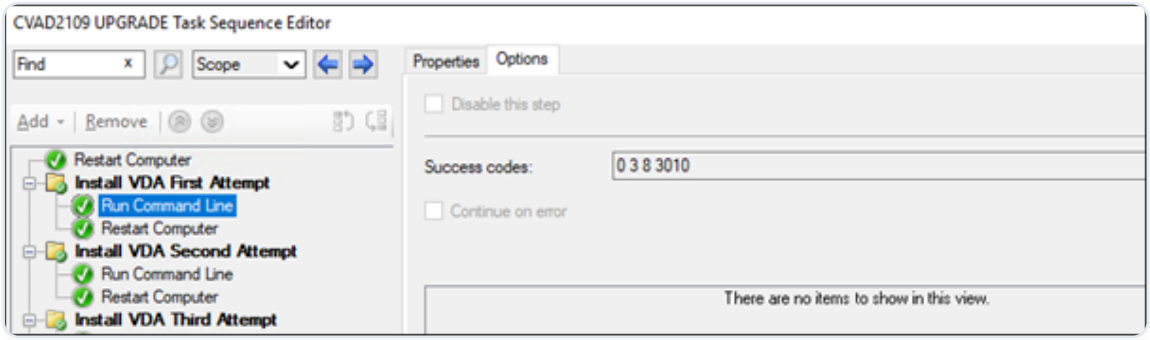
a. コマンドラインオプションに`/quiet`、`/noreboot`、および`/noresume`オプションを追加します。

b. 選択したVDAインストーラー（ローカルイメージまたは最小インストーラーのいずれか）を実行します。

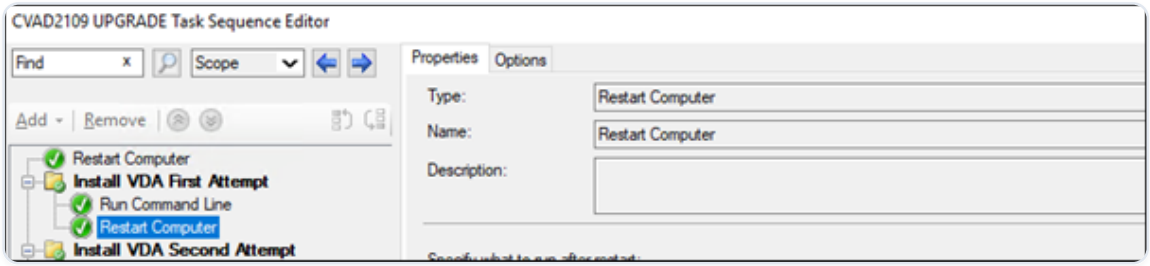


c. SCCMはリターンコードをキャプチャする必要があります。

- リターンコードが0または8の場合、インストールは完了しており、再起動が必要です。



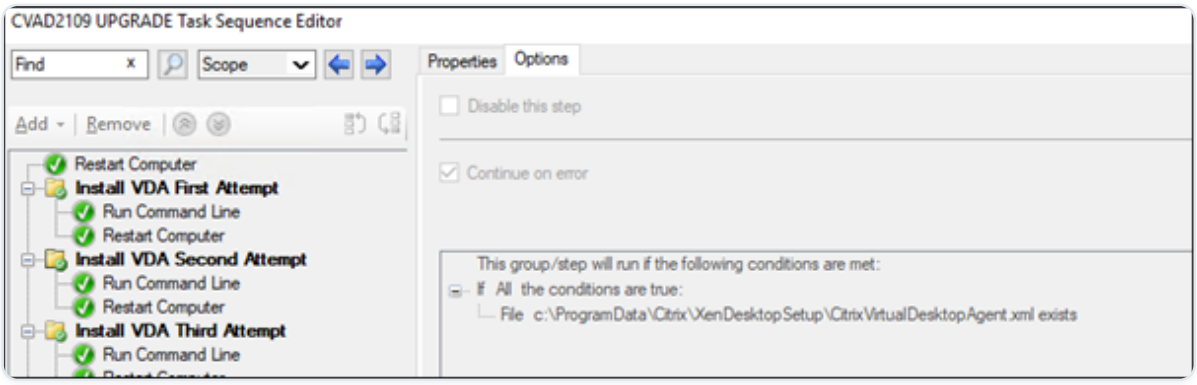
- リターンコードが3の場合、マシンを再起動してから、**VDAのインストール（2回目試行）**に制御を渡します。



3. **VDAのインストール（2回目試行）：**VDAのインストールを続行します。

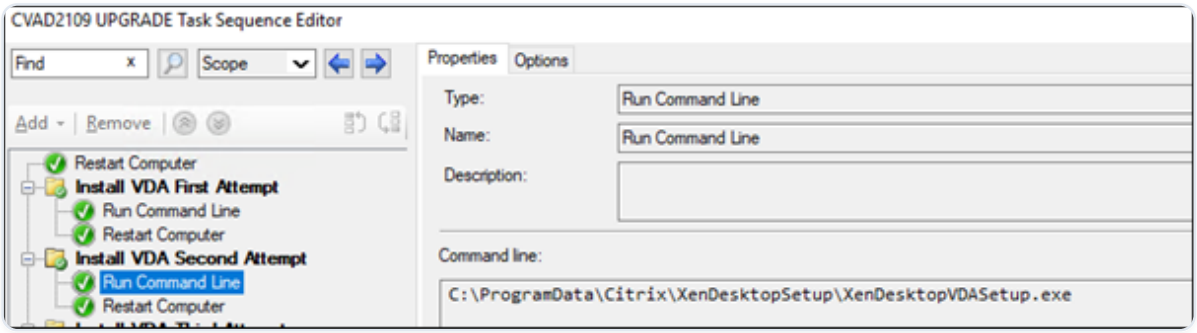
a. **VDAのインストール（初回試行）**の後、ファイル`%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml`が存在する場合、インス

トールは完了しておらず、再起動が完了した後に続行する必要があります。



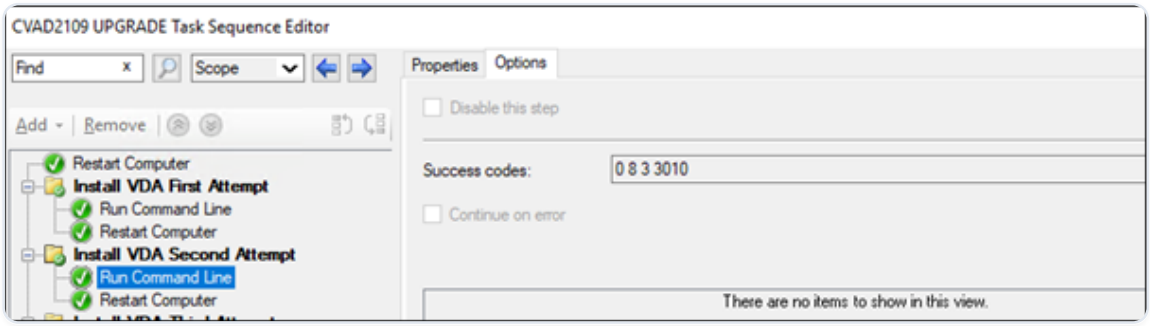
b. **VDAのインストール（2回目試行）**は、ファイル`%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml`が存在しなくなるか、0または8以外のリターンコードが返されるまで繰り返されます。その他のリターンコードはエラーとして扱い、VDAのインストール（2回目試行）はエラーを報告して停止する必要があります。

c. コマンドラインパラメーターなしで、ファイル`%programdata%\Citrix\XenDesktopSetup\`ディレクトリから適切なVDAインストーラー（ほとんどの場合`XenDesktopVdaSetup.exe`、`VDAWorkstationCoreSetup_XXXX.exe`が使用された場合は`XenDesktopRemotePCSetup.exe`）を実行して、VDAのインストールを再開します。（VDAインストーラーは、インストーラーの初回実行時に保存したパラメーターを使用します。）



d. VDAインストーラーからのリターンコードに注意してください。

- 0または8：成功、インストール完了、再起動が必要です。



- 3：インストールは完了していません。マシンを再起動し、ファイル`%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml`が存在しなくなるか、

0または8が返されるまでVDAのインストール（2回目試行）を繰り返します。その他のリターンコードはエラーとして扱い、VDAのインストール（2回目試行）はエラーを報告して終了する必要があります。

リターンコードの詳細については、Citrixインストールリターンコードを参照してください。

VDAインストールコマンドの例

利用可能なインストールオプションは、使用するインストーラーによって異なります。コマンドラインオプションの詳細については、以下の記事を参照してください。

- VDA のインストール
- コマンドラインを使用したインストール

Remote PC Access のインストールコマンド

- 次のコマンドは、シングルセッションコア VDA インストーラー（`VDAWorkstationCoreSetup.exe`）を使用します。

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

専用 VDI のインストールコマンド

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers “control.domain.com” /enable_hdx_ports /enable_remote_assistance /noresume /noreboot
  ```

サイトを作成する

> **注:**

> サイト作成中に、ハイブリッド権限ライセンスを有効にするライセンスを追加した後、サイト作成が完了するまで、パブリッククラウドホスト（Microsoft Azure、Google Cloud Platform、Amazon Web Servicesなど）は接続の種類リストに表示されません。

> サイトとは、Citrix Virtual Apps and Desktops™展開に付ける名前です。これには、Delivery Controllerとその他のコアコンポーネント、Virtual Delivery Agent (VDA)、ホストへの接続、マシンカタログ、およびデリバリーグループが含まれます。サイトは、コアコンポーネントをインストールした後、最初のマシンカタログとデリバリーグループを作成する前に作成します。

ControllerがServer Coreにインストールされている場合は、Citrix Virtual Apps and Desktops SDKのPowerShellコマンドレットを使用してサイトを作成します。

サイトを作成すると、Citrixカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。CEIPは匿名の統計情報と使用状況情報を収集し、Citrixに送信します。最初のデータパッケージは、サイト作成後約7日後にCitrixに送信されます。サイト作成後いつでも登録を変更できます。Web Studioの左ペインで**設定**を選択し、**Citrixカスタマーエクスペリエンス向上プログラム**の設定を見つけます。詳細については、`<http://more.citrix.com/XD-CEIP>`を参照してください。

サイトを作成したユーザーは、フル管理者になります。詳しくは、委任管理を参照してください。

サイトを作成する前にこの記事を確認して、何が予想されるかを知っておいてください。

ステップ1. サイト作成ウィザードを開く - Citrix Site Manager

Citrix Virtual Apps and Desktops展開（サイトとも呼ばれます）を設定するには、Citrix Site Managerツールを使用します。このツールは、Delivery Controllerをインストールすると自動的にインストールされます。

このツールを実行するには、Delivery Controllerでデスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager**を選択します。Web Studioのインストールを参照してください。

ステップ2. サイト名

はじめにページで、サイトの名前を入力します。

ステップ3. データベース

データベースページには、サイト、監視、および構成ログデータベースを設定するための選択肢が含まれています。データベースのセットアップの選択肢と要件の詳細については、データベースを参照してください。

> **注:**
>
> SQL Server Always On ListenerがTLS暗号化用に構成されている場合、データベース作成権限を持つ資格情報の入力を求められることがあります。有効な管理者資格情報を入力しても、データベースの作成は失敗します。SQL Server証明書に、Subject Alternative Names (SAN) にリスナーのDNS名が含まれていることを確認してください。詳細については、`<https://docs.microsoft.com/ja-jp/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates>` を参照してください。

> サイトデータベースとして SQL Server Express をインストールすることを選択した場合 (デフォルト)、そのソフトウェアのインストール後に再起動が発生します。サイトデータベースとして SQL Server Express ソフトウェアをインストールしないことを選択した場合は、再起動は発生しません。

デフォルトのSQL Server Expressを使用しない場合は、サイトを作成する前に、SQL Serverソフトウェアがマシンにインストールされていることを確認してください。システム要件にサポートされているバージョンが記載されています。

サイトにDelivery Controllerを追加したい場合で、すでに他のサーバーにControllerソフトウェアをインストールしている場合は、このページからそれらのControllerを追加できます。データベースを設定するスクリプトを生成する予定がある場合は、スクリプトを生成する前にControllerを追加してください。

ステップ4. ライセンス

ページで、ライセンスサーバーのアドレスを指定し、使用する (インストールする) ライセンスを示します。

- ライセンスサーバーのアドレスを `name:[port]` の形式で指定します。*name* は FQDN、NetBIOS、または IP アドレスである必要があります。FQDN を推奨します。ポート番号を省略した場合、デフォルトは 27000 です。 をクリックします。ライセンスサーバーへの接続が成功するまで、次のページに進むことはできません。

- 接続が確立されると、デフォルトで が選択されます。表示には、現在インストールされているライセンスに基づいて、この製品として構成できる互換性のある製品が一覧表示されます。
  - この製品をリストされている製品のいずれか (例: Citrix Virtual Apps Premium または Citrix Virtual Desktops™ Premium) として構成したい場合は、それらのライセンスのいずれかを使用して、そのエントリを選択します。
  - この製品で使用するためにライセンスを割り当ててダウンロード済み (Citrix Manage Licenses Tool を使用) であるが、まだライセンスをインストールしていない場合:
    - をクリックします。
    - ファイルエクスプローラーで、ダウンロードしたライセンスを見つけて選択します。関連する製品が、サイト作成ウィザードの ページに表示されます。使用したいエントリを選択します。
  - 目的の製品が表示されない場合、または割り当て済みでダウンロード済みのライセンスがない場合は、ライセンスを割り当て、ダウンロードしてインストールできます。これを行うには、ライセンスサーバーがインターネットにアクセスできる必要があります。目的の製品のライセンスアクセスコードが必要です。Citrixからそのコードがメールで送信されます。
    - をクリックします。
    - 「**ライセンスの割り当て**」ダイアログで、Citrix から送付されたライセンスアクセスコードを入力します。「**ライセンスの割り当て**」をクリックします。
    - 新しいライセンスに関連付けられた製品が、サイト作成ウィザードの「**ライセンス**」ページに表示されます。使用するエントリを選択します。

  または、「**30日間無料トライアルを使用する**」を選択し、後でライセンスをインストールします。詳細については、ライセンスドキュメントを参照してください。

ステップ5. 概要

概要ページには、指定した情報が一覧表示されます。変更する場合は、**戻る**ボタンを使用します。完了したら、**完了**をクリックします。

詳細情報

ホスト接続、ネットワーク、およびストレージ

ハイパーバイザーまたはその他のサービス上のVMを使用してアプリケーションとデスクトップを配信している場合、オプションでそのホストへの最初の接続を作成できます。その接続のスト

レージおよびネットワークリソースを指定することもできます。サイト作成後、この接続とリソースを変更したり、さらに接続を作成したりできます。詳細については、接続とリソースを参照してください。

- 「**接続**」ページで指定される情報については、接続とリソースを参照してください。
  - ハイパーバイザーまたはその他のサービス上のVMを使用していない場合（またはWeb Studioを使用して専用ブレードPC上のデスクトップを管理する場合）は、接続の種類として「**なし**」を選択します。
  - Remote PCアクセスサイトを構成していて、Wake on LAN機能を使用する予定がある場合は、「**Microsoft System Center Virtual Machine Manager**」または「**Remote PC Wake on LAN**」タイプを選択します。詳細については、Wake on LANを参照してください。

  接続の種類に加えて、Citrixツール（Machine Creation Services™など）またはその他のツールを使用してVMを作成するかどうかを指定します。
- 「**ストレージ**」および「**ネットワーク**」ページで指定される情報については、ホストストレージ、ストレージ管理、およびストレージの選択を参照してください。
- ハイブリッド権限ライセンスを所有しており、パブリッククラウドホスト接続（AWSなど）を追加している場合、それらの接続がここに一覧表示されます。それらのパブリッククラウドホスト接続を表示するには、追加後数分経ってからWeb Studioを更新してください。

Remote PCアクセス

Remote PC Accessの展開については、Remote PC Accessを参照してください。

Wake on LAN機能を使用する場合は、サイトを作成する前にMicrosoft System Center Configuration Managerで構成手順を完了してください。詳細については、Configuration ManagerとRemote PC Access Wake on LANを参照してください。

接続とリソースの作成および管理

> **重要：**
>
> Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するEnd of Life (EOL)項目を削除した後にのみ、展開を現在のリリースにアップグレードできます。

- パーソナル vDisk (PvD)
- AppDisks™
- パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

詳細については、「PVD、AppDisks、およびサポートされていないホストの削除」を参照してください。

注：

Citrix Virtual Apps and Desktopsの展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにHybrid Rights Licenseが必要です。

インストーラーがサポートされていないテクノロジーまたはHybrid Rights Licenseのないホスト接続を1つ以上検出すると、アップグレードが一時停止または停止し、説明メッセージが表示されます。インストーラーログに詳細が含まれています。詳細については、「展開のアップグレード」を参照してください。

Hybrid Rights Licenseがホスト接続に与える影響

Hybrid Rights Licenseの資格に基づいて、パブリッククラウドホストへのホスト接続が影響を受ける3つのシナリオがあります。

- パブリッククラウドホストへの新しいホスト接続を作成するには、Hybrid Rights Licenseが必要です。
- Hybrid Rights Licenseを所有しているがライセンスの有効期限が切れている場合、パブリッククラウドホストへの既存の接続は資格なしとマークされ、メンテナンスモードに入ります。既存のホスト接続がメンテナンスモードの場合、次の操作はできません。
  - ホスト接続の追加または変更
  - カタログの作成とイメージの更新
  - 電源操作を実行する

- 権限のないホスト接続が権限のあるホスト接続に変更されると、既存のホスティング接続が再度有効になります。

はじめに

サイトを作成する際に、ホスティングリソースへの最初の接続をオプションで作成できます。後で、その接続を変更したり、他の接続を作成したりできます。接続の構成には、サポートされているハイパーバイザーの中から接続タイプを選択すること、およびその接続のリソースから選択するストレージとネットワークが含まれます。

読み取り専用管理者は、接続とリソースの詳細を表示できます。接続とリソースの管理タスクを実行するには、フル管理者である必要があります。詳細については、「委任管理」を参照してください。

接続タイプに関する情報の入手先

サポートされている仮想化プラットフォームを使用して、Citrix Virtual AppsまたはCitrix Virtual Desktops環境でマシンをホストおよび管理できます。「システム要件」の記事に、サポートされている種類が記載されています。

詳細については、以下の情報源を参照してください。

- **XenServer (旧シトリックス ハイパーバイザー™):**
  - XenServer仮想化環境。
  - XenServer®ドキュメント。
- **ニュータニックス アクロポリス:**
  - Nutanix仮想化環境。
  - Nutanix ドキュメント。
- **ヴイエムウェア:**
  - VMware 仮想化環境。
  - VMware 製品ドキュメント。
- **Microsoft ハイパーV:**
  - Microsoft System Center Virtual Machine Manager 仮想化環境 の記事。
  - Microsoft ドキュメント。

- **パブリッククラウドホスト接続 (AWS、Google Cloud、Microsoft Azure、Nutanix クラウドおよびパートナーソリューション、VMware クラウドおよびパートナーソリューション):** パブリッククラウドホストに関する情報については、リソースタイプのセットアップ を参照してください。

> **注:**
>
> 情報源は Citrix DaaS™ ドキュメントを参照しています。Citrix DaaS 製品のパブリッククラウドホストに慣れている場合でも、オンプレミスバージョンにはいくつかの違いがあります。オンプレミスの Virtual Apps and Desktops では、管理インターフェイスは Web Studio と呼ばれます。更新はサービスに約4週間ごとに展開されます。そのため、サービスで利用可能な特定の機能がオンプレミスバージョンでは利用できない場合があります。

ホストストレージ

サポートされているハイパーバイザーによって管理されている場合、ストレージ製品はサポートされます。Citrix サポートは、これらのストレージ製品ベンダーが問題のトラブルシューティングと解決を支援し、必要に応じてナレッジセンターにそれらの問題を文書化します。

マシンをプロビジョニングする際、データはタイプ別に分類されます。

- オペレーティングシステム (OS) データ。これにはマスターイメージが含まれます。
- 一時データ。このデータには、MCS プロビジョニングされたマシンに書き込まれるすべての非永続データ、Windows ページファイル、ユーザープロファイルデータ、および ShareFile と同期されるデータが含まれます。このデータは、マシンが再起動するたびに破棄されます。

各データタイプに個別のストレージを提供することで、各ストレージデバイスの負荷を軽減し、パフォーマンスを向上させ、ホストの利用可能なリソースを最大限に活用できます。また、異なるデータタイプに適切なストレージを使用できるようになります。一部のデータでは、永続性と回復性が他のデータよりも重要です。

ストレージは共有（中央に配置され、どのホストからも独立しており、すべてのホストで使用される）することも、ハイパーバイザーにローカルに配置することもできます。たとえば、中央共有ストレージは、1つ以上のWindows Server 2012クラスター化ストレージボリューム（接続ストレージの有無にかかわらず）、またはストレージベンダーのアプライアンスである場合があります。中央ストレージは、ハイパーバイザーストレージ制御パスやパートナープラグインを介した直接アクセスなど、独自の最適化を提供する可能性もあります。

一時データをローカルに保存することで、共有ストレージにアクセスするためにネットワークを介する必要がなくなります。また、共有ストレージデバイスの負荷も軽減されます。共有ストレージはより高価になる可能性があるため、データをローカルに保存することで費用を抑えることができます。これらの利点は、ハイパーバイザーサーバー上の十分なストレージの可用性と比較検討する必要があります。

接続を作成する際、ハイパーバイザー間で共有されるストレージ、またはハイパーバイザーにローカルなストレージの2つのストレージ管理方法のいずれかを選択します。

1つ以上のXenServerホストで一時データストレージにローカルストレージを使用する場合、プール内の各ストレージの場所に一意の名前があることを確認してください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

ハイパーバイザーで共有されるストレージ

ハイパーバイザー間で共有されるストレージ方式は、長期的な永続性が必要なデータを中央に保存し、一元的なバックアップと管理を提供します。このストレージにはOSディスクが格納されます。

この方法を選択すると、一時的なマシンデータにローカルストレージ（同じハイパーバイザープール内のサーバー上）を使用するかどうかを選択できます。この方法は、共有ストレージ内のデータほど永続性や回復性を必要としません。これは*一時データキャッシュ*と呼ばれます。ローカルディスクは、メインOSストレージへのトラフィックを削減するのに役立ちます。このディスクは、マシンが再起動するたびにクリアされます。ディスクはライトスルーメモリキャッシュを介してアクセスされます。一時データにローカルストレージを使用する場合、プロビジョニングされたVDAは特定のハイパーバイザーホストに紐付けられます。そのホストが故障すると、VMは起動できません。

例外: Microsoft System Center Virtual Machine Managerは、クラスター共有ボリューム（CSV）を使用する場合、ローカルストレージ上の一時データキャッシュディスクを許可しません。

一時データをローカルに保存するための接続を作成し、各VMのキャッシュディスクサイズとメモリサイズの非デフォルト値を有効にして構成します。デフォルト値は接続タイプに合わせて調整されており、ほとんどのケースで十分です。詳細については、「マシンカタログの作成」を参照してください。

ハイパーバイザーは、ディスクイメージのローカルでの読み取りキャッシュを通じて最適化テクノロジーを提供することもできます。たとえば、XenServerはIntelliCache™を提供しており、これにより中央ストレージへのネットワークトラフィックが削減されます。

ハイパーバイザーのローカルストレージ

ハイパーバイザーにローカルなストレージ方式では、データをハイパーバイザーにローカルに保存します。この方式では、マスターイメージやその他のOSデータがサイト内のハイパーバイザーに転送されます。このプロセスは、最初のマシン作成時と将来のイメージ更新時に発生します。このプロセスにより、管理ネットワークでかなりのトラフィックが発生します。イメージ転送には時間がかかり、イメージは各ホストで異なるタイミングで利用可能になります。

接続とリソースを作成する

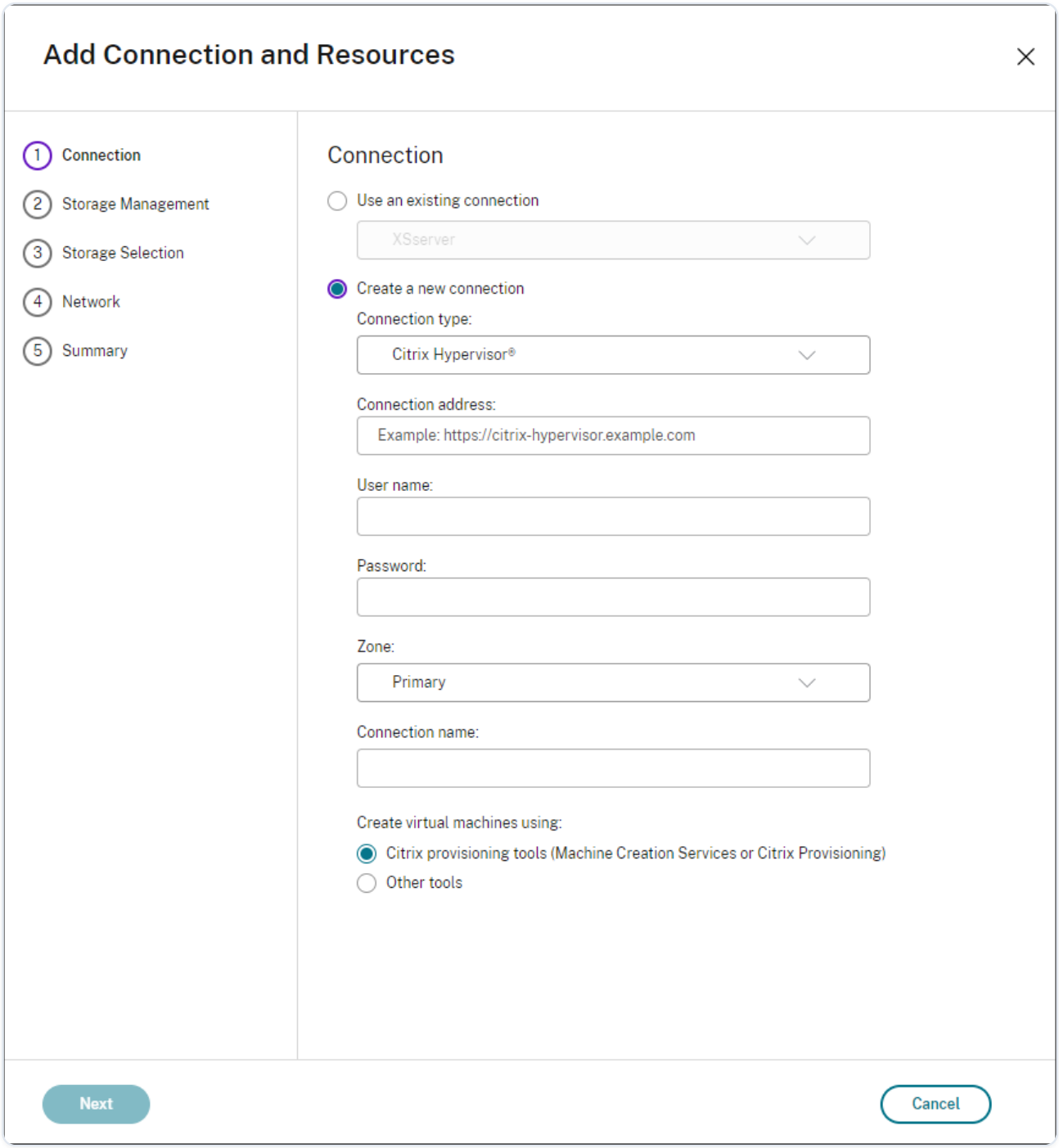
サイトを作成する際に、最初の接続をオプションで作成できます。サイト作成ウィザードには、以下のセクションで説明されている接続関連のページが含まれています。

サイトの作成後に接続を作成する場合は、手順1から開始します。

> **重要:**
>
> 接続を作成する前に、ホストリソース（ストレージとネットワーク）が利用可能である必要があります。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. アクションバーで**接続とリソースの追加**を選択します。
4. ウィザードは以下のページに沿って案内します（特定のページ内容は選択した接続タイプによって異なります）。各ページを完了したら、**概要**ページに到達するまで**次へ**をクリックします。

接続



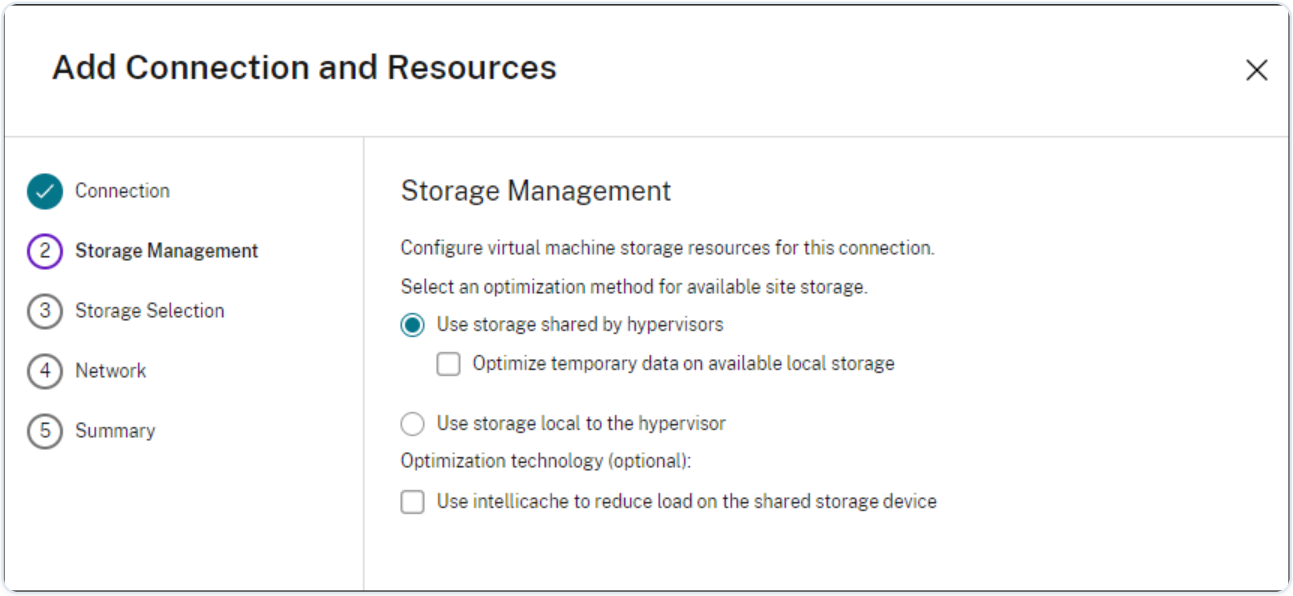
接続ページで：

- 接続を作成するには、**新しい接続の作成**を選択します。既存の接続と同じホスト構成に基づいて接続を作成するには、**既存の接続を使用**を選択し、関連する接続を選択します。
- **接続タイプ**フィールドで、使用しているハイパーバイザーを選択します。パブリッククラウドホスト接続は、ハイブリッドライツライセンスを使用している場合にのみドロップダウンリストに表示されます。または、PowerShellコマンド `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/true を使用して、以下を取得できます。

  - サードパーティ製プラグインを含む、Citrixがサポートするすべてのハイパーバイザープラグインのリスト。
  - ハイパーバイザープラグインの可用性。可用性ステータスが**false**の場合、ハイパーバイザープラグインが正しくインストールされていないか、ハイブリッドライツライセンスの資格がないことが考えられます。

- 接続アドレスと資格情報フィールドは、選択した接続タイプによって異なります。要求された情報を入力してください。
- 接続名を入力します。この名前はWeb Studioに表示されます。
- 仮想マシンの作成に使用するツールを選択します: Web Studioツール (Machine Creation Services™ や Citrix Provisioning など) またはその他のツール。

ストレージ管理



ストレージ管理の種類と方法については、「ホストストレージ」を参照してください。

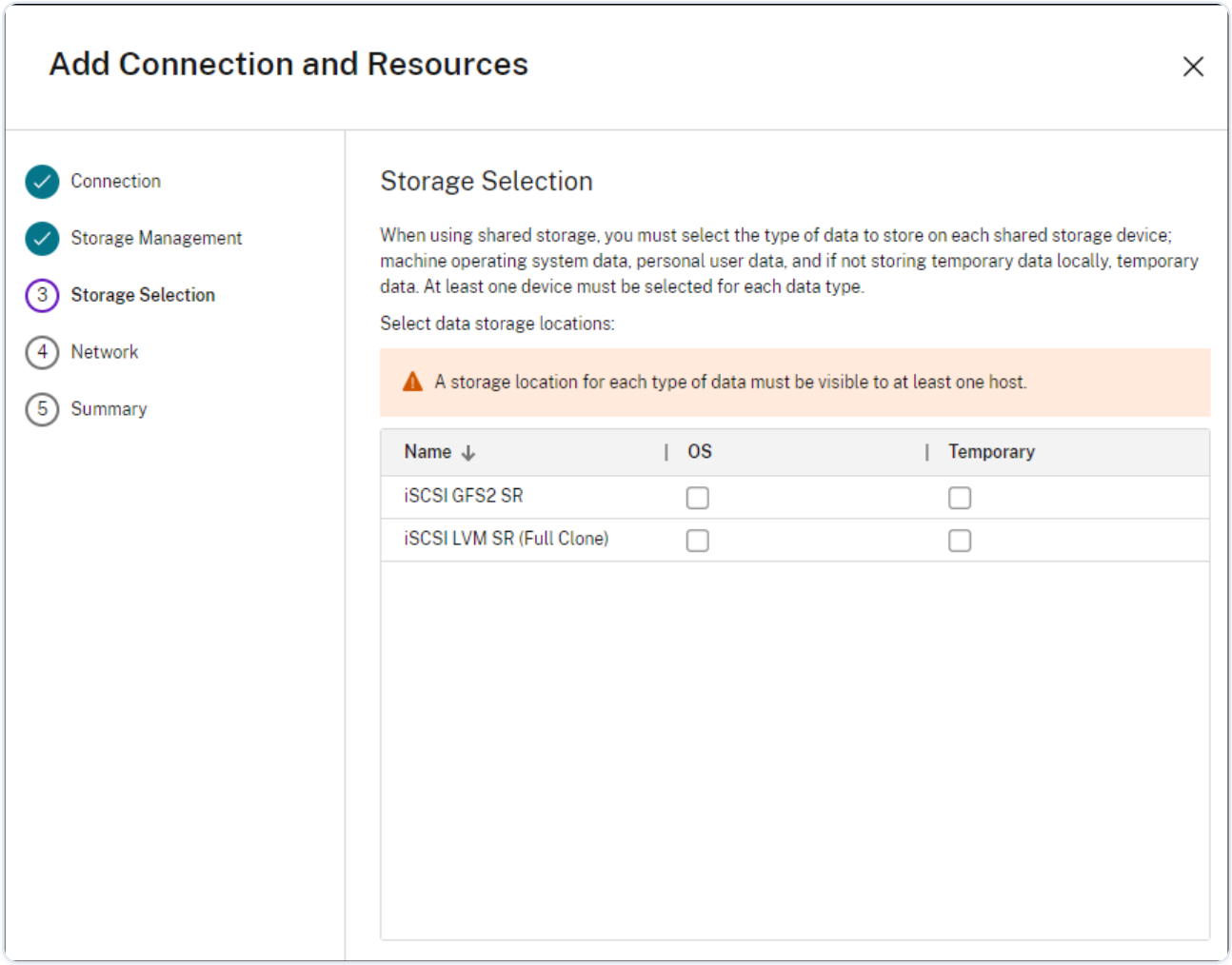
Hyper-VまたはVMwareホストへの接続を構成する場合は、クラスター名を参照して選択します。その他の接続タイプでは、クラスター名は要求されません。

ストレージ管理方法を選択します。ハイパーバイザーによって共有されるストレージ、またはハイパーバイザーにローカルなストレージ。

- ハイパーバイザーで共有されるストレージを選択した場合、利用可能なローカルストレージに一時データを保持するかどうかを指定します。(この接続を使用するマシンカタログで、デフォルト以外のサイズの一時ストレージを指定できます。) **例外:** クラスター共有ボリューム (CSV) を使用する場合、Microsoft System Center Virtual Machine Manager はローカルストレージ上の一時データキャッシュディスクを許可しません。Web Studio でそのストレージ管理設定を構成すると失敗します。

XenServerプールで共有ストレージを使用している場合、共有ストレージデバイスへの負荷を軽減するためにIntelliCacheを使用するかどうかを指定します。「XenServer接続にIntelliCacheを使用する」を参照してください。

ストレージの選択



ストレージの選択の詳細については、「ホストストレージ」を参照してください。

利用可能なデータタイプごとに、少なくとも1つのホストストレージデバイスを選択します。前のページで選択したストレージ管理方法によって、このページで選択できるデータタイプが決まります。ウィザードの次のページに進む前に、サポートされているデータタイプごとに少なくとも1つのストレージデバイスを選択してください。

ストレージの選択ページの「下部」には、ハイパーバイザー間で共有されるストレージを選択し、前のページで**利用可能なローカルストレージで一時データを最適化する**を有効にした場合に、追加の構成オプションが含まれています。一時データに使用するローカルストレージデバイスを選択できます。

現在選択されているストレージデバイスの数が表示されます (上記のグラフィックでは「1 storage device selected」)。そのエントリにカーソルを合わせると、選択されているデバイス名が表示されます。

1. 使用するストレージデバイスを変更するには、**選択**をクリックします。
2. **ストレージの選択**ダイアログボックスで、ストレージデバイスのチェックボックスをオンまたはオフにしてから、**OK**をクリックします。

ネットワーク

ネットワークページで、リソースの名前を入力します。この名前は、Web Studioに表示され、接続に関連付けられているストレージとネットワークの組み合わせを識別します。

VMが使用するネットワークを1つ以上選択します。

概要

概要ページで、選択内容を確認します。完了したら、**完了**をクリックします。

注意: 一時データをローカルに保存すると、この接続を使用するマシンを含むマシンカタログを作成するときに、一時データストレージの非デフォルト値を構成できます。「マシンカタログの作成」を参照してください。

接続設定の編集

この手順を使用して接続の名前を変更したり、接続を作成したりしないでください。それらの接続は異なる操作です。現在ホストしているマシンに新しいアドレスがある場合にのみ、アドレスを変更してください。別のアドレスを別のマシンに入力すると、接続のマシンカタログが破損します。

このリソースにアクセスするマシンカタログは、適切なGPU固有のマスターイメージを使用する必要があるため、接続の**GPU**設定を変更することはできません。接続を作成してください。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**接続の編集**を選択します。
4. 接続を編集するときに利用できる設定のガイダンスに従ってください。
5. 完了したら、**適用**をクリックして変更を適用し、ウィンドウを開いたままにするか、**保存**をクリックして変更を適用し、ウィンドウを閉じます。

接続プロパティページ:

- 接続アドレスと資格情報を変更するには、**設定の編集...**を選択し、新しい情報を入力します。
- XenServer接続の高可用性サーバーを指定するには、**サーバーの編集...**を選択し、サーバーを選択します。Citrixでは、プールマスターが失敗した場合にXenServerとの通信を可能にするために、プール内のすべてのサーバーを選択することをお勧めします。

> **注:**
>
> HTTPSを使用しており、高可用性サーバーを構成したい場合は、プール内のすべてのサーバーにワイルドカード証明書をインストールしないでください。各サーバーには個別の証明書が必要です。

詳細ページ:

- Remote PC Accessで使用されるMicrosoft System Center Configuration Manager (ConfMgr) Wake on LAN接続タイプの場合、**ConfMgr Wake Proxy**、マジックパケット、およびパケット送信情報を入力します。
- スロットリングしきい値設定を使用すると、接続で許可される電源アクションの最大数を指定できます。これらの設定は、電源管理設定によって同時に起動するマシンの数が多すぎたり少なすぎたりする場合に役立ちます。各接続タイプには、ほとんどの場合に適した特定のデフォルト値があり、変更してはなりません。
- **同時アクション（すべてのタイプ）**設定では、この接続で同時に発生できる最大絶対数と、この接続を使用するすべてのマシンの最大パーセンテージという2つの値を指定します。絶対値とパーセンテージ値の両方を指定する必要があります。実際に適用される制限は、これらの値のうち小さい方です。

  たとえば、34台のマシンがある展開で、**同時アクション（すべてのタイプ）**が絶対値10、パーセンテージ値10に設定されている場合、実際に適用される制限は3です（つまり、34の10パーセントを最も近い整数に丸めたもので、絶対値10台のマシンよりも小さい値です）。
- **1分あたりの最大新規アクション数**は絶対数です。パーセンテージ値はありません。
- **接続オプション**フィールドには、Citrixサポート担当者の指示または明示的なドキュメントの指示がある場合にのみ情報を入力してください。

共有テナントページ:

この接続のサブスクリプションとAzure Compute Galleryを共有するテナントとサブスクリプションを追加します。これにより、カタログを作成または更新する際に、それらのテナントとサブスクリプションから共有イメージを選択できます。

- この接続に関連付けられているアプリケーションの**アプリケーションID**と**アプリケーションシークレット**を入力します。この情報を使用して、Azureに認証できます。セキュリティを確保するため、定期的にキーを変更することをお勧めします。
- 共有テナントとサブスクリプションを指定します。共有テナントは最大8つ追加できます。各テナントにつき、最大8つのサブスクリプションを追加できます。
- 完了したら、**保存**と**適用**をクリックします。

接続オプションフィールドに情報を入力するのは、Citrixサポート担当者の指示がある場合に限ります。

ネットワークの編集

接続のネットワークを変更できます。次の手順を実行します。

1. に移動します。
2. 接続の下にあるターゲットリソースを選択し、アクションバーで を選択します。
3. 仮想マシンが使用するネットワークを1つ以上選択します。
4. 変更を保存して終了するには、**保存**をクリックします。

接続のメンテナンスモードをオンまたはオフにする

接続のメンテナンスモードをオンにすると、その接続に格納されているマシンに新しい電源操作が影響するのを防ぎます。メンテナンスモードのマシンにはユーザーは接続できません。ユーザーがすでに接続している場合、メンテナンスモードはログオフ時に有効になります。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択します。メンテナンスモードをオンにするには、アクションバーで**Turn On Maintenance Mode**を選択します。メンテナンスモードをオフにするには、**Turn Off Maintenance Mode**を選択します。

個々のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。また、マシンカタログまたはデリバリーグループ内のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。

接続を削除する

接続を削除すると、多数のマシンが削除され、データが失われる可能性があります。影響を受けるマシン上のユーザーデータがバックアップされているか、不要になっていることを確認してください。

接続を削除する前に、以下を確認してください。

- すべてのユーザーが接続に保存されているマシンからログオフしていること。
- 切断されたユーザーセッションが実行されていないこと。
- プールされたマシンと専用マシンのメンテナンスモードがオンになっていること。
- 接続で使用されているマシンカタログ内のすべてのマシンは電源がオフになります。

カタログによって参照されている接続を削除すると、マシンカタログは使用できなくなります。この接続がカタログによって参照されている場合、カタログを削除するオプションがあります。カタログを削除する前に、他の接続で使用されていないことを確認してください。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**接続の削除**を選択します。
4. この接続にマシンが保存されている場合、マシンを削除するかどうかを尋ねられます。削除する場合は、関連するActive Directoryコンピューターアカウントをどうするかを指定します。

接続の名前を変更またはテストする

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで または を選択します。

接続上のマシンの詳細を表示する

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**マシンの表示**を選択します。

上部のペインには、接続を介してアクセスされるマシンが一覧表示されます。マシンを選択すると、下部のペインにその詳細が表示されます。開いているセッションのセッション詳細も提供されます。

検索機能を使用して、マシンをすばやく見つけます。ウィンドウ上部のリストから保存された検索を選択するか、新しい検索を作成します。マシン名の全部または一部を入力して検索するか、高度な検索に使用する式を作成できます。式を作成するには、 をクリックし、プロパティと演算子のリストから選択します。

接続上のマシンを管理する

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、 ペインで を選択します。
4. アクションバーで次のいずれかを選択します。一部のアクションは、マシンの状態と接続ホストの種類によっては利用できません。

アクション	説明
起動	マシンが電源オフまたは一時停止状態の場合に起動します。
一時停止	マシンをシャットダウンせずに一時停止し、マシンリストを更新します。
シャットダウン	オペレーティングシステムにシャットダウンを要求します。
強制シャットダウン	マシンを強制的に電源オフにし、マシンリストを更新します。
再起動	オペレーティングシステムにシャットダウンを要求し、その後マシンを再起動します。オペレーティングシステムがこれに応じられない場合、デスクトップは現在の状態のままになります。
メンテナンスモードを有効にする	マシンへの接続を一時的に停止します。この状態では、ユーザーはマシンに接続できません。ユーザーが接続している場合、ログオフ時にメンテナンスモードが有効になります。(上記の説明のとおり、接続を介してアクセスされるすべてのマシンに対してメンテナンスモードをオンまたはオフにすることもできます。)

アクション	説明
デリバリーグループから削除	マシンをデリバリーグループから削除しても、デリバリーグループが使用するマシンカタログからは削除されません。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。
削除	マシンを削除すると、ユーザーはそのマシンにアクセスできなくなり、マシンはマシンカタログから削除されます。マシンを削除する前に、すべてのユーザーデータがバックアップされているか、不要であることを確認してください。マシンは、どのユーザーも接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが接続できないように、メンテナンスモードをオンにしてください。

マシンのシャットダウンを伴う操作の場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsが更新プログラムのインストールを試みると、更新が完了する前にマシンの電源がオフになるリスクがあります。

ストレージの編集

接続を使用するVMのオペレーティングシステムデータと一時データを保存するために使用されるサーバーのステータスを表示できます。また、各データタイプのストレージにどのサーバーを使用するかを指定することもできます。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**ストレージの編集**を選択します。
4. 左ペインで、データタイプ（オペレーティングシステムまたは一時）を選択します。
5. 選択したデータタイプに対して、1つ以上のストレージデバイスのチェックボックスをオンまたはオフにします。
6. **OK**をクリックします。

リスト内の各ストレージデバイスには、その名前とストレージステータスが含まれています。有効なストレージステータスの値は次のとおりです。

- **使用中:** ストレージはマシンの作成に使用されています。
- **置き換え済み:** ストレージは既存のマシンにのみ使用されています。このストレージには新しいマシンは追加されません。
- **未使用:** ストレージはマシンの作成に使用されていません。

現在**使用中**のデバイスのチェックボックスをオフにすると、そのステータスは**置き換え済み**に変わります。既存のマシンはそのストレージデバイスを引き続き使用し（データを書き込むこともできます）、そのため、マシンの作成に使用されなくなった後でも、その場所がいっぱいになる可能性があります。

リソースの削除、名前の変更、またはテスト

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. リソースを選択し、アクションバーで適切なエントリ（**リソースの削除**、**リソースの名前変更**、または**リソースのテスト**）を選択します。

孤立したAzureリソースの検出

孤立したリソースは、システム内に存在する使用されていないリソースであり、不要な費用につながる可能性があります。

この機能を使用すると、Citrix Virtual Apps and Desktopsサイトのホストにある孤立したAzureリソースを検出できます。

Web Studioで次の手順を実行します。

1. 「**管理**」から、左ペインで「**ホスティング**」を選択します。
2. 接続を選択し、アクションバーで「**孤立したリソースの検出**」を選択します。「**孤立したリソースの検出**」ダイアログボックスには、孤立したリソースのレポートが表示されます。
3. 孤立したリソースのレポートを表示するには、「**レポートの表示**」を選択します。

または、PowerShellを使用して孤立したAzureリソースを検出することもできます。詳細については、「孤立したリソースのリストを取得する」を参照してください。

孤立したリソースの原因を理解し、さらに進める方法については、「Citrixで孤立したAzureリソースを効率的に管理する」を参照してください。

接続タイマー

ポリシー設定を使用して、3つの接続タイマーを構成できます。

- **最大接続タイマー:** ユーザーデバイスと仮想デスクトップ間の途切れない接続の最大期間を決定します。**セッション接続タイマー**および**セッション接続タイマー間隔**のポリシー設定を使用します。
- **接続アイドルタイマー:** ユーザーからの入力がない場合に、仮想デスクトップへの途切れないユーザーデバイス接続が維持される期間を決定します。**セッションアイドルタイマー**および**セッションアイドルタイマー間隔**のポリシー設定を使用します。
- **切断タイマー:** 切断されロックされた仮想デスクトップが、セッションがログオフされるまでロックされたままになる期間を決定します。**切断セッションタイマー**および**切断セッションタイマー間隔**のポリシー設定を使用します。

これらの設定のいずれかを更新する場合は、展開全体で一貫性があることを確認してください。

詳細については、ポリシー設定のドキュメントを参照してください。

孤立したリソースのリストを取得する

MCSによって作成されたものの、MCSによって追跡されなくなった孤立したリソースのリストを取得できます。これは現在、Azure環境に適用されます。リストを取得するには、PowerShellコマンドを使用できます。接続を使用してフィルター処理できます。

> **注:**
>
> - プロビジョニングまたはイメージの更新が進行中の場合、PowerShell コマンドは拒否されます。
> - すべてのCitrixタグが付けられた顧客管理リソースは、孤立リソースとして検出されます。ただし、そのリソースに値がtrueのCitrixDetectIgnoreという別のタグを追加すると、孤立リソースの検出中にそのリソースは無視されます。

制限事項

- 組み込みのフル管理者またはクラウド管理者ロールの管理者ユーザーのみが、PowerShellコマンドを実行して孤立リソースのリストを取得できます。
- 孤立したリソースの誤認識を避けるため、孤立したリソースをフィルタリングしている間はVMの電源を入れないでください。
- 負荷が高い可能性がある場合、約2,000件のレコードが孤立として表示されます。

孤立リソースのリストを表示するには：

1. **PowerShell**ウィンドウを開きます。
2. 次のコマンドを実行します。

    a. 接続 uid を取得します。接続 uid は、HypervisorConnectionUid 属性の値です。

    ```
    Get-ChildItem xdhyp:\connections | where { $_.PluginId -like
    'Azure*' }"
    ```

    b. 孤立したリソースのリストを取得します。

    ```
    get-provorphanedresource -HypervisorConnectionUid <connection uid>
    ```

サブスクリプション ID から孤立したリソースのリストを表示するには:

1. **PowerShell**ウィンドウを開きます。
2. 次のコマンドを実行します。

    a. サブスクリプション ID を使用して接続 uid を見つけます。接続 uid は、HypervisorConnectionUid 属性の値です。

    ```
    Get-ChildItem xdhyp:\connections | where { $_.CustomProperties
    -match '<subscriptionId>' }
    ```

    b. 孤立したリソースのリストを取得します:

    ```
    get-provorphanedresource -HypervisorConnectionUid <connection uid>
    ```

注:

削除する前にリソースを慎重に確認してください。

次のステップ

特定のホストタイプへの接続については、以下を参照してください:

- AWS への接続
- XenServer への接続

- Google Cloud環境への接続
- Microsoft Azureへの接続
- マイクロソフト システムセンター バーチャルマシンマネージャー への接続
- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- VMwareへの接続
- VMwareクラウドおよびパートナーソリューションへの接続

初期展開プロセス中の場合は、マシンカタログを作成します。

AWSへの接続

(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections.html)では、接続を作成するウィザードについて説明します。以下の情報では、AWSクラウド環境に固有の詳細について説明します。

> **注:**
>
> AWSへの接続を作成する前に、まずAWSアカウントをリソースの場所として設定を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare/aws.html)を参照してください。

接続を作成する

Web Studioから接続を作成する場合：

- APIキーとシークレットキーの値を指定する必要があります。これらの値を含むキーファイルをAWSからエクスポートし、インポートできます。また、リージョン、アベイラビリティゾーン、VPC名、サブネットアドレス、ドメイン名、セキュリティグループ名、および資格情報も指定する必要があります。
- ルートAWSアカウントの資格情報ファイル（AWSコンソールから取得）は、標準のAWSユーザー向けにダウンロードされた資格情報ファイルと同じ形式ではありません。そのため、Citrix Virtual Apps and Desktops™管理では、このファイルを使用してAPIキーとシークレットキーのフィールドに入力することはできません。AWS Identity Access Management (IAM) の資格情報ファイルを使用していることを確認してください。

> **注:**

> 接続を作成した後、APIキーとシークレットキーの更新が失敗する場合があります。この問題を解決するには、プロキシサーバーまたはファイアウォールの制限を確認し、次のアドレスにアクセスできることを確認してください: `https://*.amazonaws.com`。

ホスト接続のデフォルト値

AWSクラウド環境でホスト接続を作成すると、次のデフォルト値が表示されます。

オプション	絶対値	パーセンテージ
同時実行アクション（全タイプ）	125	100
1分あたりの新規アクションの最大数	125	

MCS は、デフォルトで最大 100 の同時プロビジョニング操作をサポートしています。

サービスエンドポイントURL

標準ゾーンサービスエンドポイントURL

MCSを使用すると、APIキーとAPIシークレットを使用して新しいAWS接続が追加されます。この情報と認証済みアカウントを使用して、MCSはAWS DescribeRegions EC2 API呼び出しを使用して、サポートされているゾーンについてAWSにクエリを実行します。クエリは汎用EC2サービスエンドポイントURL `https://ec2.amazonaws.com/` を使用して行われます。MCSを使用して、サポートされているゾーンのリストから接続するゾーンを選択します。優先されるAWSサービスエンドポイントURLは、そのゾーンに対して自動的に選択されます。ただし、サービスエンドポイントURLを作成した後は、そのURLを設定または変更することはできません。

IAM権限を定義する

このセクションの情報を使用して、AWS上のCitrix Virtual Apps and DesktopsのIAM権限を定義します。AmazonのIAMサービスでは、複数のユーザーを持つアカウントが許可されており、それらのユーザーはさらにグループに編成できます。これらのユーザーは、アカウントに関連する操作を実行する能力を制御するために、異なる権限を持つことができます。IAM権限の詳細については、IAM JSON policy reference を参照してください。

IAM権限ポリシーを新しいユーザーグループに適用するには：

1. AWSマネジメントコンソールにログインし、ドロップダウンリストから **IAMサービス** を選択します。
2. **新しいユーザーグループの作成** を選択します。
3. 新しいユーザーグループの名前を入力し、**続行** を選択します。
4. 「**Permissions**」ページで、「**Custom Policy**」を選択します。「**Select**」を選択します。
5. 「**Permissions policy**」の名前を入力します。
6. 「**Policy Document**」セクションで、関連する権限を入力します。

ポリシー情報を入力したら、**Continue**を選択してユーザーグループを完了します。グループ内のユーザーには、Citrix Virtual Apps and Desktopsに必要なアクションのみを実行する権限が付与されます。

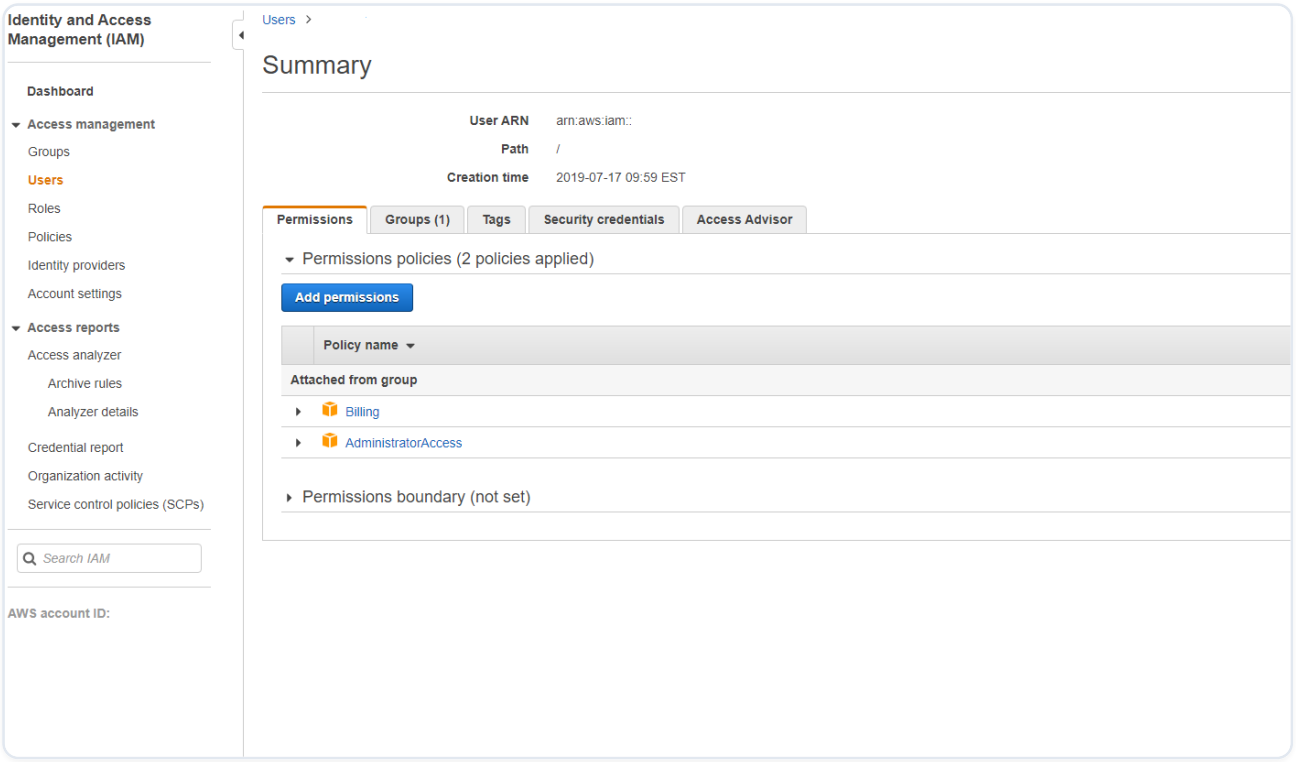
> **重要:**

> 前の例で提供されているポリシーテキストを使用して、Citrix Virtual Apps and DesktopsがAWSアカウント内でアクションを実行するために使用するアクションを、特定のリソースに制限することなくリストします。Citrixは、テスト目的でこの例を使用することをお勧めします。本番環境では、リソースにさらなる制限を追加することを選択できます。

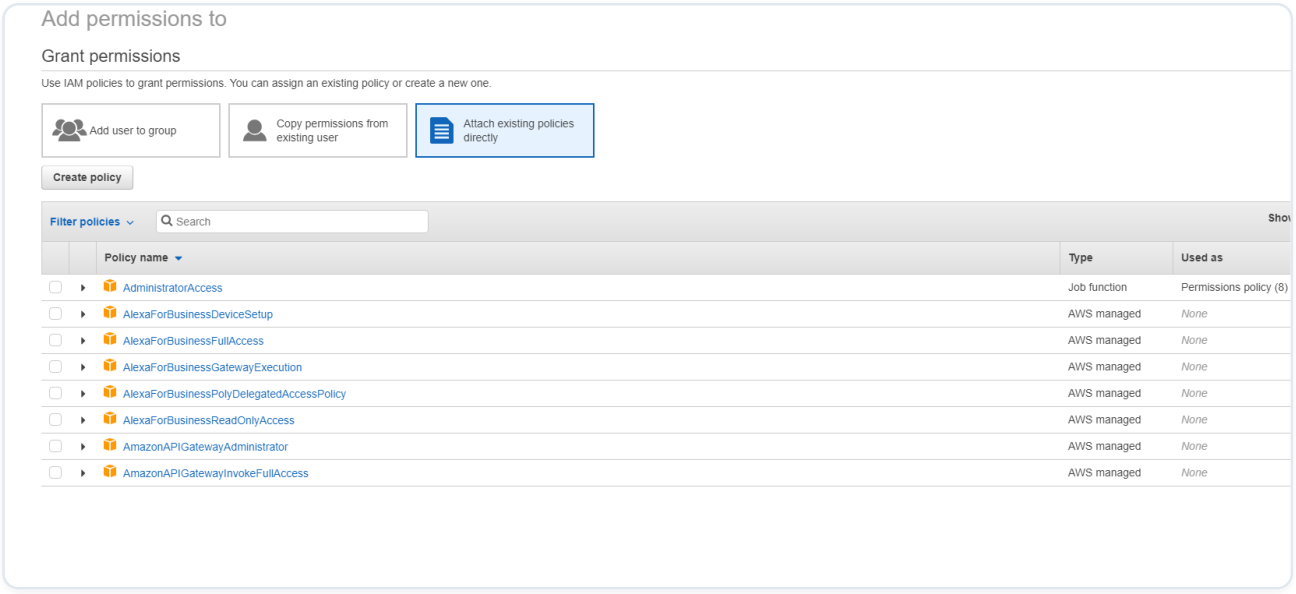
IAM権限を設定する

AWSマネジメントコンソールの**IAM**セクションで権限を設定します。

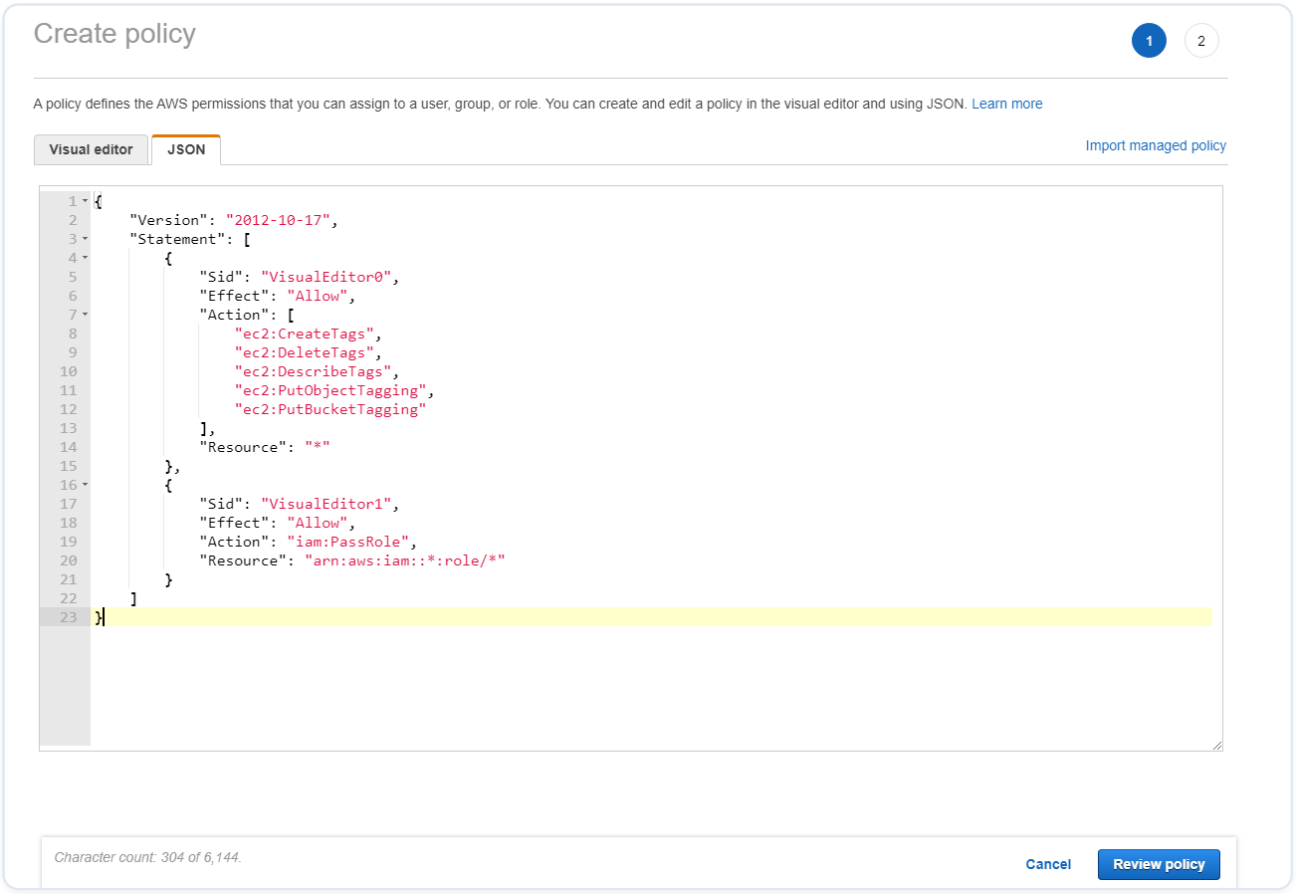
1. **概要**パネルで、**アクセス許可**タブを選択します。
2. **アクセス許可の追加**を選択します。



アクセス許可の追加先画面で、アクセス許可を付与します。



「**JSON**」タブで、以下を例として使用します。



ヒント:

記載されているJSONの例には、お使いの環境に必要なすべての権限が含まれていない場合があります。詳細については、「AWS で Citrix Virtual Apps and Desktops を実行するための ID およびアクセス管理権限を定義する方法」を参照してください。

必要なAWS権限

このセクションには、AWS権限の完全なリストが含まれています。

注:

iam:PassRole 権限は、**role_based_auth** にのみ必要です。

ホスト接続の作成

AWSからの情報を使用して、新しいホスト接続が追加されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeLaunchTemplates"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

VM の電源管理

マシンインスタンスの電源がオンまたはオフになります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DetachVolume",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstanceStatus"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

仮想マシンの作成、更新、または削除

AWSインスタンスとしてプロビジョニングされたVMを使用して、マシンカタログが作成、更新、または削除されます。

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:AttachVolume",

                "ec2:AssociateIamInstanceProfile",

                "ec2:AuthorizeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateSecurityGroup",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteVolume",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",
```

```
                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",

                "ec2:RunInstances",

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:TerminateInstances"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
```

```
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

注:

セキュリティグループに関連するEC2セクションは、カタログ作成時に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。

ディスクの直接アップロードとダウンロード

ダイレクトディスクアップロードにより、マシンカタログプロビジョニングにおけるボリュームワーカーの要件が不要になり、代わりにAWSが提供するパブリックAPIが使用されます。この機能により、追加のストレージアカウントに関連するコストと、ボリュームワーカー操作を維持するための複雑さが軽減されます。

注:

ボリュームワーカーのサポートは非推奨になりました。

以下の権限をポリシーに追加する必要があります。

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

重要:

- ボリュームワーカーAMIやボリュームワーカーVMなどのボリュームワーカー操作なしで、既存のマシンカタログにVMを追加できます。
- 既存のカタログで以前にボリュームワーカーを使用していた場合、ボリュームワーカー関連を含むすべてのアーティファクトが削除されます。

作成されたボリュームのEBS暗号化

AMIが暗号化されている場合、またはEBSがすべての新しいボリュームを暗号化するように構成されている場合、EBSは新しく作成されたボリュームを自動的に暗号化できます。ただし、この機能を実装するには、以下の権限をIAMポリシーに含める必要があります。

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
```

```
    ]

}
```

注:

ユーザーの判断により、リソースと条件ブロックを含めることで、権限を特定のキーに限定できます。例：**条件付きKMS権限**：

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"
```

```
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

以下のキーポリシーステートメントは、KMSキーに対するすべてのアクション (kms:*) の権限をIAMポリシーを使用してアカウントが委任できるようにするために必要な、KMSキーのデフォルトのキーポリシー全体です。

```
{
"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::111122223333:root"
},
"Action": "kms:",
"Resource": ""
}
```

詳細については、AWS Key Management Service 公式ドキュメントを参照してください。

IAMロールベース認証

ロールベース認証をサポートするために、以下の権限が追加されます。

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

最小限のIAM権限ポリシー

以下のJSONは、現在サポートされているすべての機能に使用できます。このポリシーを使用して、ホスト接続の作成、VMの作成、更新、削除、および電源管理を行うことができます。 このポリシーは、IAM権限の定義セクションで説明されているようにユーザーに適用することも、**role_based_auth**セキュリティキーとシークレットキーを使用してロールベース認証を使用することもできます。

> **重要:**
>
> **role_based_auth**を使用するには、まずサイト内のすべてのDelivery Controllerで目的のIAMロールを構成します。Web Studioを使用して、ホスティング接続を追加し、認証キーとシークレットにrole_based_authを指定します。これらの設定を持つホスティング接続は、ロールベース認証を使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
```

```
                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",
```

```
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
```

```
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }
```

```
    ]

}
```

注:

- SecurityGroupsに関連するEC2セクションは、カタログ作成中に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。
- KMSセクションは、EBSボリューム暗号化を使用する場合にのみ必要です。
- iam:PassRole権限セクションは、**role_based_auth**の場合にのみ必要です。
- 要件と環境に基づいて、フルアクセスではなく特定のリソースレベルの権限を追加できます。詳細については、AWSドキュメントのDemystifying EC2 Resource-Level PermissionsとAccess management for AWS resourcesを参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- AWS固有の情報については、AWSカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

XenServer®への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱っています。

注：

XenServerへの接続を作成する前に、まず、リソースの場所としてXenServerアカウントの設定を完了する必要があります。XenServer仮想化環境を参照してください。

XenServerへの接続を作成する

XenServer（旧Citrix Hypervisor™）への接続を作成する場合、VM Power Admin以上のレベルのユーザーの資格情報を提供する必要があります。

Citrixでは、XenServerとの通信を保護するためにHTTPSを使用することを推奨しています。HTTPSを使用するには、XenServerにインストールされているデフォルトの SSL証明書を置き換える必要があります。

XenServerサーバーで高可用性が有効になっている場合、それを構成できます。Citrix Virtual Apps and Desktopsのバージョン2507 LTSRより前のバージョンでは、プール内のすべてのサーバーにワイルドカード証明書をインストールすることはできません。各サーバーに個別の証明書が必要です。

XenServerがvGPUをサポートしている場合、GPUの種類とグループを選択するか、パススルーすることができます。選択に専用のGPUリソースがあるかどうかは、表示で示されます。

1つ以上のXenServerホストで一時データストレージにローカルストレージを使用する場合、プール内の各ストレージの場所に一意の名前があることを確認してください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™（MCS）を使用して、以下をプロビジョニングできます。

- サポートされているデスクトップまたはサーバーOSのVM向けレガシーBIOS。
- セキュアブートを含む、サポートされているデスクトップまたはサーバーOSのVM向けUEFI。

> **注：**
>
> MCSを構成する際には、プールオペレーター権限以上が必要です。

XenServer接続にIntelliCache™を使用する

IntelliCacheを使用すると、共有ストレージとローカルストレージの組み合わせを使用できるため、ホスト型VDI展開の費用対効果が高まります。これにより、パフォーマンスが向上し、ネットワークトラフィックが削減されます。ローカルストレージは共有ストレージからマスターイメージをキャッシュするため、共有ストレージへの読み取り回数が減少します。共有デスクトップの場合、差分ディスクへの書き込みは、共有ストレージではなくホスト上のローカルストレージに書き込まれます。

- IntelliCacheを使用する場合、共有ストレージはNFSである必要があります。

- Citrixでは、可能な限り最速のデータ転送を確保するために、高性能なローカルストレージデバイスを使用することを推奨しています。

IntelliCacheを使用するには、この製品とXenServerの両方で有効にする必要があります。

- XenServerをインストールする際に、**Enable thin provisioning (Optimized storage for Virtual Desktops)** を選択します。Citrixは、IntelliCacheが有効なサーバーと無効なサーバーが混在するプールをサポートしていません。詳細については、XenServerのドキュメントを参照してください。
- Citrix Virtual Apps and Desktops™では、IntelliCacheはデフォルトで無効になっています。この設定はXenServer接続を作成するときにのみ変更でき、後でIntelliCacheを無効にすることはできません。XenServer接続を追加するときは、次の手順を実行します。
  - ストレージの種類として **Shared** を選択します。
  - **Use IntelliCache** チェックボックスをオンにします。

必要なXenServer権限

XenServerの権限はロールベース（RBAC）です。XenServerのロールベースアクセス制御（RBAC）機能を使用すると、ユーザー、ロール、および権限を割り当てて、XenServerへのアクセス権を持つユーザーと、それらのユーザーが実行できるアクションを制御できます。XenServer RBACシステムは、ユーザー（またはユーザーグループ）を定義されたロール（名前付きの権限セット）にマッピングします。ロールには、特定の操作を実行するための関連するXenServer権限があります。

詳細については、「ロールベースアクセス制御」を参照してください。

権限が増加する順序でのロール階層は、次のとおりです。Read-Only → VM Operator → VM Admin → VM Power Admin → Pool Operator → Pool Admin。

次のセクションでは、各プロビジョニングタスクに必要な最小ロールをまとめます。

ホスト接続の作成

タスク	必要な最小ロール
XenServerから取得した情報を使用してホスト接続を追加する	読み取り専用
ユーザーとその割り当てられた役割を表示する	読み取り専用

VMの電源管理

タスク	必要な最小限の役割
VMの電源をオンまたはオフにする	VMオペレーター

VMの作成、更新、または削除

タスク	必要な最小限の役割
既存のスナップショットスケジュールにVMを追加または削除する	VM 電源管理者
スナップショットスケジュールの追加、変更、削除	プールオペレーター
マスターイメージの公開	プールオペレーター（スイッチポートロックが必要）
マシンカタログの作成	プールオペレーター: スイッチポートロックが必要
VM の追加または削除 (GPU 対応 VM 以外)	VM 管理者
VM の追加または削除 (GPU 対応 VM)	プールオペレーター
仮想ディスクまたはCDデバイスの追加、削除、または構成	VM 管理者
タグの管理	VM オペレーター

RBACの役割と権限の詳細については、「RBACの役割と権限」を参照してください。

スイッチポートロックの詳細については、「スイッチポートロックの使用」を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html)を参照してください。
- XenServer固有の情報については、「XenServerカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-citrix-hypervisor.html)を参照してください。

詳細情報

- 「接続とリソース」(/ja-jp/citrix-virtual-apps-desktops/2311/manage-deployment/connections.html)
- 「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html)

Google Cloud環境への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、Google Cloud環境に固有の詳細を扱っています。

> **注:**
>
> Google Cloud環境への接続を作成する前に、まずGoogle Cloudアカウントをリソースの場所として設定する必要があります。Google Cloud環境を参照してください。

接続の追加

接続とリソースの作成のガイダンスに従ってください。以下の説明は、ホスティング接続の設定方法を案内します。

1. **管理 > 構成**から、左側のペインで**ホスティング**を選択します。
2. アクションバーで**「接続とリソースの追加」**を選択します。
3. **「接続」ページで、**「新しい接続の作成」と「Citrix provisioning™ tools」**を選択し、**「次へ」**を選択します。
   - **接続の種類**。メニューから**Google Cloud**を選択します。
   - **接続名**。接続の名前を入力します。
4. **地域**ページで、メニューからプロジェクト名を選択し、使用するリソースを含む地域を選択して、**次へ**を選択します。
5. **ネットワーク**ページで、リソースの名前を入力し、メニューから仮想ネットワークを選択し、サブネットを選択して、**次へ**を選択します。リソース名は、地域とネットワークの組み合わせを識別するのに役立ちます。名前に*(Shared)*サフィックスが付いている仮想ネットワークは、共有VPCを表します。共有VPCのサブネットレベルのIAMロールを構成した場合、共有VPCの特定のサブネットのみがサブネットリストに表示されます。

注:

- リソース名には1～64文字を含めることができ、空白のみ、または文字 `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )` を含めることはできません。

6. 「**概要**」ページで情報を確認し、「**完了**」を選択して「**接続とリソースの追加**」ウィンドウを終了します。

接続とリソースを作成すると、作成した接続とリソースが一覧表示されます。接続を構成するには、接続を選択し、アクションバーで該当するオプションを選択します。

同様に、接続の下に作成されたリソースを削除、名前変更、またはテストできます。これを行うには、接続の下のリソースを選択し、アクションバーで該当するオプションを選択します。

サービスエンドポイントURL

次のURLにアクセスできる必要があります。

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Google Cloudプロジェクト

Google Cloudプロジェクトには基本的に2種類あります。

- プロビジョニングプロジェクト：この場合、現在の管理者アカウントがプロジェクト内のプロビジョニングされたマシンを所有します。このプロジェクトはローカルプロジェクトとも呼ばれます。
- 共有VPCプロジェクト: プロビジョニングプロジェクトで作成されたマシンが、共有VPCプロジェクトのVPCを使用するプロジェクト。プロビジョニングプロジェクトに使用される管理者アカウントは、このプロジェクトで限られた権限、具体的にはVPCを使用する権限のみを持ちます。

GCP管理トラフィックのセキュアな環境を作成する

Google Cloudプロジェクトへのプライベートアクセスを許可できます。この実装により、機密データを処理するためのセキュリティが強化されます。これを実現するには、次のいずれかを実行できます。

- Cloud BuildサービスアカウントのVPCサービスコントロールの次のイングレスルールを含めます。この手順を実行する場合は、GCPマネージドトラフィックのセキュアな環境を作成するための以下の手順に従わないでください。

```
Ingress Rule 1

From:

Identities:

<ProjectID>@cloudbuild.gserviceaccount.com

Source > All sources allowed

To:

Projects =

All projects

Services =

Service name: All services
```

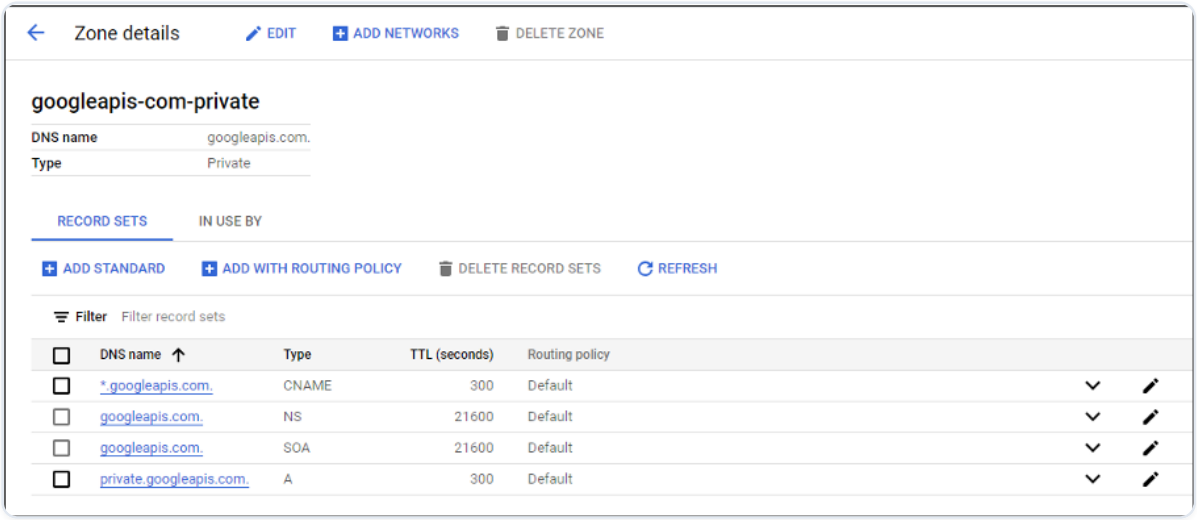
- プライベートワーカープールを使用している場合は、`CustomProperties`に`UsePrivateWorkerPool`を追加します。プライベートワーカープールについては、プライベートプール概要を参照してください。

GCPマネージドトラフィックのセキュアな環境を作成するための要件

GCPマネージドトラフィックのセキュアな環境を作成するための要件は次のとおりです。

- カスタムプロパティを更新する際は、ホスティング接続がメンテナンスモードになっていることを確認してください。
- プライベートワーカープールを使用するには、次の変更が必要です。
  - Citrix Cloud™サービスアカウントの場合、次のIAMロールを追加します。

    - Cloud Buildサービスアカウント
    - Compute Instance 管理者
    - サービスアカウントユーザー
    - サービスアカウントトークン作成者
    - Cloud Build WorkerPool オーナー
- ホスティング接続の作成に使用するのと同じプロジェクトにCitrix Cloudサービスアカウントを作成します。
- DNS構成で説明されているように、`private.googleapis.com`と`gcr.io`のDNSゾーンを設定します。



gcr.io の DNS ゾーン(/en-us/citrix-virtual-apps-desktops/2311/media/gcr-dns-zone.png)

- プライベートネットワークアドレス変換 (NAT) を設定するか、プライベートサービス接続を使用します。詳細については、「エンドポイントを介したGoogle APIへのアクセス」を参照してください。

  プライベートサービス接続(/en-us/citrix-virtual-apps-desktops/2311/media//private-service-connect.png)
- ピアリングされたVPCを使用している場合は、ピアリングされたVPCへのCloud DNSゾーンピアリングを作成します。詳細については、「ピアリングゾーンの作成」を参照してください。

  ピアリングゾーンの作成(/en-us/citrix-virtual-apps-desktops/2311/media/cloud-dns-zone-peering.png)
- VPCサービスコントロールで、APIとVMがインターネットと通信できるようにエグレスルールを設定します。イングレスルールはオプションです。例：

```
Egress Rule 1

From:

Identities:ANY_IDENTITY

To:

Projects =

All projects

Service =

Service name: All services
```

プライベートワーカープールを有効にする

プライベートワーカープールを有効にするには、ホスト接続でカスタムプロパティを次のように設定します。

1. Delivery Controller ホストから PowerShell ウィンドウを開くか、Remote PowerShell SDK を使用します。Remote PowerShell SDK の詳細については、「SDK と API」を参照してください。
2. 次のコマンドを実行します:
   a. `Add-PSSnapin citrix*`
   b. `cd XDHyp:\Connections\`
   c. `dir`
3. 接続から `CustomProperties` をメモ帳にコピーします。
4. プロパティ設定 `<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool" Value="True"/>` を追加します。例:

```
```

<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
Value="True"/>

```
</CustomProperties>

```
```

5. PowerShell ウィンドウで、変更されたカスタムプロパティに変数を割り当てます。例: `$customProperty = '<CustomProperties…</CustomProperties>'`.
6. `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"` を実行します。
7. `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"` を実行します。
8. `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force` を実行します。
9. 既存のホスト接続を更新するには、以下を実行します。

```
Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR CONNECTION NAME HERE>') -SecurePassword $securePassword -UserName $gcpServiceAccount -CustomProperties $customProperty
```

必要な GCP 権限

このセクションには、GCP 権限の完全なリストが含まれています。機能が正しく動作するように、このセクションに記載されている権限の完全なセットを使用してください。

注:

GCP は、Cloud Build Services のデフォルトの動作とサービスアカウントの使用方法について、April 29, 2024 以降に変更を導入します。詳細については、Cloud Build Service Account Change を参照してください。April 29, 2024 より前に Cloud Build API が有効になっている既存の Google プロジェクトは、この変更の影響を受けません。ただし、April 29 以降も既存の Cloud Build Service の動作を維持したい場合は、API を有効にする前に、制約の適用を無効にする組織ポリシーを作成または適用できます。新しい組織ポリシーを設定した場合でも、このセクションの既存の権限と、**Before Cloud Build Service Account Change** とマークされている項目に従うことができます。そうでない場合は、既存の権限と、**After Cloud Build Service Account Change** とマークされている項目に従ってください。
```

ホスト接続の作成

- プロビジョニングプロジェクトにおける Citrix Cloud サービスアカウントに必要な最小限の権限:

  ```
  compute.instanceTemplates.list

  compute.instances.list

  compute.networks.list

  compute.projects.get

  compute.regions.list

  compute.subnetworks.list

  compute.zones.list

  resourcemanager.projects.get
  ```

  以下の Google 定義ロールには、上記にリストされている権限があります。

  - Compute 管理者
  - クラウド データストア ユーザー

- 共有 VPC プロジェクト内の Citrix Cloud サービスアカウントの共有 VPC に必要な追加の権限:

  ```
  compute.networks.list

  compute.subnetworks.list

  resourcemanager.projects.get
  ```

  以下のGoogle定義のロールには、上記にリストされている権限があります:

  - Compute ネットワーク ユーザー

仮想マシンの電源管理

電源管理のみのカタログの場合に、プロビジョニングプロジェクト内のCitrix Cloudサービスアカウントに必要な最小限の権限:

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get

compute.zoneOperations.get
```

以下のGoogle定義のロールには、上記にリストされている権限があります:

- Compute管理者
- クラウド データストア ユーザー

仮想マシンの作成、更新、または削除

- プロビジョニングプロジェクト内のCitrix Cloudサービスアカウントに必要な最小限の権限:

```
cloudbuild.builds.create

cloudbuild.builds.get
```

```
cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly
```

```
compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get
```

```
compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get
```

```
storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

compute.networks.get

compute.resourcePolicies.use
```

以下のGoogle定義のロールには、上記にリストされている権限があります:

- Compute管理者
- Storage管理者
- Cloud Build編集者
- サービスアカウントユーザー
- クラウド データストア ユーザー

- 共有VPCプロジェクトのVPCとサブネットワークを使用してホスティングユニットを作成するために、共有VPCプロジェクト内のCitrix Cloudサービスアカウントに共有VPCで必要となる追加の権限:

```
compute.firewalls.list

compute.networks.list

compute.projects.get
```

```
compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list

resourcemanager.projects.get
```

以下に示すGoogle定義の役割には、上記の権限があります:

- コンピュート ネットワーク ユーザー
- クラウド データストア ユーザー

MCSに準備指示ディスクをダウンロードする際に必要な最小限の権限:

- (Cloud Buildサービスアカウント変更前): これらの権限をプロビジョニングプロジェクトのCloud Buildサービスアカウントに割り当てます。
- (Cloud Buildサービスアカウント変更後): これらの権限をプロビジョニングプロジェクトのCloud Computeサービスアカウントに割り当てます。

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list
```

```
compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.machineTypes.list

compute.networks.get

compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get
```

```
source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list
```

以下に示すGoogle定義の役割には、上記の権限があります:

- Cloud Buildサービスアカウント (Cloud Buildサービスアカウント変更後、Cloud Compute サービスアカウント)
- Compute Instance管理者
- サービスアカウントユーザー

- 準備指示ディスクをMCSにダウンロードする際にGoogle Cloud Buildサービスによって必要とされる、プロビジョニングプロジェクトのCloud Computeサービスアカウントに必要な最小限の権限:

```
resourcemanager.projects.get

storage.objects.create

storage.objects.get

storage.objects.list
```

以下に示すGoogle定義の役割には、上記の権限があります:

- コンピュートネットワークユーザー

- ストレージアカウントユーザー
- クラウド データストア ユーザー

MCSに準備指示ディスクをダウンロードする際のShared VPCに必要な追加の権限:

- (Cloud Buildサービスアカウントの変更前): これらの権限をプロビジョニングプロジェクトのCloud Buildサービスアカウントに割り当てます。
- (Cloud Buildサービスアカウントの変更後): これらの権限をプロビジョニングプロジェクトのCloud Computeサービスアカウントに割り当てます。

```
compute.firewalls.list

compute.networks.list

compute.subnetworks.list

compute.subnetworks.use

resourcemanager.projects.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります。

- コンピュート ネットワーク ユーザー
- ストレージアカウントユーザー
- クラウド データストア ユーザー

- プロビジョニングプロジェクトのCitrix Cloudサービスアカウントに対するCloud Key Management Service (KMS) に必要な追加の権限:

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります。

- Compute KMS閲覧者

一般的な権限

以下は、MCSでサポートされているすべての機能について、プロビジョニングプロジェクトのCitrix Cloudサービスアカウントに対する権限です。これらの権限は、今後の最高の互換性を提供します。

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create
```

```
compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags
```

```
compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice

compute.instances.updateSecurity

compute.instances.updateShieldedInstanceConfig

compute.instances.updateShieldedVmConfig

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels
```

```
compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get
```

```
cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp

iam.serviceAccounts.actAs

compute.resourcePolicies.use
```

次のステップ

- 初期展開プロセスを行っている場合は、マシンカタログの作成を参照してください。
- Google Cloud Platform (GCP) 固有の情報については、Google Cloud Platformカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

HPE Moonshot への接続 (プレビュー)

「接続とリソースの作成と管理」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections.html)では、接続を作成するウィザードについて説明しています。以下の情報は、HPE Moonshot に固有の詳細を扱っています。

注:

HPE Moonshot への接続を作成する前に、まず HPE アカウントの設定を完了する必要があります。「HPE Moonshot 仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare/hpe-moonshot.html)を参照してください。

接続を作成する

HPE Moonshot への接続は、以下を使用して作成できます。

- ウェブスタジオ
- PowerShell コマンド

Web Studio を使用して接続を作成する

1. **接続とリソースの追加**ページで、接続の種類として**HPE Moonshot**を選択します。
2. Moonshot iLO シャーシマネージャーの接続アドレスを入力します。アドレスには、IPアドレス、ホスト名、またはFQDNを使用できます。
3. シャーシの管理者資格情報と、わかりやすい接続名を入力します。

接続設定は、次のいずれかの状況で停止します。

- Citrix Virtual Apps and Desktops™ がエラーのある公開CA署名証明書を受信した場合：エラーメッセージが表示されます。画面の指示に従って問題を修正してください。そうしないと、接続の作成に進むことができません。
- Citrix Virtual Apps and Desktops がプライベートCA署名証明書を受信した場合：警告ページが表示されます。受信したサムプリントをサーバーの証明書の有効性と比較します。有効な場合は、**証明書を信頼する**を選択し、**OK**をクリックして接続の作成に進みます。Citrix Virtual Apps and Desktops はその証明書を信頼し、将来の検証のためにサムプリントを保存します。

PowerShellコマンドを使用して接続を作成する

PowerShellコマンドを使用して接続を作成する場合、次の情報を提供します。

- IP: HPEサーバーのIPアドレス
- ユーザー名: HPEユーザー名
- パスワード: HPEパスワード

例:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} -Path
@("XDHyp:\Connections\$connectionName") -Persist -PluginId
"HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
$UserName -sslthumbprint $SslThumbprint New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $HypervisorConnectionID
```

> **注:**
>
> `sslthumbprint`パラメーターは、プライベートCA署名付き証明書の場合にのみ必要です。

証明書とサムプリントの検証

HPE Moonshotへの接続を正常に作成するには、証明書にエラーがなく、サムプリントが正しい値である必要があります。以下は、証明書とサムプリントの検証に関連するユースケースです。

- パブリックCA署名付き証明書にエラーがあります。接続は正常に作成されません。エラーの詳細を確認し、問題を解決してください。
- エラーのないパブリックCA署名付き証明書。接続は正常に作成され、`SslThumbprints`の値は**Null**です。
- エラーがなく、`sslthumbprint`値を持つプライベートCA署名付き証明書。接続は正しい`SslThumbprints`値で正常に作成されます。
- 不正確なサムプリント値を持つプライベートCA署名付き証明書。接続は正常に作成されません。
- エラーのないプライベートCA署名付き証明書。接続は正常に作成されます。接続作成時、`SSlThumbprints`は**Null**です。`SSlThumbprints`値はサイトサービスによって値に更新されます。

接続の管理

このセクションでは、接続を管理する方法について詳しく説明します。

- Web Studioを使用して証明書の問題を修正する
- PowerShellコマンドを使用してサムプリント値を更新する

証明書の問題を修正する

証明書の問題が発生すると、Citrix Virtual Apps and DesktopsはHPE Moonshot接続をブロックし、関連するHPE Moonshotノードでのワークロードの配信と管理を妨げます。**ホスト接続**リストの接続の横にエラーアイコンが表示されます。特定の問題と解決策については、次の表を参照してください。

問題	解決策
公開 CA 署名証明書で証明書エラーが発生する	接続をクリックし、**トラブルシューティング**タブを選択し

問題	解決策
	ます。エラーの詳細を表示し、問題を解決します。
受信した証明書がプライベート CA 署名であるか、期限切れである。	ホスト接続を編集して証明書のサムプリントを更新します。詳細な手順 1. 接続を選択し、**接続の編集**をクリックします。 2. 「**Connection Properties**」ページで、「**Edit settings**」をクリックします。 3. HPE Moonshotシャーシに接続するためのパスワードを入力し、「**Save**」をクリックします。 4. 表示される「**Warning**」ページで、受信したサムプリントをサーバーのサムプリントと比較して、証明書の有効性を確認します。 5. 同じである場合は、「**Trust certificate**」を選択し、「**OK**」をクリックします。

サムプリント値の更新

接続を作成した後、`Set-Item` PowerShellコマンドを使用して接続のサムプリント値を更新できます。たとえば、次のコマンドを実行します。

1. 接続の接続詳細を取得します。例：

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. サムプリント値を更新します。例:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. 更新されたサムプリント値を確認します。例:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

注:

`Set-Item` コマンドで誤ったサムプリント値を指定すると、更新は失敗します。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- AWS固有の情報については、「HPE Moonshotマシンカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Microsoft Azure への接続

「接続とリソースの作成および管理」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections.html)では、接続を作成するウィザードについて説明しています。以下の情報は、Azure Resource Managerクラウド環境に固有の詳細を扱っています。

注:

Microsoft Azure への接続を作成する前に、リソースの場所として Azure アカウントの設定を完了する必要があります。「Microsoft Azure Resource Manager クラウド環境」を参照してください。

サービスプリンシパルと接続の作成

接続を作成する前に、接続がAzureリソースにアクセスするために使用するサービスプリンシパルを設定する必要があります。接続は2つの方法で作成できます。

- Web Studio を使用してサービスプリンシパルと接続を同時に作成する
- 以前に作成したサービスプリンシパルを使用して接続を作成する

このセクションでは、次のタスクを完了する方法を示します。

- 「Web Studioを使用してサービスプリンシパルと接続を作成する」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections/connection-azure-resource-manager.html#create-a-service-principal-and-connection-using-web-studio)
- 「PowerShellを使用してサービスプリンシパルを作成する」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections/connection-azure-resource-manager.html#create-a-service-principal-using-powershell)
- 「Azureでアプリケーションシークレットを取得する」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections/connection-azure-resource-manager.html#get-the-application-secret-in-azure)
- 「既存のサービスプリンシパルを使用して接続を作成する」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections/connection-azure-resource-manager.html#create-a-connection-using-an-existing-service-principal)

考慮事項

- Citrix® は、共同作成者ロールを持つサービスプリンシパルの使用を推奨しています。ただし、最小限の権限のリストについては、「最小限の権限」セクションを参照してください。
- 最初の接続を作成するとき、Azure は必要な権限を付与するよう求めます。今後の接続では、引き続き認証が必要ですが、Azure は以前の同意を記憶しており、プロンプトを再度表示することはありません。
- 認証に使用されるアカウントは、サブスクリプションの共同管理者である必要があります。
- 認証に使用されるアカウントは、サブスクリプションのディレクトリのメンバーである必要があります。注意すべきアカウントの種類は、「職場または学校」と「個人用 Microsoft アカウント」の2種類です。詳細については、CTX219211 を参照してください。
- 既存の Microsoft アカウントをサブスクリプションのディレクトリのメンバーとして追加して使用することはできますが、ユーザーが以前にディレクトリのリソースのいずれかへのゲストアクセスを許可されていた場合、問題が発生する可能性があります。この場合、ディレクトリ

内に必要な権限を付与しないプレースホルダーエントリが存在し、エラーが返される可能性があります。

これを修正するには、ディレクトリからリソースを削除し、明示的に再度追加します。ただし、このオプションは、アカウントがアクセスできる他のリソースに意図しない影響を与える可能性があるため、慎重に実行してください。

- 特定のアカウントが実際にはメンバーであるにもかかわらず、ディレクトリゲストとして検出される既知の問題があります。このような構成は、通常、古くから確立されたディレクトリアカウントで発生します。回避策：適切なメンバーシップ値を持つアカウントをディレクトリに追加します。
- リソースグループは単にリソースのコンテナであり、自身のリージョン以外のリージョンからのリソースを含むことができます。リソースグループのリージョンに表示されるリソースが利用可能であると期待している場合、これは混乱を招く可能性があります。
- 必要な数のマシンをホストするのに十分な大きさのネットワークとサブネットがあることを確認してください。これにはある程度の先見性が必要ですが、Microsoft はアドレス空間の容量に関するガイダンスを提供し、適切な値を指定するのに役立ちます。

Web Studio を使用してサービスプリンシパルと接続を作成する

> **重要:**
>
> この機能は、Azure China サブスクリプションではまだ利用できません。

> Web Studio を使用すると、単一のワークフローでサービスプリンシパルと接続の両方を作成できます。サービスプリンシパルは、接続に Azure リソースへのアクセスを許可します。サービスプリンシパルを作成するために Azure に認証すると、アプリケーションが Azure に登録されます。登録されたアプリケーションには、秘密鍵 (クライアントシークレットまたはアプリケーションシークレットと呼ばれます) が作成されます。登録されたアプリケーション (この場合は接続) は、クライアントシークレットを使用して Azure AD に認証します。

開始する前に、以下の前提条件を満たしていることを確認してください。

- サブスクリプションの Azure Active Directory テナントにユーザーアカウントがあること。
- Azure AD ユーザーアカウントが、リソースのプロビジョニングに使用する Azure サブスクリプションの共同管理者でもあること。

- 認証には、グローバル管理者、アプリケーション管理者、またはアプリケーション開発者の権限が必要です。これらの権限は、ホスト接続を作成した後に取り消すことができます。役割の詳細については、「Azure AD の組み込みロール」を参照してください。

サービスプリンシパルと接続を同時に作成するには、**接続とリソースの追加**ウィザードを使用します。

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンを作成するために使用するツールを選択し、**次へ**を選択します。
3. ページで、Azure サブスクリプション ID と接続の名前を入力します。サブスクリプション ID を入力すると、 ボタンが有効になります。

   > **注:**
   >
   > 接続名には1～64文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. を選択し、Azure Active Directory アカウントのユーザー名とパスワードを入力します。
5. **サインイン**を選択します。
6. **承認**を選択して、Citrix Virtual Apps and Desktops™に一覧表示された権限を付与します。Citrix Virtual Apps and Desktopsは、指定されたユーザーに代わってAzureリソースを管理できるサービスプリンシパルを作成します。
7. **承認**を選択すると、ウィザードの**接続**ページに戻ります。

   > **注:**
   >
   > Azure への認証が正常に完了すると、「**Create new**」ボタンと「**Use existing**」ボタンが消えます。「**Connection successful**」というテキストが緑色のチェックマークとともに表示され、Azure サブスクリプションへの接続が成功したことを示します。

8. 「**Connection Details**」ページで、「**Next**」を選択します。

   > **注:**

> Azure への認証が正常に完了し、必要な権限の付与に同意するまで、次のページに進むことはできません。

9. 接続のリソースを構成します。リソースには、リージョンとネットワークが含まれます。
   - **リージョン**ページで、リージョンを選択します。
   - **ネットワーク**ページで、以下を実行します。
     - リージョンとネットワークの組み合わせを識別するために、1〜64文字のリソース名を入力します。リソース名には、空白のみを含めることや、文字`\/;:#.*?=<>|[]{}"'()'`を含めることはできません。
     - 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名をリソースグループとペアにすることで、一意の組み合わせが提供されます。）前のページで選択したリージョンに仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがあるリージョンを選択してください。
10. **概要**ページで、設定の概要を確認し、**完了**を選択してセットアップを完了します。

アプリケーションIDを表示する

接続を作成した後、その接続がAzureリソースへのアクセスに使用するアプリケーションIDを表示できます。

接続とリソースの追加リストで、接続を選択して詳細を表示します。**詳細**タブにアプリケーションIDが表示されます。

PowerShellを使用してサービスプリンシパルを作成する

PowerShellを使用してサービスプリンシパルを作成するには、Azure Resource Managerサブスクリプションに接続し、以下のセクションで提供されているPowerShellコマンドレットを使用します。

以下の項目を準備してください。

- **SubscriptionId:** VDAをプロビジョニングするサブスクリプションのAzure Resource Manager `SubscriptionID`。
- **ActiveDirectoryID**: Azure ADに登録したアプリケーションのテナントID。
- **ApplicationName:** Azure ADで作成するアプリケーションの名前。

詳細な手順は次のとおりです。

Azure Resource Managerサブスクリプションに接続します。

```
`Connect-AzAccount`
```

1. サービスプリンシパルを作成するAzure Resource Managerサブスクリプションを選択します。

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription
   ```

2. ADテナントでアプリケーションを作成します。

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. サービスプリンシパルを作成します。

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. サービスプリンシパルにロールを割り当てます。

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. PowerShellコンソールの出力ウィンドウからApplicationIdをメモします。ホスト接続を作成する際に、そのIDを指定します。

Azureでアプリケーションシークレットを取得する

既存のサービスプリンシパルを使用して接続を作成するには、まずAzureポータルでサービスプリンシパルのアプリケーションIDとシークレットを取得する必要があります。

詳細な手順は次のとおりです。

1. Web StudioまたはPowerShellを使用して、**アプリケーションID**を取得します。
2. Azureポータルにサインインします。
3. Azure で、「**Azure Active Directory**」を選択します。
4. Azure AD の「**App registrations**」から、アプリケーションを選択します。
5. **証明書とシークレット**に移動します。
6. **クライアントシークレット**をクリックします。

既存のサービスプリンシパルを使用して接続を作成する

サービスプリンシパルが既にある場合は、それを使用してWeb Studioで接続を作成できます。

次の項目を準備してください。

- SubscriptionId
- ActiveDirectoryID (テナントID)
- アプリケーションID
- アプリケーションシークレット

  詳細については、「アプリケーションシークレットの取得」を参照してください。
- シークレットの有効期限

詳細な手順は次のとおりです。

接続とリソースの追加ウィザードで、:

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンを作成するために使用するツールを選択し、**次へ**を選択します。
3. 「**接続の詳細**」ページで、Azure サブスクリプション ID と接続の名前を入力します。

   > **注:**
   >
   > 接続名には 1～64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. **既存を使用**を選択します。**既存のサービスプリンシパルの詳細**ウィンドウで、既存のサービスプリンシパルに対して次の設定を入力します。詳細を入力すると、**保存**ボタンが有効になります。**保存**を選択します。有効な詳細情報を提供するまで、このページから先に進むことはできません。

   - **サブスクリプションID**。AzureサブスクリプションIDを入力します。サブスクリプションIDを取得するには、Azureポータルにサインインし、**サブスクリプション > 概要**に移動します。
   - **Active Directory ID**（テナントID）。Azure ADに登録したアプリケーションのディレクトリ（テナント）IDを入力します。
   - **アプリケーションID**。Azure ADに登録したアプリケーションのアプリケーション（クライアント）IDを入力します。
   - **アプリケーションシークレット**。シークレットキー（クライアントシークレット）を作成します。登録されたアプリケーションは、このキーを使用してAzure ADに認証します。セ

キュリティ上の理由から、キーを定期的に変更することをお勧めします。キーは後で取得できないため、必ず保存してください。

- **シークレットの有効期限**。アプリケーションシークレットの有効期限が切れる日付を入力します。シークレットキーの有効期限が切れる14日前から、**ホスティング**ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

  > **注:**
  >
  > セキュリティ上の理由から、有効期限は現在から2年を超えることはできません。

- **認証 URL**。このフィールドは自動的に入力され、編集できません。
- **管理 URL**。このフィールドは自動的に入力され、編集できません。
- **ストレージサフィックス**。このフィールドは自動的に入力され、編集できません。

  AzureでMCSカタログを作成するには、以下のエンドポイントへのアクセスが必要です。これらのエンドポイントへのアクセスにより、ネットワークとAzureポータルおよびそのサービス間の接続が最適化されます。

  - 認証URL: `<https://login.microsoftonline.com/>`
  - 管理URL: `<https://management.azure.com/>`。これはAzure Resource ManagerプロバイダーAPIのリクエストURLです。管理用のエンドポイントは環境によって異なります。例えば、Azure Globalの場合は`<https://management.azure.com/>`、Azure US Governmentの場合は`<https://management.usgovcloudapi.net/>`です。
  - ストレージサフィックス: `<https://*.core.windows.net./>`。これは(*)ストレージサフィックスのワイルドカード文字です。例えば、`https://demo.table.core.windows.net/`。

5. **保存**を選択すると、「**接続の詳細**」ページに戻ります。「**次へ**」を選択して次のページに進みます。
6. 接続のリソースを構成します。リソースは、リージョンとネットワークで構成されます。

   - **リージョン**ページで、リージョンを選択します。
   - **ネットワーク**ページで、以下を実行します。

- リージョンとネットワークの組み合わせを識別するために、1〜64文字のリソース名を入力します。リソース名には、空白のみ、または文字`\/;:#.*?=<>|[]{}"'()'`を含めることはできません。
- 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名とリソースグループをペアにすることで一意の組み合わせが提供されます。）前のページで選択したリージョンに仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがあるリージョンを選択してください。

7. 「**概要**」ページで、設定の概要を確認し、「**完了**」を選択してセットアップを完了します。

サービスプリンシパルと接続の管理

このセクションでは、サービスプリンシパルと接続を管理する方法について詳しく説明します。

- Azureスロットリング設定の構成
- Azureでのイメージ共有の有効化
- フル構成を使用して共有テナントを接続に追加する
- PowerShellを使用したイメージ共有の実装
- アプリケーションシークレットとシークレットの有効期限の管理

Azureスロットリング設定の構成

Azure Resource Managerは、サブスクリプションとテナントのリクエストをスロットリングし、プロバイダーの特定のニーズに合わせて定義された制限に基づいてトラフィックをルーティングします。詳細については、MicrosoftサイトのResource Managerリクエストのスロットリングを参照してください。サブスクリプションとテナントには制限があり、多数のマシンを管理すると問題が発生する可能性があります。たとえば、多数のマシンを含むサブスクリプションでは、電源操作に関連するパフォーマンスの問題が発生する可能性があります。

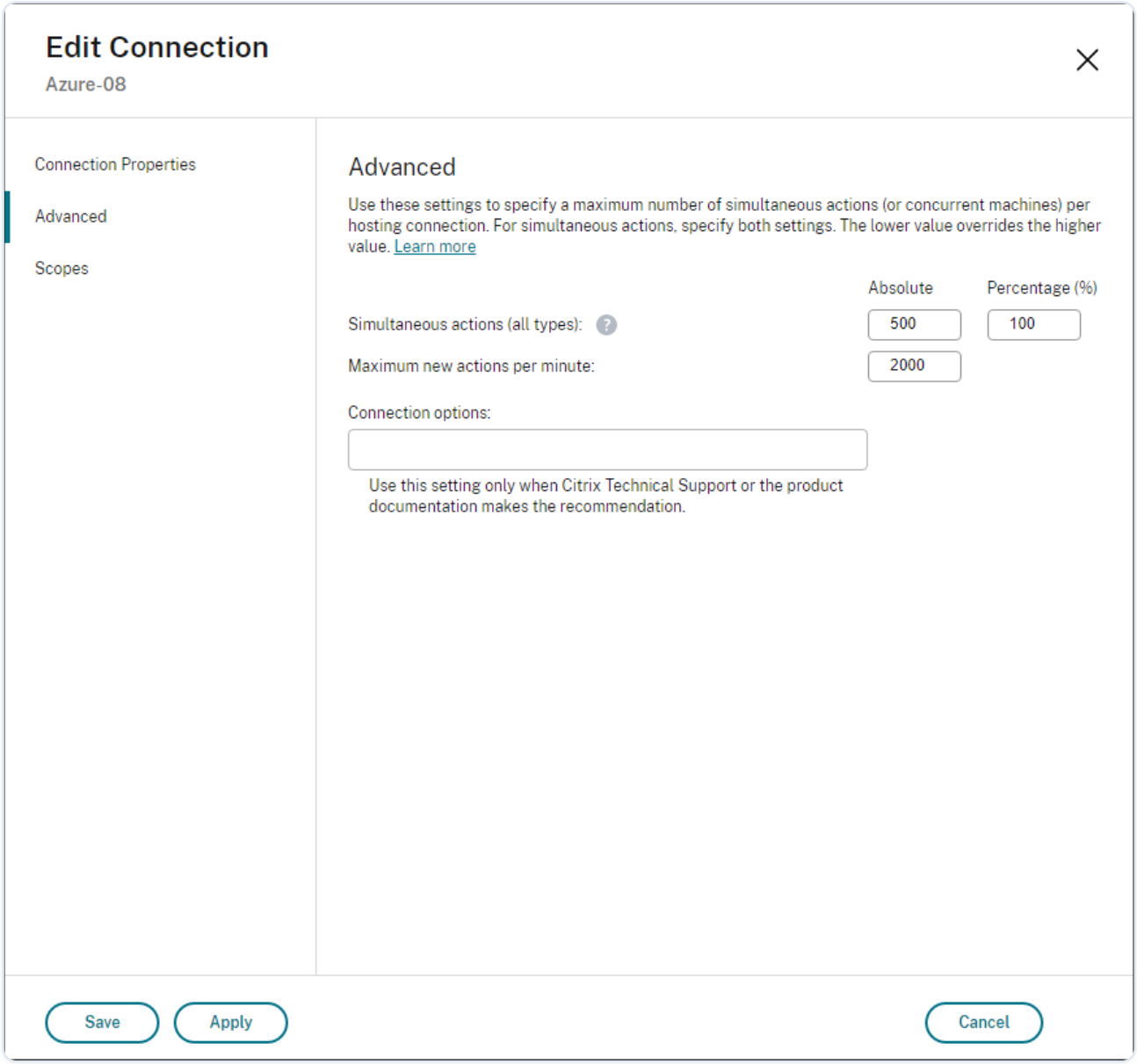
> **ヒント:**
>
> 詳細については、Machine Creation ServicesによるAzureパフォーマンスの向上を参照してください。
>
> これらの問題を軽減するために、MCSの内部スロットリングを削除して、Azureから利用可能なリクエストクォータをより多く使用できます。

大規模なサブスクリプション（たとえば、1,000台のVMを含むもの）でVMの電源をオンまたはオフにする場合、以下の最適な設定をお勧めします。

- 同時操作の絶対数: 500
- 1分あたりの新規操作の最大数: 2000
- 操作の最大同時実行数: 500

Web Studio を使用して、特定の Azure 接続の Azure 操作を構成します。

1. Web Studio で、左ペインの を選択します。
2. 接続を選択します。
3. ウィザードで、 を選択します。
4. ページで、構成オプションを使用して、同時アクションの数、1分あたりの最大新規アクション数、および追加の接続オプションを指定します。



MCS はデフォルトで最大 500 の同時操作をサポートします。または、Remote PowerShell SDK を使用して、同時操作の最大数を設定することもできます。

PowerShell プロパティ `MaximumConcurrentProvisioningOperations` を使用して、Azure プロビジョニングの同時操作の最大数を指定します。このプロパティを使用する際は、以下を考慮してください。

- `MaximumConcurrentProvisioningOperations` のデフォルト値は 500 です。
- PowerShell コマンド `Set-item` を使用して、`MaximumConcurrentProvisioningOperations` パラメーターを構成します。

Azure でのイメージ共有を有効にする

マシンカタログを作成または更新する際、異なる Azure テナントおよびサブスクリプション (Azure Compute Gallery を介して共有) から共有イメージを選択できます。テナント内またはテナント間でイメージ共有を有効にするには、Azure で必要な設定を行う必要があります。

- テナント内 (サブスクリプション間) でイメージを共有する
- テナント間でイメージを共有する

テナント内 (サブスクリプション間) でイメージを共有する

別のサブスクリプションに属するAzure Compute Galleryのイメージを選択するには、そのイメージをそのサブスクリプションのサービスプリンシパル (SPN) と共有する必要があります。

たとえば、Studioで次のように構成されているサービスプリンシパル (SPN 1) があるとします。

サービスプリンシパル: SPN 1

サブスクリプション: サブスクリプション 1

テナント: テナント 1

イメージは別のサブスクリプションにあり、Studioで次のように構成されています。

サブスクリプション: サブスクリプション 2

テナント: テナント 1

サブスクリプション 2 のイメージをサブスクリプション 1 (SPN 1) と共有したい場合は、サブスクリプション 2 に移動し、リソースグループを SPN1 と共有します。

イメージは、Azure ロールベースのアクセス制御 (RBAC) を使用して、別の SPN と共有する必要があります。Azure RBAC は、Azure リソースへのアクセスを管理するために使用される承認システムです。Azure RBAC の詳細については、Microsoft ドキュメントの「 (https://learn.microsoft.com/ja-jp/azure/role-based-access-control/overview)」を参照してください。アクセスを許可するには、リソースグループスコープで共同作成者ロールを持つサービスプリンシパルにロールを割り当てます。Azure ロールを割り当てるには、ユーザーアクセス管理者や所有者などの `Microsoft.Authorization/roleAssignments/write` 権限が必要です。別の SPN とイメージを共有する方法の詳細については、Microsoft ドキュメントの「Azure portal を使用して Azure ロールを割り当てる」を参照してください。

PowerShell コマンドを使用して別のサブスクリプションからイメージを選択する方法については、「別のサブスクリプションからイメージを選択する」を参照してください。

テナント間で画像を共有する

Azure Compute Gallery を使用してテナント間でイメージを共有するには、アプリケーション登録を作成します。

たとえば、2 つのテナント (テナント 1 とテナント 2) があり、イメージギャラリーをテナント 1 と共有したい場合は、次の手順を実行します。

1. テナント 1 のアプリケーション登録を作成します。詳細については、「アプリ登録を作成する」を参照してください。
2. ブラウザを使用してサインインを要求することで、テナント2にアプリケーションへのアクセスを許可します。`Tenant2 ID` をテナント1のテナントIDに置き換えます。`Application (client) ID` を作成したアプリケーション登録のアプリケーションIDに置き換えます。置換が完了したら、URLをブラウザに貼り付け、サインインプロンプトに従ってテナント2にサインインします。例:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
   client_id=<Application (client)
   ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   ```

   詳細については、「テナント2にアクセスを許可する」を参照してください。
3. アプリケーションにテナント2のリソースグループへのアクセスを許可します。テナント2としてサインインし、ギャラリーイメージを持つリソースグループにアプリケーション登録のアクセスを許可します。詳細については、「テナント間で要求を認証する」を参照してください。

PowerShell コマンドを使用して別のテナントのイメージからカタログを作成するには:

1. 「」(#update-hosting-connection-custom-properties-with-shared-tenant-ids)。
2. 「」(#select-an-image-from-a-different-tenant)。

フル構成を使用して共有テナントを接続に追加する

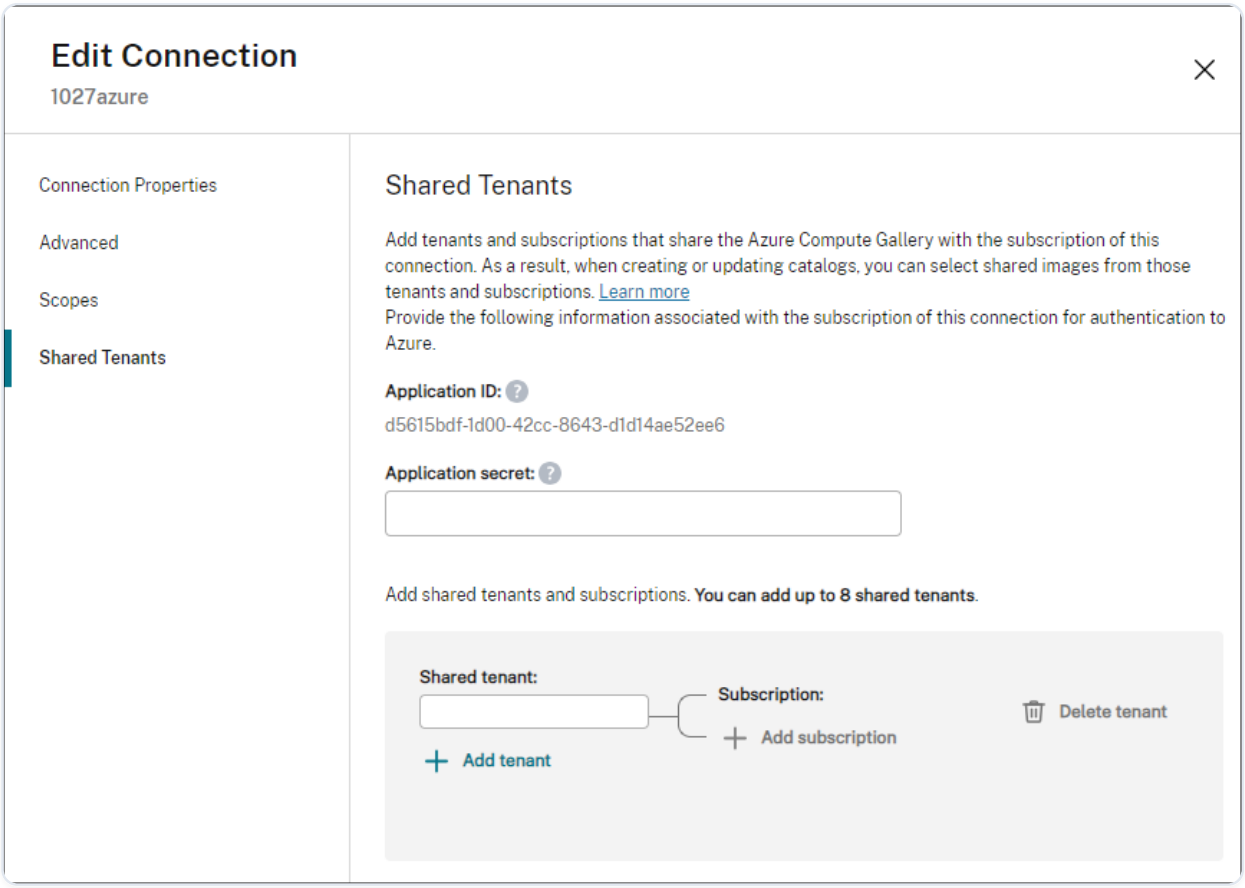
Web Studioでマシンカタログを作成または更新する際、異なるAzureテナントおよびサブスクリプション（Azure Compute Galleryを通じて共有される）から共有イメージを選択できます。この機能を使用するには、関連するホスト接続の共有テナントおよびサブスクリプション情報を提供する必要があります。

> **注:**
>
> テナント間でイメージ共有を有効にするために、Azureで必要な設定が構成されていることを確認してください。詳細については、「テナント間でイメージを共有する」を参照してください。

接続に対して次の手順を実行します。

1. Web Studio で、左側のペインの を選択します。

2. 接続を選択し、アクションバーで**接続の編集**を選択します。



3. 「**共有テナント**」で、以下を実行します。

   - 接続のサブスクリプションに関連付けられているアプリケーションIDとアプリケーションシークレットを指定します。Citrix Virtual Apps and Desktops は、この情報を使用して Azure AD に認証します。
   - 接続のサブスクリプションと Azure Compute Gallery を共有するテナントとサブスクリプションを追加します。各テナントにつき、最大8つの共有テナントと8つのサブスクリプションを追加できます。

4. 完了したら、**適用**を選択して行った変更を適用し、ウィンドウを開いたままにするか、**OK**を選択して変更を適用し、ウィンドウを閉じます。

PowerShell を使用したイメージ共有の実装

このセクションでは、PowerShell を使用してイメージを共有するプロセスについて説明します。

- 別のサブスクリプションからイメージを選択する
- 共有テナントIDでホスティング接続のカスタムプロパティを更新する
- 別のテナントからイメージを選択する

別のサブスクリプションからイメージを選択する

PowerShell コマンドを使用して MCS カタログを作成および更新するために、同じ Azure テナント内の別の共有サブスクリプションに属する Azure Compute Gallery のイメージを選択できます。

1. ホスティングユニットのルートフォルダーに、Citrix は `sharedsubscription` という新しい共有サブスクリプションフォルダーを作成します。
2. テナント内のすべての共有サブスクリプションを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\sharedsubscription.folder"
```

3. 1つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription"
```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup"
```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\testgallery.gallery"
```

6. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\sigtestdef.imagedefinition"
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ

- ギャラリー
- ギャラリーイメージ定義
- ギャラリーイメージバージョン

Remote PowerShell SDK を使用したカタログの作成方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

共有テナントIDでホスティング接続のカスタムプロパティを更新する

`Set-Item` を使用して、共有テナントIDとサブスクリプションIDでホスティング接続のカスタムプロパティを更新します。`CustomProperties` にプロパティ `SharedTenants` を追加します。`Shared Tenants` の形式は次のとおりです。

```
[{"Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":
["7bb42f40-8d7f-4230-a920-be2781f6d5d9"]},{"Tenant":"50e83564-c4e5-4209-
b43d-815c45659564","Subscriptions":["06ab8944-6a88-47ee-
a975-43dd491a37d0"]}]
```

例:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`" /
>

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` />
```

```
</CustomProperties>"

-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "advc345"
-SecurePassword

$psd
```

注:

複数のテナントを追加できます。各テナントは複数のサブスクリプションを持つことができます。

別のテナントからイメージを選択する

PowerShellコマンドを使用してMCSカタログを作成および更新するために、別のAzureテナントに属するAzure Compute Galleryのイメージを選択できます。

1. ホスティングユニットのルートフォルダーに、Citrixは`sharedsubscription`という新しい共有サブスクリプションフォルダーを作成します。
2. すべての共有サブスクリプションを一覧表示します。

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
   ```

3. 1つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription
   ```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription\
   xyz.resourcegroup
   ```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery
```

6. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery\hij.imagedefinition
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

   Remote PowerShell SDK を使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

アプリケーションシークレットとシークレットの有効期限を管理する

シークレットの有効期限が切れる前に、接続のアプリケーションシークレットを必ず変更してください。シークレットキーの有効期限が切れる14日前から、**Hosting** ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

AZURE でアプリケーションシークレットを作成する

Azureポータルを通じて、接続のアプリケーションシークレットを作成できます。

1. 「**Azure Active Directory**」を選択します。
2. Azure AD の「**アプリの登録**」から、アプリケーションを選択します。
3. 「**証明書とシークレット**」に移動します。
4. 「**クライアントシークレット > 新しいクライアントシークレット**」をクリックします。
5. シークレットの説明を入力し、期間を指定します。完了したら、「**追加**」を選択します。

> **注:**
>
> クライアントシークレットは後で取得できないため、必ず保存してください。

6. クライアントシークレットの値と有効期限をコピーします。
7. Web Studioで、対応する接続を編集し、「**アプリケーションシークレット**」および「**シークレットの有効期限**」フィールドの内容をコピーした値に置き換えます。

シークレットの有効期限を変更する

Web Studioを使用して、使用中のアプリケーションシークレットの有効期限を追加または変更できます。

> **注:**
>
> シークレットキーの有効期限が切れる14日前から、「**ホスティング**」ノードの特定のホスト接続に警告アイコンが表示されます。

1. 「**接続とリソースの追加**」ウィザードで、接続を右クリックし、「**接続の編集**」をクリックします。
2. 「**接続プロパティ**」ページで、「**シークレットの有効期限**」をクリックして、使用中のアプリケーションシークレットの有効期限を追加または変更します。

必要な Azure 権限

このセクションには、Azure に必要な最小限の一般的な権限が含まれています。

最小限の権限

最小限の権限は、より優れたセキュリティ制御を提供します。ただし、追加の権限を必要とする新機能は、最小限の権限のみを使用しているため失敗します。

ホスト接続の作成

Azure から取得した情報を使用して、新しいホスト接続を追加します。

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",
```

```
"Microsoft.Compute/disks/read",
```

VM の電源管理

マシンインスタンスの電源をオンまたはオフにします。

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",
```

VM の作成、更新、または削除

マシンカタログを作成し、マシンを追加、削除、更新し、マシンカタログを削除します。

以下は、マスターイメージがマネージドディスクであるか、スナップショットがホスティング接続と同じリージョンにある場合に必要となる最小限の権限のリストです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",
```

```
"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",
```

以下の機能には、最小限の権限に加えて、以下の追加権限が必要です。

- マスターイメージが、ホスティング接続と同じリージョンにあるストレージアカウント内の VHD である場合:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",
```

- マスターイメージが Shared Image Gallery の ImageVersion である場合:

```
"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",
```

- マスターイメージがマネージドディスクであり、スナップショットまたは VHD がホスティング接続のリージョンとは異なるリージョンにある場合:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/delete",
```

- Citrix管理のリソースグループを使用する場合:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- マスターイメージを共有イメージギャラリーに配置する場合:

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",
```

```
"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/versions/delete",
```

- Azure専用ホストサポートを使用する場合:

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/hostGroups/hosts/read",
```

- カスタマーマネージドキー (CMK) を使用してサーバー側暗号化 (SSE) を使用する場合:

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- ARM テンプレート (マシンプロファイル) を使用して VM を展開する場合:

```
"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/delete",
```

- Azure テンプレート仕様をマシンプロファイルとして使用する場合:

```
"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

アンマネージドディスクを使用したマシンの作成、更新、削除

マスターイメージがVHDであり、管理者が提供するリソースグループを使用する場合に必要な最小限の権限のリストは次のとおりです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action"
```

一般的な権限

共同作成者ロールは、すべてのリソースを管理するためのフルアクセス権を持っています。この権限セットは、新機能の取得を妨げるものではありません。

以下の権限セットは、現在の機能セットで必要とされる以上の権限を含んでいますが、今後最高の互換性を提供します。

```
"Microsoft.Compute/diskEncryptionSets/read",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/write",

"Microsoft.Compute/hostGroups/hosts/read",

"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",
```

```
"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
```

```
"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Azure固有の情報については、「Microsoft Azureカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

マイクロソフト システムセンター バーチャルマシンマネージャー への接続

(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections.html)では、接続を作成するウィザードについて説明します。以下の情報では、Microsoft System Center Virtual Machine Manager（VMM）に固有の詳細について説明します。

> **注:**
>
> VMM への接続を作成する前に、まず VMM アカウントをリソースの場所として設定する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare/msscvmm.html)を参照してください。

接続を作成する

MCSを使用してVMをプロビジョニングした場合は、接続作成ウィザードで次の操作を行います。

- ホストサーバーの完全修飾ドメイン名としてアドレスを入力します。
- 以前に設定した管理者アカウントの資格情報を入力します。このアカウントには、新しいVMを作成する権限が必要です。
- ［ホストの詳細］ダイアログボックスで、VMの作成時に使用するクラスターまたはスタンドアロンホストを選択します。

  > **重要**
  >
  > 単一のHyper-Vホスト展開を使用している場合でも、クラスターまたはスタンドアロンホストを参照してください。

次の手順

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- SMB 3 ファイル共有でMCSを使用してマシンカタログを作成する方法については、(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-mscvmm.html)を参照してください。

詳細情報

- 接続とリソース(/ja-jp/citrix-virtual-apps-desktops/2311/manage-deployment/connections.html)

- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html)

Nutanixへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、Nutanixに固有の詳細を扱っています。

> **注:**
>
> Nutanixへの接続を作成する前に、まずNutanixアカウントをリソースの場所として設定を完了する必要があります。Nutanix仮想化環境を参照してください。

Nutanixへの接続を作成する

以下の情報は、接続とリソースのガイダンスを補足するものです。Nutanix接続を作成するには、その記事の一般的なガイダンスに従い、Nutanixに固有の詳細に注意してください。

接続とリソースの追加ウィザードで、**接続**ページでNutanix接続の種類を選択し、アドレスと資格情報、および接続の名前を指定します。**ネットワーク**ページで、ホスティングユニットのネットワークを選択します。

以下の接続タイプを選択できます：**Nutanix AHV**、**Nutanix AHV DRaaS**、**Nutanix AHV PC**。

- **Nutanix AHV**の場合、Prism Element（PE）クラスターのアドレスと資格情報を指定します。
- **Nutanix AHV PC**の場合、Prism Central（PC）のアドレスと資格情報を指定します。

  > **注:**
  >
  > 現在、Nutanix AHV PC接続タイプは、Azure上のNutanix Cloud Cluster (NC2)への接続を作成するためにのみ使用されます。また、マシンカタログは、Azure接続上のNC2内の単一クラスターでのみホストできます。

- **Nutanix AHV DRaaS**の場合、DRaaSテナントのアドレスとユーザー名を指定します。プライベートおよびパブリックのNutanix DRaaS資格情報ファイル (`.pem`) をインポートします。

> **ヒント:**

> Nutanix AHV (Prism Element) をリソースとして使用してマシンを展開する場合、仮想マシンのディスクが存在するコンテナを選択します。

次のステップ

- 初期展開プロセス中の場合は、マシンカタログの作成を参照してください。
- Nutanix固有の情報については、Nutanixカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Nutanix クラウドおよびパートナーソリューションへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、Nutanix クラウドおよびパートナーソリューションに固有の詳細を扱っています。

Citrix Virtual Apps and Desktops™ は、以下の Nutanix クラウドおよびパートナーソリューションをサポートしています。

- AWS 上の ニュータニックス クラウド クラスター

> **注:**
>
> Nutanix クラウドおよびパートナーソリューションへの接続を作成する前に、まず、それぞれのアカウントをリソースの場所として設定を完了する必要があります。「Nutanix クラウドおよびパートナーソリューション」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare/nutanix-cloud-patrner-solutions.html)を参照してください。

Nutanix Prism への接続

Nutanix クラスターを作成したら、Nutanix Prism に接続します。

Nutanix Prism に接続するには：

1. 10.0.129.0/24 サブネットに踏み台 VM を作成します。
2. 踏み台 VM に RDP 接続し、前のセクションでコピーした **Prism Element** の URL にアクセスします。

3. デフォルトの資格情報 `admin:nutanix/4u` を使用してログインします。パスワードを変更することを忘れないでください。

Nutanix クラスター上に VM を作成する

Nutanix Prism に接続した後、Nutanix クラスター上に VM を作成します。

VM がインターネットアクセスを必要とする場合

1. AWS コンソールに移動します。
2. Nutanix CFS によって作成された VPC と同じ VPC に、新しいサブネット 10.0.130.0/24 を作成します。
3. このサブネットのルートテーブルに、すべての非ローカルトラフィックを上記のNATゲートウェイに転送するルートを追加します。
4. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。
5. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet** に移動します。AWS で使用したのと同じサブネット 10.0.130.0/24 を使用します。
6. その新しいサブネットにすべての VM (AD、CC、VDA など) を作成します。

VM がインターネットアクセスを必要としない場合

1. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。
2. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet** に移動します。サブネット 10.0.129.0/24 を使用します。
3. そのサブネットにすべての VM (AD、CC、VDA など) を作成します。

> **ヒント:**
>
> VM の時刻とタイムゾーン情報が正しく設定されていることを確認してください。これは特に AD に当てはまります。

ホスト接続を作成する

1. Web Studioを起動します。
2. ホスティングノードを選択し、**Add Connection and Resources**をクリックします。

3. 「**接続**」画面で「**新しい接続を作成**」を選択し、「**接続アドレス**」に`https://xxx.xxx.xxx.xxx:9440`と入力します。
4. UIに従ってウィザードを完了します。

> **注：**
>
> Web StudioでNutanixのオプションを表示するには、すべてのコネクタVMにNutanixプラグインがインストールされている必要があります。Nutanixゾーンで使用されていない場合でも同様です。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Nutanix 固有の情報については、「Nutanix カタログの作成」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-nutanix.html)

詳細情報

- 接続とリソース
- マシンカタログの作成

VMwareへの接続

「接続とリソースの作成および管理」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections.html)では、接続を作成するウィザードについて説明しています。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMwareへの接続を作成する前に、まずVMwareアカウントをリソースの場所として設定を完了する必要があります。「VMware仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare/vmware.html)を参照してください。

接続を作成する

接続作成ウィザードで、次の操作を行います。

1. VMware接続の種類を選択します。
2. vCenter SDKのアクセスポイントのアドレスを指定します。
3. 以前に設定した、VMを作成する権限を持つVMwareユーザーアカウントの資格情報を指定します。ユーザー名は「ドメイン/ユーザー名」の形式で指定します。

VMware SSLサムプリント

VMware SSLサムプリント機能により、VMware vSphereハイパーバイザーへのホスト接続を手動で作成する必要がなくなります。接続を作成する前に、サイト内のDelivery Controllerとハイパーバイザーの証明書との間に信頼関係を手動で作成する必要はなくなりました。

VMware SSLサムプリント機能は、信頼されていない証明書のサムプリントをサイトデータベースに保存します。この構成により、ハイパーバイザーはControllerによって信頼されていなくても、Citrix Virtual Apps and Desktops™によって継続的に信頼されていると識別されます。

StudioでvSphereホスト接続を作成する際、接続先のマシンの証明書を表示できるダイアログボックスが表示されます。その後、それを信頼するかどうかを選択できます。

必要な権限

この記事に記載されている権限の一部またはすべてを持つVMwareユーザーアカウントと1つ以上のVMwareロールを作成します。ロールの作成は、ユーザーがいつでもさまざまなCitrix DaaS™操作を要求するために必要な権限の特定の粒度レベルに基づいて行います。ユーザー固有の権限をいつでも付与するには、データセンターレベル以上で、**子に伝播**オプションを選択して、それぞれのロールに関連付けます。ただし、`StorageProfile`権限と特定の`Tags`権限については、**子に伝播**なしで、ルートvCenter Serverレベルで権限を適用します。各テーブルの注記を参照してください。

次の表は、Citrix Virtual Apps and Desktopsの操作と、必要な最小限のVMware権限とのマッピングを示しています。

> **注:**
>
> 権限リストの表示名、特に *ユーザーインターフェイス* は、一部の vSphere バージョンで異なります。たとえば、vSphere 6.7 では、*ユーザーインターフェイス* 権限は、このページに記載されている必要な権限で説明されている **Settings** および **Memory** ではなく、**Change Memory** および **Change Settings** です。

接続とリソースを追加する

SDK	ユーザーインターフェイス
システム. アノニマス、システム. リード、および システム. ビュー	自動的に追加されます。組み込みの読み取り専用ロールを使用できます。

電源管理

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	仮想マシン > 相互作用 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 相互作用 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット
VirtualMachine.Interact.Suspend	仮想マシン > 操作 > サスペンド
Datastore.Browse	データストア > データストアを参照

マシンのプロビジョニング (Machine Creation Services™)

MCS を使用してマシンをプロビジョニングするには、次の権限が必須です:

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	データストア > スペースの割り当て
Datastore.Browse	データストア > データストアを参照
Datastore.FileManagement	データストア > 低レベルファイル操作
ネットワーク.割り当て	ネットワーク > ネットワークの割り当て
リソース.VMをプールに割り当て	リソース > 仮想マシンをリソースプールに割り当て
仮想マシン.構成.既存ディスクの追加	仮想マシン > 構成 > 既存ディスクの追加
仮想マシン.構成.新規ディスクの追加	仮想マシン > 構成 > 新規ディスクの追加
仮想マシン.構成.デバイスの追加または削除	仮想マシン > 構成 > デバイスの追加または削除

SDK	ユーザーインターフェイス
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリの変更
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定の変更
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット
VirtualMachine.Interact.Suspend	仮想マシン > 操作 > サスペンド
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成
VirtualMachine.State.CreateSnapshot	vSphere 5.0、Update 2、vSphere 5.1、Update 1、および vSphere 6.x、Update 1: 仮想マシン > 状態 > スナップショットの作成; vSphere 5.5: 仮想マシン > スナップショット管理 > スナップショットの作成

イメージの更新とロールバック

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	データストア > スペースの割り当て
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	データストア > 低レベルファイル操作

SDK	ユーザーインターフェイス
Network.Assign	ネットワーク > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成

プロビジョニングされたマシンの削除

SDK	ユーザーインターフェース
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	Datastore > 低レベルファイル操作
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除

ストレージプロファイル (vSAN)

vSANデータストアでカタログ作成中にストレージポリシーを表示、作成、または削除するには、次の権限が必要です。

SDK	ユーザーインターフェイス
StorageProfile.Update	プロファイル駆動型ストレージ > プロファイル駆動型ストレージの更新。vSphere 8 の場合: VMストレージポリシー > VMストレージポリシーの更新
StorageProfile.View	PROFILE-DRIVEN STORAGE > プロファイル駆動型ストレージビュー。vSphere 8 の場合: VM ストレージポリシー > VM ストレージポリシーの表示

注：

ストレージプロファイルの権限は、**子に伝播**せずに、ルートvCenter Serverレベルで適用します。

タグとカスタム属性

タグとカスタム属性を使用すると、vSphereインベントリで作成されたVMにメタデータを添付でき、これらのオブジェクトの検索とフィルタリングが容易になります。タグまたはカテゴリを作成、編集、割り当て、削除するには、以下の権限が必要です。

SDK	ユーザーインターフェイス
InventoryService.Tagging.CreateTag	vSphereタグ付け > vSphereタグの作成
InventoryService.Tagging.CreateCategory	vSphereタグ付け > vSphereタグカテゴリの作成
InventoryService.Tagging.EditTag	vSphere Tagging > vSphere タグの編集
InventoryService.Tagging.EditCategory	vSphere Tagging > vSphere タグカテゴリの編集
InventoryService.Tagging.DeleteTag	vSphere Tagging > vSphere タグの削除

SDK	ユーザーインターフェイス
InventoryService.Tagging.DeleteCategory	vSphere Tagging > vSphere タグカテゴリの削除
InventoryService.Tagging.AttachTag	vSphere Tagging > vSphere タグの割り当てまたは割り当て解除
InventoryService.Tagging.ObjectAttachable	vSphere Tagging > オブジェクト上での vSphere タグの割り当てまたは割り当て解除
Global.ManageCustomFields	グローバル > カスタム属性の管理
Global.SetCustomField	グローバル > カスタム属性の設定

注:

- MCSがマシンカタログを作成すると、ターゲットVMに特別な名前タグが付けられます。これらのタグは、マスターイメージとMCSによって作成されたVMを区別し、MCSによって作成されたVMがイメージ準備に使用されるのを防ぎます。vCenterの `XdProvisioned` 属性の値で違いを識別できます。MCSがVMを作成する場合、属性は**True**に設定されます。
- ルートvCenter Serverレベルで、**子に伝播**なしで `InventoryService.Tagging.AttachTag` 権限を適用します。

暗号化操作

暗号化操作の権限は、誰がどの種類のオブジェクトに対してどの種類の暗号化操作を実行できるかを制御します。vSphere Native Key Providerは `Cryptographer.*` 権限を使用します。暗号化操作には、以下の最小限の権限が必要です。

注:

これらの権限は、vTPMを搭載したVMでMCSマシンカタログを作成するために必要です。

SDK	ユーザーインターフェイス
Cryptographer.Access	特権 > すべての特権 > 暗号化操作 > 直接アクセス
Cryptographer.AddDisk	特権 > すべての特権 > 暗号化操作 > ディスクの追加
Cryptographer.Clone	特権 > すべての特権 > 暗号化操作 > クローン
Cryptographer.Encrypt	特権 > すべての特権 > 暗号化操作 > 暗号化
Cryptographer.EncryptNew	特権 > すべての特権 > 暗号化操作 > 新規暗号化
Cryptographer.Decrypt	特権 > すべての特権 > 暗号化操作 > 復号化
Cryptographer.Migrate	特権 > すべての特権 > 暗号化操作 > 移行
Cryptographer.ReadKeyServersInfo	特権 > すべての特権 > 暗号化操作 > KMS情報の読み取り

マシンのプロビジョニング (Citrix Provisioning™)

テンプレートをクローンして展開するためのこれらの権限は、Citrix Virtual Apps and Desktops セットアップウィザードと、Citrix Provisioning コンソールを介したデバイスのエクスポートウィザードを使用してVMをプロビジョニングするために必要です。ホスティング接続の作成時に権限を設定します。マシンのプロビジョニング (Machine Creation Services) からのすべての権限と、以下の権限が必要です。

SDK	ユーザーインターフェイス
VirtualMachine.Config.AddRemoveDevice	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリ
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定

SDK	ユーザーインターフェイス
VirtualMachine.Provisioning.CloneTemplate	仮想マシン > プロビジョニング > テンプレートのクローン作成
VirtualMachine.Provisioning.DeployTemplate	仮想マシン > プロビジョニング > テンプレートの展開
VApp.Export	vApp > エクスポート

注:

`VApp.Export` は、マシンプロファイルを使用して MCS マシンカタログを作成するために必要です。

証明書を取得してインポートする

vSphere 通信を保護するために、Citrix® は HTTP ではなく HTTPS を使用することを推奨しています。

HTTPS にはデジタル証明書が必要です。組織のセキュリティポリシーに準拠した認証局から発行されたデジタル証明書を使用してください。

認証局から発行されたデジタル証明書を使用できない場合は、VMware がインストールした自己署名証明書を使用できます。この方法は、組織のセキュリティポリシーで許可されている場合にのみ使用してください。VMware vCenter 証明書を各 Delivery Controller に追加します。

1. vCenter Server を実行しているコンピューターの完全修飾ドメイン名 (FQDN) を、そのサーバーの hosts ファイルの `%SystemRoot%/WINDOWS/system32/Drivers/etc/` に追加します。この手順は、vCenter Server を実行しているコンピューターの FQDN がドメインネームシステムにまだ存在しない場合にのみ必要です。
2. 以下のいずれかの方法で vCenter 証明書を取得します。

   vCenter サーバーから。

   a. rui.crt ファイルを vCenter サーバーから Delivery Controller でアクセス可能な場所にコピーします。

   b. Controller で、エクスポートされた証明書の場所に移動し、rui.crt ファイルを開きます。

Web ブラウザーを使用して証明書をダウンロードします。 Internet Explorer を使用している場合は、Internet Explorer を右クリックし、 を選択して証明書をダウンロードまたはインストールします。

a. Web ブラウザーを開き、vCenter サーバーへの安全な Web 接続を行います (例: `<https://server1.domain1.com)>`。
b. セキュリティ警告を受け入れます。
c. 証明書エラーが表示されているアドレスバーをクリックします。
d. 証明書を表示し、 タブをクリックします。
e. 「**ファイルにコピーして.CER形式でエクスポート**」を選択し、プロンプトが表示されたら名前を指定します。
f. エクスポートした証明書を保存します。
g. エクスポートした証明書の場所に移動し、.CERファイルを開きます。

管理者として実行している Internet Explorer から直接インポートします。

- Web ブラウザーを開き、vCenter サーバーへの安全な Web 接続を行います (例: `<https://server1.domain1.com)>`)。
- セキュリティ警告を受け入れます。
- 証明書エラーが表示されているアドレスバーをクリックします。
- 証明書を表示します。

3. 各Controllerの証明書ストアに証明書をインポートします。

a. **証明書のインストール**オプションをクリックし、**ローカルコンピューター**を選択して、**次へ**をクリックします。
b. **証明書をすべて次のストアに配置する**を選択し、**参照**をクリックします。**信頼されたユーザー**を選択し、**OK**をクリックします。**次へ**をクリックし、**完了**をクリックします。

インストール後にvSphereサーバーの名前を変更した場合は、新しい証明書をインポートする前に、そのサーバーで新しい自己署名証明書を生成する必要があります。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- VMware固有の情報については、「VMwareカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

VMware クラウドおよびパートナーソリューションへの接続

Azure VMware Solution (AVS) クラスター、Google Cloud VMware Engine、およびVMware Cloud on AWSをセットアップした後、接続を作成します。接続の作成については、VMwareへの接続を参照してください。

次の手順

- 初期展開プロセス中の場合は、マシンカタログの作成を参照してください。
- VMware固有の情報については、VMwareカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

マシンカタログを作成する

> **重要:**

> Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了（EOL）アイテムを削除した後にのみ、現在のリリースに展開をアップグレードできます。

> - パーソナルvDisk (PvDs)
> - AppDisks™
> - パブリッククラウドホストの種類: Citrix CloudPlatform、Microsoft Azure Classic

> 詳細については、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。

> **注:**

> Citrix Virtual Apps and Desktopsの展開は、Web Studio (Webベース) とCitrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> 展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにHybrid Rights Licenseが必要です。

インストーラーがサポートされていないテクノロジーの1つ以上、またはハイブリッド権限ライセンスのないホスト接続を検出すると、アップグレードは一時停止または停止します。説明メッセージが表示されます。インストーラーログには詳細が含まれています。詳細については、「展開のアップグレード」を参照してください。

はじめに

物理マシンまたは仮想マシンのコレクションは、マシンカタログと呼ばれる単一のエンティティとして管理されます。カタログ内のすべてのマシンは、マルチセッションOSまたはシングルセッションOS、およびWindowsまたはLinuxマシンという同じ種類のオペレーティングシステムを持っています。

Web Studioは、サイトを作成した後、最初のマシンカタログを作成するようにガイドします。最初のカタログを作成した後、Web Studioは最初のデリバリーグループを作成するようにガイドします。後で、作成したカタログを変更したり、さらにカタログを作成したりできます。

> **ヒント:**

> 既存の展開をアップグレードすると、Machine Creation Services (MCS) ストレージ最適化 (MCS I/O) 機能が有効になり、追加の構成は不要です。Virtual Delivery Agent (VDA) と Delivery Controller のアップグレードが MCS I/O のアップグレードを処理します。

概要

VM のカタログを作成するときは、それらの VM をプロビジョニングする方法を指定します。Machine Creation Services™ (MCS) を使用することも、独自のツールを使用してマシンを提供することもできます。

考慮事項:

- MCS は、仮想マシンイメージからの単一のシステムディスクをサポートします。そのイメージに接続されている残りのデータディスクは無視されます。
- MCS を使用して VM をプロビジョニングする場合、カタログに同一の VM を作成するためにマスターイメージ (またはイメージのスナップショット) を提供します。カタログを作成する前に、まずツールを使用してマスターイメージを作成および構成します。このプロセスには、イメージへの Virtual Delivery Agent (VDA) のインストールが含まれます。次に、Web Studio でマシンカタログを作成します。そのイメージ (またはスナップショット) を選択し、カタログに作成する VM の数を指定し、追加情報を構成します。
- マシンがすでに利用可能な場合でも、それらのマシン用に1つ以上のマシンカタログを作成する必要があります。
- PowerShell SDK を直接使用してカタログを作成する場合、イメージやスナップショットではなく、ハイパーバイザーテンプレート (**VMTemplates**) を指定できます。
- テンプレートを使用してカタログをプロビジョニングすることは、実験的な機能と見なされます。この方法を使用すると、仮想マシンの準備が失敗する可能性があります。その結果、テンプレートを使用してカタログを公開できません。

MCS または Citrix Provisioning™ を使用して最初のカタログを作成する場合、サイトを作成したときに構成したホスト接続を使用します。後で (最初のカタログとデリバリーグループを作成した後)、その接続に関する情報を変更したり、さらに接続を作成したりできます。

カタログ作成ウィザードを完了すると、正しく構成されていることを確認するためにテストが自動的に実行されます。テストが完了すると、テストレポートを表示できます。Web Studio からいつでもテストを実行できます。

> **注:**
>
> MCSはWindows 10 IoT CoreおよびWindows 10 IoT Enterpriseをサポートしていません。詳細については、Microsoftサイトを参照してください。

> Citrix Provisioning ツールに関する技術的な詳細については、「Citrix Virtual Apps and Desktops Image Management」を参照してください。

RDSライセンスチェック

Web Studioは現在、WindowsマルチセッションOSマシンを含むマシンカタログの作成中に、有効なMicrosoft RDSライセンスのチェックを実行しません。Windows **マルチセッションOSマシン**のMicrosoft RDSライセンスのステータスを表示するには、Citrix Directorに移動します。**マシン詳細**

パネルでMicrosoft RDSライセンスのステータスを表示します。このパネルは、**マシン詳細とユーザー詳細**ページにあります。詳細については、「Microsoft RDSライセンスの正常性」を参照してください。

VDA登録

ブローカーセッションを起動する際には、VDAをDelivery Controller™に登録する必要があります。未登録のVDAは、利用可能なリソースの活用不足につながる可能性があります。VDAが登録されない理由はさまざまであり、その多くは管理者がトラブルシューティングできます。Web Studioは、カタログ作成ウィザードで、およびカタログからデリバリーグループにマシンを追加した後に、トラブルシューティング情報を提供します。

ウィザードを使用して既存のマシンを追加した後、コンピューターアカウント名のリストは、各マシンがカタログに追加するのに適しているかどうかを示します。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージで問題のあるマシンが特定された場合、そのマシンを削除するか、マシンを追加します。たとえば、マシンに関する情報が取得できない可能性があることを示すメッセージが表示された場合でも、マシンを追加します。

詳細については、以下を参照してください。

- VDA登録のトラブルシューティングガイダンスについては、CTX136668を参照してください
- VDAのバージョンと機能レベル
- VDA登録方法

MCSカタログ作成の概要

カタログ作成ウィザードで情報を提供した後の、デフォルトのMCSアクションの概要を以下に示します。

- マスターイメージ（スナップショットではなく）を選択した場合、MCSはスナップショットを作成します。
- MCSはスナップショットの完全なコピーを作成し、ホスト接続で定義されている各ストレージの場所にそのコピーを配置します。
- MCSはマシンをActive Directoryに追加し、これにより一意のIDが作成されます。
- MCSは、ウィザードで指定された数のVMを作成し、各VMに2つのディスクが定義されています。VMごとに2つのディスクに加えて、マスターも同じストレージの場所に保存されます。複数のストレージの場所が定義されている場合、それぞれが次のディスクタイプを取得します。
    - 新しく作成されたVM間で共有される、読み取り専用のスナップショットの完全なコピー。

- 各VMに一意のIDを付与する、一意の16MBのIDディスク。各VMはIDディスクを取得します。
- VMへの書き込みを保存するための一意の差分ディスク。このディスクはシンプロビジョニングされており（ホストストレージでサポートされている場合）、必要に応じてマスターイメージの最大サイズまで増加します。各VMは差分ディスクを取得します。差分ディスクには、セッション中に加えられた変更が保持されます。専用デスクトップの場合は永続的です。プールされたデスクトップの場合、デリバリーコントローラーを介した再起動ごとに削除され、新しいものが作成されます。

あるいは、静的デスクトップを提供するためにVMを作成する際、カタログ作成ウィザードの**マシン**ページで、シック（完全コピー）VMクローンを指定できます。完全クローンは、すべてのデータストアにマスターイメージを保持する必要はありません。各VMは独自のファイルを持っています。

MCSストレージに関する考慮事項

MCSのストレージソリューション、構成、容量を決定する際には、多くの要因があります。以下の情報は、ストレージ容量に関する適切な考慮事項を提供します。

容量に関する考慮事項:

- ディスク

  DeltaまたはDifferencing (Diff) ディスクは、ほとんどのMCS展開において、各VMで最大のスペースを消費します。MCSによって作成される各VMには、作成時に最低2つのディスクが割り当てられます。

  - Disk0 = 差分ディスク：マスターベースイメージからコピーされたOSが含まれます。
  - Disk1 = IDディスク: 16 MB - 各VMのActive Directoryデータを格納します。

  製品の進化に伴い、特定のユースケースや機能の消費を満たすために、さらにディスクを追加する必要がある場合があります。例:

  - MCSストレージ最適化は、各VMのライトキャッシュスタイルのディスクを作成します。
  - MCSは、前のセクションで説明したDeltaディスクのシナリオとは対照的に、フルクローンを使用する機能を追加しました。

  ハイパーバイザーの機能も考慮に入れる必要があるかもしれません。例:

  - XenServer IntelliCacheは、各XenServerのローカルストレージに読み取りディスクを作成します。このオプションにより、共有ストレージの場所に保持されている可能性のあるマスターイメージに対するIOPSを節約できます。

- ハイパーバイザーのオーバーヘッド

  異なるハイパーバイザーは、VM のオーバーヘッドを発生させる特定のファイルを使用します。ハイパーバイザーは、管理および一般的なログ記録操作にもストレージを使用します。以下のオーバーヘッドを含めてスペースを計算してください。

  - ログファイル
  - ハイパーバイザー固有のファイル。例：
    - VMware は、**VM ストレージ**フォルダーにさらにファイルを追加します。VMware のベストプラクティスを参照してください。
    - 仮想マシンの合計サイズ要件を計算します。仮想ディスクに 20 GB、スワップファイルに 16 GB、ログファイルに 100 MB を含む仮想マシンを考慮すると、合計 36.1 GB を消費します。
  - XenServer のスナップショット; VMware のスナップショット。

- プロセスオーバーヘッド

  カタログの作成、マシンの追加、カタログの更新には、それぞれ固有のストレージへの影響があります。例：

  - 初期カタログ作成では、ベースディスクのコピーを各ストレージの場所にコピーする必要があります。
    - また、一時的に準備VMを作成する必要があります。
  - カタログにマシンを追加する場合、ベースディスクを各ストレージの場所にコピーする必要はありません。カタログの作成は、選択された機能によって異なります。
  - カタログを更新すると、各ストレージの場所に余分なベースディスクが作成されます。カタログの更新では、カタログ内の各 VM が一定期間 2 つの差分ディスクを持つため、一時的なストレージのピークも発生します。

その他の考慮事項：

- **RAMサイジング：** I/O最適化ディスク、ライトキャッシュ、スナップショットファイルなど、特定のハイパーバイザーファイルとディスクのサイズに影響します。
- **シンプロビジョニング/シックプロビジョニング:** シンプロビジョニング機能があるため、NFS ストレージが推奨されます。

Machine Creation Services (MCS) ストレージ最適化

MCS I/O と呼ばれる Machine Creation Services (MCS) ストレージ最適化機能では、次のようになります。

- ライトキャッシュコンテナは、Citrix Provisioning と同じ機能である *ファイルベース* です。たとえば、Citrix Provisioning のライトキャッシュファイル名は `D:\vdiskdif.vhdx` で、MCS I/O のライトキャッシュファイル名は `D:\mcsdif.vhdx` です。
- ライトキャッシュディスクに書き込まれる Windows クラッシュダンプファイルのサポートを含めることで、診断の改善を実現します。
- MCS I/O は、最適な多層ライトキャッシュソリューションを提供するために、*RAM 内キャッシュとハードディスクへのオーバーフロー* というテクノロジーを保持しています。この機能により、管理者は各層（RAM とディスク）のコストとパフォーマンスのバランスを取り、目的のワークロード要件を満たすことができます。

ライトキャッシュ方式を *ディスクベース* から *ファイルベース* に更新するには、次の変更が必要です。

1. MCS I/O は RAM のみのキャッシュをサポートしなくなりました。マシンカタログ作成時に Web Studio でディスクサイズを指定してください。
2. VM ライトキャッシュディスクは、VM を初めて起動するときに自動的に作成およびフォーマットされます。VM が起動すると、ライトキャッシュファイル `mcsdif.vhdx` がフォーマットされたボリューム `MCSWCDisk` に書き込まれます。
3. ページファイルはこのフォーマットされたボリューム `MCSWCDisk` にリダイレクトされます。その結果、このディスクサイズはディスク領域の合計量を考慮します。これには、ディスクサイズと生成されたワークロードの差分にページファイルサイズを加えたものが含まれます。これは通常、VM の RAM サイズに関連付けられます。

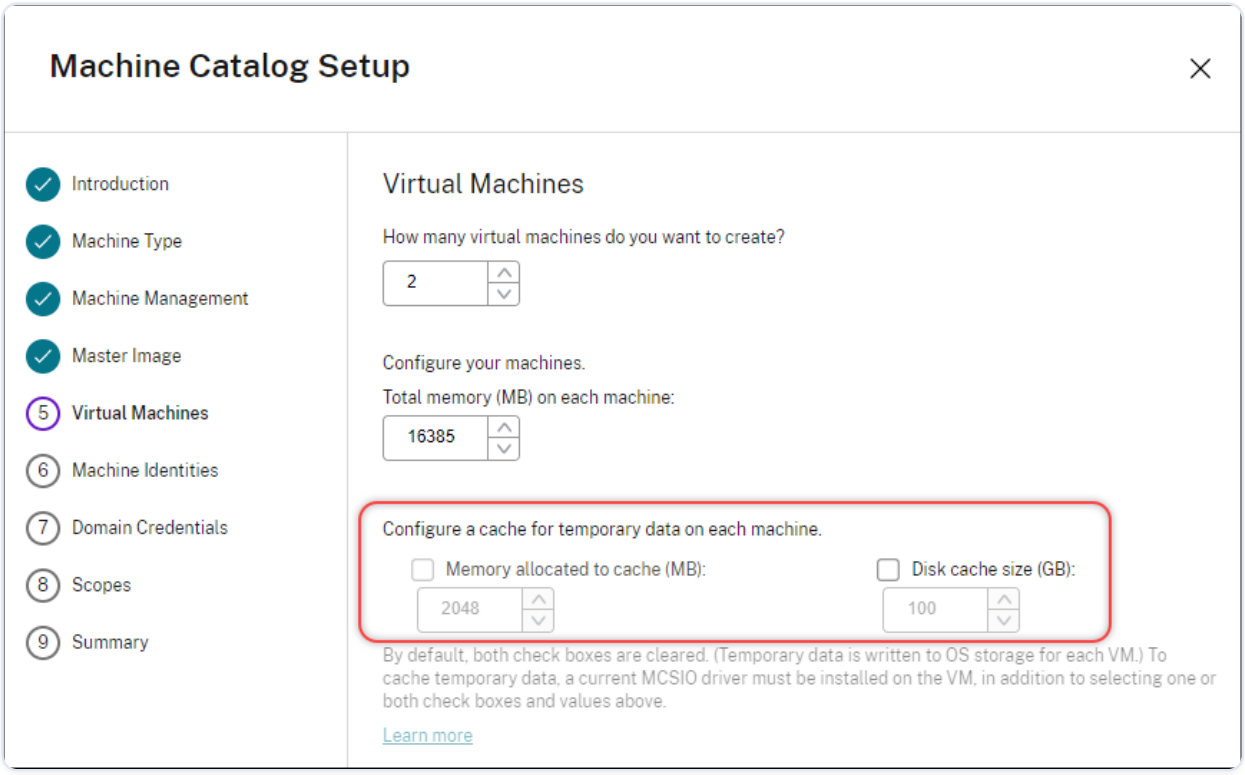
MCS ストレージ最適化の更新の有効化

MCS I/O ストレージ最適化機能を有効にするには、Delivery Controller と VDA を Citrix Virtual Apps and Desktops の最新バージョンにアップグレードしてください。

> **注:**
>
> MCS I/O が有効になっている既存の展開をアップグレードする場合、追加の構成は不要です。VDA と Delivery Controller のアップグレードによって MCS I/O のアップグレードが処理されます。

MCS ストレージ最適化の更新を有効にする際は、次の点を考慮してください。

- マシンカタログを作成する際、管理者は RAM とディスクサイズを構成できます。



- 既存のマシンカタログを、バージョン1903用に構成されたVDAを含む新しいVMスナップショットに更新すると、次の動作が発生します。新しいスナップショットは、既存のカタログのRAMおよびディスクサイズに対するMCS I/O設定を引き続き使用します。既存の生ディスクはフォーマットされます。

重要:

Citrix Virtual Apps and Desktops バージョン 1903 で MCS ストレージ最適化が変更されました。このリリースでは、ファイルベースのライトキャッシュテクノロジがサポートされ、パフォーマンスと安定性が向上しています。MCS I/O によって提供される新しい機能では、以前の Citrix Virtual Apps and Desktops リリースと比較して、より高いライトキャッシュストレージ要件が必要になる場合があります。Citrix は、割り当てられたワークフローと追加のページファイルサイズに対して十分なディスク容量があることを確認するために、ディスクサイズを再評価することをお勧めします。ページファイルサイズは通常、システム RAM の量に関連しています。既存のカタログディスクサイズが不十分な場合は、マシンカタログを作成し、より大きなライトキャッシュディスクを割り当ててください。

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てる

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この実装により、使用するアプリケーションのドライブ文字とMCS I/Oライトバックキャッシュディスクのドライブ文字との間の競合を回避できます。これを行うには、PowerShellコマンドを使用できます。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、およびXenServerです。

> **注:**
>
> この機能には、VDAバージョン2305以降が必要です。

制限事項

- Windowsオペレーティングシステムのみに適用
- ライトバックキャッシュディスクに適用可能なドライブ文字：`E`から`Z`
- Azure一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用されます

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには:

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. `WriteBackCacheDriveLetter`プロパティを持つ`New-ProvScheme`コマンドを使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `
```

```
-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
```

```
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. カタログの作成を完了します。詳細については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

マスターイメージを準備する

接続ホストの作成については、「接続とリソース」を参照してください。

マスターイメージには、オペレーティングシステム、仮想化されていないアプリケーション、VDA、およびその他のソフトウェアが含まれています。

知っておくと良いこと:

- マスターイメージは、クローンイメージ、ゴールデンイメージ、ベースVM、またはベースイメージとも呼ばれます。ホストベンダーは異なる用語を使用します。
- 作成されるマシンの数に対応できる十分なプロセッサ、メモリ、ストレージがホストにあることを確認してください。
- デスクトップおよびアプリケーションに必要なハードディスク容量を正しく構成します。この値は、後で変更したり、マシンカタログで変更したりすることはできません。
- Remote PC Accessマシンカタログはマスターイメージを使用しません。
- MCS 使用時の Microsoft KMS アクティベーションに関する考慮事項: 展開に XenServer 6.1 または 6.2、vSphere、または Microsoft System Center Virtual Machine Manager ホストを使用する 7.x VDA が含まれている場合、Microsoft Windows または Microsoft Office を手動で再アームする必要はありません。

マスターイメージに次のソフトウェアをインストールして構成します。

- ハイパーバイザー用の統合ツール (Citrix VM Tools、Hyper-V 統合サービス、VMware Tools など)。この手順を省略すると、アプリケーションやデスクトップが正しく機能しない可能性があります。

- VDA。Citrix は、最新機能にアクセスできるように、最新バージョンをインストールすることを推奨します。マスターイメージに VDA をインストールしないと、カタログの作成が失敗します。
- 必要に応じて、ウイルス対策ソフトウェアや電子ソフトウェア配布エージェントなどのサードパーティ製ツール。ユーザーとマシンタイプに適した設定 (更新機能など) でサービスを構成します。
- 仮想化しないサードパーティ製アプリケーション。Citrix はアプリケーションの仮想化を推奨します。仮想化により、アプリケーションの追加または再構成後にマスターイメージを更新する必要がなくなるため、コストが削減されます。また、インストールされるアプリケーションが少ないほど、マスターイメージのハードディスクのサイズが小さくなり、ストレージコストが節約されます。
- App-V アプリケーションを公開する予定がある場合は、推奨設定の App-V クライアント。App-V クライアントは Microsoft から入手できます。
- MCS を使用する場合、Microsoft Windows をローカライズする場合は、ロケールと言語パックをインストールします。プロビジョニング中にスナップショットが作成されると、プロビジョニングされた VM はインストールされているロケールと言語パックを使用します。

重要:

MCS を使用している場合は、マスターイメージで Sysprep を実行しないでください。

マスターイメージを準備するには：

1. ハイパーバイザーの管理ツールを使用してマスターイメージを作成し、オペレーティングシステム、すべてのサービスパック、および更新プログラムをインストールします。vCPU の数を指定します。PowerShell を使用してマシンカタログを作成する場合も、vCPU の値を指定できます。Web Studio を使用してカタログを作成する場合、vCPU の数を指定することはできません。デスクトップとアプリケーションに必要なハードディスク容量を構成します。この値は後で変更したり、カタログ内で変更したりすることはできません。
2. ハードディスクがデバイスの場所 0 に接続されていることを確認します。ほとんどの標準マスターイメージテンプレートではこの場所がデフォルトで構成されていますが、一部のカスタムテンプレートではそうでない場合があります。
3. 上記にリストされているソフトウェアをマスターイメージにインストールして構成します。
4. MCS を使用していない場合は、マスターイメージをアプリケーションとデスクトップが属するドメインに参加させます。マスターイメージがマシンが作成されるホストで利用可能である

ことを確認します。MCS を使用している場合、マスターイメージをドメインに参加させる必要はありません。プロビジョニングされたマシンは、カタログ作成ウィザードで指定されたドメインに参加します。

5. Citrixでは、マスターイメージのスナップショットを作成して名前を付けることをお勧めします。カタログ作成時にスナップショットではなくマスターイメージを指定した場合、Web Studioはスナップショットを作成します。そのスナップショットに名前を付けることはできません。

ボリュームライセンス認証

MCSは、WindowsオペレーティングシステムとMicrosoft Officeのアクティベーションを自動化および管理するためのボリュームライセンス認証をサポートしています。MCSがサポートするボリュームライセンス認証の3つのモデルは次のとおりです。

- キー管理サービス (KMS)
- Active Directoryベースのアクティベーション (ADBA)
- マルチプルアクティベーションキー (MAK)

マシンカタログを作成した後で、アクティベーション設定を変更できます。

キー管理サービス (KMS)

KMSは、専用のシステムを必要とせず、他のサービスを提供するシステム上で簡単に共同ホストできる軽量サービスです。この機能は、Citrixがサポートするすべてのバージョンでサポートされています。イメージ準備中に、MCSはMicrosoft WindowsおよびMicrosoft OfficeのKMSリアームを実行します。コマンド `Set-Provserviceconfigurationdata` を実行することで、リアームをスキップできます。イメージ準備中のMicrosoft Windows KMSリアームおよびMicrosoft Office KMSリアームの詳細については、「Machine Creation Services: Image Preparation Overview and Fault-Finding」を参照してください。KMSアクティベーションの詳細については、「Activate using Key Management Service」を参照してください。

> **注:**
>
> コマンド `Set-Provserviceconfigurationdata` の実行後に作成されたすべてのマシンカタログは、コマンドで指定されたものと同じ設定になります。

Active Directoryベースのアクティベーション (ADBA)

ADBAを使用すると、ドメイン接続を介してマシンをアクティベートできます。マシンはドメインに参加するとすぐにアクティベートされます。これらのマシンは、ドメインに参加し、ドメインと連絡を取り合っている限りアクティベートされたままになります。この機能は、Citrixがサポートするすべてのバージョンでサポートされています。Active Directoryベースのアクティベーションの詳細については、「Active Directory-based activation」を使用してアクティベートするを参照してください。

マルチプルアクティベーションキー (MAK)

MAKは、Microsoftサーバーの助けを借りて、ボリュームをアクティベートし、Windowsシステムを認証する方法です。MicrosoftからMAKキーを購入する必要があります。このキーには、固定されたアクティベーションカウントが割り当てられています。Windowsシステムがアクティベートされるたびに、アクティベーションカウントは減少します。システムをアクティベートする方法は2つあります。

- オンラインアクティベーション: アクティベートしたいWindowsシステムがインターネットにアクセスできる場合、システムはプロダクトキーのインストール時にWindowsを自動的にアクティベートします。このプロセスにより、対応するMAKのライセンス認証カウントが1つ減少します。
- オフラインアクティベーション: Windowsシステムがオンラインアクティベーションのためにインターネットに接続できない場合、MCSはMicrosoftサーバーから確認IDとインストールIDを取得し、Windowsシステムをアクティベートします。このアクティベーション方法は、非永続的なマシンカタログに役立ちます。

> **注:**
>
> - MCSはMAKを使用したMicrosoft Officeのアクティベーションをサポートしていません。
> - 必要なVDAの最小バージョンは2303です。

主な要件

- Delivery Controllerはインターネットにアクセスできる必要があります。
- 更新する新しいイメージが元のイメージと異なるMAKキーを持っている場合は、新しいカタログを作成します。
- マスターイメージにMAKキーをインストールします。WindowsシステムにMAKキーをインストールする手順については、「MAKアクティベーションの展開」を参照してください。

- イメージ準備を使用しない場合:

  a. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下にレジストリDWORD値 `Manual` を追加します。

  b. 値を `1` に設定します。

アクティベーション数

MAKキーの残りアクティベーション数を表示したり、VMが2つ以上のアクティベーションを消費しているかどうかを確認したりするには、ボリュームライセンス認証管理ツール (VAMT) を使用します。「VAMTのインストール」を参照してください。

MAKを使用してWindowsシステムをアクティベートする

MAKを使用してWindowsシステムをアクティベートするには：

1. マスターイメージにプロダクトキーをインストールします。この手順で1つのアクティベーションカウントが消費されます。
2. MCSマシンカタログを作成します。
3. イメージ準備を使用しない場合：

   a. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下にレジストリDWORD値`Manual`を追加します。

   b. 値を`1`に設定します。

   この方法では、オンラインアクティベーションのオプションが無効になります。
4. マシンカタログにVMを追加します。
5. VMの電源を入れます。
6. オンラインアクティベーションかオフラインアクティベーションかに応じて、Windowsシステムがアクティブ化されます。

   - オンラインアクティベーションの場合、プロダクトキーのインストール後に Windows システムがアクティベートされます。
   - オフラインアクティベーションの場合、MCS はプロビジョニングされた VM と通信して Windows システムのアクティベーションステータスを取得します。その後、MCS は Microsoft サーバーから確認 ID とインストール ID を取得します。これらの ID は Windows システムのアクティベーションに使用されます。

トラブルシューティング

プロビジョニングされた VM がインストール済みの MAK キーでアクティベートされない場合は、PowerShell ウィンドウで `Get-ProvVM` または `Get-ProvScheme` コマンドを実行します。

- `Get-ProvScheme`コマンド：最新のマスターイメージからMCSマシンカタログに関連付けられているパラメーター`WindowsActivationType`を参照してください。
- `Get-ProvVM` コマンド。パラメーター `WindowsActivationType`、`WindowsActivationStatus`、`WindowsActivationStatusErrorCode`、および`WindowsActivationStatusError` を参照してください。

エラーを確認し、問題を解決するための手順を検証できます。

Web Studio を使用してマシンカタログを作成する

カタログを作成する前に:

- このセクションを読んで、選択する項目と提供する情報について確認してください。
- ハイパーバイザー、クラウドサービス、またはマシンをホストするその他のリソースへの接続が作成されていることを確認してください。
- マシンをプロビジョニングするためのマスターイメージを作成した場合は、そのイメージにVDAがインストールされていることを確認してください。

カタログ作成ウィザードを開始するには：

1. これが最初に作成するカタログである場合、適切な選択肢（「マシンをセットアップし、アプリとデスクトップを実行するためのマシンカタログを作成する」など）に誘導されます。カタログ作成ウィザードが開きます。
2. すでにカタログを作成しており、別のカタログを作成したい場合は、次の手順に従ってください。

    a. Web Studio にサインインし、左ペインで を選択し、アクションバーで を選択します。

    b. フォルダーを使用してカタログを整理するには、デフォルトの フォルダーの下にフォルダーを作成します。詳細については、「カタログフォルダーの作成」を参照してください。

    c. カタログを作成するフォルダーを選択し、 をクリックします。カタログ作成ウィザードが開きます。

ウィザードは以下の項目について案内します。表示されるウィザードページは、選択内容によって異なります。

オペレーティングシステム

各カタログには、1種類のマシンのみが含まれます。いずれかを選択してください。

- **マルチセッションOS:** マルチセッションOSカタログは、ホストされた共有デスクトップを提供します。マシンはWindowsまたはLinuxオペレーティングシステムのサポートされているバージョンを実行できますが、カタログに両方を含めることはできません。（そのOSの詳細については、Linux VDAドキュメントを参照してください。）
- **シングルセッションOS:** シングルセッションOSカタログは、さまざまなユーザーに割り当てることができるVDIデスクトップを提供します。
- **Remote PC Access:** Remote PC Accessカタログは、ユーザーに物理的なオフィスデスクトップマシンへのリモートアクセスを提供します。Remote PC Accessは、セキュリティを提供するためにVPNを必要としません。

マシン管理

このページは、Remote PC Accessカタログを作成しているときには表示されません。

マシン管理ページには、マシンの管理方法と、マシンの展開に使用するツールが示されます。

カタログ内のマシンをWeb Studio経由で電源管理するかどうかを選択します。

- マシンはWeb Studioを介して電源管理されます。たとえば、VMやブレードPCなどです。このオプションは、ホストへの接続をすでに構成している場合にのみ利用可能です。
- マシンはWeb Studioを介して電源管理されません。たとえば、物理マシンなどです。

マシンがWeb Studio経由で電源管理されることを示した場合は、VMの作成に使用するツールを選択します。

- Citrix Provisioning テクノロジー
  - **Citrix Machine Creation Services (MCS):** マスターイメージを使用して仮想マシンを作成および管理します。MCSは物理マシンでは利用できません。
  - **Citrix Provisioning Services (PVS)** MCSを使用してプロビジョニングされ、PVSを使用してイメージ化されたVMのカタログを作成します。これらのVMはPVSターゲットデバイスとして機能し、PVSサーバーは単一の共有ディスクイメージをそれらにストリーミングできます。

    > **注:**

- このオプションは、Citrix Cloud™に登録されているPVSサイトでのみ利用可能であり、現在、Azureリソースに限定されています。
- Citrix Provisioningカタログを作成する際、ターゲットデバイスページで、プロビジョニングするマシンのファームとサイトを選択するドロップダウンメニューに、存在しないファームとサイトがリストされている場合があります。回避策として、PowerShellコマンドUnregister-HypPvsSiteを実行して、データベースからファームとサイトを削除できます。PowerShellコマンドの詳細については、「Unregister-HypPvsSite」を参照してください。

- **その他:** データセンターにすでに存在するマシンを管理するツール。Citrixでは、カタログ内のマシンの一貫性を確保するために、Microsoft System Center Configuration Managerまたはその他のサードパーティ製アプリケーションを使用することをお勧めします。

デスクトップの種類（デスクトップエクスペリエンス）

このページは、シングルセッションOSマシンを含むカタログを作成している場合にのみ表示されます。

デスクトップエクスペリエンスページでは、ユーザーがログオンするたびに何が起こるかを決定します。次のいずれかを選択します。

- ユーザーはログオンするたびに新しい（ランダムな）デスクトップに接続します。
- ユーザーはログオンするたびに同じ（静的な）デスクトップに接続します。

マスターイメージ

このページは、MCSを使用してVMを作成している場合にのみ表示されます。

マスターイメージページで、ホストへの接続を選択し、以前に作成したスナップショットまたはVMを選択します。最初のカタログを作成している場合、利用可能な接続は、サイトを作成したときに構成した接続のみです。

注意：

- MCSを使用している場合、マスターイメージでSysprepを実行しないでください。
- スナップショットではなくマスターイメージを指定した場合、Web Studioはスナップショットを作成しますが、名前を付けることはできません。

最新の製品機能を使用できるように、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。デフォルトの最小VDA選択を変更しないでください。ただし、以前のVDAバージョンを使用する必要がある場合は、「VDA versions and functional levels」を参照してください。

ウィザードで以前に選択したマシン管理テクノロジーと互換性のないスナップショットまたはVMを選択すると、エラーメッセージが表示されます。

マシン

リモートPCアクセス カタログを作成している場合、このページは表示されません。

このページのタイトルは、**マシン管理**ページで選択した内容（**マシン**、**仮想マシン**、または**VMとユーザー**）によって異なります。

MCSを使用する場合：

- 作成する仮想マシンの数を指定します。作成しない場合は**0**（ゼロ）を入力します。後で、**Add machines**を実行して、空のカタログにVMを作成できます。
- 各 VM が持つメモリ量 (MB 単位) を選択します。
- 作成された各VMにはハードディスクがあります。そのサイズはマスターイメージで設定されます。カタログでハードディスクのサイズを変更することはできません。
- 展開に複数のゾーンが含まれている場合、カタログのゾーンを選択できます。
- 静的デスクトップVMを作成する場合は、仮想マシンコピーモードを選択します。「仮想マシンコピーモード」を参照してください。
- vDiskを使用しないランダムデスクトップVMを作成する場合は、各マシンの一時データに使用するキャッシュを構成できます。「一時データ用のキャッシュの構成」を参照してください。

その他のツールを使用する場合：

Active Directoryマシンアカウント名を追加（またはリストをインポート）します。VMを追加/インポートした後で、そのActive Directoryアカウント名を変更できます。**デスクトップエクスペリエンス**ページで静的マシンを指定した場合、追加する各VMのActive Directoryユーザー名をオプションで指定できます。

名前を追加またはインポートした後、このページにいる間は「**削除**」ボタンを使用してリストから名前を削除できます。

他のツールを使用する場合（ただしMCSではない場合）：

追加（またはインポート）された各マシンに表示されるアイコンとツールヒントは、カタログに追加できない可能性のあるマシンや、Delivery Controllerに登録できない可能性のあるマシンを特定するのに役立ちます。詳細については、「VDAバージョンと機能レベル」を参照してください。

仮想マシン作成時にSIDを追加する

新しい仮想マシンの作成中に、パラメーター`ADAccountSid`を追加してマシンを一意に識別できるようになりました。

これを行うには：

1. サポートされているIDタイプでカタログを作成します。
2. `NewProvVM`を使用してカタログにマシンを追加します。例：

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID ")  -
RunAsynchronously
```

ただし、次の条件のいずれかに該当するマシンをプロビジョニングすることはできません。

- カタログIDプールにないADアカウント
- 利用可能な状態ではないADアカウント

仮想マシンのコピーモード

「**マシン**」ページで指定するコピーモードによって、MCSがマスターイメージからシン（高速コピー）クローンを作成するか、シック（完全コピー）クローンを作成するかが決まります。（デフォルト = シンクローン）

- ストレージ使用効率とマシン作成速度を向上させるには、高速コピーのクローンを使用します。
- マシンの作成後にIOPSが削減される可能性はありますが、データ回復と移行のサポートを向上させるには、完全コピーのクローンを使用します。

VDAのバージョンと機能レベル

カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要です。機能レベルを設定すると、そのバージョンで導入されたすべての機能（および機能レベルが変更されない場合はそれ以降のバージョンで導入された機能）がカタログ内のマシンで利用可能になります。ただし、そのカタログ内の以前のVDAバージョンのマシンは登録できません。

「**マシン**」（または「**デバイス**」）ページの下部にあるメニューで、最小VDAレベルを選択できます。これにより、カタログの最小機能レベルが設定されます。デフォルトでは、オンプレミス展開の場合、最新の機能レベルが選択されます。Citrixの推奨に従って、常にVDAとコアコンポーネントを最新バージョンにインストールおよびアップグレードする場合は、この選択を変更する必要はありません。ただし、古いVDAバージョンを使い続ける必要がある場合は、正しい値を選択してください。

Citrix Virtual Apps and Desktopsのリリースには、新しいVDAバージョンが含まれていない場合や、新しいVDAが機能レベルに影響を与えない場合があります。このような場合、機能レベルは、インストールまたはアップグレードされたコンポーネントよりも古いVDAバージョンを示すことがあります。たとえば、バージョン7.17には7.17 VDAが含まれていますが、デフォルトの機能レベル（「7.9以降」）は最新のままです。したがって、コンポーネント7.9～7.16を7.17にインストールまたはアップグレードした後も、デフォルトの機能レベルを変更する必要はありません。各リリースの新機能の記事には、デフォルトの機能レベルの変更が示されています。

選択された機能レベルは、その上にあるマシンのリストに影響を与えます。リストでは、各エントリの横にあるツールチップが、そのマシンのVDAがその機能レベルでカタログと互換性があるかどうかを示します。

各マシンのVDAが選択された最小機能レベルを満たしていないか、超えていない場合、ページにメッセージが表示されます。ウィザードを続行することはできますが、それらのマシンは後でControllerに登録できない可能性が高くなります。または、次のいずれかの操作を実行できます。

- 古いVDAを含むマシンをリストから削除し、VDAをアップグレードしてから、カタログに再度追加します。
- 最新の製品機能へのアクセスを妨げる、より低い機能レベルを選択します。

マシンタイプが正しくないためにマシンがカタログに追加されなかった場合も、メッセージが表示されます。例としては、シングルセッションOSカタログにサーバーを追加しようとしたり、ランダム割り当て用に作成されたシングルセッションOSマシンを静的マシンのカタログに追加したりする場合があります。

> **重要:**
>
> リリース1811で、追加の機能レベル「**1811 (or newer)**」が追加されました。このレベルは、将来のCitrix Virtual Apps and Desktops機能で使用することを目的としています。「**7.9 (or newer)**」の選択はデフォルトのままです。このデフォルトは、現在すべての展開で有効です。

「**1811 (or newer)**」を選択した場合、そのカタログ内の以前のVDAバージョンはControllerに登録できません。ただし、カタログにバージョン1811以降のサポートされているVDAのみが含まれている場合、それらはすべて登録可能です。これには、現在のリリースより前のバージョン1903およびその他の19XXリリースを含む、後のCitrix Virtual Apps and Desktopsリリース用に構成されたVDAを含むカタログも含まれます。

一時データのキャッシュを構成する

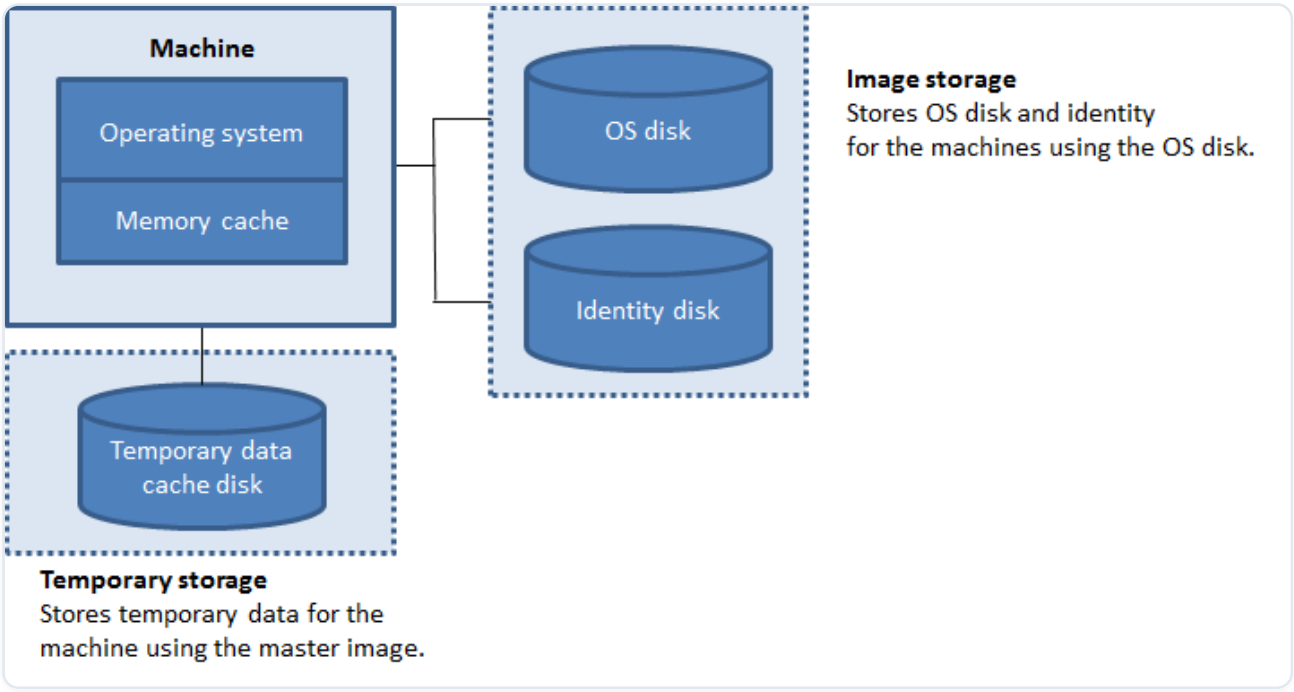
VMに一時データをローカルでキャッシュすることはオプションです。MCSを使用してカタログ内のプールされた（専用ではない）マシンを管理する場合、マシン上の一時データキャッシュの使用を有効にできます。カタログが一時データのストレージを指定する接続を使用している場合、カタログの作成時に一時データキャッシュ情報を有効にして構成できます。

重要:

この機能には、最新のMCS I/Oドライバーが必要です。このドライバーのインストールは、VDAをインストールまたはアップグレードする際のオプションです。デフォルトでは、このドライバーはインストールされていません。

一時データが共有ストレージを使用するかローカルストレージを使用するかは、カタログが使用する接続を作成するときに指定します。詳しくは、「接続とリソース」を参照してください。各マシンで一時データのキャッシュを構成するには、次の2つのオプションを使用できます。「**キャッシュに割り当てられるメモリ（MB）**」と「**ディスクキャッシュサイズ（GB）**」です。デフォルトでは、この2つのオプションはクリアされています。「キャッシュに割り当てられるメモリ（MB）」オプションを有効にするには、「ディスクキャッシュサイズ（GB）」チェックボックスをオンにします。「**ディスクキャッシュサイズ**」チェックボックスが選択されていない場合、「**キャッシュに割り当てられるメモリ**」オプションはグレー表示されます。接続の種類によっては、これらのオプションのデフォルト値が異なる場合があります。一般的に、デフォルト値はほとんどの場合で十分です。ただし、次の点に必要な領域を考慮してください。

- Windows自体によって作成される一時データファイル（Windowsページファイルを含む）。
- ユーザープロファイルデータ。
- ユーザーのセッションに同期されるShareFileデータ。
- セッションユーザーまたはユーザーがセッション内にインストールする可能性のあるアプリケーションによって作成またはコピーされる可能性のあるデータ。



各マシンの一時データキャッシュを構成するには、以下の3つのシナリオに注意してください。

- ディスクキャッシュサイズチェックボックスとメモリ割り当てキャッシュチェックボックスを選択しない場合、一時データはキャッシュされません。各VMの差分ディスク（OSストレージにあります）に直接書き込まれます。（これはバージョン7.8以前のプロビジョニングアクションです。）
- ディスクキャッシュサイズチェックボックスを選択し、メモリ割り当てキャッシュチェックボックスを選択しない場合、一時データは最小限のメモリキャッシュを使用して、キャッシュディスクに直接書き込まれます。
- ディスクキャッシュサイズチェックボックスとメモリ割り当てキャッシュチェックボックスを選択した場合、一時データは最初にメモリキャッシュに書き込まれます。メモリキャッシュが構成された制限（キャッシュに割り当てられるメモリ値）に達すると、最も古いデータは一時データキャッシュディスクに移動されます。

重要:

- ディスクキャッシュの容量が不足すると、ユーザーセッションは使用できなくなります。
- この機能は、Nutanixホスト接続を使用している場合は利用できません。
- マシン作成後、マシンカタログのキャッシュ値を変更することはできません。

注:

- メモリキャッシュは、各マシンの総メモリ量の一部です。したがって、「キャッシュに割り当てられたメモリ」オプションを有効にする場合は、各マシンの総メモリ量を増やすことを検討してください。
- ディスクキャッシュのサイズをデフォルト値から変更すると、パフォーマンスに影響を与える可能性があります。サイズはユーザーの要件とマシンにかかる負荷に合わせる必要があります。

NIC

リモートPCアクセス カタログを作成している場合、このページは表示されません。

「**ネットワークインターフェイスカード**」ページで、複数のNICを使用する予定がある場合は、各カードに仮想ネットワークを関連付けます。たとえば、1つのカードを特定のセキュアネットワークへのアクセスに割り当て、別のカードをより一般的に使用されるネットワークへのアクセスに割り当てることができます。このページからNICを追加または削除することもできます。

マシンアカウント

このページは、リモートPCアクセス カタログを作成する場合にのみ表示されます。

マシンアカウントページで、ユーザーまたはユーザーグループに対応する追加するActive Directoryマシンアカウントまたは組織単位（OU）を指定します。OU名にスラッシュ（/）を使用しないでください。

OUを追加する際、ドメインがリストに表示されない場合は、次のことができます。

- 完全一致で検索します。
- すべてのドメインを参照して見つけます。

以前に構成した電源管理接続を選択するか、電源管理を使用しないことを選択できます。電源管理を使用したいが、適切な接続がまだ構成されていない場合は、後でその接続を作成し、マシンカタログを編集して電源管理設定を更新できます。

マシンID

このページは、MCSを使用してVMを作成する場合にのみ表示されます。

カタログ内の各マシンには一意のIDが必要です。このページでは、カタログ内のマシンのIDを構成できます。マシンはプロビジョニング後にIDに結合されます。カタログ作成後にIDの種類を変更することはできません。

このページで設定を構成するための一般的なワークフローは次のとおりです。

1. リストからIDを選択します。
2. アカウントを作成するか既存のアカウントを使用するか、およびそれらのアカウントの場所（ドメイン）を指定します。

次のいずれかのオプションを選択できます。

- **オンプレミスActive Directory**。組織が所有し、その組織に属するActive Directoryアカウントでサインインするマシン。これらはオンプレミスに存在します。
- **ハイブリッドAzure Active Directory参加済み**。組織が所有し、その組織に属するActive Directory Domain Servicesアカウントでサインインするマシン。これらはクラウドとオンプレミスに存在します。要件、制限、考慮事項については、「ハイブリッドAzure Active Directory参加済み」を参照してください。

> **注:**
>
> - ハイブリッド Azure Active Directory 参加を使用する前に、Azure 環境が前提条件を満たしていることを確認してください。`<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/hybrid-azuread-join-managed-domains>`を参照してください。
> - このオプションでは、マスターイメージがオペレーティングシステムの前提条件を満たしている必要があります。詳細については、Microsoft のドキュメントを参照してください: `<https://learn.microsoft.com/ja-jp/azure/active-directory/devices/concept-azure-ad-join-hybrid>`。

> **重要:**
>
> - IDの種類として**オンプレミスActive Directory**または**ハイブリッドAzure Active Directory参加済み**を選択した場合、カタログ内の各マシンには対応するActive Directoryコンピューターアカウントが必要です。

> アカウントを作成する場合、マシンが存在するOUにコンピューターアカウントを作成する権限が必要です。カタログ内の各マシンは一意の名前を持つ必要があります。作成するマシンのアカウント命名スキームを指定します。詳細については、「マシンアカウント命名スキーム」を参照してください。

> **注:**
>
> OU名にスラッシュ（`/`）を使用しないようにしてください。

> 既存のアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。インポートされるファイルの内容は次の形式を使用する必要があります。

- ADcomputeraccountname.domain

追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Web Studioインターフェースがそれらのアカウントを管理します。したがって、そのインターフェースにすべてのアカウントのパスワードをリセットさせるか、すべてのアカウントで同じである必要があるアカウントパスワードを指定してください。

物理マシンまたは既存のマシンを含むカタログの場合、既存のアカウントを選択またはインポートし、各マシンをActive Directoryコンピューターアカウントとユーザーアカウントの両方に割り当てます。

マシンアカウントの命名スキーム

カタログ内の各マシンには一意の名前が必要です。カタログを作成する際には、マシンアカウントの命名スキームを指定する必要があります。名前に表示される連続した数字または文字のプレースホルダーとして、ワイルドカード（ハッシュマーク）を使用します。

命名スキームを指定する際は、以下の規則に注意してください。

- 命名スキームには少なくとも1つのワイルドカードが含まれている必要があります。すべてのワイルドカードはまとめて配置する必要があります。
- ワイルドカードを含む名前全体は、2文字以上15文字以下である必要があります。少なくとも1つの非数字文字と1つの#（ワイルドカード）文字を含める必要があります。
- 名前にスペースや次の文字を含めることはできません: `,~!@'$%\^&.()}{\/*?"<>|=+[];:_".`。

- 名前の末尾にハイフン (-) を含めることはできません。

また、命名スキームを指定する際には、将来の拡張に十分な余裕を持たせてください。次の例を考えてみましょう。「veryverylong#」というスキームで1,000個のマシンアカウントを作成した場合、最後に作成されるアカウント名（veryverylong1000）は16文字になります。したがって、この命名スキームでは、最大15文字を超えるマシン名が1つ以上生成されることになります。

連続する値が数字 (0-9) か文字 (A-Z) かを示すことができます。

- **0-9**。選択した場合、指定されたワイルドカードは連番に解決されます。

> **注:**
>
> ワイルドカードが1つ（#）の場合、アカウント名は1から始まります。2つの場合、アカウント名は01から始まります。3つの場合、アカウント名は001から始まり、以降同様です。

- **A-Z**。選択した場合、指定されたワイルドカードは連続する文字に解決されます。

例えば、PC-Sales-## (**0-9** が選択されている場合) という命名スキームでは、PC-Sales-01、PC-Sales-02、PC-Sales-03 などのアカウントが作成されます。

オプションで、アカウント名の開始文字を指定できます。

- **0-9** を選択すると、アカウントは指定された数字から順に命名されます。前のフィールドで使用するワイルドカードの数に応じて、1桁以上の数字を入力します。たとえば、2つのワイルドカードを使用する場合は、2桁以上の数字を入力します。
- **A-Z** を選択すると、アカウントは指定された文字から順に命名されます。前のフィールドで使用するワイルドカードの数に応じて、1文字以上の文字を入力します。たとえば、2つのワイルドカードを使用する場合は、2文字以上の文字を入力します。

ドメイン資格情報

資格情報の入力を選択し、ターゲットのActive Directoryドメインでアカウント操作を実行する権限を持つ管理者の資格情報を入力します。

名前の確認オプションを使用して、ユーザー名が有効か一意であるかを確認します。このオプションは、たとえば次のような場合に役立ちます。

- 複数のドメインに同じユーザー名が存在する場合。目的のユーザーを選択するよう求められます。

- ドメイン名を思い出せない場合。ドメイン名を指定せずにユーザー名を入力できます。チェックが成功すると、ドメイン名が自動的に入力されます。

> **注:**
>
> **マシンID**で選択したIDの種類が**ハイブリッドAzure Active Directory参加済み**の場合、入力する資格情報には`Write userCertificate`権限が付与されている必要があります。

概要、名前、および説明

「**概要**」ページで、指定した設定を確認します。カタログの名前と説明を入力します。この情報はWeb Studioに表示されます。

完了したら、**「完了」をクリックしてカタログの作成を開始します。 完了したら、**「完了」**を選択してカタログの作成を開始します。

マシンカタログに、新しいカタログがインラインの進行状況バーとともに表示されます。

作成の進行状況の詳細を表示するには：

1. マシンカタログにマウスカーソルを合わせます。
2. 表示されるツールヒントで、**詳細の表示**をクリックします。

   以下の項目を確認できる、段階的な進行状況グラフが表示されます。

   - ステップの履歴
   - 現在のステップの進行状況と実行時間
   - 残りのステップ

MCSの時刻同期

時刻同期は、マスターイメージと、参加しているマシンIDカタログのタイプによって決定されます。マスターイメージとカタログに応じて、次の時刻同期方法が適用されます。

マスターイメージ	カタログ	結果の時刻同期方法
NDJ	ADまたはハイブリッドAzure AD	デフォルトではNT5DSです。マスターイメージのレジストリ設定を使用して、MCSが時

マスターイメージ	カタログ	結果の時刻同期方法
		刻同期設定を変更するのを無効にできます。
NDJ	NDJ または Azure AD	元の時刻同期設定と同じ
AD または Hybrid Azure AD	AD または Hybrid Azure AD	元の時刻同期設定と同じ
アジュール エーディー	アジュール エーディー	元の時刻同期設定と同じ

注:

元の時刻同期は、以下のレジストリ設定によって制御されており、変更できません。

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

値: MaxAllowedPhaseOffset、MaxNegPhaseCorrection、および MaxPosPhaseCorrection

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

値: Type

MCSが時刻同期設定を変更しないようにするには、マスターイメージで以下のレジストリ設定の値を設定します。

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- 名前: TimeSyncMethodKeep
- 種類: DWORD
- 0（または、値TimeSyncMethodKeepが構成されていない場合）：元の時刻同期設定を保持しません。
- 1: 元の時刻同期設定とデフォルトのパラメーター値を保持します。

カスタムプロパティの設定に関する重要な考慮事項

GCPおよびAzure環境では、`New-ProvScheme`と`Set-ProvScheme`でカスタムプロパティを正しく設定する必要があります。存在しないカスタムプロパティを指定すると、以下のエラーメッセージが表示され、コマンドは実行に失敗します。

- Azureの場合: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`.
- GCPの場合: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`.

トラブルシューティング

> **重要:**

> Web Studioを使用してマシンカタログを作成した後、`Get-ProvTask` PowerShellコマンドを使用してマシンカタログ作成に関連するタスクを取得することはできません。この制限は、カタログが正常に作成されたかどうかにかかわらず、Web Studioがマシンカタログ作成後にそれらのタスクを削除するためです。

> Citrixは、サポートチームが解決策を提供できるよう、ログを収集することをお勧めします。Citrix Provisioningを使用している場合は、以下の手順でログファイルを生成します。

1. マスターイメージで、値 1 (DWORD (32 ビット) 値として) を持つ次のレジストリキーを作成します: `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. マスターイメージをシャットダウンし、スナップショットを作成します。
3. Delivery Controller で、次の PowerShell コマンドを実行します: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`。
4. そのスナップショットに基づいてカタログを作成します。
5. ハイパーバイザー上に準備用VMが作成されたら、ログインしてC:\\のルートから次のファイル（Image-prep.logとPvsVmAgentLog.txt）を抽出します。
6. マシンをシャットダウンすると、その時点で障害が報告されます。
7. イメージ準備マシンの自動シャットダウンを再度有効にするには、次の PowerShell コマンドを実行します: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`。

次のステップ

特定のクラウドサービスカタログの作成については、以下を参照してください。

- AWS カタログを作成する
- XenServerカタログを作成する
- Google Cloud Platform カタログを作成する
- Microsoft Azure カタログを作成する
- Microsoft System Center Virtual Machine Manager カタログを作成する
- Nutanix カタログを作成する
- VMwareカタログを作成する

これが最初に作成するカタログである場合、Web Studioはデリバリーグループの作成を案内します。

設定プロセス全体を確認するには、インストールと構成を参照してください。

Full ConfigurationインターフェイスとPowerShellを使用して、Citrix Provisioningカタログを作成できます。 この実装には、次の利点があります。

- MCSとCitrix Provisioningカタログの両方を管理するための単一の統合コンソール。
- ID管理ソリューション、オンデマンドプロビジョニングなど、Citrix Provisioningカタログの新機能があります。

現在、この機能はAzureワークロードでのみ利用可能です。詳細については、「」を参照してください。(/ja-jp/provisioning/current-release/configure/citrix-provisioning-catalog-in-studio).

詳細情報

- 接続とリソースの作成および管理
- 異なる参加タイプのカタログを作成する
- マシンカタログの管理

AWSカタログを作成する

マシンカタログを作成するウィザードについては、(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html)で説明しています。以下の情報では、AWS仮想化環境に固有の詳細について説明します。

> **注:**
>
> AWSカタログを作成する前に、AWSへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections/connection-aws.html)を参照してください。

制限事項

Citrix Virtual Apps and Desktops™ 2203 LTSR以降では、MCS AWSプラグインが `DescribeInstanceTypes` AWS APIコールを実行し、それが成功すると、MCSはAPI応答から作成されたインベントリ名を使用します。

したがって、CVAD 1912から2203以降にアップグレードする場合は、AWSで `DefineInstanceType` 権限を無効にし、 `Set-ProvScheme` コマンドを使用して既存のカタログを更新してAWSの命名スキームに合わせます。その後、カタログの更新が完了し、サービス提供がAWSの命名スキームと一致したら、 `DescribeInstanceType` 権限を再度追加します。

イメージ準備中のネットワーク設定

イメージ準備中に、元のVMに基づいて準備用仮想マシン（VM）が作成されます。この準備用VMはネットワークから切断されます。準備用VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。このネットワークセキュリティグループは永続化され、再利用されます。ネットワークセキュリティグループの名前は `Citrix.XenDesktop.IsolationGroup-GUID` で、GUIDはランダムに生成されます。

AWSテナンシーの構成

AWSは以下のテナンシーオプションを提供します。

- 共有テナンシー（デフォルトタイプ）：異なる顧客の複数のAmazon EC2インスタンスが、同じ物理ハードウェア上に存在する場合があります。
- 専用テナンシー：お客様のEC2インスタンスは、お客様が展開した他のインスタンスと同じハードウェア上でのみ実行されます。他の顧客は同じハードウェアを使用しません。

PowerShellを使用して、MCSでAWS専用ホストをプロビジョニングできます。

PowerShellを使用したAWS専用ホストテナンシーの構成

PowerShell を使用してホストテナンシーが定義されたマシンカタログを作成できます。

Amazon 専用ホストは、インスタンス容量を持つ物理サーバーであり、完全に専用であるため、既存のソケットごとまたはVMごとのソフトウェアライセンスを使用できます。

専用ホストには、インスタンスタイプに基づいて事前設定された利用率があります。たとえば、C4 Large インスタンスタイプの単一の割り当て済み専用ホストは、16 インスタンスの実行に制限されます。詳細については、AWS サイト を参照してください。

AWSホストへのプロビジョニングの要件は次のとおりです。

- インポートされたBYOL（bring your own license）イメージ（AMI）。専用ホストでは、既存のライセンスを使用および管理します。
- プロビジョニング要求を満たすのに十分な利用率を持つ専用ホストの割り当て。
- **自動配置**を有効にします。

PowerShell を使用して AWS の専用ホストにプロビジョニングするには、**New-ProvScheme** コマンドレットをパラメータ `TenancyType` を *Host* に設定して使用します。

詳細については、Citrix Developer Documentation を参照してください。

AMI からマシンプロパティをキャプチャする

AWS で Machine Creation Services (MCS) を使用してマシンをプロビジョニングするためのカタログを作成する場合、そのカタログのマスター/ゴールデンイメージを表す AMI を選択します。その AMI から、MCS はディスクのスナップショットを使用します。以前のリリースでは、マシンにロールやタグを付けたい場合、AWS コンソールを使用して個別に設定していました。この機能はデフォルトで有効になっています。

> **ヒント:**
>
> AWS インスタンスプロパティのキャプチャを使用するには、AMI に関連付けられた VM が必要です。

> このプロセスを改善するために、**MCS は** AMI が取得されたインスタンスからプロパティを読み取り、そのマシンの Identity Access Management (IAM) ロールとタグを、特定のカタログ用にプロビジョニングされたマシンに適用します。このオプション機能を使用する場合、カタログ作成プロセスは選択された AMI ソースインスタンスを見つけ、限られたプロパティセットを読み取ります。これらのプロパティは AWS 起動テンプレートに保存され、そのカ

> タログのマシンをプロビジョニングするために使用されます。カタログ内のすべてのマシンは、キャプチャされたインスタンスプロパティを継承します。

キャプチャされるプロパティには以下が含まれます。

- IAM ロール – プロビジョニングされたインスタンスに適用されます。
- タグ - プロビジョニングされたインスタンス、そのディスク、および NIC に適用されます。これらのタグは、S3 バケットとオブジェクト、AMI、スナップショット、起動テンプレートなど、一時的な Citrix® リソースに適用されます。

> **ヒント:**
>
> 一時的なCitrixリソースのタグ付けはオプションであり、カスタムプロパティ `AwsOperationalResourcesTagging` を使用して構成できます。

AWS インスタンスプロパティをキャプチャする

AWSホスティング接続のプロビジョニングスキームを作成する際に、カスタムプロパティ `AwsCaptureInstanceProperties` を指定することで、この機能を使用できます。

`New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true" …<standard provscheme parameters`

詳細については、Citrix Developer Documentationを参照してください。

> **注:**
>
> `AwsCaptureInstanceProperties` は非推奨です。

マシンプロファイルからマシンプロパティをキャプチャする

MCSを使用してAWSマシンをプロビジョニングするためのカタログを作成する際、マシンプロファイルを使用して特定のマシンプロパティ設定をプリセットできます。

そのためには、以下の手順に従ってください。

1. このカタログを作成するリソースと同じアベイラビリティゾーンにマシンプロファイルを保存します。

2. カタログ作成ウィザードの**マシンテンプレート**ページで、**マシンプロファイルを使用**を選択します。選択したリソースと同じ利用可能なゾーンにあるマシンプロファイルが表示されます。
3. 必要に応じてマシンプロファイルを選択します。

> **注:**
>
> マシンプロファイルまたはAMIのいずれかを使用して、マシンプロパティをキャプチャできます。Web Studioで**マシンプロファイルを使用**を選択すると、**仮想マシンにマシンテンプレートプロパティを適用**オプションは自動的に非表示になります。

AWS運用リソースのタグ付け

MCSを使用してAWSでマシンをプロビジョニングするためのカタログを作成する際、IAMロールとタグプロパティをそれらのマシンに適用するかどうかを制御できます。また、マシンタグを運用リソースに適用するかどうかも制御できます。

Amazon Machine Image (AMI) は、Amazon Cloud環境内で仮想マシンを作成するために使用される仮想アプライアンスの一種で、一般にEC2と呼ばれます。AMIを使用して、EC2環境を使用するサービスを展開します。AWS向けMCSを使用してマシンをプロビジョニングするためのカタログを作成する際、そのカタログのゴールデンイメージとして機能する**AMI**を選択します。

> **重要:**
>
> 運用リソースのタグ付けを使用するには、インスタンスプロパティと起動テンプレートをキャプチャしてカタログを作成する必要があります。

> AWSカタログを作成するには、まずゴールデンイメージとするインスタンスのAMIを作成する必要があります。MCSはそのインスタンスからタグを読み取り、起動テンプレートに組み込みます。その後、起動テンプレートのタグは、AWS環境で作成されたすべてのCitrixリソースに適用されます。これには以下が含まれます。

- 仮想マシン
- VMディスク
- VMネットワークインターフェイス
- S3バケット
- S3オブジェクト

- 起動テンプレート
- AMI

運用リソースにタグを付ける

PowerShell を使用してリソースにタグを付けるには：

1. DDC ホストから PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、コマンド `asnp citrix` を実行します。

プロビジョニングされた VM のリソースにタグを付けるには、新しいカスタムプロパティ `AwsOperationalResourcesTagging` を使用します。このプロパティの構文は次のとおりです:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true" …<standard provscheme parameters>
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studio は デリバリーグループを作成するように案内します。
- 構成プロセス全体を確認するには、インストールと構成 を参照してください。
- カタログを管理するには、マシンカタログの管理 および AWS カタログの管理 を参照してください。

VM上のタグをコピーする

マシンプロファイルで指定されている NIC とディスク（ID ディスク、ライトバックキャッシュディスク、OS ディスク）のタグを、MCS マシンカタログで新しく作成された VM にコピーできます。これらのタグは、マシンプロファイルの任意のソース（AWS VM インスタンスまたは AWS 起動テンプレートバージョン）で指定できます。この機能は、永続的および非永続的なマシンカタログと VM に適用されます。

> **注:**
>
> - AWS EC2 コンソールでは、**起動テンプレートバージョンのリソースタグ**の下に**ネットワークインターフェイスのタグ**の値を確認できません。ただし、PowerShell コマンド `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` を実行してタグの仕様を確認できます。

- マシンプロファイルのソース（VMまたは起動テンプレートバージョン）に2つのネットワークインターフェイス（eni-1とeni-2）があり、eni-1にタグt1、eni-2にタグt2がある場合、VMは両方のネットワークインターフェイスのタグを取得します。

マシンプロファイルを使用してカタログを作成する

AWSでMachine Creation Services™ (MCS) を使用してマシンをプロビジョニングするためのカタログを作成する際、マシンプロファイルを使用してEC2インスタンス (VM) または起動テンプレートバージョンからハードウェアプロパティを取得し、プロビジョニングされたマシンに適用できるようになりました。取得されるプロパティには、例えば、EBSボリュームプロパティ、インスタンスタイプ、EBS最適化、その他のサポートされているAWS構成が含まれます。カタログを編集する際、別のVMまたは起動テンプレートを提供することで、プロビジョニングされたマシンのマシンプロファイルを変更できます。

注:

EBSボリュームプロパティは、マシンプロファイルからのみ派生します。

重要な考慮事項

MCSマシンカタログを作成する際の重要な考慮事項:

- `New-ProvScheme`および`Set-ProvScheme`コマンドでマシンハードウェアプロパティパラメータを追加すると、パラメータで指定された値がマシンプロファイル内の値を上書きします。
- `AwsCaptureInstanceProperties`を`true`として設定し、`MachineProfile`プロパティを設定しない場合、IAMロールとタグのみがキャプチャされます。
- `AwsCaptureInstanceProperties`と`MachineProfile`を同時に設定することはできません。

  **注記：

  `AwsCaptureInstanceProperties` は非推奨です。

- 以下のプロパティの値を明示的に指定する必要があります。

  - TenancyType
  - セキュリティグループ
  - NIC または仮想ネットワーク

- `AwsCaptureInstanceProperties` を有効にするか、マシンプロファイルを指定した場合にのみ、`AwsOperationalResourcesTagging` を有効にできます。

MCS マシンカタログ作成後の重要な考慮事項：

- カタログに追加された新しいVMのみが変更の影響を受けます。
- マシンプロファイルベースのカタログを非マシンプロファイルベースのカタログに変更することはできません。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してマシンカタログを作成するには：

1. **PowerShell** ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするために `asnp citrix*` を実行します。
3. まだ作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain abcdf -NamingSchemeType Numeric
```

4. New-ProvScheme コマンドを実行します。例：

```
New-ProvScheme -ProvisioningSchemeName demet-test-1

-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1

-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4

-CleanOnBoot

-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-demet-
ami.0 (ami-0ca813xxxxxx061ef).template'

-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-
east-1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).vm'
```

5. カタログの作成を完了します。詳細については、「Citrix PowerShell SDK」を参照してください。

マシンプロファイルで最初にプロビジョニングされたカタログのマシンプロファイルを更新するには:

1. `Set-ProvScheme` コマンドを実行します。例：

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

起動テンプレートバージョンでカタログを作成する

起動テンプレートバージョンをマシンプロファイルの入力として使用して、MCS マシンカタログを作成できます。また、マシンプロファイルカタログの入力を、VM から起動テンプレートバージョンへ、および起動テンプレートバージョンから VM へと更新することもできます。

AWS EC2 コンソールでは、起動テンプレートのインスタンス構成情報をバージョン番号とともに提供できます。マシンカタログの作成または更新時に、起動テンプレートバージョンをマシンプロファイルの入力として指定すると、その起動テンプレートバージョンのプロパティがプロビジョニングされた VDA VM にコピーされます。

以下のプロパティは、マシンプロファイルの入力として、または `New-ProvScheme` または `Set-ProvScheme` コマンドのパラメーターとして明示的に指定できます。これらが `New-ProvScheme` または `Set-ProvScheme` コマンドで提供された場合、これらのプロパティのマシンプロファイル値よりも優先されます。

- サービスオファリング
- ネットワーク
- セキュリティグループ
- テナンシータイプ

> **注:**

サービス提供がマシンプロファイルの起動テンプレートで提供されていない場合、または `New-ProvScheme` コマンドのパラメーターとして提供されていない場合、適切なエラーが発生します。

起動テンプレートバージョンをマシンプロファイルの入力として使用してカタログを作成するには：

1. **PowerShell** ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. 起動テンプレートの起動テンプレートバージョンの一覧を取得します。例：

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. 作成されていない場合は、ID プールを作成します。例：

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. 起動テンプレートバージョンをマシンプロファイルの入力として使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
```

```
-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

サービス提供、セキュリティグループ、テナンシー、ネットワークなどのパラメータを上書きすることもできます。例：

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid " c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid " bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxx).launchtemplate\lt-01xxxx (1).launchtemplateversion" `

-ServiceOffering "XDHyp:\HostingUnits\xxxd-ue1a\T3 Large
Instance.serviceoffering"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例：

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `
```

```
-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. カタログの作成を完了します。詳細については、Citrix PowerShell SDKを参照してください。

マシンプロファイルカタログの入力を、VMから起動テンプレートバージョンへ、または起動テンプレートバージョンからVMへ更新することもできます。例:

- マシンプロファイルカタログの入力をVMから起動テンプレートバージョンに更新するには:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx
(1).launchtemplateversion"
```

- マシンプロファイルカタログの入力を起動テンプレートバージョンからVMに更新するには:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

VMインスタンスのフィルタリング

マシンプロファイルVMとして使用するAWS EC2インスタンスは、マシンカタログが正しく作成され機能するために互換性がある必要があります。マシンプロファイルの入力VMとして使用できるAWS EC2インスタンスを一覧表示するには、`Get-HypInventoryItem`コマンドを使用できます。このコマンドは、ホスティングユニットで利用可能なVMのインベントリをページングおよびフィルタリングできます。

ページネーション:

Get-HypInventoryItemは、2つのページネーションモードをサポートしています。

- ページングモードでは、`-MaxRecords`と`-Skip`パラメーターを使用してアイテムのセットを返します。
  - `-MaxRecords`：デフォルトは**1**です。これは、返すアイテムの数を制御します。

  - `-Skip`：デフォルトは**0**です。これは、ハイパーバイザー内のリストの絶対的な先頭（または絶対的な末尾）からスキップするアイテムの数を制御します。

- スクロールモードでは、`-MaxRecords`、`-ForwardDirection`、および`-ContinuationToken`パラメーターを使用してレコードのスクロールを可能にします。

  - `-ForwardDirection`：デフォルトは**True**です。これは、`-MaxRecords`とともに使用され、一致するレコードの次のセットまたは前のセットのいずれかを返します。
  - `-ContinuationToken`: `ContinuationToken`で指定された項目を含まず、その直後（または`ForwardDirection`が**false**の場合は直前）の項目を返します。

ページネーションの例:

- 最も名前の小さいマシンテンプレートの単一レコードを返します。`AdditionalData` フィールドには `TotalItemsCount` と `TotalFilteredItemsCount` があります。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- 最も名前が小さいマシンテンプレートのレコードを10件返すには:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- 最も名前が大きいレコードで終わるレコードの配列を返すには:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- 指定された`ContinuationToken`に関連付けられたマシンテンプレートから始まるレコードの配列を返すには:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

フィルタリング:

フィルタリングには、以下の追加のオプションパラメータがサポートされています。これらのパラメータは、ページネーションオプションと組み合わせることができます。

- `-ContainsName "my_name"`: 指定された文字列がAMI名の一部と一致する場合、そのAMIは`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: AMIがこれらのタグの少なくとも1つを持っている場合、それは`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

> **注:**
>
> 2つのタグ値がサポートされています。**タグなし**タグ値は、タグのリストに指定されたタグがない項目と一致します。**すべての値**タグ値は、タグの値に関係なくタグを持つ項目と一致します。それ以外の場合、一致は、項目がタグを持ち、その値がフィルターで指定されたものと等しい場合にのみ発生します。

- `-Id "ami-0a2d913927e0352f3"`: AMIが指定されたIDと一致する場合、それは`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

AdditionalDataパラメーターでのフィルタリング:

`AdditionalData`フィルターパラメーターは、テンプレートまたはVMを、その機能、サービス提供、またはAdditionalDataにある任意のプロパティに基づいてリストします。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

互換性のないVMを示すために、`-Warn` パラメーターを追加することもできます。VMには、**Warning**という名前の`AdditionalData`フィールドが含まれます。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

詳細情報

- 接続とリソースの作成および管理
- AWSへの接続
- マシンカタログの作成

XenServer® カタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html) には、マシンカタログを作成するウィザードについて説明されています。以下の情報は、XenServer 仮想化環境に固有の詳細を扱っています。

> **注:**
>
> XenServer カタログを作成する前に、XenServer への接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections/connection-citrix-hypervisor.html) を参照してください。

XenServer 接続を使用してマシンカタログを作成する

GPU 対応マシンには、専用のマスターイメージが必要です。これらの VM には、GPU をサポートするビデオカードドライバーが必要です。GPU 対応マシンを構成して、VM が GPU を使用するソフトウェアで動作できるようにします。

1. XenCenter® で、標準 VGA、ネットワーク、および vCPU を備えた VM を作成します。
2. VM 構成を更新して、GPU の使用（パススルーまたは vGPU のいずれか）を有効にします。
3. サポートされているオペレーティングシステムをインストールし、RDP を有効にします。
4. Citrix VM Tools と NVIDIA ドライバーをインストールします。
5. Virtual Network Computing (VNC) Admin Console をクリアしてパフォーマンスを最適化し、VM を再起動します。

6. RDP を使用するように求められます。RDP を使用して VDA をインストールし、VM を再起動します。
7. オプションで、他の GPU マスターイメージのベースラインテンプレートとして、VM のスナップショットを作成します。
8. RDP を使用して、XenCenter で構成され、GPU 機能を使用する顧客固有のアプリケーションをインストールします。

制限事項

- Citrix Virtual Apps and Desktops展開で、Citrix Hypervisor 8.2でホストされているVMが単一のMCSカタログで複数のGFS2 SRを使用している場合、カタログ内のVMは展開中にVDIにアクセスできません。「VDI is currently in use」というエラーが報告されます。
- XenServerは、GFS2 SRを使用したMCSフルクローンVMをサポートしていません。

詳細については、「制約事項」を参照してください。

マシンプロファイルを使用してマシンカタログを作成する

MCSを使用してマシンをプロビジョニングするためのカタログを作成するときに、マシンプロファイルを使用して仮想マシンからハードウェアプロパティをキャプチャし、カタログ内の新しくプロビジョニングされたVMに適用できます。`MachineProfile`パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージVMまたはスナップショットからキャプチャされます。

> **注:**
>
> 現在、マシンプロファイルの入力として使用できるのは VM のみです。

> マシンプロファイルの入力にあるパラメータの値を上書きするために、以下のパラメータを明示的に構成できます。

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

マシンプロファイルを使用してカタログを作成するには：

1. PowerShellウィンドウを開きます。

2. `asnp citrix*`を実行します。
3. IDプールを作成します。IDプールは、作成するVMのActive Directory (AD) アカウントのコンテナです。例：

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -IdentityPoolName
"ExampleIdentityPool" -NamingScheme "abc1-##" -NamingSchemeType
"Numeric" -Scope @() -ZoneUid "xxxxxxxx"
```

4. 必要なADコンピューターアカウントをActive Directoryに作成します。

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -Force

New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count 10
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. カタログを作成するには、`New-ProvScheme`コマンドを実行します。例：

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
-IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

</CustomProperties>'

-MasterImageVM "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleVDA.vm\ExampleVDA.snapshot"
-ProvisioningSchemeName "ExampleCatalog" -Scope @() -SecurityGroup @()

-MachineProfile "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfile.vm"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例：

```
$ConfigZone = Get-ConfigZone | Where-Object { $_.Name -eq "xxxxxx" }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -Description
"Machine profile catalog" -ProvisioningSchemeId fe7df345-244e-4xxxx-
xxxxxxxxx -ProvisioningType Mcs -SessionSupport MultiSession
-PersistUserChanges Discard -ZoneUid ($ConfigZone.Uid)
```

7. カタログにVMを追加します。

新しいマシンプロファイルでカタログを更新するには：

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -MachineProfile
"XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfileVm.vm\ExampleMach
ineProfileSnapshot.snapshot"
```

Set-ProvSchemeコマンドの詳細については、「Set-ProvScheme」を参照してください。

注：

- この場合、`Set-ProvScheme`コマンドはカタログ内の既存のVMのマシンプロファイルを変更しません。カタログに追加された新しく作成されたVMのみが新しいマシンプロファイルを持ちます。
- マシンプロファイルベースのマシンカタログを、非マシンプロファイルベースのマシンカタログに変換することはできません。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください。
- カタログを管理するには、「マシンカタログの管理」および「XenServerカタログの管理」を参照してください。

詳細情報

- 接続とリソースの作成および管理(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections.html)
- XenServerへの接続(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections/connection-citrix-hypervisor.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html)

Google Cloud Platformカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html)は、マシンカタログを作成するウィザードについて説明しています。以下の情報は、Google Cloud環境に固有の詳細を扱っています。

> **注:**
>
> Google Cloud Platform (GCP) カタログを作成する前に、GCPへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections/connection-gcp.html)を参照してください。

マスターVMインスタンスと永続ディスクを準備する

> **ヒント:**
>
> 永続ディスクは、仮想ディスクを指すGoogle Cloudの用語です。

マスターVMインスタンスを準備するには、計画しているマシンカタログ内のクローンVDAインスタンスに求める構成と一致するプロパティを持つVMインスタンスを作成および構成します。この構成は、インスタンスのサイズとタイプにのみ適用されるわけではありません。メタデータ、タグ、GPU割り当て、ネットワークタグ、サービスアカウントのプロパティなどのインスタンス属性も含まれます。

マスタリングプロセスの一環として、MCSはマスターVMインスタンスを使用してGoogle Cloudの*インスタンステンプレート*を作成します。このインスタンステンプレートは、マシンカタログを構成するクローンVDAインスタンスの作成に使用されます。クローンインスタンスは、インスタンス

テンプレートが作成されたマスターVMインスタンスのプロパティ（VPC、サブネット、永続ディスクのプロパティを除く）を継承します。

マスターVMインスタンスのプロパティを特定の要件に合わせて構成した後、インスタンスを起動し、そのインスタンスの永続ディスクを準備します。

ディスクのスナップショットを手動で作成することをお勧めします。これにより、意味のある命名規則を使用してバージョンを追跡し、マスターイメージの以前のバージョンを管理するためのより多くのオプションが得られ、マシンカタログ作成の時間を節約できます。独自のスナップショットを作成しない場合、MCSが一時的なスナップショットを作成します（これはプロビジョニングプロセスの終了時に削除されます）。

マシンカタログを作成する

マシンカタログは、次の2つの方法で作成できます。

- (/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-gcp.html#create-a-machine-catalog-using-web-studio)を使用してマシンカタログを作成する
- (/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-gcp.html#create-a-machine-catalog-using-powershell)を使用してマシンカタログを作成する

Web Studio を使用してマシンカタログを作成する

> **注:**

> マシンカタログを作成する前に、リソースを作成してください。マシンカタログを構成する際は、Google Cloud が定めた命名規則を使用してください。詳細については、バケットとオブジェクトの命名ガイドラインを参照してください。

> (/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html)のガイダンスに従ってください。以下の説明は、Google Cloud カタログに固有のものです。

1. Web Studio にサインインし、左側のペインで を選択します。
2. アクションバーで を選択します。
3. ページで、 を選択し、 を選択します。
    - Citrix Virtual Apps and Desktops™ は、シングルセッションOSもサポートしています。

4. ページで、 と オプションを選択し、 を選択します。複数のリソースがある場合は、メニューから1つ選択します。
5. 「**マスターイメージ**」ページで、必要に応じてこれらの手順を完了し、「**次へ**」をクリックします。

   a. スナップショットまたはVMをマスターイメージとして選択します。単一テナンシー機能を使用する場合は、ノードグループプロパティが正しく構成されているイメージを選択してください。「ゾーン選択の有効化」を参照してください。

   b. 既存のVMをマシンプロファイルとして使用するには、 を選択し、そのVMを選択します。

   > **注:**
   >
   > 現在、このカタログ内のVMは、ディスク暗号化セットID、マシンサイズ、ストレージタイプ、およびゾーン設定をマシンプロファイルから継承します。

   c. カタログの最小機能レベルを選択します。単一テナンシー機能を使用する場合は、ノードグループプロパティが正しく構成されているイメージを選択してください。

6. ページで、このマシンカタログのオペレーティングシステムを格納するために使用するストレージの種類を選択します。以下の各ストレージオプションには、独自の価格とパフォーマンス特性があります。（IDディスクは常にゾーン標準永続ディスクを使用して作成されます。）

   - 標準永続ディスク
   - バランス永続ディスク
   - SSD永続ディスク

   Google Cloud のストレージオプションの詳細については、`<https://cloud.google.com/compute/docs/disks/>`を参照してください。

7. 「**仮想マシン**」ページで、作成するVMの数を指定し、VMの詳細な仕様を表示して、「**次へ**」を選択します。マシンカタログに単一テナントノードグループを使用する場合は、予約済みの単一テナントノードが利用可能なゾーンを**のみ**選択するようにしてください。「」(#enable-zone-selection)を参照してください。
8. 「**コンピューターアカウント**」ページで、Active Directoryアカウントを選択し、「**次へ**」を選択します。

   - 「**新しいActive Directoryアカウントを作成**」を選択した場合、ドメインを選択し、Active Directoryで作成されるプロビジョニングされたVMコンピューターアカウントの命名スキー

ムを表す文字のシーケンスを入力します。アカウントの命名スキームは1〜64文字で、空白、非ASCII文字、または特殊文字を含めることはできません。

- 「**既存のActive Directoryアカウントを使用**」を選択した場合、「**参照**」を選択して、選択したマシンの既存のActive Directoryコンピューターアカウントに移動します。

9. 「**ドメイン資格情報**」ページで、「**資格情報を入力**」を選択し、ユーザー名とパスワードを入力して、「**保存**」を選択し、「**次へ**」を選択します。

   - 入力する資格情報には、Active Directoryアカウント操作を実行する権限が必要です。

10. 「**概要**」ページで、情報を確認し、カタログの名前を指定して、「**完了**」を選択します。

> **注:**
>
> カタログ名は1〜39文字で、空白のみ、または次の文字を含めることはできません `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`。

マシンカタログの作成には時間がかかる場合があります。マシンがターゲットノードグループに作成されていることを確認するには、Google Cloudコンソールに移動します。

手動で作成されたGoogle Cloudマシンをインポートする

Google Cloudへの*接続を作成*し、その後、Google Cloudマシンを含む*カタログを作成*できます。その後、Citrix Virtual Apps and Desktopsを介してGoogle Cloudマシンを手動で電源サイクルできます。この機能を使用すると、次のことができます。

- 手動で作成されたGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsマシンカタログにインポートする。
- 手動で作成されたGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsカタログから削除する。
- 既存のCitrix Virtual Apps and Desktopsの電源管理機能を使用して、Google Cloud WindowsマルチセッションOSマシンの電源を管理する。たとえば、それらのマシンの再起動スケジュールを設定する。

この機能は、既存のCitrix Virtual Apps and Desktopsのプロビジョニングワークフローに変更を加えたり、既存の機能を削除したりする必要はありません。手動で作成されたGoogle Cloudマシンをインポートする代わりに、Web StudioでMCSを使用してマシンをプロビジョニングすることをお勧めします。

共有仮想プライベートクラウド

共有仮想プライベートクラウド（VPC）は、共有サブネットが利用可能になるホストプロジェクトと、そのリソースを使用する1つ以上のサービスプロジェクトで構成されます。共有VPCは、共有企業Googleクラウド資産の一元的な制御、使用、および管理を提供するため、大規模なインストールに適したオプションです。詳細については、Googleドキュメントサイトを参照してください。

この機能により、Machine Creation Services（MCS）は、共有VPCに展開されたマシンカタログのプロビジョニングと管理をサポートします。このサポートは、現在ローカルVPCで提供されているサポートと機能的に同等ですが、次の2つの点で異なります。

1. ホスト接続の作成に使用されるサービスアカウントに追加の権限を付与する必要があります。このプロセスにより、MCSは共有VPCリソースにアクセスして使用できるようになります。
2. イングレス用とエグレス用にそれぞれ1つずつ、2つのファイアウォールルールを作成する必要があります。これらのファイアウォールルールは、イメージマスタリングプロセス中に使用されます。

必要な新しい権限

ホスト接続を作成する際には、特定の権限を持つGoogle Cloudサービスアカウントが必要です。これらの追加権限は、共有VPCベースのホスト接続の作成に使用されるすべてのサービスアカウントに付与する必要があります。

> **ヒント:**
>
> これらの追加の権限は、Citrix Virtual Apps and Desktopsにとって新しいものではありません。これらはローカルVPCの実装を容易にするために使用されます。共有VPCでは、これらの追加の権限により、他の共有VPCリソースへのアクセスが可能になります。

> Shared VPCをサポートするために、ホスト接続に関連付けられたサービスアカウントに最大4つの追加権限を付与する必要があります。

1. **compute.firewalls.list** - この権限は必須です。これにより、MCSはShared VPCに存在するファイアウォールルールのリストを取得できます。
2. **compute.networks.list** - この権限は必須です。これにより、MCSはサービスアカウントが利用できるShared VPCネットワークを識別できます。
3. **compute.subnetworks.list** – この権限は、VPCの使用方法によってオプションです。これにより、MCSは可視のShared VPC内のサブネットを識別できます。この権限はローカルVPCを

使用する際にはすでに必要ですが、Shared VPCホストプロジェクトでも割り当てる必要があります。

4. **compute.subnetworks.use** - この権限は、VPCの使用方法によってオプションです。プロビジョニングされたマシンカタログでサブネットリソースを使用するために必要です。この権限はローカルVPCを使用する際にはすでに必要ですが、Shared VPCホストプロジェクトでも割り当てる必要があります。

これらの権限を使用する際には、マシンカタログの作成に使用される権限の種類に基づいて異なるアプローチがあることを考慮してください。

- プロジェクトレベルの権限:
  - ホストプロジェクト内のすべてのShared VPCへのアクセスを許可します。
  - 権限 #3 と #4 をサービスアカウントに割り当てる必要があります。
- サブネットレベルの権限:
  - Shared VPC内の特定のサブネットへのアクセスを許可します。
  - 権限 #3 と #4 はサブネットレベルの割り当てに固有のものであるため、サービスアカウントに直接割り当てる必要はありません。

組織のニーズとセキュリティ基準に合ったアプローチを選択してください。

> **ヒント:**
>
> プロジェクトレベルとサブネットレベルの権限の違いの詳細については、Google Cloud ドキュメントを参照してください。

ファイアウォールルール

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンにアタッチされます。このVMは、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する分離された環境で実行する必要があります。これは、インバウンドトラフィック用とアウトバウンドトラフィック用の2つのすべて拒否ファイアウォールルールによって実現されます。Google CloudローカルVPCを使用する場合、MCSはこのファイアウォールをローカルネットワークに作成し、マスタリング用のマシンに適用します。マスタリングが完了すると、ファイアウォールルールはイメージから削除されます。

共有VPCを使用するために必要な新しい権限の数を最小限に抑えることをお勧めします。共有VPCはより上位の企業リソースであり、通常、より厳格なセキュリティプロトコルが導入されています。このため、ホストプロジェクトの共有VPCリソースに、イングレス用とエグレス用の2つのファイアウォールルールを作成してください。それらに最高の優先順位を割り当てます。次の値を使用して、これらの各ルールに新しいターゲットタグを適用します。

`citrix-provisioning-quarantine-firewall`

MCSがマシンカタログを作成または更新すると、このターゲットタグを含むファイアウォールルールを検索します。次に、ルールの正確性を確認し、カタログのマスターイメージを準備するために使用されるマシンに適用します。ファイアウォールルールが見つからない場合、またはルールは見つかったものの、ルールまたはその優先順位が正しくない場合は、次のようなメッセージが表示されます。

`"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. " Please ensure you have created 'deny all' firewall rules with the network tag 'citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."`

共有 VPC の構成

Web Studioで共有VPCをホスト接続として追加する前に、プロビジョニングするプロジェクトからサービスアカウントを追加するために、次の手順を完了します。

1. IAMロールを作成します。
2. CVADホスト接続の作成に使用されるサービスアカウントを、共有VPCホストプロジェクトのIAMロールに追加します。
3. プロビジョニングするプロジェクトのCloud Buildサービスアカウントを、共有VPCホストプロジェクトのIAMロールに追加します。
4. ファイアウォールルールを作成します。

IAMロールを作成する

ロールのアクセスレベルを決定します — *プロジェクトレベルアクセス*、またはより制限されたモデルである *サブネットレベルアクセス* を使用します。

IAMロールのプロジェクトレベルアクセス。プロジェクトレベルのIAMロールには、次の権限を含めます。

- compute.firewalls.list
- compute.networks.list

- compute.subnetworks.list
- compute.subnetworks.use

プロジェクトレベルのIAMロールを作成するには：

1. Google Cloud コンソールで、**IAM と管理 > ロール**に移動します。
2. **ロール**ページで、**ロールを作成**を選択します。
3. **ロールの作成**ページで、ロール名を指定します。**権限を追加**を選択します。
    a. **権限の追加**ページで、ロールに個別に権限を追加します。権限を追加するには、**テーブルをフィルタリング**フィールドに権限の名前を入力します。権限を選択し、**追加**を選択します。
    b. **作成**を選択します。

サブネットレベルのIAMロール。このロールは、**ロールを作成**を選択した後に、権限`compute.subnetworks.list`と`compute.subnetworks.use`の追加を省略します。このIAMアクセスレベルの場合、権限`compute.firewalls.list`と`compute.networks.list`を新しいロールに適用する必要があります。

サブネットレベルのIAMロールを作成するには：

1. Google Cloud コンソールで、**VPC ネットワーク** > **共有 VPC**に移動します。**共有 VPC**ページが表示され、ホストプロジェクトに含まれる共有 VPC ネットワークのサブネットが表示されます。
2. **共有 VPC**ページで、アクセスしたいサブネットを選択します。
3. 右上隅で、サービスアカウントを追加するために**メンバーを追加**を選択します。
4. 「**メンバーを追加**」ページで、次の手順を実行します。
    a. 「**新しいメンバー**」フィールドにサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. 「**ロールを選択**」フィールドを選択し、「**Compute Network User**」を選択します。
    c. 「**保存**」を選択します。
5. Google Cloud コンソールで、「**IAM と管理**」>「**ロール**」に移動します。
6. 「**ロール**」ページで、「**ロールを作成**」を選択します。
7. 「**ロールを作成**」ページで、ロール名を指定します。「**権限を追加**」を選択します。

a. 「**権限を追加**」ページで、ロールに権限を個別に追加します。権限を追加するには、「**テーブルをフィルタ**」フィールドに権限の名前を入力します。権限を選択し、「**追加**」を選択します。

b. 「**作成**」を選択します。

ホストプロジェクトのIAMロールにサービスアカウントを追加する

IAMロールを作成したら、ホストプロジェクトのサービスアカウントを追加するために次の手順を実行します。

1. Google Cloud コンソールで、ホストプロジェクトに移動し、次に「**IAM と管理 > IAM**」に移動します。
2. 「**IAM**」ページで、「**追加**」を選択してサービスアカウントを追加します。
3. 「**メンバーを追加**」ページで：

   a. 「**新しいメンバー**」フィールドにサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。

   b. 「ロール」フィールドを選択し、作成したIAMロールを入力して、メニューからそのロールを選択します。

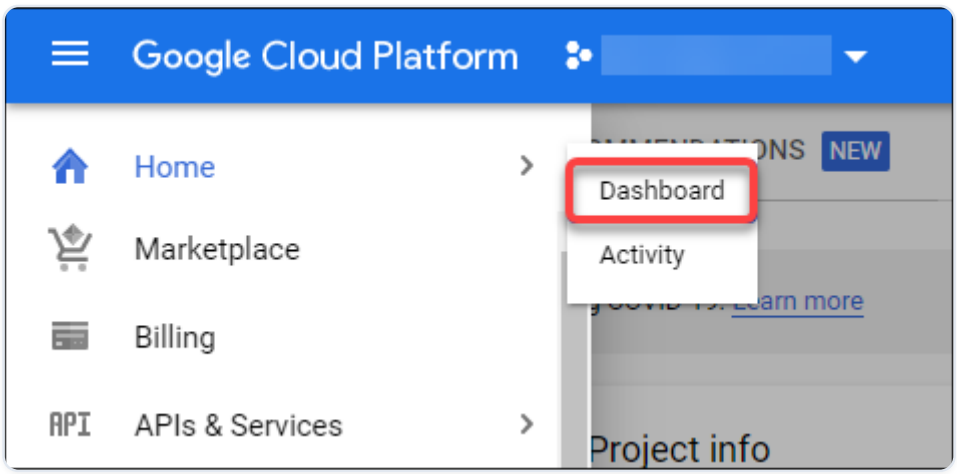
   c. を選択します。

これで、サービスアカウントがホストプロジェクト用に構成されました。

クラウドビルドサービスアカウントを共有VPCに追加する

すべてのGoogle Cloudサブスクリプションには、プロジェクトID番号の後に `cloudbuild.gserviceaccount` が続くサービスアカウントがあります。例: `705794712345@cloudbuild.gserviceaccount`。

Google Cloudコンソールで と を選択すると、プロジェクトのプロジェクトID番号を確認できます。



画面の 領域の下にある を見つけます。

クラウドビルドサービスアカウントを共有VPCに追加するには、次の手順を実行します。

1. Google Cloudコンソールで、ホストプロジェクトに移動し、 > に移動します。
2. ページで、 を選択してアカウントを追加します。
3. ページで、次の手順を実行します。
    a. フィールドに、Cloud Buildサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. フィールドを選択し、`Computer Network User`と入力して、メニューからそのロールを選択します。
    c. を選択します。

ファイアウォールルールを作成する

マスタリングプロセスの一環として、MCS は選択されたマシンイメージをコピーし、それを使用してカタログ用のマスターイメージシステムディスクを準備します。マスタリング中、MCS はディスクを一時的な仮想マシンに接続し、その仮想マシンが準備スクリプトを実行します。この VM は、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを禁止する分離された環境で実行する必要があります。分離された環境を作成するために、MCS は2つの *すべて拒否* ファイアウォールルール（イングレスルールとエグレスルール）を必要とします。したがって、*ホストプロジェクト* に次の2つのファイアウォールルールを作成します。

1. Google Cloud コンソールで、ホストプロジェクトに移動し、次に **VPC network > Firewall** に移動します。
2. **ファイアウォール** ページで、**ファイアウォールルールを作成** を選択します。
3. **ファイアウォールルールを作成** ページで、以下を完了します。
    - **名前**。ルールの名前を入力します。
    - **ネットワーク**。イングレスファイアウォールルールを適用する共有 VPC ネットワークを選択します。
    - **優先度**。値が小さいほど、ルールの優先度が高くなります。小さい値（例: 10）をお勧めします。
    - **トラフィックの方向**。**イングレス** を選択します。
    - **一致時のアクション**。**拒否** を選択します。
    - **ターゲット**。デフォルトの **指定されたターゲットタグ** を使用します。
    - **ターゲットタグ**。`citrix-provisioning-quarantine-firewall` と入力します。

- **ソースフィルタ**。デフォルトの **IP 範囲** を使用します。
- **ソース IP 範囲**。すべてのトラフィックに一致する範囲を入力します。`0.0.0.0/0` と入力します。
- **プロトコルとポート**。**すべて拒否** を選択します。

4. 「**作成**」を選択してルールを作成します。
5. 手順1～4を繰り返して別のルールを作成します。「**トラフィックの方向**」には「**下り**」を選択します。

接続の追加

Google Cloud環境への接続を追加します。「接続の追加」を参照してください。

ゾーン選択を有効にする

Citrix Virtual Apps and Desktops はゾーン選択をサポートしています。ゾーン選択を使用すると、VM を作成するゾーンを指定できます。ゾーン選択を使用すると、管理者は選択したゾーンに単一テナントノードを配置できます。単一テナンシーを構成するには、Google Cloud で以下を完了する必要があります。

- Google Cloud の単一テナントノードを予約する
- VDA マスターイメージを作成する

Google Cloud の単一テナントノードを予約する

単一テナントノードを予約するには、Google Cloud のドキュメントを参照してください。

> **重要:**
>
> ノードテンプレートは、ノードグループに予約されているシステムのパフォーマンス特性を示すために使用されます。これらの特性には、vGPU の数、ノードに割り当てられるメモリ量、およびノード上に作成されるマシンに使用されるマシンタイプが含まれます。詳細については、Google Cloud のドキュメントを参照してください。

VDA マスターイメージの作成

単一テナントノードにマシンを正常に展開するには、マスターVMイメージを作成する際に追加の手順を実行する必要があります。Google Cloud上のマシンインスタンスには、*ノードアフィニティラベル*と呼ばれるプロパティがあります。単一テナントノードに展開されるカタログのマス

ターイメージとして使用されるインスタンスには、**ターゲットノードグループ**の名前と一致する*ノードアフィニティラベル*が必要です。これを実現するには、次の点に留意してください。

- 新しいインスタンスの場合、インスタンスの作成時にGoogle Cloudコンソールでラベルを設定します。詳細については、「インスタンス作成時にノードアフィニティラベルを設定する」を参照してください。
- 既存のインスタンスの場合、**gcloud** コマンドラインを使用してラベルを設定します。詳細については、既存のインスタンスのノードアフィニティラベルを設定するを参照してください。

> **注:**
>
> 共有VPCで単一テナンシーを使用する場合は、共有仮想プライベートクラウドを参照してください。

インスタンス作成時にノードアフィニティラベルを設定する

ノードアフィニティラベルを設定するには：

1. Google Cloudコンソールで、**Compute Engine > VMインスタンス**に移動します。
2. **VMインスタンス**ページで、**インスタンスを作成**を選択します。
3. **インスタンスの作成**ページで、必要な情報を入力または構成し、設定パネルを開くために**管理、セキュリティ、ディスク、ネットワーク、単一テナンシー**を選択します。
4. **単一テナンシー**タブで、**参照**を選択して、現在のプロジェクトで利用可能なノードグループを表示します。**単一テナントノード**ページが表示され、利用可能なノードグループのリストが表示されます。
5. **単一テナントノード**ページで、リストから該当するノードグループを選択し、**選択**を選択して**単一テナンシー**タブに戻ります。ノードアフィニティラベルフィールドには、選択した情報が入力されます。この設定により、インスタンスから作成されたマシンカタログが選択されたノードグループに展開されることが保証されます。
6. **作成**を選択してインスタンスを作成します。

既存のインスタンスにノードアフィニティラベルを設定する

ノードアフィニティラベルを設定するには：

1. Google Cloud Shellターミナルウィンドウで、*gcloud compute instances*コマンドを使用してノードアフィニティラベルを設定します。**gcloud**コマンドに次の情報を含めます:
   - **VMの名前**。たとえば、`s*2019-vda-base`.*という既存のVMを使用します。

- **ノードグループの名前**。以前に作成したノードグループ名を使用します。たとえば、`mh-sole-tenant-node-group-1`。
- **インスタンスが存在するゾーン**。たとえば、VMは`*us-east-1b* zone`にあります。

たとえば、ターミナルウィンドウで次のコマンドを入力します。

- `gcloud compute instances set-scheduling "s2019-vda-base" --node-group="mh-sole-tenant-node-group-1" --zone="us-east1-b"`

*gcloud compute instances*コマンドの詳細については、Google Developer Toolsのドキュメント（`<https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling>`）を参照してください。

2. インスタンスの**VMインスタンスの詳細**ページに移動し、**ノードアフィニティ**フィールドにラベルが入力されていることを確認します。

マシンカタログを作成する

ノードアフィニティラベルを設定したら、マシンカタログを構成します。

顧客管理の暗号化キー（CMEK）

MCSカタログには、顧客管理の暗号化キー（CMEK）を使用できます。この機能を使用する場合、Google Cloud Key Management Serviceの`CryptoKey Encrypter/Decrypter`ロールをCompute Engineサービスエージェントに割り当てます。Citrix Virtual Apps and Desktopsアカウントは、キーが保存されているプロジェクトで適切な権限を持っている必要があります。詳細については、「Cloud KMSキーを使用してリソースを保護する」を参照してください。

Compute Engineサービスエージェントは、`service-<Project _Number>@compute-system.iam.gserviceaccount.com`の形式です。この形式は、デフォルトのCompute Engineサービスアカウントとは異なります。

> **注：**
>
> このCompute Engineサービスアカウントは、Google Consoleの**IAM権限**表示に表示されない場合があります。そのような場合は、「Cloud KMSキーを使用してリソースを保護する」で説明されているように、`gcloud`コマンドを使用してください。

Citrix Virtual Apps and Desktops アカウントに権限を割り当てる

Google Cloud KMSの権限は、さまざまな方法で構成できます。*プロジェクトレベル*のKMS権限または*リソースレベル*のKMS権限のいずれかを提供できます。詳細については、「権限とロール」を参照してください。

プロジェクトレベルの権限

1つのオプションは、Citrix Virtual Apps and Desktops アカウントに Cloud KMS リソースを参照するためのプロジェクトレベルの権限を付与することです。これを行うには、カスタムロールを作成し、次の権限を追加します。

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

このカスタムロールを Citrix Virtual Apps and Desktops に割り当てます。これにより、インベントリ内の関連プロジェクトでリージョンキーを参照できます。

リソースレベルの権限

もう1つのオプションであるリソースレベルの権限については、Google Cloudコンソールで、MCSプロビジョニングに使用する`cryptoKey`に移動します。Citrix Virtual Apps and Desktopsアカウントを、カタログプロビジョニングに使用するキーリングまたはキーに追加します。

> **ヒント:**
>
> このオプションでは、Citrix Virtual Apps and DesktopsアカウントがCloud KMSリソースに対するプロジェクトレベルのリスト権限を持っていないため、インベントリでプロジェクトのリージョンキーを参照することはできません。ただし、以下に説明する`ProvScheme`カスタムプロパティで正しい`cryptoKeyId`を指定することにより、CMEKを使用してカタログをプロビジョニングすることは可能です。

カスタムプロパティを使用した CMEK でのプロビジョニング

PowerShellを介してプロビジョニングスキームを作成する際に、`ProvScheme` `CustomProperties`で`CryptoKeyId`プロパティを指定します。例:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

`cryptoKeyId`は次の形式で指定する必要があります。

`projectId:location:keyRingName:cryptoKeyName`

例えば、キーリング `my-example-key-ring` のリージョン `us-east1` と ID `my-example-project-1` のプロジェクトで、キー `my-example-key` を使用したい場合、`ProvScheme` のカスタム設定は次のようになります。

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />

</CustomProperties>'
```

このプロビジョニングスキームに関連するすべてのMCSプロビジョニング済みディスクとイメージは、この顧客管理暗号化キーを使用します。

ヒント:

グローバルキーを使用する場合、顧客プロパティの場所は `global` と記述する必要があり、上記の例では **us-east1** である **region** 名ではありません。例: `<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`。

顧客管理キーのローテーション

Google Cloudは、既存の永続ディスクまたはイメージでのキーのローテーションをサポートしていません。マシンがプロビジョニングされると、作成時に使用されていたキーのバージョンに紐付けられます。ただし、新しいバージョンのキーを作成でき、その新しいキーは、新しくプロビ

ジョニングされたマシンや、新しいマスターイメージでカタログが更新されたときに作成されるリソースに使用されます。

キーリングに関する重要な考慮事項

キーリングの名前変更や削除はできません。また、設定時に予期せぬ料金が発生する可能性があります。キーリングを削除または削除すると、Google Cloud はエラーメッセージを表示します。

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
nor key rings are billed for, just the active key versions within the
keys.
```

ヒント:

詳細については、「コンソールからキーリングを編集または削除する」を参照してください。

均一なバケットレベルのアクセス互換性

Citrix Virtual Apps and Desktops は、Google Cloud の均一なバケットレベルのアクセス制御ポリシーと互換性があります。この機能は、ストレージバケットを含むリソースの操作を許可するためにサービスアカウントに権限を付与する IAM ポリシーの使用を強化します。均一なバケットレベルのアクセス制御により、Citrix Virtual Apps and Desktops は、ストレージバケットまたはそこに保存されているオブジェクトへのアクセスを制御するためにアクセス制御リスト (ACL) を使用することを可能にします。Google Cloud の均一なバケットレベルのアクセスに関する概要情報については、「均一なバケットレベルのアクセス」を参照してください。構成情報については、「均一なバケットレベルのアクセスを要求する」を参照してください。

PowerShell を使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について詳しく説明します。

- 永続的なライトバックキャッシュディスクを持つカタログを作成する
- MCSIO で起動パフォーマンスを向上させる
- マシンプロファイルを使用してマシンカタログを作成する
- インスタンステンプレートとしてマシンプロファイルを持つマシンカタログを作成する
- PowerShell を使用してシールドされた VM でカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShell パラメーター `New-ProvScheme` `CustomProperties` を使用します。

ヒント:

ここで PowerShell パラメーターを使用するのは、クラウドベースのホスティング接続の場合のみです。オンプレミスソリューション（XenServer® など）で永続的なライトバックキャッシュディスクを使用してマシンをプロビジョニングする場合、ディスクは自動的に永続化されるため、PowerShell は必要ありません。

このパラメーターは、MCSでプロビジョニングされたマシンに対してライトバックキャッシュディスクがどのように永続化されるかを決定するために使用される追加プロパティ `PersistWBC` をサポートします。`PersistWBC` プロパティは、`UseWriteBackCache` パラメーターが指定され、`WriteBackCacheDiskSize` パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

注:

この動作は、AzureとGCPの両方に適用され、電源サイクル時にデフォルトのMCSIOライトバックキャッシュディスクが削除され、再作成されます。ディスクの削除と再作成を避けるために、ディスクを永続化することを選択できます。

`PersistWBC` プロパティを `true` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC` プロパティを `false` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注:

`PersistWBC` プロパティが省略された場合、プロパティはデフォルトで `false` になり、管理インターフェイスからマシンがシャットダウンされるとライトバックキャッシュが削除されます。

例えば、CustomProperties パラメーターを使用して `PersistWBC` を `true` に設定する場合：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

注:

`PersistWBC` プロパティは、`New-ProvScheme` PowerShell コマンドレットを使用してのみ設定できます。プロビジョニングスキームの作成後に `CustomProperties` を変更しよう

としても、マシンカタログや、マシンのシャットダウン時のライトバックキャッシュディスクの永続性には影響しません。

例えば、`New-ProvScheme` をライトバックキャッシュを使用するように設定し、`PersistWBC` プロパティを `true` に設定する場合：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127
```

```
-WriteBackCacheMemorySize 256
```

MCSIOで起動パフォーマンスを向上させる

MCSIO が有効な場合、Azure および GCP のマネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、`New-ProvScheme` コマンドで PowerShell の `PersistOSDisk` カスタムプロパティを使用します。`New-ProvScheme` に関連するオプションは次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk` カスタムプロパティを `true` に設定します。例：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"
```
```

```
-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

マシンプロファイルを使用してマシンカタログを作成する

Machine Creation Services (MCS) を使用してマシンをプロビジョニングするカタログを作成する場合、マシンプロファイルを使用して仮想マシンからハードウェアプロパティをキャプチャし、カタログ内の新しくプロビジョニングされた VM に適用できます。`MachineProfile` パラメーターが使用されない場合、ハードウェアプロパティはマスターイメージ VM またはスナップショットからキャプチャされます。 明示的に定義する一部のプロパティ（例えば、`StorageType`、`CatalogZones`、`CryptoKeyIs`）は、マシンプロファイルから無視されます。

- マシンプロファイルを使用してカタログを作成するには、`New-ProvScheme` コマンドを使用します。例えば、`New-ProvScheme –MachineProfile "path to VM"` です。`MachineProfile` パラメーターを指定しない場合、ハードウェアプロパティはマスターイメージ VM からキャプチャされます。
- 新しいマシンプロファイルでカタログを更新するには、`Set-ProvScheme` コマンドを使用します。例えば、`Set-ProvScheme –MachineProfile "path to new VM"` です。このコマンドは、カタログ内の既存の VM のマシンプロファイルを変更しません。カタログに追加された新しく作成された VM のみが新しいマシンプロファイルを持ちます。

- マスターイメージを更新することもできますが、マスターイメージを更新してもハードウェアプロパティは更新されません。ハードウェアプロパティを更新したい場合は、`Set-ProvScheme` コマンドを使用してマシンプロファイルを更新する必要があります。これらの変更は、カタログ内の新しいマシンにのみ適用されます。既存のマシンのハードウェアプロパティを更新するには、`-StartsNow` および `-DurationInMinutes -1` パラメーターを指定して `Set-ProvVMUpdateTimeWindow` コマンドを使用できます。

  > **注:**
  >
  > - `StartsNow` は、スケジュールされた開始時刻が現在の時刻であることを示します。
  > - 負の数（例：-1）を指定した `DurationInMinutes` は、スケジュールの時間枠に上限がないことを示します。

マシンプロファイルとしてインスタンステンプレートを使用してマシンカタログを作成する

マシンプロファイルの入力としてGCPインスタンステンプレートを選択できます。インスタンステンプレートはGCPの軽量リソースであるため、非常に費用対効果が高いです。

マシンプロファイルとしてインスタンステンプレートを使用して新しいマシンカタログを作成する

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
3. 次のコマンドを使用して、GCPプロジェクト内のインスタンステンプレートを見つけます。

```
cd XDHyp:\HostingUnits\<HostingUnitName>\instanceTemplates.folder
```

4. NewProvSchemeコマンドを使用して、マシンプロファイルとしてインスタンステンプレートを持つ新しいマシンカタログを作成します。

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -HostingUnitName
<HostingUnitName> -IdentityPoolName <identity pool name> -MasterImageVM

XDHyp:\HostingUnits\<HostingUnitName> \Base.vm\Base.snapshot
-MachineProfile XDHyp:
```

```
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\mytemplate.tem
plate
```

New-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/を参照してください。

5. PowerShell コマンドを使用してマシンカタログの作成を完了します。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する詳細な手順は次のとおりです。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 次のコマンドを実行します。

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -MachineProfile
XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\<TemplateName>
.template
```

Set-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/を参照してください。

PowerShell を使用して、シールドされた VM を含むカタログを作成する

シールドされたVMプロパティを持つMCSマシンカタログを作成できます。シールドされた仮想マシンは、セキュアブート、仮想トラステッドプラットフォームモジュール、UEFIファームウェア、整合性監視などの高度なプラットフォームセキュリティ機能を使用して、Compute Engineインスタンスの検証可能な整合性を提供する一連のセキュリティ制御によって強化されています。

MCSは、マシンプロファイルワークフローを使用してカタログを作成することをサポートしています。マシンプロファイルワークフローを使用する場合、VMインスタンスのシールドされたVMプロパティを有効にする必要があります。その後、このVMインスタンスをマシンプロファイルの入力として使用できます。

マシンプロファイルワークフローを使用して、シールドされた VM を含む MCS マシンカタログを作成するには。

1. Google Cloud コンソールでVMインスタンスのシールドされたVMオプションを有効にします。クイックスタート: シールドされたVMオプションを有効にするを参照してください。
2. VMインスタンスを使用して、マシンプロファイルワークフローでMCSマシンカタログを作成します。

   a. PowerShell ウィンドウを開きます。

   b. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。

   c. まだ作成されていない場合は、IDプールを作成します。

   d. `New-ProvScheme`コマンドを実行します。例：

   ```
   New-ProvScheme -ProvisioningSchemeName <catalog-name>

   -HostingUnitName gcp-hostint-unit

   -MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm

   -MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
   machine.vm
   ```

3. マシンカタログの作成を完了します。

新しいマシンプロファイルでマシンカタログを更新するには:

1. `Set-ProvScheme`コマンドを実行します。例：

   ```
   Set-ProvScheme -ProvisioningSchemeName <catalog-name>

   -MasterImageVM XDHyp:\HostingUnits\<hostin-unit>\catalog-vda.vm

   -MachineProfile "DHyp:\HostingUnits\<hostin-unit>\catalog-machine.vm
   ```

`Set-ProvScheme`で行った変更を既存のVMに適用するには、`Set-ProvVMUpdateTimeWindow`コマンドを実行します。

1. `Set-ProvVMUpdateTimeWindow`コマンドを実行します。例:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

2. VMを再起動します。

Google Cloud マーケットプレイス

Citrixが**Google Cloud Marketplace**で提供するイメージを参照して選択し、マシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルワークフローのみをサポートしています。

Google Cloud Marketplaceを通じてCitrix VDA VM製品を検索するには、https://console.cloud.google.com/marketplaceにアクセスしてください。

Google Cloud MarketplaceでカスタムイメージまたはCitrix ready®イメージを使用して、マシンカタログのイメージを更新できます。

> **注:**
>
> マシンプロファイルにストレージタイプ情報が含まれていない場合、その値はカスタムプロパティから派生します。

> サポートされているGoogle Cloud Marketplaceイメージは次のとおりです。

- Windows 2019シングルセッション
- Windows 2019 マルチセッション
- ウブントゥ

Citrix対応イメージをマシンカタログ作成のソースとして使用する例:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \

-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \

-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
win2019-single-vda-v20220819.publicimage \

-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループを作成するように案内します。

- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログの管理およびGoogle Cloud Platformカタログの管理を参照してください。

詳細情報

- 接続とリソースを作成および管理する
- Google Cloud環境への接続
- マシンカタログを作成する

HPE Moonshot マシンカタログを作成する（プレビュー）

(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明しています。以下の情報は、HPE Moonshot環境に固有の詳細を扱っています。

> **注:**
>
> - HPE Moonshotへの接続を作成する
> - 1つ以上のHPE Moonshotノードが利用可能であることを確認し、それらのノードにVDAをインストールしてください。
> - 初期のHPE Moonshotカートリッジイメージの作成については、MoonshotでのOS展開ユーザーガイドを参照してください。

HPE Moonshotマシンカタログは、以下を使用して作成できます。

- ウェブスタジオ
- PowerShellコマンド

Web Studio を使用してマシンカタログを作成する

マシンカタログのセットアップウィザードで、:

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシン**と**別のサービスまたはテクノロジー**を選択します。

3. **仮想マシン**ページで、マシンとそのActive Directoryマシンアカウントを追加します。次のいずれかを実行できます。

   - **マシンの追加**をクリックして、マシンを手動で追加します。**VMの選択**ウィンドウが表示されます。以前に作成したHPE Moonshotシャーシ接続を展開し、追加するノード（VM）を選択します。次に、関連するマシンアカウント名を追加します。
   - 「**CSVファイルの追加**」をクリックして、マシンを一括追加します。CSVファイルを使用してマシンを追加する方法については、「CSVファイルを使用してマシンをカタログに一括追加する」を参照してください。

「**スコープ**」ページと「**概要**」ページには、HPE Moonshot固有の情報は含まれていません。

PowerShellコマンドを使用してマシンカタログを作成する

ブローカーカタログを作成し、マシンをブローカーカタログにインポートするには、`New-BrokerCatalog`および`New-BrokerMachine` PowerShellコマンドを実行します。

例:

```
New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

次のステップ

- これが最初に作成するカタログである場合、Web Studioはデリバリーグループを作成する手順を案内します。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください。
- カタログを管理するには、「マシンカタログの管理」および「HPE Moonshotカタログの管理」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- HPE Moonshotへの接続
- マシンカタログの作成

Microsoft Azureカタログの作成

「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱っています。

> **注:**
>
> Microsoft Azureカタログを作成する前に、Microsoft Azureへの接続の作成を完了する必要があります。Microsoft Azureへの接続を参照してください。

マシンカタログの作成

マシンカタログは次の2つの方法で作成できます。

- Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する
- PowerShellを使用してマシンカタログを作成する

Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する

イメージは、ディスク、スナップショット、またはAzure Compute Gallery内のイメージ定義のイメージバージョンであり、マシンカタログ内のVMを作成するために使用されます。マシンカタログを作成する前に、Azure Resource Managerでイメージを作成します。イメージに関する一般的な情報については、「マシンカタログの作成」を参照してください。

> **注:**
>
> ホスト接続で構成されているものとは異なるリージョンのマスターイメージを使用するサポートは非推奨になりました。Azure Compute Galleryを使用して、マスターイメージを目的のリージョンにレプリケートしてください。

> MCSマシンカタログを作成する際、DHCPの有効化やライセンスのリアームなどの準備タスクを実行するために、元のVMに基づいて一時的なVMが作成されます。この一時的なVMは準備VMと呼ばれます。この準備VMの名前は**Preparati-84x9n**という形式に従い、最後の5文字は重複を避けるためにランダムに生成されます。この準備VMの命名規則は固定されており、カスタマイズできません。準備タスクが完了すると、準備VMは破棄されます。

準備VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。ネットワークセキュリティグループは、カタログごとに1回自動的に作成されます。ネットワークセキュリティグループの名前は`Citrix-Deny-All-a3pgu-GUID`で、GUIDはランダムに生成されます。例：`Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`。

マシンカタログ作成ウィザードで:

- 「**マシンタイプ**」ページと「**マシン管理**」ページには、Azure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。
- 「**マスターイメージ**」ページで、カタログ内のすべてのマシンでマスターイメージとして使用するイメージを選択します。「**イメージの選択**」ウィザードが表示されます。

  a. (テナント内またはテナント間で共有イメージを使用して構成された接続にのみ適用) イメージが存在するサブスクリプションを選択します。

  b. リソースグループを選択します。

  c. Azure VHD、Azure Compute Gallery、またはAzureイメージバージョンに移動します。必要に応じて、選択したイメージにメモを追加します。

  イメージを選択する際は、次の点を考慮してください。

  - イメージにCitrix VDAがインストールされていることを確認します。
  - VMに接続されているVHDを選択する場合は、次の手順に進む前にVMをシャットダウンする必要があります。

> **注:**
>
> - カタログ内のマシンを作成した接続（ホスト）に対応するサブスクリプションは、緑色の点で示されます。その他のサブスクリプションは、Azure Compute Galleryがそのサブスクリプションと共有されているものです。これらのサブスクリプションでは、共有ギャラリーのみが表示されます。共有サブスクリプションの構成方法につい

ては、テナント内（サブスクリプション間）でのイメージの共有およびテナント間でのイメージの共有を参照してください。

- 信頼できる起動が有効になっているイメージまたはスナップショットを選択する場合、**セキュリティの種類**として信頼できる起動を持つマシンプロファイルを使用することが必須です。その後、マシンプロファイルでSecureBootとvTPMの値を指定することで、それらを有効または無効にできます。信頼できる起動はShared Image Galleryではサポートされていません。Azureの信頼できる起動の詳細については、`<https://docs.microsoft.com/ja-jp/azure/virtual-machines/trusted-launch>`を参照してください。
- Windowsで信頼できる起動を使用して、エフェメラルOSディスクを使用したプロビジョニングスキームを作成できます。信頼できる起動が有効なイメージを選択する場合、vTPMが有効な信頼できる起動を持つマシンプロファイルを選択する必要があります。エフェメラルOSディスクを使用してマシンカタログを作成する方法については、エフェメラルOSディスクを使用してマシンを作成する方法を参照してください。
- イメージのレプリケーションが進行中でも、イメージをマスターイメージとして選択し、セットアップを完了できます。ただし、イメージのレプリケーション中はカタログ作成に時間がかかる場合があります。MCSは、カタログ作成から1時間以内にレプリケーションが完了することを要求します。レプリケーションがタイムアウトすると、カタログ作成は失敗します。Azureでレプリケーションステータスを確認できます。レプリケーションがまだ保留中の場合、またはレプリケーションが完了した後に再度試してください。
- Azureでマシンカタログのマスターイメージを選択すると、MCSは選択したマスターイメージとマシンプロファイルに基づいてOSタイプを識別します。MCSが識別できない場合は、マスターイメージに一致するOSタイプを選択してください。
- Gen2イメージを使用してGen2 VMカタログをプロビジョニングすることで、起動時間のパフォーマンスを向上させることができます。ただし、Gen1イメージを使用してGen2マシンカタログを作成することはサポートされていません。同様に、Gen2イメージを使用してGen1マシンカタログを作成することもサポートされていません。また、世代情報を持たない古いイメージはすべてGen1イメージです。

カタログ内のVMがマシンプロファイルから構成を継承するかどうかを選択します。デフォルトでは、「**マシンプロファイルを使用する (Azure Active Directory に必須)**」

> チェックボックスが選択されています。「**マシンプロファイルの選択**」をクリックして、リソースグループのリストからVMまたはARMテンプレート仕様を参照します。

ARMテンプレート仕様を検証し、マシンカタログを作成するためのマシンプロファイルとして使用できることを確認します。ARMテンプレート仕様を検証する方法は2つあります。

- リソースグループリストからARMテンプレート仕様を選択した後、**次へ**をクリックします。ARMテンプレート仕様にエラーがある場合、エラーメッセージが表示されます。
- 次のPowerShellコマンドのいずれかを実行します。
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

VMがマシンプロファイルから継承できる構成の例は次のとおりです。

- 高速ネットワーク
- ブート診断
- ホストディスクキャッシュ (OSおよびMCSIOディスクに関連)
- マシンサイズ (別途指定がない限り)
- VMに配置されたタグ

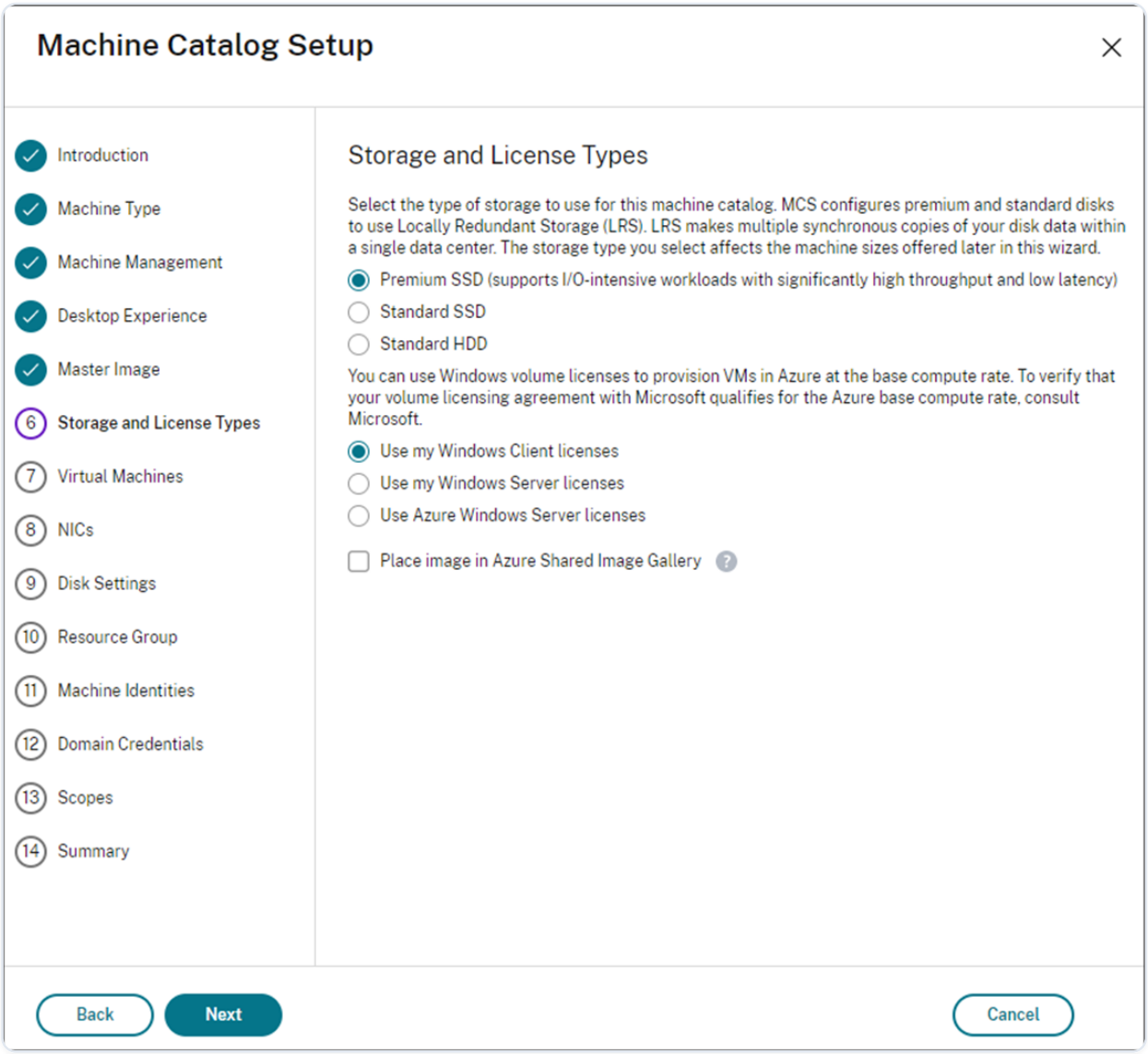
カタログを作成した後、イメージがマシンプロファイルから継承する構成を表示できます。**マシンカタログ**ノードでカタログを選択し、下部のペインでその詳細を表示します。次に、**テンプレートプロパティ**タブをクリックして、マシンプロファイルのプロパティを表示します。**タグ**セクションには最大3つのタグが表示されます。VMに配置されたすべてのタグを表示するには、**すべて表示**をクリックします。

MCSでAzure専用ホストにVMをプロビジョニングする場合は、**専用ホストグループを使用する**チェックボックスを有効にしてから、リストからホストグループを選択します。ホストグループは、専用ホストのコレクションを表すリソースです。専用ホストは、1つ以上のVMをホストする物理サーバーを提供するサービスです。お使いのサーバーはAzureサブスクリプション専用であり、他のサブスクライバーと共有されません。専用ホストを使用すると、AzureはVMがそのホストで実行されている唯一のマシンであることを保証します。この機能は、規制または内部セキュリティ要件を満たす必要があるシナリオに適しています。ホストグループとその使用に関する考慮事項の詳細については、「Azure dedicated hosts」を参照してください。

重要：

- Azure自動配置が有効になっているホストグループのみが表示されます。
- ホストグループを使用すると、ウィザードの後半で提供される**仮想マシン**ページが変更されます。選択したホストグループに含まれるマシンサイズのみがそのページに表示されます。また、可用性ゾーンは自動的に選択され、選択できません。

- **ストレージとライセンスの種類**ページは、Azure Resource Managerイメージを使用する場合にのみ表示されます。



マシンカタログで使用できるストレージの種類は次のとおりです。

- **プレミアム SSD**。I/O集中型ワークロードを持つ仮想マシンに適した、高性能で低遅延のディスクストレージオプションを提供します。

- **Standard SSD**。低いIOPSレベルで一貫したパフォーマンスを必要とするワークロードに適した、費用対効果の高いストレージオプションを提供します。
- **Standard HDD**。待機時間に影響を受けにくいワークロードを実行する VM に適した、信頼性の高い低コストのディスクストレージオプションを提供します。
- **Azureエフェメラルosディスク**。VMのローカルディスクを再利用してオペレーティングシステムディスクをホストする、費用対効果の高いストレージオプションを提供します。または、PowerShellを使用してエフェメラルOSディスクを使用するマシンを作成することもできます。詳細については、「Azureエフェメラルディスク」を参照してください。エフェメラルOSディスクを使用する際は、次の考慮事項に注意してください。
  - Azure エフェメラル OS ディスクと MCS I/O は同時に有効にできません。
  - エフェメラル OS ディスクを使用するマシンを更新するには、VM のキャッシュディスクまたは一時ディスクのサイズを超えないイメージを選択する必要があります。
  - ウィザードの後半で提供される**電源サイクル中に VM とシステムディスクを保持**オプションは使用できません。

> **注:**
>
> 選択したストレージの種類に関係なく、IDディスクは常にStandard SSDを使用して作成されます。

> ストレージの種類によって、ウィザードの**仮想マシン**ページで提供されるマシンのサイズが決まります。MCSは、プレミアムディスクと標準ディスクをローカル冗長ストレージ（LRS）を使用するように構成します。LRSは、単一のデータセンター内でディスクデータの複数の同期コピーを作成します。AzureエフェメラルOSディスクは、VMのローカルディスクを使用してオペレーティングシステムを保存します。Azureストレージの種類とストレージレプリケーションの詳細については、以下を参照してください。

- `<https://docs.microsoft.com/ja-jp/azure/storage/common/storage-introduction/>`
- `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/premium-storage-performance/>`
- `<https://docs.microsoft.com/ja-jp/azure/storage/common/storage-redundancy/>`

既存のWindowsライセンスまたはLinuxライセンスを使用するかどうかを選択します。

- Windowsライセンス：WindowsライセンスをWindowsイメージ（Azureプラットフォームサポートイメージまたはカスタムイメージ）とともに使用すると、AzureでWindows VMを低コストで実行できます。ライセンスには次の2種類があります。
  - **Windows Serverライセンス**。Windows ServerまたはAzure Windows Serverライセンスを使用でき、Azureハイブリッド特典を利用できます。詳細については、`<https://azure.microsoft.com/ja-jp/pricing/hybrid-benefit/>`を参照してください。Azureハイブリッド特典は、AzureでVMを実行するコストを基本コンピューティング料金に削減し、Azureギャラリーからの追加のWindows Serverライセンスのコストを免除します。
  - **Windowsクライアントライセンス**。Windows 10およびWindows 11ライセンスをAzureに持ち込むことができ、追加のライセンスなしでAzureでWindows 10およびWindows 11 VMを実行できます。詳細については、「クライアントアクセスライセンスと管理ライセンス」を参照してください。

プロビジョニングされたVMがライセンス特典を使用しているかどうかは、次のPowerShellコマンドを実行して確認できます: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`。

- Windows Serverライセンスタイプの場合、ライセンスタイプが **Windows_Server** であることを確認します。詳細な手順は `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>` で入手できます。
- Windows Clientライセンスタイプの場合、ライセンスタイプが **Windows_Client** であることを確認します。詳細な手順は `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>` で入手できます。

あるいは、`Get-Provscheme` PowerShell SDKを使用して検証を行うこともできます。例: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`。このコマンドレットの詳細については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>` を参照してください。

- Linuxライセンス：BYOS（bring-your-own-subscription）Linuxライセンスを使用すると、ソフトウェアの料金を支払う必要はありません。BYOS料金には、コンピューティングハードウェア料金のみが含まれます。ライセンスには次の2種類があります。
  - **RHEL_BYOS**: RHEL_BYOSタイプを正常に使用するには、AzureサブスクリプションでRed Hat Cloud Accessを有効にします。

- **SLES_BYOS**: SLESのBYOSバージョンには、SUSEからのサポートが含まれています。

LicenseTypeの値を`New-ProvScheme`および`Set-ProvScheme`のLinuxオプションに設定できます。

LicenseTypeをRHEL_BYOSに設定する例（`New-ProvScheme`）：

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog"
-RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="RHEL_BYOS" /></CustomProperties>'
```

LicenseTypeをSLES_BYOSに設定する例（`Set-ProvScheme`）：

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
CustomProperties>'
```

> **注：**
>
> `LicenseType`の値が空の場合、デフォルト値はOsTypeの値に応じてAzure Windows Server LicenseまたはAzure Linux Licenseになります。

> LicenseTypeを空に設定する例：

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /></
CustomProperties>'
```

ライセンスの種類とその利点については、以下のドキュメントを参照してください。

- `<https://docs.microsoft.com/ja-jp/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>`
- `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/linux/azure-hybrid-benefit-linux>`

Azure Compute Gallery（旧称Azure Shared Image Gallery）は、イメージを管理および共有するためのリポジトリです。これにより、組織全体でイメージを利用できるようになります。大規模な非永続マシンカタログを作成する際には、イメージをSIGに保存することをお勧めします。そうすることで、VDA OSディスクのリセットが高速化されるためです。**Azure Compute Galleryに準備されたイメージを配置**を選択すると、**Azure Compute Gallery設定**セクションが表示され、追加のAzure Compute Gallery設定を指定できます。

- **仮想マシンとイメージレプリカの比率**。Azureが保持する仮想マシンとイメージレプリカの比率を指定できます。デフォルトでは、Azureは非永続マシン40台ごとに1つのイメージレプリカを保持します。永続マシンの場合、その数はデフォルトで1,000です。
- **最大レプリカ数**。Azureが保持するイメージレプリカの最大数を指定できます。デフォルトは10です。

> **注：**

> イメージを保存するためにACGにギャラリーが作成されます。このギャラリーは、VM作成のためにMCSからのみアクセス可能であり、**イメージの選択**ページには表示されません。

- **仮想マシン**ページで、作成するVMの数を指定します。少なくとも1つを指定し、マシンサイズを選択する必要があります。カタログ作成後、カタログを編集してマシンサイズを変更できます。
- **NIC**ページには、Azure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。
- **ディスク設定**ページで、ライトバックキャッシュを有効にするかどうかを選択します。MCSストレージ最適化機能が有効になっている場合、カタログ作成時に以下の設定を構成できます。これらの設定は、Azure と GCP の両方の環境に適用されます。

  マシンカタログ設定 - ディスク設定(/en-us/citrix-virtual-apps-desktops/2311/media/catalog-setup-disk-settings.png)

  ライトバックキャッシュを有効にした後、以下を実行できます。

  - 一時データのキャッシュに使用されるディスクとRAMのサイズを構成します。詳細については、「一時データのキャッシュを構成する」を参照してください。
  - ライトバックキャッシュディスクのストレージタイプを選択します。ライトバックキャッシュディスクには、次のストレージオプションを使用できます。
    - プレミアム SSD
    - スタンダード SSD
    - スタンダード HDD
  - プロビジョニングされたVMに対してライトバックキャッシュディスクを永続化するかどうかを選択します。オプションを有効にするには、**ライトバックキャッシュを有効にする**を選択します。デフォルトでは、**非永続ライトバックキャッシュディスクを使用する**が選択されています。
  - ライトバックキャッシュディスクの種類を選択します。
    - **非永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクは電源サイクル中に削除されます。そこにリダイレクトされたデータはすべて失われます。VMの一時ディスクに十分な空き容量がある場合、コストを削減するためにライトバックキャッシュディスクをホストするために使用されます。カタログ作成後、プロビジョニングされたマシンが一時ディスクを使用しているかどうかを

確認できます。これを行うには、カタログをクリックし、**テンプレートプロパティ**タブの情報を確認します。一時ディスクが使用されている場合、**非永続ライトバックキャッシュディスク**が表示され、その値は**はい（VMの一時ディスクを使用）**となります。そうでない場合、非永続ライトバックキャッシュディスクが表示され、その値は**いいえ（VMの一時ディスクを使用しない）**となります。

- **永続ライトバックキャッシュディスクを使用する。**選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに対して永続的になります。このオプションを有効にすると、ストレージコストが増加します。

- 電源サイクル中にVDAのVMとシステムディスクを保持するかどうかを選択します。

  電源サイクル中に VM とシステムディスクを保持する。ライトバックキャッシュを有効にするを選択した場合に利用可能です。デフォルトでは、VM とシステムディスクはシャットダウン時に削除され、起動時に再作成されます。VM の再起動時間を短縮したい場合は、このオプションを選択します。このオプションを有効にすると、ストレージコストも増加することに注意してください。

- **ストレージコストの節約**を有効にするかどうかを選択します。有効にすると、VMがシャットダウンしたときにストレージディスクをStandard HDDにダウングレードすることで、ストレージコストを節約できます。VMは再起動時に元の設定に戻ります。このオプションは、ストレージディスクとライトバックキャッシュディスクの両方に適用されます。または、PowerShellを使用することもできます。「VMシャットダウン時にストレージタイプを下位層に変更する」を参照してください。

  > **注記:**
  >
  > Microsoftは、VMシャットダウン中のストレージタイプの変更に制限を課しています。また、Microsoftが将来的にストレージタイプの変更をブロックする可能性もあります。詳しくは、このMicrosoftの記事を参照してください。

- カタログでプロビジョニングされたマシン上のデータを暗号化するかどうかを選択します。顧客管理の暗号化キーを使用したサーバー側暗号化により、管理ディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。詳しくは、Azureサーバー側暗号化を参照してください。

- **リソースグループ** ページで、リソースグループを作成するか、既存のグループを使用するかを選択します。

  - リソースグループを作成することを選択した場合は、**次へ**を選択します。

- 既存のリソースグループを使用することを選択した場合は、**利用可能なプロビジョニングリソースグループ**リストからグループを選択します。**注意**: カタログで作成するマシンを収容するのに十分な数のグループを選択してください。少なすぎるグループを選択すると、メッセージが表示されます。後でカタログにVMを追加する予定がある場合は、最低限必要な数よりも多く選択することをお勧めします。カタログ作成後にリソースグループをカタログに追加することはできません。

詳しくは、Azureリソースグループを参照してください。

- **マシンID**ページで、IDタイプを選択し、このカタログ内のマシンのIDを構成します。VMを**Azure Active Directory参加済み**として選択した場合、それらをAzure ADセキュリティグループに追加できます。詳細な手順は次のとおりです。

  a. **IDタイプ**フィールドから、**Azure Active Directory参加済み**を選択します。**Azure ADセキュリティグループ（オプション）**オプションが表示されます。

  b. **Azure ADセキュリティグループ: 新規作成**をクリックします。

  c. グループ名を入力し、**作成**をクリックします。

  d. 画面の指示に従って Azure にサインインします。 グループ名が Azure に存在しない場合、緑色のアイコンが表示されます。それ以外の場合は、新しい名前を入力するよう求めるエラーメッセージが表示されます。

  e. VM のマシンアカウントの命名スキームを入力します。

  カタログ作成後、Citrix Virtual Apps and Desktops™はユーザーに代わってAzureにアクセスし、セキュリティグループと、そのグループの動的メンバーシップルールを作成します。このルールに基づき、このカタログで指定された命名スキームを持つVMは自動的にセキュリティグループに追加されます。

  このカタログに異なる命名スキームを持つ VM を追加するには、Azure にサインインする必要があります。その後、Citrix Virtual Apps and Desktops は Azure にアクセスし、新しい命名スキームに基づいて動的メンバーシップルールを作成できます。

  このカタログを削除する際、Azure からセキュリティグループを削除するには、Azure へのサインインも必要です。

- **ドメイン資格情報**および**概要**ページには、Azure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。

ウィザードを完了します。

Azure一時ディスクがライトバックキャッシュディスクとして適格であるための条件

Azure一時ディスクをライトバックキャッシュディスクとして使用できるのは、以下のすべての条件が満たされている場合のみです。

- Azure一時ディスクは永続的なデータに適していないため、ライトバックキャッシュディスクは非永続的である必要があります。
- 選択したAzure VMサイズには、一時ディスクが含まれている必要があります。
- エフェメラルOSディスクを有効にする必要はありません。
- ライトバックキャッシュファイルをAzure一時ディスクに配置することを受け入れます。
- Azure一時ディスクのサイズは、（ライトバックキャッシュディスクサイズ + ページングファイル用の予約スペース + 1 GBのバッファースペース）の合計サイズよりも大きい必要があります。

非永続ライトバックキャッシュディスクのシナリオ

次の表は、マシンカタログの作成時に一時ディスクをライトバックキャッシュに使用する場合の3つの異なるシナリオについて説明しています。

シナリオ	結果
ライトバックキャッシュに一時ディスクを使用するためのすべての条件が満たされています。	WBCファイル `mcsdif.vhdx` は一時ディスクに配置されます。
一時ディスクには、ライトバックキャッシュの使用に十分なスペースがありません。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。
一時ディスクにはライトバックキャッシュの使用に十分なスペースがありますが、`UseTempDiskForWBC` が **false** に設定されています。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。

Azure テンプレート仕様を作成する

Azure ポータルで Azure テンプレート仕様を作成し、Web Studio および PowerShell コマンドで使用して、MCS マシンカタログを作成または更新できます。

既存のVMのAzureテンプレートスペックを作成するには：

1. Azure ポータルに移動します。リソースグループを選択し、VM とネットワークインターフェイスを選択します。上部にある **...** メニューから、**Export template** をクリックします。
2. カタログプロビジョニング用のテンプレート仕様を作成する場合は、**Include parameters** チェックボックスをオフにします。JSON ファイルで `parameters` および `variables` セクションが次のようになっていることを確認します。

```
"parameters": {},

"variables": {}
```

3. テンプレートを JSON ファイルとして保存するには、**Download** をクリックします。
4. Azure ポータルで、**Template specs** を選択し、**Import Template** をクリックします。
5. コンピューターに保存されているマシンプロファイル（JSON 形式）を参照してインポートします。
6. **Name**、**Subscription**、**Resource Group**、**Location**、および **Version** を指定します。**Next: Edit Template** をクリックします。
7. **Review+Create** を作成し、テンプレート仕様を作成します。
8. 「**テンプレート仕様**」ページで、作成したばかりのテンプレート仕様を確認します。テンプレート仕様をクリックします。左側のパネルで、「**バージョン**」をクリックします。
9. 「**新しいバージョンを作成**」をクリックして、新しいバージョンを作成できます。新しいバージョン番号を指定し、現在のテンプレート仕様に変更を加え、「**確認 + 作成**」をクリックして、テンプレート仕様の新しいバージョンを作成します。

以下のPowerShellコマンドを使用して、テンプレートスペックとテンプレートバージョンの情報を取得できます。

- テンプレートスペックの情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec
```

- テンプレート仕様のバージョンに関する情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec\bgg1.0.templatespecversion
```

カタログの作成または更新でテンプレート仕様を使用する

MCSマシンカタログは、マシンプロファイル入力としてテンプレート仕様を使用して作成または更新できます。これを行うには、Web StudioまたはPowerShellコマンドを使用できます。

- Web Studioについては、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。
- PowerShellについては、「PowerShellを使用してカタログを作成または更新する際にテンプレート仕様を使用する」を参照してください。

Azureサーバー側暗号化

Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介したAzureマネージドディスクの顧客管理暗号化キーをサポートしています。このサポートにより、独自の暗号化キーを使用してマシンカタログのマネージドディスクを暗号化することで、組織およびコンプライアンス要件を管理できます。詳細については、「Azure Disk Storageのサーバー側暗号化」を参照してください。

マネージドディスクでこの機能を使用する場合：

- ディスクの暗号化に使用するキーを変更するには、`DiskEncryptionSet` で現在のキーを変更します。その `DiskEncryptionSet` に関連付けられているすべてのリソースは、新しいキーで暗号化されるように変更されます。
- キーを無効にするか削除すると、そのキーを使用しているディスクを持つVMはすべて自動的にシャットダウンします。シャットダウン後、キーが再度有効になるか、新しいキーを割り当てるまで、VMは使用できません。そのキーを使用しているカタログは電源をオンにできず、VMを追加することもできません。

顧客管理暗号化キーを使用する際の重要な考慮事項

この機能を使用する際は、以下を考慮してください。

- お客様が管理するキーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- お客様が管理する暗号化キーを一度有効にすると、後で無効にすることはできません。お客様が管理する暗号化キーを無効にするか削除したい場合は、すべてのデータを、お客様が管理する暗号化キーを使用していない別のマネージドディスクにコピーしてください。
- サーバー側暗号化とお客様が管理するキーを使用して暗号化されたカスタムイメージから作成されたディスクは、同じお客様が管理するキーを使用して暗号化する必要があります。これらのディスクは同じサブスクリプションに存在する必要があります。

- サーバー側暗号化とお客様が管理するキーで暗号化されたディスクから作成されたスナップショットは、同じお客様が管理するキーで暗号化する必要があります。
- お客様が管理するキーで暗号化されたディスク、スナップショット、およびイメージは、別のリソースグループやサブスクリプションに移動できません。
- 現在または以前にAzure Disk Encryptionを使用して暗号化されたマネージドディスクは、お客様が管理するキーを使用して暗号化することはできません。
- ディスク暗号化セットのリージョンごとの制限については、Microsoft サイトを参照してください。

> **注:**
>
> Azure サーバー側暗号化の構成については、クイックスタート: Azure portal を使用して Key Vault を作成する を参照してください。

Azureのお客様が管理する暗号化キー

マシンカタログを作成する際、カタログにプロビジョニングされたマシン上のデータを暗号化するかどうかを選択できます。お客様が管理する暗号化キーを使用したサーバー側暗号化により、マネージドディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。ディスク暗号化セット（DES）は、お客様が管理するキーを表します。この機能を使用するには、まずAzureでDESを作成する必要があります。DESは次の形式です。

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

リストからDESを選択します。選択するDESは、リソースと同じサブスクリプションおよびリージョンにある必要があります。イメージがDESで暗号化されている場合は、マシンカタログの作成時に同じDESを使用します。カタログ作成後にDESを変更することはできません。

暗号化キーを使用してカタログを作成し、後でAzureで対応するDESを無効にした場合、カタログ内のマシンの電源をオンにしたり、マシンを追加したりすることはできなくなります。

「顧客管理キーを使用したマシンカタログの作成」を参照してください。

ホストでのAzureディスク暗号化

ホストでの暗号化機能を備えたMCSマシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルワークフローのみをサポートしています。マシンプロファイルの入力として、VMまたはテンプレート仕様を使用できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

制限事項：

ホストでのAzureディスク暗号化は次のとおりです。

- すべてのAzureマシンサイズでサポートされているわけではありません
- Azure ディスク暗号化と互換性がありません

ホストでの暗号化機能を持つマシンカタログを作成するには：

1. サブスクリプションでホストでの暗号化機能が有効になっているかどうかを確認します。これを行うには、`<https://learn.microsoft.com/ja-jp/rest/api/resources/features/get?tabs=HTTP/>`を参照してください。有効になっていない場合は、サブスクリプションでこの機能を有効にする必要があります。サブスクリプションで機能を有効にする方法については、`<https://learn.microsoft.com/ja-jp/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>`を参照してください。
2. 特定のAzure VMサイズがホストでの暗号化をサポートしているかどうかを確認します。これを行うには、PowerShellウィンドウで次のいずれかを実行します。

   ```
   PS XDHyp:\Connections\<your connection>\east
   us.region\serviceoffering.folder>
   ```

   ```
   PS XDHyp:\HostingUnits\<your hosting unit>\serviceoffering.folder>
   ```

3. ホストでの暗号化が有効になっているVMまたはテンプレート仕様を、マシンプロファイルの入力としてAzureポータルで作成します。
   - VMを作成する場合は、ホストでの暗号化をサポートするVMサイズを選択します。VMを作成すると、VMプロパティの**ホストでの暗号化**が有効になります。
   - テンプレート仕様を使用する場合は、`securityProfile`内でパラメーター`Encryption at Host`を**true**として割り当てます。
4. VMまたはテンプレート仕様のいずれかを選択して、マシンプロファイルワークフローでMCSマシンカタログを作成します。

- OSディスク / データディスク: 顧客管理キーおよびプラットフォーム管理キーによって暗号化されます
- エフェメラルOSディスク: プラットフォーム管理キーのみによって暗号化されます
- キャッシュディスク: 顧客管理キーおよびプラットフォーム管理キーによって暗号化されます

Web StudioまたはPowerShellコマンドを実行して、マシンカタログを作成できます。

マシンプロファイルからホストでの暗号化情報を取得する

`AdditionalData`パラメーターを指定してPowerShellコマンドを実行すると、マシンプロファイルからホストでの暗号化情報を取得できます。`EncryptionAtHost`パラメーターが**True**の場合、ホストでの暗号化がマシンプロファイルに対して有効になっていることを示します。

例: マシンプロファイルの入力が VM の場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def.v
m).AdditionalData
```

例: マシンプロファイルの入力がテンプレート仕様の場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def_t
emplatespec.templatespec\EncryptionAtHost.templatespecversion).AdditionalD
ata
```

マネージドディスクの二重暗号化

二重暗号化を使用してマシンカタログを作成できます。この機能で作成されたカタログはすべて、プラットフォーム管理キーと顧客管理キーの両方でサーバー側で暗号化されたディスクを持ちます。Azure Key Vault、暗号化キー、およびディスク暗号化セット (DES) はお客様が所有および管理します。

二重暗号化は、プラットフォーム側暗号化（デフォルト）と顧客管理暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念するセキュリティ意識の高いお客様は、この二重暗号化を選択できます。永続的なOSディスクとデータディスク、スナップショット、およびイメージはすべて、二重暗号化によって保存時に暗号化されます。

注:

- Web StudioおよびPowerShellコマンドを使用して、二重暗号化でマシンカタログを作成および更新できます。PowerShellコマンドについては、「二重暗号化でマシンカタログを作成する」を参照してください。
- 二重暗号化でマシンカタログを作成または更新するために、マシンプロファイルに基づかないワークフローまたはマシンプロファイルに基づくワークフローを使用できます。
- マシンプロファイルに基づかないワークフローを使用してマシンカタログを作成する場合、保存されている`DiskEncryptionSetId`を再利用できます。
- マシンプロファイルを使用する場合、VMまたはテンプレート仕様をマシンプロファイルの入力として使用できます。

制限事項:

- Ultra DisksまたはPremium SSD v2ディスクでは、二重暗号化はサポートされていません。
- アンマネージドディスクでは、二重暗号化はサポートされていません。
- カタログに関連付けられているDiskEncryptionSetキーを無効にすると、カタログのVMも無効になります。
- お客様が管理するキーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- サブスクリプションごとに、リージョンあたり最大50個のディスク暗号化セットしか作成できません。
- 異なる`DiskEncryptionSetId`を持つ`DiskEncryptionSetId`が既に存在するマシンカタログを更新することはできません。

Azureリソースグループ

Azureプロビジョニングリソースグループは、ユーザーにアプリケーションとデスクトップを提供するVMをプロビジョニングする方法を提供します。MCSマシンカタログを作成する際に、既存の空のAzureリソースグループを追加したり、新しいリソースグループを作成させたりすることができます。Azureリソースグループの詳細については、Microsoftドキュメントを参照してください。

Azureリソースグループの使用状況

Azureリソースグループあたりの仮想マシン、マネージドディスク、スナップショット、イメージの数に制限はありません。（Azureリソースグループあたりのマネージドディスク800個につきVM240個という制限は削除されました。）

- フルスコープのサービスプリンシパルを使用してマシンカタログを作成する場合、MCSは1つのAzureリソースグループのみを作成し、そのグループをカタログに使用します。
- ナロースコープのサービスプリンシパルを使用してマシンカタログを作成する場合、カタログ用に空の、事前に作成されたAzureリソースグループを提供する必要があります。

Azureエフェメラルディスク

Azure エフェメラルディスクを使用すると、キャッシュディスクまたは一時ディスクを再利用して、Azure対応仮想マシンのOSディスクを保存できます。この機能は、標準のHDDディスクよりも高性能なSSDディスクを必要とするAzure環境で役立ちます。Azure エフェメラルディスクを使用してカタログを作成する方法については、Azure エフェメラルディスクを使用してカタログを作成するを参照してください。

> **注:**
>
> 永続カタログは、エフェメラルOSディスクをサポートしていません。
>
> エフェメラルOSディスクでは、プロビジョニングスキームでマネージドディスクと共有イメージギャラリーを使用する必要があります。

エフェメラルOS一時ディスクの保存

エフェメラルOSディスクをVMの一時ディスクまたはリソースディスクに保存するオプションがあります。この機能により、キャッシュがない、またはキャッシュが不十分なVMでエフェメラルOSディスクを使用できます。このようなVMには、`Ddv4`などのエフェメラルOSディスクを保存するための一時ディスクまたはリソースディスクがあります。

次の点を考慮してください。

- エフェメラルディスクは、VMキャッシュディスクまたはVMの一時（リソース）ディスクのいずれかに保存されます。キャッシュディスクがOSディスクのコンテンツを保持するのに十分な大きさでない限り、一時ディスクよりもキャッシュディスクが優先されます。
- 更新の場合、キャッシュディスクより大きく、一時ディスクより小さい新しいイメージは、エフェメラルOSディスクをVMの一時ディスクに置き換えることになります。

Azure エフェメラルディスクとMachine Creation Services（MCS）ストレージ最適化（MCS I/O）

Azure エフェメラルOSディスクとMCS I/Oは同時に有効にできません。

重要な考慮事項は次のとおりです。

- エフェメラルOSディスクとMCS I/Oの両方を同時に有効にしてマシンカタログを作成することはできません。
- PowerShellパラメーター（`UseWriteBackCache`および`UseEphemeralOsDisk`）を`New-ProvScheme`または`Set-ProvScheme`で**true**に設定すると、適切なエラーメッセージが表示されて失敗します。
- 両方の機能が有効になっている既存のマシンカタログの場合でも、次のことができます。
  - マシンカタログを更新する。
  - VMを追加または削除する。
  - マシンカタログを削除する。

アジュール コンピュート ギャラリー

AzureでMCSによってプロビジョニングされたマシンの公開イメージリポジトリとして、Azure Compute Gallery (旧称 Azure Shared Image Gallery) を使用します。ギャラリーに公開イメージを保存することで、OSディスクの作成とハイドレーションを高速化し、非永続VMの起動時間とアプリケーション起動時間を改善できます。共有イメージギャラリーには、次の3つの要素が含まれています。

- *ギャラリー*: イメージはここに保存されます。MCSは、各マシンカタログに対して1つのギャラリーを作成します。
- *ギャラリーイメージ定義*: この定義には、公開イメージに関する情報（オペレーティングシステムの種類と状態、Azureリージョン）が含まれます。MCSは、カタログ用に作成された各イメージに対して1つのイメージ定義を作成します。
- *ギャラリーイメージバージョン*: 共有イメージギャラリー内の各イメージは複数のバージョンを持つことができ、各バージョンは異なるリージョンに複数のレプリカを持つことができます。各レプリカは、公開イメージの完全なコピーです。

> **注：**
>
> Shared Image Gallery機能はマネージドディスクとのみ互換性があります。レガシーマシンカタログでは利用できません。

> 詳細については、Azure Compute Galleryの概要を参照してください。

PowerShellを使用してAzure Compute Galleryイメージでマシンカタログを作成または更新する方法については、Azure Compute Galleryイメージを使用してマシンカタログを作成または更新するを参照してください。

Azure 機密 VM

Azure 機密コンピューティング VM は、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCSを使用してAzure機密VMを含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。VMとARMテンプレート仕様の両方をマシンプロファイル入力として使用できます。

機密VMに関する重要な考慮事項

サポートされているVMサイズと機密VMを使用したマシンカタログの作成に関する重要な考慮事項は次のとおりです。

- サポートされているVMサイズ：機密VMは次のVMサイズをサポートしています。
  - DCasv5 シリーズ
  - DCadsv5 シリーズ
  - ECasv5 シリーズ
  - ECadsv5 シリーズ
- 機密VMを使用してマシンカタログを作成します。
  - Web StudioおよびPowerShellコマンドを使用して、Azure機密VMでマシンカタログを作成できます。
  - Azure機密VMでマシンカタログを作成するには、マシンプロファイルベースのワークフローを使用する必要があります。VMまたはテンプレート仕様をマシンプロファイルの入力として使用できます。
  - マスターイメージとマシンプロファイルの入力は、両方とも同じ機密セキュリティタイプで有効にする必要があります。セキュリティタイプは次のとおりです。
    - **VMGuestStateOnly**：VMゲスト状態のみが暗号化された機密VM

- **DiskWithVMGuestState**：OSディスクとVMゲスト状態の両方がプラットフォーム管理キーまたは顧客管理キーで暗号化された機密VM。通常ディスクとエフェメラルOSディスクの両方を暗号化できます。

- マネージドディスク、スナップショット、Azure Compute Galleryイメージ、VM、ARMテンプレート仕様など、さまざまなリソースタイプの機密VM情報をAdditionalDataパラメーターを使用して取得できます。例：

  ```
  PS C:\Users\username> (get-item XDHyp:
  \HostingUnits\mynetwork\image.folder\username-dev-testing-
  rg.resourcegroup\username-dev-tsvda.vm).AdditionalData
  ```

  追加データフィールドは次のとおりです。

  - DiskSecurityType
  - ConfidentialVMDiskEncryptionSetId
  - DiskSecurityProfiles

  マシンサイズの機密コンピューティングプロパティを取得するには、次のコマンドを実行します: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

  追加データフィールドは`ConfidentialComputingType`です。

- マスターイメージまたはマシンプロファイルを、機密から非機密セキュリティタイプへ、または非機密から機密セキュリティタイプへ変更することはできません。

- 誤った構成に対しては、適切なエラーメッセージが表示されます。

マスターイメージとマシンプロファイルを準備する

機密VMのセットを作成する前に、以下の手順に従ってマスターイメージとマシンプロファイルを準備します。

1. Azureポータルで、次のような特定の構成で機密VMを作成します。

   - **セキュリティの種類**: 機密仮想マシン
   - **機密OSディスク暗号化**: 有効。
   - **キー管理**: プラットフォーム管理キーによる機密ディスク暗号化 機密VMの作成について詳しくは、この Microsoft の記事を参照してください。

2. 作成したVM上でマスターイメージを準備します。作成したVMに必要なアプリケーションとVDAをインストールします。

> **注:**
>
> VHDを使用した機密VMの作成はサポートされていません。代わりに、この目的のためにAzure Compute Gallery、マネージドディスク、またはスナップショットを使用してください。

3. 次のいずれかの方法でマシンプロファイルを作成します。

   - 必要なマシンプロパティを備えている場合は、ステップ1で作成した既存のVMを使用します。
   - マシンプロファイルとしてARMテンプレート仕様を選択する場合は、必要に応じてテンプレート仕様を作成します。具体的には、*SecurityEncryptionType*や*diskEncryptionSet*（顧客管理キーの場合）など、機密VMの要件を満たすパラメーターを構成します。詳細については、「Azureテンプレート仕様の作成」を参照してください。

     > **注:**
     >
     > - マスターイメージとマシンプロファイルが同じセキュリティキータイプであることを確認してください。
     > - 顧客管理キーによる機密OSディスク暗号化を必要とする機密VMを作成するには、マスターイメージとマシンプロファイルの両方でディスク暗号化セットIDが同一であることを確認してください。

Web Studio または PowerShell コマンドを使用して機密VMを作成する

機密VMのセットを作成するには、マスターイメージと、目的の機密VMから派生したマシンプロファイルを使用してマシンカタログを作成します。

Web Studioを使用してカタログを作成するには、「マシンカタログの作成」に記載されている手順に従ってください。以下の考慮事項に留意してください。

- 「**イメージ**」ページで、機密VM作成のために準備したマスターイメージとマシンプロファイルを選択します。マシンプロファイルの選択は必須であり、選択したマスターイメージと同じセキュリティ暗号化タイプに一致するプロファイルのみが選択可能です。

- 「**仮想マシン**」ページでは、機密VMをサポートするマシンサイズのみが選択肢として表示されます。
- 「**ディスク設定**」ページでは、選択したマシンプロファイルから継承されるため、ディスク暗号化セットを指定することはできません。

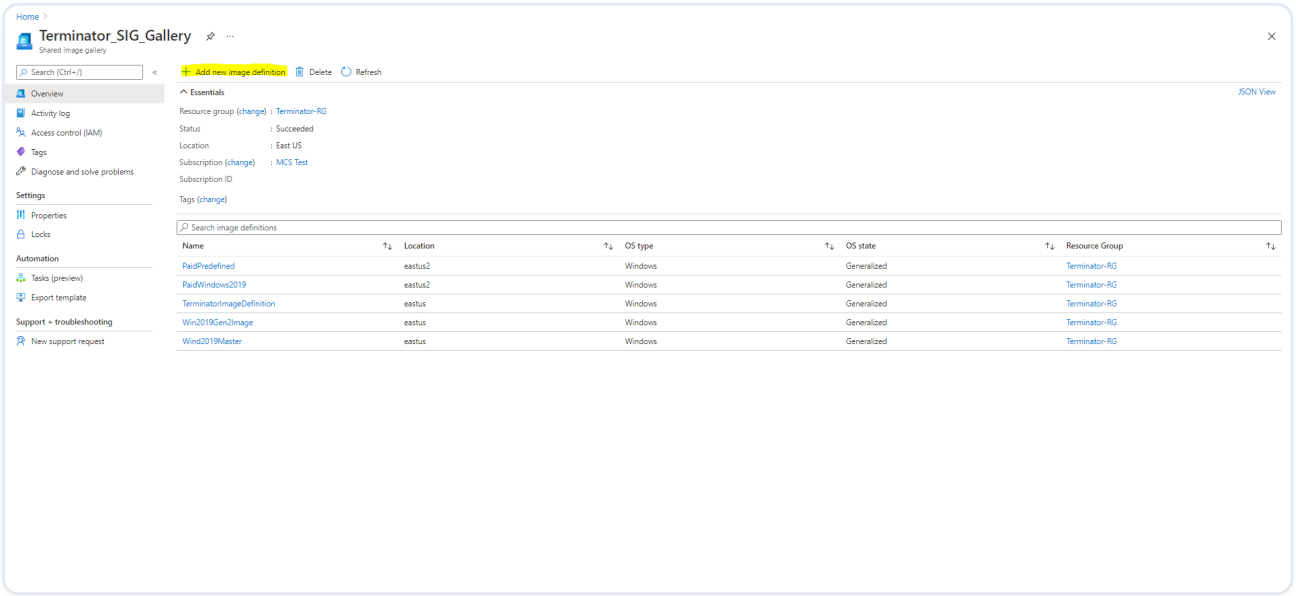
Azure Marketplace (アジュール マーケットプレイス)

Citrix Virtual Apps and Desktopsは、マシンカタログを作成するためのプラン情報を含むAzure上のマスターイメージの使用をサポートしています。詳細については、「Microsoft Azure Marketplace」を参照してください。

> **ヒント:**
>
> Azure Marketplaceで見つかる一部のイメージ（標準のWindows Serverイメージなど）は、プラン情報を付加しません。Citrix Virtual Apps and Desktopsの機能は、有料イメージ向けです。

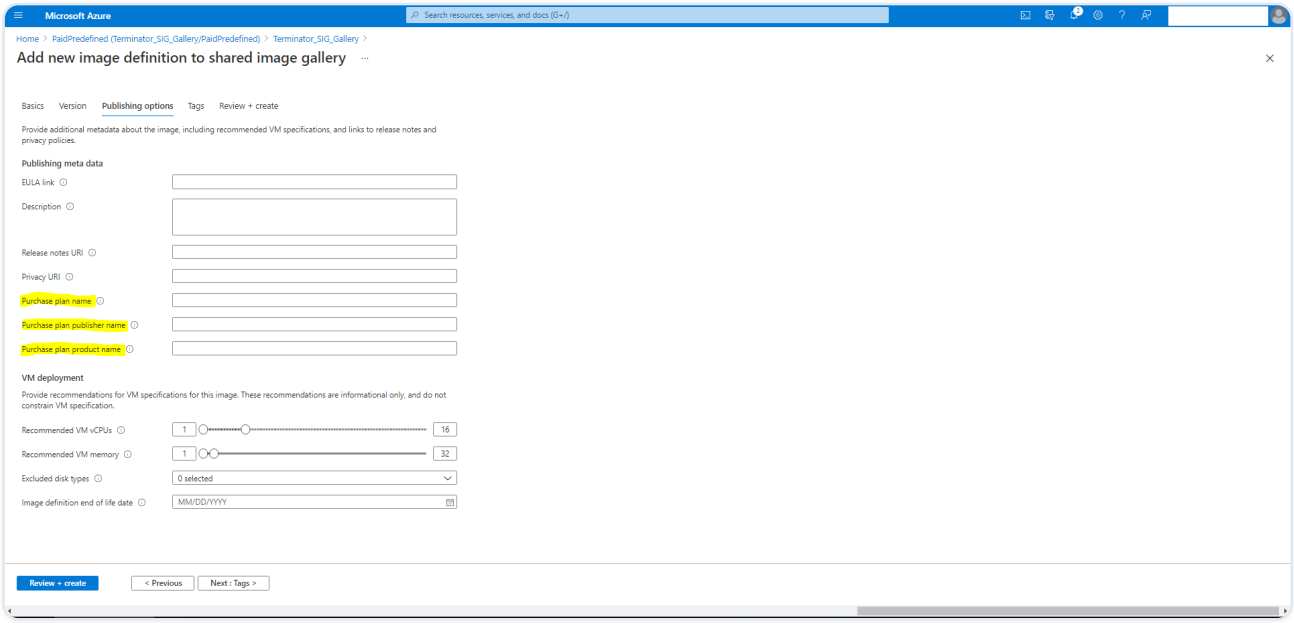
Shared Image Galleryで作成されたイメージにAzureプラン情報が含まれていることを確認してください

このセクションの手順を使用して、Web StudioでShared Image Galleryのイメージを表示します。これらのイメージは、オプションでマスターイメージとして使用できます。イメージをShared Image Galleryに配置するには、ギャラリーでイメージ定義を作成します。

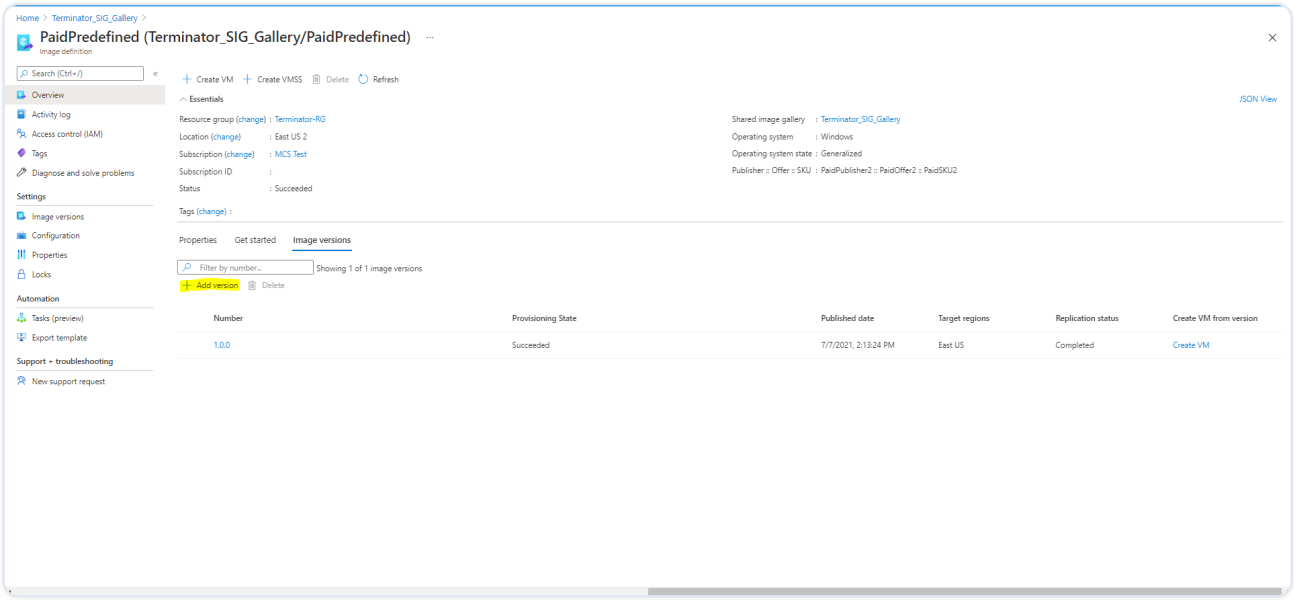


公開オプションページで、購入プラン情報を確認します。

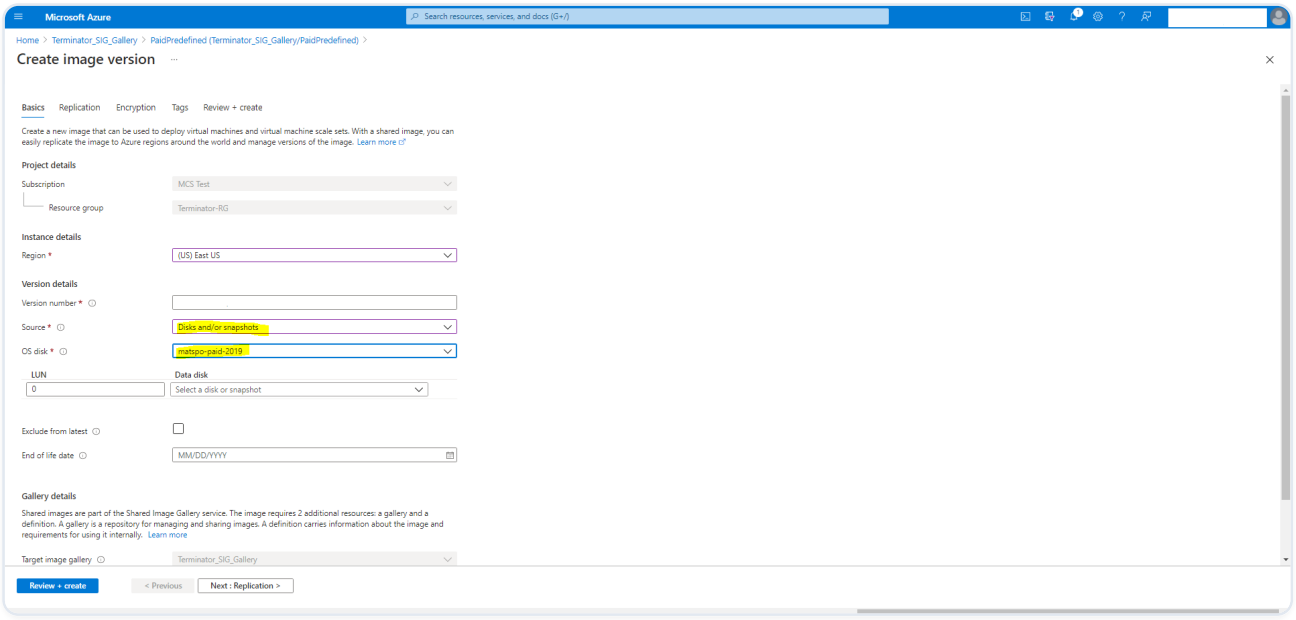
購入プラン情報フィールドは、最初は空です。イメージに使用された購入プラン情報でこれらのフィールドに入力します。購入プラン情報を入力しないと、マシンカタログのプロセスが失敗する可能性があります。



購入プラン情報を確認した後、定義内でイメージバージョンを作成します。これはマスターイメージとして使用されます。**バージョンを追加**をクリックします。



バージョン詳細セクションで、イメージスナップショットまたはマネージドディスクをソースとして選択します。



PowerShell を使用してマシンカタログを作成する

このセクションでは、PowerShellを使用してカタログを作成する方法について詳しく説明します。

- 非永続的なライトバックキャッシュディスクを使用してカタログを作成する
- 永続的なライトバックキャッシュディスクを持つカタログを作成する
- MCSIOで起動パフォーマンスを向上させる
- PowerShellを使用してカタログを作成または更新する際にテンプレート仕様を使用する
- トラステッド起動によるマシンカタログ
- マシンプロファイルのプロパティ値を使用する
- 顧客管理の暗号化キーを使用してマシンカタログを作成する
- 二重暗号化を使用してマシンカタログを作成する
- Azureエフェメラルディスクを使用してカタログを作成する
- Azure専用ホスト
- Azure Compute Galleryイメージを使用してマシンカタログを作成または更新する
- 共有イメージギャラリーを構成する
- 指定された可用性ゾーンにマシンをプロビジョニングする
- ストレージの種類
- ページファイルの場所
- ページファイル設定を更新する

- 「Azure スポット VM を使用してカタログを作成する」(#create-a-catalog-using-azure-spot-vms)
- 「バックアップ VM サイズを構成する」(#configure-backup-vm-sizes)
- 「すべてのリソースにタグをコピーする」(#copy-tags-on-all-resources)
- 「Azure Monitor Agent がインストールされたカタログ VM をプロビジョニングする」(#provision-catalog-vms-with-azure-monitor-agent-installed)

非永続的なライトバックキャッシュディスクを持つカタログの作成

非永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShell パラメーター `New-ProvScheme CustomProperties` を使用します。カスタムプロパティ `UseTempDiskForWBC` は、ライトバックキャッシュファイルを保存するために Azure 一時ストレージの使用を受け入れるかどうかを示します。一時ディスクをライトバックキャッシュディスクとして使用したい場合は、`New-ProvScheme` の実行時にこれを true に構成する必要があります。このプロパティが指定されていない場合、パラメーターはデフォルトで **False** に設定されます。

例えば、`CustomProperties` パラメーターを使用して `UseTempDiskForWBC` を **true** に設定する場合：

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/
> `
```

```
</CustomProperties>'
```

注:

マシンカタログをライトバックキャッシュファイルに Azure ローカル一時ストレージを使用するようにコミットした後、後で VHD を使用するように変更することはできません。

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。このパラメーターは、MCSプロビジョニングされたマシンに対してライトバックキャッシュディスクがどのように永続化するかを決定するために使用される追加のプロパティ`PersistWBC`をサポートします。`PersistWBC`プロパティは、`UseWriteBackCache`パラメーターが指定され、`WriteBackCacheDiskSize`パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

`PersistWBC`をサポートする前の`CustomProperties`パラメーターで見つかったプロパティの例は次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

これらのプロパティを使用する際は、`CustomProperties`パラメーターからプロパティが省略された場合、それらがデフォルト値を含むことを考慮してください。`PersistWBC`プロパティには、**true** または **false** の2つの値があります。

`PersistWBC`プロパティを**true**に設定すると、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC`プロパティを**false**に設定すると、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注:

`PersistWBC`プロパティが省略されている場合、プロパティはデフォルトで**false**になり、Web Studioを使用してマシンがシャットダウンされるとライトバックキャッシュは削除されます。

たとえば、`CustomProperties`パラメーターを使用して`PersistWBC`をtrueに設定するには：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

重要:

`PersistWBC`プロパティは、`New-ProvScheme` PowerShellコマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームの`CustomProperties`を変更しようと

しても、マシンカタログや、マシンがシャットダウンされたときのライトバックキャッシュディスクの永続性には影響しません。

たとえば、`New-ProvScheme`を設定してライトバックキャッシュを使用し、`PersistWBC`プロパティをtrueに設定するには：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127
```

```
-WriteBackCacheMemorySize 256
```

MCSIOを使用して起動パフォーマンスを向上させる

MCSIOが有効になっている場合、AzureおよびGCPマネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、PowerShellの`PersistOSDisk`カスタムプロパティを`New-ProvScheme`コマンドで使用します。`New-ProvScheme`に関連するオプションは次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk`カスタムプロパティを`true`に設定します。例：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"
```
```

```
-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

PowerShell を使用してカタログを作成または更新する際にテンプレート仕様を使用する

マシンプロファイルの入力としてテンプレート仕様を使用してMCSマシンカタログを作成または更新できます。これを行うには、Web StudioまたはPowerShellコマンドを使用できます。

Web Studioについては、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。(#create-a-machine-catalog-using-an-azure-resource-manager-image-in-web-studio)

PowerShellコマンドを使用する場合：

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. カタログを作成または更新します。
    - カタログを作成するには:
        a. テンプレート仕様をマシンプロファイルの入力として使用して、`New-ProvScheme` コマンドを使用します。例:

```
New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
image.folder/fgthj.resourcegroup/nab-ws-
vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>

[-LoggingId <Guid>]

[-BearerToken <String>][-AdminAddress <String>]

[<CommonParameters>]
```

b. カタログの作成を完了します。

- カタログを更新するには、テンプレート仕様をマシンプロファイルの入力として使用して、`Set-ProvScheme`コマンドを使用します。例:

```
Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
Us.region/vm.folder/MasterDisk.vm'

MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/testing.templatespec/V1.templatespecversion'

[-ProvisioningSchemeName] <String>

[-CustomProperties <String>][-ServiceOffering <String>] [-PassThru]

[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <String>]
[<CommonParameters>]
```

信頼された起動によるマシンカタログ

信頼された起動でマシンカタログを正常に作成するには、以下を使用します。

- 信頼された起動を備えたマシンプロファイル
- 信頼された起動をサポートするVMサイズ
- 信頼された起動をサポートするWindows VMバージョン。現在、Windows 10、Windows 11、Windows Server 2016、2019、および2022が信頼された起動をサポートしています。

重要:

MCSは、信頼された起動が有効なVMを使用して新しいカタログを作成することをサポートしています。ただし、既存の永続カタログと既存のVMを更新するには、Azureポータルを使用する必要があります。非永続カタログの信頼された起動を更新することはできません。詳細については、Microsoftドキュメント「既存のAzure VMで信頼された起動を有効にする」を参照してください。

Citrix Virtual Apps and Desktopsの提供インベントリアイテムを表示し、VMサイズが信頼された起動をサポートしているかどうかを判断するには、次のコマンドを実行します。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix*** を実行します。
3. 次のコマンドを実行します。

```
$s = (ls XDHyp:\HostingUnits\<name of hosting
unit>\serviceoffering.folder\"<VM size>.serviceoffering)
```

4. `$s | select -ExpandProperty Additionaldata` を実行します。
5. `SupportsTrustedLaunch` 属性の値を確認します。
   - もし `SupportsTrustedLaunch` が**True**の場合、VMサイズは信頼できる起動をサポートしています。
   - もし `SupportsTrustedLaunch` が**False**の場合、VMサイズは信頼できる起動をサポートしていません。

AzureのPowerShellに従って、信頼できる起動をサポートするVMサイズを特定するために、次のコマンドを使用できます。

```
(Get-AzComputeResourceSku | where {$_.Locations.Contains($region) -and
($_.Name -eq "<VM size>") })[0].Capabilities
```

Azure PowerShellコマンドを実行した後、VMサイズが信頼できる起動をサポートしているかどうかを説明する例を以下に示します。

- *例1*: Azure VMがGeneration 1のみをサポートしている場合、そのVMは信頼できる起動をサポートしていません。したがって、Azure PowerShellコマンドを実行しても、`TrustedLaunchDisabled`機能は表示されません。
- *例2*: Azure VMがGeneration 2のみをサポートし、`TrustedLaunchDisabled`機能が**True**の場合、Generation 2 VMサイズは信頼できる起動にはサポートされていません。
- *例3*: Azure VMがGeneration 2のみをサポートし、PowerShellコマンドを実行しても`TrustedLaunchDisabled`機能が表示されない場合、Generation 2 VMサイズは信頼できる起動にサポートされています。

Azure仮想マシンのトラステッド起動の詳細については、Microsoftドキュメント「Azure仮想マシンのトラステッド起動」を参照してください。

トラステッド起動でマシンカタログを作成する

1. 信頼できる起動が有効なマスターイメージを作成します。Microsoftドキュメント「Trusted launch VM Images」を参照してください。
2. セキュリティの種類を**信頼できる起動仮想マシン**としてVMまたはテンプレート仕様を作成します。VMまたはテンプレート仕様の作成の詳細については、Microsoftドキュメント「Deploy a trusted launch VM」を参照してください。
3. Web StudioまたはPowerShellコマンドを使用してマシンカタログを作成します。

   - Web Studioを使用する場合は、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure#create-a-machine-catalog-using-an-azure-resource-manager-image-in-web-studio)を参照してください。
   - PowerShellコマンドを使用する場合は、VMまたはテンプレート仕様をマシンプロファイルの入力として、`New-ProvScheme`コマンドを使用します。カタログを作成するためのコマンドの完全なリストについては、カタログの作成を参照してください。

     VMをマシンプロファイルの入力とする`New-ProvScheme`の例:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name"
     -IdentityPoolName "name" -InitialBatchSizeHint 1

     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
     fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     ```

```
-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<mac
hine profile vm.vm>"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

テンプレート仕様をマシンプロファイルの入力とする`New-ProvScheme`の例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name"
-IdentityPoolName "name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

信頼された起動でマシンカタログを作成する際のエラー

信頼された起動でマシンカタログを作成する際に、以下のシナリオで適切なエラーが発生します。

シナリオ	エラー
アンマネージドカタログの作成中にマシンプロファイルを選択した場合	`MachineProfileNotSupportedForUnmanagedCatalog`
マスターイメージとしてアンマネージドディスクを使用するカタログの作成中に、信頼できる起動をサポートするマシンプロファイルを選択した場合	`SecurityTypeNotSupportedForUnmanagedDisk`
セキュリティの種類として信頼できる起動を持つマスターイメージソースでマネージドカタログを作成する際に、マシンプロファイルを選択しなかった場合	`MachineProfileNotFoundForTrustedLaunchMasterImage`
マスターイメージのセキュリティの種類とは異なるセキュリティの種類を持つマシンプロファイルを選択した場合	`SecurityTypeConflictBetweenMasterImageAndMachineProfile`
カタログ作成時に、信頼できる起動をサポートしないVMサイズを選択したが、信頼できる起動をサポートするマスターイメージを使用した場合	`MachineSizeNotSupportTrustedLaunch`

マシンプロファイルプロパティ値の使用

マシンカタログでは、カスタムプロパティで定義されている次のプロパティが使用されます。

- アベイラビリティゾーン
- 専用ホストグループID
- ディスク暗号化セットID
- OSの種類
- ライセンスの種類
- ストレージの種類

これらのカスタムプロパティが明示的に定義されていない場合、プロパティ値は、マシンプロファイルとして使用されるARMテンプレート仕様またはVMから設定されます。さらに、`ServiceOffering`が指定されていない場合、マシンプロファイルから設定されます。

> **注：**

> マシンプロファイルから一部のプロパティが欠落しており、カスタムプロパティで定義されていない場合、該当する場所ではプロパティのデフォルト値が適用されます。

> 次のセクションでは、`CustomProperties`がすべてのプロパティを定義しているか、値がMachineProfileから派生している場合の、`New-ProvScheme`および`Set-ProvScheme`でのいくつかのシナリオについて説明します。

- New-ProvScheme シナリオ
  - MachineProfile にすべてのプロパティがあり、CustomProperties が定義されていない場合。例:

    `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

    カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>
```

```
</CustomProperties>
```

- MachineProfile に一部のプロパティがあり、CustomProperties が定義されていない場合。例: MachineProfile には LicenseType と OsType のみがあります。

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

  カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>

</CustomProperties>
```

- MachineProfile と CustomProperties の両方がすべてのプロパティを定義している場合。例:

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

  カスタムプロパティが優先されます。カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>
```

```
<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones"
Value="<CustomPropertiesA-value>"/>

</CustomProperties>
```

- MachineProfile に一部のプロパティが定義されており、CustomProperties に一部のプロパティが定義されている場合。例:
  - CustomProperties は LicenseType と StorageAccountType を定義します
  - MachineProfile は LicenseType、OsType、および Zones を定義します

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>
```

```
<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- 一部のプロパティはMachineProfileで定義されており、一部のプロパティはCustomPropertiesで定義されています。さらに、ServiceOfferingは定義されていません。
例:
  - CustomProperties は StorageType を定義します
  - MachineProfile は LicenseType を定義します

```
New-ProvScheme -MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mp
.vm"

-ServiceOffering "XDHyp:
\HostingUnits\azureunit\serviceoffering.folder\<explicit-machine-
size>.serviceoffering"
```

以下の値がカタログのカスタムプロパティとして設定されます:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<explicit-machine-size>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="explicit-storage-type"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="value-
```

```
from-machineprofile"/>

</CustomProperties>
```

- OsTypeがCustomPropertiesにもMachineProfileにもない場合、次のようになります:
  - 値はマスターイメージから読み取られます。
  - マスターイメージがアンマネージドディスクの場合、OsTypeはWindowsに設定されます。例:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -MasterImageVM "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-image.manageddisk"`

マスターイメージからの値は、この場合 Linux のカスタムプロパティに書き込まれます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="Linux"/>

</CustomProperties>
```

- Set-ProvSchemeのシナリオ
  - 既存のカタログで:
    - `StorageAccountType`およびOsTypeのCustomProperties
    - ゾーンを定義するMachineProfile `mpA.vm`
  - 更新:
    - StorageAccountType を定義する MachineProfile mpB.vm
    - LicenseType と OsType を定義する新しいカスタムプロパティセット $CustomPropertiesB

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm" -CustomProperties $CustomPropertiesB`

カタログのカスタムプロパティとして、以下の値が設定されています。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesB-value>"/>

    </CustomProperties>
```

- 既存のカタログで、以下を含むもの:
  - S`torageAccountType` と OsType の CustomProperties
  - StorageAccountType と LicenseType を定義する MachineProfile `mpA.vm`
- 更新:
  - StorageAccountType と OsType を定義する新しいカスタムプロパティセット $CustomPropertiesB。

`Set-ProvScheme -CustomProperties $CustomPropertiesB`

カタログのカスタムプロパティとして、以下の値が設定されています。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
```

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mp-A-
value>"/>

</CustomProperties>
```

- 既存のカタログで、以下を含むもの:
  - `StorageAccountType` と OsType の CustomProperties
  - Zones を定義する MachineProfile `mpA.vm`
- 更新:
  - StorageAccountType と LicenseType を定義する MachineProfile mpB.vm
  - `ServiceOffering`は指定されていません

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm"`

カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<value-from-machineprofile>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<prior-
```

```
CustomProperties-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpB-
value>"/>

</CustomProperties>
```

Azure Monitor Agentがインストールされたカタログ VMをプロビジョニングする

Azure監視は、Azureおよびオンプレミス環境からのテレメトリデータを収集、分析、および処理するために使用できるサービスです。

Azure Monitor Agent (AMA) は、仮想マシンなどのコンピューティングリソースから監視データを収集し、そのデータをAzure Monitorに配信します。現在、イベントログ、Syslog、パフォーマンスメトリックの収集をサポートしており、Azure Monitor MetricsおよびAzure Monitor Logsデータソースに送信します。

監視データ内のVMを一意に識別して監視を有効にするには、AMAを拡張機能としてインストールしたMCSマシンカタログのVMをプロビジョニングできます。

要件

- 権限: Azure権限についてに指定されている最小限のAzure権限と、Azure Monitorを使用するための次の権限があることを確認してください。
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- データ収集ルール: Azureポータルでデータ収集ルールを設定します。DCRの設定については、データ収集ルールを作成するを参照してください。DCRはプラットフォーム固有（WindowsまたはLinux）です。必要なプラットフォームに応じてDCRを作成してください。 AMAは、データ収集ルール (DCR) を使用して、VMなどのリソースと、Azure Monitor MetricsやAzure Monitor Logsなどのデータソース間のマッピングを管理します。
- デフォルトワークスペース: Azureポータルでワークスペースを作成します。ワークスペースの作成については、「Log Analyticsワークスペースの作成」を参照してください。ログとデータを収集すると、その情報はワークスペースに保存されます。ワークスペースには、一意のワークスペースIDとリソースIDがあります。ワークスペース名は、指定されたリソースグループ内

で一意である必要があります。ワークスペースを作成したら、データソースとソリューションを設定して、そのデータをワークスペースに保存します。

- 監視拡張機能のホワイトリスト登録: 拡張機能 `AzureMonitorWindowsAgent` および `AzureMonitorLinuxAgent` は、Citrixが定義したホワイトリスト登録済み拡張機能です。ホワイトリスト登録済み拡張機能のリストを表示するには、PoSHコマンド `Get-ProvMetadataConfiguration` を使用します。
- マスターイメージ: Microsoftは、既存のマシンから新しいマシンを作成する前に、既存のマシンから拡張機能を削除することを推奨しています。拡張機能が削除されない場合、残存ファイルや予期しない動作につながる可能性があります。詳細については、「既存のVMからVMを再作成する場合」を参照してください。

AMA を有効にしてカタログ VM をプロビジョニングするには:

1. マシンプロファイルテンプレートを設定します。
   - VMをマシンプロファイルテンプレートとして使用する場合：
     a. Azure portal で VM を作成します。
     b. VMの電源を入れます。
     c. **リソース**の下のデータ収集ルールにVMを追加します。これにより、テンプレートVMにエージェントのインストールが呼び出されます。

> **注:**
>
> Linuxカタログを作成する必要がある場合は、Linuxマシンを設定します。

   - テンプレート仕様をマシンプロファイルテンプレートとして使用する場合：
     a. テンプレート仕様を設定します。
     b. 生成されたテンプレート仕様に、次の拡張機能とデータ収集ルール関連付けを追加します。

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",

"apiVersion": "2022-03-01",
```

```
"name": "<vm-name>/AzureMonitorWindowsAgent",

"dependsOn": [

    "Microsoft.Compute/virtualMachines/<vm-name>"

],

"location": "<azure-region>",

"properties": {

    "publisher": "Microsoft.Azure.Monitor",

    "type": "AzureMonitorWindowsAgent",

    "typeHandlerVersion": "1.0",

    "autoUpgradeMinorVersion": true,

    "enableAutomaticUpgrade": true

}

},

 {

    "type": "Microsoft.Insights/dataCollectionRuleAssociations",

    "apiVersion": "2021-11-01",

    "name": "<associatio-name>",

    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",

    "dependsOn": [

     "Microsoft.Compute/virtualMachines/<vm-name>",

    "Microsoft.Compute/virtualMachines/<vm-name>/extensions/
AzureMonitorWindowsAgent"
```

```
    ],

    "properties": {

       "description": "Association of data collection rule.
Deleting this association will break the data collection for this
Arc server.",

     "dataCollectionRuleId": "/subscriptions/<azure-
subscription>/resourcegroups/<azure-resource-group>/providers/
microsoft.insights/datacollectionrules/<azure-data-collection-
rule>"

     }

    }
```

2. 既存のMCSマシンカタログを作成または更新します。

   - 新しいMCSカタログを作成するには:

     a. Web Studio で、その VM またはテンプレート仕様をマシンプロファイルとして選択します。

     b. カタログを作成するための次の手順に進みます。

   - 既存の MCS カタログを更新するには、次の PoSH コマンドを使用します。

     - 新しい VM に更新されたマシンプロファイルテンプレートを取得させるには、次のコマンドを実行します。

```
Set-ProvScheme -ProvisioningSchemeName "name"

-MachineProfile "XDHyp:
\HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-
machine-profile.vm"
```

     - 既存の VM を更新されたマシンプロファイルテンプレートで更新するには：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

3. カタログVMの電源を入れます。
4. Azure portal に移動し、モニター拡張機能が VM にインストールされていること、および VM が DCR のリソースの下に表示されていることを確認します。数分後、監視データが Azure Monitor に表示されます。

トラブルシューティング

Azure Monitor Agentのトラブルシューティングガイダンスについては、以下を参照してください。

- https://learn.microsoft.com/ja-jp/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/ja-jp/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

顧客管理の暗号化キーでマシンカタログを作成する

顧客管理の暗号化キーを使用してマシンカタログを作成する詳細な手順は次のとおりです。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. `cd xdhyp:/`を入力します。
4. `cd .\HostingUnits\(your hosting unit)`を入力します。
5. `cd diskencryptionset.folder`を入力します。
6. ディスク暗号化セットのリストを取得するために`dir`を入力します。
7. ディスク暗号化セットのIDをコピーします。
8. ディスク暗号化セットのIDを含めるカスタムプロパティ文字列を作成します。例：

```
$customProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"persistWBC`"
Value=`"False`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"false`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/resourceGroups/
abc/providers/Microsoft.Compute/diskEncryptionSets/abc-des`"/>

</CustomProperties>
```

9. まだ作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain def.local -NamingSchemeType Numeric
```

10. New-ProvSchemeコマンドを実行します。例：

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\azure-
res2\image.folder\def.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-res2\
\virtualprivatecloud.folder\def.resourcegroup\def-
vnet.virtualprivatecloud\subnet1.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\azure-
res2\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<machin
e profile vm.vm>"

-CustomProperties $customProperties
```

11. マシンカタログの作成を完了します。

二重暗号化でマシンカタログを作成する

Web Studio および PowerShell コマンドを使用して、二重暗号化されたマシンカタログを作成および更新できます。

二重暗号化されたマシンカタログを作成する詳細な手順は次のとおりです。

1. プラットフォーム管理キーと顧客管理キーを使用してAzure Key VaultとDESを作成します。Azure Key VaultとDESの作成方法については、「マネージドディスクの保存時の二重暗号化を有効にするためにAzureポータルを使用する」を参照してください。
2. ホスティング接続で利用可能なDiskEncryptionSetsを参照するには:

   a. **PowerShell** ウィンドウを開きます。

   b. 次のPowerShellコマンドを実行します。

      i. `asnp citrix*`

      ii. `cd xdhyp:`:

      iii. `cd HostingUnits`

      iv. `cd YourHostingUnitName`（例えば、azure-east）

      v. `cd diskencryptionset.folder`

      vi. `dir`

   `DiskEncryptionSet` のIDを使用して、カスタムプロパティでカタログを作成または更新できます。
3. マシンプロファイルワークフローを使用する場合は、VMまたはテンプレート仕様をマシンプロファイルの入力として作成します。

   - VMをマシンプロファイルの入力として使用する場合は、:

     a. Azure PortalでVMを作成します。

     b. **ディスク>キー管理** に移動し、`DiskEncryptionSetID` を使用してVMを直接暗号化します。

   - テンプレート仕様をマシンプロファイルの入力として使用する場合は、:

     a. テンプレートで、`properties>storageProfile>osDisk>managedDisk` の下に、`diskEncryptionSet` パラメーターを追加し、二重暗号化DESのIDを追加します。
4. マシンカタログを作成します。

- Web Studioを使用している場合は、マシンカタログの作成の手順に加えて、次のいずれかを実行します。
  - マシンプロファイルベースのワークフローを使用しない場合は、**ディスク設定**ページで、**次のキーを使用して各マシン上のデータを暗号化する**を選択します。次に、ドロップダウンリストから二重暗号化DESを選択します。カタログの作成を続行します。
  - マシンプロファイルワークフローを使用している場合は、**マスターイメージ**ページでマスターイメージとマシンプロファイルを選択します。マシンプロファイルのプロパティにディスク暗号化セットIDがあることを確認してください。

  カタログで作成されたすべてのマシンは、選択した DES に関連付けられたキーによって二重に暗号化されます。
- PowerShellコマンドを使用する場合は、次のいずれかを実行します。
  - マシンプロファイルベースのワークフローを使用しない場合は、`New-ProvScheme`コマンドにカスタムプロパティ`DiskEncryptionSetId`を追加します。例:

```
New-ProvScheme -CleanOnBoot -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />

</CustomProperties>'

-HostingUnitName "Redacted"

-IdentityPoolName "Redacted"

-InitialBatchSizeHint 1

-MasterImageVM "Redacted"
```

```
-NetworkMapping @{"0"="Redacted"}

-ProvisioningSchemeName "Redacted"

-ServiceOffering "Redacted"
```

- マシンプロファイルベースのワークフローを使用する場合は、`New-ProvScheme`コマンドでマシンプロファイル入力を利用します。例:

```
New-ProvScheme -CleanOnBoot

-HostingUnitName azure-east

-IdentityPoolName aio-ip

-InitialBatchSizeHint 1

-MasterImageVM XDHyp:\HostingUnits\azure-
east\image.folder\abc.resourcegroup\fgb-vda-snapshot.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-
east\virtualprivatecloud.folder\apa-
resourceGroup.resourcegroup\apa-resourceGroup-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName aio-test

-MachineProfile XDHyp:\HostingUnits\azure-
east\machineprofile.folder\abc.resourcegroup\abx-
mp.templatespec\1.0.0.templatespecversion
```

5. リモートPowerShell SDKを使用してカタログの作成を完了します。リモートPowerShell SDKを使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。カタログで作成されたすべてのマシンは、選択したDESに関連付けられたキーによって二重に暗号化されます。

暗号化されていないカタログを二重暗号化を使用するように変換する

マシンカタログの暗号化タイプ（カスタムプロパティまたはマシンプロファイルを使用）は、カタログが以前に暗号化されていなかった場合にのみ更新できます。

- マシンプロファイルベースのワークフローを使用しない場合は、`Set-ProvScheme`コマンドにカスタムプロパティDiskEncryptionSetIdを追加します。例:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/12345678-xxxx-1234-1234-123456789012/resourceGroups/
Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/
SampleEncryptionSet" />

</CustomProperties>'
```

- マシンプロファイルベースのワークフローを使用する場合は、`Set-ProvScheme`コマンドでマシンプロファイル入力を利用します。例:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
XDHyp:\HostingUnits\azure-
east\machineprofile.folder\aelx.resourcegroup\elx-
mp.templatespec\1.0.0.templatespecversion
```

成功すると、カタログに追加するすべての新しいVMは、選択したDESに関連付けられたキーによって二重暗号化されます。

カタログが二重暗号化されていることを確認する

- ウェブスタジオで:

  a. **マシンカタログ**に移動します。

  b. 確認するカタログを選択します。画面下部にある**テンプレートプロパティ**タブをクリックします。

  c. **Azureの詳細**の下で、**ディスク暗号化セット**のディスク暗号化セットIDを確認します。カタログのDES IDが空白の場合、カタログは暗号化されていません。

  d. Azure Portal で、DES ID に関連付けられている DES の暗号化の種類がプラットフォーム管理キーと顧客管理キーであることを確認します。

- PowerShellコマンドを使用する:

a. **PowerShell** ウィンドウを開きます。

b. `asnp citrix*` を実行して、Citrix 固有の PowerShell モジュールをロードします。

c. `Get-ProvScheme` を使用して、マシンカタログの情報を取得します。例:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

d. マシンカタログの DES ID カスタムプロパティを取得します。例:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-1234-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />
```

e. Azure Portal で、DES ID に関連付けられている DES の暗号化の種類がプラットフォーム管理キーと顧客管理キーであることを確認します。

Azureエフェメラルディスクを使用してカタログを作成する

エフェメラルディスクを使用するには、`New-ProvScheme` の実行時にカスタムプロパティ `UseEphemeralOsDisk` を **true** に設定する必要があります。

注:

カスタムプロパティ`UseEphemeralOsDisk`が**false**に設定されているか、値が指定されていない場合、プロビジョニングされたすべてのVDAはプロビジョニングされたOSディスクを引き続き使用します。

以下は、プロビジョニングスキームで使用するカスタムプロパティのセットの例です。

```
"CustomProperties": [

            {

                "Name": "UseManagedDisks",

                "Value": "true"

            },
```

```
        {
            "Name": "StorageType",
            "Value": "Standard_LRS"
        },
        {
            "Name": "UseSharedImageGallery",
            "Value": "true"
        },
        {
            "Name": "SharedImageGalleryReplicaRatio",
            "Value": "40"
        },
        {
            "Name": "SharedImageGalleryReplicaMaximum",
            "Value": "10"
        },
        {
            "Name": "LicenseType",
            "Value": "Windows_Server"
        },
        {
            "Name": "UseEphemeralOsDisk",
```

```
                "Value": "true"

            }

        ],
```

カタログのエフェメラルディスクを構成する

カタログのAzureエフェメラルOSディスクを構成するには、`Set-ProvScheme`の`UseEphemeralOsDisk`パラメーターを使用します。`UseEphemeralOsDisk`パラメーターの値を**true**に設定します。

> **注:**
>
> この機能を使用するには、`UseManagedDisks`と`UseSharedImageGallery`のパラメーターも有効にする必要があります。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

エフェメラルディスクに関する重要な考慮事項

`New-ProvScheme`を使用してエフェメラルOSディスクをプロビジョニングするには、次の制約を考慮してください。

- カタログに使用されるVMサイズは、エフェメラルOSディスクをサポートしている必要があります。
- VMサイズに関連付けられているキャッシュまたは一時ディスクのサイズは、OSディスクのサイズ以上である必要があります。
- 一時ディスクのサイズは、キャッシュディスクのサイズよりも大きくする必要があります。

以下の際にもこれらの問題を考慮してください:

- プロビジョニングスキームを作成する際。
- プロビジョニングスキームを変更する際。
- イメージを更新する際。

Azure 専用ホスト

MCS を使用して、Azure 専用ホストに VM をプロビジョニングできます。Azure 専用ホストに VM をプロビジョニングする前に、次の手順を実行します。

- ホストグループを作成します。
- そのホストグループにホストを作成します。
- カタログと仮想マシンを作成するために、十分なホスト容量が予約されていることを確認してください。

次の PowerShell スクリプトを使用して、ホストテナンシーが定義されたマシンのカタログを作成できます。

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
Value="myResourceGroup/myHostGroup" />

 ...other Custom Properties...

 </CustomProperties>
```

MCS を使用して Azure 専用ホストに仮想マシンをプロビジョニングする場合、次の点を考慮してください。

- *専用ホスト*はカタログプロパティであり、カタログ作成後に変更することはできません。専用テナンシーは現在、Azure ではサポートされていません。
- `HostGroupId` パラメーターを使用する場合、ホスティングユニットのリージョンに事前に構成された Azure ホストグループが必要です。
- Azure の自動配置が必要です。この機能は、ホストグループに関連付けられたサブスクリプションをオンボードする要求を行います。詳細については、「VM Scale Set on Azure Dedicated Hosts - Public Preview」を参照してください。自動配置が有効になっていない場合、MCS はカタログ作成中にエラーをスローします。

Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する

マシンカタログを作成するために使用するイメージを選択する際、Azure Compute Gallery で作成したイメージを選択できます。

これらのイメージを表示するには、次の手順を実行する必要があります。

1. Citrix Virtual Apps and Desktops サイトを構成します。
2. Azure Resource Manager に接続します。
3. Azureポータルで、リソースグループを作成します。詳細については、「ポータルを使用してAzure Compute Galleryを作成する」を参照してください。
4. リソースグループで、Azure Compute Galleryを作成します。
5. Azure Compute Galleryで、イメージ定義を作成します。
6. イメージ定義で、イメージバージョンを作成します。

Azure Compute Galleryのイメージを使用してマシンカタログを作成または更新するには、次のPowerShellコマンドを使用します。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group")
```

4. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery")
```

5. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery\sigtestimage.imagedefinitio
n")
```

6. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

   Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。

共有イメージギャラリーの構成

`New-ProvScheme` コマンドを使用して、Shared Image Gallery をサポートするプロビジョニングスキームを作成します。`Set-ProvScheme` コマンドを使用して、プロビジョニングスキームのこの機能を有効または無効にし、レプリカ比率とレプリカの最大値を変更します。

共有イメージギャラリー機能をサポートするために、プロビジョニングスキームに3つのカスタムプロパティが追加されました。

`UseSharedImageGallery`

- 公開されたイメージの保存に Shared Image Gallery を使用するかどうかを定義します。**True** に設定すると、イメージは Shared Image Gallery イメージとして保存され、それ以外の場合はスナップショットとして保存されます。
- 有効な値は**True**と**False**です。
- プロパティが定義されていない場合、デフォルト値は**False**です。

`SharedImageGalleryReplicaRatio`

- マシンとギャラリーイメージバージョンレプリカの比率を定義します。
- 有効な値は0より大きい整数です。
- プロパティが定義されていない場合、デフォルト値が使用されます。永続OSディスクのデフォルト値は1000、非永続OSディスクのデフォルト値は40です。

`SharedImageGalleryReplicaMaximum`

- 各ギャラリーイメージバージョンのレプリカの最大数を定義します。
- 有効な値は0より大きい整数です。
- プロパティが定義されていない場合、デフォルト値は10です。
- Azureは現在、ギャラリーイメージの単一バージョンに対して最大10個のレプリカをサポートしています。プロパティがAzureでサポートされている値よりも大きい値に設定されている場合、MCSは指定された値を使用しようとします。Azureはエラーを生成し、MCSはそれをログに記録し、現在のレプリカ数は変更されません。

> **ヒント:**
>
> MCS プロビジョニングカタログの公開イメージを保存するために Shared Image Gallery を使用する場合、MCS はカタログ内のマシンの数、レプリカ比率、およびレプリカの最大値に基づいて、ギャラリーイメージバージョンのレプリカ数を設定します。レプリカ数は、カタログ内のマシンの数をレプリカ比率で除算し（最も近い整数に切り上げ）、その値を最大レプリカ数で制限することによって計算されます。たとえば、レプリカ比率が20、最大値が5の場合、0〜20台のマシンには1つのレプリカが作成され、21〜40台には2つのレプリカ、41〜60台には3つのレプリカ、61〜80台には4つのレプリカ、81台以上には5つのレプリカが作成されます。

ユースケース: Shared Image Galleryのレプリカ比率とレプリカ最大値の更新

既存のマシンカタログは Shared Image Gallery を使用しています。`Set-ProvScheme` コマンドを使用して、カタログ内のすべての既存マシンおよび将来のマシンのカスタムプロパティを更新します。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
```

```
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ユースケース: スナップショットカタログをShared Image Galleryカタログに変換する

このユースケースの場合:

1. `UseSharedImageGallery`フラグを**True**に設定して`Set-ProvScheme`を実行します。オプションで`SharedImageGalleryReplicaRatio`および`SharedImageGalleryReplicaMaximum`プロパティを含めます。
2. カタログを更新します。
3. マシンをパワーサイクルして、更新を強制します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ヒント:

パラメータ`SharedImageGalleryReplicaRatio`と`SharedImageGalleryReplicaMaximum`は必須ではありません。`Set-ProvScheme`コマンドが完了しても、Shared Image Galleryイメージはまだ作成されていません。カタログがギャラリーを使用するように構成されると、次のカタログ更新操作で公開イメージがギャラリーに保存されます。カタログ更新コマンドは、ギャラリー、ギャラリーイメージ、およびイメージバージョンを作成します。マシンをパワーサイクルすると更新され、その時点で必要に応じてレプリカ数が更新されます。それ以降、既存のすべての非永続マシンはShared

> Image Galleryイメージを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはイメージを使用して作成されます。古いスナップショットは数時間以内に自動的にクリーンアップされます。

ユースケース: Shared Image Galleryカタログをスナップショットカタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery` フラグを **False** に設定するか、未定義のままにして `Set-ProvScheme` を実行します。
2. カタログを更新します。
3. マシンをパワーサイクルして、強制的に更新します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

> **ヒント:**
>
> スナップショットから共有イメージギャラリーカタログへの更新とは異なり、各マシンのカスタムデータは、新しいカスタムプロパティを反映するようにまだ更新されていません。元の共有イメージギャラリーのカスタムプロパティを表示するには、次のコマンドを実行します: `Get-ProvVm -ProvisioningSchemeName catalog-name`。`Set-ProvScheme`コマンドが完了しても、イメージスナップショットはまだ作成されていません。カタログがギャラリーを使用しないように構成されると、次回のカタログ更新操作で公開されたイメージがスナップショットとして保存されます。その時点から、既存のすべての非永続マシンはスナップショットを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはスナップショットから作成されます。マシンをパワーサイクルすると更新され、その時点でカスタムマシンデータが更新され、`UseSharedImageGallery`が**False**に設定されていることが反映されます。古い共有イメージギャラリーのアセット（ギャラリー、イメージ、バージョン）は、数時間以内に自動的にクリーンアップされます。

指定された可用性ゾーンにマシンをプロビジョニングする

Azure環境では、特定の可用性ゾーンにマシンをプロビジョニングできます。これはPowerShellを使用して実現できます。

> **注:**
>
> ゾーンが指定されていない場合、MCSはAzureにリージョン内にマシンを配置させます。複数のゾーンが指定されている場合、MCSはそれらのゾーンにマシンをランダムに分散させます。

PowerShellによるアベイラビリティゾーンの構成

PowerShellを使用して、`Get-Item`で提供されているインベントリアイテムを表示できます。たとえば、*米国東部リージョン*の`Standard_B1ls`サービス提供を表示するには：

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

ゾーンを表示するには、アイテムの`AdditionalData`パラメーターを使用します:

`$serviceOffering.AdditionalData`

可用性ゾーンが指定されていない場合、マシンのプロビジョニング方法に変更はありません。

PowerShell を介して可用性ゾーンを構成するには、`New-ProvScheme` 操作で利用できる **Zones** カスタムプロパティを使用します。**Zones** プロパティは、マシンをプロビジョニングする可用性ゾーンのリストを定義します。これらのゾーンには、1つ以上の可用性ゾーンを含めることができます。たとえば、ゾーン1と3の場合は `<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>` となります。

プロビジョニングスキームのゾーンを更新するには、`Set-ProvScheme`コマンドを使用します。

無効なゾーンが提供された場合、プロビジョニングスキームは更新されず、無効なコマンドを修正する方法に関する指示を提供するエラーメッセージが表示されます。

> **ヒント:**

無効なカスタムプロパティを指定すると、プロビジョニングスキームは更新されず、関連するエラーメッセージが表示されます。

ストレージの種類

MCS を使用する Azure 環境の仮想マシンには、異なるストレージの種類を選択します。ターゲット VM の場合、MCS は以下をサポートします。

- OS ディスク: Premium SSD、SSD、または HDD
- ライトバックキャッシュディスク: Premium SSD、SSD、または HDD

これらのストレージの種類を使用する場合、以下を考慮してください。

- 選択したストレージの種類をVMがサポートしていることを確認してください。
- 構成でAzureエフェメラルディスクを使用している場合、ライトバックキャッシュディスク設定のオプションは表示されません。

ヒント:

`StorageType` はOSタイプとストレージアカウント用に構成されます。`WBCDiskStorageType` はライトバックキャッシュストレージタイプ用に構成されます。通常のカタログの場合、`StorageType` が必要です。`WBCDiskStorageType` が構成されていない場合、`StorageType` が `WBCDiskStorageType` のデフォルトとして使用されます。

WBCDiskStorageType が構成されていない場合、StorageType が WBCDiskStorageType のデフォルトとして使用されます。

ストレージの種類を構成する

VMのストレージタイプを構成するには、`New-ProvScheme` の `StorageType` パラメーターを使用します。`StorageType` パラメーターの値をサポートされているストレージタイプのいずれかに設定します。

以下は、プロビジョニングスキームにおける `CustomProperties` パラメーターの設定例です。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>'
```

ゾーン冗長ストレージを有効にする

カタログ作成時にゾーン冗長ストレージを選択できます。これにより、Azure マネージドディスクが複数のアベイラビリティゾーン間で同期的にレプリケートされ、あるゾーンでの障害発生時に他のゾーンの冗長性を利用して復旧できます。

ストレージタイプのカスタムプロパティで **Premium_ZRS** および **StandardSSD_ZRS** を指定できます。ZRSストレージは、既存のカスタムプロパティを使用するか、**MachineProfile** テンプレートを介して設定できます。ZRSストレージは、`-StartsNow` および `-DurationInMinutes -1` パラメーターを持つ `Set-ProvVMUpdateTimeWindow` コマンドでもサポートされており、既存のマシンをLRSからZRSストレージに変更できます。

制限事項:

- マネージドディスクのみをサポート
- プレミアムおよび標準ソリッドステートドライブ (SSD) のみでサポート
- `StorageTypeAtShutdown` ではサポートされていません
- 特定のリージョンでのみ利用可能。
- 大規模に ZRS ディスクを作成すると、Azure のパフォーマンスが低下します。そのため、最初の電源投入時には、マシンを小規模なバッチ (一度に 300 台未満) で起動してください。

ゾーン冗長ストレージをディスクストレージの種類として設定する

ゾーン冗長ストレージは、最初のカタログ作成時に選択することも、既存のカタログでストレージの種類を更新することもできます。

POWERSHELL コマンドを使用してゾーン冗長ストレージを選択する

Azure で新しいカタログを作成する際に、`New-ProvScheme` PowerShell コマンドを使用する場合、`StorageAccountType` の値として `Standard_ZRS` を使用します。 例:

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_ZRS" />
```

この値を設定すると、それが適切に使用できるかどうかを判断する動的APIによって検証されます。カタログでZRSの使用が有効でない場合、次の例外が発生する可能性があります:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: StorageTypeAtShutdownカスタムプロパティはZRSストレージでは使用できません。
- **StorageAccountTypeNotSupportedInRegion**: この例外は、ZRSをサポートしていないAzureリージョンでZRSストレージを使用しようとすると発生します。
- **ZrsRequiresManagedDisks**: ゾーン冗長ストレージは、マネージドディスクでのみ使用できます。

次のカスタムプロパティを使用して、ディスクストレージタイプを設定できます:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **注:**
>
> カタログ作成時、カスタムプロパティが設定されていない場合、マシンプロファイルのOSディスク `StorageType` が使用されます。

マシンプロファイルからVMとNICの診断設定をキャプチャする

マシンカタログの作成時、既存のマシンカタログの更新時、および既存のVMの更新時に、マシンプロファイルからVMとNICの診断設定をキャプチャできます。

VMまたはテンプレート仕様をマシンプロファイルのソースとして作成できます。

主な手順

1. Azureで必要なIDを設定します。これらのIDはテンプレート仕様で指定する必要があります。
    - ストレージアカウント
    - Log Analyticsワークスペース
    - 標準ティアの価格設定を持つイベントハブの名前空間

2. マシンプロファイルのソースを作成します。
3. 新しいマシンカタログを作成するか、既存のカタログを更新するか、既存のVMを更新します。

Azureで必要なIDを設定する

Azureで次のいずれかを設定します。

- ストレージアカウント
- Log Analyticsワークスペース
- 標準ティアの価格設定を持つイベントハブの名前空間

ストレージアカウントを設定する

Azureで標準ストレージアカウントを作成します。テンプレート仕様では、ストレージアカウントの完全なresourceIdを`storageAccountId`として指定します。

VMがストレージアカウントにデータをログするように設定されると、データは`insights-metrics-pt1m`コンテナの下で見つけることができます。

ログ分析ワークスペースを設定する

ログ分析ワークスペースを作成します。テンプレート仕様では、ログ分析ワークスペースの完全なresourceIdをworkspaceIdとして指定します。

VMがワークスペースにデータをログ記録するように設定されると、Azureのでデータをクエリできます。Azureので次のコマンドを実行すると、リソースによってログ記録されたすべてのメトリックの数を表示できます。

```
AzureMetrics | summarize Count=count() by ResourceId
```

イベントハブを設定する

Azureポータルでイベントハブを設定するには、次の手順を実行します。

1. 標準ティアの価格設定でイベントハブ名前空間を作成します。
2. 名前空間の下にイベントハブを作成します。
3. イベントハブの下にある****に移動します。Avro出力タイプでキャプチャするようにトグルをオンにします。
4. ログをキャプチャするために、既存のストレージアカウントに新しいコンテナを作成します。
5. テンプレートスペックで、次の形式で`eventHubAuthorizationRuleId`を指定します: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/`

`providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`

6. イベントハブの名前を指定します。

VMがイベントハブにデータをログ記録するように設定されると、データは構成されたストレージコンテナにキャプチャされます。

マシンプロファイルソースを作成する

VMまたはテンプレートスペックをマシンプロファイルソースとして作成できます。

診断設定を含むVMベースのマシンプロファイルを作成する

VMをマシンプロファイルとして作成する場合は、まずテンプレートVM自体に診断設定をセットアップします。詳細な手順については、MicrosoftドキュメントのAzure Monitor の診断設定を参照してください。

VMまたはNICに関連付けられた診断設定が現在存在することを確認するには、次のコマンドを実行できます。

```
az monitor diagnostic-settings list --resource-group matspo --resource matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

診断設定を含むテンプレートスペックベースのマシンプロファイルを作成する

診断設定がすでに有効になっているVMを使用し、それをARMテンプレートスペックにエクスポートする場合、これらの設定はテンプレートに自動的に含まれません。ARMテンプレート内で診断設定を手動で追加または変更する必要があります。

ただし、VMをマシンプロファイルとして使用する場合、MCSは、重要な診断設定が正確にキャプチャされ、MCSカタログ内のリソースに適用されることを保証します。

1. VMとNICを定義する標準テンプレート仕様を作成します。
2. 仕様に従って診断設定をデプロイするための追加リソースを追加します: Microsoft.Insights diagnosticSettings。スコープについては、テンプレート内のVMまたはNICを部分的なIDを持つ名前で参照します。たとえば、テンプレート仕様内のtest-VMという名前のVMにアタッチされた診断設定を作成する場合、スコープを次のように指定します。

```
"scope": "microsoft.compute/virtualMachines/test-VM",
```

3. テンプレートスペックをマシンプロファイルソースとして使用します。

診断設定を含むカタログを作成または更新する

マシンプロファイルソースを作成した後、`New-ProvScheme`コマンドを使用してマシンカタログを作成したり、`Set-ProvScheme`コマンドを使用して既存のマシンカタログを更新したり、`Request-ProvVMUpdate`コマンドを使用して既存のVMを更新したりできます。

ページファイルの場所

Azure環境では、VMが最初に作成されるときにページファイルが適切な場所に設定されます。ページファイルの設定は`<page file location>[min size] [max size]`の形式で構成されます（サイズはMB単位）。詳細については、Microsoftドキュメントの適切なページファイルを決定する方法を参照してください。

イメージ準備中に`ProvScheme`を作成すると、MCSは特定のルールに基づいてページファイルの場所を決定します。`ProvScheme`を作成した後：

- 受信VMサイズによってページファイル設定が異なる場合、VMサイズの変更はブロックされます。
- マシンプロファイルの更新によりページファイル設定が異なるため、サービスオファリングが変更された場合、マシンプロファイルの更新はブロックされます。
- エフェメラルOSディスク (EOS) およびMCSIOのプロパティは変更できません。

ページファイルの場所の決定

EOSやMCSIOなどの機能には、それぞれ独自の予期されるページファイルの場所があり、互いに排他的です。次の表は、各機能の予期されるページファイルの場所を示しています。

機能	予期されるページファイルの場所
EOS	OSディスク
MCSIO	まずAzure一時ディスク、それ以外の場合はライトバックキャッシュディスク

注:

> イメージ準備がプロビジョニングスキームの作成から切り離されていても、MCSはページファイルの場所を正しく決定します。デフォルトのページファイルの場所はOSディスク上です。

ページファイル設定のシナリオ

次の表は、イメージ準備中およびプロビジョニングスキーム更新中のページファイル設定のいくつかの可能なシナリオについて説明しています。

状況	シナリオ	結果
イメージの準備	ソースイメージのページファイルが一時ディスクに設定されているが、プロビジョニングスキームで指定されたVMサイズには一時ディスクがない	ページファイルはOSディスクに配置される
イメージの準備	ソースイメージのページファイルがOSディスクに設定されているが、プロビジョニングスキームで指定されたVMサイズには一時ディスクがある。	ページファイルは一時ディスクに配置される
イメージの準備	ソースイメージのページファイルが一時ディスクに設定されているが、プロビジョニングスキームでエフェメラルOSディスクが有効になっている。	ページファイルはOSディスクに配置される
プロビジョニングスキームの更新	プロビジョニングスキームを更新しようとすると、元のVMサイズには一時ディスクがあるが、ターゲットVMには一時ディスクがない。	エラーメッセージとともに変更を拒否する
プロビジョニングスキームの更新	プロビジョニングスキームの更新を試行すると、元のVMサイズには一時ディスクがな	エラーメッセージとともに変更を拒否します

状況	シナリオ	結果
	く、ターゲットVMには一時ディスクがあります。	

ページファイル設定の更新

ページファイル設定（場所とサイズを含む）は、PowerShellコマンドを使用して明示的に指定することもできます。これにより、MCSによって決定された値が上書きされます。これを行うには、`New-ProvScheme`コマンドを実行し、以下のカスタムプロパティを含めます。

- `PageFileDiskDriveLetterOverride`: ページファイルの場所のディスクドライブ文字
- `InitialPageFileSizeInMB`: 初期ページファイルサイズ (MB)
- `MaxPageFileSizeInMB`: ページファイルの最大サイズ (MB)

カスタムプロパティの使用例:

```
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property
xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride" Value="d"/>
`


<Property
xsi:type="StringProperty" Name="InitialPageFileSizeInMB" Value="2048"/> `

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value="8196"/
> `

<Property
xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS"/> `

<Property
xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client"/> `
```

```
</CustomProperties>'
```

制約:

- ページファイル設定は、`New-ProvScheme`コマンドを実行してプロビジョニングスキームを作成するときにのみ更新でき、後で変更することはできません。
- ページファイル設定に関連するすべてのプロパティ（`PageFileDiskDriveLetterOverride`、`InitialPageFileSizeInMB`、および`MaxPageFileSizeInMB`）をカスタムプロパティで指定するか、または何も指定しないでください。
- 初期ページファイルサイズは16 MBから16777216 MBの間である必要があります。
- 最大ページファイルサイズは、初期ページファイルサイズ以上で、かつ16777216 MB未満である必要があります。
- この機能はWeb Studioではサポートされていません。

Azure Spot VMを使用してカタログを作成する

Azure Spot VM を使用すると、Azure の未使用のコンピューティング容量を大幅なコスト削減で活用できます。ただし、Azure Spot VM を割り当てる機能は、現在の容量と価格設定に依存します。そのため、Azure は実行中の VM を強制排除したり、VM の作成に失敗したり、強制排除ポリシーに従って VM の電源をオンにできなかったりする可能性があります。したがって、Azure Spot VM は、一部の重要でないアプリケーションやデスクトップに適しています。詳細については、「Azure Spot Virtual Machines の使用」を参照してください。

制限事項

- すべてのVMサイズがAzure Spot VMでサポートされているわけではありません。詳細については、制限事項を参照してください。

  VMサイズがSpot VMをサポートしているかどうかを確認するには、次のPowerShellコマンドを実行します。VMサイズがSpot VMをサポートしている場合、`SupportsSpotVM`は**True**になります。

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-
  conn2\serviceoffering.folder\Standard_D2ds_v4.serviceoffering").
  AdditionalData
  ```

- 現在、Azure Spot VMは休止状態をサポートしていません。

要件

Azure Spot VM カタログ用のマシンプロファイルソース (VM またはテンプレート仕様) を作成する際、Azure Spot Instance (VM を使用する場合) を選択するか、`priority` を `Spot` (テンプレート仕様を使用する場合) に設定する必要があります。

Azure Spot VMを使用してカタログを作成する手順

1. マシンプロファイルソース (VM または起動テンプレート) を作成します。

   - Azureポータルを使用してVMを作成するには、Azureポータルを使用してAzure Spot Virtual Machinesを展開するを参照してください。
   - テンプレート仕様を作成するには、テンプレート仕様の**resources > type: Microsoft.Compute/virtualMachines > properties**の下に次のプロパティを追加します。例：

     ```
     "priority": "Spot",

     "evictionPolicy": "Deallocate",

     "billingProfile": {

     "maxPrice": 0.01

     }
     ```

注:

- 強制排除ポリシーは **Deallocate** または **Delete** にすることができます。
  - 非永続 VM の場合、MCS は常に強制排除ポリシーを **Delete** に設定します。VM が強制排除されると、非永続ディスク (例: OS ディスク) とともに削除されます。永続ディスク (例: Identity ディスク) は削除されません。ただし、カタログタイプが永続的であるか、`PersistOsDisk` カスタムプロパティが True に設定されている場合、OS ディスクは永続的です。同様に、`PersistWbc` カスタムプロパティが **True** に設定されている場合、WBC ディスクは永続的です。

    - 永続 VM の場合、MCS は常に強制排除ポリシーを Deallocate に設定します。VM が強制排除されると、割り当て解除されます。ディスクに変更は加えられません。

- 最大価格は、1時間あたりに支払う意思のある価格です。**Capacity Only**を使用している場合、これは**-1**です。最大価格は、null、-1、またはゼロより大きい小数である必要があります。詳細については、価格を参照してください。

2. マシンプロファイルがAzure Spot VM対応であるかどうかを確認するには、次のPowerShellコマンドを実行します。`SpotEnabled`パラメーターが**True**で、`SpotEvictionPolicy`が**Deallocate**または**Delete**に設定されている場合、マシンプロファイルはAzure Spot VM対応です。例：

    - マシンプロファイルのソースがVMの場合、次のコマンドを実行します。

    ```
    (Get-Item "XDHyp:\HostingUnits\azure-res-
    conn2\machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-
    delete.vm"). AdditionalData
    ```

    - マシンプロファイルのソースがテンプレート仕様の場合、次のコマンドを実行します。

    ```
    (Get-Item "XDHyp:\HostingUnits\azure-res-
    conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
    templatespec.templatespec\14.0.0-spot-
    delete.templatespecversion").AdditionalData
    ```

3. `New-ProvScheme` PowerShellコマンドを使用して、マシンプロファイルでマシンカタログを作成します。

`Set-ProvScheme`コマンドを使用してカタログを更新できます。既存のVMをPowerShellコマンド`Set-ProvVmUpdateTimeWindow`を使用して更新することもできます。マシンプロファイルは次回の電源投入時に更新されます。

実行中のAzure Spot VMでの強制排除

計算能力が利用できない場合、または1時間あたりの価格が設定された最大価格よりも高い場合、Azureは実行中のSpot VMを強制排除します。デフォルトでは、強制排除の通知はされません。VMは単にフリーズし、強制排除されます。Microsoftは、強制排除を監視するためにScheduled Eventsを使用することを推奨しています。強制排除を継続的に監視するを参照してください。強

制排除の前に通知を受け取るために、VM内からスクリプトを実行することもできます。例えば、MicrosoftはPythonでポーリングスクリプトScheduledEvents.csを提供しています。

トラブルシューティング

- プロビジョニングされたVMのcustomMachineDataで、`Get-ProvVM`コマンドを使用してSpot VMのプロパティを確認できます。優先度フィールドが**Spot**に設定されている場合、Spotが使用されています。
- Azure PortalでVMがSpotを使用しているかどうかを確認できます。

  a. Azure PortalでVMを見つけます。

  b. **概要**ページに移動します。

  c. 下にスクロールして、**Azure Spot**セクションを見つけます。

    - Spotが使用されていない場合、このフィールドは空です。
    - Spotが使用されている場合、**Azure Spot**と**Azure Spot eviction policy**フィールドが設定されます。

1. 構成ページで、VMの課金プロファイルまたは1時間あたりの最大価格を確認できます。

バックアップVMサイズの構成

パブリッククラウドでは、特定のVMサイズの容量が不足することがあります。また、Azure Spot VMを使用している場合、Azureの容量要件に基づいてVMはいつでも強制排除されます。Azureの容量不足やSpot VMの電源投入失敗といった場合、MCSはバックアップVMサイズにフォールバックします。MCSマシンカタログの作成または更新時に、カスタムプロパティ`BackupVmConfiguration`を使用してバックアップVMサイズのリストを提供できます。MCSは、リストで指定された順序でバックアップVMサイズにフォールバックしようとします。

MCSがVMに特定のバックアップ構成を使用する場合、次回のシャットダウンまでその構成を使い続けます。次回の電源投入時には、MCSはプライマリVM構成を起動しようとします。失敗した場合、MCSはリストに従ってバックアップVMサイズ構成を再度起動しようとします。

この機能は以下でサポートされています:

- マシンプロファイルを使用するカタログ
- 永続的および非永続的なMCSマシンカタログ
- 現在のAzure環境

重要な考慮事項

- リストには複数のバックアップVMサイズを指定できます。
- リストは一意である必要があります。
- リスト内の各VMにインスタンスタイププロパティを追加できます。タイプは**Spot**または**Regular**のいずれかです。タイプが指定されていない場合、MCSはVMを**Regular**と見なします。
- `Set-ProvScheme` PowerShellコマンドを使用して、既存のカタログのバックアップVMサイズリストを変更できます。
- `Set-ProvVMUpdateTimeWindow`コマンドを使用して、カタログに関連付けられたプロビジョニングスキームから作成された既存のVMを更新できます。
- 選択した既存のMCS VMのバックアップVMサイズリストは、`Set-ProvVM`コマンドを使用して構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow`を使用してVMの更新時間枠を設定し、その時間枠内でVMを起動します。VMで`Set-ProvVm`コマンドが使用された場合、プロビジョニングスキーム上のリストが後で更新されても、その特定のVMに設定されたバックアップVMサイズリストが引き続き使用されます。`Set-ProvVM`を`-RevertToProvSchemeConfiguration`と組み合わせて使用すると、VMにプロビジョニングスキーム上のバックアップリストを使用させることができます。

バックアップVMサイズでカタログを作成する

> **注:**
>
> Studio UI のフリーズの問題に対処するには、PowerShell コマンドを実行する際に、すべてのシングルクォートを `"` に置き換えてください。

1. **PowerShell**ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. Broker カタログを作成します。このカタログには、これから作成されるマシンが投入されます。
4. ID プールを作成します。これは、作成されるマシン用に作成された AD アカウントのコンテナになります。
5. マシンプロファイルを使用してプロビジョニングスキームを作成します。「バックアップ構成を構成する方法」を参照してください。
6. プロビジョニングスキームの一意の ID で BrokerCatalog を更新します。

7. VM を作成してカタログに追加します。

既存のカタログを更新する

`Set-ProvScheme` コマンドを使用してプロビジョニングスキームを更新できます。「バックアップ構成を構成する方法」を参照してください。

既存のVMを更新する

`Set-ProvVMUpdateTimeWindow` PowerShell コマンドを使用して、カタログ内の既存の VM を更新できます。このコマンドは、指定された時間枠内で次回の電源投入時に、カタログに関連付けられたプロビジョニングスキームから作成された VM を更新します。例:

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "3/12/2022 3am" -DurationInMinutes 60`
- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

> **注：**
>
> `StartsNow`はスケジュールされた開始時間を示します。`DurationInMinutes`はスケジュールの時間枠です。

> 選択した既存のMCS VMのバックアップVMサイズリストは、`Set-ProvVM` コマンドを使用して構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow` を使用してVMの更新時間枠を設定し、その時間枠内にVMを起動します。例：

1. 選択した既存のMCS VMのバックアップVMサイズリストを構成するには、`Set-ProvVM` コマンドを実行します。例：

```
Set-ProvVM -ProvisioningSchemeName "name"-VMName "Vm-001"

-CustomProperties

"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`"/>

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"true`"/>

<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`"
Value=`"[{&quot;ServiceOffering&quot;: &quot;Standard_D2as_v4&quot;,
&quot;Type&quot;: &quot;Spot&quot;}, {&quot;ServiceOffering&quot;:
&quot;Standard_D2s_v3&quot;, &quot;Type&quot;: &quot;Regular&quot;},
{&quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;,
&quot;Type&quot;: &quot;Spot&quot;}]`"/>

</CustomProperties>"
```

2. 更新を適用するには、`Set-ProvVMUpdateTimeWindow` コマンドを実行します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

すべてのリソースにタグをコピーする

マシンプロファイルで指定されたタグを、新しいVMまたはマシンカタログ内の既存のVMのすべてのリソース（複数のNICやディスク（OSディスク、IDディスク、ライトバックキャッシュディスクなど））にコピーできます。マシンプロファイルのソースは、VMまたはARMテンプレート仕様にすることができます。

注：

リソースにタグを保持するには、タグにポリシーを追加するか（タグコンプライアンスのポリシー定義の割り当て を参照）、マシンプロファイルソースにタグを追加する必要があります。

前提条件

VM、ディスク、およびそのVMのNICにタグを付けるには、マシンプロファイルソース（VMまたはARMテンプレート仕様）を作成します。

- VMをマシンプロファイルの入力として使用する場合は、AzureポータルでVMとすべてのリソースにタグを適用します。Azureポータルでタグを適用する を参照してください。
- ARMテンプレート仕様をマシンプロファイルの入力として使用する場合は、各リソースの下に次のタグブロックを追加します。

```
 "tags": {

"TagC": "Value3"

},
```

注:

テンプレート仕様には、最大1つのディスクと少なくとも1つのNICを含めることができます。

新しいマシンカタログ内のVMのリソースにタグをコピーする

1. VMまたはARMテンプレート仕様をマシンプロファイルの入力として使用して、非永続または永続カタログを作成します。
2. カタログにVMを追加し、電源をオンにします。マシンプロファイルで指定されたタグが、そのVMの対応するリソースにコピーされていることを確認する必要があります。

注:

マシンプロファイルで提供されるNICの数と、VMが使用するNICの数との間に不一致がある場合、エラーが発生します。

既存のVMのリソース上のタグを変更する

1. すべてのリソースにタグを付けたマシンプロファイルを作成します。
2. 既存のマシンカタログを、更新されたマシンプロファイルで更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName>
-MachineProfile <PathToYourMachineProfile>
```

3. 更新を適用したいVMの電源をオフにします。
4. VMのスケジュールされた更新を要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <YourCatalogName>  -
VMName machine1 -StartsNow -DurationInMinutes -1
```

5. VMの電源をオンにします。
6. マシンプロファイルで指定されたタグが、対応するリソースにコピーされていることを確認する必要があります。

注:

マシンプロファイルで提供されるNICの数と、`Set-ProvScheme`で提供されるNICの数に不一致がある場合、エラーが発生します。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure.html)を参照してください。
- カタログを管理するには、「」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html)および「」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage/manage-machine-catalog-azure.html)を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Microsoft Azure リソース マネージャーへの接続(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections/connection-azure-resource-manager.html)
- マシンカタログの作成

「マイクロソフト システム センター バーチャル マシン マネージャー」カタログの作成

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明します。以下の情報では、Microsoft System Center Virtual Machine Manager (VMM) 仮想化環境に固有の詳細について説明します。

> **注:**
>
> VMMカタログを作成する前に、VMMへの接続の作成を完了する必要があります。Microsoft System Center Virtual Machine Managerへの接続を参照してください。

マスターVMの作成

1. マスターVMにVDAをインストールし、パフォーマンスを向上させるためにデスクトップを最適化するオプションを選択します。
2. バックアップとして使用するために、マスターVMのスナップショットを作成します。
3. 仮想デスクトップを作成します。

SMB 3ファイル共有上のMCS

VMストレージ用のSMB 3ファイル共有上でMCSを使用して作成されたマシンカタログの場合、資格情報が以下の要件を満たしていることを確認してください。これらの要件により、ControllerのHypervisor Communications Library (HCL) からの呼び出しがSMBストレージに正常に接続されます。

- VMMユーザーの資格情報には、SMBストレージへの完全な読み取り/書き込みアクセスが含まれている必要があります。
- VMライフサイクルイベント中のストレージ仮想ディスク操作は、VMMユーザーの資格情報を使用してHyper-Vサーバーを介して実行されます。

SMBストレージを使用する場合、Controllerから個々のHyper-VマシンへのAuthentication Credential Security Support Provider (CredSSP) を有効にします。このプロセスは、Windows Server 2012上のHyper-VとVMM 2012 SP1で使用します。詳細については、CTX137465を参照してください。

HCLは`CredSSP`を使用してHyper-Vマシンへの接続を開きます。この機能は、Kerberosで暗号化されたユーザー資格情報をHyper-Vマシンに渡します。リモートHyper-Vマシン上のセッションに

おける**PowerShell**コマンドは、提供された資格情報で実行されます。この場合、VMMユーザーの資格情報が使用されるため、ストレージへの通信コマンドが正しく機能します。

次のタスクでは、HCLで生成され、SMB 3.0ストレージに対して動作するためにHyper-Vマシンに送信されるPowerShellスクリプトを使用します。

- **マスターイメージの統合**：マスターイメージは、MCSプロビジョニングスキーム（マシンカタログ）を作成します。マスターVMをクローンしてフラット化し、新しく作成されたディスクからVMを作成できるようにします（元のマスターVMへの依存関係を削除します）。

  root\\virtualization\\v2 名前空間の ConvertVirtualHardDisk

  例：

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

- **差分ディスクの作成**：マスターイメージを統合して生成されたマスターイメージから差分ディスクを作成します。その後、差分ディスクは新しいVMに接続されます。

  root\\virtualization\\v2 名前空間の CreateVirtualHardDisk

  例：

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);

$result
```

- **IDディスクのアップロード**：HCLはIDディスクをSMBストレージに直接アップロードできません。そのため、Hyper-VマシンがIDディスクをストレージにアップロードしてコピーする必要があります。Hyper-Vマシンはコントローラーからディスクを読み取ることができないため、HCLはまずHyper-Vマシンを介してIDディスクを次のようにコピーする必要があります。

  a. HCLは、管理者共有を介してIDをHyper-Vマシンにアップロードします。

  b. Hyper-Vマシンは、PowerShellリモートセッションで実行されているPowerShellスクリプトを介して、ディスクをSMBストレージにコピーします。Hyper-Vマシン上にフォルダー

が作成され、そのフォルダーのアクセス許可はVMMユーザーのみにロックされます（リモートPowerShell接続を介して）。

c. HCLは、管理者共有からファイルを削除します。

d. HCLがIDディスクのHyper-Vマシンへのアップロードを完了すると、リモートPowerShellセッションはIDディスクをSMBストレージにコピーします。その後、Hyper-Vマシンから削除します。

IDディスクフォルダーは、削除された場合でも再利用できるように再作成されます。

- **IDディスクのダウンロード**：アップロードと同様に、IDディスクはHyper-Vマシンを介してHCLに渡されます。以下のプロセスでは、Hyper-Vサーバー上にVMMユーザー権限のみを持つフォルダーが存在しない場合に作成します。

  a. Hyper-Vマシンは、PowerShellスクリプトを介してSMBストレージからローカルのHyper-Vストレージにディスクをコピーします。このスクリプトは、PowerShell V3リモートセッションで実行されます。

  b. HCLは、Hyper-Vマシンの管理者共有からディスクをメモリに読み込みます。

  c. HCL は管理者共有からファイルを削除します。

マシンプロファイルを使用してカタログを作成する

マシンプロファイルを使用して、System Center Virtual Machine Manager (SCVMM) 環境でMCSマシンカタログを作成および更新できます。また、ネストされた仮想化とvTPMを有効にすることもできます。

重要な考慮事項

- マスターイメージはスナップショットのみで、VM にすることはできません。
- マシンプロファイルのソースとして使用できるのは VM のみです。
- Hyper-V コンソールから VTPM を構成できますが、SCVMM コンソールからは構成できません。
- マスターイメージで vTPM が有効になっている場合は、マシンプロファイルソースで vTPM を有効にする必要があります。
- vTPM は第2世代のマシンでのみサポートされています。
- 以下のパラメーターは、個別に指定された場合、マシンプロファイルでキャプチャされた値を上書きします。
  - VMCpuCount
  - VMMemoryMB

    - ディスクストレージ

- `Set-ProvScheme` コマンドを使用して、既存のカタログを更新できます。

マシンプロファイルを使用してカタログを作成する手順

1. マシンプロファイルのソースとなるVMを作成します。詳細については、「VMMファブリックでの仮想マシンのプロビジョニング」を参照してください。**Generation**は一度選択すると変更できません。

    - ネストされた仮想化を有効にする場合は、**Select Source**ページで**Enable Nested Virtualization**チェックボックスをオンにします。
    - vTPMを有効にする場合は、VMを作成した後、Hyper-Vホストにログインし、**Hyper-V Manager**でVMを見つけます。VMを右クリックし、**Settings**に移動します。**Security**の下で、**Enable Trusted Platform Module**チェックボックスをオンにします。

2. **PowerShell**ウィンドウを開きます。
3. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
4. Brokerカタログを作成します。このカタログには、これから作成されるマシンが格納されます。
5. IDプールを作成します。これは、作成されるマシン用に作成されたADアカウントのコンテナになります。
6. マシンプロファイルを使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme -HostingUnitName "<hostingunit name>"

-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<path
to the checkpoint/snapshot>"

-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:\<path
to the machine profile VM>"
```

7. プロビジョニングスキームの一意のIDでBrokerカタログを更新します。
8. カタログにVMを作成して追加します。

Set-ProvSchemeコマンドを使用して、既存のカタログを更新できます。例:

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
"XDHyp:\<path to the machine profile VM>"
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studio は デリバリーグループの作成 に誘導します
- 構成プロセス全体を確認するには、インストールと構成 を参照してください
- カタログを管理するには、マシンカタログの管理 および Microsoft System Center Virtual Machine Manager カタログの管理 を参照してください

詳細情報

- 接続とリソースの作成および管理(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections.html)
- マイクロソフト システム センター バーチャル マシン マネージャー への接続
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html)

Nutanixカタログを作成する

「(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html)」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Nutanix仮想化環境に固有の詳細を扱っています。

> **注:**
>
> Nutanixカタログを作成する前に、Nutanixへの接続の作成を完了する必要があります。「(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections/connection-nutanix.html)」を参照してください。

Nutanixスナップショットを使用してマシンカタログを作成する

選択したスナップショットは、カタログ内のVMを作成するために使用されるテンプレートです。カタログを作成する前に、Nutanixでイメージとスナップショットを作成してください。詳細については、Nutanixのドキュメントを参照してください。

カタログ作成ウィザードで：

- **Operating System**ページと**Machine Management**ページには、Nutanix固有の情報は含まれていません。
- **Container**または**Cluster and Container**ページはNutanix固有のものです。

リソースとしてNutanix AHV XIを使用してマシンを展開する場合、**Container**ページが表示されます。VMのIDディスクが配置されるコンテナを選択します。

リソースとしてNutanix AHV Prism Central (PC)を使用してマシンを展開する場合、**Cluster and Container**ページが表示されます。VMの展開に使用するクラスターを選択し、次にコンテナを選択します。

- **Master Image**ページで、イメージスナップショットを選択します。Citrix Virtual Apps and Desktopsで使用するには、Acropolisスナップショット名に「XD_」をプレフィックスとして付ける必要があります。必要に応じて、Acropolisコンソールを使用してスナップショットの名前を変更してください。スナップショットの名前を変更した場合は、カタログ作成ウィザードを再起動して、更新されたリストを表示してください。
- **Virtual Machines**ページで、仮想CPUの数とvCPUあたりのコア数を指定します。
- **Network Cards**ページで、関連するネットワークをフィルタリングするためにNICタイプを選択します。NICタイプは**VLAN**と**OVERLAY**の2種類があります。マスターイメージに含まれるNICを1つ以上選択し、次に各NICに関連付けられた仮想ネットワークを選択します。
- **Machine Identities**、**Domain Credentials**、**Scopes**、および**Summary**ページには、Nutanix固有の情報は含まれていません。

制限事項

Nutanixホスト接続（具体的にはNutanix AHVプラグイン2.7.1）を使用してMCSカタログを作成すると、プロビジョニングされたVMのハードディスクサイズがWeb Studioに正しく表示されません。表示されるサイズは、実際のストレージサイズ（50 GB）よりもはるかに小さく（1 GB）なります。ハードディスクサイズはNutanixコンソールに正しく表示されます。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成に誘導します。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、「マシンカタログの管理」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- マシンカタログの作成

VMwareカタログを作成する

「マシンカタログを作成する」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明します。以下の情報は、VMware仮想化環境に固有の詳細を扱います。

> **注:**
>
> VMwareカタログを作成する前に、VMwareへの接続の作成を完了する必要があります。「VMwareへの接続」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections/connection-vmware-virtualization-environments.html)を参照してください。

マスターVMを作成する

マシンカタログでユーザーデスクトップとアプリケーションを提供するために、マスターVMを使用します。ハイパーバイザーで:

1. マスターVMにVDAをインストールし、デスクトップを最適化するオプションを選択します。これによりパフォーマンスが向上します。
2. バックアップとして使用するために、マスターVMのスナップショットを取得します。

> **注:**
>
> vSAN 8.0環境でMCSを使用してVMをプロビジョニングできます。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してMCSマシンカタログを作成できます。マシンプロファイル入力のソースはVMwareテンプレートです。マシンプロファイルはVMwareテンプレートからハードウェアプロパティをキャプチャし、それらをカタログ内の新しくプロビジョニングされたVMに適用します。

> **注:**
>
> - マスターイメージ入力（スナップショット）およびマシンプロファイル入力（VMwareテンプレート）は、vTPMが有効であるか、またはvTPMが無効であるかのいずれかである

必要があります。このルールは、`New-ProvScheme`と`Set-ProvScheme`の両方に適用されます。

- マスターイメージでvTPMが有効になっている場合、VMwareテンプレートは、マスターイメージと同じVMソースからのみ取得できます。
- 暗号化ストレージポリシーはフルクローンのみサポートします。
- マシンプロファイルベースのカタログは、提供されたVMwareテンプレートを利用してストレージコントローラー情報を収集します。これは、接続されている仮想ディスクに依存します。テンプレートには、仮想マシンの仮想ディスクを構成するために使用されるストレージコントローラー情報を取得するために必要な仮想ディスクが含まれている必要があります。

マシンプロファイル内のVMwareテンプレートは、カタログへのVMのプロビジョニングを可能にするため、カタログのライフサイクル中に存在している必要があります。VMwareテンプレートがない場合、新しいVMをプロビジョニングすることはできません。VMwareテンプレートが削除された場合は、`Set-ProvScheme`コマンドを使用して新しいテンプレートを提供する必要があります。

- MCSはVMwareテンプレートのプロパティをキャプチャします。Get-Provschemeコマンドを使用して、VMwareテンプレートの保存されたプロパティを参照する新しいVMwareテンプレートを作成できます。
- あるいは、マシンカタログとプロビジョニングされたVMが存在する場合、MCSでプロビジョニングされたマシンを使用して新しいVMwareテンプレートを作成することもできます。

異なるOSに基づいて、異なる構成でマシンカタログを作成できます。

- マスターイメージにWindows 11がインストールされている場合、マスターイメージでvTPMを有効にする必要があります。したがって、マシンプロファイルのソースであるVMwareテンプレートにはvTPMがアタッチされている必要があります。
- マスターイメージにvTPMがアタッチされていないWindows 10がインストールされている場合、非vTPM VMwareテンプレートをマシンプロファイルのソースとして使用してマシンカタログを作成できます。

暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、フルコピーディスクモードでマシンカタログを作成できる別の構成があります。

マシンプロファイルを入力としてPowerShellコマンドを使用してマシンカタログを作成するには：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. 次のコマンドを実行します。

   - マシンプロファイル入力のソースとしてvTPMがアタッチされたVMwareテンプレートを使用し、Windows 11がインストールされたマスターイメージでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool  -IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme  -CleanOnBoot

-HostingUnitName "vSanRg"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<network name>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4

-VMMemoryMB 6144

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template" -TenancyType Shared
```

```
-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<catalog name>"

-ProvisioningType 'MCS'

-Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- マシンプロファイルのソースとして非vTPM VMwareテンプレートを使用し、Windows 10がインストールされたマスターイメージでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###" -NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-CleanOnBoot -HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、フルコピーディスクモードでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "XDHyp:
\HostingUnits\<hosting unit name>\<template name>.template"

-TenancyType Shared

-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"
```

```
-PersistUserChanges  "OnLocal"

-Description "<string>"  -IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<string>" -ProvisioningType 'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

マシンプロファイルを更新するには、Set-ProvSchemeコマンドを使用します。例：

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
-MachineProfile 'XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template'
```

トラブルシューティング

カタログの作成に失敗した場合は、CTX294978を参照してください。

次のステップ

- これが最初に作成するカタログである場合、Web Studioはデリバリーグループの作成に誘導します。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログの管理およびVMwareカタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- VMwareへの接続
- マシンカタログの作成

異なる参加タイプのカタログの作成

ハイブリッドAzure Active Directory参加済みカタログの作成

この記事では、ハイブリッド Azure Active Directory (AD) 参加済みカタログを作成する方法について説明します。

Web Studio または PowerShell を使用して、Azure AD 参加済みカタログを作成できます。

要件、制限、および考慮事項については、「ハイブリッドAzure Active Directory参加済み」を参照してください。

Web Studioの使用

以下の情報は、マシンカタログの作成 のガイダンスを補足するものです。ハイブリッド Azure AD 参加済みカタログを作成するには、その記事の一般的なガイダンスに従い、ハイブリッド Azure AD 参加済みカタログに固有の詳細に注意してください。

カタログ作成ウィザードで：

- **Machine Identities**ページで、**Hybrid Azure Active Directory joined**を選択します。作成されたマシンは組織が所有し、その組織に属するActive Directory Domain Servicesアカウントでサインインされます。これらはクラウドとオンプレミスの両方に存在します。

> **注:**
>
> IDタイプとして**Hybrid Azure Active Directory joined**を選択した場合、カタログ内の各マシンには対応するADコンピューターアカウントが必要です。

PowerShellの使用

以下は、Web Studio での操作に相当する PowerShell の手順です。Remote PowerShell SDK を使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

オンプレミスAD参加済みカタログとハイブリッドAzure AD参加済みカタログの違いは、IDプールとマシンアカウントの作成方法にあります。

ハイブリッドAzure AD参加済みカタログのIDプールとアカウントを作成するには：

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -Domain
"corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -NamingScheme
"HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU
"CN=AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"

New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
-ADUserName "corp\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -All
-ADUserName "corp\admin1" -ADPassword $password
```

注:

`$password` は、書き込み権限を持つADユーザーアカウントの一致するパスワードです。

ハイブリッド Azure AD 参加済みカタログの作成に使用されるその他のコマンドはすべて、従来のオンプレミス AD 参加済みカタログの場合と同じです。

ハイブリッド Azure AD 参加プロセスのステータスを表示する

Web Studio では、デリバリーグループ内のハイブリッド Azure AD 参加済みマシンが電源オン状態の場合に、ハイブリッド Azure AD 参加プロセスのステータスが表示されます。ステータスを表示するには、検索 を使用してそれらのマシンを特定し、下部ペインの タブで各マシンの を確認します。 には、次の情報が表示されます。

- ハイブリッド Azure AD参加済み
- Azure AD にまだ参加していません

注記:

- マシンの初回起動時に、ハイブリッド Azure AD 参加に遅延が発生する場合があります。これは、デフォルトのマシン ID 同期間隔 (Azure AD Connect の 30 分) が原因です。マシンは、マシン ID が Azure AD Connect を介して Azure AD に同期された後にのみ、ハイブリッド Azure AD 参加済み状態になります。

- マシンがハイブリッド Azure AD 参加済み状態にならない場合、それらは Delivery Controller に登録されません。登録ステータスは と表示されます。

また、Web Studio を使用して、マシンが利用できない理由を知ることができます。これを行うには、 ノードでマシンをクリックし、下部ペインの タブで を確認し、ツールヒントを読んで追加情報を確認します。

トラブルシューティング

マシンがハイブリッド Azure AD 参加に失敗した場合は、次の操作を行います。

- マシンアカウントが Microsoft Azure AD ポータルを介して Azure AD に同期されているか確認します。同期されている場合、「**まだ Azure AD に参加していません**」と表示され、登録ステータスが保留中であることを示します。

  マシンアカウントをAzure ADに同期するには、以下を確認してください。

  - マシンアカウントが、Azure AD と同期するように構成されている OU にあること。**userCertificate** 属性を持たないマシンアカウントは、同期するように構成されている OU にあっても Azure AD に同期されません。
  - 属性 **userCertificate** がマシンアカウントに設定されます。Active Directory Explorer を使用して属性を表示します。
  - マシンアカウントが作成された後、Azure AD Connect が少なくとも一度は同期されている必要があります。そうでない場合は、Azure AD Connect マシンの PowerShell コンソールで `Start-ADSyncSyncCycle -PolicyType Delta` コマンドを手動で実行して、即時同期をトリガーします。

- ハイブリッド Azure AD 参加用の Citrix 管理対象デバイスキーペアが、**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix** の下の **DeviceKeyPairRestored** の値を照会することで、マシンに正しくプッシュされているかを確認します。

  値が1であることを確認します。そうでない場合、考えられる理由は次のとおりです。

  - プロビジョニングスキームに関連付けられている ID プールの `IdentityType` が `HybridAzureAD` に設定されていません。これは `Get-AcctIdentityPool` を実行して確認できます。
  - マシンがマシンカタログと同じプロビジョニングスキームを使用してプロビジョニングされていません。

  - マシンがローカルドメインに参加していません。ローカルドメインへの参加は、ハイブリッド Azure AD 参加の前提条件です。

- MCSでプロビジョニングされたマシンで`dsregcmd /status /debug`コマンドを実行して、診断メッセージを確認します。

  - ハイブリッド Azure AD 参加が成功した場合、コマンドラインの出力で **AzureAdJoined** と **DomainJoined** が **YES** になります。
  - そうでない場合、問題をトラブルシューティングするにはMicrosoftのドキュメントを参照してください: `<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>`。
  - エラーメッセージ「**Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**」が表示された場合は、ユーザー証明書を修復するために次のPowerShellコマンドを実行します。

    ```
    Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
    UserCertificate
    ```

    ユーザー証明書の問題の詳細については、CTX566696を参照してください。

ドメインに参加していないカタログを作成する

この記事では、Citrix Virtual Apps and Desktops を使用して、ドメインに参加していないカタログを作成する方法について説明します。

要件、制限、および考慮事項については、ドメインに参加していないを参照してください。

マシンカタログを作成する前に、次のものが必要です。

1. 新しいリソースの場所

   - Citrix Cloud™ 管理 UI > 左上のハンバーガーメニュー > **リソースの場所** に移動します。
   - 「**+ リソースの場所**」をクリックします。
   - 新しいリソースの場所の名前を入力し、「**保存**」をクリックします。

2. ホスティング接続を作成します。詳細については、「接続の作成と管理」セクションを参照してください。

Citrix Virtual Apps and Desktops を使用すると、ワークグループまたはドメインに参加していないマシンに基づいてカタログを作成できます。ドメインに参加していないマシンの作成は、アカウ

ントIDプールがどのように作成されるかによって異なります。アカウントIDプールは、カタログプロビジョニング中にマシン名を作成および追跡するためにMCSが使用するメカニズムです。

現在、ドメインに参加していないカタログは、PowerShell コマンドのみを使用して作成できます。

PowerShell を使用する

Remote PowerShell SDK を使用して、ドメインに参加していないカタログのIDプールを作成できます。

PowerShell パラメータの **WorkgroupMachine** と **IdentityType** を使用して、ドメインに参加していないカタログのIDプールを作成します。これらのパラメータにより、ドメイン管理者資格情報を含むすべてのAD固有のパラメータを指定する必要がなくなります。

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup"
-WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme
"NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"
```

ドメインに参加していないカタログを作成するために使用される他のすべてのコマンドは、従来のオンプレミスActive Directoryに参加しているカタログの場合と同じです。

マシンカタログを管理する

注:

Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

マシンカタログへのマシンの追加または削除、名前の変更、説明の変更、またはカタログのActive Directoryコンピューターアカウントの管理を行うことができます。

カタログの保守には、各マシンに最新のOSアップデートが適用されていることを確認することも含まれます。これには、ウイルス対策の更新、オペレーティングシステムのアップグレード、または構成の変更が含まれます。

- Machine Creation Services™ (MCS) を使用して作成されたプールされたランダムマシンを含むカタログは、カタログで使用されているマスターイメージを更新し、その後マシンを更新することで、マシンを保守します。この方法により、多数のユーザーマシンを効率的に更新できます。
- 静的で永続的に割り当てられたマシンを含むカタログ、およびリモートPCアクセス マシンカタログの場合、Web Studioの外部でユーザーマシンの更新を管理します。このタスクは、個別に、またはサードパーティのソフトウェア配布ツールを使用してまとめて実行します。

ホストハイパーバイザーへの接続の作成と管理については、接続とリソースを参照してください。

> **注:**
>
> MCSはWindows 10 IoT CoreおよびWindows 10 IoT Enterpriseをサポートしていません。詳細については、Microsoftサイトを参照してください。

永続インスタンスについて

永続インスタンスまたは専用インスタンスを使用して作成されたMCSカタログを更新する場合、カタログ用に作成された新しいマシンは、更新されたイメージを使用します。既存のインスタンスは元のインスタンスを引き続き使用します。イメージの更新プロセスは、他の種類のカタログと同じ方法で行われます。以下を考慮してください。

- 永続ディスクカタログの場合、既存のマシンは新しいイメージに更新されませんが、カタログに追加された新しいマシンは新しいイメージを使用します。
- 非永続ディスクカタログの場合、マシンがリセットされると、次回の起動時にマシンイメージが更新されます。
- 永続的なマシンカタログの場合、イメージを更新すると、それを使用するカタログインスタンスも更新されます。
- 永続的でないカタログの場合、異なるマシンに異なるイメージを使用したい場合は、イメージは別々のカタログに存在する必要があります。

マシンカタログの管理

マシンカタログは、次の2つの方法で管理できます。

- Web Studioの使用
- PowerShellの使用

Web Studioの使用

このセクションでは、Web Studioを使用してカタログを管理する方法について詳しく説明します。

- カタログへのマシンの追加
- カタログからのマシンの削除
- カタログの編集
- カタログの名前変更
- カタログを別のゾーンに移動
- カタログの削除
- カタログ内のActive Directoryコンピューターアカウントの管理
- カタログを更新する(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html#update-a-catalog)
- 機能レベルを変更するか、変更を元に戻す(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html#change-the-functional-level-or-undo-the-change)
- カタログをクローンする(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html#clone-a-catalog)
- フォルダーを使用してカタログを整理する(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html#organize-catalogs-using-folders)

マシンをカタログに追加する

開始する前に:

- 仮想化ホストに、追加のマシンを収容するのに十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- 十分な未使用のActive Directoryコンピューターアカウントがあることを確認してください。既存のアカウントを使用している場合、追加できるマシンの数は利用可能なアカウントの数によって制限されます。
- 追加のマシン用にActive Directoryコンピューターアカウントを作成するためにWeb Studioを使用する場合、適切なドメイン管理者権限が必要です。

カタログにマシンを追加するには:

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. マシンカタログを選択し、アクションバーで**マシンの追加**を選択します。
4. 追加する仮想マシンの数を選択します。
5. 追加するVMの数に対して既存のActive Directoryアカウントが不足している場合は、アカウントが作成されるドメインと場所を選択します。連続する数字または文字が表示される場所を示すためにハッシュマークを使用して、アカウントの命名スキームを指定します。OU名にスラッシュ (/) を使用しないでください。名前は数字で始めることはできません。たとえば、PC-Sales-## (0-9が選択されている場合) の命名スキームは、PC-Sales-01、PC-Sales-02、PC-Sales-03などのコンピューターアカウントになります。
6. 既存のActive Directoryアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Web Studioはこれらのアカウントを管理します。Web Studioにすべてのアカウントのパスワードをリセットさせるか、すべてのアカウントで同じである必要があるアカウントパスワードを指定します。

マシンはバックグラウンドプロセスとして作成され、多数のマシンを作成する場合は時間がかかることがあります。Web Studioを閉じてもマシンの作成は続行されます。

カタログからマシンを削除する

マシンカタログからマシンを削除すると、ユーザーはアクセスできなくなるため、マシンを削除する前に、以下を確認してください。

- ユーザーデータがバックアップされているか、不要になっている。
- すべてのユーザーがログオフしている。メンテナンスモードをオンにすると、マシンへの新しい接続が停止されます。
- マシンの電源がオフになっている。

カタログからマシンを削除するには：

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マシンの表示**を選択します。
4. 1つ以上のマシンを選択し、アクションバーで**削除**を選択します。

削除するマシンを削除するかどうかを選択します。マシンを削除することを選択した場合、それらのマシンのActive Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを編集する

1. **説明**ページで、カタログの説明を変更します。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの編集**を選択します。
4. **スコープ**ページで、スコープを変更します。
5. カタログの種類によっては、追加のページが表示される場合があります。

   Azure Resource Managerイメージを使用して作成されたカタログの場合、次のページが表示されます。行った変更は、後でカタログに追加するマシンにのみ適用されることに注意してください。既存のマシンは変更されません。

   - **Virtual Machines**ページで、マシンを作成するマシンサイズと可用性ゾーンを変更します。

     > **注:**
     >
     > - カタログがサポートするマシンサイズのみが表示されます。
     > - 必要に応じて、**Show only machine sizes used in other machine catalogs**を選択して、マシンサイズリストをフィルターします。

   - **Machine Profile**ページで、マシンプロファイルを使用するか変更するかを選択します。
   - (カタログが専用ホストグループで構成されている場合にのみ表示) **専用ホストグループ**ページで、ホストグループを変更するかどうかを選択します。
   - **ストレージとライセンスの種類**ページで、ストレージの種類、ライセンスの種類、およびAzure Computer Galleryの設定を変更するかどうかを選択します (**準備されたイメージをAzure Galleryに配置**が使用されている場合にのみ利用可能)。

   > **注:**

> 新しく選択した設定が現在のマシンサイズをサポートしていない場合、設定を変更するとマシンサイズ設定がリセットされることを通知する警告ダイアログボックスが表示されます。続行を選択すると、**仮想マシン**メニューの横に赤い点が表示され、新しいマシンサイズを選択するように促されます。

- **ライセンスの種類**ページで、WindowsライセンスまたはLinuxライセンスの設定を変更するかどうかを選択します。

Remote PC Accessカタログの場合、次のページが表示されます。

- **電源管理**ページで、電源管理設定を変更し、電源管理接続を選択します。
- **組織単位**ページで、Active Directory OUを追加または削除します。

6. **適用**をクリックして変更を適用し、**保存**をクリックして終了します。

カタログの名前を変更する

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの名前を変更**を選択します。
4. 新しい名前を入力します。

カタログを別のゾーンに移動する

展開に複数のゾーンがある場合、カタログをあるゾーンから別のゾーンに移動できます。

カタログ内のVMを含むハイパーバイザー以外のゾーンにカタログを移動すると、パフォーマンスに影響します。

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**移動**を選択します。
4. カタログを移動したいゾーンを選択します。

カタログを削除する

カタログを削除する前に、以下を確認してください。

- すべてのユーザーがログオフしており、切断されたセッションが実行されていないこと。

- カタログ内のすべてのマシンでメンテナンスモードがオンになっており、新しい接続が確立できないこと。
- カタログ内のすべてのマシンが電源オフになっていること。
- カタログがデリバリーグループに関連付けられていないこと。つまり、デリバリーグループにそのカタログのマシンが含まれていないこと。

カタログを削除するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの削除**を選択します。
4. カタログ内のマシンを削除するかどうかを指定します。マシンを削除することを選択した場合、それらのマシンのActive Directoryコンピューターアカウントを保持するか、無効にするか、削除するかを指定します。

カタログ内のActive Directoryコンピューターアカウントを管理する

マシンカタログ内のActive Directoryアカウントを管理するには、次の操作を実行できます。

- シングルセッションOSおよびマルチセッションOSカタログからActive Directoryコンピューターアカウントを削除して、未使用のマシンアカウントを解放します。これらのアカウントは、他のマシンで使用できます。
- カタログにマシンが追加されたときに、コンピューターアカウントがすでに存在するようにアカウントを追加します。OU名にスラッシュ (/) を使用しないでください。

Active Directoryアカウントを管理するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**Manage AD accounts**を選択します。
4. コンピューターアカウントを追加するか削除するかを選択します。アカウントを追加する場合は、アカウントのパスワードをどうするかを指定します。すべてリセットするか、すべてのアカウントに適用されるパスワードを入力します。

   現在のアカウントパスワードが不明な場合は、パスワードをリセットできます。パスワードリセットを実行する権限が必要です。パスワードを入力すると、アカウントがインポートされるときにパスワードが変更されます。アカウントを削除するときは、Active Directory内のアカウントを保持するか、無効にするか、削除するかを選択します。

カタログからマシンを削除したり、カタログを削除したりするときに、Active Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを更新する

カタログ内のマシンを更新する前に、マスターイメージのコピーまたはスナップショットを保存することをお勧めします。データベースは、各マシンカタログで使用されたマスターイメージの履歴レコードを保持します。ユーザーがデスクトップに展開した更新プログラムで問題が発生した場合、カタログ内のマシンを以前のバージョンのマスターイメージに戻す（ロールバックする）ことができます。これにより、ユーザーのダウンタイムが最小限に抑えられます。マスターイメージを削除、移動、または名前変更しないでください。それらを使用してカタログを元に戻すことはできません。

マシンが更新されると、自動的に再起動します。

マスターイメージを更新または作成する

マシンカタログを更新する前に、既存のマスターイメージを更新するか、ホストハイパーバイザー上に新しいマスターイメージを作成します。

1. ハイパーバイザー上で、現在のVMのスナップショットを取得し、意味のある名前を付けます。このスナップショットは、必要に応じてカタログ内のマシンを元に戻す（ロールバックする）ために使用できます。
2. 必要に応じて、マスターイメージの電源を入れ、ログオンします。
3. マスターイメージに更新プログラムをインストールするか、必要な変更を加えます。
4. VMの電源を切ります。
5. VMのスナップショットを作成します。Web Studioでカタログが更新されたときに認識されるような、意味のある名前を付けます。Web Studioでスナップショットを作成することもできますが、Citrixではハイパーバイザー管理コンソールを使用して作成することをお勧めします。その後、Web Studioでそのスナップショットを選択します。このプロセスにより、自動生成された名前ではなく、意味のある名前と説明を提供できます。GPUマスターイメージの場合、マスターイメージはXenServer®コンソールからのみ変更できます。

マスターイメージを変更する

カタログ内のすべてのマシンに更新プログラムを準備して展開するには：

1. Web Studioにサインインします。
2. 左側のペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マスターイメージの変更**を選択します。

4. **マスターイメージ**ページで、ホストと展開するイメージを選択します。

   ヒント：

   MCSで作成されたカタログの場合、イメージにメモを追加して注釈を付けることができます。メモは最大500文字まで含めることができます。マスターイメージを変更するたびに、メモを追加したかどうかにかかわらず、メモ関連のエントリが作成されます。メモを追加せずにカタログを更新した場合、エントリはnull (-)として表示されます。イメージのメモ履歴を表示するには、カタログを選択し、下部のペインで**テンプレートプロパティ**をクリックし、**メモ履歴の表示**をクリックします。

5. **展開戦略**ページで、マシンカタログ内のマシンを新しいマスターイメージで更新するタイミング（次回のシャットダウン時または即時）を選択します。

   注：

   展開戦略ページは、展開が非永続VMにのみ適用されるため、永続VMでは利用できません。

6. **概要**ページで情報を確認し、**完了**をクリックします。各マシンは更新後に自動的に再起動します。

更新の進行状況を追跡するには、「**マシンカタログ**」でカタログを見つけ、インラインの進行状況バーと段階的な進行状況グラフを表示します。

Web StudioではなくPowerShell SDKを直接使用してカタログを更新する場合は、ハイパーバイザーテンプレート（**VMTemplates**）を指定します。これは、イメージまたはイメージのスナップショットの代替として使用します。

展開戦略：

次回シャットダウン時にイメージを更新すると、現在使用されていないマシン、つまりアクティブなユーザーセッションがないマシンにすぐに影響します。使用中のシステムは、現在のアクティブなセッションが終了したときに更新を受け取ります。以下を考慮してください。

- 該当するマシンでの更新が完了するまで、新しいセッションを起動することはできません。
- シングルセッションOSマシンでは、マシンが使用されていないとき、またはユーザーがログインしていないときに、マシンはすぐに更新されます。

- 子マシンを持つマルチセッションOSの場合、再起動は自動的に行われません。更新されたマスターイメージを適用するには、Studio、PowerShell、またはWorkspaceを使用してマシンを再起動します。マシンまたはハイパーバイザーから再起動しても、更新は適用されません。

> **ヒント:**
>
> ホスト接続の詳細設定を使用して、再起動されるマシンの数を制限します。これらの設定を使用して、特定のカタログに対して実行されるアクションを変更します。詳細設定はハイパーバイザーによって異なります。

マスターイメージをロールバックする

更新された、または新しいマスターイメージを展開した後、それをロールバックできます。このプロセスは、新しく更新されたマシンで問題が発生した場合に必要になることがあります。ロールバックすると、カタログ内のマシンは最後に機能していたイメージにロールバックされます。新しいイメージを必要とする新機能は利用できなくなります。展開と同様に、マシンをロールバックすると再起動が含まれます。

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで を選択します。
4. 展開操作の前のセクションで説明されているように、以前のマスターイメージをマシンに適用するタイミングを指定します。

ロールバックは、元に戻す必要があるマシンにのみ適用されます。新しいまたは更新されたマスターイメージで更新されていないマシンは、通知メッセージを受信せず、ログオフを強制されません。

ロールバックの進行状況を追跡するには、 でカタログを見つけて、インラインの進行状況バーと段階的な進行状況グラフを表示します。

機能レベルを変更または変更を元に戻す

マシン上のVDAを新しいバージョンにアップグレードした後、マシンカタログの機能レベルを変更します。Citrixは、すべての最新機能へのアクセスを可能にするために、すべてのVDAを最新バージョンにアップグレードすることを推奨します。

マシンカタログの機能レベルを変更する前に、次の点に注意してください。

- アップグレードされたマシンを起動して、Controllerに登録させます。このプロセスにより、Web Studioはカタログ内のマシンがアップグレードを必要としていることを判断できます。

カタログの機能レベルを変更するには：

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択します。下部ペインの**詳細**タブにバージョン情報が表示されます。
4. **機能レベルの変更**を選択します。Web Studioがカタログのアップグレードが必要であると検出した場合、メッセージが表示されます。プロンプトに従います。1つ以上のマシンをアップグレードできない場合、その理由を説明するメッセージが表示されます。すべてのマシンが適切に機能するように、Citrixは**変更**をクリックして続行する前に、マシンの問題を解決することを推奨します。

カタログの変更が完了したら、カタログを選択し、アクションバーで**機能レベルの変更を元に戻す**を選択することで、マシンを以前のVDAバージョンに戻すことができます。

カタログを複製する

カタログを複製する前に、次の考慮事項に注意してください。

- オペレーティングシステムおよびマシン管理に関連する設定は変更できません。クローンされたカタログは、元のカタログからそれらの設定を継承します。
- カタログのクローン作成には時間がかかる場合があります。必要に応じて、**進行状況を非表示**を選択して、バックグラウンドでクローン作成を実行します。
- クローン作成されたカタログは元の名前を継承し、`Copy`というサフィックスが付きます。名前は変更できます。「カタログの名前を変更する」を参照してください。
- クローン作成が完了したら、クローン作成されたカタログをデリバリーグループに必ず割り当ててください。

1. Web Studioにサインインし、左側のペインで**マシンカタログ**を選択します。
2. カタログを選択し、アクションバーで**クローン**を選択します。
3. **選択したマシンカタログのクローン作成**ウィンドウで、クローン作成されたカタログの設定を表示し、必要に応じて設定を構成します。**次へ**を選択して次のページに進みます。
4. **概要**ページで設定の概要を確認し、**完了**を選択してクローン作成を開始します。
5. 必要に応じて、**進行状況を非表示**を選択して、バックグラウンドでクローン作成を実行します。

フォルダーを使用してカタログを整理する

フォルダーを作成してカタログを整理し、簡単にアクセスできるようにすることができます。たとえば、イメージの種類別または組織構造別にカタログを整理できます。

カタログフォルダーを作成する

開始する前に、まずカタログの整理方法を計画してください。次の点を考慮してください。

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- カタログフォルダーには、カタログとサブフォルダーを含めることができます。
- Web Studioのすべてのノード（**マシンカタログ**ノードや**アプリケーション**ノードなど）は、バックエンドでフォルダーツリーを共有しています。フォルダーの名前変更や移動時に他のノードとの名前の競合を避けるため、異なるノードの第1レベルフォルダーには異なる名前を付けることをお勧めします。

カタログフォルダーを作成するには、次の手順に従います。

1. 左側のペインで **［マシンカタログ］** を選択します。
2. フォルダー階層でフォルダーを選択し、**［アクション］** バーで **［フォルダーの作成］** を選択します。
3. 新しいフォルダーの名前を入力し、**［完了］** をクリックします。

> **ヒント：**
>
> 意図しない場所にフォルダーを作成した場合でも、正しい場所にドラッグできます。

カタログを移動する

カタログはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左側のペインで **［マシンカタログ］** を選択します。
2. フォルダー別にカタログを表示します。フォルダー階層の上にある **［すべて表示］** をオンにして、すべてのカタログを一度に表示することもできます。
3. カタログを右クリックし、**［マシンカタログの移動］** を選択します。
4. カタログの移動先のフォルダーを選択し、**［完了］** をクリックします。

> **ヒント：**

> カタログをフォルダーにドラッグできます。

カタログフォルダーの管理

カタログフォルダーの削除、名前の変更、移動ができます。

フォルダーとそのサブフォルダーにカタログが含まれていない場合にのみ、フォルダーを削除できます。

フォルダーを管理するには、次の手順に従います。

1. 左側のペインで、**Machine Catalogs**を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて**アクション**バーでアクションを選択します。
   - フォルダーの名前を変更するには、**フォルダーの名前を変更**を選択します。
   - フォルダーを削除するには、**フォルダーの削除**を選択します。
   - フォルダーを移動するには、**フォルダーの移動**を選択します。
3. 画面の指示に従って、残りの手順を完了します。

PowerShellを使用する

このセクションでは、PowerShellを使用してカタログを管理する方法について詳しく説明します。

- カタログに関連付けられた警告とエラーを取得する
- イメージに説明を追加する
- OSディスクをリセットする
- 既存のプロビジョニングスキームのネットワーク設定を変更する
- マシンカタログのバージョンを管理する(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html#manage-versions-of-a-machine-catalog)
- マシンプロファイルに基づかないマシンカタログを、マシンプロファイルに基づくマシンカタログに変換する(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html#convert-a-non-machine-profile-based-machine-catalog-to-machine-profile-based-machine-catalog)
- アクティブなコンピューターアカウントの識別情報を修復する(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html#repair-the-identity-information-of-active-computer-accounts)

- 既存のマシンカタログのキャッシュ構成を変更する(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html#change-cache-configuration-on-an-existing-machine-catalog)

カタログに関連付けられている警告とエラーを取得する

履歴エラーと警告を取得して、MCSマシンカタログの問題を理解し、それらの問題を修正できます。

PowerShellコマンドを使用して、次のことができます。

- エラーまたは警告のリストを取得する
- 警告の状態を**新規**から**確認済み**に変更する
- エラーまたは警告を削除する

PowerShellコマンドを実行するには:

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行して、Citrix固有のPowerShellモジュールをロードします。

エラーと警告のリストを取得するには：

`Get-ProvOperationEvent` コマンドを実行します。

- パラメーターなし: すべてのエラーと警告を取得します
- `LinkedObjectType` と `LinkedObjectUid` パラメーターを使用すると: 特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告を取得します
- `EventId` パラメーターを使用すると: このイベントIDに一致する特定のエラーまたは警告を取得します
- `Filter` パラメーターを使用すると: カスタマイズされたフィルターによってエラーまたは警告を取得します

エラーまたは警告の状態を **New** から **Acknowledged** に変更するには：

`Confirm-ProvOperationEvent` コマンドを実行します。

- `EventId` パラメーターを使用すると: このイベントIDに一致する特定のエラーまたは警告の状態を設定します。特定のエラーまたは警告の `EventId` は、`Get-ProvOperationEvent` コマンドの出力として取得できます

- `LinkedObjectType` と `LinkedObjectUid` パラメーターを使用すると: 特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告の状態を設定します
- `All` パラメーターを使用すると: すべてのエラーと警告の状態を **確認済み** に設定します

エラーまたは警告を削除するには：

`Remove-ProvOperationEvent` コマンドを実行します。

- `EventId` パラメーターを使用すると: このイベントIDに一致する特定のエラーまたは警告を削除します。特定のエラーまたは警告の `EventId` は、`Get-ProvOperationEvent` コマンドの出力として取得できます
- `LinkedObjectType` と `LinkedObjectUid` パラメーターを使用すると: 特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告を削除します
- `All` パラメーターを使用すると: すべてのエラーと警告を削除します

詳しくは、Citrix PowerShell SDKを参照してください。

イメージに説明を追加する

マシンカタログのイメージ更新に関連する変更について、情報を提供する説明を追加できます。この機能を使用して、カタログの作成時、またはカタログの既存のマスターイメージを更新する際に説明を追加します。カタログ内の各マスターイメージの情報を表示することもできます。イメージの説明を追加または表示するには、次のコマンドを使用します。

- マスターイメージを使用してマシンカタログを作成する際にメモを追加するには、`NewProvScheme` コマンドでパラメーター `MasterImageNote` を使用します。例:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -HostingUnitName
<name> -IdentityPoolName <name> -MasterImageVM

XDHyp:\HostingUnits\<hosting unit name>\<vm name>.vm\Base.snapshot
-MasterImageNote "Note"
```

- マシンカタログに関連付けられているマスターイメージを更新するには、`Publish-ProvMasterVMImage` コマンドでパラメーター `MasterImageNote` を使用します。例:

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name>
-MasterImageVM XDHyp:\HostingUnits\<hosting unit name>\<vm
name>.vm\base.snapshot -MasterImageNote "Note"
```

- 各イメージの情報を表示するには、Get-ProvSchemeMasterVMImageHistory コマンドを使用します。例:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
MyScheme -Showall
```

ロールバックの進行状況を追跡するには、 でカタログを見つけて、インラインの進行状況バーと段階的な進行状況グラフを表示します。

次のシナリオを含む特定の状況では、ロールバックできません。（**マスターイメージのロールバック**オプションは表示されません）。

- ロールバックする権限がありません。
- カタログがMCSを使用して作成されていません。
- カタログがOSディスクのイメージを使用して作成されています。
- カタログの作成に使用されたスナップショットが破損しています。
- カタログ内のマシンに対するユーザーの変更が保持されません。
- カタログ内のマシンが実行中です。

OSディスクをリセットする

PowerShell コマンド `Reset-ProvVMDisk` を使用して、MCS で作成されたマシンカタログ内の永続VMのOSディスクをリセットします。現在、この機能はAWS、Azure、XenServer、Google Cloud、SCVMM、およびVMware仮想化環境に適用できます。

PowerShellコマンドを正常に実行するには、以下を確認してください。

- ターゲットVMが永続MCSカタログ内にあること。
- MCSマシンカタログが正常に機能していること。
- これは、プロビジョニングスキームとホストが存在し、プロビジョニングスキームに正しいエントリがあることを意味します。
- ハイパーバイザーがメンテナンスモードではないこと。
- ターゲットVMの電源がオフになっており、メンテナンスモードになっていること。

OSディスクをリセットするには、以下の手順を実行します。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために、**asnp citrix*** を実行します。

3. 以下のいずれかの方法でPowerShellコマンド `Reset-ProvVMDisk` を実行します。

   - VMのリストをコンマ区切りで指定し、各VMでリセットを実行します。

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc","def")
     -OS
     ```

   - `Get-ProvVM` コマンドからの出力としてVMのリストを指定し、各VMでリセットを実行します。

     ```
     (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc"
     -OS
     ```

   - 名前で単一のVMを指定します。

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
     ```

   - `Get-ProvVM` コマンドによって返された各VMに対して個別のリセットタスクを作成します。これは、各タスクがハイパーバイザーの機能チェック、各VMの接続チェックなど、同じ冗長なチェックを実行するため、効率が低下します。

     ```
     Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk
     -ProvisioningSchemeName "xxx" -OS
     ```

4. リセットされるVMのリストと、回復不能な操作であるという警告メッセージが表示される確認プロンプトが表示されます。回答を入力せずに **Enter** キーを押すと、それ以上のアクションは実行されません。

   > **注:**
   >
   > リセットプロセスが完了するまで、VMをメンテナンスモードから解除したり、電源をオンにしたりしないでください。

   > PowerShellコマンド `-WhatIf` を実行して、実行されるアクションを出力し、アクションを実行せずに終了できます。

   次のいずれかの方法を使用して、確認プロンプトをバイパスすることもできます。

- `-Force` パラメーターを指定します。

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Force
```

- `-Confirm:$false` パラメーターを指定します。

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Confirm:$false
```

- `Reset-ProvVMDisk` を実行する前に、`$ConfirmPreference` を**None**に変更します。

```
PS C:\Windows\system32> $ConfirmPreference='None'

PS C:\Windows\system32> $ConfirmPreference

None

PS C:\Windows\system32> Reset-ProvVMDisk -ProvisioningSchemeName
"xxx" -VMName "abc" -OS
```

5. `Get-ProvTask` を実行して、`Reset-ProvVMDisk` コマンドによって返されたタスクのステータスを取得します。

既存のプロビジョニングスキームのネットワーク設定を変更する

既存のプロビジョニングスキームのネットワーク設定を変更して、新しいVMが新しいサブネットワーク上に作成されるようにすることができます。ネットワーク設定を変更するには、`Set-ProvScheme` コマンドで `-NetworkMapping` パラメーターを使用します。

注:

この機能は、Citrix Virtual Apps and Desktops 2203 LTSR CU3以降のバージョンでサポートされています。

既存のプロビジョニングスキームのネットワーク設定を変更するには、次の手順を実行します。

1. PowerShellウィンドウで、コマンド `asnp citrix*` を実行してPowerShellモジュールをロードします。
2. 変更するネットワークパスに移動するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` を実行します。
3. 新しいネットワーク設定に変数を割り当てます。例:

```
$NewNetworkMap = @{"0"= "XDHYP:\HostingUnits\MyNetworks\Network
0.network"}
```

4. `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap` を実行します。
5. 既存のプロビジョニングスキームの新しいネットワーク設定を確認するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` を実行します。

マシンカタログのバージョンを管理する

MCSマシンカタログが`Set-ProvScheme`コマンドで更新されると、現在の構成がバージョンとして保存されます。その後、PowerShellコマンドを使用して、マシンカタログのさまざまなバージョンを管理できます。次のことができます。

- マシンカタログのバージョンリストを表示する
- 以前のバージョンを使用してマシンカタログを更新する
- そのマシンカタログのVMで使用されていないバージョンを手動で削除する
- マシンカタログによって保持される最大バージョン数を変更する（デフォルトは99）

バージョンには、マシンカタログの次の情報が含まれます。

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- ネットワークマッピング
- セキュリティグループ

マシンカタログのさまざまなバージョンを管理するには、次のコマンド（例として提供）を実行します。

- マシンカタログのさまざまなバージョンの構成詳細を表示するには：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- マシンカタログの特定のバージョンの構成詳細を表示するには：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version 2
```

- マシンカタログに関連付けられているバージョンの総数を確認するには：

```
(Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count
```

- 以前のバージョンを使用してマシンカタログを更新するには：

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- マシンカタログのVMで使用されていないバージョンを手動で削除するには：

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version
3
```

- マシンカタログによって保持される最大バージョン数を設定するには（デフォルトは99）。この設定はすべてのカタログに適用されます。たとえば、この場合、すべてのMCSプロビジョニング済みカタログに対して最大15バージョンが保持されます。

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -Value
15
```

バージョン数が最大バージョン数に達した場合、古いバージョンがマシンカタログ内のいずれかのVMで使用されていると、新しいバージョンを作成できません。その場合は、次のいずれかを実行します。

- マシンカタログによって保持される最大バージョン数の制限を増やします。
- 古いバージョンを使用している一部のVMを更新して、それらの古いバージョンがどのVMからも参照されなくなり、削除できるようにします。

マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換する

VM、テンプレート仕様（Azureの場合）、または起動テンプレート（AWSの場合）をマシンプロファイルの入力として使用して、マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換できます。カタログに追加された新しいVMは、明示的なカスタムプロパティによって上書きされない限り、マシンプロファイルからプロパティ値を取得します。

> **注:**
>
> 既存のマシンプロファイルベースのマシンカタログを、非マシンプロファイルベースのマシンカタログに変更することはできません。

これを行うには：

1. VMを使用し、マシンプロファイルを使用しない永続的または非永続的なマシンカタログを作成します。
2. **PowerShell**ウィンドウを開きます。
3. マシンプロファイルからマシンカタログに追加された新しいVMにプロパティ値を適用するには、`Set-ProvScheme`コマンドを実行します。例：

   - Azureの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile XDHyp:
     \HostingUnits\<HostingUnitName>\machineprofile.folder\<Resourc
     eGroupName>\<TemplateSpecName>\<VersionName>
     ```

   - AWSの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile "XDHyp:
     \HostingUnits\<hosting-unit>\<launch-
     template>.launchtemplate\<launch-template-
     version>.launchtemplateversion"
     ```

アクティブなコンピューターアカウントのID情報を修復する

ID関連の問題があるアクティブなコンピューターアカウントのID情報をリセットできます。マシンパスワードと信頼キーのみをリセットするか、IDディスクのすべての構成をリセットするかを選択できます。この実装は、永続的および非永続的な両方のMCSマシンカタログに適用できます。

> **注:**
>
> 現在、この機能はAzureおよびVMware仮想化環境でのみサポートされています。

条件

IDディスクを正常にリセットするには、以下を確認してください。

- VMをシャットダウンし、メンテナンスモードに設定します
- PowerShellコマンドにパラメーター-OSを含めないでください

IDディスクをリセットする

IDディスクをリセットするには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. ID情報をリセットします。
   - マシンパスワードと信頼キーのみをリセットするには、次のコマンドを実行します。

     ```
     Repair-AcctIdentity -IdentityAccountName TEST\VM1
     -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
     -Target IdentityInfo
     ```

     コマンドで使用されるパラメーターの説明は次のとおりです。

     - `IdentityAccountName`: 修復する必要があるIDアカウントの名前。
     - `PrivilegedUserName`: IDプロバイダー（ADまたはAzureAD）に対する書き込み権限を持つユーザーアカウント。
     - `PrivilegedUserPassword`: PrivilegedUserNameのパスワード。

- `Target`: 修復アクションのターゲット。アカウントのパスワード/信頼キーを修復するためのIdentityInfo、およびハイブリッドAzureAD参加済みマシンIDのユーザー証明書属性を修復するためのUserCertificateを指定できます。

- IDディスクのすべての構成をリセットするには、次のコマンドを次の順序で実行します。

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1
-PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
-Target IdentityInfo
```

```
Reset-ProvVMDisk ProvisioningSchemeName &lt;name> -VMName &lt;name>
 -Identity
```

- IDディスクを完全に再作成するには:

```
Reset-ProvVMDisk -ProvisioningSchemeName &lt;name> -VMname &lt;name>
-Identity -Recreate
```

4. アクションを確認するには、「**y**」と入力します。`-Force`パラメーターを使用して確認プロンプトをスキップすることもできます。例：

```
Reset-ProvVMDisk -ProvisioningSchemeName &lt;name> -VMName &lt;name>
-Identity -Force
```

5. 更新されたIDディスク設定を確認するには、`Get-ProvVM -ProvisioningSchemeName <name -VMName <name>`を実行します。IDディスクの属性（例：`IdentityDiskId`）は更新されている必要があります。`StorageId`と`IdentityDiskIndex`は変更されていてはなりません。

既存のマシンカタログのキャッシュ構成を変更する

MCSIOを有効にして非永続カタログを作成した後、Set-ProvSchemeコマンドを使用して次のパラメーターを変更できます。

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

この機能は現在、以下に適用されます。

- GCPおよびMicrosoft Azure環境、および

- MCSIOが有効な非永続カタログ

要件

キャッシュ構成を変更するための要件は次のとおりです。

- VDAを最新バージョン（2308以降）に更新します。
- 既存のマシンカタログに対してパラメーター `UseWriteBackCache` を有効にします。`UseWriteBackCache` が有効なマシンカタログを作成するには、`New-ProvScheme` を使用します。例：

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -HostingUnitUid
$HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

-MasterImageVM $MasterImage `

-ServiceOffering $ServiceOffering `

-NetworkMap $NetworkMap `

-SecurityGroup $SecurityGroup `

-UseWriteBackCache -WriteBackCacheDiskSize 8
```

キャッシュ構成を変更する

Set-ProvSchemeコマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.ProvisioningSchemeName
-WriteBackCacheDisk32 -WriteBackCacheMemorySize 128
```

注：

- 少なくとも1GBのキャッシュディスクストレージが必要なため、`WriteBackCacheDiskSize` の値はゼロより大きくする必要があります。

- `WriteBackCacheMemorySize` の値は、マシンカタログのメモリサイズよりも小さくする必要があります。
- これらの変更は、変更後にカタログに追加された新しい VM にのみ影響します。既存の VM はこれらの変更の影響を受けません。

トラブルシューティング

- 「電源状態不明」のステータスを持つマシンについては、ガイダンスとしてCTX131267を参照してください。
- 電源状態が不明と継続的に表示されるVMを修正するには、電源状態が不明と継続的に表示されるVMを修正する方法を参照してください。

次のステップ

特定のクラウドサービスカタログの管理については、以下を参照してください。

- AWSカタログの管理
- XenServerカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage/manage-machine-catalog-citrix-hypervisor.html)
- Google Cloud Platformカタログの管理
- Microsoft Azureカタログの管理
- マイクロソフト System Center Virtual Machine Manager カタログの管理
- VMwareカタログの管理

AWSカタログの管理

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、AWSクラウド環境に固有の詳細を扱います。

注:

AWSカタログを管理する前に、AWSカタログの作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-aws.html)を参照してください。

タグを削除する

カタログまたはVMを作成すると、MCSによって作成されたタグが以下のリソースに作成されます。

- 仮想マシン
- ルートディスクボリューム
- 識別ディスクボリューム
- NIC
- ルートディスクイメージ (AMI)
- 起動テンプレート
- AMIまたはルートディスクのスナップショット

Citrix®データベースからVMとマシンカタログを削除し、MCSによって作成されたタグを削除できます。以下を使用できます。

- `Remove-ProvVM`を`ForgetVM`パラメーターとともに使用して、マシンカタログから単一のVMまたはVMのリストからVMとMCSによって作成されたタグを削除します。
- Citrixデータベースからマシンカタログを、またマシンカタログからリソースを削除するには、`ForgetVM`パラメーターを指定して`Remove-ProvScheme`を実行します。

この機能は永続VMにのみ適用されます。

これを行うには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. VMを削除する前に、VMのロックを解除します。例：

   ```
   Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
   ```

4. 以下のいずれかのコマンドを実行して、リソースからVM、マシンカタログ、およびMCSによって作成されたタグを削除します。

   - CitrixデータベースからVMを、またVMからタグを削除するには、`ForgetVM`を指定して`Remove-ProvVM`を実行します。例：

```
Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
-ForgetVM
```

- Citrixデータベースからマシンカタログを、またマシンカタログからリソースを削除するには、`Remove-ProvScheme`を実行します。例：

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
```

5. VMがDelivery Controller™から削除されているが、ハイパーバイザーからは削除されていないことを確認します。

   a. `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`を実行します。これは何も返さないはずです。

   b. AWS EC2コンソールに移動します。VMが表示されるはずですが、タグは削除されています。次のリソースからタグが削除されます：

      - 仮想マシン
      - ルートディスクボリューム
      - IDディスクボリューム
      - NIC

6. マシンカタログを削除した場合は、カタログがDelivery Controllerから削除されていることを確認します。

   a. `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`を実行します。これによりエラーが返されるはずです。

   b. AWS EC2コンソールで、以下のリソースが削除されていることを確認します。

      - ルートディスクイメージ (AMI)
      - 起動テンプレート
      - AMIまたはルートディスクのスナップショット

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"名前": "VMName_IdentityDisk"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
NIC	"説明": "XD NIC"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"名前": "VMName_rootDisk"
	"XdConfig": "XdProvisioned=True"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix リソース": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
PrepVM	"名前": "準備 - CatalogName - xxxxxxxxxx"
	"Xd構成": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix リソース": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""

リソース名	タグ
発行済みスナップショット	"XdConfig": "XdProvisioned=true"
	Volume Worker AMI のスナップショットでない場合、"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
テンプレート	[when AwsCaptureInstanceProperties = true] "XdConfig": "XdProvisioned=true"
	[when AwsCaptureInstanceProperties = true] "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
カタログ内の VM	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:id":"lt-xxxx"
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:version": "n"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
ボリュームワーカー AMI	"Xd設定": "Xdプロビジョニング済み=true"
ボリュームワーカーブートストラッパー	"名前": "XenDesktop® 一時"

リソース名	タグ
	"Xd設定": "Xdプロビジョニング済み=true"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixVolumeWorkerBootstrapper": ""
ボリュームワーカーインスタンス	"名前": "Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx"
	"Xd設定": "Xdプロビジョニング済み=true"

詳細情報

- 接続とリソースの作成および管理
- AWSへの接続
- マシンカタログの作成
- AWS カタログを作成する
- マシンカタログの管理

XenServer®カタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱います。

> **注:**
>
> XenServerカタログを管理する前に、XenServerカタログの作成を完了する必要があります。「XenServerカタログの作成」を参照してください。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
公開されたベースディスクと、各ネットワークまたはローカルストレージ上のそのコピー	"シトリックスプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
IDディスク	"シトリックスプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
準備用VM	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
カタログ内のVM	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
WBCディスク	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

詳細情報

- 接続とリソースの作成および管理
- XenServerへの接続
- マシンカタログの作成
- XenServerカタログを作成する
- マシンカタログの管理

Google Cloud Platformカタログの管理

(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html)では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Google Cloud環境に固有の詳細を扱います。

> **注:**
>
> Google Cloud Platformカタログを管理する前に、Google Cloud Platformカタログの作成を完了する必要があります。Google Cloud Platformカタログの作成を参照してください。

マシンカタログの管理

カタログへのマシンの追加、マシンの更新、および更新のロールバックについては、(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html)を参照してください。

電源管理

Citrix DaaS™では、Google Cloudマシンの電源管理が可能です。左ペインの**検索**ノードを使用して、電源管理したいマシンを見つけます。以下の電源操作が利用可能です。

- 削除
- 起動
- 再起動
- 強制再起動
- シャットダウン
- 強制シャットダウン
- デリバリーグループに追加
- タグの管理
- メンテナンスモードをオンにする

Autoscale を使用して Google Cloud マシンを電源管理することもできます。そのためには、Google Cloud マシンをデリバリーグループに追加し、そのデリバリーグループで Autoscale を有効にします。Autoscale の詳細については、Autoscaleを参照してください。

PowerShellを使用してプロビジョニングされたマシンを更新する

`Set-ProvScheme`コマンドはプロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShell コマンド `Set-ProvVMUpdateTimeWindow` を使用すると、現在のプロビジョニングスキームを既存の永続マシンまたは非永続マシン、あるいはマシンセットに適用できるようになりました。現在、GCP では、この機能でサポートされているプロパティの更新はマシンプロファイルです。

更新できるもの:

- 単一の VM
- 特定の VM のリスト、またはプロビジョニングスキーム ID に関連付けられているすべての既存の VM
- 特定の VM のリスト、またはプロビジョニングスキーム名に関連付けられているすべての既存の VM

既存の VM を更新するには:

1. 既存のマシンの構成を確認します。例えば、,

```
Get-ProvScheme | select ProvisioningSchemeName,
ProvisioningSchemeVersion
```

2. プロビジョニングスキームを更新します。例えば、,

```
`Set-ProvScheme –ProvisioningSchemeName "my-catalog" –MachineProfile
"XDHyp:\HostingUnits\<hosting-unit>\machineprofileinstance.vm"
```

3. VM の現在のプロパティが現在のプロビジョニングスキームと一致するか、および VM に保留中の更新アクションがあるかを確認します。例:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

   特定のバージョンを持つマシンを見つけることもできます。例:

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

4. 既存のマシンを更新します。

   - すべての既存のマシンを更新するには：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

   - 特定のマシンのリストを更新するには：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

   - `Get-ProvVM` の出力に基づいてマシンを更新するには：

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

5. 更新がスケジュールされているマシンを検索します。例:

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

6. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。以下のコマンドを使用して更新されたステータスを確認できます。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

既存のカタログのディスク関連のカスタムプロパティを変更する

既存のカタログおよびカタログの既存のVMの、以下のディスク関連のカスタムプロパティを変更できます。

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

注:

- `StorageType` プロパティは OS ディスク用です
- `PersistOsDisk` プロパティは、ライトバックキャッシュが有効な非永続カタログに対してのみ設定できます

この実装により、カタログ作成後でも異なるディスクに異なるストレージタイプを選択できるようになり、異なるストレージタイプに関連する価格設定のバランスを取ることができます。

これを行うには、PowerShell コマンド `Set-ProvScheme` と `Set-ProvVMUpdateTimeWindow` を使用します。

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. カスタムプロパティを取得するには、`Get-ProvVM -VMName <VM name>` を実行します。
4. カスタムプロパティ文字列を変更します。
   a. カスタムプロパティをメモ帳にコピーし、カスタムプロパティを変更します。
   b. **PowerShell** ウィンドウで、メモ帳から変更されたカスタムプロパティを貼り付け、変更されたカスタムプロパティに変数を割り当てます。例:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com/2014/xd/
machinecreation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CatalogZones" Value="" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" /
>

<Property xsi:type="StringProperty" Name="PersistOSDisk"
Value="true" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="pd-standard" />

<Property xsi:type="StringProperty" Name="StorageType" Value="pd-
standard" />

</CustomProperties>'
```

5. 既存のカタログを更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName>
-CustomProperties $cp
```

6. 既存の VM を更新します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. VMを再起動します。次回の電源投入時に、カスタムプロパティの変更が既存のVMに適用されます。

偶発的なマシン削除からの保護

Citrix DaaS を使用すると、Google Cloud 上の MCS リソースを保護し、誤った削除を防ぐことができます。プロビジョニングされた VM は、`deletionProtection` フラグを TRUE に設定して構成します。

デフォルトでは、MCSまたはGoogle Cloudプラグインを介してプロビジョニングされたVMは、InstanceProtectionが有効な状態で作成されます。この実装は、永続カタログと非永続カタログの両方に適用されます。非永続カタログは、インスタンスがテンプレートから再作成されるときに更新されます。既存の永続マシンについては、Google Cloudコンソールでフラグを設定できます。フラグの設定の詳細については、「Googleドキュメントサイト」を参照してください。永続カタログに追加される新しいマシンは、`deletionProtection`が有効な状態で作成されます。

`deletionProtection`フラグを設定したVMインスタンスを削除しようとすると、リクエストは失敗します。ただし、`compute.instances.setDeletionProtection`権限が付与されているか、IAMの**Compute Admin**ロールが割り当てられている場合は、フラグをリセットしてリソースを削除できるようにすることができます。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"CitrixResource": "内部"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
イメージ	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"CitrixResource": "内部"

リソース名	タグ
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
PrepVM	"Citrixリソース": "内部"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
公開されたスナップショット	"CitrixResource": "内部"
ストレージバケット	"Citrixresource": "内部向け"
テンプレート	"CitrixResource": "内部"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
カタログ内のVM	"CitrixResource": "内部"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"。プラグインは、MCSでプロビジョニングされたVMにこのラベルも追加します: "citrix-provisioning-scheme-id": "provSchemeId"。このラベルを使用して、GCPコンソールでカタログ別にフィルタリングできます。
WBCディスク	"CitrixResource": "内部"
	CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

注:

MCSによって作成されたリソースとして識別するために**CitrixResource**タグが追加されている場合、VMはCitrixインベントリに表示されません。タグを削除または名前変更することで、表示されるようになります。

詳細情報

- 接続とリソースの作成および管理
- Google Cloud環境への接続
- マシンカタログの作成
- Google Cloud Platformカタログの作成
- マシンカタログの管理

HPE Moonshot カタログを管理する (プレビュー)

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。次の情報では、HPE Moonshotカタログに固有の詳細について説明します。

> **注:**
>
> HPE Moonshotカタログを管理する前に、HPE Moonshotカタログの作成を完了する必要があります。

電源管理

Citrix Virtual Apps and Desktops™では、HPE Moonshotマシンの電源管理を行うことができます。ナビゲーションペインの**検索**ノードを使用して、電源管理するマシンを見つけます。次の電源操作が利用可能です。

- 起動
- シャットダウン
- 強制シャットダウン
- 再起動
- リセット

> **注:**
>
> **一時停止**および**再開**の電源操作はサポートされていません。

詳細情報

- 接続とリソースの作成および管理
- HPE Moonshotへの接続
- マシンカタログの作成
- HPE Moonshotマシンカタログの作成
- マシンカタログの管理

Microsoft Azureカタログを管理する

マシンカタログを管理するウィザードについては、(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html)で説明しています。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱います。

> **注意：**

> Microsoft Azureカタログを管理する前に、Microsoft Azureカタログの作成を完了する必要があります。「Microsoft Azureカタログを作成する」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html)を参照してください。

VMシャットダウン時にストレージタイプを下位層に変更する

VMをシャットダウンするときに、管理ディスクのストレージタイプを下位層に切り替えることで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown`カスタムプロパティを使用します。

VMをシャットダウンすると、ディスクのストレージタイプは下位層（`StorageTypeAtShutdown`カスタムプロパティで指定）に変更されます。VMの電源をオンにすると、ストレージタイプは元の状態（`StorageType`カスタムプロパティまたは`WBCDiskStorageType`カスタムプロパティで指定）に戻ります。

> **重要:**

> ディスクはVMが少なくとも一度電源オンになるまで存在しません。したがって、VMを最初に電源オンにしたときにストレージタイプを変更することはできません。

要件

- 管理ディスクに適用されます。これは、カスタムプロパティ`UseManagedDisks`をtrueに設定することを意味します。
- 永続OSディスクを持つ永続および非永続カタログに適用されます。これは、カスタムプロパティ`persistOsDisk`をtrueに設定することを意味します。
- 永続WBCディスクを持つ非永続カタログに適用されます。これは、カスタムプロパティ`persistWBC`をtrueに設定することを意味します。

制限

- Microsoftによると、ディスクの種類は1日2回までしか変更できません。Microsoftドキュメントを参照してください。Citrixによると、VMの開始または割り当て解除アクションがあるたびに`StorageType`更新が行われます。したがって、VMあたりの電源アクションの数を1日2回に制限してください。たとえば、午前中にVMを開始するための電源アクションを1回、夕方にVMを割り当て解除するための電源アクションを1回とします。

ストレージの種類を下位層に変更する

手順を進める前に、要件と制限を参照してください。

1. カスタムプロパティ`StorageTypeAtShutdown`を追加し、値をStandard_LRS (HDD)に設定して、`New-ProvScheme`を使用してカタログを作成します。PowerShellを使用したカタログの作成については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

   > **注:**
   >
   > `StorageTypeAtShutdown`が空またはStandard_LRS (HDD)以外の値を持つ場合、操作は失敗します。

   永続カタログ作成時のカスタムプロパティ設定例：

   ```
   $customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
   2014/xd/machinecreation"

   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

   <Property xsi:type="StringProperty" Name="UseManagedDisks"
   Value="true" />
   ```

```
<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

非永続カタログ作成時のカスタムプロパティ設定例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
```

```
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

注:

マシンプロファイルを使用する場合、カスタムプロパティは`MachineProfile`で定義されたプロパティよりも優先されます。

2. VMをシャットダウンし、AzureポータルでVMのストレージの種類を確認します。ディスクのストレージの種類は、`StorageTypeAtShutdown`カスタムプロパティで指定された下位層に変更されます。
3. VMを起動します。ディスクのストレージの種類は、以下に記載されているストレージの種類に戻ります。
   - OSディスクの`StorageType`カスタムプロパティ
   - WBCディスクの`WBCDiskStorageType`カスタムプロパティ（`CustomProperties`で指定した場合のみ）。それ以外の場合は、`StorageType`に記載されているストレージの種類に戻ります。

既存のカタログに`StorageTypeAtShutdown`を適用する

手順を進める前に、要件と制限を参照してください。

`Set-ProvScheme`を使用して、既存のカタログに VM を追加します。この機能は、`Set-ProvScheme`の実行後に追加された新しい VM に適用されます。既存のマシンには影響しません。

既存のカタログに VM を追加する際のカスタムプロパティ設定の例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'



$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName



Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName
-CustomProperties $customProperties
```

既存の VM のストレージタイプをシャットダウン時に下位層に変更する

手順に進む前に、要件 と 制限 を参照してください。

VM のシャットダウン時に既存の VM のストレージタイプを下位層に変更することで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown` カスタムプロパティを使用します。

VM のシャットダウン時に、カタログ内の既存のマシンのストレージタイプを下位層に変更するには：

1. PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. `Get-Provscheme -ProvisioningSchemeName $CatalogName` を実行します。
4. カスタムプロパティ文字列を変更します。

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

5. 既存のカタログのプロビジョニングスキームを更新します。この更新は、`Set-ProvScheme` の実行後に追加された新しい VM に適用されます。

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -CustomProperties
$customProperties
```

6. `StorageTypeAtShutdown` を有効にするために、既存の VM を更新します。

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName
-StartsNow -DurationInMinutes -1
```

7. 次回マシンを起動すると、マシンの `StorageTypeAtShutdown` プロパティが更新されます。ストレージタイプは次回のシャットダウン時に変更されます。
8. カタログ内の各 VM の `StorageTypeAtShutdown` の値を表示するには、次のコマンドを実行します。

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach { $vmName =
$_.VMName; $storageTypeAtShutdown = ($_.CustomVmData | ConvertFrom-
Json).StorageTypeAtShutdown.DiskStorageAccountType; return New-Object
psobject -Property @{ "VMName" = $vmName; "StorageTypeAtShutdown" =
$storageTypeAtShutdown } }
```

プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する

`Set-ProvScheme` コマンドはプロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShell コマンド `Set-ProvVMUpdateTimeWindow` を使用すると、現在のプロビジョニングスキームを既存の永続的または非永続的なマシン、またはマシンセットに適用できます。また、既存の MCS プロビジョニング済みマシンの構成更新のタイムスロットをスケジュールすることもできます。スケジュールされたタイムスロット中の電源オンまたは再起動は、スケジュールされたプロビジョニングスキームの更新をマシンに適用します。現在、Azure では、`ServiceOffering`、`MachineProfile` および以下のカスタムプロパティを更新できます。

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

注:

- Azure 環境でマネージドディスクを使用するカタログの場合、`StorageType`、`WBCDiskStorageType`、および `IdentityDiskStorageType` のカスタムプロパティのみを更新できます。
- `Set-ProvVMUpdateTimeWindow` を2回実行した場合、最新のコマンドが有効になります。

更新できるもの:

- 単一のVM
- 特定のVMのリスト、またはプロビジョニングスキームIDに関連付けられたすべての既存のVM
- プロビジョニングスキーム名（マシンカタログ名）に関連付けられている特定のVMまたはすべての既存VMのリスト

プロビジョニングスキームに以下の変更を加えると、Azureの永続カタログの場合、VMインスタンスが再作成されます:

- `MachineProfile`を変更する
- 削除 `LicenseType`
- 削除 `DedicatedHostGroupId`

> **注:**
>
> 既存のマシンのOSディスクとそのすべてのデータはそのまま残り、新しいVMがそのディスクに接続されます。

既存のVMを更新する前に:

1. 既存のマシンの構成を確認します。たとえば、,

   ```
   Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
   ```

2. プロビジョニングスキームを更新します。例えば、,

   - マシンプロファイルの入力としてVMを使用する場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog" -MachineProfile
     "XDHyp:\HostingUnits\<hosting-unit>\machineprofile.folder\<resource-
     group>.resourcegroup\<virtual-machine>.vm"
     ```

   - マシンプロファイルの入力としてテンプレート仕様を使用する場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog"

     -MachineProfile "XDHyp:\HostingUnits\<hosting-
     unit>\machineprofile.folder\<resource-
     ```

```
group>.resourcegroup\<template-spec>.templatespec\<template-spec-
version>.templatespecversion"

-ServiceOffering "XDHyp:\HostingUnits\<hosting-
unit>\serviceoffering.folder\<service-offering>.serviceoffering"
```

- サービス提供のみの場合:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
"XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
offering>.serviceoffering"
```

3. VMの現在のプロパティが現在のプロビジョニングスキームと一致しているか、およびVMに保留中の更新アクションがあるかを確認します。例えば、,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

特定のバージョンのマシンを見つけることもできます。たとえば、,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

既存のマシンに次回の再起動時に適用される更新を要求するには:

1. 既存のマシンを更新し、次回再起動時に更新を適用するには、次のコマンドを実行します。

- すべての既存のマシンを更新します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

- 特定の仮想マシンのリストを更新します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

- Get-ProvVM の出力に基づいてマシンを更新します。例：

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

注:

- `StartsNow` は、スケジュールされた開始時刻が現在の時刻であることを示します。
- 負の数（例：–1）の `DurationInMinutes` は、スケジュールの時間枠に上限がないことを示します。

2. 更新がスケジュールされているマシンを見つける。例：

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

3. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。以下のコマンドを使用して、更新されたステータスを確認できます。例：

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

スケジュールされた時間枠内で次回起動時に最新のプロビジョニング設定に更新されるように VM をスケジュールするには：

1. 次のコマンドを実行します。

- 開始時刻を現在時刻として更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName vm1 -StartsNow -DurationInMinutes 120
```

- 週末に更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1” -StartTimeInUTC “10/15/2022 9:00am” -DurationInMinutes
(New –TimeSpan –Days 2).TotalMinutes
```

> **注:**
>
> - `VMName` はオプションです。指定しない場合、更新はカタログ全体に対してスケジュールされます。
> - `StartTimeInUTC` の代わりに、`StartsNow` を使用して、スケジュール開始時刻が現在時刻であることを示します。
> - `DurationInMinutes` はオプションです。デフォルトは120分です。負の数（例：-1）は、スケジュールの時間枠に上限がないことを示します。

2. 更新ステータスを確認します。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

3. VM の電源を入れます。スケジュールされた時間枠の後にマシンの電源を入れた場合、構成の更新は適用されません。スケジュールされた時間枠内にマシンの電源を入れた場合、,
   - マシンがオフになっていて、
     - マシンを起動しない場合、構成の更新は適用されません
     - マシンを起動すると、構成の更新が適用されます
   - マシンの電源が入っていて、
     - マシンを再起動しない場合、構成の更新は適用されません
     - マシンを再起動すると、構成の更新が適用されます。

構成の更新をキャンセルするには：

単一のVM、複数のVM、またはカタログ全体の構成更新をキャンセルすることもできます。構成更新をキャンセルするには：

1. `Clear-ProvVMUpdateTimeWindow` を実行します。例：
   - 単一のVMに対してスケジュールされた構成更新をキャンセルするには：

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1”
```

- 複数のVMに対してスケジュールされた構成更新をキャンセルするには：

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
-VMName "vm1","vm2"
```

> **注:**
>
> VM は同じカタログのものである必要があります。

個々のVMのプロパティを更新する

永続的なMCSマシンカタログ内の個々のVMのプロパティは、PowerShellコマンド`Set-ProvVM`を使用して更新できます。ただし、更新はすぐに適用されません。更新を適用するには、PowerShellコマンド`Set-ProvVMUpdateTimeWindow`を使用して時間枠を設定する必要があります。

この実装により、マシンカタログ全体を更新することなく、個々のVMを効率的に管理できます。現在、この機能はAzure環境にのみ適用可能です。

現在、更新できるプロパティは次のとおりです。

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

この機能を使用すると、次のことができます。

- VMのプロパティを更新する
- マシンカタログの更新後にVMで更新されたプロパティを保持する
- VMに適用された構成の更新を元に戻す

VMのプロパティを更新する前に：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールを読み込むには、`asnp citrix*`を実行します。
3. 既存のマシンカタログの構成を確認します。例：

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

4. 更新を適用するVMの構成を確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

VMのプロパティを更新する

VMのプロパティを更新するには、次の手順を実行します。

1. 更新を適用したいVMをシャットダウンします。
2. VMのプロパティを更新します。たとえば、VMのストレージタイプ (`StorageType`) カスタムプロパティを更新したい場合は、次を実行します。

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

マシンカタログ内の2つのVMのプロパティを同時に更新できます。例:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2
-CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

注:

更新はすぐに適用されません。

3. 更新対象として指定されたプロパティのリストと構成バージョンを取得します。例:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -VMName
machine1
```

`Version`のプロパティ値と、更新されるプロパティ (この場合は`StorageType`) を確認します。

4. 構成バージョンを確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion`のプロパティ値を確認します。更新はまだ適用されていません。VMはまだ古い構成のままです。

5. スケジュールされた更新を要求します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog
-StartsNow -DurationInMinutes -1
```

スケジュールされた更新の詳細については、プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する を参照してください。

> **注：**
>
> 保留中のプロビジョニングスキームの更新も適用されます。

6. VMを再起動します。例：

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

7. 構成バージョンを確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion`のプロパティ値を確認します。更新が適用されました。VMに新しい構成が適用されました。

8. VMにさらに構成アップデートを適用するには、VMをオフにして、手順を繰り返します。

マシンカタログの更新後にVMで更新されたプロパティを保持する

VMで更新されたプロパティを保持するには、次の手順を実行します。

1. 更新を適用したいVMの電源をオフにします。

2. マシンカタログを更新します。たとえば、VMサイズ (`ServiceOffering`) とストレージタイプ (`StorageType`) を変更したい場合は、以下を実行します。

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -ServiceOffering
Standard_E4_v3 -CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

3. マシンカタログの構成詳細を取得します。例：

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

`ProvisioningSchemeVersion` が1つ増えました。VMサイズとストレージタイプも更新されます。

4. VMのプロパティを更新します。たとえば、VMにマシンプロファイルを提供します。

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-group>.resourcegroup\<template-
spec>.templatespec\<template-spec-version>.templatespecversion"
```

注:

マシンプロファイルの入力には、タグと異なるVMサイズ (`ServiceOffering`) が指定されています。

5. VM上の構成更新とマシンカタログ更新をマージした後でVMが持つことになるプロパティのリストを取得します。例:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

注:

VMに対するすべてのアップデートは、マシンカタログで行われたアップデートを上書きします。

6. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

7. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

   VMは、マシンプロファイルから派生した更新済みのVMサイズを保持します。マシンプロファイルで指定されたタグ値もVMに適用されます。ただし、ストレージタイプは最新のプロビジョニングスキームから派生します。

8. VMの構成バージョンを取得します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

   `ProvisioningSchemeVersion` と `ProvVMConfigurationVersion` は最新バージョンを表示します。

VMに適用された構成の更新を元に戻す

1. VMに更新を適用した後、VMをオフにします。
2. 次のコマンドを実行して、VMに適用された更新を削除します。例:

```
Set-ProvVM -RevertToProvSchemeConfiguration -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

3. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

4. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. VMの構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` の値が、マシンカタログの構成バージョンになりました。

Azure VM、スナップショット、OSディスク、ギャラリーイメージ定義の情報を取得する

Azure VMのOSディスクと種類、スナップショット、ギャラリーイメージ定義を含む情報を表示できます。この情報は、マシンカタログが割り当てられている場合、マスターイメージ上のリソースに対して表示されます。この機能を使用して、LinuxまたはWindowsイメージを表示および選択します。PowerShellプロパティ `TemplateIsWindowsTemplate` が `AdditionDatafield` パラメーターに追加されました。このフィールドには、VMの種類、OSディスク、ギャラリーイメージ情報、OSの種類情報など、Azure固有の情報が含まれています。`TemplateIsWindowsTemplate` を **True** に設定するとOSの種類がWindowsであることを示し、`TemplateIsWindowsTemplate` を **False** に設定するとOSの種類がLinuxであることを示します。

ヒント:

`TemplateIsWindowsTemplate` PowerShellプロパティによって表示される情報は、Azure APIから取得されます。場合によっては、このフィールドが空になることがあります。たとえば、データディスクからのスナップショットには、スナップショットからOSの種類を取得できないため、`TemplateIsWindowsTemplate` フィールドは含まれません。

たとえば、PowerShellを使用してWindows OSタイプの場合、Azure VM `AdditionData` パラメーターを **True** に設定します。

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value

ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192
```

```
ServiceOfferingCores 2

TemplateIsWindowsTemplate True

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

MCSによって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
イメージ	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
NIC	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
OSディスク	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
PrepVM	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
公開スナップショット	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"

リソース名	タグ
リソースグループ	"CitrixResource" : "内部"
	CitrixSchemaVersion: 2.0
	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ストレージアカウント	"シトリックスプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
カタログ内のVM	"シトリックスプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
WBCディスク	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"

注：

CitrixResourceタグがMCSによって作成されたリソースとして識別するために追加されている場合、VMはCitrixインベントリに表示されません。タグを削除または名前変更することで、表示させることができます。

詳細情報

- 接続とリソースの作成および管理
- Microsoft Azureへの接続
- マシンカタログの作成
- Microsoft Azureカタログの作成
- マシンカタログの管理

Microsoft System Center Virtual Machine Manager カタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) 仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMMカタログを管理する前に、VMMカタログの作成を完了する必要があります。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-mscvmm.html)を参照してください。

MCSによって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
準備VM	タグの文字列は次のとおりです: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	カスタムプロパティエントリ: 「"XdConfig:"XdProvisioned=True"」
カタログ内のVM	タグの文字列は次のとおりです: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	カスタムプロパティエントリ: 「"XdConfig:"XdProvisioned=True"」

詳細情報

- 接続とリソースを作成および管理する(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/connections.html)
- マイクロソフト システムセンター バーチャルマシンマネージャーへの接続
- マシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create.html)

- Microsoft System Center Virtual Machine Managerカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-mscvmm.html)
- マシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html)

VMwareカタログの管理

「マシンカタログの管理」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html)では、マシンカタログを管理するウィザードについて説明します。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMwareカタログを管理する前に、VMwareカタログの作成を完了する必要があります。「VMwareカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-vmware.html)を参照してください。

マシンカタログのフォルダーIDを更新する

MCSマシンカタログのフォルダーIDは、`Set-ProvScheme`コマンドのカスタムプロパティで`FolderId`を指定することで更新できます。フォルダーIDの更新後に作成されたVMは、この新しいフォルダーIDの下に作成されます。このプロパティが`CustomProperties`で指定されていない場合、VMはマスターイメージが配置されているフォルダーの下に作成されます。

マシンカタログのフォルダーIDを更新するには、次の手順を実行します。

1. Webブラウザーを開き、**vSphere Web Client**のURLを入力します。
2. 資格情報を入力し、**ログイン**をクリックします。
3. **vSphere Web Client**でVM配置フォルダーを作成します。
4. PowerShellウィンドウを開きます。
5. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix®***を実行します。
6. `Set-ProvScheme`の`CustomProperties`で`FolderID`を指定します。この例では、フォルダーIDの値は`group-v2406`です。

```
Set-ProvScheme -ProvisioningSchemeUid
"50bb319c-2e83-4a37-9ea1-94f630687372" -CustomProperties
"<CustomProperties xmlns=""http://schemas.citrix.com/2014/xd/
machinecreation"" xmlns:xsi=""http://www.w3.org/2001/XMLSchema-
instance""><Property xsi:type=""StringProperty"" Name=""FolderId""
Value=""group-v2406"" /></CustomProperties>"
```

7. Studioを使用してマシンカタログにVMを追加します。
8. vSphere Web Clientで新しいVMを確認します。新しいVMは新しいフォルダーの下に作成されます。

vSphereでフォルダーIDを検索する

VM のフォルダー ID を見つけるには、任意の ESXi または vCenter サーバーシステムで Managed Object Browser (MOB) にアクセスします。

MOBは、すべてのESX/ESXiおよびvCenterサーバーシステムに組み込まれているWebベースのサーバーアプリケーションです。このvSphereユーティリティを使用すると、VM、データストア、リソースプールなどのオブジェクトに関する詳細情報を表示できます。

1. Web ブラウザーを開き、`http://x.x.x.x/mob` を入力します。ここで、x.x.x.x は vCenter Server または ESX/ESXi ホストの IP アドレスです。例: `<https://10.60.4.70/mob>`。
2. MOB の **Home** ページで、プロパティ **content** の値をクリックします。
3. **rootFolder** の値をクリックします。
4. **childEntity** の値をクリックします。
5. **vmFolder** の値をクリックします。
6. フォルダー ID は **childEntity** の値で見つけることができます。

VMのストレージ移行

既存のVMのディスクストレージを古いストレージから新しいストレージに移動できます。移行中、MCSは電源管理、OSディスクのリセットなどのVM機能を保持します。新しいディスクストレージを使用して、新しいVMをマシンカタログに追加することもできます。これを行うには、PowerShellコマンド`Move-ProvVMDisk`を使用します。

現在、フルクローン永続 VM のみ移行できます。

新しいストレージは、次の条件を満たす必要があります。

- 古いストレージと同じクラスター内にある必要があります。

- VMが実行されているホストは、古いデータストアと新しいデータストアの両方にアクセスできる必要があります。

次のタスクを実行できます。

- ディスクストレージの移行
- 古いストレージを非推奨にする

ディスクストレージの移行

ディスクストレージを移行するには：

1. 既存のホスティングユニットに新しいストレージを追加します。古いストレージを**Superseded**に変更します。これはWeb StudioまたはPowerShellコマンドを使用して実行できます。
    - Web Studioを使用している場合は、ストレージの編集を参照してください。
    - PowerShellコマンドを使用している場合：
        - 既存のホスティングユニットに新しいストレージを追加するには、`Add-Hyphostingunitstorage`を実行します。
        - 古いストレージでの新しいVM作成を無効にするには、**Superseded**をtrueとして`Set-Hyphostingunitstorage`を実行します。
2. VMをシャットダウンし、**メンテナンスモード**をオンにします。
3. VMのディスクストレージを新しいストレージに移動し、ストレージ情報を更新します。例:

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -VMName
("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,Identity
-DestinationStorageId datastore1,datastore1
```

4. 移行のタスクIDを取得します。例:

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName xxxxx -DiskType OS,Identity
-DestinationStorageId datastore1,datastore1
```

5. 移行のステータスを確認します。

- `(Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines`: ディスク移行が成功したVMのリストを提供します。これには、すでに新しいストレージに移行されたVMも含まれます。
- `(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines`: 移行に失敗したVMのリストを提供します。
- `(Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines`: 移行がまだ開始されていないVMのリストを提供します。
- `Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware-TestVM01`: 移行後の更新されたVMプロパティを提供します。`StorageId`、`AssignedImage`、`BootedImage`、`IdentityDiskId`、`IdentityDiskStorage`、および`LastBootTime`などのプロパティを確認してください。

スナップショット付きのMCSで作成されたVMのディスクを移行した後、**vSphere Clientで統合が必要です**という警告が表示されることがあります。統合してデータ損失を回避するには：

1. VMware VMのバックアップを作成します。たとえば、すべてのVMファイルをデータストア上の別のフォルダーに転送します。
2. 警告が表示されたら、**Consolidate**をクリックし、次に**OK**をクリックして統合を確定します。

古いストレージの廃止

VMディスクの移行後に古いストレージを非推奨にするには：

1. ホスティングユニットの各ディスクストレージにおけるベースディスクとマシン数に関する情報を取得します。例：

   ```
   $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName xxxxx

   $result

   $result.ProvResourceInStorage | Format-List -Property *
   ```

   移行が成功すると、MCSは古いベースディスクを自動的に削除し、古いストレージにはマシンが存在しなくなります。したがって、コマンドを実行した後、古いストレージにマシンとベースディスクがないことを確認してください。
2. ホスティングユニットから古いストレージを完全に削除するには、`Remove-Hyphostingunitstorage`を実行します。Web Studio を使用して古いストレージを削除することもできます。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
準備用VM	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=True"
カタログ内のVM	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=True"

詳細情報

- 接続とリソースの作成および管理
- VMwareへの接続
- マシンカタログの作成
- VMwareカタログを作成する
- マシンカタログの管理

電源管理

Citrix Virtual Apps and Desktops™ を使用すると、さまざまなサポート対象のハイパーバイザーおよびクラウドサービスでMCSプロビジョニングされたVMの電源を管理できます。電源管理操作により、以下が提供されます。

- 最適なユーザーエクスペリエンス
- コスト管理と電力節約

利用可能な電源操作は次のとおりです。

- 起動
- シャットダウン
- 再起動
- 一時停止
- 再開

- 強制再起動
- 強制シャットダウン

> **注:**
>
> - 非永続VMの場合、電源サイクル（シャットダウン/起動および再起動）はOSディスクのリセットにつながります。
> - 電源操作の機能と動作は、ハイパーバイザーまたはクラウドサービスによって異なります。

> この記事では、特定のサポート対象ハイパーバイザーに関連する主要な電源管理機能について説明します。

- AWS VM の電源管理
- Azure VM の電源管理

AWS VM の電源管理

必要な権限については、必要なAWS権限を参照してください。

インスタンスのハイバネーション

ハイバネーションプロセスは、インスタンスのインメモリ状態と、そのプライベートおよびエラスティックIPアドレスを保存し、中断したところから正確に再開できるようにします。

インスタンスにハイバネートするよう指示されると、インメモリ状態をルートEBSボリュームのファイルに書き込み、その後シャットダウンします。Amazon EBSボリュームは、インスタンスにアタッチできる耐久性のあるブロックレベルのストレージデバイスです。ボリュームをインスタンスにアタッチすると、物理ハードドライブと同じように使用できます。インスタンスのルートEBSボリュームを暗号化します。暗号化により、機密データがメモリからEBSボリュームにコピーされる際に適切に保護されます。EBS暗号化の詳細については、Amazon EBS暗号化を参照してください。

サポートされているインスタンスハイバネーションの制限事項は次のとおりです。

- インスタンスメモリ（RAM）は最大150 GBまでのみサポートされています
- UEFIブートモードはサポートされていません

- 汎用SSDとプロビジョンドIOPS SSDのみがEBSボリュームタイプとしてサポートされています。

ハイバネーション対応VMの作成

ハイバネーション対応VMを作成するには：

1. ホスト接続を作成します。AWSへの接続を参照してください。
2. EBSルートが暗号化され、**Stop-Hibernate**プロパティが有効になっているインスタンスを起動します。インスタンスの起動方法、ルートEBSボリュームの暗号化、およびハイバネーションの有効化の詳細については、`<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/>`を参照してください。このインスタンスをマスターイメージとして使用してAMIを作成します。
3. マスターイメージを準備します。
   a. マスターイメージにVDAをインストールします。Citrixは、最新機能にアクセスできるように、最新バージョンのインストールを推奨しています。マスターイメージにVDAをインストールしないと、カタログの作成が失敗します。VDAのインストール方法の詳細については、VDAのインストールを参照してください。
   b. マスターイメージを、アプリケーションとデスクトップが属するドメインに参加させます。マスターイメージが、マシンが作成されるホストで利用可能であることを確認してください。
4. そのインスタンスからAMIを作成します。インスタンスからAMIを作成する方法については、「Amazon EC2インスタンスからAMIを作成する」を参照してください。
5. `New-ProvScheme`コマンドを使用してマシンカタログを作成します。`AwsCaptureInstanceProperties`カスタムプロパティを**True**に設定します。完全構成インターフェイスでAWSインスタンスプロパティを有効にする方法については、「完全構成インターフェイスでAWSインスタンスプロパティを適用し、運用リソースにタグ付けする」を参照してください。

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot

-CustomProperties "AwsCaptureInstanceProperties,true;"

-HostingUnitName "xxx" -IdentityPoolName $catalog_name
-InitialBatchSizeHint 1

-MasterImageVM "xyz.template" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\MyConn\\us-east-2a.availabilityzone\10.0.0.0``/24
```

```
(vpc-0f1771e45671aedcd).network"}

-ProvisioningSchemeName $catalog_name

-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -ServiceOffering
"xxx"
```

PowerShell コマンドを使用してマシンカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/>` を参照してください。

ハイバネート可能な VM は、次の場合に作成されます。

- **Stop-Hibernate** プロパティが有効になっているマスターイメージから作成された AMI を選択した場合。
- マスター VM がドメインに参加しており、VDA がインストールされている場合。
- 休止状態を処理できる正しいVMサイズ（サービス提供）を選択します。

New-ProvSchemeコマンドは、次の場合に適切なエラーメッセージを表示して失敗します。

- マスターVMは休止状態が有効になっていますが、サービス提供は休止状態を処理できません。
- マスターVMがドメインに参加しておらず、VDAがインストールされていない場合。

サービス提供とAMIの休止状態

サービス提供とAMI（テンプレート）の休止状態を取得するには、次のコマンドを実行します。

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

既存のハイバネーション対応プロビジョニングスキームのサービスオファリングを更新する

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering
<String>
```

サービス提供に互換性がない場合、システムは例外メッセージを表示します。

ハイバネーションをサポートするマシンカタログを更新する

既存のマシンカタログを、ハイバネーションをサポートしないマシンカタログで更新しようとすると、更新は失敗し、適切なエラーメッセージが表示されます。

休止状態のVMの電源管理

休止状態のVMに対して、以下の電源管理操作を実行できます。

1. 実行状態からVMをサスペンドします。
2. サスペンド状態からVMを再開します。
3. サスペンド状態からVMを再起動します。

Azure VMの電源管理

必要な権限については、「必要なAzure権限」を参照してください。

Azureオンデマンドプロビジョニング

Azureオンデマンドプロビジョニングでは、プロビジョニングが完了した後、Citrix Virtual Apps and Desktops™が電源オンアクションを開始したときにのみVMが作成されます。

MCSを使用してAzure Resource Managerでマシンカタログを作成する場合、Azureオンデマンドプロビジョニング機能は次のことを行います。

- ストレージコストを削減します
- より高速なカタログ作成を提供します

MCSカタログを作成すると、Azureポータルにリソースグループ内のネットワークセキュリティグループ、ネットワークインターフェイス、ベースイメージ、およびIDディスクが表示されます。

Azureポータルには、Citrix Virtual Apps and Desktopsが電源オンアクションを開始するまでVMは表示されません。次の違いを持つ2種類のマシンがあります。

- プールされたマシンの場合、オペレーティングシステムディスクとライトバックキャッシュはVMが存在する場合にのみ存在します。コンソールでプールされたマシンをシャットダウンすると、VMはAzureポータルに表示されません。定期的にマシンをシャットダウンする場合（たとえば、営業時間外）、ストレージコストを大幅に節約できます。
- 専用マシンの場合、オペレーティングシステムディスクはVMが最初に電源オンされたときに作成されます。AzureポータルのVMは、マシンIDが削除されるまでストレージに残ります。コ

ンソールで専用マシンをシャットダウンしても、VMはAzureポータルに表示されたままになります。

電源サイクル時にプロビジョニングされた仮想マシンを保持する

電源サイクル時にプロビジョニングされた仮想マシンを保持するかどうかを選択します。PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。このパラメーターは、プロビジョニングされた仮想マシンが電源サイクル時に永続化するかどうかを決定するために使用される追加のプロパティ`PersistVm`をサポートします。電源オフ時に仮想マシンを永続化するには`PersistVm`プロパティを**true**に設定し、電源オフ時に仮想マシンが保持されないようにするには**false**に設定します。

> **注:**
>
> `PersistVm`プロパティは、`CleanOnBoot`および`UseWriteBackCache`プロパティが有効になっているプロビジョニングスキームにのみ適用されます。非永続仮想マシンに対して`PersistVm`プロパティが指定されていない場合、それらは電源オフ時にAzure環境から削除されます。

> 「次の例では、`New-ProvScheme CustomProperties`パラメーターは`PersistVm`プロパティを **true** に設定します。」:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />

<Property xsi:type="StringProperty" Name="LicenseType"
```

```
Value="Windows_Client" />

</CustomProperties>
```

以下の例では、`New-ProvScheme CustomProperties` パラメーターは、ライトバックキャッシュを保持するために `PersistVM` を **true** に設定します。

```
 New-ProvScheme

 -AzureAdJoinType "None"

 -CleanOnBoot

 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache
```

```
-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

ヒント:

`PersistVm` プロパティは、プロビジョニングされた仮想マシンを保持するかどうかを決定します。`PersistOsdisk` プロパティは、OSディスクを永続化するかどうかを決定します。プロビジョニングされた仮想マシンを保持するには、まずOSディスクを保持します。仮想マシンを削除せずにOSディスクを削除しないでください。`PersistVm` パラメーターを指定せずに `PersistOsdisk` プロパティを使用できます。

ストレージタイプの変更失敗時の電源オン動作をカスタマイズする

電源オン時に、Azureでの障害により、管理ディスクのストレージタイプが目的のタイプに変更できない場合があります。このようなシナリオでは、VMはオフのままで、障害メッセージが送信されます。ただし、ストレージが構成されたタイプに復元できない場合でもVMの電源をオンにするか、VMをオフのままにするかを選択できます。

- カスタムプロパティ `FailSafeStorageType` を **true** (デフォルト設定) に構成した場合、または `New-ProvScheme` または `Set-ProvScheme` コマンドで指定しない場合:
  - 電源オン時に、VMは誤ったストレージタイプで電源がオンになります。
  - シャットダウン時に、VMは誤ったストレージタイプでオフのままになります。
- `New-ProvScheme` または `Set-ProvScheme` コマンドでカスタムプロパティ `FailSafeStorageType` を **false** に構成した場合:
  - 電源オン時に、VMは誤ったストレージタイプでオフのままになります。
  - シャットダウン時に、VMは誤ったストレージタイプでオフのままになります。

マシンカタログを作成するには：

1. PowerShellウィンドウを開きます。
2. `asnp citrix*` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. 既に作成されていない場合は、IDプールを作成します。
4. `New-ProvScheme` にカスタムプロパティを追加します。例：

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\Azure-
Resources-1\image.folder\abc.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\Azure-
Resources-1\ght.folder\abc.resourcegroup\abc-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\Azure-
Resources-1\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"true`" />

</CustomProperties>"
```

5. マシンカタログを作成します。Remote PowerShell SDK を使用したカタログの作成方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

既存のマシンカタログを更新して、`FailSafeStorageType`カスタムプロパティを含めます。この更新は既存のVMには影響しません。

1. `Set-ProvScheme`コマンドでカスタムプロパティを更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "

<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
```

```
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"false`" />

</CustomProperties>"
```

Set-ProvScheme で行われた変更を既存のVMに適用するには、`-StartsNow` と`-DurationInMinutes -1`パラメーターを指定して`Set-ProvVMUpdateTimeWindow`コマンドを実行します。

1. `-StartsNow`と`-DurationInMinutes -1`パラメーターを指定して`Set-ProvVMUpdateTimeWindow`コマンドを実行します。例：

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

2. VMを再起動します。

休止状態対応VMを作成する

Azure環境では、休止状態をサポートするMCSマシンカタログを作成できます。この機能を使用すると、VMを中断し、ユーザーが再度サインインしたときにVMの以前の状態に再接続できます。

休止状態機能は以下に適用されます。

- シングルセッションOS
- 永続VMおよび非永続VM
- 静的およびランダム（プールされた）VDIデスクトップ

VDI デスクトップが静的かランダムかに関わらず、VM を休止状態にした後、同じセッションに再開できます。

このセクションでは、以下を参照してください。

- 前提条件

- 制限事項
- 休止状態対応のマシンカタログの作成と管理
- 既存の休止状態対応VM用のマシンカタログの作成
- 休止状態プロパティの確認
- VMの電源管理（手動および自動）

休止状態を使用するための前提条件

休止状態を使用するには、以下のタスクを完了していることを確認してください。

- WindowsとLinuxの両方のマスターイメージにAzure VMエージェントをインストールします。Windowsイメージのページファイルは一時ディスクに配置できます。マシンカタログで休止状態が有効になっている場合、MCSはページファイルの場所をベースディスクのC:ドライブに設定します。
- MCSは、生成されたリソースの休止状態プロパティを自動的に設定します。休止状態をサポートするために、マスターリソースのプロパティを構成する必要はありません。
- サブスクリプションで休止状態をサポートするVMサイズを使用してください。
- VMが休止状態機能を継承できるように、休止状態対応のマシンプロファイル（VMまたはテンプレート仕様）を作成します。VMの作成については、休止状態の概要を参照してください。

> **注:**
>
> Microsoftによると、OSディスクから休止状態が有効なVMを展開できます。この機能は現在一部のリージョンでサポートされており、まもなくすべてのリージョンで利用可能になります。詳細については、「OSディスクから休止状態が有効なVMを展開する」を参照してください。

> テンプレートスペックを作成するには、次の手順を実行します。

a. Azure Portalを開きます。テンプレートで使用する構成のVMを選択します。左側のペインで**テンプレートのエクスポート**を選択します。

b. **パラメーターを含める**チェックボックスをオフにします。コンテキストをコピーし、例えば`VMExportTemplate.json`のようなJSONファイルとして保存します。

c. テンプレートでパラメーター`hibernationEnabled`が`true`であることを確認します。パラメーターが`true`でない場合は、使用したVM構成を確認してください。テンプレート

ファイルでサポートされているVMサイズを指定できます。ただし、カタログの作成時にマシンサイズを指定することもできます。

d. ネットワークインターフェースリソースのテンプレートをJSONファイル `VMExportTemplate.json` に追加します。その結果、2つのリソースを持つARMテンプレートファイルができます。

e. **Azure Portal > テンプレートスペック > テンプレートのインポート > ローカルテンプレートファイルの選択**を選択して、このテンプレートファイルをARMテンプレートスペックとしてインポートします。

f. ARMテンプレート仕様が作成されたら、それをマシンプロファイルとして使用できます。

> **注：**
>
> Citrix Studioに同期されるまで数分かかる場合があります。

詳細については、Microsoftドキュメントの休止状態を使用するための前提条件を参照してください。

制限事項

- シングルセッションOSマシンカタログ（永続的および非永続的）のみがサポートされています。
- エフェメラルOSディスクとMCS I/O機能は、Azureの休止状態をサポートしていません。
- 自動Windowsアップデート中に休止状態が失敗する可能性があります。

詳細については、Microsoftドキュメントを参照してください。

休止状態対応のマシンカタログを作成および管理する

休止状態対応VMを作成するには、以下を使用して休止状態対応マシンカタログを作成および管理できます。

- Web Studio、または
- PowerShellコマンド

WEB STUDIOを使用してカタログを作成する

1. **「マシンカタログの作成」**を選択します。カタログ作成ウィザードが開きます。
2. **「マシンタイプ」ページで、このカタログの「シングルセッションOS」**マシンタイプを選択します。

3. **「マシン管理」**ページで、次のように設定を選択します。
   a. **「電源管理されているマシン（仮想マシンやブレードPCなど）」**を選択します。
   b. **「Citrix Machine Creation Services™ (MCS)」**を選択します。
4. **「デスクトップエクスペリエンス」**ページで、必要に応じてランダムまたは静的デスクトップエクスペリエンスを選択します。
5. **「イメージ」ページで、マスターイメージを選択します。**「マシンプロファイルを使用する」**チェックボックスをオンにし、休止状態をサポートするマシンプロファイルを選択します。ツールヒントをクリックして、マシンプロファイルが休止状態をサポートしているかどうかを確認します。
6. **「ストレージとライセンスの種類」**ページで、このカタログに使用するストレージとライセンスを選択します。
7. **「仮想マシン」**ページで、VMの数、VMサイズ、および可用性ゾーンを選択します。

> **注:**
>
> ハイバネーションをサポートするマシンサイズのみが、選択肢として表示されます。

8. **NIC**ページで、VMで使用するNICを追加します。
9. **ディスク設定**ページで、ライトバックキャッシュディスクのストレージタイプとサイズを選択します。
10. **リソースグループ**ページで、VMをプロビジョニングするリソースグループを選択します。
11. **マシンID**ページで、**「新しいActive Directoryアカウントを作成する」**を選択します。次に、アカウント命名スキームを指定します。
12. **ドメイン資格情報**ページで、**「資格情報を入力」**をクリックします。ターゲットのActive Directoryドメインでアカウント作成を実行するために、ドメイン資格情報を入力します。
13. **「概要」**ページで、マシンカタログの名前を入力し、**「完了」**をクリックします。

MCSマシンカタログの作成が完了したら、カタログリストでそのカタログを見つけ、**テンプレートプロパティ**タブをクリックします。パラメーター**ハイバネーション**の値は**サポート済み**である必要があります。

マシンカタログを編集する場合は、以下の制限事項を考慮してください。

- 現在のマシンカタログがハイバネーションをサポートしている場合、次のことはできません。

  - VMサイズをハイバネーション非対応のものに変更する。
  - マシンプロファイルをハイバネーション非対応のものに変更する。

- 現在のマシンカタログがハイバネーションをサポートしていない場合、次のことはできません。
  - 現在のところ、Web Studioを使用してマシンプロファイルをハイバネーション対応のものに変更する。

既存のハイバネーション対応VMを管理するためのマシンカタログを作成する

既に休止状態対応VMがあり、それらを一時停止および再開したい場合は、それらのVMを電源管理のためにインポートするマシンカタログを作成します。

> **注:**
>
> 休止状態に対応しているVMと対応していないVMの両方を含むマシンカタログを作成できます。ただし、休止状態に関連する機能が必要な場合は、休止状態に対応しているVMのみを含むマシンカタログを作成する必要があります。

> Web Studioを使用して既存の休止状態対応VMのカタログを作成するには、画面の指示に従って手順を完了し、以下の主要な設定に注意してください。

1. 「**マシン管理**」ページで、「**電源管理されているマシン**」を選択し、マシンの展開方法として「**その他のサービスまたはテクノロジー**」を選択します。
2. 「**仮想マシン**」ページで、休止状態に対応しているVMのみを追加またはインポートします。

POWERSHELLコマンドを使用してマシンカタログを作成する

休止状態を使用するためのすべての要件を満たした後、`New-ProvScheme`コマンドを使用して休止状態対応のマシンカタログを作成できます。Remote PowerShell SDKを使用してカタログを作成する方法については、New-ProvSchemeを参照してください。

カタログの作成中に、以下のPowerShellコマンドを使用して、VMサイズとマシンプロファイルが休止状態をサポートしているかどうかを確認できます。

- VMサイズの場合、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.folder") |
select Name, AdditionalData | ConvertTo-Json
```

- マシンプロファイルの場合、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork>
\machineprofile.folder\abc.resourcegroup")|select Name, AdditionalData|
ConvertTo-Json
```

マシンカタログを編集する場合は、次の制限事項を考慮してください。

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません。
  - VMサイズを休止状態非対応のものに変更する
  - マシンプロファイルを休止状態非対応のものに変更する
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません。
  - 現在、Web Studioを使用してマシンプロファイルを休止状態対応のものに変更します。

Remote PowerShell SDKを使用してカタログのVMサイズとマシンプロファイルを変更する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/>`を参照してください。

休止状態プロパティの確認

PowerShellコマンドを使用して、マシンカタログ、VM、およびブローカーマシンの休止状態プロパティを確認できます。

- プロビジョニングスキームの休止状態プロパティを確認するには、次のPowerShellコマンドを実行します。`HibernationEnabled`パラメーターは`True`である必要があります。

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).VMMetadata
-join "" |  ConvertFrom-Json | Select HibernationEnabled
```

- プロビジョニングVMの休止状態プロパティを確認するには、次のPowerShellコマンドを実行します。`SupportsHibernation`パラメーターは`True`である必要があります。

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json |
Select SupportsHibernation
```

- ブローカーマシンの休止状態容量を確認するには、次のPowerShellコマンドを実行します。**Suspend** および **Resume** の電源アクションは、休止状態機能を示します。

```
(Get-BrokerMachine -MachineName
<YourMachineName>).SupportedPowerActions
```

休止状態対応VMの電源管理

休止状態対応VMに対して、以下の電源管理操作を実行できます。

- 実行状態のVMを**一時停止**する
- 一時停止状態のVMを**再開**する
- 一時停止状態のVMを**強制シャットダウン**する
- 一時停止状態のVMを**強制再起動**する

詳細については、以下を参照してください。

- 一時停止
- 再開

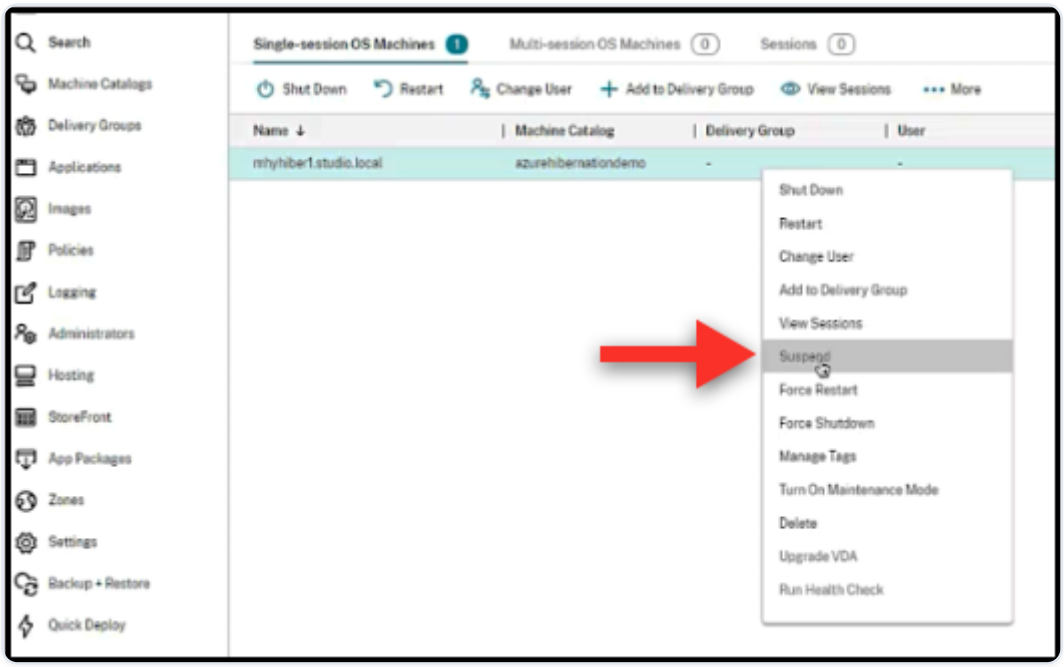
一時停止

VMを一時停止するには、次のいずれかの方法を使用できます。

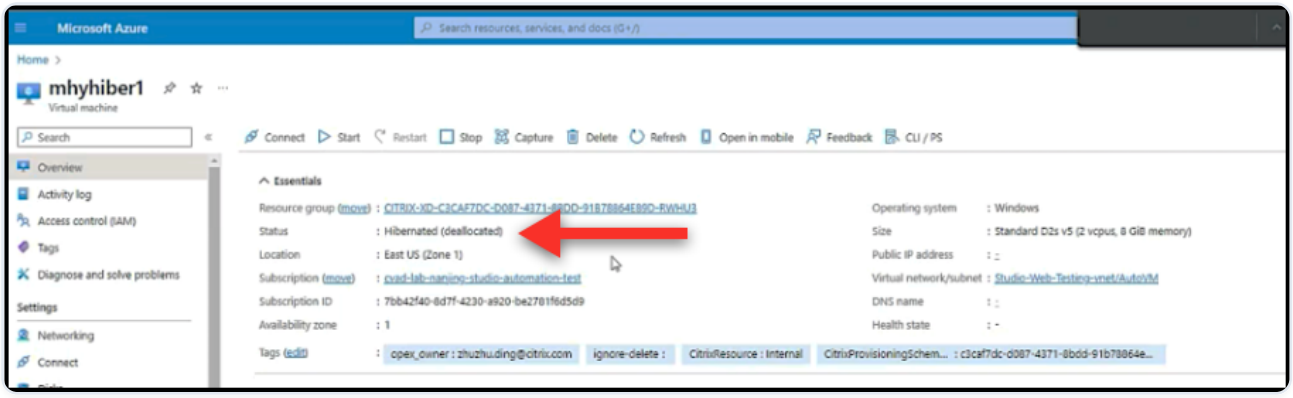
- **手動で** Web Studioを使用する
- **自動的に** タイムアウトポリシーを使用する: 詳細については、その他の設定を参照してください。

VMを手動で一時停止するには:

1. VMを右クリックし、 を選択します。 をクリックしてアクションを確定します。 が から に変わります。



AzureポータルでVMのステータスを確認できます。



再開

休止状態のVMを再開するには、次のいずれかの方法を使用します。

- **手動で：**
  - 管理者はWeb Studioを使用してVMを再開できます。

    Web Studioを使用してVMを再開する(/en-us/citrix-virtual-apps-desktops/2311/media/resume-hibernation-vms.png)
  - エンドユーザーは、デスクトップアイコンをクリックすると、Citrix Workspace™メニューを使用してVMを起動できます。

    Citrix Workspaceを使用してVMを再開する(/en-us/citrix-virtual-apps-desktops/2311/media/resume-vm-workspace.png)
- **自動的に：**

- ピーク時間を正しく設定すると、Autoscale™は休止状態のマシンを自動的に起動できます。タイムスケジュールをクリックすることで、ピーク時間を30分間隔で設定できます。各青いフレームは、ピーク時間としてマークされたタイムスロットを表します。ピーク時間には、連続したタイムスロットと非連続のタイムスロットの両方を含めることができます。
  - 連続したタイムスロット

    連続したピークタイムスロット(/en-us/citrix-virtual-apps-desktops/2311/media/consecutive-peak-time-autoscale.png)
  - 連続しない時間帯

    非連続のピークタイムスロット(/en-us/citrix-virtual-apps-desktops/2311/media/non-consecutive-peak-time-autoscale.png)

> **注:**
>
> **Manage Autoscale > Load-based Settings**で、**Action**が**Suspend**として構成されている場合、そのデリバリーグループ内のすべてのVMが休止機能を備えていることを確認してください。そうでない場合、休止できないVMは実行を継続します。

> Autoscaleの負荷ベース設定を管理する(/en-us/citrix-virtual-apps-desktops/2311/media/azure-hibernation-autoscale.png)

詳細情報

Citrix Azureの休止機能の詳細については、Citrix Tech Zoneの記事を参照してください。

セキュリティポリシー

この記事では、さまざまなサポート対象クラウドサービスにおけるセキュリティ機能について説明します。セキュリティ機能には、次のものが含まれます。

- セキュリティグループ(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/security-policies/security-group.html)
- セキュアブート(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/security-policies/secure-boot.html)

- 暗号化機能(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/security-policies/encryption-capabilities.html)

セキュリティグループ

セキュリティグループは、仮想ネットワーク内のリソース間のネットワークトラフィックをフィルタリングするためのセキュリティルールのグループです。セキュリティルールは、いくつかの種類のリソースへのインバウンドネットワークトラフィック、またはそれからのアウトバウンドネットワークトラフィックを許可または拒否します。各ルールは次のプロパティを指定します。

- 名前: ネットワークセキュリティグループ内の一意の名前
- 優先度: ルールは優先度順に処理されます。数値が小さいほど優先度が高いため、数値が小さいものが数値が大きいものより先に処理されます。
- 送信元または宛先: 任意、または個別のIPアドレス、クラスレスドメイン間ルーティング (CIDR) ブロック (例: 10.0.0.0/24)、サービスタグ、またはアプリケーションセキュリティグループ
- プロトコル: 各セキュリティグループに対してルールを追加する際のプロトコル
- 方向: ルールがインバウンドトラフィックまたはアウトバウンドトラフィックに適用されるかどうか
- ポート範囲: 個別のポートまたはポート範囲を指定できます
- アクション: 許可または拒否

サポートされているハイパーバイザーの詳細については、以下を参照してください。

- AWS のセキュリティグループ
- Microsoft Azure のセキュリティグループ
- Google Cloud Platform のセキュリティグループ

AWS のセキュリティグループ

セキュリティグループは、VPC 内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。これらのセキュリティグループをVPC内の各インスタンスに関連付けることもできます。インバウンドルールはインスタンスへの受信トラフィックを制御し、アウトバウンドルールはインスタンスからの送信トラフィックを制御します。

イメージ準備中のネットワーク設定の詳細については、イメージ準備中のネットワーク設定を参照してください。

インスタンスを起動するときに、1つ以上のセキュリティグループを指定できます。セキュリティグループを構成するには、「セキュリティグループの構成」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-prepare/aws.html#task-2-configure-security-groups)を参照してください。

Microsoft Azure のセキュリティグループ

Citrix Virtual Apps and Desktops は、Azure のネットワークセキュリティグループをサポートしています。ネットワークセキュリティグループは、サブネットに関連付けられることが想定されています。詳細については、ネットワークセキュリティグループを参照してください。

イメージの準備中に作成されるネットワークセキュリティグループの詳細については、「Azure Resource Manager イメージを使用してマシンカタログを作成する」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-machine-catalog-using-an-azure-resource-manager-image-in-web-studio)を参照してください。

Google Cloud Platform のセキュリティグループ

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。この VM は、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する分離された環境で実行する必要があります。これは、すべてのトラフィックを拒否するファイアウォールルールによって実現されます。詳細については、「ファイアウォールルール」(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-create/create-machine-catalog-gcp.html#firewall-rules)を参照してください。

セキュアブートとvTPM

セキュアブートは、システムの起動を担当するUnified Extensible Firmware Interface (UEFI) の機能です。起動プロセス中に信頼できるソフトウェアのみがロードされることを保証します。

トラステッドプラットフォームモジュール (TPM) は、暗号化キーやその他の機密データを安全に保存するためのハードウェアチップです。仮想トラステッドプラットフォームモジュール (vTPM) は、TPM と同じ機能を実行しますが、暗号化コプロセッサ機能をソフトウェアで実行します。TPM はセキュリティを強化できますが、セキュアブートの要件ではありません。

サポートされているクラウドサービスの詳細については、以下を参照してください。

- Google Cloud PlatformでのセキュアブートとvTPM
- Microsoft AzureでのセキュアブートとvTPM

- VMwareでのvTPM

Google Cloud Platformでのセキュアブートとv TPM

Google Cloud Platform (GCP) でシールドされた仮想マシンをプロビジョニングできます。シールドされたVMの検証可能な整合性は、次の機能を使用して実現されます。

- セキュアブート
- vTPM対応メジャーブート
- 整合性監視

PowerShellを使用してシールドされたVMでカタログを作成する方法の詳細については、PowerShellを使用してシールドされたVMでカタログを作成するを参照してください。

Microsoft Azureでのセキュアブートとv TPM

Azure環境では、Trusted Launchが有効なマシンカタログを作成できます。Azureは、第2世代VMのセキュリティを向上させるシームレスな方法としてTrusted Launchを提供します。Trusted Launchは、高度で永続的な攻撃手法から保護します。Trusted Launchを有効にするには、マシンプロファイルベースのカタログ構成を使用します。Trusted Launchの根幹には、VMのセキュアブートがあります。Trusted Launchは、クラウドによるリモートアテステーションを実行するためにvTPMも使用します。これは、プラットフォームのヘルスチェックと信頼に基づく意思決定に使用されます。セキュアブートとvTPMは個別に有効にできます。Trusted Launchでマシンカタログを作成する方法の詳細については、Trusted Launchでのマシンカタログを参照してください。

VMware における vTPM

MCS は vTPM を使用したマシンカタログの作成をサポートしています。マスターイメージに Windows 11 がインストールされている場合、マスターイメージで vTPM を有効にすることが要件となります。マシンプロファイルベースの構成が使用され、vTPM が有効になっている場合、カタログ内の VM は VM テンプレートから同じ vTPM コンテンツを継承します。マシンプロファイルが使用されておらず、マスターイメージで vTPM が有効になっている場合、カタログ内の VM は空の vTPM を持ちます。詳細については、「マシンプロファイルを使用したマシンカタログの作成」を参照してください。

暗号化機能

暗号化機能は、共有仮想マシンホスト上の悪意のあるゲストによる攻撃や、ホスト上のすべての仮想マシンを管理するハイパーバイザー制御ソフトウェアによる攻撃から、仮想マシンのコンテンツを保護します。

サポートされているクラウドサービスの詳細については、以下を参照してください。

- AWS の暗号化機能
- Google Cloud Platform の暗号化機能
- Microsoft Azure の暗号化機能

AWS の暗号化機能

このセクションでは、AWS 仮想化環境における暗号化機能について説明します。

自動暗号化

アカウントで作成された新しい Amazon EBS ボリュームとスナップショットコピーの自動暗号化を有効にできます。詳細については、「自動暗号化」を参照してください。

Google Cloud Platform の暗号化機能

このセクションでは、Google Cloud Platform (GCP) 仮想化環境における暗号化機能について説明します。

Google マネージド暗号化キーで許可されているよりもキー操作を詳細に制御する必要がある場合は、顧客管理の暗号化キーを使用できます。顧客管理の暗号化キーを使用する場合、オブジェクトがバケットに保存されるときに Cloud Storage によってキーで暗号化され、リクエスターに提供されるときに Cloud Storage によって自動的に復号化されます。詳細については、「顧客管理の暗号化キー」を参照してください。

MCS カタログに顧客管理の暗号化キー (CMEK) を使用できます。詳細については、「顧客管理の暗号化キー (CMEK) の使用」を参照してください。

Microsoft Azure の暗号化機能

このセクションでは、Azure仮想化環境における暗号化機能について説明します。

Azureサーバー側暗号化

ほとんどのAzureマネージドディスクは、Azure Storage暗号化によって暗号化されます。これは、サーバー側暗号化（SSE）を使用してデータを保護し、セキュリティとコンプライアンスのコミットメントを満たすのに役立ちます。Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介したAzureマネージドディスクの顧客管理暗号化キーをサポートしています。詳細については、「Azureサーバー側暗号化」を参照してください。

ホストでのAzureディスク暗号化

ホストでの暗号化機能を持つMCSマシンカタログを作成できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

ホストでの暗号化機能を持つMCSマシンカタログの作成の詳細については、「ホストでのAzureディスク暗号化」を参照してください。

Azure二重暗号化

二重暗号化は、プラットフォーム側暗号化（デフォルト）と顧客管理暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念するセキュリティ意識の高いお客様は、この二重暗号化を選択できます。永続的なOSディスクとデータディスク、スナップショット、およびイメージはすべて、二重暗号化によって保存時に暗号化されます。詳細については、「マネージドディスクの二重暗号化」を参照してください。

Azure機密VM

Azure機密コンピューティングVMは、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCSを使用して、Azure機密VMを含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。マシンプロファイルの入力として、VMとARMテンプレート仕様の両方を使用できます。

詳細については、「Azure機密VM」を参照してください。

デリバリーグループの作成

> **注:**
>
> Citrix Virtual Apps and Desktops™の展開は、Web Studio (Webベース) とCitrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> デリバリーグループは、1つ以上のマシンカタログから選択されたマシンのコレクションです。デリバリーグループは、どのユーザーがそれらのマシンを使用できるか、およびそれらのユーザーが利用できるアプリケーションとデスクトップを指定します。

デリバリーグループの作成は、サイトの作成とマシンカタログの作成の後に、展開を構成する次のステップです。後で、最初のデリバリーグループの初期設定を変更したり、他のデリバリーグループを作成したりできます。デリバリーグループの作成時ではなく、編集時にのみ構成できる機能と設定もあります。

Remote PC Accessの場合、サイトを作成すると、「Remote PC Access Desktops」という名前のデリバリーグループが自動的に作成されます。

デリバリーグループを作成するには：

1. サイトとマシンカタログを作成したが、デリバリーグループを作成していない場合、Web Studioは、デリバリーグループを作成するための適切な開始場所に案内します。
2. すでにデリバリーグループを作成しており、別のデリバリーグループを作成したい場合は、次の手順に従ってください:

    a. **デリバリーグループ**を選択します。アクションペインで**デリバリーグループの作成**を選択します。

    b. フォルダーを使用してデリバリーグループを整理するには、デフォルトの**デリバリーグループ**フォルダーの下にフォルダーを作成します。詳しくは、「フォルダーの作成」を参照してください。

    c. グループを作成するフォルダーを選択し、**デリバリーグループの作成**をクリックします。グループ作成ウィザードが開きます。

3. ウィザードは**はじめに**ページから起動します。このページは、今後のウィザード起動時に表示しないように設定できます。
4. ウィザードは、次のセクションで説明されているページを順に案内します。各ページの作業が完了したら、最後のページに到達するまで**次へ**をクリックします。

ステップ1. マシン

Machinesページで、カタログを選択し、そのカタログから使用するマシンの数を選択します。

知っておくと良いこと:

- 選択したカタログには、少なくとも1台の未使用のマシンが残っている必要があります。
- カタログは複数のデリバリーグループで指定できます。マシンは1つのデリバリーグループでのみ使用できます。
- デリバリーグループは複数のカタログのマシンを使用できますが、それらのカタログには同じマシンタイプ（マルチセッションOS、シングルセッションOS、またはRemote PC Access）が含まれている必要があります。つまり、デリバリーグループ内でマシンタイプを混在させる

ことはできません。同様に、展開にWindowsマシンのカタログとLinuxマシンのカタログがある場合、デリバリーグループにはどちらかのOSタイプのマシンを含めることができますが、両方を含めることはできません。

- Citrixでは、すべてのマシンに最新のVDAバージョンをインストールまたはアップグレードすることを推奨しています。必要に応じて、カタログとデリバリーグループをアップグレードしてください。デリバリーグループを作成する際に、異なるVDAバージョンがインストールされているマシンを選択した場合、デリバリーグループは最も古いVDAバージョンと互換性があります。これはグループの*機能レベル*と呼ばれます。たとえば、マシンの1つがVDAバージョン7.1で、他のマシンが現在のバージョンである場合、グループ内のすべてのマシンはVDA 7.1でサポートされていた機能のみを使用できます。これは、より新しいVDAバージョンを必要とする一部の機能が、そのデリバリーグループでは利用できない可能性があることを意味します。
- Remote PC Accessカタログの各マシンは、自動的にデリバリーグループに関連付けられます。Remote PC Accessサイトを作成すると、「Remote PC Access Machines」というカタログと「Remote PC Access Desktops」というデリバリーグループが自動的に作成されます。
- 以下の互換性チェックが実行されます。
  - MinimumFunctionalLevelが互換性があること
  - SessionSupportが互換性があること
  - AllocationTypeがSingleSessionと互換性があること
  - ProvisioningTypeが互換性があること
  - PersistChangesがMCSおよびCitrix Provisioning™と互換性があること
  - RemotePCカタログはRemote PC Accessカタログとのみ互換性があること
  - AppDisk関連のチェック

ステップ 2. ロードバランシング

デリバリーグループの作成中にロードバランシング設定を構成するには：

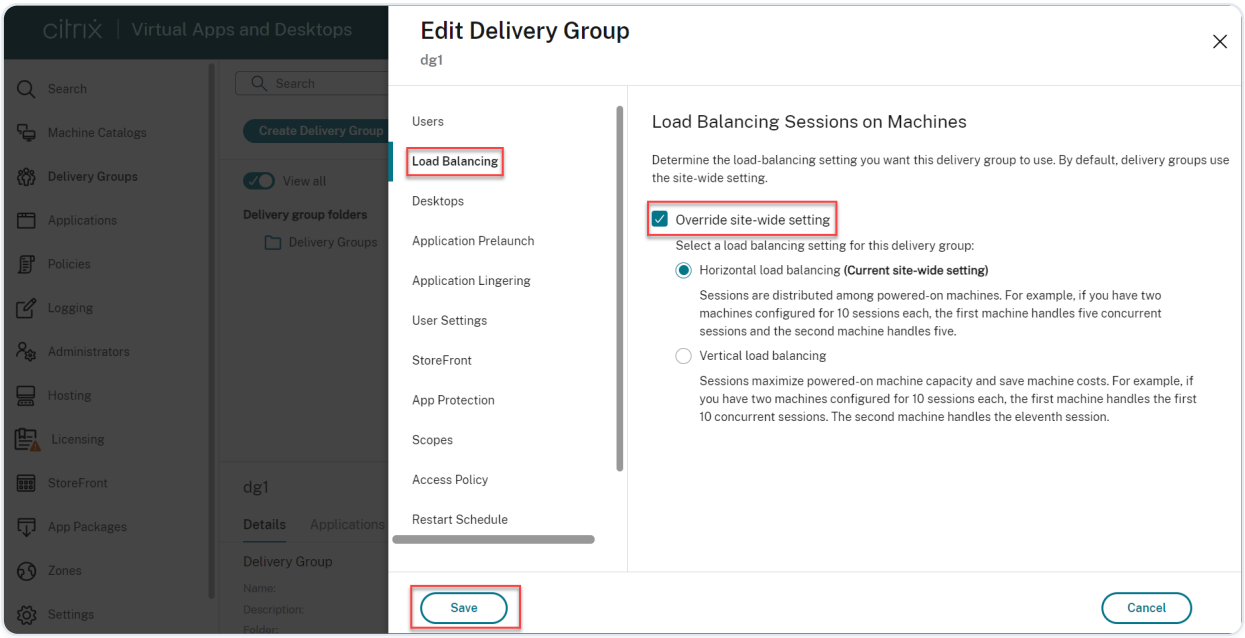
1. Web Studioにサインインします。
2. 左側のナビゲーションで、**Delivery Groups**をクリックします。
3. **Delivery Groups**ページで、**Create Delivery Group**をクリックします。
4. **Create Delivery Group**ウィザードで、**次へ**をクリックします。**Machine**ウィザードが開きます。
5. **Machines**ウィザードで、必要なマシンカタログを選択し、**次へ**をクリックします。**Load Balancing**ウィザードが開きます。

6. **Load Balancing**ウィザードで、**Override site-wide setting**チェックボックスを選択します。
7. 必要に応じて、**Horizontal load balancing**または**Vertical load balancing**オプションを選択し、**次へ**をクリックします。

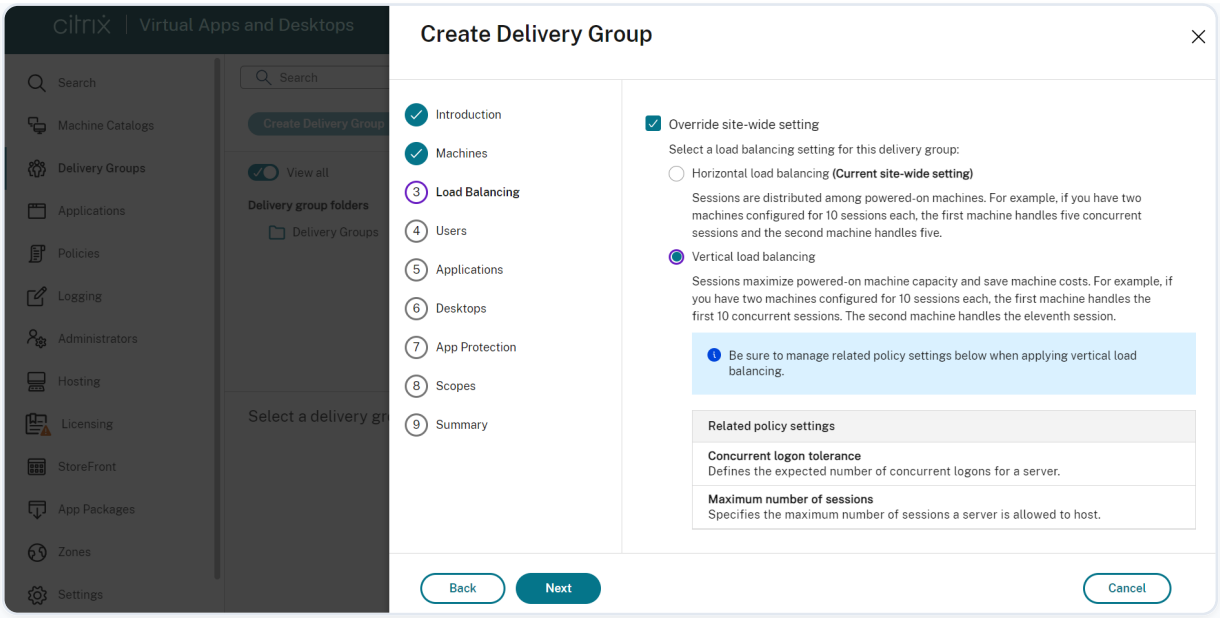
   デリバリーグループ作成中の負荷分散設定(/en-us/citrix-virtual-apps-desktops/2311/media/load-balance-create-delivery-group.png)

既存のデリバリーグループを編集中にロードバランシング設定を構成するには：

1. Web Studioにサインインします。
2. 左側のナビゲーションで、**Delivery Groups**をクリックします。
3. リストから**Delivery Group**を選択し、**編集**をクリックします。**Edit Delivery Group**ウィザードが開きます。
4. **Edit Delivery Group**ページで、**Load Balancing**をクリックします。
5. **サイト全体の詳細設定を上書き**チェックボックスをオンにします。
6. 必要に応じて、**水平負荷分散**または**垂直負荷分散**オプションを選択し、**保存**をクリックします。



> **注:**
>
> 垂直負荷分散設定が適用されている場合、**同時ログオン許容数**および**最大セッション数**ポリシーが適切に構成されていることを確認してください。



サイトおよびデリバリーグループレベルでの負荷分散の詳細については、「マシンの負荷分散」を参照してください。

ステップ3. 配信の種類

このページは、静的（割り当て済み）シングルセッションOSマシンを含むカタログを選択した場合にのみ表示されます。

配信の種類ページで、**アプリケーション**または**デスクトップ**のいずれかを選択します。両方を有効にすることはできません。

マルチセッションOSまたはシングルセッションOSのランダム（プールされた）カタログからマシンを選択した場合、配信の種類はアプリケーションとデスクトップであると見なされます。アプリケーション、デスクトップ、またはその両方を配信できます。

ステップ4. ユーザー

デリバリーグループ内のアプリケーションとデスクトップを使用できるユーザーとユーザーグループを指定します。

ユーザーリストの指定場所

Active Directory ユーザーリストは、以下を作成または編集する際に指定されます。

- Web Studio を介して構成されないサイトのユーザーアクセスリスト。デフォルトでは、アプリケーションエンタイトルメントポリシーのルールには全員が含まれます。詳細については、PowerShell SDK の `BrokerAppEntitlementPolicyRule` コマンドレットを参照してください。

- アプリケーショングループ (構成されている場合)。
- デリバリーグループ。
- アプリケーション。

StoreFront™ を介してアプリケーションにアクセスできるユーザーのリストは、上記のユーザーリストの共通部分によって形成されます。たとえば、他のグループへのアクセスを不当に制限することなく、特定の部門にアプリケーションAの使用を構成するには、次の手順を実行します。

- 全員を含むデフォルトのアプリケーションエンタイトルメントポリシーのルールを使用します。
- デリバリーグループのユーザーリストを構成して、すべての本社ユーザーがデリバリーグループで指定された任意のアプリケーションを使用できるようにします。
- (アプリケーショングループが構成されている場合) アプリケーショングループのユーザーリストを構成して、管理および財務ビジネスユニットのメンバーがアプリケーションAからLにアクセスできるようにします。
- アプリケーションAのプロパティを構成して、その可視性を管理および財務部門の売掛金担当者のみに制限します。

認証済みユーザーと未認証ユーザー

ユーザーには、認証済みと未認証 (未認証は匿名とも呼ばれます) の2種類があります。デリバリーグループでは、いずれか一方または両方のタイプを構成できます。

- **認証済み:** アプリケーションとデスクトップにアクセスするには、名前で指定したユーザーとグループメンバーが、スマートカードやユーザー名とパスワードなどの資格情報をStoreFrontまたはCitrix Workspace™アプリに提示する必要があります。シングルセッションOSマシンを含むデリバリーグループの場合、デリバリーグループを編集することで、後でユーザーデータ (ユーザーのリスト) をインポートできます。
- **未認証 (匿名):** マルチセッションOSマシンを含むデリバリーグループの場合、ユーザーはStoreFrontまたはCitrix Workspaceアプリに資格情報を提示することなく、アプリケーションとデスクトップにアクセスできます。たとえば、キオスクではアプリケーションに資格情報が必要な場合がありますが、Citrixアクセス ポータルとツールは必要ありません。最初のDelivery Controllerをインストールすると、匿名ユーザーグループが作成されます。

  未認証ユーザーにアクセスを許可するには、デリバリーグループ内の各マシンにWindows Server OS用VDA (最小バージョン7.6) がインストールされている必要があります。未認証ユーザーが有効になっている場合、未認証のStoreFrontストアが必要です。

未認証ユーザーアカウントは、セッションが起動されたときにオンデマンドで作成され、Anon*XYZ*という名前が付けられます。ここで、*XYZ*は一意の3桁の値です。

認証されていないユーザーセッションには、デフォルトで10分間のアイドルタイムアウトがあり、クライアントが切断されると自動的にログオフされます。再接続、クライアント間のローミング、およびWorkspace Controlはサポートされていません。

次の表は、**ユーザー**ページでの選択肢について説明しています。

アクセスを有効にする	ユーザーとユーザーグループを追加/割り当てますか？	「認証されていないユーザーにアクセスを許可する」チェックボックスを有効にしますか？
認証済みユーザーのみ	はい	いいえ
認証されていないユーザーのみ	いいえ	はい
認証済みユーザーと未認証ユーザーの両方	はい	はい

ステップ5. アプリケーション

知っておくと良いこと：

- Remote PC Accessデリバリーグループにはアプリケーションを追加できません。
- デフォルトでは、追加する新しいアプリケーションはApplicationsという名前のフォルダーに配置されます。別のフォルダーを指定することもできます。詳しくは、「アプリケーションの管理」の記事を参照してください。
- アプリケーションのプロパティは、デリバリーグループに追加するとき、または後で変更できます。詳しくは、「アプリケーションの管理」の記事を参照してください。
- アプリケーションを追加しようとしたときに、同じ名前のアプリケーションがそのフォルダーに存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。拒否した場合、アプリケーションはそのアプリケーションフォルダー内で一意になるようにサフィックスが付けられて追加されます。
- アプリケーションを複数のデリバリーグループに追加する場合、それらすべてのデリバリーグループでアプリケーションを表示するのに十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのデリバリーグループを含むようにスコープを拡張してください。

- 同じ名前のアプリケーションを同じユーザーに2つ公開する場合、Web Studioで「Application name (for user)」プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にすることになります。

アプリケーションソースを表示するには、**［追加］** をクリックします。

- **［スタートメニューから］**：選択したカタログのマスターイメージから作成されたマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションを選択し、**［OK］** をクリックします。
- **［手動］**：デリバリーグループ内のVDA、またはネットワーク上の別の場所にあるアプリケーション。このソースを選択すると、新しいページが開き、次の方法で追加するアプリケーションを指定できます。
  - 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
  - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、**［参照］** をクリックし、VDAにアクセスするための資格情報を入力し、VDAへの接続が確立されるまで待ってから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページのフィールドに自動的に入力されます。
- **［既存］**：以前にサイトに追加されたアプリケーション（別のデリバリーグループにある可能性もあります）。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。アプリケーションを追加し、**［OK］** をクリックします。
- **［アプリケーションパッケージ］**：App-V、MSIX、MSIX app attach、またはFlexAppアプリケーションパッケージ内のアプリケーション。このソースを選択すると、**［パッケージからアプリケーションを追加］** ページが起動します。アプリケーションパッケージソースを選択し、表示された結果から追加するアプリケーションを選択して、**［OK］** を選択します。詳しくは、「アプリパッケージの展開と配信」を参照してください。

アプリケーションソースまたはアプリケーションが利用できないか無効な場合、表示されないか、選択できません。たとえば、サイトにアプリケーションが追加されていない場合、**［既存］** ソースは利用できません。または、アプリケーションが選択したカタログ内のマシンのサポートされているセッションタイプと互換性がない場合があります。

ステップ 6. デスクトップ

このページのタイトルは、**マシン**ページで選択したカタログによって異なります。

- プールされたマシンを含むカタログを選択した場合、このページは**デスクトップ**というタイトルになります。
- 割り当てられたマシンを含むカタログを選択し、**配信の種類**ページで「デスクトップ」を指定した場合、このページは**デスクトップユーザーの割り当て**というタイトルになります。
- 割り当てられたマシンを含むカタログを選択し、**配信の種類**ページで「アプリケーション」を指定した場合、このページは**アプリケーションマシンのユーザー割り当て**というタイトルになります。

追加をクリックします。ダイアログボックスで:

- 表示名と説明のフィールドに、Citrix Workspaceアプリに表示する情報を入力します。
- デスクトップにタグ制限を追加するには、**このタグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。詳細については、タグを参照してください。
- ラジオボタンを使用して、デスクトップを起動するか、デスクトップの起動時にマシンを割り当てます。ユーザーは、このデリバリーグループにアクセスできるすべてのユーザー、または特定のユーザーとユーザーグループのいずれかです。
- グループに割り当てられたマシンが含まれている場合は、ユーザーあたりのデスクトップの最大数を指定します。これは1以上の値である必要があります。
- デスクトップ（プールされたマシン用）またはデスクトップ割り当てルール（割り当てられたマシン用）を有効または無効にします。デスクトップを無効にすると、デスクトップの配信が停止します。デスクトップ割り当てルールを無効にすると、ユーザーへのデスクトップの自動割り当てが停止します。
- ダイアログボックスでの作業が完了したら、「**OK**」をクリックします。

サイト内のデスクトップの最大インスタンス数（PowerShellのみ）

サイト内のデスクトップの最大インスタンス数を構成するには（PowerShellのみ）:

- PowerShellで、適切なBrokerEntitlementPolicyRuleコマンドレットをMaxPerEntitlementInstancesパラメーターとともに使用します。たとえば、次のコマンドレットは`tsvda-desktop`ルールを変更して、サイトで許可されるデスクトップの最大同時インスタンス数を2に設定します。2つのデスクトップインスタンスが実行されているときに、3番目のサブスクライバーがデスクトップを起動しようとすると、エラーが発生します。

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop
  -MaxPerEntitlementInstances 2
  ```

- ガイダンスについては、Get-Help コマンドレットを使用してください。たとえば、`Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`。

手順7. 概要

デリバリーグループの名前を入力します。説明を任意で入力することもできます。この説明は、Citrix Workspace アプリと Web Studio に表示されます。

概要情報を確認し、**「完了」**をクリックします。

デリバリーグループの管理

> **注:**
>
> Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

この記事では、管理コンソールからデリバリーグループを管理する手順について説明します。グループ作成時に指定した設定を変更するだけでなく、デリバリーグループの作成時には利用できないその他の設定も構成できます。

手順のカテゴリには、一般、ユーザー、マシン、セッションが含まれます。一部のタスクは複数のカテゴリにまたがります。たとえば、「ユーザーがマシンに接続できないようにする」はマシンのカテゴリで説明されていますが、ユーザーにも影響します。あるカテゴリでタスクが見つからない場合は、関連するカテゴリを確認してください。

その他の関連情報を含む記事：

- アプリケーションには、デリバリーグループ内のアプリケーションの管理に関する情報が含まれています。
- デリバリーグループの管理には、Delivery Group Administratorの組み込みロール権限が必要です。詳細については、委任管理を参照してください。

全般

- デリバリーの種類を変更する
- StoreFront™アドレスを変更する
- 機能レベルを変更する
- Remote PC Accessデリバリーグループを管理する
- フォルダーを使用してデリバリーグループを整理する
- 「アプリ保護の管理」(#manage-app-protection)

デリバリーグループのデリバリーの種類を変更する

デリバリーの種類は、グループが提供できるもの（アプリケーション、デスクトップ、またはその両方）を示します。

アプリケーションのみまたは**デスクトップとアプリケーション**のタイプを**デスクトップのみ**のタイプに変更する前に、グループからすべてのアプリケーションを削除してください。

1. 左側のペインで、**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. ページで、目的のデリバリーの種類を選択します。
4. **［適用］をクリックして変更を適用し、ウィンドウを開いたままにします。または、［保存］**をクリックして変更を適用し、ウィンドウを閉じます。

StoreFrontアドレスを変更する

1. 左側のペインで、**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **［StoreFront］**ページで、StoreFrontのURLを選択または追加します。これらのURLは、デリバリーグループ内の各マシンにインストールされているCitrix Workspace™アプリによって使用されます。
4. **［適用］をクリックして変更を適用し、ウィンドウを開いたままにします。または、［保存］**をクリックして変更を適用し、ウィンドウを閉じます。

左側のペインで**［StoreFront］**を選択して、StoreFrontサーバーアドレスを指定することもできます。

機能レベルを変更する

デリバリーグループの機能レベルは、そのマシン上のVDAと、デリバリーグループで使用されるマシンを含むマシンカタログをアップグレードした後に変更します。

開始する前に:

- Citrix Provisioning™ (旧Provisioning Services) を使用している場合は、Citrix Provisioningコンソールで VDAバージョンをアップグレードします。
- アップグレードされたVDAを含むマシンを起動し、Delivery Controllerに登録できるようにします。このプロセスにより、デリバリーグループでアップグレードが必要なものがコンソールに通知されます。
- 以前のVDAバージョンを引き続き使用する必要がある場合、新しい製品機能は利用できません。詳細については、アップグレードドキュメントを参照してください。

デリバリーグループの機能レベルを変更するには:

1. 左ペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。 アクションは、アップグレードされたVDAが検出された場合にのみ表示されます。
3. をクリックします。

表示には、機能レベルに変更できないマシンがある場合、そのマシンと理由が示されます。その後、変更アクションをキャンセルし、マシンの問題を解決してから、変更アクションを再度実行できます。

変更が完了したら、マシンを以前の状態に戻すことができます。デリバリーグループを選択し、アクションバーで を選択します。

Remote PC Accessデリバリーグループの管理

Remote PC Accessマシンカタログ内のマシンが割り当てられていない場合、そのマシンは一時的にそのカタログに関連付けられたデリバリーグループに割り当てられます。この一時的な割り当てにより、後でマシンをユーザーに割り当てることができます。

デリバリーグループとマシンカタログの関連付けには優先度値があります。優先度は、マシンがシステムに登録されるとき、またはユーザーがマシン割り当てを必要とするときに、マシンに割り当てられるデリバリーグループを決定します。値が低いほど優先度が高くなります。Remote PC Accessマシンカタログに複数のデリバリーグループ割り当てがある場合、ソフトウェアは最も優先度の高い一致を選択します。この優先度値を設定するには、PowerShell SDKを使用します。

Remote PC Accessマシンカタログは、最初に作成されたときにデリバリーグループに関連付けられます。後でカタログに追加されたマシンアカウントまたは組織単位は、デリバリーグループに追加できます。この関連付けは、オンまたはオフに切り替えることができます。

Remote PC Accessマシンカタログとデリバリーグループの関連付けを追加または削除するには：

1. 左側のペインで**デリバリーグループ**を選択します。
2. Remote PC Accessグループを選択します。
3. **詳細**セクションで、**マシンカタログ**タブをクリックし、Remote PC Accessカタログを選択します。
4. 関連付けを追加または復元するには、**デスクトップの追加**をクリックします。関連付けを削除するには、**関連付けの削除**をクリックします。

フォルダーを使用したデリバリーグループの整理

デリバリーグループに簡単にアクセスできるように、フォルダーを作成できます。

必要な役割

デフォルトでは、デリバリーグループフォルダーを作成および管理するには、Cloud Administrator、Full Administrator、またはDelivery Group Administratorの組み込み役割が必要です。必要に応じて、デリバリーグループフォルダーを作成および管理するための役割をカスタマイズできます。詳細については、「必要な権限」を参照してください。

デリバリーグループフォルダーを作成する

開始する前に、デリバリーグループをどのように整理するか計画してください。次の点を考慮してください。

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、デリバリーグループとサブフォルダーを含めることができます。
- すべてのノード（**Machine Catalogs**、**Applications**、**Delivery groups**ノードなど）は、バックエンドでフォルダーツリーを共有します。フォルダーの名前変更または移動時に他のノードとの名前の競合を避けるため、異なるノードの第一レベルフォルダーには異なる名前を付けることをお勧めします。

デリバリーグループフォルダーを作成するには、次の手順に従います。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダー階層でフォルダーを選択し、**アクション**バーで **Create Folder** を選択します。
3. 新しいフォルダーの名前を入力し、**Done** をクリックします。

> **ヒント:**
>
> 意図しない場所にフォルダーを作成してしまった場合は、正しい場所にドラッグできます。

デリバリーグループを移動する

デリバリーグループはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダーごとにグループを表示します。フォルダー階層の上にある**すべて表示**をオンにして、すべてのグループを一度に表示することもできます。
3. グループを右クリックし、**Move Delivery Group** を選択します。
4. グループを移動するフォルダーを選択し、**Done** をクリックします。

> **ヒント:**
>
> グループをフォルダーにドラッグできます。

デリバリーグループフォルダーの管理

デリバリーグループフォルダーの削除、名前の変更、移動ができます。

フォルダーとそのサブフォルダーにデリバリーグループが含まれていない場合にのみ、フォルダーを削除できることに注意してください。

フォルダーを管理するには、次の手順に従います。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて**アクション**バーでアクションを選択します。
   - フォルダーの名前を変更するには、**Rename Folder**を選択します。
   - フォルダーを削除するには、**Delete Folder**を選択します。
   - フォルダーを移動するには、**Move Folder**を選択します。
3. 画面の指示に従って、残りの手順を完了してください。

必要な権限

次の表に、デリバリーグループフォルダーに対してアクションを実行するために必要な権限を示します。

アクション	必要な権限
デリバリーグループフォルダの作成	デリバリーグループフォルダの作成
デリバリーグループフォルダの削除	デリバリーグループフォルダーの削除
デリバリーグループフォルダーの移動	デリバリーグループフォルダーの移動
デリバリーグループフォルダーの名前変更	デリバリーグループフォルダーの編集
デリバリーグループをフォルダーに移動	デリバリーグループフォルダーの編集とデリバリーグループプロパティの編集

アプリ保護の管理

以下の情報は、アプリ保護 を補足するものです。以下の詳細に注意してください。

- 有効なアプリ保護の資格が必要です。アプリ保護機能を購入するには、Citrix の営業担当者にお問い合わせください。
- アプリ保護には XML 信頼が必要です。XML 信頼を有効にするには、**［設定］>［XML 信頼を有効にする］** に移動します。
- 画面キャプチャ防止について：
  - Windows および macOS では、保護されたコンテンツのウィンドウのみが空白になります。保護されたウィンドウが最小化されていない場合、アプリ保護はアクティブになります。
  - Linux では、キャプチャ全体が空白になります。保護されたウィンドウが最小化されているかどうかにかかわらず、アプリ保護はアクティブになります。

デリバリーグループのアプリ保護方法を選択するには、次の手順に従います。

1. 左側のペインで **デリバリーグループ** を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. **アプリ保護**ページで、**キーロギング対策**および**画面キャプチャ対策**を有効にできます。

ユーザー

- ユーザー設定の変更
- ユーザーの追加または削除

デリバリーグループでユーザー設定を変更する

このページの名前は、**ユーザー設定**または**基本設定**として表示されます。

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **ユーザー設定**（または**基本設定**）ページで、次の表の設定を変更します。
4. **適用**をクリックして行った変更を適用し、ウィンドウを開いたままにします。または、**保存**をクリックして変更を適用し、ウィンドウを閉じます。

設定	説明
説明	Citrix Workspace（またはStoreFront）が使用し、ユーザーに表示されるテキスト。
デリバリーグループを有効にする	デリバリーグループが有効になっているかどうか。
タイムゾーン	このデリバリーグループのマシンが存在する必要があるタイムゾーン。このオプションには、サイトでサポートされているタイムゾーンが一覧表示されます。**注：**デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動する場合があります。これを回避するには、稼働時間外にタイムゾーン設定を変更してください。
Secure ICA® を有効にする	ICAプロトコルを暗号化するSecureICAを使用して、デリバリーグループ内のマシンとの間の通信を保護します。デフォルトのレベルは128ビットです。このレベルはSDKを使用して変更できます。Citrixは、パブリックネットワークを介して通信する場合、TLS暗号化などのより強力な暗号化方法を使用することを推奨します。また、SecureICAはデータ整合性をチェックしません。

デリバリーグループでのユーザーの追加または削除

ユーザーの詳細については、「ユーザー」を参照してください。

1. 左ペインで**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーで**［編集］**をクリックします。
3. **［ユーザー］**ページで：
   - ユーザーを追加するには、**［追加］**をクリックし、追加するユーザーを指定します。
   - ユーザーを削除するには、1人以上のユーザーを選択し、**［削除］**をクリックします。
   - 認証されていないユーザーによるアクセスを許可するには、チェックボックスをオンまたはオフにします。
4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

ユーザーリストのインポートまたはエクスポート

物理的なシングルセッションOSマシンを含むデリバリーグループの場合、デリバリーグループの作成後に.csvファイルからユーザー情報をインポートできます。ユーザー情報を.csvファイルにエクスポートすることもできます。.csvファイルには、以前の製品バージョンのデータを含めることができます。

CSVファイルの最初の行には、コンマで区切られた2つの列ヘッダーが含まれている必要があります。最初のヘッダーが `Machine Account` で、2番目のヘッダーが `User Names` であることを確認してください。（追加のヘッダーを含めることはできますが、サポートされていません。）ファイルの以降の行には、コンマ区切りのデータが含まれます。`Machine Account` エントリは、コンピューターSID、FQDN、またはドメインとコンピューター名のペアにすることができます。

ユーザー情報をインポートまたはエクスポートするには：

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **マシン割り当て**ページで、**リストのインポート**または**リストのエクスポート**を選択し、ファイルの場所を参照します。
4. 「**適用**」をクリックして変更を適用し、ウィンドウを開いたままにします。または、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

マシン

- マシンからユーザーへの割り当てを変更する
- ユーザーあたりの最大マシン数を変更する
- マシンを更新する
- デスクトップのタグ制限を追加、変更、または削除する
- マシンを削除する
- マシンへのアクセスを制限する
- ユーザーがマシンに接続できないようにする（メンテナンスモード）
- マシンをシャットダウンして再起動する
- マシンの再起動スケジュールを作成および管理する
- 1回限りの再起動スケジュールを有効にする
- 管理対象マシンをロードする
- 管理対象マシンの電源を管理する

デリバリーグループ内のマシンからユーザーへの割り当てを変更する

MCSでプロビジョニングされたシングルセッションOSマシンの割り当てを変更できます。マルチセッションOSマシンまたはCitrix Provisioningでプロビジョニングされたマシンの割り当ては変更できません。

1. 左側のペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. または ページ（ページタイトルはデリバリーグループが使用するマシンカタログの種類によって異なります）で、新しいユーザーを指定します。
4. をクリックして変更を適用し、ウィンドウを開いたままにします。または、 をクリックして変更を適用し、ウィンドウを閉じます。

デリバリーグループ内のユーザーあたりの最大マシン数を変更する

1. 左側のペインで を選択します。
2. グループを選択し、アクションバーの**編集**をクリックします。
3. **デスクトップ割り当てルール**ページで、ユーザーあたりの最大デスクトップ数を設定します。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

デリバリーグループ内のマシンを更新する

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーの**マシンの表示**をクリックします。
3. マシンを選択し、アクションバーの**マシンの更新**をクリックします。

別のイメージを選択するには、**マスターイメージ**を選択し、次にスナップショットを選択します。

変更を適用してマシンユーザーに通知するには、**エンドユーザーへのロールアウト通知**を選択します。次に、以下を指定します。

- マスターイメージを更新するタイミング: 今すぐ、または次回の再起動時
- 再起動の配布時間（グループ内のすべてのマシンの更新を開始するまでの合計時間）
- ユーザーに再起動が通知されるかどうか
- ユーザーが受信するメッセージ

デスクトップのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、起動対象となるデスクトップに予期せぬ影響を与える可能性があります。「タグ」の考慮事項と注意点を確認してください。

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **デスクトップ**ページで、デスクトップを選択し、**編集**をクリックします。
4. タグ制限を追加するには、**タグを持つマシンへの起動を制限**を選択し、タグを選択します。
5. タグ制限を変更または削除するには、次のいずれかの操作を行います。
    - 別のタグを選択します。
    - **このタグを持つマシンへの起動を制限**の選択を解除して、タグ制限を削除します。
6. **適用**をクリックして変更を適用し、ウィンドウを開いたままにします。または、**保存**をクリックして変更を適用し、ウィンドウを閉じます。

デリバリーグループからマシンを削除する

マシンを削除すると、デリバリーグループから削除されます。ただし、デリバリーグループが使用するマシンカタログからは削除されません。そのため、そのマシンは別のデリバリーグループに割り当てることができます。

マシンは、削除する前にシャットダウンする必要があります。マシンを削除している間、ユーザーがマシンに接続するのを一時的に停止するには、シャットダウンする前にマシンをメンテナンスモードにします。

マシンには個人データが含まれている可能性があるため、別のユーザーにマシンを割り当てる前に注意してください。マシンの再イメージングを検討してください。

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**マシンの表示**をクリックします。
3. マシンがシャットダウンされていることを確認します。
4. マシンを選択し、アクションバーで**デリバリーグループから削除**をクリックします。

マシンが使用する接続を介して、デリバリーグループからマシンを削除することもできます。

デリバリーグループ内のマシンへのアクセスを制限する

デリバリーグループ内のマシンへのアクセスを制限するために行った変更は、使用する方法に関係なく、以前の設定に優先します。次のことができます。

- **委任管理スコープを使用して管理者へのアクセスを制限する：** 管理者がすべてのアプリケーションにアクセスできるようにするスコープと、特定のアプリケーションのみにアクセスできるようにする別のスコープを作成して割り当てます。詳細については、「委任管理」を参照してください。
- **SmartAccessポリシー式を使用してユーザーへのアクセスを制限する：** ポリシー式を使用して、Citrix Gatewayを介して行われるユーザー接続をフィルタリングします。

  a. 左ペインで**「デリバリーグループ」**を選択します。

  b. グループを選択し、アクションバーの**「編集」**をクリックします。

  c. **「アクセスポリシー」ページで、「NetScaler® Gateway経由の接続」**を選択します。

  d. これらの接続のサブセットを選択するには、**「次のいずれかのフィルターに一致する接続」**を選択します。次に、Citrix Gatewayサイトを定義し、許可されたユーザーアクセスシナリオのSmartAccessポリシー式を追加、編集、または削除します。詳細については、Citrix Gatewayのドキュメントを参照してください。

  e. **「適用」をクリックして変更を適用し、ウィンドウを開いたままにします。または、「保存」**をクリックして変更を適用し、ウィンドウを閉じます。

- **除外フィルターを使用してユーザーへのアクセスを制限する：** SDKで設定したアクセスポリシーに除外フィルターを使用します。アクセスポリシーは、接続を絞り込むためにデリバリーグループに適用されます。たとえば、マシンアクセスをユーザーのサブセットに制限したり、

許可されたユーザーデバイスを指定したりできます。除外フィルターは、アクセスポリシーをさらに絞り込みます。たとえば、セキュリティのために、ユーザーまたはデバイスのサブセットへのアクセスを拒否できます。デフォルトでは、除外フィルターは無効になっています。

たとえば、企業ネットワークのサブネット上にある教育ラボで、そのラボから特定のデリバリーグループへのアクセスを禁止する場合などです。ラボ内のマシンを誰が使用しているかに関係なく、次のコマンドを使用します。`Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`。

アスタリスク (*) ワイルドカードを使用して、同じポリシー式で始まるすべてのタグを照合します。たとえば、あるマシンにタグ`VPDesktops_Direct`を追加し、別のマシンに`VPDesktops_Test`を追加した場合、`Set-BrokerAccessPolicy`スクリプトでタグを`VPDesktops_*`に設定すると、両方のマシンにフィルターが適用されます。

Webブラウザーを使用している場合、またはストアでCitrix Workspaceアプリのユーザーエクスペリエンス機能が有効になっている場合は、クライアント名除外フィルターを使用できません。

デリバリーグループ内のマシンへのユーザー接続を防止する（メンテナンスモード）

マシンへの新規接続を一時的に停止する必要がある場合、デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオンにできます。これは、パッチを適用したり、管理ツールを使用したりする前に行うことがあります。

- マルチセッションOSマシンがメンテナンスモードの場合、ユーザーは既存のセッションに接続できますが、新しいセッションを開始することはできません。
- シングルセッションOSマシン（またはリモートPCアクセスを使用するPC）がメンテナンスモードの場合、ユーザーは接続または再接続できません。現在の接続は、切断またはログオフするまで接続されたままになります。

メンテナンスモードをオンまたはオフにするには：

1. 左ペインで****を選択します。
2. グループを選択します。
3. デリバリーグループ内のすべてのマシンでメンテナンスモードをオンにするには、アクションバーで**メンテナンスモードをオンにする**をクリックします。

   1台のマシンでメンテナンスモードをオンにするには、アクションバーで**マシンを表示**をクリックします。マシンを選択し、アクションバーで**メンテナンスモードをオンにする**をクリックします。

4. デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオフにするには、前述の手順に従いますが、アクションバーで**メンテナンスモードをオフにする**をクリックします。

Windowsリモートデスクトップ接続（RDC）の設定も、マルチセッションOSマシンがメンテナンスモードであるかどうかに影響します。以下のいずれかの状況でメンテナンスモードがオンになります。

- 前述のとおり、メンテナンスモードがオンに設定されている場合。
- RDCが**このコンピューターへの接続を許可しない**に設定されている場合。
- RDCが**このコンピューターへの接続を許可しない**に設定されていない場合。**リモートホスト構成ユーザーログオンモード**の設定が、**再接続を許可するが、新規ログオンを禁止する**、または**再接続を許可するが、サーバーが再起動されるまで新規ログオンを禁止する**のいずれかである場合。

以下の項目についても、メンテナンスモードをオンまたはオフにできます。

- 接続。その接続を使用しているマシンに影響します。
- マシンカタログ。そのカタログ内のマシンに影響します。

デリバリーグループ内のマシンのシャットダウンと再起動

この手順は、リモートPCアクセス マシンではサポートされていません。

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**マシンを表示**をクリックします。
3. マシンを選択し、アクションバーで次のいずれかのエントリをクリックします。

    - **強制シャットダウン:** マシンの電源を強制的にオフにし、マシンの一覧を更新します。
    - **再起動:** オペレーティングシステムにシャットダウンを要求し、その後マシンを再度起動します。オペレーティングシステムがこれに応じられない場合、マシンは現在の状態のままになります。
    - **強制再起動:** オペレーティングシステムを強制的にシャットダウンし、その後マシンを再起動します。
    - **一時停止:** マシンをシャットダウンせずに一時停止し、マシンの一覧を更新します。
    - **シャットダウン:** オペレーティングシステムにシャットダウンを要求します。

強制ではないアクションの場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsが更新プログラムのインストールを試みると、更新が完了する前にマシンの電源がオフになるリスクがあります。

Citrixでは、シングルセッションOSマシンユーザーがセッション内で**シャットダウン**を選択しないようにすることをお勧めします。詳細については、Microsoftのポリシーに関するドキュメントを参照してください。

接続でマシンをシャットダウンして再起動することもできます。

デリバリーグループ内のマシンの再起動スケジュールを作成および管理する

> **注：**
>
> - Autoscale™ が有効なデリバリーグループに再起動スケジュールが適用されると、そのマシンは電源がオフにされるだけで、Autoscale が電源をオンにするまでそのままになります。
> - ランダムなシングルセッションマシンに再起動スケジュールが適用されると、コストを節約するために、それらのマシンは再起動されるのではなく電源がオフになります。マシンの電源をオンにするには Autoscale を使用することをお勧めします。
> - デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動される可能性があります。これを避けるため、タイムゾーン設定は稼働時間外に変更するようにしてください。

> 再起動スケジュールは、デリバリーグループ内のマシンが定期的に再起動されるタイミングを指定します。デリバリーグループに対して1つ以上のスケジュールを作成できます。スケジュールは、次のいずれかに影響します。

- グループ内のすべてのマシン。
- グループ内の1つ以上の（ただしすべてではない）マシン。マシンは、マシンに適用するタグによって識別されます。これはタグ制限と呼ばれます。タグは、アクションをそのタグを持つアイテムのみに制限するためです。

たとえば、すべてのマシンが1つのデリバリーグループにあるとします。すべてのマシンを週に1回再起動し、経理チームが使用するマシンを毎日再起動したいとします。これを実現するには、すべ

てのマシンに対して1つのスケジュールを設定し、経理部門のマシンのみに対して別のスケジュールを設定します。

スケジュールには、再起動が開始される曜日と時刻、および期間が含まれます。

スケジュールを有効または無効にできます。スケジュールを無効にすることは、テスト中、特別な期間中、またはスケジュールが必要になる前に準備する際に役立ちます。

管理コンソールから自動電源オンまたはシャットダウンにスケジュールを使用することはできません。再起動のみに使用できます。

スケジュールの重複

複数のスケジュールが重複する可能性があります。上記の例では、両方のスケジュールが経理部門のマシンに影響します。これらのマシンは日曜日に2回再起動される可能性があります。スケジューリングコードは、意図したよりも頻繁に同じマシンを再起動しないように設計されていますが、保証はできません。

- スケジュールが開始時刻と期間で正確に一致する場合、マシンが再起動されるのは1回だけである可能性が高くなります。
- スケジュールの開始時刻と期間が異なるほど、複数の再起動が発生する可能性が高くなります。
- スケジュールによって影響を受けるマシンの数も、重複の可能性に影響します。例では、すべてのマシンに影響する週次スケジュールは、経理部門のマシンに対する日次スケジュールよりも早く再起動を開始する可能性があります。これは、それぞれに指定された期間によって異なります。

再起動スケジュールについて詳しく知るには、「再起動スケジュールの内部」を参照してください。

再起動スケジュールの表示

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **Restart Schedule**ページを選択します。

Restart Scheduleページには、構成された各スケジュールについて次の情報が含まれています。

- スケジュール名。
- 使用されているタグ制限（ある場合）。
- マシンの再起動がどのくらいの頻度で発生するか。

- マシンユーザーが通知を受け取るかどうか。
- スケジュールが有効になっているかどうか。

タグの追加（適用）

タグ制限を使用する再起動スケジュールを構成する場合は、そのスケジュールが影響するマシンにタグが追加されていることを確認してください。上記の例では、経理チームが使用する各マシンにタグが適用されています。詳細については、「タグ」を参照してください。

1台のマシンに複数のタグを適用できますが、再起動スケジュールで指定できるタグは1つだけです。

1. 左ペインで を選択します。
2. スケジュールによって制御されるマシンを含むグループを選択します。
3. 「**マシンの表示**」をクリックし、タグを追加するマシンを選択します。
4. アクションバーで「**タグの管理**」をクリックします。
5. タグが存在する場合は、タグ名の横にあるチェックボックスをオンにします。タグが存在しない場合は、「**作成**」をクリックし、タグの名前を指定します。タグが作成されたら、新しく作成されたタグ名の横にあるチェックボックスをオンにします。
6. 「**タグの管理**」ダイアログで「**保存**」をクリックします。

再起動スケジュールの作成

> **注:**
>
> 再起動スケジュールは、電源管理されているマルチセッションマシンと電源管理されていないマルチセッションマシンのすべてに適用できます。

1. 左ペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. 「**再起動スケジュール**」ページで、「**追加**」をクリックします。
4. 「**再起動スケジュールの追加**」ページで、次のようにします。
   - スケジュールを有効にするには、「**はい**」を選択します。スケジュールを無効にするには、「**いいえ**」を選択します。
   - スケジュール名と説明を入力します。
   - 「**タグに制限**」で、タグの制限を適用します。

- 「**メンテナンスモードのマシンを含める**」で、メンテナンスモードのマシンをこのスケジュールに含めるかどうかを選択します。代わりにPowerShellを使用するには、「メンテナンスモードのマシンのスケジュールされた再起動」を参照してください。
- 「**再起動頻度**」で、再起動の発生頻度（毎日、毎週、毎月、または1回）を選択します。「**毎週**」または「**毎月**」を選択した場合は、1つ以上の特定の日を指定できます。
- 「**繰り返し間隔**」で、スケジュールを実行する頻度を指定します。
- 「**開始日**」で、スケジュールの初回実行の開始日を指定します。
- 「**再起動開始時刻**」で、再起動を開始する時刻を24時間形式で指定します。
- 「**再起動期間**」について：
  - 自然な再起動を使用しない場合は、「**すべてのマシンを同時に再起動**」または「**すべてのマシンを一定期間内に再起動**」を選択します。
  - 自然な再起動を使用する場合は、「**すべてのセッションがドレインされた後にすべてのマシンを再起動**」を選択します。

    自然な再起動を使用するように構成された再起動スケジュールを開始すると、次のようになります。

    - デリバリーグループに属するすべてのアイドル状態のマシンはすぐに再起動されます
    - 1つ以上の有効なセッションを持つデリバリーグループに属する各マシンは、すべてのセッションがログオフされたときに再起動されます。

    > **注:**
    >
    > 自然な再起動スケジュールは、電源管理されたマシンのみを再起動できます。

- 「**ユーザーに通知を送信**」で、再起動が始まる前に該当するマシンに通知メッセージを表示するかどうかを選択します。デフォルトでは、メッセージは表示されません。
- 再起動が始まる15分前にメッセージを表示することを選択した場合、（**通知頻度**で）最初のメッセージの後に5分ごとにメッセージを繰り返すように選択できます。デフォルトでは、メッセージは繰り返されません。
- 通知のタイトルとテキストを入力します。デフォルトのテキストはありません。

メッセージに再起動までのカウントダウンを含める場合は、変数 **%m%** を含めます。すべてのマシンを同時に再起動することを選択しない限り、メッセージは再起動前の適切なタイミングで各マシンに表示されます。

5. をクリックして変更を適用し、 ウィンドウを閉じます。
6. 「**適用**」をクリックして変更を適用し、ウィンドウを開いたままにします。または、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

ドレイン後の再起動

PowerShell を使用してマシンの再起動スケジュールを作成または更新する場合 (`New-BrokerRebootSchedulev2` または `Set-BrokerRebootSchedulev2`)、別の再起動期間値を使用できます。

`-UseNaturalReboot <Boolean>` パラメーターでドレイン後の再起動機能を有効にすると、すべてのセッションがドレインされた後にすべてのマシンが再起動されます。再起動時刻になると、マシンはドレイン状態になり、すべてのセッションがログオフされた後に再起動されます。

この機能は、シングルセッションまたはマルチセッションマシンを含むデリバリーグループでサポートされています。このオプションは、電源管理されているマシンと電源管理されていないマシンの両方で使用できます。

オンプレミス環境では、この機能は PowerShell を使用する場合にのみサポートされます。この機能は Web Studio では利用できません。

再起動スケジュールの編集、削除、有効化、または無効化

1. 左側のペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **再起動スケジュール**ページで、スケジュールのチェックボックスを選択します。
   - スケジュールを編集するには、 をクリックします。再起動スケジュールの作成 のガイダンスに従って、スケジュール構成を更新します。
   - スケジュールを有効または無効にするには、 をクリックします。 チェックボックスをオンまたはオフにします。
   - スケジュールを削除するには、 をクリックします。削除を確認します。スケジュールを削除しても、影響を受けるマシンに適用されているタグには影響しません。

データベース障害により遅延したスケジュールされた再起動

> **注:**
>
> この機能はPowerShellでのみ利用可能です。

> デリバリーグループ内のマシン（VDA）のスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了したときに再起動が開始されます。これにより、意図しない結果が生じる可能性があります。

たとえば、デリバリーグループの再起動を非稼働時間中（午前3:00開始）に発生するようにスケジュールしたとします。スケジュールされた再起動が開始される1時間前（午前2:00）にサイトデータベースの停止が発生します。停止は6時間続きます（午前8:00まで）。Delivery Controllerとサイトデータベース間の接続が復元されると、再起動スケジュールが開始されます。VDAの再起動は元のスケジュールから5時間後に開始され、稼働時間中にVDAが再起動することになります。

この状況を回避するために、`New-BrokerRebootScheduleV2`および`Set-BrokerRebootScheduleV2`コマンドレットの`MaxOvertimeStartMins`パラメーターを使用できます。この値は、再起動スケジュールが開始できる、スケジュールされた開始時刻からの最大分数を示します。

- その時間内（スケジュールされた時間 + `MaxOvertimeStartMins`）にデータベース接続が復元された場合、VDAの再起動が開始されます。
- その時間内にデータベース接続が復元されない場合、VDAの再起動は開始されません。
- このパラメーターが省略されているか、値がゼロの場合、停止期間に関係なく、データベースへの接続が復元されたときにスケジュールされた再起動が開始されます。

詳細については、コマンドレットのヘルプを参照してください。この機能は PowerShell でのみ利用できます。Web Studio で再起動スケジュールを構成する際には、この値を設定できません。

メンテナンスモードのマシンのスケジュールされた再起動

> **注:**
>
> この機能は PowerShell でのみ利用できます。オプション`IgnoreMaintenanceMode`は、Citrix Virtual Apps and Desktops 7 2006 以降でサポートされています。

> 再起動スケジュールがメンテナンスモードのマシンに影響するかどうかを示すには、`BrokerRebootScheduleV2` コマンドレットで `IgnoreMaintenanceMode` オプションを使用します。

たとえば、次のコマンドレットは、メンテナンスモードではないマシンに加えて、メンテナンスモードのマシンを再起動するスケジュールを作成します。

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup>
-IgnoreMaintenanceMode $true
```

次のコマンドレットは、既存の再起動スケジュールを変更します。

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

詳細については、コマンドレットのヘルプを参照してください。この機能はPowerShellでのみ利用可能です。

1回限りの再起動スケジュールを有効にする

PowerShellを使用して1回限りの再起動スケジュールを有効にする場合は、次の `BrokerCatalogRebootSchedule` PowerShellコマンドを使用して、再起動スケジュールを作成、変更、削除します。

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- Remove-BrokerCatalogRebootSchedule コマンドレット
- Rename-BrokerCatalogRebootSchedule コマンドレット

制限事項:

- タイムゾーンが構成されていないカタログに関連付けられたカタログ再起動スケジュールは作成されますが、開始されません。
- カタログ再起動スケジュールが作成されると、その再起動スケジュールはデリバリーグループに属するカタログVMでのみ実行されます。

例、,

- **BankTellers** という名前のカタログ内のVMの再起動スケジュールを、Feb 3, 2022 の午前2時から午前4時の間に開始するように作成します。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -CatalogName
BankTellers  -StartDate "2022-02-03" -StartTime "02:00" -Enabled $true
-RebootDuration 120
```

- UID 17 のカタログ内のVMの再起動スケジュールを、Feb 3, 2022 の午前1時から午前5時の間に開始するように作成します。再起動の10分前に、各VMはすべてのユーザーセッションで、タイトルが **WARNING: Reboot pending**、メッセージが **Save your work** のメッセージボックスを表示するように設定されます。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot'
-CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -Enabled
$true -RebootDuration 240 -WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
```

- **Old Name** という名前のカタログ再起動スケジュールを **New Name** に変更します。

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName
"New Name"
```

- UID 1 のすべてのカタログ再起動スケジュールを表示し、その後、UID 1 のカタログ再起動スケジュールを **New Name** に変更します。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- **Accounting** という名前のカタログ再起動スケジュールを、各VMの再起動の10分前に、タイトルが **WARNING: Reboot pending, and the message**、メッセージが **Save your work** のメッセージを表示するように設定します。このメッセージは、そのVM上のすべてのユーザーセッションに表示されます。

```
C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage
"Save your work" -WarningDuration 10 -WarningTitle "WARNING: Reboot
pending"
```

- 無効になっているすべての再起動スケジュールを表示し、その後、無効になっているすべての再起動スケジュールを有効にします。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
BrokerCatalogRebootSchedule -Enabled $true
```

- UID 17 のカタログ再起動スケジュールを、各VMの再起動の15分前、10分前、5分前に **Rebooting in %m% minutes** というメッセージを表示するように設定します。

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
%m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
```

- **MyCatalog** という名前のカタログのタイムゾーンを設定します。

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone &lt;TimeZone>
```

デリバリーグループ内の負荷管理されたマシン

負荷管理できるのはマルチセッションOSマシンのみです。

負荷管理は、サーバーの負荷を測定し、現在の環境条件でどのサーバーを選択するかを決定します。この選択は、以下に基づいています。

- **サーバーメンテナンスモードのステータス:** マルチセッションOSマシンは、メンテナンスモードがオフの場合にのみ負荷分散の対象となります。
- **サーバー負荷インデックス:** マルチセッションOSマシンを提供するサーバーが接続を受信する可能性を決定します。このインデックスは、セッション数やCPU、ディスク、メモリ使用量などのパフォーマンスメトリックの設定といった負荷評価指標の組み合わせです。負荷評価指標は、負荷管理ポリシー設定で指定されます。

  サーバー負荷インデックスが10000の場合、サーバーが完全に負荷されていることを示します。他に利用可能なサーバーがない場合、ユーザーはセッションを起動したときに、デスクトップまたはアプリケーションが利用できないというメッセージを受け取る可能性があります。

  負荷インデックスは、Director (Monitor)、Web Studio (Manage) 検索、およびSDKで監視できます。

  コンソール表示で、**サーバー負荷インデックス**列（デフォルトでは非表示）を表示するには、マシンを選択し、列ヘッダーを右クリックして、**列の選択**を選択します。**マシンカテゴリ**で、**負荷インデックス**を選択します。

SDKでは、`Get-BrokerMachine` コマンドレットを使用します。詳細については、「CTX202150」を参照してください。

- **同時ログオン許容ポリシー設定**: サーバーへの同時ログオン要求の最大数。（この設定は、XenApp 6.xバージョンでの負荷スロットリングに相当します。）

  すべてのサーバーが同時ログオン許容設定以上の場合、次のログオン要求は、保留中のログオンが最も少ないサーバーに割り当てられます。複数のサーバーがこれらの条件を満たす場合、ロードインデックスが最も低いサーバーが選択されます。

デリバリーグループ内の電源管理されたマシン

電源管理できるのは、仮想シングルセッションOSマシンのみであり、物理マシン（リモートPCアクセスを含む）はできません。GPU機能を備えたシングルセッションOSマシンは一時停止できないため、電源オフ操作は失敗します。マルチセッションOSマシンについては、再起動スケジュールを作成できます。

プールされたマシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のいずれかの状態になります。

- ランダムに割り当てられ、使用中
- 割り当てられておらず、未接続

静的マシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のようになります。

- 永続的に割り当てられ、使用中
- 永続的に割り当てられ、未接続（ただし準備完了）
- 割り当てられておらず、未接続

通常の使用では、静的デリバリーグループには、永続的に割り当てられたマシンと割り当てられていないマシンの両方が含まれます。最初は、デリバリーグループの作成時に手動で割り当てられたマシンを除き、すべてのマシンが割り当てられていません。ユーザーが接続すると、マシンは永続的に割り当てられます。これらのデリバリーグループ内の割り当てられていないマシンは完全に電源管理できますが、永続的に割り当てられたマシンは部分的にしか管理できません。

- **プールとバッファー:** プールされたデリバリーグループおよび割り当てられていないマシンを持つ静的デリバリーグループの場合、プール（このインスタンスでは）とは、電源オン状態に保たれ、ユーザーが接続する準備ができている、割り当てられていない、または一時的に割り当てられたマシンのセットです。ユーザーはログオン後すぐにマシンを取得します。プールサ

イズ（電源オン状態に保たれるマシンの数）は、時間帯によって構成可能です。静的デリバリーグループの場合、SDK を使用してプールを構成します。

バッファーとは、プール内のマシンの数がしきい値を下回ったときに電源がオンになる、割り当てられていないマシンの追加のスタンバイセットです。しきい値は、デリバリーグループサイズのパーセンテージです。大規模なデリバリーグループの場合、しきい値を超えるとかなりの数のマシンがオンになる可能性があります。そのため、デリバリーグループのサイズを慎重に計画するか、SDK を使用してデフォルトのバッファーサイズを調整してください。

- **電源状態タイマー:** 電源状態タイマーを使用して、ユーザーが指定された時間切断された後にマシンを中断できます。たとえば、ユーザーが少なくとも10分間切断された場合、勤務時間外にマシンは自動的に中断されます。

  タイマーは、平日と週末、およびピーク時と非ピーク時の間隔で構成できます。

- **永続的に割り当てられたマシンの部分的な電源管理:** 永続的に割り当てられたマシンでは、電源状態タイマーを設定できますが、プールやバッファーは設定できません。マシンは各ピーク期間の開始時にオンになり、各オフピーク期間の開始時にオフになります。消費されたマシンを補うために利用可能になるマシンの数について、割り当てられていないマシンで行うようなきめ細かな制御はできません。

仮想シングルセッションOSマシンの電源管理

1. 左ペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. ページで、 の を選択します。デフォルトでは、平日は月曜日から金曜日です。
4. ランダムデリバリーグループの場合、 で をクリックし、平日のプールサイズを指定します。次に、電源をオンにするマシンの数を選択します。
5. で、各日のピーク時間とオフピーク時間を設定します。
6. 平日のピーク時間と非ピーク時間の電源状態タイマーを設定します。 > で、デリバリーグループ内の切断されたマシンを中断するまでの遅延時間（分）を指定し、 を選択します。 > で、デリバリーグループ内のログオフされたマシンをオフにするまでの遅延時間を指定し、 を選択します。このタイマーは、ランダムマシンを含むデリバリーグループでは使用できません。
7. で を選択し、週末のピーク時間と電源状態タイマーを構成します。
8. 「**適用**」をクリックして加えた変更を適用し、ウィンドウを開いたままにします。または、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

SDKを使用して、次の操作を行います。

- 電源状態タイマーに応じて、マシンを中断ではなくシャットダウンする、またはタイマーを接続解除ではなくログオフに基づいて設定する場合。
- デフォルトの平日と週末の定義を変更する。
- 電源管理を無効にします。CTX217289を参照してください。

切断されたセッションを持つVDIマシンが異なる時間帯に移行する際の電源管理

> **重要:**

> この機能強化は、切断されたセッションを持つVDIマシンにのみ適用されます。ログオフされたセッションを持つVDIマシンには適用されません。

> 以前のリリースでは、アクション（切断アクション = 「**中断**」または「**シャットダウン**」）が必要な時間帯に移行するVDIマシンは、電源が入ったままでした。このシナリオは、アクション（切断アクション = 「**何もしない**」）が不要な時間帯（ピーク時またはオフピーク時）にマシンが切断された場合に発生しました。

Citrix Virtual Apps and Desktops 7 1909以降、指定された切断時間が経過すると、宛先時間帯に構成されている切断アクションに応じて、マシンは中断または電源オフになります。

たとえば、VDIデリバリーグループに対して次の電源ポリシーを構成します。

- `PeakDisconnectAction`を「何もしない」に設定
- `OffPeakDisconnectAction`を「シャットダウン」に設定
- `OffPeakDisconnectTimeout`を「10」に設定

電源ポリシーの切断アクションの詳細については、https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policyおよびhttps://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/を参照してください。

以前のリリースでは、ピーク時にセッションが切断されたVDIマシンは、ピークからオフピークに移行しても電源がオンのままでした。Citrix Virtual Apps and Desktops 7 1909以降、期間移行時に`OffPeakDisconnectAction`および`OffPeakDisconnectTimeout`ポリシーアクションがVDIマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作に戻したい場合（つまり、ピークからオフピークへ、またはオフピークからピークへセッションが切断された状態で移行するマシンに対して何もアクションを実行しない場合）は、次のいずれかを実行します。

- `LegacyPeakTransitionDisconnectedBehaviour`レジストリ値を`1`（以前の動作を有効にするtrueに相当）に設定します。デフォルトでは、値は`0`（またはfalse）であり、期間移行時に切断電源ポリシーアクションがトリガーされます。
  - パス: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - 名前: `LegacyPeakTransitionDisconnectedBehaviour`
  - 種類: `REG_DWORD`
  - データ: `0x00000001 (1)`
- `Set-BrokerServiceConfigurationData` PowerShellコマンドを使用して設定を構成します。例：
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

期間移行時に電源ポリシーアクションを適用するには、マシンが次の条件を満たしている必要があります。

- 切断されたセッションがあること。
- 保留中の電源アクションがないこと。
- 異なる期間に移行するVDI（シングルセッション）デリバリーグループに属していること。
- 特定の期間（ピーク時またはオフピーク時）にセッションが切断され、電源アクションが割り当てられている期間に移行すること。

カタログの電源オン状態のVDAの割合を変更する

1. デリバリーグループのピーク時間を、デリバリーグループの**電源管理**セクションから調整します。
2. デスクトップグループ名をメモします。
3. 管理者権限でPowerShellを起動し、次のコマンドを実行します。「Desktop Group Name」を、実行中のVDAの割合が変更されたデスクトップグループの名前に置き換えます。

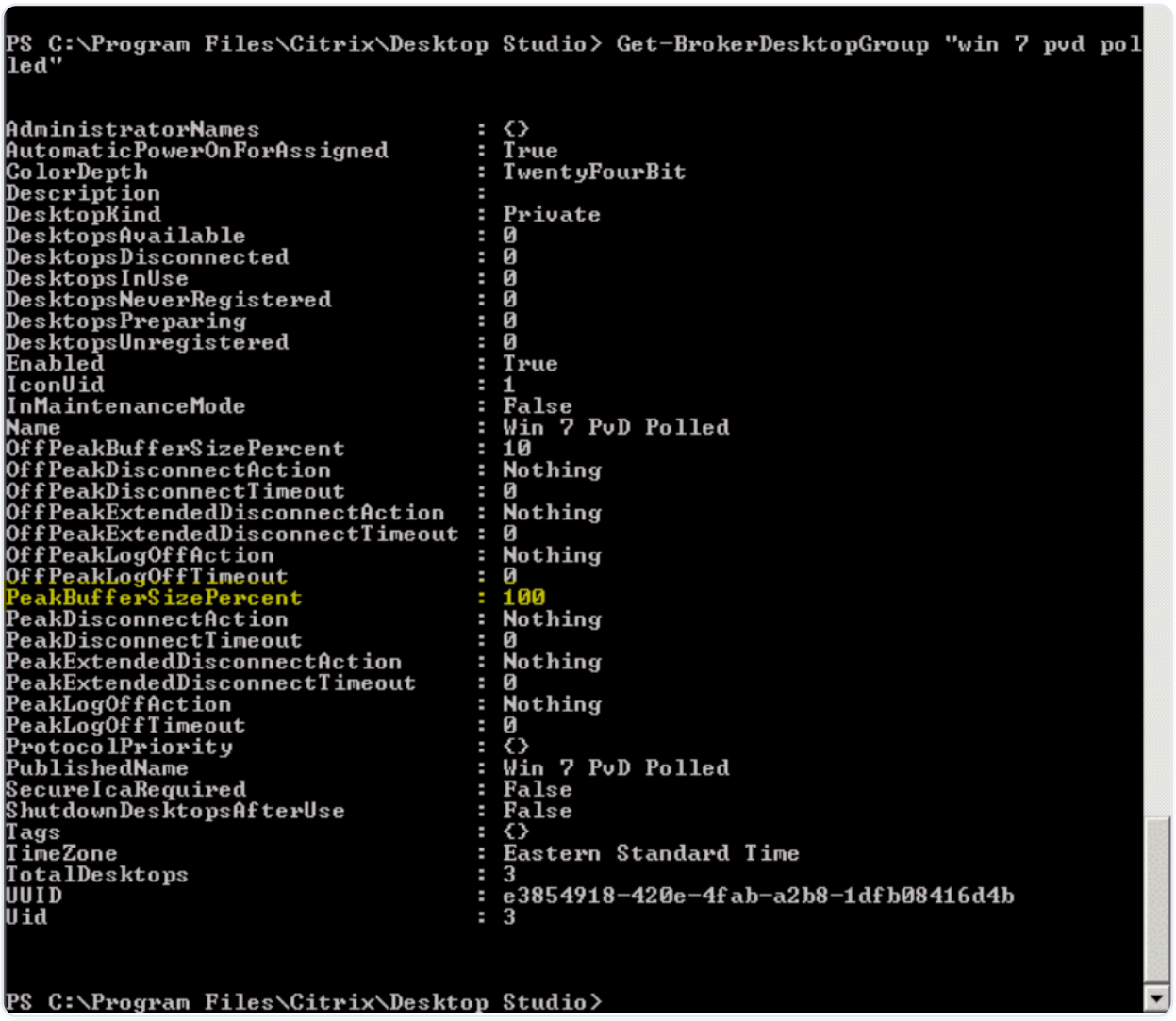
   ```
   asnp Citrix*
   ```

   ```
   # Set-BrokerDesktopGroup "Desktop Group Name" -PeakBufferSizePercent 100
   ```

値が100の場合、VDAの100%が準備完了状態であることを意味します。

4. 次を実行してソリューションを確認します。

```
#Get-BrokerDesktopGroup "Desktop Group Name"
```



変更が有効になるまでに最大1時間かかる場合があります。

ユーザーがログオフした後にVDAをシャットダウンするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name" -ShutDownDesktopsAfterUse $True
```

ピーク時間中にVDAを再起動して、ユーザーがログオフした後に使用できるようにするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssignedDuringPeak $True
```

セッション

- セッションのログオフまたは切断、またはユーザーへのメッセージ送信
- セッションのプレ起動とセッションの維持を構成する
- メンテナンスモードのマシンから切断された場合のセッション再接続を制御する
- セッションローミングを構成する

セッションのログオフまたは切断

1. 左側のペインで、**Delivery Groups**を選択します。
2. デリバリーグループを選択し、アクションバーで**View Machines**を選択します。
3. 中央のペインでマシンを選択し、アクションバーで**View Sessions**を選択してから、セッションを選択します。
    - または、中央のペインで**Session**タブを選択し、セッションを選択します。
4. セッションからログオフするには、アクションバーで**Log off**を選択します。セッションが閉じられ、ユーザーはログアウトされます。マシンが特定のユーザーに割り当てられていない限り、他のユーザーが利用できるようになります。
5. セッションを切断するには、アクションバーで**Disconnect**を選択します。アプリケーションはセッション内で実行を継続し、マシンはそのユーザーに割り当てられたままになります。ユーザーは同じマシンに再接続できます。

シングルセッションOSマシンでは、未使用のセッションを自動的に処理するように電源状態タイマーを構成できます。詳細については、「Power managed machines」を参照してください。

デリバリーグループにメッセージを送信する

1. 左側のペインで、**Delivery Groups**を選択します。
2. デリバリーグループを選択し、アクションバーで**View Machines**を選択します。
3. 中央ペインで、メッセージを送信するマシンを選択します。
4. アクションバーで**View Sessions**を選択します。
5. 中央ペインで、すべてのセッションを選択し、アクションバーで**メッセージの送信**を選択します。
6. メッセージを入力し、**OK**をクリックします。必要に応じて、重大度レベルを指定できます。オプションには、**重大**、**質問**、**警告**、**情報**があります。

または、Citrix Directorを使用してメッセージを送信することもできます。詳しくは、「ユーザーへのメッセージの送信」を参照してください。

デリバリーグループでセッションの事前起動とセッションの維持を構成する

これらの機能は、マルチセッションOSマシンでのみサポートされています。

セッションの事前起動とセッションの維持機能は、要求される前にセッションを開始し（セッションの事前起動）、ユーザーがすべてのアプリケーションを閉じた後もアプリケーションセッションをアクティブに保つ（セッションの維持）ことで、指定されたユーザーがアプリケーションにすばやくアクセスできるようにします。

デフォルトでは、セッションの事前起動とセッションの維持は使用されません。セッションは、ユーザーがアプリケーションを起動したときに開始され（起動）、セッション内の最後に開いたアプリケーションが閉じられるまでアクティブなままです。

考慮事項:

- デリバリーグループはアプリケーションをサポートしている必要があり、マシンはマルチセッションOS用のVDA（最小バージョン7.6）を実行している必要があります。
- これらの機能は、Windows向けCitrix Workspaceアプリを使用している場合にのみサポートされており、追加のCitrix Workspaceアプリ構成も必要です。手順については、お使いのWindows向けCitrix Workspaceアプリバージョンの製品ドキュメントで「session prelaunch」を検索してください。
- HTML5向けCitrix Workspaceアプリはサポートされていません。
- セッションの事前起動を使用している場合、ユーザーのマシンがサスペンドモードまたは休止モードになると、事前起動は機能しません（セッションの事前起動設定に関係なく）。ユーザーはマシン/セッションをロックできます。ただし、ユーザーがCitrix Workspaceアプリからログオフすると、セッションは終了し、事前起動は適用されなくなります。
- セッションの事前起動を使用している場合、物理クライアントマシンはサスペンドまたは休止の電源管理機能を使用できません。クライアントマシンのユーザーはセッションをロックできますが、ログオフしてはいけません。
- 事前起動セッションと残存セッションは同時実行ライセンスを消費しますが、接続されている場合に限ります。ユーザー/デバイスライセンスを使用している場合、ライセンスは90日間有効です。未使用の事前起動セッションと残存セッションは、デフォルトで15分後に切断されます。この値はPowerShell (`New/Set-BrokerSessionPreLaunch` コマンドレット) で構成できます。
- これらの機能が互いに補完し合うように調整するには、ユーザーのアクティビティパターンを慎重に計画し、監視することが不可欠です。最適な構成は、ユーザーがより早くアプリケーションを利用できるという利点と、ライセンスの使用とリソースの割り当てを維持するコストとのバランスを取ります。

- Citrix Workspaceアプリで、セッションの事前起動を特定の時刻にスケジュール設定することもできます。

未使用の事前起動セッションと残存セッションがアクティブなままになる期間

ユーザーがアプリケーションを起動しない場合に、未使用のセッションがアクティブなままになる期間を指定する方法はいくつかあります。構成されたタイムアウトとサーバー負荷のしきい値です。これらすべてを構成できます。最初に発生したイベントにより、未使用のセッションが終了します。

- **タイムアウト：** 構成されたタイムアウトは、未使用の事前起動セッションまたは残存セッションがアクティブなままになる分数、時間、または日数を指定します。タイムアウトを短く設定しすぎると、事前起動セッションは、ユーザーがより迅速にアプリケーションにアクセスできるという利点を提供する前に終了してしまいます。タイムアウトを長く設定しすぎると、サーバーに十分なリソースがないため、受信ユーザー接続が拒否される可能性があります。

  このタイムアウトは、管理コンソールからではなく、SDK (`New/Set-BrokerSessionPreLaunch` コマンドレット) からのみ有効にできます。タイムアウトを無効にすると、そのデリバリーグループのコンソール表示や、**デリバリーグループの編集**ページには表示されません。

- **しきい値：** サーバー負荷に基づいて事前起動セッションと残存セッションを自動的に終了することで、サーバーリソースが利用可能である限り、セッションが可能な限り長く開いたままになることが保証されます。未使用の事前起動セッションと残存セッションは、新しいユーザーセッションにリソースが必要なときに自動的に終了するため、接続拒否の原因にはなりません。

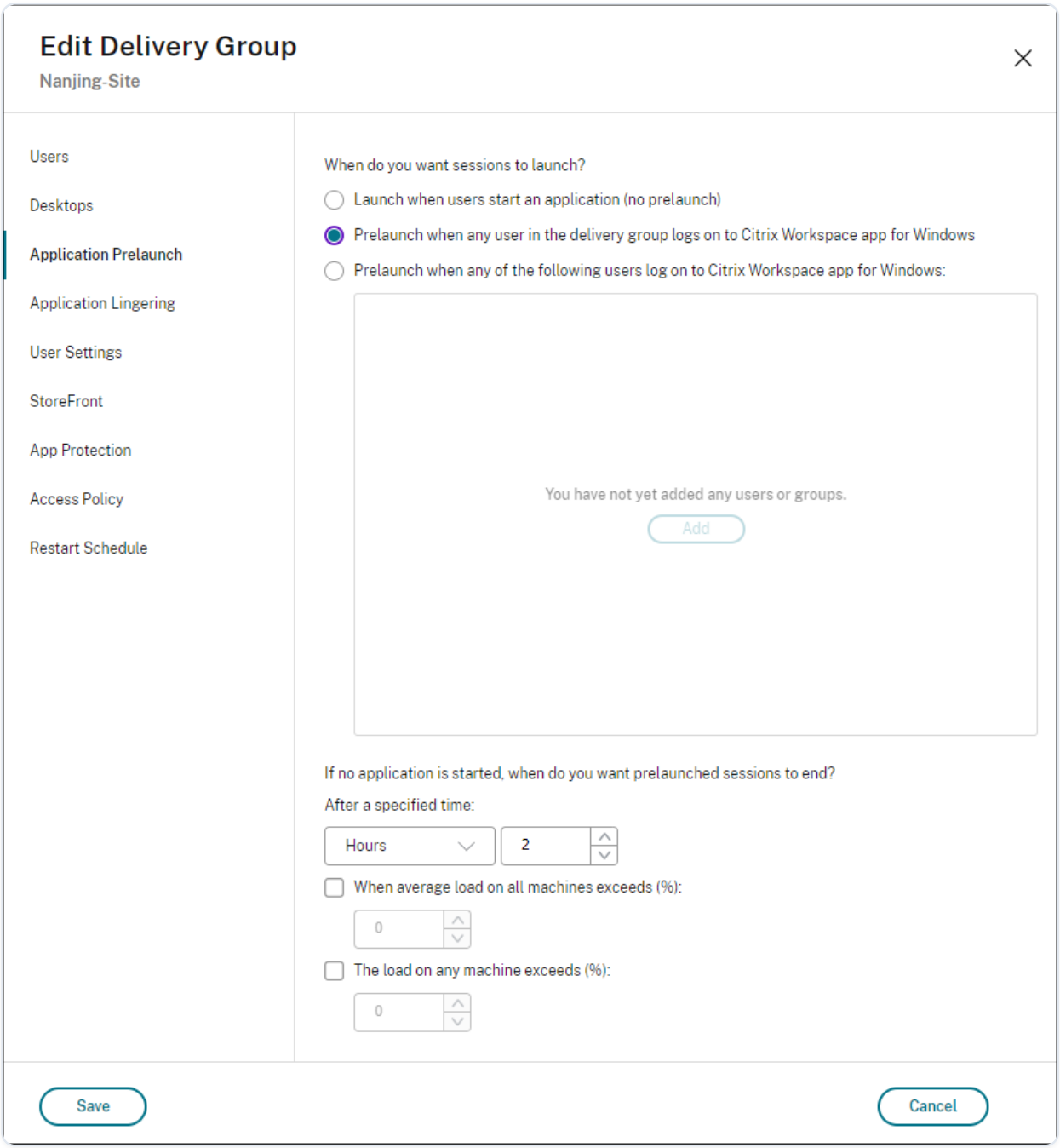
  2つのしきい値を構成できます。デリバリーグループ内のすべてのサーバーの平均負荷率と、グループ内の単一サーバーの最大負荷率です。しきい値を超えると、事前起動または残存状態にあった時間が最も長いセッションが終了します。負荷がしきい値を下回るまで、セッションは1分間隔で1つずつ終了します。しきい値を超えている間は、新しい事前起動セッションは開始されません。

Controllerに登録されていないVDAを持つサーバーと、メンテナンスモードのサーバーは、完全にロードされていると見なされます。計画外の停止が発生すると、容量を解放するために事前起動セッションと残存セッションが自動的に終了します。

セッションの事前起動を有効にするには

1. グループを選択し、アクションバーで**デリバリーグループの編集**をクリックします。
2. **アプリケーションの事前起動**ページで、セッションを起動するタイミングを選択して、セッションの事前起動を有効にします。

- ユーザーがアプリケーションを起動したとき。これはデフォルト設定です。セッションの事前起動は無効になっています。
- デリバリーグループ内のいずれかのユーザーがWindows用Citrix Workspaceアプリにログオンしたとき。
- ユーザーとユーザーグループのリストのいずれかのユーザーがWindows用Citrix Workspaceアプリにログオンしたとき。このオプションを選択する場合は、ユーザーまたはユーザーグループも指定してください。



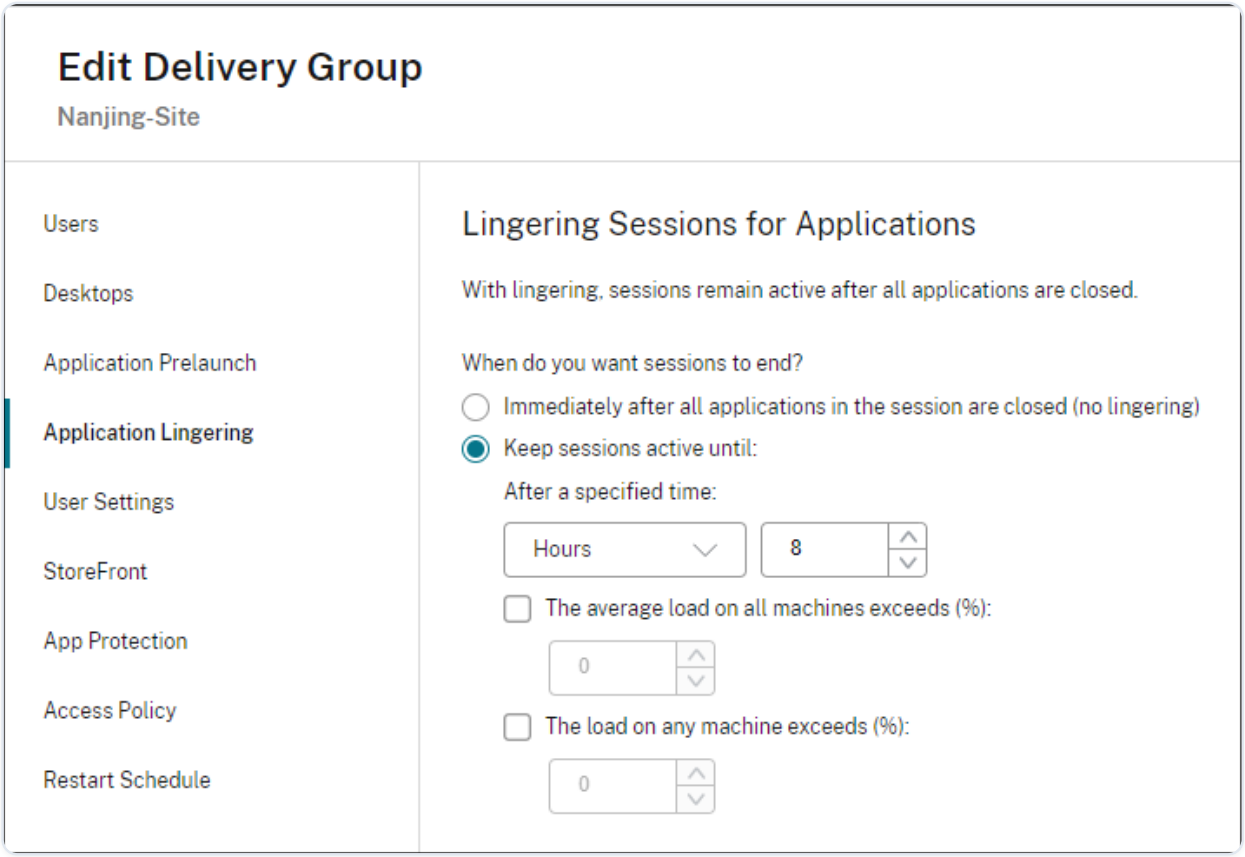
3. ユーザーがアプリケーションを起動すると、事前起動セッションは通常のセッションに置き換えられます。ユーザーがアプリケーションを起動しない場合（事前起動セッションが未使用の場合）、次の設定がそのセッションがアクティブな状態を維持する期間に影響します。

- 指定された時間間隔が経過したとき。時間間隔（1～99日、1～2376時間、または1～142,560分）を変更できます。
- デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1～99%）を超えたとき。
- デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1～99%）を超えたとき。

まとめ：事前起動セッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブな状態を維持します。

セッションの残存を有効にするには

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**デリバリーグループの編集**をクリックします。
3. **アプリケーションの残存**ページで、**セッションをアクティブに維持する期間**を選択してセッションの残存を有効にします。



4. ユーザーが別のアプリケーションを起動しない場合、いくつかの設定が残存セッションがアクティブな状態を維持する期間に影響します。

- 指定された時間間隔が経過したとき。時間間隔（1〜99日、1〜2376時間、または1〜142,560分）を変更できます。
- デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1〜99%）を超えたとき。
- デリバリーグループ内のいずれかのマシンの負荷が指定されたパーセンテージ（1〜99%）を超えた場合。

まとめ：残存セッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままです。

メンテナンスモードのマシンから切断された場合のセッションの再接続を制御する

> **注：**
>
> この機能はPowerShellでのみ利用可能です。

> メンテナンスモードのマシンで切断されたセッションが、デリバリーグループ内のマシンに再接続できるかどうかを制御できます。

バージョン2106より前は、メンテナンスモードのマシンから切断されたシングルセッションのプールされたデスクトップセッションの再接続は許可されていませんでした。バージョン2106以降では、メンテナンスモードのマシンから切断された後の再接続（セッションの種類に関係なく）を許可または禁止するようにデリバリーグループを構成できます。

デリバリーグループを作成または編集する際（`New-BrokerDesktopGroup`、`Set-BrokerDesktopGroup`）、`-AllowReconnectInMaintenanceMode <boolean>`パラメーターを使用して、メンテナンスモードのマシンから切断されたマシンへの再接続を許可または禁止します。

- trueに設定すると、セッションはグループ内のマシンに再接続できます。
- 「false」に設定されている場合、セッションはグループ内のマシンに再接続できません。

デフォルト値:

- シングルセッション: 無効
- マルチセッション: 有効

セッションローミングの構成

デフォルトでは、デリバリーグループに対してセッションローミングが有効になっています。セッションはユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、アプリケーションは両方のデバイスで同時に利用可能になります。複数のデバイスでアプリケーションを表示できます。アプリケーションは、デバイスや現在のセッションの有無にかかわらず追従します。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追従します。または、PowerShellを使用することもできます。詳しくは、「セッションローミング」を参照してください。

アプリケーションのセッションローミングの構成

アプリケーションのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左ペインの**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**デリバリーグループの編集**を選択します。
3. **ユーザー**ページで、**ユーザーがデバイス間を移動するときにセッションをローミングする**チェックボックスをオンにして、セッションローミングを有効にします。

   - 有効にすると、ユーザーがアプリケーションセッションを起動し、別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスで利用できます。無効にすると、セッションはデバイス間をローミングしなくなります。

4. **OK**を選択して変更を適用し、ウィンドウを閉じます。

デスクトップのセッションローミングを構成する

デスクトップのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左ペインの**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. **デスクトップ**ページで、デスクトップを選択し、**編集**を選択します。
4. **セッションローミング**チェックボックスをオンにして、セッションローミングを有効にします。

- 有効にすると、ユーザーがデスクトップを起動し、別のデバイスに移動した場合、同じセッションが使用され、アプリケーションは両方のデバイスで利用できます。無効にすると、セッションはデバイス間をローミングしなくなります。

OKを選択して変更を適用し、ウィンドウを閉じます。

トラブルシューティング

- Delivery Controllerに登録されていないVDAは、仲介されたセッションの起動時に考慮されません。これにより、利用可能なリソースが十分に活用されないことになります。VDAが登録されない理由はさまざまあり、その多くは管理者がトラブルシューティングできます。詳細表示には、カタログ作成ウィザードおよびデリバリーグループにカタログを追加した後のトラブルシューティング情報が表示されます。

  デリバリーグループを作成した後、デリバリーグループの詳細ペインには、登録可能だが登録されていないマシンの数が表示されます。たとえば、1台以上のマシンが電源オンでメンテナンスモードではないが、現在Controllerに登録されていない場合などです。「登録されていないが、登録されるべき」マシンを表示するときは、詳細ペインの**トラブルシューティング**タブで考えられる原因と推奨される是正措置を確認してください。

  機能レベルに関するメッセージについては、「VDAのバージョンと機能レベル」を参照してください。

  VDA登録のトラブルシューティングについては、「CTX136668」を参照してください。
- デリバリーグループの表示では、詳細ペインの**インストール済みVDAバージョン**が、マシンに実際にインストールされているバージョンと異なる場合があります。マシンのWindowsの「プログラムと機能」表示には、実際のVDAバージョンが表示されます。
- **電源状態不明**のステータスのマシンについては、CTX131267を参照してください。

アプリケーショングループの作成

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されるアプリケーション、またはデリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションに対して、アプリケーショングループを作成します。アプリケーショングループはオプションであり、同じアプリケーションを複数のデリバリー

グループに追加する代替手段を提供します。デリバリーグループを複数のアプリケーショングループに関連付けたり、アプリケーショングループを複数のデリバリーグループに関連付けたりできます。

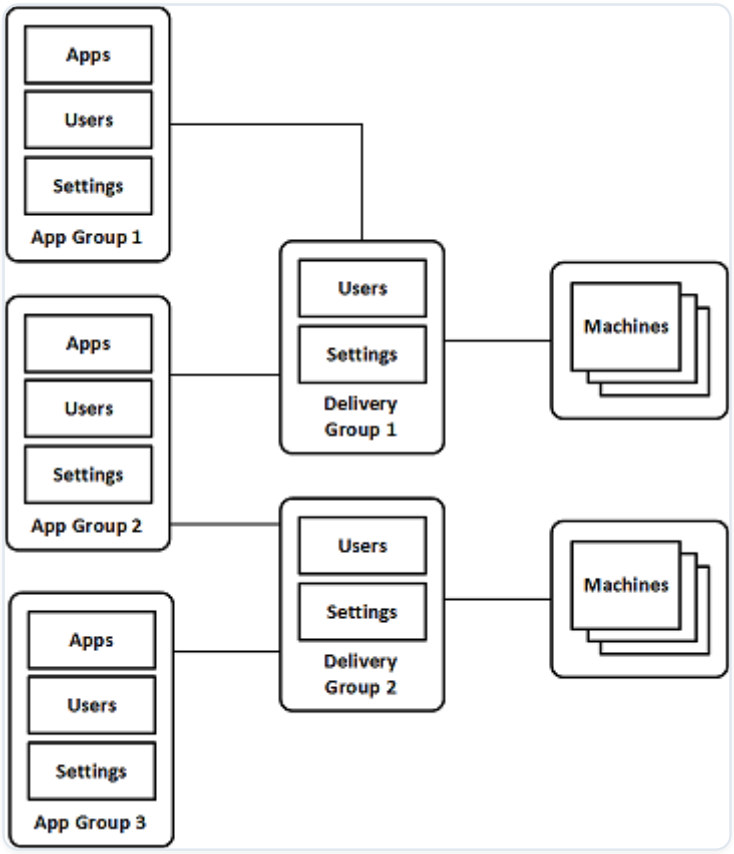
アプリケーショングループを使用すると、より多くのデリバリーグループを使用する場合と比較して、アプリケーション管理とリソース制御の利点が得られます。

- アプリケーションとその設定を論理的にグループ化することで、それらのアプリケーションを単一の単位として管理できます。たとえば、同じアプリケーションを個々のデリバリーグループに1つずつ追加（公開）する必要はありません。
- アプリケーショングループ間のセッション共有により、リソース消費を節約できます。その他の場合、アプリケーショングループ間のセッション共有を無効にすることが有益な場合もあります。
- タグ制限機能を使用すると、選択したデリバリーグループ内のマシンの一部のみを考慮して、アプリケーショングループからアプリケーションを公開できます。タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、追加のマシンの展開と管理に関連するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。タグ制限付きのアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンの一部を分離してトラブルシューティングする際に役立ちます。

構成例

例 1:

次の図は、アプリケーショングループを含むCitrix Virtual Apps and Desktops展開を示しています。



この構成では、アプリケーションはデリバリーグループではなくアプリケーショングループに追加されます。デリバリーグループは、どのマシンが使用されるかを指定します。（図には示されていませんが、マシンはマシンカタログ内にあります。）

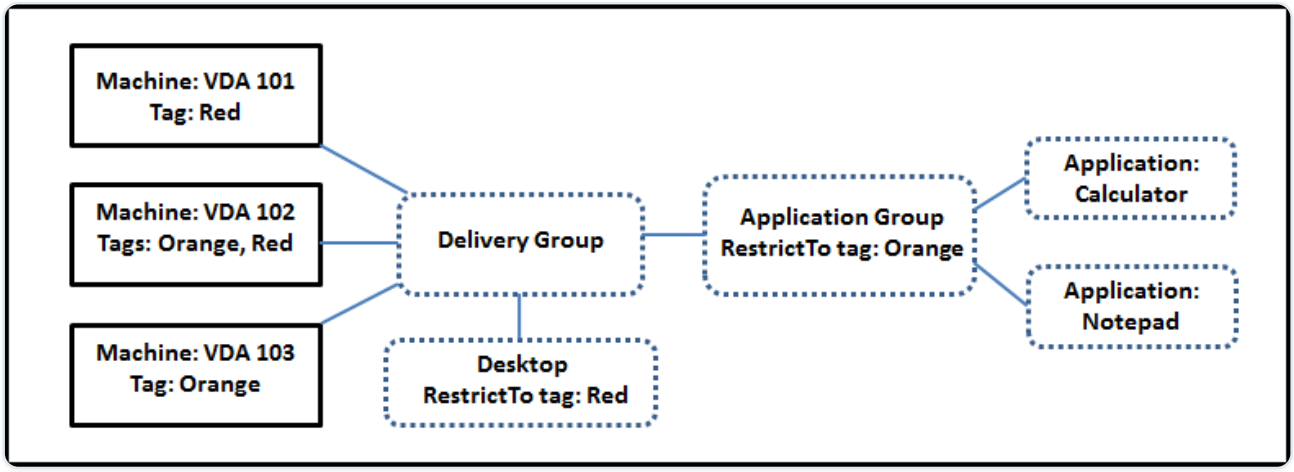
アプリケーショングループ1はデリバリーグループ1に関連付けられています。アプリケーショングループ1のアプリケーションには、アプリケーショングループ1で指定されたユーザーがアクセスします。これらのグループは、デリバリーグループ1のユーザーリストにも含まれている場合にのみ表示されます。この構成は、アプリケーショングループのユーザーリストが、関連付けられたデリバリーグループのユーザーリストのサブセット（制限）であるというガイダンスに従っています。アプリケーショングループ1の設定（アプリケーショングループ間のアプリケーションセッション共有、関連付けられたデリバリーグループなど）は、そのグループ内のアプリケーションとユーザーに適用されます。デリバリーグループ1の設定は、アプリケーショングループ1と2のユーザーに適用されます。これは、これらのアプリケーショングループがそのデリバリーグループに関連付けられているためです。

アプリケーショングループ2は、2つのデリバリーグループ（1と2）に関連付けられています。これらのデリバリーグループのそれぞれには、アプリケーショングループ2で優先順位が割り当てられており、アプリケーションが起動されたときにデリバリーグループがチェックされる順序を示します。優先順位が同じデリバリーグループは負荷分散されます。アプリケーショングループ2のアプリケーションには、アプリケーショングループ2で指定されたユーザーがアクセスします。ただ

し、それらのユーザーはデリバリーグループ1とデリバリーグループ2のユーザーリストにも含まれている必要があります。

例 2:

このシンプルなレイアウトでは、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限します。このサイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。



3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。

アプリケーショングループは「Orange」タグ制限付きで作成されました。その各アプリケーションは、そのデリバリーグループ内で「Orange」タグを持つマシン（VDA 102および103）でのみ起動されます。

アプリケーショングループ（およびデスクトップ）でタグ制限を使用するためのより包括的な例とガイダンスについては、「タグ」を参照してください。

ガイダンスと考慮事項

Citrixでは、アプリケーションをアプリケーショングループまたはデリバリーグループのいずれかに追加することをお勧めします。両方に追加することはお勧めしません。そうしないと、2種類のグループにアプリケーションが存在することで複雑さが増し、管理が困難になる可能性があります。

デフォルトでは、アプリケーショングループは有効になっています。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

デフォルトでは、アプリケーショングループ間のアプリケーションセッション共有は有効になっています。「アプリケーショングループ間のセッション共有」を参照してください。

Citrixでは、デリバリーグループを現在のバージョンにアップグレードすることをお勧めします。このプロセスには、次のものが必要です。

1. デリバリーグループで使用されているマシンのVDAをアップグレードする。
2. それらのマシンを含むマシンカタログをアップグレードする。
3. デリバリーグループをアップグレードする。

詳細については、「デリバリーグループの管理」を参照してください。

アプリケーショングループを使用するには、コアコンポーネントが最低バージョン7.9である必要があります。

アプリケーショングループを作成するには、Delivery Group Administratorの組み込みロールの委任管理権限が必要です。詳細については、委任管理を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」ことについて言及しています。これは、利用可能なソースからそのアプリケーションのインスタンスを追加する操作とは区別されます。同様に、デリバリーグループは、互いの追加やコンポーネントではなく、アプリケーショングループに関連付けられます。

アプリケーショングループとのセッション共有

アプリケーションセッション共有が有効になっている場合、すべてのアプリケーションは同じアプリケーションセッションで起動します。これにより、より多くのアプリケーションセッションを起動することに関連するコストが削減され、コピー＆ペースト操作など、クリップボードを伴うアプリケーション機能の使用が可能になります。ただし、状況によってはセッション共有をクリアできます。

アプリケーショングループを使用する場合、デリバリーグループのみを使用する場合に利用できる標準のセッション共有動作を拡張する、次の3つの方法でアプリケーションセッション共有を構成できます。

- アプリケーショングループ間でセッション共有が有効になっている。
- 同じアプリケーショングループ内のアプリケーション間でのみセッション共有が有効になっている。
- セッション共有が無効になっている。

アプリケーショングループ間のセッション共有

アプリケーショングループ間でアプリケーションセッション共有を有効にすることも、無効にして同じアプリケーショングループ内のアプリケーションのみにアプリケーションセッション共有を制限することもできます。

- **アプリケーショングループ間のセッション共有を有効にすることが役立つ例:**

  アプリケーショングループ1には、WordやExcelなどのMicrosoft Officeアプリケーションが含まれています。アプリケーショングループ2には、メモ帳や電卓などの他のアプリケーションが含まれており、両方のアプリケーショングループは同じデリバリーグループにアタッチされています。両方のアプリケーショングループにアクセスできるユーザーが、Wordを起動してアプリケーションセッションを開始し、次にメモ帳を起動します。コントローラーが、Wordを実行しているユーザーの既存のセッションがメモ帳の実行に適していると判断した場合、メモ帳は既存のセッション内で開始されます。既存のセッションからメモ帳を実行できない場合（たとえば、タグ制限によってセッションが実行されているマシンが除外されている場合）、セッション共有を使用するのではなく、適切なマシン上に新しいセッションが作成されます。

- **アプリケーショングループ間のセッション共有を無効にすることが役立つ例:**

  同じマシンにインストールされている他のアプリケーションと相互運用性が低いアプリケーションのセットを含む構成。たとえば、同じソフトウェアスイートの2つの異なるバージョンや、同じWebブラウザの2つの異なるバージョンなどです。ユーザーが同じセッションで両方のバージョンを起動することを許可しない方がよい場合。

  ソフトウェアスイートのバージョンごとにアプリケーショングループを作成し、各バージョンのアプリケーションを対応するアプリケーショングループに追加します。これらのアプリケーショングループ間でセッション共有が無効になっている場合、それらのグループで指定されたユーザーは、同じセッションで同じバージョンのアプリケーションを実行できます。ユーザーは同時に他のアプリケーションを実行できますが、同じセッションでは実行できません。異なるバージョンのアプリケーション、またはアプリケーショングループに含まれていないアプリケーションを起動すると、そのアプリケーションは新しいセッションで起動されます。

このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。これは完璧ではなく、ユーザーが他の手段（たとえば、Windowsエクスプローラーを介して）でセッションにアプリケーションを起動するのを防ぐことはできません。

マシンが容量に達している場合、新しいセッションはそのマシンでは開始されません。必要に応じて、セッション共有を使用して、新しいアプリケーションがそのマシンの既存のセッションで開始されます。

プレローンチされたセッションは、アプリケーションセッション共有が許可されているアプリケーショングループでのみ利用可能です。（セッションリンガー機能を使用するセッションは、すべてのアプリケーショングループで利用可能です。）これらの機能は、アプリケーショングループに関連付けられている各デリバリーグループで有効にして構成する必要があります。アプリケーショングループでは構成できません。

デフォルトでは、アプリケーショングループを作成すると、アプリケーショングループ間のアプリケーションセッション共有が有効になります。グループ作成時にこれを変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループ内でのセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でのアプリケーションセッション共有を防ぐことができます。

- **アプリケーショングループ内でのセッション共有を無効にすることが役立つ例:**

  ユーザーに、別々のモニターでアプリケーションの複数の同時フルスクリーンセッションにアクセスさせたい場合。

  アプリケーショングループを作成し、そこにアプリケーションを追加します。

デフォルトでは、アプリケーショングループを作成すると、アプリケーションセッション共有が有効になります。グループ作成時にこの設定を変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループを作成する

アプリケーショングループを作成するには：

1. Web Studioにサインインします。
2. 左ペインで**Applications**を選択し、**Application Groups**タブを選択します。
3. フォルダーを使用してアプリケーショングループを整理するには、**Application Groups**ルートフォルダーの下にフォルダーを作成します。
4. グループを作成するフォルダーを選択し、**Create Application Group**をクリックします。グループ作成ウィザードが**Introduction**ページとともに起動します。このページは、今後のウィザード起動時に表示しないように設定できます。
5. ウィザードに従って、以下に説明するページで設定を構成します。各ページの作業が完了したら、**Summary**ページに到達するまで**Next**を選択します。

手順1. デリバリーグループ

Delivery Groupsページには、すべてのデリバリーグループと、各グループに含まれるマシンの数が表示されます。

- **Compatible Delivery Groups**リストには、選択可能なデリバリーグループが含まれています。互換性のあるデリバリーグループには、ランダム（永続的または静的に割り当てられていない）なマルチセッションまたはシングルセッションOSマシンが含まれています。
- **Incompatible Delivery Groups**リストには、選択できないデリバリーグループが含まれています。各エントリには、静的に割り当てられたマシンが含まれているなど、互換性がない理由が説明されています。

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループに共有マシンが含まれており、XenDesktopバージョン7.9より前に作成されたものである。
- デリバリーグループの編集権限がある。

アプリケーショングループ作成ウィザードがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

関連付けられたデリバリーグループがないアプリケーショングループを作成することはできますが（アプリケーションを整理するため、または現在使用されていないアプリケーションのストレージとして機能させるためなど）、少なくとも1つのデリバリーグループが指定されるまで、そのアプリケーショングループをアプリケーションの配信に使用することはできません。また、デリバリーグループが指定されていない場合、**From Start**メニューソースからアプリケーショングループにアプリケーションを追加することはできません。

選択したデリバリーグループは、アプリケーションの配信に使用されるマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグ制限を追加するには、「**タグを持つマシンへの起動を制限する**」を選択し、ドロップダウンリストからタグを選択します。

手順2. ユーザー

アプリケーショングループでアプリケーションユーザーを指定します。前のページで選択したデリバリーグループ内のすべてのユーザーとユーザーグループを許可するか、それらのデリバリーグループから特定のユーザーとユーザーグループを選択します。指定されたユーザーに利用を制限する場合、デリバリーグループで指定されたユーザーのうち、アプリケーショングループで指定されたユーザーのみが、このグループのアプリケーションにアクセスできます。基本的に、アプリケーショングループのユーザーリストは、デリバリーグループのユーザーリストに対するフィルターとして機能します。

認証されていないユーザーによるアプリケーションの使用の有効化または無効化は、アプリケーショングループではなく、デリバリーグループでのみ利用できます。

展開でユーザーリストが指定される場所については、「ユーザーリストが指定される場所」を参照してください。

ステップ3. アプリケーション

知っておくと良いこと:

- デフォルトでは、追加する新しいアプリケーションは**アプリケーション**という名前のフォルダーに配置されます。別のフォルダーを指定することもできます。アプリケーションを追加しようとして、同じ名前のアプリケーションがそのフォルダーに存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提案された一意の名前に同意すると、その新しい名前でアプリケーションが追加されます。そうでない場合は、追加する前に自分で名前を変更する必要があります。詳細については、「アプリケーションフォルダーの管理」を参照してください。
- アプリケーションのプロパティ（設定）は、追加時または後で変更できます。「アプリケーションプロパティの変更」を参照してください。同じ名前のアプリケーションを2つ同じユーザーに公開する場合、Web Studioで**アプリケーション名（ユーザー向け）**プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にすることになります。
- アプリケーションを複数のアプリケーショングループに追加する場合、それらのすべてのグループでアプリケーションを表示する十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのグループを含むようにスコープを拡張してください。

アプリケーションソースを表示するには、ドロップダウンメニューから「**追加**」をクリックします。

- **スタートメニューから**：選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。

  以下のいずれかを選択した場合、このソースは選択できません。

  - 関連付けられたデリバリーグループがないアプリケーショングループ。
  - 関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループ。
  - マシンが含まれていないデリバリーグループ。

- **手動で定義:** サイト内またはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、新しいページが起動し、実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者とユーザーの表示名を入力します。この情報を入力したら、**OK**をクリックします。
- **既存:** 以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、**OK**をクリックします。サイトにアプリケーションがない場合、このソースは選択できません。
- **App-V:** App-Vパッケージ内のアプリケーション。このソースを選択すると、新しいページが起動し、**App-Vサーバー**または**アプリケーションライブラリ**を選択します。表示された画面から、追加するアプリケーションのチェックボックスをオンにして、**OK**をクリックします。詳細については、「App-Vアプリケーションの展開と配信」を参照してください。サイトでApp-Vが構成されていない場合、このソースは選択できません（または表示されない場合があります）。

前述のとおり、そのタイプの有効なソースがない場合、**追加**ドロップダウンメニューの一部のエントリは選択できません。互換性のないソースはまったく表示されません（たとえば、アプリケーショングループにアプリケーショングループを追加することはできないため、アプリケーショングループを作成するときにそのソースは表示されません）。

ステップ4. スコープ

このページは、以前にカスタムスコープを作成した場合にのみ表示されます。デフォルトでは、**すべて**のスコープが選択されています。詳細については、「委任管理」を参照してください。

ステップ5. 概要

アプリケーショングループの名前を入力します。説明を（オプションで）入力することもできます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーショングループの管理

> **注:**
>
> Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

この記事では、作成したアプリケーショングループを管理する方法について説明します。

アプリケーショングループまたはデリバリーグループでアプリケーションを管理する方法については、アプリケーションを参照してください。以下を含みます。

- アプリケーショングループ内のアプリケーションを追加または削除する。
- アプリケーショングループの関連付けを変更する。

アプリケーショングループの管理には、Delivery Group Administratorの組み込みロールの委任管理権限が必要です。詳細については、委任管理を参照してください。

アプリケーショングループを有効または無効にする

アプリケーショングループが有効になっている場合、そのグループに追加されたアプリケーションを配信できます。アプリケーショングループを無効にすると、そのグループ内の各アプリケーションが無効になります。ただし、それらのアプリケーションが他の有効なアプリケーショングループにも関連付けられている場合、それらの他のグループから配信できます。アプリケーションがアプリケーショングループに関連付けられたデリバリーグループに明示的に追加された場合、アプリケーショングループを無効にしても、それらのデリバリーグループ内のアプリケーションには影響しません。

アプリケーショングループは作成時に有効になります。グループの作成時にこの設定を変更することはできません。

1. 左側のペインで**アプリケーション**を選択し、次に**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **設定**ページで、**アプリケーショングループを有効にする**チェックボックスをオンまたはオフにします。
4. 「**適用**」をクリックしてウィンドウを開いたままにするか、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーショングループ間のアプリケーションセッション共有を有効または無効にする

アプリケーショングループを作成すると、アプリケーショングループ間のセッション共有が有効になります。グループの作成時にこの構成を変更することはできません。詳細については、「アプリケーショングループとのセッション共有」を参照してください。

1. 左ペインで「**アプリケーション**」を選択し、「**アプリケーショングループ**」タブを選択します。
2. アプリケーショングループを選択し、アクションバーで「**アプリケーショングループの編集**」を選択します。
3. 「**設定**」ページで、「**アプリケーショングループ間のアプリケーションセッション共有を有効にする**」チェックボックスをオンまたはオフにします。
4. 「**適用**」をクリックしてウィンドウを開いたままにするか、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーショングループ内でのアプリケーションセッション共有を無効にする

アプリケーションセッション共有は、アプリケーショングループの作成時に有効になります。この構成は、グループの作成時に変更できません。詳細については、「アプリケーショングループとのセッション共有」を参照してください。

PowerShell SDKを使用して、含まれるアプリケーション間でアプリケーションセッション共有が無効になっているアプリケーショングループを構成できます。特定の状況では、このオプションが

望ましい場合があります。たとえば、ユーザーにシームレスではないアプリケーションを、個別のモニター上の全画面表示のアプリケーションウィンドウで起動させたい場合があります。

アプリケーショングループ内でアプリケーションセッション共有を無効にすると、そのグループ内の各アプリケーションは新しいアプリケーションセッションで起動します。同じアプリケーションを実行している適切な切断セッションが利用可能な場合、そのセッションは再接続されます。たとえば、メモ帳を実行している切断セッションでメモ帳を起動する場合、新しいセッションを作成する代わりにそのセッションが再接続されます。複数の適切な切断セッションが利用可能な場合、ランダムではあるが決定論的な方法で、いずれかのセッションが再接続のために選択されます。同じ状況でこの状況が再発生した場合、同じセッションが選択されますが、それ以外の場合、セッションは必ずしも予測可能ではありません。

PowerShell SDKを使用して、既存のアプリケーショングループ内のすべてのアプリケーションのアプリケーションセッション共有を無効にするか、アプリケーションセッション共有が無効になっているグループを作成します。

PowerShellコマンドレットの例

セッション共有を無効にするには、Broker PowerShellコマンドレット`New-BrokerApplicationGroup`または`Set-BrokerApplicationGroup`を使用し、パラメーター`SessionSharingEnabled`を`False`に設定し、パラメーター`SingleAppPerSession`を`True`に設定します。

- たとえば、グループ内のすべてのアプリケーションのアプリケーションセッション共有が無効になっているアプリケーショングループを作成するには、次の手順を実行します。

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

- 例えば、既存のアプリケーショングループ内のすべてのアプリケーション間でアプリケーションセッション共有を無効にするには:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

考慮事項

- `SingleAppPerSession`プロパティを有効にするには、`SessionSharingEnabled`プロパティをFalseに設定する必要があります。2つのプロパティを同時に有効にすることはできません。`SessionSharingEnabled`パラメーターは、アプリケーショングループ間のセッション共有を指します。

- アプリケーションセッション共有は、アプリケーショングループに関連付けられているがデリバリーグループには関連付けられていないアプリケーションに対してのみ機能します。デリバリーグループに直接関連付けられているすべてのアプリケーションは、デフォルトでセッションを共有します。
- アプリケーションが複数のアプリケーショングループに割り当てられている場合、グループに競合する設定がないことを確認してください。例えば、オプションが`True`に設定されているグループと、オプションが`False`に設定されている別のグループでは、予測できない動作が発生します。

アプリケーショングループの名前を変更する

1. 左ペインで**アプリケーション**を選択し、次に**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの名前を変更**を選択します。
3. 新しい一意の名前を指定し、次に**OK**をクリックします。

アプリケーショングループとのデリバリーグループの関連付けを追加、削除、または優先度を変更する

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループに共有マシンが含まれており、7.9より前のバージョンで作成されたものである。
- 「デリバリーグループの編集」権限が必要です。

Edit Application Groupダイアログがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

1. 左ペインで**「アプリケーション」を選択し、「アプリケーショングループ」**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**「アプリケーショングループの編集」**を選択します。
3. **「デリバリーグループ」**ページを選択します。

4. デリバリーグループを追加するには、**「追加」をクリックします。利用可能なデリバリーグループのチェックボックスを選択します。（互換性のないデリバリーグループは選択できません。）選択が完了したら、「OK」**をクリックします。
5. デリバリーグループを削除するには、削除するグループのチェックボックスを選択し、**「削除」**をクリックします。プロンプトが表示されたら削除を確定します。
6. デリバリーグループの優先度を変更するには、デリバリーグループのチェックボックスを選択し、**「優先度の編集」をクリックします。優先度（0 = 最高）を入力し、「OK」**をクリックします。
7. 変更を適用してウィンドウを開いたままにするには**「適用」をクリックし、変更を適用してウィンドウを閉じるには「保存」**をクリックします。

アプリケーショングループのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、アプリケーション起動の対象となるマシンに予期せぬ影響を与える可能性があります。タグの考慮事項と注意点を確認してください。

1. 左ペインで**「アプリケーション」を選択し、「アプリケーショングループ」**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**「アプリケーショングループの編集」**を選択します。
3. **「デリバリーグループ」**ページを選択します。
4. タグ制限を追加するには、**「タグを持つマシンへの起動を制限する」**を選択し、ドロップダウンリストからタグを選択します。
5. タグ制限を変更または削除するには、別のタグを選択するか、**このタグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。
6. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

アプリケーショングループのユーザーを追加または削除する

ユーザーの詳細については、「アプリケーショングループの作成」を参照してください。

1. 左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **ユーザー**ページを選択します。関連付けられたデリバリーグループのすべてのユーザーにアプリケーショングループ内のアプリケーションの使用を許可するか、特定のユーザーとグループ

のみに許可するかを指定します。ユーザーを追加するには、**追加**をクリックし、追加するユーザーを指定します。ユーザーを削除するには、1人以上のユーザーを選択し、**削除**をクリックします。

4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

アプリケーショングループ内のアプリケーションアイコンを追加、変更、または削除する

アプリケーションアイコンを追加、変更、または削除するには、次の手順を実行します。

1. 左ペインで **Applications** を選択します。
2. **Applications** タブで、アプリケーションを選択し、**Properties** を選択します。

   アプリケーショングループレベルで変更を行うには、**Application Groups** タブに移動し、グループ内のアプリケーションを選択して、**Properties** を選択します。
3. **Delivery** ページを選択し、**Change** を選択します。**Select Icon** ウィンドウが表示されます。
4. **Select Icon** ウィンドウで、次のいずれかを実行します。

   - アイコンを追加するには、**Add** を選択し、アイコンを参照します。
   - アイコンを削除するには、アイコンを選択し、**Remove** を選択します。
   - アイコンを変更するには、アプリケーションのアイコンを選択します。

   重要:

   - サイズが200 KBを超えるアイコンを追加することはできません。
   - .iconファイルのみを追加できます。
   - 組み込みアイコンを削除することはできません。
   - 使用中のアプリケーションのアイコンを削除することはできません。
5. **Save** を選択して変更を適用し、ウィンドウを閉じます。

アプリケーショングループのスコープを変更する

スコープは、作成した場合にのみ変更できます（「すべてのスコープ」は編集できません）。詳しくは、「委任管理」を参照してください。

1. 左側のペインで を選択し、次に タブを選択します。
2. アプリケーショングループを選択し、次にアクションバーで を選択します。
3. ページを選択します。スコープの横にあるチェックボックスをオンまたはオフにします。
4. 加えた変更を適用してウィンドウを開いたままにするには をクリックするか、変更を適用してウィンドウを閉じるには をクリックします。

アプリケーショングループのスコープを変更する

スコープを作成した場合にのみ、スコープを変更できます (すべてのスコープは編集できません)。詳細については、「委任管理」を参照してください。

1. 左側のペインで を選択し、次に タブを選択します。
2. アプリケーショングループを選択し、次にアクションバーで を選択します。
3. ページを選択します。変更するスコープの横にあるチェックボックスをオンまたはオフにします。
4. 加えた変更を適用してウィンドウを開いたままにするには を選択するか、変更を適用してウィンドウを閉じるには を選択します。

アプリケーショングループを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている必要があります。アプリケーショングループを削除した結果、1つ以上のアプリケーションがどのグループにも属さなくなった場合、そのグループを削除するとそれらのアプリケーションも削除されるという警告が表示されます。その後、削除を確定またはキャンセルできます。

アプリケーションを削除しても、元のソースから削除されるわけではありません。ただし、再度利用可能にする場合は、もう一度追加する必要があります。

1. 左側のペインで を選択し、次に タブを選択します。
2. アプリケーショングループを選択し、次にアクションバーで を選択します。
3. プロンプトが表示されたら削除を確定します。

フォルダーを使用してアプリケーション グループを整理する

フォルダーを作成してアプリケーション グループを整理し、簡単にアクセスできるようにすることができます。

必要な役割

デフォルトでは、以下の組み込みロールのいずれかを持っている場合、アプリケーショングループのフォルダーを作成および管理できます。

- クラウド管理者
- フル管理者
- アプリケーショングループ管理者

カスタム ロールを作成することで、管理アクションを他のユーザーに委任できます。次の表に、各アクションに必要な権限を示します。

アクション	必要な権限
アプリケーショングループフォルダーの作成	アプリケーショングループフォルダーの作成
アプリケーショングループフォルダーの削除	アプリケーショングループフォルダーの削除
アプリケーショングループフォルダーの移動	アプリケーショングループフォルダーの移動
アプリケーショングループフォルダーの名前変更	アプリケーショングループフォルダーの編集
アプリケーショングループをフォルダーに移動する	アプリケーショングループフォルダーの編集、アプリケーショングループプロパティの編集

詳しくは、「役割の作成と管理」を参照してください。

フォルダーの作成と管理

アクションバーまたは右クリックメニューを使用して、アプリケーショングループフォルダーを作成および管理できます。さらに、アプリケーショングループまたはフォルダーをフォルダーツリー内の目的の場所にドラッグすることもできます。

知っておくと良いこと:

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、アプリケーショングループとサブフォルダーを含めることができます。フォルダーを削除できるのは、そのフォルダーとサブフォルダーにアプリケーショングループが含まれていない場合のみです。

- すべてのノード（マシンカタログ、デリバリーグループ、アプリケーション、アプリケーショングループなど）は、バックエンドでフォルダーツリーを共有します。フォルダーの名前変更や移動時に、他のリソースフォルダーとの名前の競合を避けるため、異なるフォルダーツリー内の第一レベルフォルダーには異なる名前を付けることをお勧めします。

リモートPCアクセス

注:

Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

リモートPCアクセスは、Citrix Virtual Apps and Desktopsの機能であり、組織が従業員に企業リソースへのリモートアクセスを安全に簡単に許可できるようにします。Citrixプラットフォームは、ユーザーが物理的なオフィスPCにアクセスできるようにすることで、この安全なアクセスを可能にします。ユーザーがオフィスPCにアクセスできれば、仕事に必要なすべてのアプリケーション、データ、リソースにアクセスできます。リモートPCアクセスは、テレワークに対応するための他のツール（例えば、仮想デスクトップやアプリケーション、およびそれらに関連するインフラストラクチャなど）を導入・提供する必要性を排除します。

リモートPCアクセスは、仮想デスクトップとアプリケーションを提供するCitrix Virtual Apps and Desktopsのコンポーネントと同じものを使用します。その結果、リモートPCアクセスの展開と構成の要件およびプロセスは、仮想リソースの提供のためにCitrix Virtual Apps and Desktopsを展開する際に必要なものと同じです。この一貫性により、統一された管理エクスペリエンスが提供されます。ユーザーは、Citrix HDX™を使用してオフィスPCセッションを配信することで、最高のユーザーエクスペリエンスを得られます。

この機能は、**リモートPCアクセス**タイプのマシンカタログで構成されており、以下の機能を提供します。

- OUを指定してマシンを追加する機能。この機能により、PCの一括追加が容易になります。
- オフィスWindows PCにログオンするユーザーに基づいた自動ユーザー割り当て。シングルユーザーおよび複数ユーザーの割り当てをサポートしています。デフォルトでは、複数のユーザーを次の未割り当てマシンに自動的に割り当てます。自動割り当てを単一ユーザーに制限す

るには、Web Studioにサインインし、**設定**に移動して、**リモートPCアクセスでの複数ユーザーの自動割り当てを有効にする**設定をオフにします。

Citrix Virtual Apps and Desktopsは、他の種類のマシンカタログを使用することで、物理PCのより多くのユースケースに対応できます。これらのユースケースには、次のものが含まれます。

- 物理Linux PC
- プールされた物理PC（つまり、ランダムに割り当てられ、専用ではないもの）

注:

サポートされているOSバージョンの詳細については、シングルセッションOSおよびLinux VDAのVDAのシステム要件を参照してください。

オンプレミス展開の場合、リモートPCアクセスはCitrix Virtual Apps and Desktops AdvancedまたはPremiumライセンスでのみ有効です。セッションは、他のCitrix Virtual Desktops™セッションと同じ方法でライセンスを消費します。Citrix Cloudの場合、リモートPCアクセスはCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）およびWorkspace Premium Plusで有効です。

考慮事項

Citrix Virtual Apps and Desktops全般に適用されるすべての技術要件と考慮事項はRemote PC Accessにも適用されますが、物理PCの使用事例により関連性が高い、または排他的なものもあります。

重要:

Windows 11の物理システム（および一部のWindows 10を実行しているシステム）には、仮想化ベースのセキュリティ機能が含まれており、VDAソフトウェアがそれらを仮想マシンとして誤って検出する原因となります。この問題を軽減するには、以下のオプションがあります。

- VDAコマンドラインインストールの一部として、「/remotepc」オプションとともに「/physicalmachine」オプションを使用する

- 前述のオプションを使用しなかった場合、VDAのインストール後に以下のレジストリ値を追加します `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
  - 名前: ForceEnableRemotePC
  - 種類: DWORD
  - データ: 1

展開に関する考慮事項

Remote PC Accessの展開を計画する際には、いくつかの一般的な決定を下します。

- 既存のCitrix Virtual Apps and Desktops展開にRemote PC Accessを追加できます。このオプションを選択する前に、以下を考慮してください。
  - 現在のDelivery ControllerまたはCloud Connectorは、Remote PC Access VDAに関連する追加の負荷をサポートするのに適切なサイズですか？
  - オンプレミスサイトのデータベースおよびデータベースサーバーは、Remote PC Access VDAに関連する追加の負荷をサポートするのに適切なサイズですか？
  - 既存のVDAと新しいRemote PC Access VDAの合計が、サイトごとにサポートされる最大VDA数を超えることはありませんか？
- VDAは、自動化されたプロセスを通じてオフィスPCに展開する必要があります。利用可能なオプションは次のとおりです。
  - Electronic Software Distribution (ESD) ツール (SCCM など): SCCM を使用した VDA のインストール。
  - 展開スクリプト: スクリプトを使用した VDA のインストール。
- Remote PC Access のセキュリティに関する考慮事項 を確認してください。

注:

Remote PC Access を設計する際は、リモート PC の GPU に接続され、現在構成/動作している物理モニターの数を考慮する必要があります。モニターが Citrix セッションで使用されていなくても、GPU によって検出された場合、そのモニターの存在は GPU がサポートする最大モニター数にカウントされます。

マシンカタログに関する考慮事項

必要なマシンカタログの種類は、ユースケースによって異なります。

- Remote PC Access マシンカタログ
  - Windows 専用 PC
  - Windows 専用マルチユーザー PC。このユースケースは、複数のユーザーが異なるシフトでリモートからアクセスできる物理的なオフィス PC に適用されます。
  - プールされた Windows PC。このユースケースは、コンピューターラボなど、複数の不特定多数のユーザーがアクセスできる物理 PC に適用されます。
- シングルセッション OS マシンカタログ
  - 静的 - 専用 Linux PC
  - ランダム - プールされた Linux PC

マシンカタログの種類を特定したら、次の点を考慮してください。

- マシンは一度に1つのマシンカタログにのみ割り当てることができます。
- 委任管理を容易にするために、地理的な場所、部門、または各カタログの管理を適切な管理者に委任しやすくするその他のグループに基づいてマシンカタログを作成することを検討してください。
- マシンアカウントが存在するOUを選択する際は、より詳細な粒度を得るために下位レベルのOUを選択してください。そのような粒度が必要ない場合は、上位レベルのOUを選択できます。たとえば、Bank/Officers/Tellers の場合、より詳細な粒度を得るには **Tellers** を選択します。それ以外の場合は、要件に基づいて **Officers** または **Bank** を選択できます。
- Remote PC Access マシンカタログに割り当てられた後にOUを移動または削除すると、VDAの関連付けに影響を与え、将来の割り当てで問題が発生します。したがって、マシンカタログのOU割り当ての更新がActive Directoryの変更計画に考慮されるように、適切に計画してください。
- OU構造のためにマシンカタログにマシンを追加するOUを選択するのが容易でない場合、OUを選択する必要はありません。後でPowerShellを使用してカタログにマシンを追加できます。デスクトップの割り当てがデリバリーグループで正しく構成されていれば、ユーザーの自動割り当ては引き続き機能します。ユーザー割り当てとともにマシンカタログにマシンを追加するサンプルスクリプトは、GitHubで入手できます。
- 統合Wake on LANは、**Remote PC Access**タイプのマシンカタログでのみ利用可能です。

Linux VDAに関する考慮事項

以下の考慮事項は、Linux VDAに固有のものです。

- 物理マシンでは、Linux VDAを非3Dモードでのみ使用してください。NVIDIAドライバーの制限により、HDX 3Dモードが有効になっている場合、PCのローカル画面をブラックアウトできず、セッションのアクティビティが表示されます。この画面を表示することはセキュリティリスクです。
- 物理Linuxマシンには、シングルセッションOSタイプのマシンカタログを使用します。
- 自動ユーザー割り当てはLinuxマシンでは利用できません。
- ユーザーがすでにローカルでPCにログオンしている場合、StoreFront™からPCを起動しようとすると失敗します。
- 省電力オプションはLinuxマシンでは利用できません。

技術要件と考慮事項

このセクションでは、物理PCの技術要件と考慮事項について説明します。

- 以下はサポートされていません。
  - セッションを切断できるKVMスイッチまたはその他のコンポーネント。
  - オールインワンPCやNVIDIA Optimus搭載のノートPCおよびPCを含むハイブリッドPC。
  - デュアルブートマシン。
- キーボードとマウスはPCに直接接続してください。モニターや、電源を切ったり切断したりできるその他のコンポーネントに接続すると、これらの周辺機器が利用できなくなる可能性があります。入力デバイスをモニターなどのコンポーネントに接続する必要がある場合は、それらのコンポーネントの電源を切らないでください。
- PCはActive Directory Domain Servicesドメインに参加している必要があります。
- セキュアブートはWindows 10およびWindows 11でのみサポートされています。
- PCにはアクティブなネットワーク接続が必要です。信頼性と帯域幅を向上させるため、有線接続が推奨されます。
- Wi-Fiを使用する場合は、以下を実行します。

  a. 電源設定でワイヤレスアダプターをオンのままにするように設定します。

  b. ユーザーがログオンする前にワイヤレスネットワークに自動的に接続できるように、ワイヤレスアダプターとネットワークプロファイルを構成します。そうしないと、ユーザーが

ログオンするまでVDAは登録されません。ユーザーがログオンするまで、PCはリモートアクセスに使用できません。

c. Wi-FiネットワークからDelivery ControllerまたはCloud Connectorに到達できることを確認します。

- ノートPCでRemote PC Accessを使用できます。ノートPCがバッテリーではなく電源に接続されていることを確認してください。ノートPCの電源オプションをデスクトップPCのオプションと一致するように構成します。例：

  a. 休止状態機能を無効にします。

  b. スリープ機能を無効にします。

  c. 蓋を閉じたときの動作を**何もしない**に設定します。

  d. 「電源ボタンを押したときの動作」を**シャットダウン**に設定します。

  e. ビデオカードとNICの省電力機能を無効にします。

- Remote PC Accessは、Windows 10を搭載したSurface Proデバイスでサポートされています。前述のノートPCと同じガイドラインに従ってください。
- ドッキングステーションを使用している場合、ノートPCのドッキング解除と再ドッキングが可能です。ノートPCをドッキング解除すると、VDAはWi-Fi経由でDelivery ControllerまたはCloud Connectorに再登録されます。ただし、ノートPCを再ドッキングしても、ワイヤレスアダプターを切断しない限り、VDAは有線接続に切り替わりません。一部のデバイスには、有線接続が確立されたときにワイヤレスアダプターを切断する組み込み機能が備わっています。その他のデバイスでは、ワイヤレスアダプターを切断するためにカスタムソリューションまたはサードパーティ製ユーティリティが必要です。前述のWi-Fiに関する考慮事項を確認してください。

  Remote PC Accessデバイスのドッキングとドッキング解除を有効にするには、次の操作を行います。

  a. **スタート**メニューで、**設定 > システム > 電源とスリープ**を選択し、**スリープ**を**なし**に設定します。

  b. **デバイスマネージャー > ネットワークアダプター > イーサネットアダプター**で、**電源の管理**に移動し、**電力の節約のために、コンピューターでこのデバイスの電源をオフにできるようにする**のチェックを外します。**このデバイスで、コンピューターのスタンバイ状態を解除できるようにする**がチェックされていることを確認します。

- 同じオフィスPCにアクセスできる複数のユーザーは、Citrix Workspaceで同じアイコンを見ます。ユーザーがCitrix Workspaceにログオンすると、そのリソースが他のユーザーによってすでに使用されている場合、利用不可として表示されます。
- オフィスPCにアクセスする各クライアントデバイス（例：自宅のPC）にCitrix Workspaceアプリをインストールします。

構成シーケンス

このセクションでは、**Remote PC Access**タイプのマシンカタログを使用する場合にRemote PC Accessを構成する方法の概要を説明します。その他の種類のマシンカタログの作成方法については、マシンカタログの作成を参照してください。

1. オンプレミスサイトのみ - 統合されたWake on LAN機能を使用するには、「Wake on LAN」に記載されている前提条件を構成します。
2. Remote PC Access用に新しいCitrix Virtual Apps and Desktopsサイトが作成された場合：

   a. **Remote PC Access**サイトタイプを選択します。

   b. 「**電源管理**」ページで、デフォルトのRemote PC Accessマシンカタログの電源管理を有効または無効にするかを選択します。この設定は、後でマシンカタログのプロパティを編集して変更できます。Wake on LANの構成について詳しくは、「Wake on LAN」を参照してください。

   c. 「**ユーザー**」ページと「**マシンアカウント**」ページで情報を入力します。

   これらの手順を完了すると、**Remote PC Access Machines**という名前のマシンカタログと、**Remote PC Access Desktops**という名前のデリバリーグループが作成されます。
3. 既存のCitrix Virtual Apps and Desktopsサイトに追加する場合：

   a. **Remote PC Access**タイプのマシンカタログを作成します（ウィザードのオペレーティングシステムページ）。マシンカタログの作成方法について詳しくは、「マシンカタログの作成」を参照してください。ターゲットPCがRemote PC Accessで使用できるように、正しいOUを割り当ててください。

   b. マシンカタログ内のPCへのユーザーアクセスを提供するデリバリーグループを作成します。デリバリーグループの作成方法について詳しくは、「デリバリーグループの作成」を参照してください。デリバリーグループを、PCへのアクセスを必要とするユーザーを含むActive Directoryグループに割り当ててください。
4. オフィスPCにVDAを展開します。

- シングルセッションOSコアVDAインストーラー（VDAWorkstationCoreSetup.exe）を使用することをお勧めします。
- シングルセッションフルVDAインストーラー（VDAWorkstationSetup.exe）を`/remotepc/physicalmachine`オプションとともに使用することもできます。これは、コアVDAインストーラーを使用した場合と同じ結果になります。

> **注:**
>
> RemotePCのインストールでは、特定のユーザーシナリオでVDAが期待どおりに動作するように、`/remotepc`とともに`/physicalmachine`引数を使用します。

- ヘルプデスクチームがCitrix Directorを介してリモートサポートを提供できるように、Windowsリモートアシスタンスを有効にすることを検討してください。これを行うには、`/enable_remote_assistance`オプションを使用します。詳しくは、「コマンドラインを使用したインストール」を参照してください。
- Directorでログオン期間情報を表示できるようにするには、シングルセッションのフルVDAインストーラーを使用し、「**Citrix User Profile Management WMI Plugin**」コンポーネントを含める必要があります。このコンポーネントを含めるには、`/includeadditional`オプションを使用します。詳しくは、「コマンドラインを使用したインストール」を参照してください。
- SCCMを使用してVDAを展開する方法については、「SCCMを使用したVDAのインストール」を参照してください。
- 展開スクリプトを使用してVDAを展開する方法については、「スクリプトを使用したVDAのインストール」を参照してください。

手順2～4を正常に完了すると、ユーザーがPCにローカルでログオンしたときに、自分のマシンに自動的に割り当てられます。

5. ユーザーに、オフィスPCにリモートでアクセスするために使用する各クライアントデバイスにCitrix Workspaceアプリをダウンロードしてインストールするよう指示します。Citrix Workspaceアプリは、`https://www.citrix.com/downloads/`またはサポートされているモバイルデバイスのアプリケーションストアから入手できます。

レジストリを介して管理される機能

> **注意:**

> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは、ご自身の責任において使用してください。編集する前に、必ずレジストリをバックアップしてください。

複数ユーザーの自動割り当てを無効にする

各Delivery Controller™で、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- 名前: AllowMultipleRemotePCAssignments
- 種類: DWORD
- データ: 0

スリープモード (最小バージョン 7.16)

Remote PC Accessマシンをスリープ状態にするには、VDAにこのレジストリ設定を追加し、マシンを再起動します。再起動後、オペレーティングシステムの省電力設定が適用されます。事前設定されたアイドルタイマーが経過すると、マシンはスリープモードに入ります。マシンがウェイクアップすると、Delivery Controllerに再登録されます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前：DisableRemotePCSleepPreventer
- 種類: DWORD
- データ: 1

セッション管理

既定では、ローカルユーザーがそのマシンでセッションを開始したとき（CTRL+ALT+DELを押すことによって）、リモートユーザーのセッションは自動的に切断されます。この自動的な動作を防ぐには、オフィスPCに以下のレジストリエントリを追加し、その後、マシンを再起動します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: SasNotification
- 種類: DWORD
- データ: 1

既定では、タイムアウト期間内に接続メッセージが確認されない場合、リモートユーザーがローカルユーザーよりも優先されます。この動作を構成するには、この設定を使用します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaMode
- 種類: DWORD
- データ:
  - 1 - 指定されたタイムアウト期間内にメッセージングUIに応答しない場合、リモートユーザーが常に優先されます。この設定が構成されていない場合、この動作が既定となります。
  - 2 - ローカルユーザーが優先されます。

リモートPCアクセスモードを適用するためのタイムアウトは、デフォルトで30秒です。このタイムアウトは構成できますが、30秒より短く設定しないでください。タイムアウトを構成するには、次のレジストリ設定を使用します。

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaTimeout
- 種類: DWORD
- データ: タイムアウトの秒数（10進値）

ユーザーが強制的にコンソールアクセスを取得したい場合: ローカルユーザーは、10秒間隔でCtrl+Alt+Delを2回押すことで、リモートセッションのローカル制御を取得し、切断イベントを強制できます。

レジストリ変更とマシンの再起動後、リモートユーザーが使用中にローカルユーザーがCtrl+Alt+Delを押してそのPCにログオンしようとすると、リモートユーザーにプロンプトが表示されます。このプロンプトでは、ローカルユーザーの接続を許可するか拒否するかを尋ねます。接続を許可すると、リモートユーザーのセッションは切断されます。

セッション管理のログ記録

リモートPCアクセスには、アクティブなICA®セッションを持つPCに誰かがアクセスしようとしたときにログを記録するログ機能が追加されました。これにより、不要なアクティビティや予期しないアクティビティがないか環境を監視し、インシデントを調査する必要がある場合にそのようなイベントを監査できます。

イベントはWindowsイベントビューアーを使用してログに記録され、**アプリケーションとサービス > Citrix > HostCore > ICA Service > Admin**にあります。

リモートPCアクセスを使用すると、3つの異なるイベントがログに記録されます。

Ctrl+Alt+Delイベント

このイベントは、アクティブなリモートセッション中にローカルユーザーがコンソールキーボードでCtrl+Alt+Delを押したときに表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 43, 44, 45
- ソース: ICA サービス

イベント ID 43

このイベントIDは、SasNotification レジストリ値が存在しない場合、または SasNotification レジストリ値が 0 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to automatically disconnect the
remote session.
```

イベント ID 44

このイベントIDは、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 1 の場合、または RpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user. The
user preference is set to remote user.
```

イベント ID 45

このイベントIDは、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 2 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user.

The user preference is set to local user.
```

リモートセッション切断イベント

このイベントは、さまざまな理由でリモートセッションが切断された場合に表示されます。

イベント詳細

- ログ名: アプリケーションとサービス
- イベント ID: 46, 47, 48
- ソース: ICA Service

イベントID 46

このイベントIDは、リモートセッションが切断され、SasNotificationレジストリ値が存在しないか、SasNotificationレジストリ値が0の場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected.
```

イベントID 47

このイベントIDは、リモートユーザーがセッションの切断に同意し、SasNotificationレジストリ値が1で、RpcaModeレジストリ値が1、またはRpcaModeレジストリ値が2、またはRpcaModeレジストリ値が存在しない場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user accepted the request to disconnect the session.
```

イベントID 48

このイベントIDは、リモートユーザーが指定されたタイムアウト期間内に切断要求を拒否せず、SasNotificationレジストリ値が1で、RpcaModeレジストリ値が2の場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user did not decline the disconnection request within the
configured timeout period (&lt;timeout period>).
```

Ctrl+Alt+Del 2回押しイベント

このイベントは、Ctrl+Alt+Delが10秒以内に2回押された場合に表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 49
- ソース: ICA Service

イベントID 49

このイベントIDは、Ctrl+Alt+Delが10秒以内に2回押されたときに表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been forcibly
disconnected.
```

ウェイク・オン・LAN

Remote PC AccessはWake on LANをサポートしており、ユーザーは物理PCをリモートで起動できます。この機能により、ユーザーは使用していないときにオフィスPCの電源を切ったままにして、エネルギーコストを節約できます。また、誤ってマシンの電源が切れてしまった場合でも、リモートアクセスを可能にします。

Wake on LAN機能を使用すると、デリバリーコントローラーからの指示があった場合、PC上で実行されているVDAから、そのPCが存在するサブネットにマジックパケットが直接送信されます。これにより、追加のインフラストラクチャコンポーネントやマジックパケット配信のためのサードパーティソリューションに依存することなく、この機能が動作します。

Wake on LAN機能は、従来のSCCMベースのWake on LAN機能とは異なります。SCCMベースのWake on LANの詳細については、「Wake on LAN – SCCM-integrated」を参照してください。

制限事項

Wake on LAN機能を使用するRemote PC Accessは、ピーク時の自動電源オンをサポートしていません。

システム要件

Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- コントロールプレーン:
  - シトリックス DaaS™
  - Citrix Virtual Apps and Desktops 2009 以降のバージョン
- 物理PC:
  - VDAバージョン2009以降
  - Windows 10またはWindows 11。サポートの詳細については、VDAシステム要件を参照してください。
  - BIOS/UEFIでWake on LANが有効になっていること
  - Windows構成内のネットワークアダプターのプロパティでWake on LANが有効になっていること

Wake on LANの構成

オンプレミスのCitrix Virtual Apps and Desktopsを使用している場合、統合されたWake on LANの構成はPowerShellを使用してのみサポートされます。

Wake on LANを構成するには:

1. Remote PC Accessマシンカタログがまだない場合は作成します。
2. Wake on LANホスト接続がまだない場合は作成します。

> **注:**
>
> Wake on LAN機能を使用するには、「Microsoft Configuration Manager Wake on LAN」タイプのホスト接続がある場合、新しいホスト接続を作成します。

3. Wake on LANホスト接続の一意の識別子を取得します。
4. Wake on LANホスト接続をマシンカタログに関連付けます。

Wake on LAN ホスト接続を作成するには：

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `

                -ConnectionType Custom `

                -PluginId VdaWOLMachineManagerFactory `

                -CustomProperties "<CustomProperties></CustomProperties>"
`

                -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid



# Wait for the connection to be ready before trying to use it
```

```
while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

}
```

ホスト接続の準備ができたら、次のコマンドを実行してホスト接続の一意の識別子を取得します。

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

接続の一意の識別子を取得したら、次のコマンドを実行して、その接続を Remote PC Access マシンカタログに関連付けます。

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

設計上の考慮事項

Remote PC Access で Wake on LAN を使用する予定がある場合は、次の点を考慮してください。

- 複数のマシンカタログで同じWake on LANホスト接続を使用できます。
- あるPCが別のPCを起動するには、両方のPCが同じサブネット内にあり、同じWake on LANホスト接続を使用する必要があります。PCが同じマシンカタログにあるか異なるマシンカタログにあるかは関係ありません。
- ホスト接続は特定のゾーンに割り当てられます。展開に複数のゾーンが含まれている場合は、各ゾーンにWake on LANホスト接続が必要です。これはマシンカタログにも当てはまります。
- マジックパケットは、グローバルブロードキャストアドレス255.255.255.255を使用してブロードキャストされます。このアドレスがブロックされていないことを確認してください。
- そのサブネット内のマシンを起動できるようにするには、Wake on LAN接続ごとに、サブネット内で少なくとも1台のPCがオンになっている必要があります。

運用上の考慮事項

Wake on LAN機能を使用する際の考慮事項は次のとおりです。

- 統合されたWake on LAN機能を使用してPCを起動するには、VDAが少なくとも1回登録されている必要があります。
- Wake on LANはPCの起動にのみ使用できます。再起動やシャットダウンなどの他の電源操作はサポートしていません。
- Wake on LAN接続が作成されると、Web Studioに表示されます。ただし、Citrix Virtual Apps and Desktopsオンプレミスを使用している場合、Web Studio内でのプロパティの編集はサポートされていません。
- マジックパケットは次の2つの方法のいずれかで送信されます。

  a. ユーザーがPCへのセッションを起動しようとし、VDAが登録されていない場合

  b. 管理者がWeb StudioまたはPowerShellから手動で電源オンコマンドを送信する場合

- デリバリーコントローラーはPCの電源状態を認識しないため、Web Studioでは電源状態の下に**サポートされていません**と表示されます。デリバリーコントローラーは、VDAの登録状態を使用してPCのオン/オフを判断します。

Wake on LAN – SCCM統合

SCCM統合Wake on LANは、オンプレミスのCitrix Virtual Apps and Desktopsでのみ利用可能な、Remote PC Accessの代替Wake on LANオプションです。

システム要件

SCCM統合Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- Citrix Virtual Apps and Desktops 1912 以降のバージョン
- 物理PC:
  - VDAバージョン1912以降
  - Windows 10。サポートの詳細については、VDAシステム要件を参照してください。
  - BIOS/UEFIでWake on LANが有効になっていること
  - Windows構成内のネットワークアダプターのプロパティでWake on LANが有効になっていること
- システムセンター コンフィギュレーションマネージャー (SCCM) 2012 R2 以降

SCCM統合型Wake on LANの構成

以下の前提条件を満たしてください。

1. 組織内でSCCM 2012 R2、2016、または2019を構成します。次に、すべてのRemote PC AccessマシンにSCCMクライアントを展開し、スケジュールされたSCCMインベントリサイクルが実行されるのを待つか、必要に応じて手動で強制実行します。
2. Wake Proxyのサポートについては、SCCMでオプションを有効にします。Remote PC AccessのWake on LAN機能を使用するPCを含む組織内の各サブネットについて、3台以上のマシンがセンチネルマシンとして機能できることを確認してください。
3. マジックパケットのサポートについては、サブネット指向ブロードキャストまたはユニキャストのいずれかを使用して、マジックパケットの送信を許可するようにネットワークルーターとファイアウォールを構成します。
4. 各PCのBIOS/UEFI設定でWake on LANを構成します。
5. まだVDAを展開していない場合は、物理PCにVDAを展開します。

前提条件を満たしたら、Delivery ControllerがSCCMと通信できるように、以下の手順を完了します。

1. SCCMのホスト接続を作成します。詳細については、「接続とリソース」を参照してください。
    - 接続の種類として、**Microsoft Configuration Manager Wake on LAN**を選択します。
    - 入力された資格情報には、スコープ内のコレクションへのアクセス権があり、**Remote Tools Operator**の役割が必要です。
2. Web Studioで接続を選択し、**接続の編集**を選択して、**詳細設定**をクリックします。
3. Wake on LANの処理に適したオプションを選択します。
    - Wake-upプロキシを使用している場合は、最初のオプションである**Microsoft System Center Configuration Manager Wake-upプロキシ**を選択します。
    - マジックパケットを使用している場合は、2番目のオプションである**Delivery Controllerによって送信されるWake on LANパケット**を選択します。
        - 適切な送信方法（**サブネット指向ブロードキャスト**または**ユニキャスト**）を選択します。

ホスト接続を作成したら、その接続をRemote PC Accessカタログに関連付けます。

- 新しいRemote PC Accessカタログを作成する場合は、カタログ作成ウィザードの**オペレーティングシステム**ページで、カタログの種類として**Remote PC Access**を選択し、ドロップダウンリストから適切な接続を選択します。
- 既存のRemote PC AccessカタログにWake on LANを追加するには：

  a. Web Studioの**マシンカタログ**ノードに移動し、マシンカタログを選択して、**マシンカタログの編集**を選択します。

  b. **電源管理**タブを選択し、**はい**を選択してマシンカタログの電源管理を有効にします。

  c. ドロップダウンリストから適切な接続を選択し、**OK**をクリックします。

トラブルシューティング

モニターのブランキングが機能しない

アクティブなHDXセッション中にWindows PCのローカルモニターがブランクにならない場合（ローカルモニターにセッションで発生していることが表示される場合）、GPUベンダーのドライバーに問題がある可能性があります。この問題を解決するには、次のレジストリ値を設定して、Citrix Indirect Displayドライバー（IDD）にグラフィックカードのベンダードライバーよりも高い優先順位を付与します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名前：CitrixIDD
- 種類：DWORD
- データ：3

ディスプレイアダプターの優先順位とモニターの作成について詳しくは、Knowledge Centerの記事CTX237608を参照してください。

セッション管理通知が有効になっているマシンでCtrl+Alt+Delを選択すると、セッションが切断されます

SasNotificationレジストリ値によって制御されるセッション管理通知は、VDAでRemote PC Accessモードが有効になっている場合にのみ機能します。物理PCでHyper-Vの役割または仮想化ベースのセキュリティ機能が有効になっている場合、そのPCは仮想マシンとして報告されます。VDAが仮想マシン上で実行されていることを検出すると、Remote PC Accessモードを自動的に無効にします。Remote PC Accessモードを有効にするには、次のレジストリ値を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC

- 種類: DWORD
- データ: 1

設定を有効にするには、PCを再起動します。

診断情報

Remote PC Accessに関する診断情報は、Windowsアプリケーションイベントログに書き込まれます。情報メッセージはスロットリングされません。エラーメッセージは、重複するメッセージを破棄することでスロットリングされます。

- 3300（情報）: マシンがカタログに追加されました
- 3301（情報）: マシンがデリバリーグループに追加されました
- 3302（情報）: マシンがユーザーに割り当てられました
- 3303 (エラー): 例外

電源管理

リモートPCアクセスの電源管理が有効になっている場合、サブネット指向ブロードキャストでは、コントローラーとは異なるサブネットにあるマシンを起動できないことがあります。サブネット指向ブロードキャストを使用してサブネット間で電源管理が必要で、AMTサポートが利用できない場合は、Wake-upプロキシまたはユニキャスト方式を試してください。これらの設定が電源管理接続の詳細プロパティで有効になっていることを確認してください。

アクティブなリモートセッションはローカルのタッチスクリーン入力を記録します

VDAがリモートPCアクセスモードを有効にすると、アクティブなセッション中にマシンはローカルのタッチスクリーン入力を無視します。物理PCにHyper-Vロールまたは仮想化ベースのセキュリティ機能が有効になっている場合、PCは仮想マシンとして報告されます。VDAが仮想マシン上で実行されていることを検出すると、リモートPCアクセスモードを自動的に無効にします。リモートPCアクセスモードを有効にするには、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PC を再起動してください。

その他のリソース

リモートPCアクセスに関するその他のリソースは次のとおりです。

- ソリューション設計ガイダンス: Remote PC Access Design Decisions。
- リモートPCアクセスアーキテクチャの例: Reference Architecture for Citrix Remote PC Access Solution。

コンテンツを公開する

> **注:**
>
> Citrix Virtual Apps and Desktops™の展開は、Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> Microsoft WordドキュメントやWebリンクなどのリソースへのURLまたはUNCパスであるアプリケーションを公開できます。この機能は公開コンテンツとして知られています。コンテンツを公開する機能により、ユーザーへのコンテンツ配信方法に柔軟性が加わります。既存のアクセス制御とアプリケーション管理の恩恵を受けることができます。また、コンテンツを開くためにローカルアプリケーションを使用するか、公開アプリケーションを使用するかを指定することもできます。

公開されたコンテンツは、StoreFront™およびCitrix Workspace™アプリの他のアプリケーションと同様に表示されます。ユーザーはアプリケーションにアクセスするのと同じ方法でアクセスします。クライアントでは、リソースは通常どおり開きます。

- ローカルにインストールされたアプリケーションが適切な場合、そのアプリケーションが起動されてリソースが開かれます。
- ファイルの種類関連付けが定義されている場合、公開されたアプリケーションが起動されてリソースが開かれます。

コンテンツはPowerShell SDKを使用して公開します。Web Studioを使用してコンテンツを公開することはできません。ただし、公開後にWeb Studioを使用してアプリケーションのプロパティを編集することはできます。

構成の概要と準備

コンテンツの公開には、次の主要なプロパティを持つ`New-BrokerApplication`コマンドレットを使用します。（すべてのコマンドレットプロパティの説明については、コマンドレットのヘルプを参照してください。）

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

`ApplicationType`プロパティは`PublishedContent`である必要があります。

`CommandLineExecutable`プロパティは、公開コンテンツの場所を指定します。以下の形式がサポートされており、255文字の制限があります。

- HTMLウェブサイトアドレス（例: `<http://www.citrix.com>`）
- ウェブサーバー上のドキュメントファイル（例: `https://www.citrix.com/press/pressrelease.doc`）
- FTPサーバー上のディレクトリ（例: `ftp://ftp.citrix.com/code`）
- FTPサーバー上のドキュメントファイル（例: `ftp://ftp.citrix.com/code/Readme.txt`>）
- UNC ディレクトリパス (例: `file://myServer/myShare or \\\\myServer\\myShare`)
- UNC ファイルパス (例: `file://myServer/myShare/myFile.asf` または `\\myServer\myShare\myFile.asf`)

正しいSDKがあることを確認してください。

- Citrix DaaS (旧Citrix Virtual Apps and Desktopsサービス) の展開の場合、ダウンロード して、Citrix Virtual Apps and Desktops Remote PowerShell SDKをインストールします。
- オンプレミスのCitrix Virtual Apps and Desktops展開の場合、Delivery Controllerとともにインストールされているの PowerShell SDKを使用します。公開コンテンツアプリケーションを追加するには、最低バージョン7.11のDelivery Controllerが必要です。

以下の手順では例を使用しています。例では次のようになります。

- マシンカタログが作成されています。
- `PublishedContentApps`という名前のデリバリーグループが作成されています。このグループは、カタログからマルチセッションOSマシンを使用します。WordPadアプリケーションがグループに追加されています。

- デリバリーグループ名、`CommandLineExecutable` の場所、およびアプリケーション名が割り当てられます。

はじめに

PowerShell SDKを含むマシンでPowerShellを開きます。

次のコマンドレットは、適切なPowerShell SDKスナップインを追加し、返されたデリバリーグループレコードを割り当てます。

`Add-PsSnapin Citrix* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps`

Citrix DaaSを使用している場合は、Citrix Cloud™の資格情報を入力して認証します。複数の顧客がいる場合は、いずれかを選択します。

URLを公開する

場所とアプリケーション名を割り当てた後、以下のコマンドレットは、Citrixのホームページをアプリケーションとして公開します。

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"



New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

成功を確認します:

- StoreFrontを開き、PublishedContentAppsデリバリーグループ内のアプリケーションにアクセスできるユーザーとしてログオンします。表示には、デフォルトのアイコンが付いた新しく作成されたアプリケーションが含まれています。アイコンのカスタマイズについては、`<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`を参照してください。
- **Citrix Home Page**アプリケーションをクリックします。URLは、ローカルで実行されているデフォルトブラウザの新しいタブで起動します。

UNCパスにあるリソースを公開する

この例では、管理者はすでに`PublishedResources`という名前の共有を作成しています。場所とアプリケーション名を割り当てた後、以下のコマンドレットは、その共有内のRTFファイルとDOCXファイルをリソースとして公開します。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"

$docxAppName = "PublishedDOCX"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

成功を確認する:

- StoreFrontウィンドウを更新して、新しく公開されたドキュメントを表示します。
- **PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。各ドキュメントは、ローカルで実行されているWordPadで開きます。

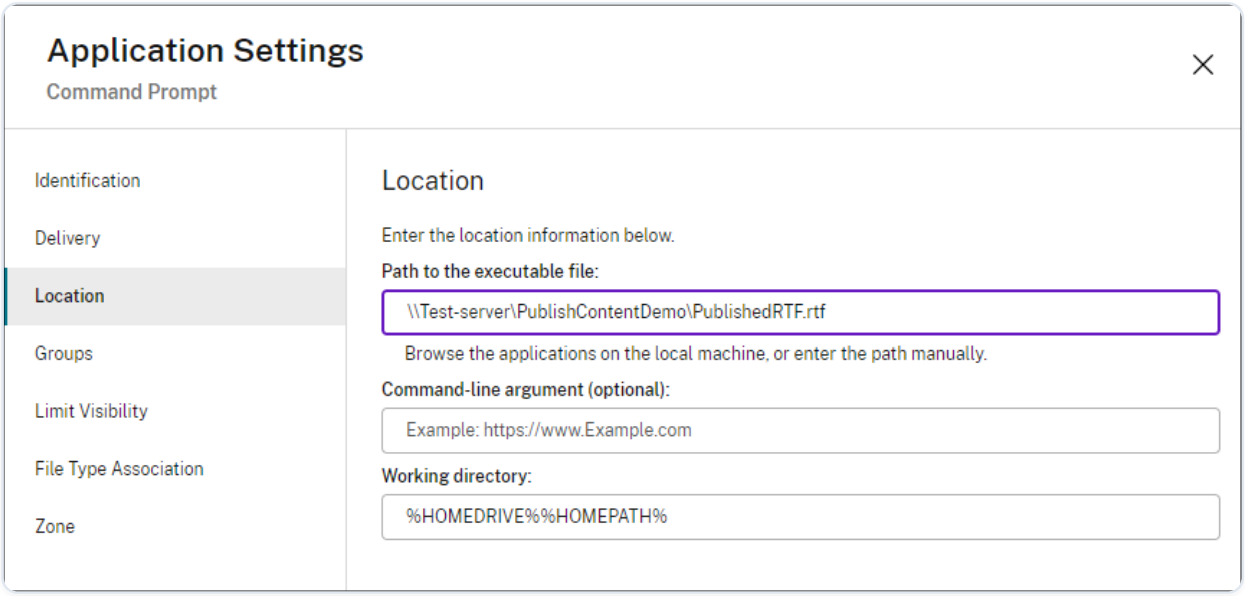
PublishedContentアプリケーションの表示と編集

公開されたコンテンツは、他のアプリケーションタイプに使用するのと同じ方法で管理します。

`PublishedContent`アプリケーションを表示および編集するには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで**Applications**を選択します。
2. **Applications**タブで、PublishedContentアプリケーションを選択し、**Properties**を選択します。

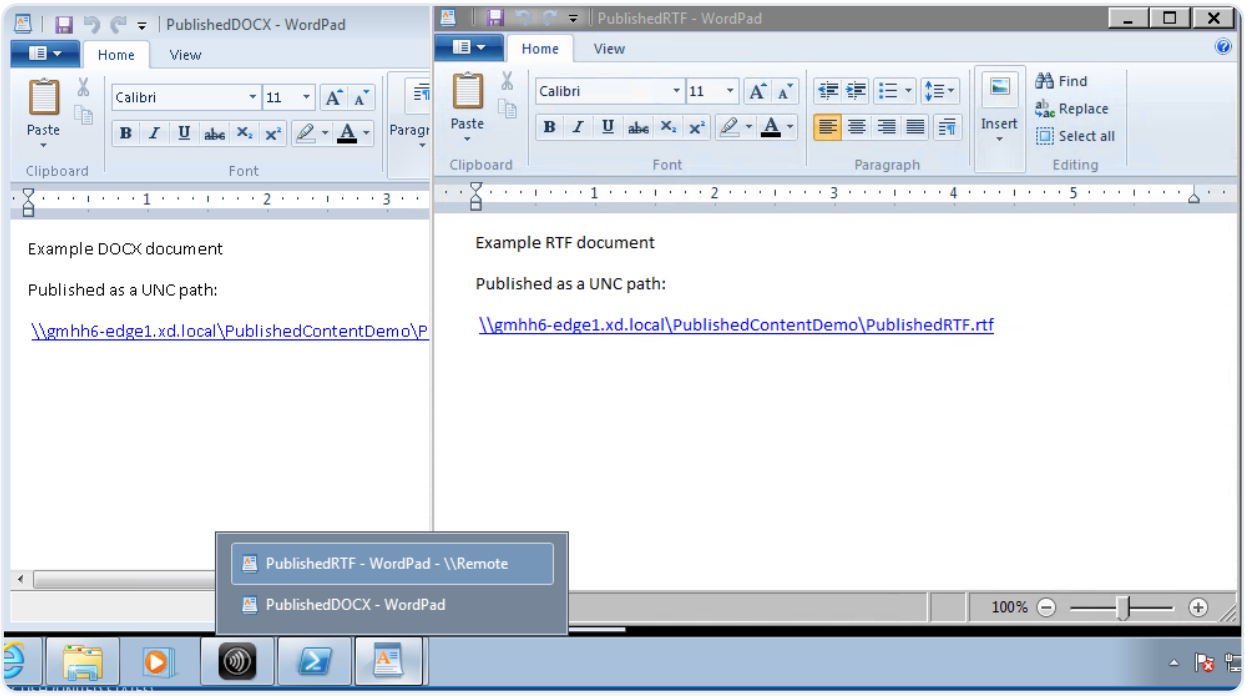
   アプリケーションのプロパティ（ユーザーの可視性、グループの関連付け、ショートカットなど）は、公開されたコンテンツに適用されます。ただし、**場所**ページでは、コマンドライン引数または作業ディレクトリのプロパティを変更することはできません。
3. リソースを変更するには、そのページの**実行可能ファイルへのパス**フィールドを変更します。



4. 公開アプリケーションを使用して`PublishedContent`アプリケーション（ローカルアプリケーションではなく）を開くには、次の手順に従います。

   この例では、公開されたWordPadアプリケーションが編集され、.rtfファイル用のファイルタイプ関連付けが作成されます。

   a. デリバリーグループのメンテナンスモードをオンにします。
   b. **ファイルタイプ関連付け**プロパティを編集します。
   c. 完了したら、メンテナンスモードをオフにします。
   d. StoreFrontを更新してファイルタイプ関連付けの変更を読み込み、**PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。違いに注目してください。**PublishedDOCX**は引き続きローカルのWordPadで開きます。しかし、**PublishedRTF**はファイルタイプ関連付けにより、公開されたWordPadで開くようになりました。



詳細情報

- マシンカタログを作成する
- デリバリーグループを作成する
- アプリケーションプロパティを変更する

サーバー VDI

Server VDI (Virtual Desktop Infrastructure) 機能を使用して、単一ユーザー向けにサーバーオペレーティングシステムからデスクトップを配信します。

- エンタープライズ管理者は、サーバーオペレーティングシステムをVDIデスクトップとして配信できます。これは、エンジニアやデザイナーなどのユーザーにとって価値があります。
- サービスプロバイダーは、クラウドからデスクトップを提供できます。これらのデスクトップは、Microsoft Services Provider License Agreement (SPLA) に準拠しています。

サポート:

- Citrix Virtual Apps and Desktops™ および Citrix DaaS (旧 Citrix Virtual Apps and Desktops service) の展開では、Server VDI は Windows Server 2022、Windows Server 2019、および Windows Server 2016 でサポートされています。
- すべてのServer VDI展開は、ユーザーパーソナライゼーションレイヤーテクノロジーをサポートしています。

- Server VDIがスキャナーなどのTWAINデバイスで動作するには、Windows Serverのデスクトップエクスペリエンス機能がインストールされている必要があります。
- 以下の機能はServer VDIでは使用できません:
  - ホスト型アプリケーション
  - ローカルアプリアクセス
  - 直接（ブローカーなし）デスクトップ接続
  - リモートPCアクセス

Server VDIのインストールと構成

1. Windowsサーバーをインストール用に準備します。
   - Windows Server Manager を使用して、リモートデスクトップサービス役割サービスがインストールされていないことを確認します。以前にインストールされていた場合は、削除してください。これらの役割サービスがインストールされている場合、VDA のインストールは失敗します。
   - **各ユーザーを単一セッションに制限する** プロパティが有効になっていることを確認します。Windows サーバーで、ターミナルサーバー設定のレジストリを編集します。

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

     `DWORD fSingleSessionPerUser = 1`
2. Citrix Virtual Apps and Desktops インストーラーのコマンドラインインターフェイスを使用して、サポートされているサーバーまたはサーバーマスターイメージに VDA をインストールし、`/quiet` および `/servervdi` オプションを指定します。(デフォルトでは、インストーラーのグラフィカルインターフェイスは、サーバーオペレーティングシステム上の Windows シングルセッション OS VDA をブロックします。コマンドラインを使用すると、この動作が上書きされます。) 次のいずれかのコマンドを使用します。
   - Citrix Virtual Apps and Desktops 展開の場合:
     - `XenDesktopVdaSetup.exe /quiet /servervdi`
     - `VDAWorkstationSetup.exe /quiet /servervdi`
   - Citrix DaaS™ 展開の場合:
     - `VDAWorkstationSetup.exe /quiet /servervdi`

   その他のオプション:

- Delivery Controller または Cloud Connector を指定するには、`/controllers` を使用します。
- ファイアウォールを手動で構成する場合を除き、ファイアウォールでポートを開くには `/enable_hdx_ports` を使用します。
- イメージに VDA をインストールし、そのイメージから MCS を使用してサーバー VM を作成する場合は、`/mastermcsimage` (または `/masterimage`) を使用します。
- すべてのオプションの詳細については、「コマンドラインを使用したインストール」を参照してください。

3. Server VDI用のマシンカタログを作成します。カタログ作成ウィザードで:
   - **オペレーティングシステム**ページで、**シングルセッションOS**を選択します。
   - **概要**ページで、Server VDI であることを明確に識別できるマシンカタログ名と管理者向けの記述を指定します。これは、カタログがServer VDIをサポートしていることをStudioで示す唯一のインジケーターです。

   Studioで検索を使用すると、VDAがマルチセッションマシンにインストールされている場合でも、Server VDIカタログは**シングルセッションOSマシン**タブに表示されます。
4. デリバリーグループを作成し、作成したServer VDIカタログを選択します。

VDAのインストール中にDelivery ControllerまたはCloud Connectorを指定しなかった場合は、後でそれらを指定することを忘れないでください。詳細については、「VDA登録」を参照してください。

ユーザーパーソナライゼーションレイヤー

> **注:**

> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> Citrix Virtual Apps and Desktopsのユーザーパーソナライゼーションレイヤー機能は、非永続マシンカタログの機能を拡張し、ユーザーのデータとローカルにインストールされたアプリケーションをセッション間で保持します。基盤となるCitrix App Layeringテクノロジーを搭載

したユーザーパーソナライゼーションレイヤー機能は、非永続マシンカタログでCitrix ProvisioningおよびMachine Creation Services™ (MCS) をサポートします。

マスターイメージ内でVirtual Delivery Agentとともにユーザーパーソナライゼーションレイヤーコンポーネントをインストールします。VHDファイルには、ユーザーがローカルにインストールしたアプリケーションが保存されます。イメージにマウントされたVHDは、ユーザー自身の仮想ハードドライブとして機能します。

重要:

Citrix Virtual Apps and Desktopsでユーザーパーソナライゼーションレイヤーを展開するか、イメージテンプレートで有効になっているApp Layeringユーザーレイヤーを展開することができますが、両方を展開することはできません。App Layering内のレイヤーにユーザーパーソナライゼーションレイヤー機能をインストールしないでください。

この機能はPersonal vDisk (PvD) に代わるものであり、非永続的な（プールされた）デスクトップ環境でユーザーに永続的なワークスペースエクスペリエンスも提供します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、記事に詳述されている手順を使用してインストールおよび構成します。

アプリケーションのサポート

以下の例外を除き、ユーザーがデスクトップにローカルでインストールするすべてのアプリケーションは、ユーザーパーソナライゼーションレイヤーでサポートされます。

例外

以下のアプリケーションは例外であり、ユーザーパーソナライゼーションレイヤーではサポートされません。

- MS OfficeやVisual Studioなどのエンタープライズアプリケーション。
- ネットワークスタックまたはハードウェアを変更するアプリケーション。例：VPNクライアント。
- ブートレベルドライバーを持つアプリケーション。例：ウイルススキャナー。
- ドライバー ストアを使用するドライバーを持つアプリケーション。例：プリンター ドライバー。

> **注：**
>
> Windowsグループポリシーオブジェクト（GPO）を使用してプリンターを利用可能にできます。

サポートされていないアプリケーションをユーザーがローカルにインストールすることを*許可しないでください*。代わりに、これらのアプリケーションをマスターイメージに直接インストールしてください。

ローカルユーザーまたは管理者アカウントを必要とするアプリケーション

ユーザーがアプリケーションをローカルにインストールすると、そのアプリはユーザーレイヤーに入ります。その後、ユーザーがローカルユーザーまたはグループを追加または編集しても、変更はセッションを超えて保持されません。

> **重要：**
>
> 必要なローカルユーザーまたはグループは、マスターイメージに追加してください。

要件

ユーザーパーソナライゼーションレイヤー機能には、次のコンポーネントが必要です。

- Citrix Virtual Apps and Desktops のバージョン 7 1909 以降
- Virtual Delivery Agent (VDA)、バージョン1912以降
- Citrix Provisioning™、バージョン1909以降
- Windowsファイル共有（SMB）、またはオンプレミスAD認証が有効なAzure Files

ユーザーパーソナライゼーションレイヤー機能は、OSがシングルセッションとして展開されている場合、以下のWindowsバージョンで展開できます。サポートは、シングルセッション上の単一ユーザーに限定されます。

- ウィンドウズ 11 エンタープライズ x64
- Windows 10 Enterprise x64、バージョン1607以降
- ウィンドウズ サーバー 2016 (Azure Files対応)
- ウィンドウズ サーバー 2019 (Azure Files対応)
- ウィンドウズ サーバー 2022 (Azure Files対応)

Citrix Virtual Apps and Desktops 7の場合、Azure Filesとユーザーパーソナライゼーションレイヤーの使用は、Windows Server 2022、Windows Server 2019、Windows Server 2016、およびWindows 10クライアントでサポートされています。

> **注:**
>
> サーバーOSを使用している場合、Server VDIのみがサポートされます。展開の詳細については、Server VDIの記事を参照してください。

> ユーザーパーソナライゼーションレイヤーは、マシンごとに一度に1人のユーザーのみをサポートし、その後、ディスクをリセットするためにマシンを再起動する必要があります。ユーザーパーソナライゼーションレイヤーは、マルチセッションサーバーオペレーティングシステムでは使用できず、シングルセッションサーバーシステムでのみ使用できます。ユーザーパーソナライゼーションレイヤーは、非永続デスクトップのみでサポートされています。

> ユーザーパーソナライゼーションレイヤー機能がインストールされている場合は、アンインストールします。最新リリースをインストールする前に、マスターイメージを再起動します。

ファイル共有を設定する

ユーザーパーソナライゼーションレイヤー機能には、Windows Server Message Block (SMB) ストレージが必要です。Windowsファイル共有を作成するには、使用しているWindowsオペレーティングシステムの通常の手順に従ってください。

Azureベースのカタログでは Azure Filesを使用する方法の詳細については、「ユーザーパーソナライゼーションレイヤー用のAzure Filesストレージを設定する」を参照してください。

推奨事項

ユーザーパーソナライゼーションレイヤーの展開を成功させるには、このセクションの推奨事項に従ってください。

マイクロソフト システムセンター コンフィグレーションマネージャー (SCCM)

ユーザーパーソナライゼーションレイヤー機能でSCCMを使用している場合は、VDI環境でイメージを準備するためのMicrosoftのガイドラインに従ってください。詳細については、このMicrosoft TechNet記事を参照してください。

ユーザーレイヤーのサイズ

ユーザーレイヤーは、ディスク上のスペースが使用されるにつれて拡張するシンプロビジョニングディスクです。ユーザーレイヤーに許可されるデフォルトサイズは10 GBで、これは推奨される最小値です。

> **注：**
>
> インストール中に値がゼロ（0）に設定されている場合、デフォルトのユーザーレイヤーサイズは10 GBに設定されます。

> ユーザーレイヤーのサイズを変更したい場合は、**User Layer Size**ポリシーに別の値を入力できます。「**Optional: Click Select next to User Layer Size in GB.**」の下にある「**Step 5: Create delivery group custom policies**」を参照してください。

ユーザーレイヤーサイズを上書きするためのツール（オプション）

Windowsツールを使用してユーザーレイヤーファイル共有にクォータを定義することで、ユーザーレイヤーのサイズを上書きできます。

Usersという名前のユーザーレイヤーディレクトリにハードクォータを設定するには、次のMicrosoftクォータツールのいずれかを使用します。

- ファイルサーバーリソースマネージャー (FSRM)
- クォータマネージャー

> **注：**
>
> クォータを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。クォータを減らすと、新しいユーザーレイヤーのみに影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

ユーザーパーソナライゼーションレイヤーを展開する

ユーザーパーソナライゼーション機能を展開する際は、Web Studio内でポリシーを定義します。その後、その機能を展開するマシンカタログにバインドされたデリバリーグループにポリシーを割り当てます。

マスターイメージにユーザーパーソナライゼーションレイヤーの設定がない場合、サービスはアイドル状態のままであり、オーサリングアクティビティを妨げません。

マスターイメージでポリシーを設定すると、サービスはマスターイメージ内でユーザーレイヤーを実行およびマウントしようとします。マスターイメージは予期しない動作や不安定性を示します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、以下の手順をこの順序で完了します。

- ステップ1：Citrix Virtual Apps and Desktops環境の可用性を確認します。
- ステップ2：マスターイメージを準備します。
- ステップ3：マシンカタログを作成します。
- ステップ4：デリバリーグループを作成します。
- ステップ5：デリバリーグループのカスタムポリシーを作成します。

> **注：**
>
> イメージ上でWindows 10をアップグレードした後、初めてログインする際には通常よりも時間がかかります。ユーザーレイヤーが新しいバージョンのWindows 10用に更新される必要があり、その結果、ログオン時間が増加します。

ステップ1：Citrix Virtual Apps and Desktops環境が利用可能であることを確認します

この新機能を使用するために、Citrix Virtual Apps and Desktops環境が利用可能であることを確認してください。セットアップの詳細については、「Citrix Virtual Apps and Desktopsのインストールと構成」を参照してください。

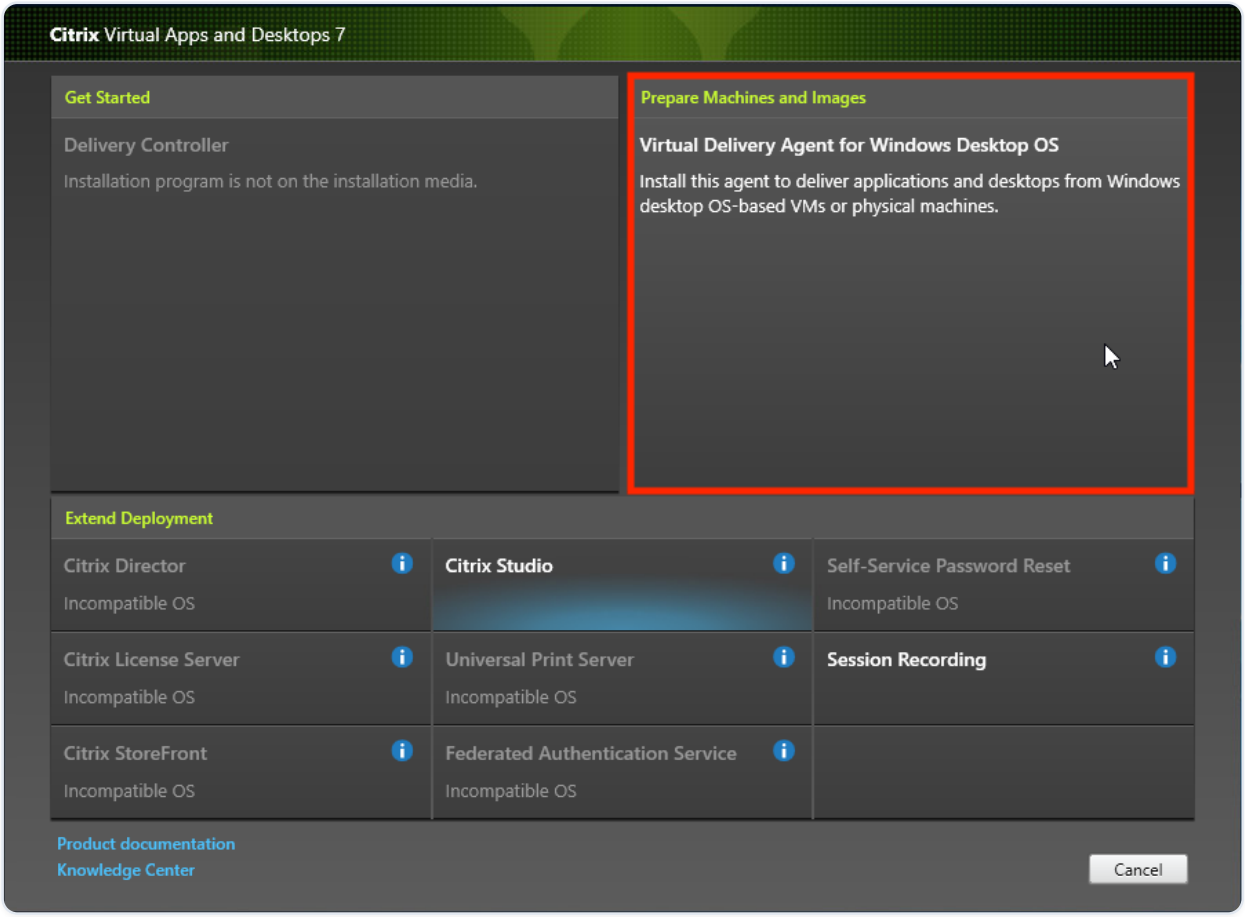
ステップ2：マスターイメージを準備します

マスターイメージを準備するには:

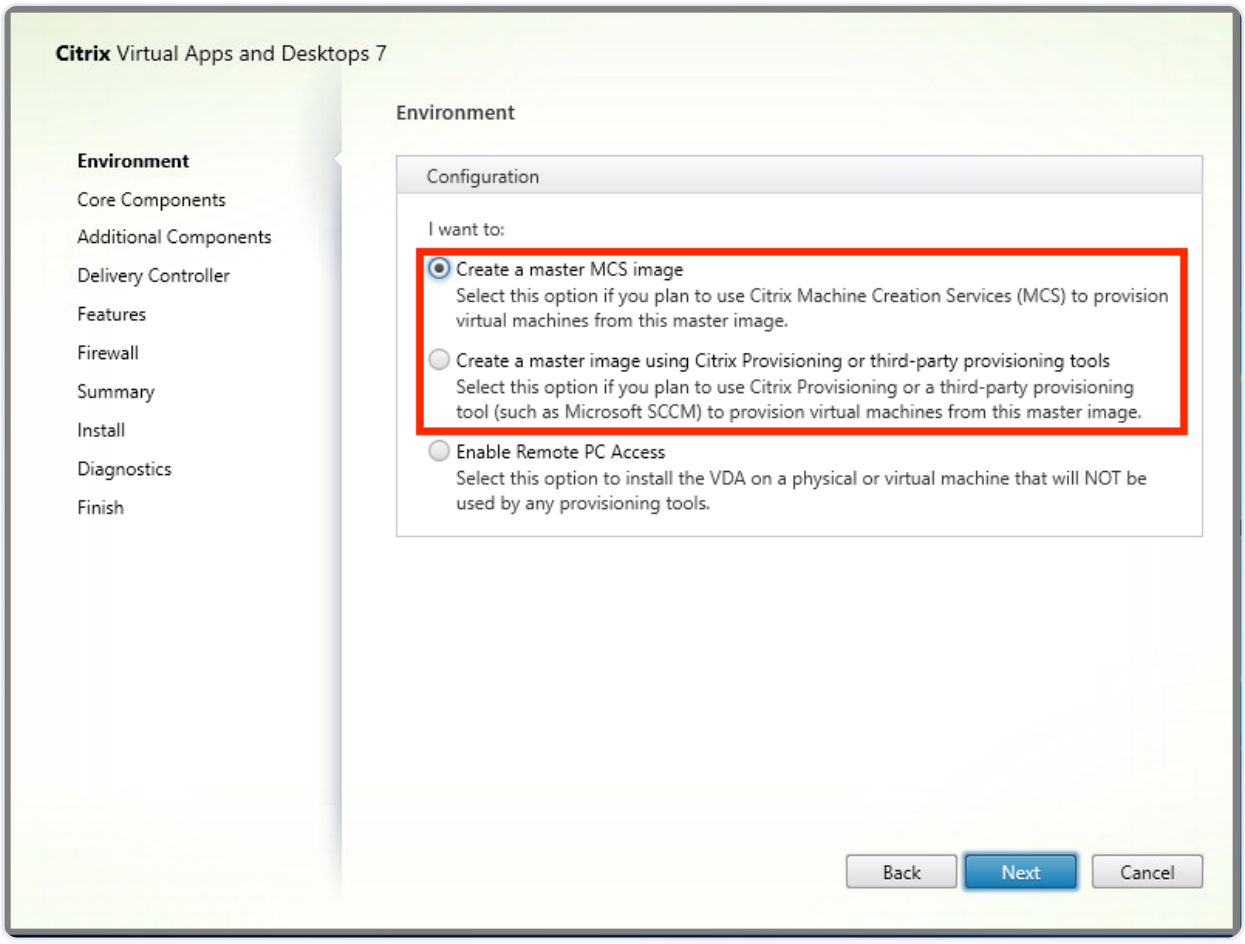
1. マスターイメージを見つけます。組織のエンタープライズアプリケーションと、ユーザーが一般的に役立つと感じるその他のアプリをインストールします。
2. Server VDIを展開している場合は、Server VDIの記事の手順に従ってください。オプションコンポーネントである**User personalization layer**を必ず含めてください。詳細については、VDAインストール用のコマンドラインオプションを参照してください。

3. Windows 10を使用している場合は、Virtual Delivery Agent (VDA) 1912以降をインストールします。以前のバージョンのVDAがすでにインストールされている場合は、まず古いバージョンをアンインストールしてください。新しいバージョンをインストールする際は、オプションコンポーネントである**Citrix User Personalization Layer**を次のように選択してインストールしてください。

   a. **Virtual Delivery Agent for Windows Desktop OS**タイルをクリックします。

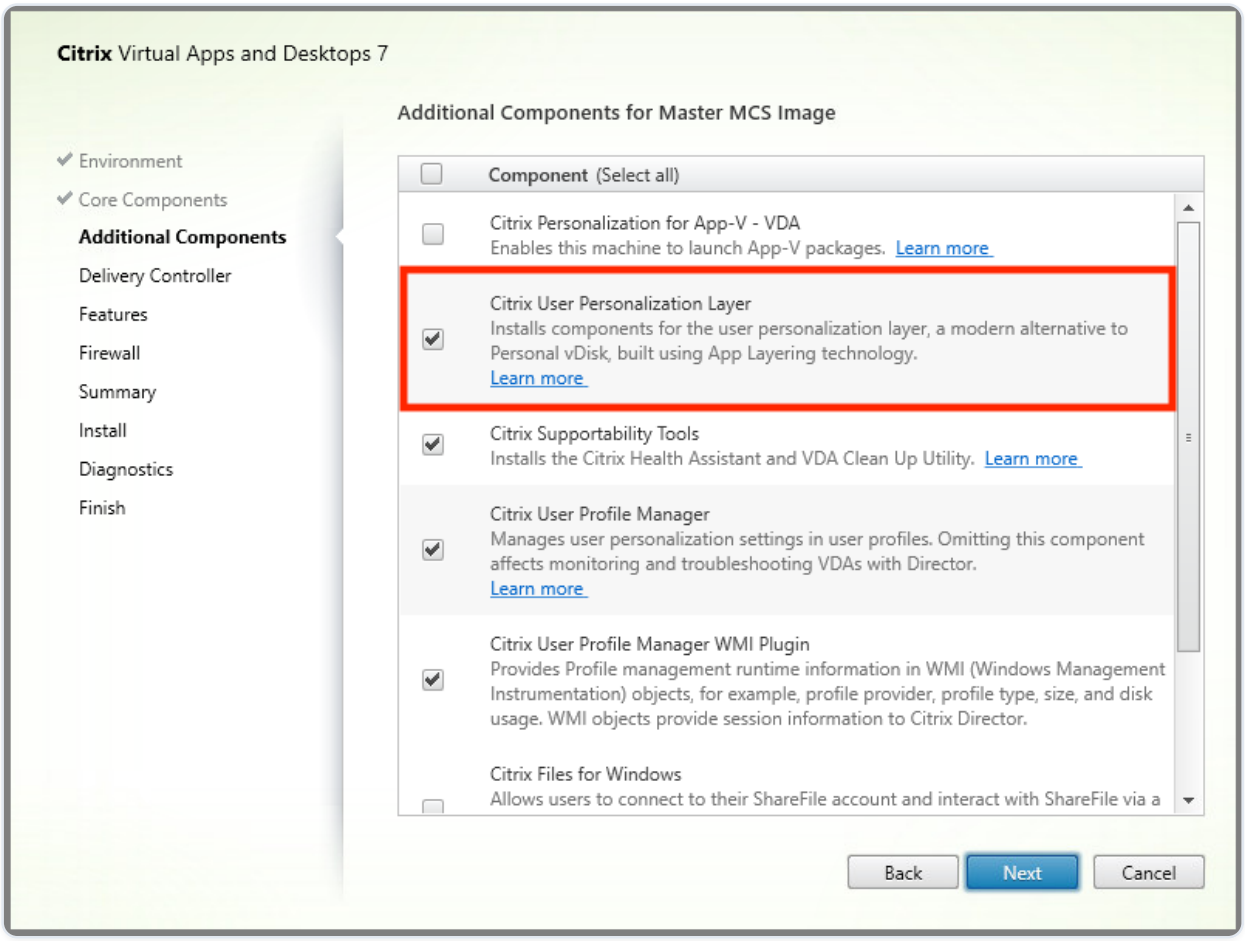


   a. **環境:**「**Create a master MCS image**」または「**Create a master image using Citrix Provisioning or third-party provisioning tools**」のいずれかを選択します。



a. **Core Components:** 「**Next**」をクリックします。

b. **追加コンポーネント:** 「**Citrix User Personalization Layer**」をチェックします。



a. 残りのインストール画面をクリックして進み、必要に応じてVDAを構成し、「**Install**」をクリックします。インストール中にイメージが1回以上再起動します。

4. **Windows updates**は無効のままにしてください。ユーザーパーソナライゼーションレイヤーインストーラーは、イメージ上のWindows更新を無効にします。更新は無効のままにしてください。

イメージをWeb Studioにアップロードする準備ができました。

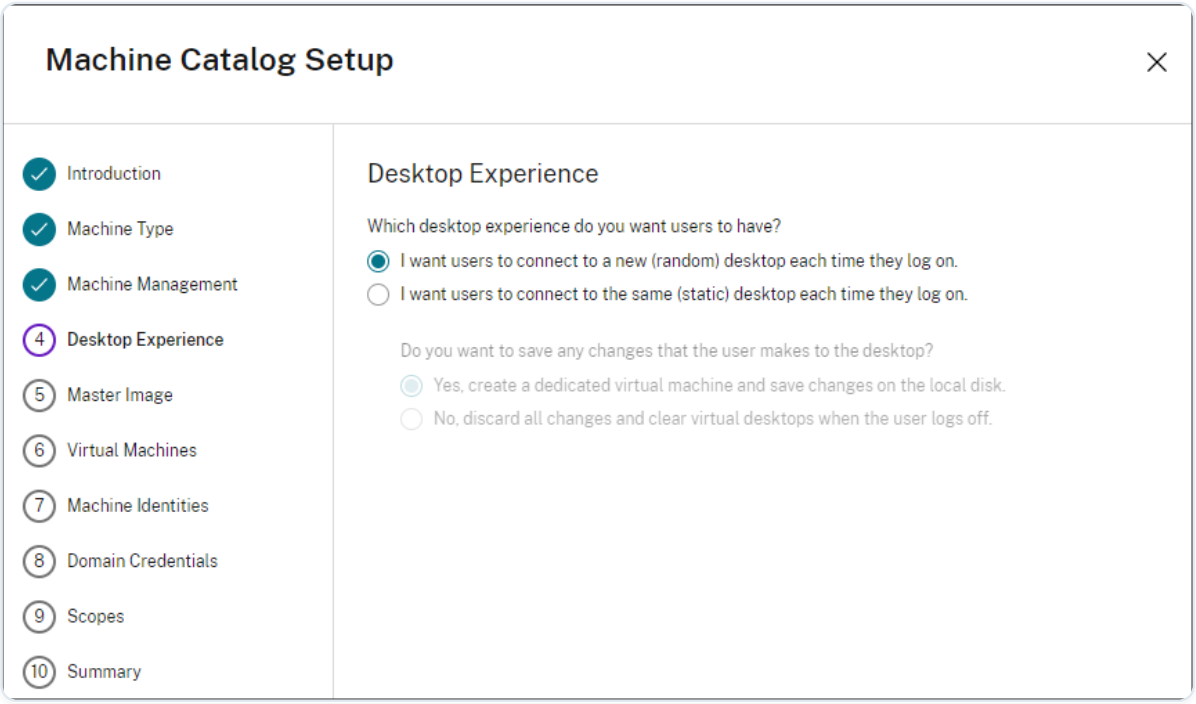
> **注:**
>
> ユーザーパーソナライゼーションレイヤー (UPL) をアップグレードするだけであれば、UPLの新しいバージョンとスタンドアロンパッケージを使用してアップグレードできます。VDAをアップグレードする必要はありません。

ステップ3：マシンカタログを作成する

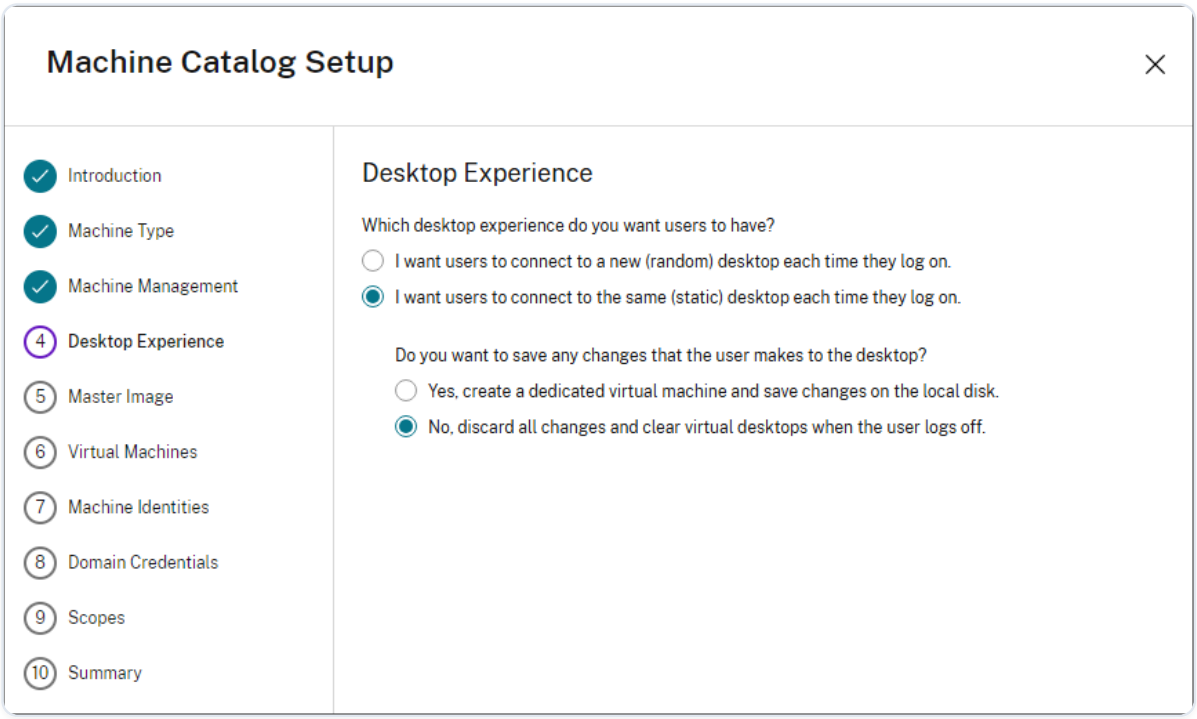
Web Studio で、マシンカタログを作成する手順に従います。カタログ作成時に、以下のオプションを使用します。

1. **オペレーティングシステム**を選択し、**シングルセッションOS**に設定します。
2. **マシン管理**を選択し、**電源管理されているマシン**に設定します。たとえば、仮想マシンやブレードPCなどです。
3. **デスクトップエクスペリエンス**を選択し、以下の例のように、**プールされたランダム**または**プールされた静的**のいずれかのカタログタイプに設定します。

   - **プールされたランダム：**



   - **プールされた静的：** プールされた静的を選択した場合、以下のスクリーンショットに示すように、ユーザーがログオフしたときにすべての変更を破棄し、仮想デスクトップをクリアするようにデスクトップを構成します。



> **注：**
>
> ユーザーパーソナライゼーションレイヤーは、Citrix Personal vDiskを使用するように構成されている、または専用仮想マシンとして割り当てられているプールされた静的カタログをサポートしていません。

4. MCSを使用している場合は、**マスターイメージ**と、前のセクションで作成したイメージのスナップショットを選択します。
5. 環境に合わせて、残りのカタログプロパティを構成します。

ステップ4：デリバリーグループを作成する

作成したマシンカタログのマシンを含む**デリバリーグループ**を作成および構成します。詳細については、デリバリーグループの作成を参照してください。

ステップ 5: デリバリーグループのカスタムポリシーを作成する

Virtual Delivery Agent 内でユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- ユーザーレイヤーディスクの最大許容サイズ。

パラメーターを Web Studio でカスタム Citrix ポリシーとして定義し、デリバリーグループに割り当てます。

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。

   Studioでポリシーを選択(/en-us/citrix-virtual-apps-desktops/2311/media/upl-studio-select-policies.png)

2. アクションバーで**ポリシーの作成**を選択します。「ポリシーの作成」ウィンドウが表示されます。
3. 検索フィールドに `user layer` と入力します。利用可能なポリシーのリストに、次の3つのポリシーが表示されます。

   - ユーザーレイヤーの除外
   - ユーザーレイヤーリポジトリパス
   - ユーザーレイヤーサイズGB

   > **注:**
   >
   > サイズを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。サイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

   ユーザーレイヤーポリシーの選択(/en-us/citrix-virtual-apps-desktops/2311/media/user-layer-policies.png)

4. 「**ユーザーレイヤーリポジトリパス**」の横にあるチェックボックスをオンにし、「**編集**」をクリックします。「**設定の編集**」ウィンドウが表示されます。
5. 「**値**」フィールドにパスを入力し、「**保存**」をクリックします。

   - **パス形式:** `\\server-name-or-address\share-name\folder`
   - **パスの例:** `\\Server\Share\UPLUsers`
   - **結果のパスの例: CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のとおりです。 `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

   リポジトリパス(/en-us/citrix-virtual-apps-desktops/2311/media/upl-user-layer-repo-enter-path-no-variables.png)

`%USERNAME%`と`%USERDOMAIN%`変数、マシン環境変数、およびActive Directory (AD) 属性を使用してパスをカスタマイズできます。これらの変数を展開すると、明示的なパスになります。

環境変数の例:

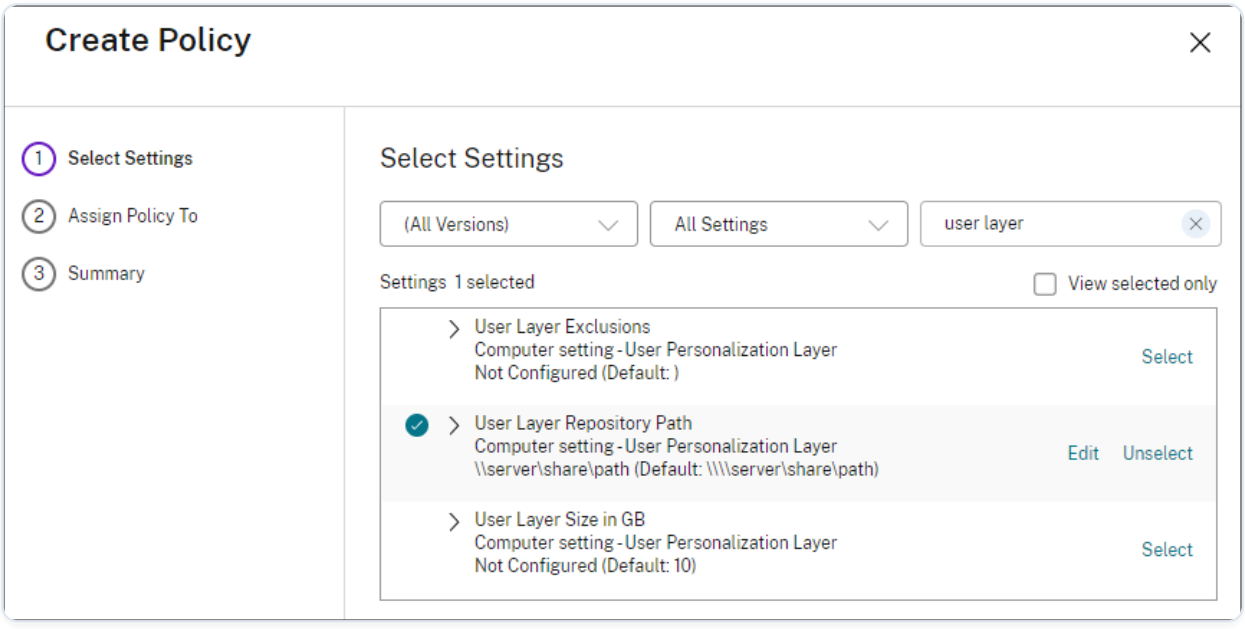
- **パス形式:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **パスの例:** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **結果のパスの例: CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のようになります。`\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`

環境変数を含むリポジトリパス(/en-us/citrix-virtual-apps-desktops/2311/media/upl-user-layer-repo-enter-path-variables.png)

カスタム AD 属性の例:

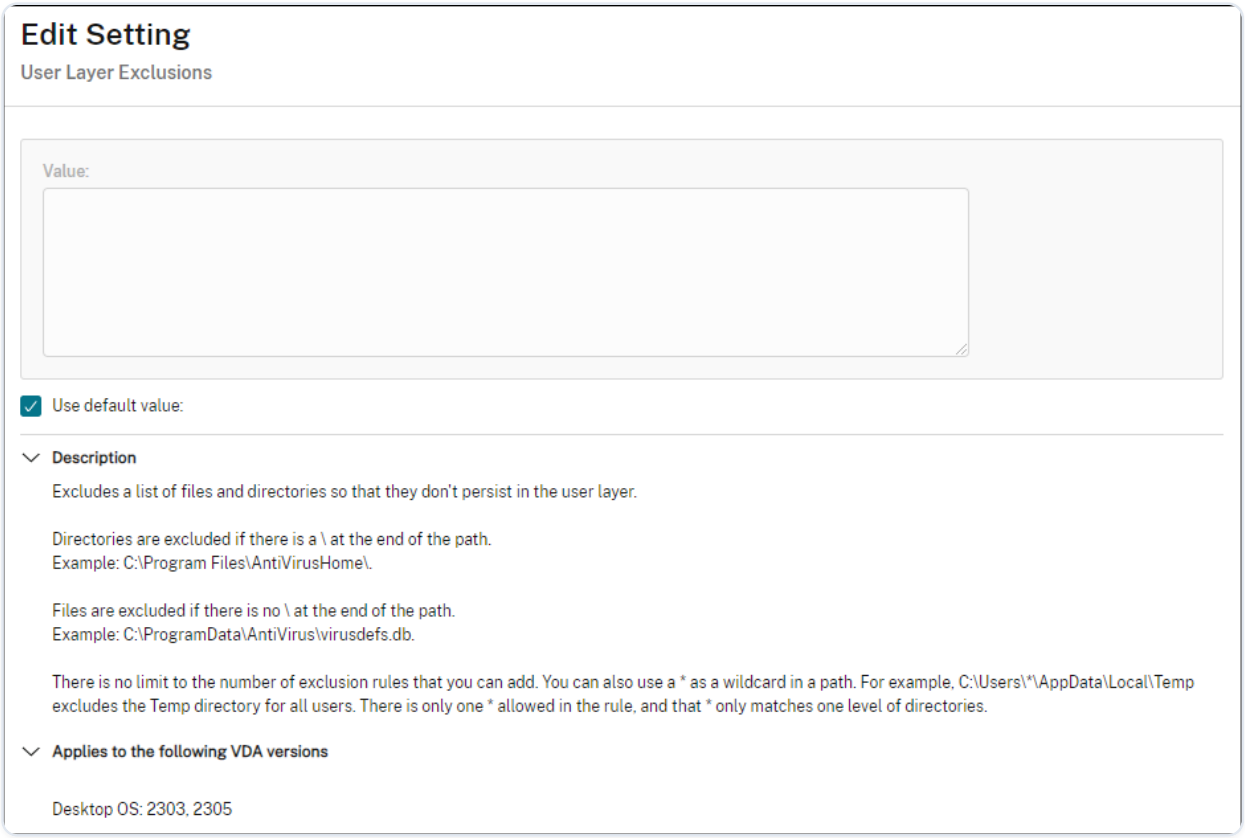
- パス形式: `\\Server-name-or-address\share-name\AD-attribute`
- パスの例: `\\Server\share#sAMAccountName#`
- 結果のパスの例: `\\Server\share\JohnSmith` (現在のユーザーに対して #sAMAccountName# が JohnSmith に解決される場合)

6. オプション: **ユーザーレイヤーサイズ (GB)** の横にあるチェックボックスをオンにして、**編集**をクリックします。

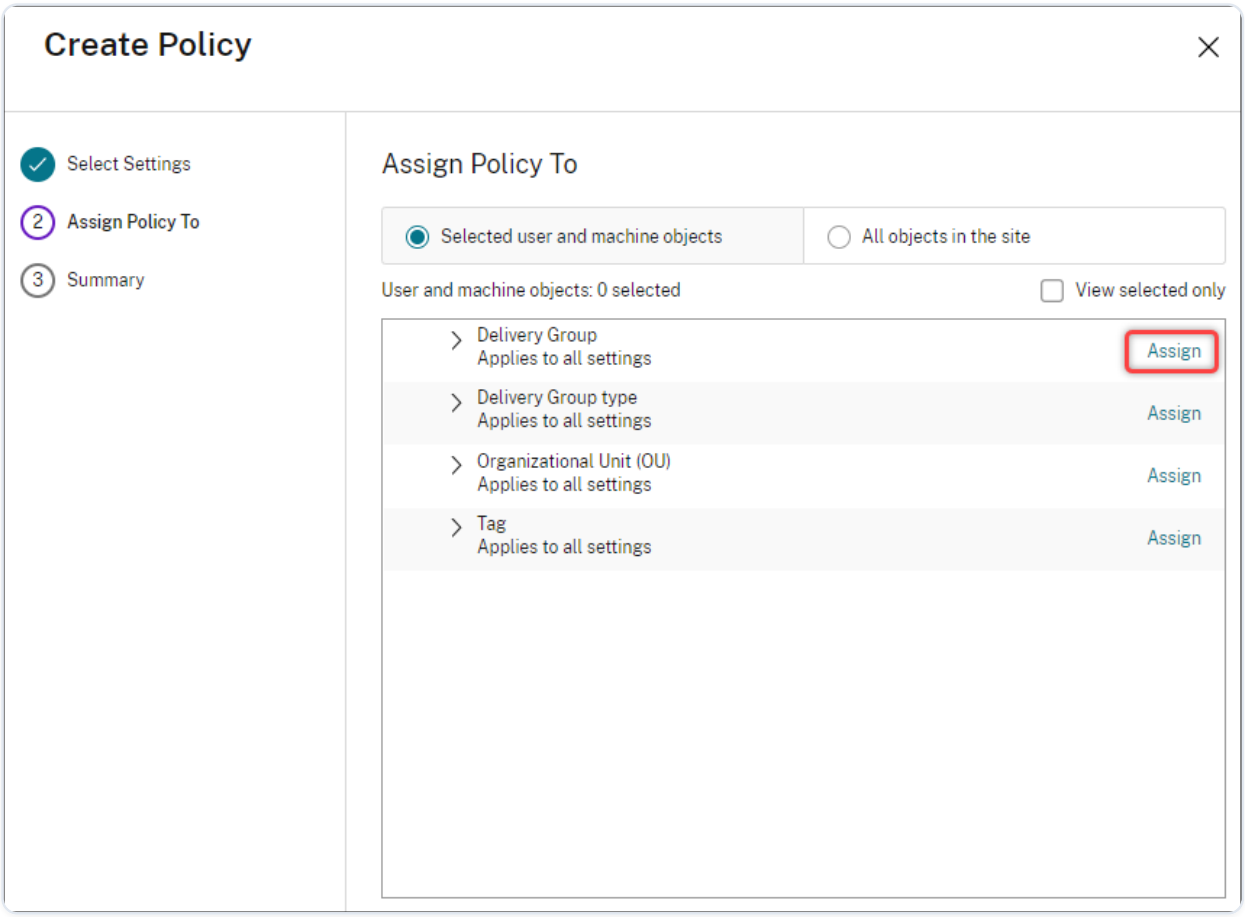


設定の編集ウィンドウが表示されます。

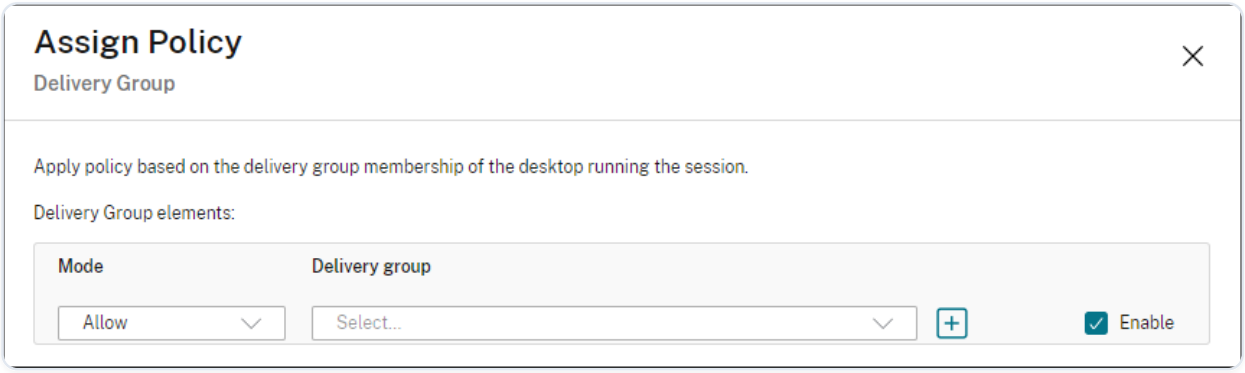
7. オプション: **10 GB** のデフォルト値を、各ユーザーレイヤーが拡張できる最大サイズに変更します。**保存** をクリックします。
8. オプション: **User Layer Exclusions** の横にあるチェックボックスをオンにして、**Edit** をクリックします。



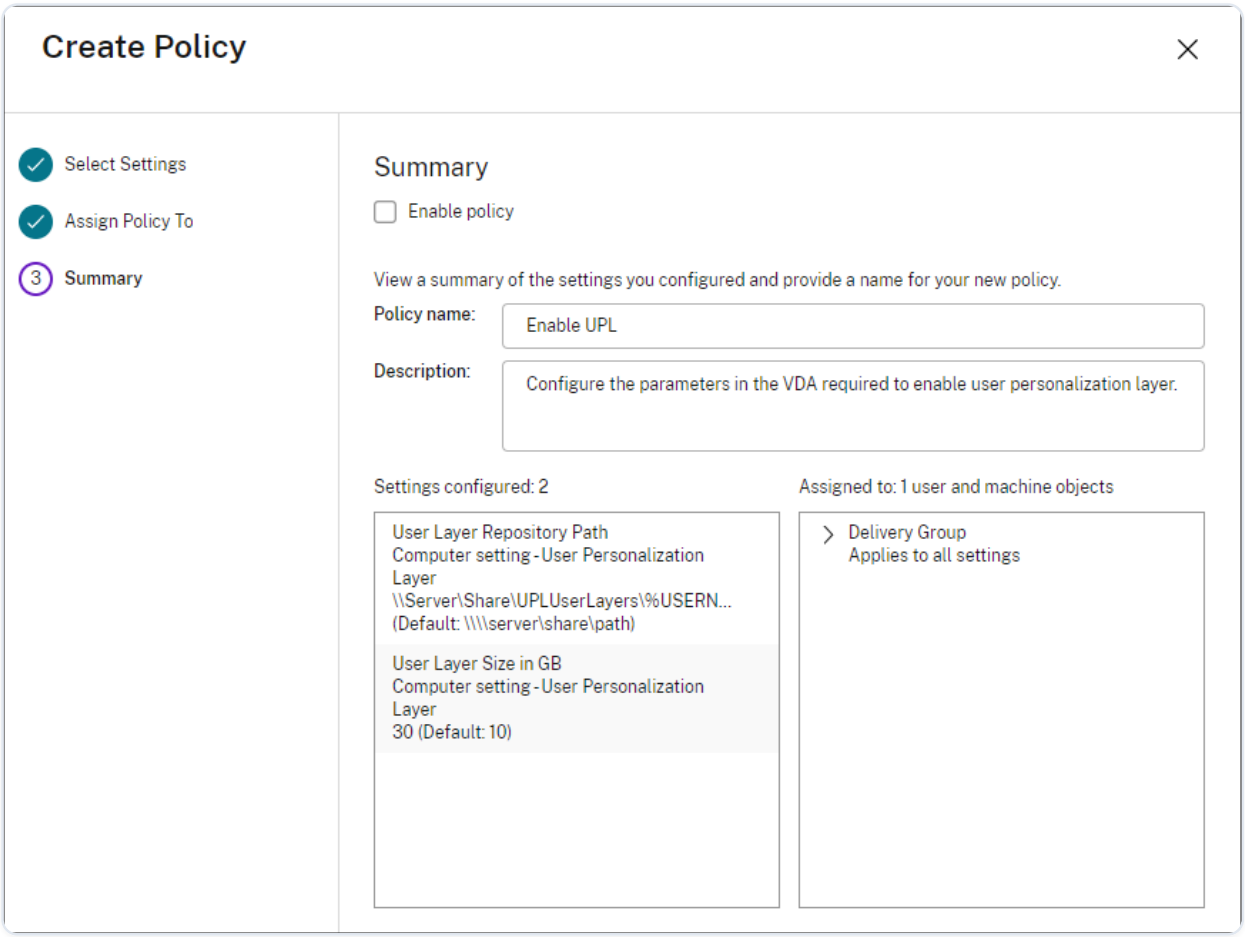
9. オプション: 除外するファイルとフォルダーを指定し、**Save** をクリックします。詳細については、Citrix App Layering のドキュメント を参照してください。
10. 割り当てるユーザーとマシンを設定するには、**Next** をクリックします。この画像で強調表示されている **Delivery Group Assign** リンクをクリックします。



11. **Delivery Group** メニューで、前のセクションで作成したデリバリーグループを選択します。**OK** をクリックします。



12. ポリシーの名前を入力します。ポリシーを有効にするチェックボックスをオンにして、**完了** をクリックします。



ユーザーレイヤーフォルダーのセキュリティ設定を構成する

ドメイン管理者として、ユーザーレイヤーのストレージの場所を複数指定できます。各ストレージの場所（デフォルトの場所を含む）に `\Users` サブフォルダーを作成します。次の設定を使用して、各場所を保護します。

設定名	値	適用先	
作成者/所有者	変更	サブフォルダーとファイルのみ	
所有者の権限	変更	サブフォルダーとファイルのみ	
ユーザーまたはグループ	フォルダーの作成/データの追加; フォルダーの走査/ファイルの実行; フォルダーの一覧表示/データの読み取り; 属性の読み取り	選択したフォルダーのみ	

設定名	値	適用先	
システム	フルコントロール	選択したフォルダー、サブフォルダー、およびファイル	
ドメイン管理者、および選択した管理者グループ	フルコントロール	選択したフォルダー、サブフォルダー、およびファイル	

ユーザーレイヤーメッセージ

ユーザーが自分のユーザーレイヤーにアクセスできない場合、次のいずれかの通知メッセージが表示されます。

- **ユーザーレイヤーが使用中です**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーレイヤーが利用できません**

  `We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーサインアウト後にシステムがリセットされませんでした**

  `This system was not shut down properly. Please log off immediately and contact your system administrator.`.

トラブルシューティング時に使用するログファイル

ログファイル ulayersvc.log には、変更がログに記録されるユーザーパーソナライゼーションレイヤーソフトウェアの出力が含まれています。

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

ユーザーレイヤー/UPL領域の再利用

ユーザーがログオフするたびにVHDXファイルを自動的に圧縮するには、**ユーザーレイヤー/UPL領域の再利用**を使用できます。 詳細については、「ユーザーレイヤー/UPL領域の再利用」を参照してください。

制限事項

ユーザーパーソナライゼーションレイヤー機能をインストールして使用する際は、以下の制限事項に留意してください。

- App Layering内のレイヤーにユーザーパーソナライゼーションレイヤーソフトウェアを展開しようとしないでください。ユーザーパーソナライゼーションレイヤーはCitrix Virtual Apps and Desktopsに展開するか、App Layeringイメージテンプレートでユーザーレイヤーを有効にするかのいずれかにしてください。両方を行うことはできません。どちらのプロセスでも、必要なユーザーレイヤーが生成されます。
- ユーザーパーソナライゼーションレイヤー機能を永続的なマシンカタログで構成しないでください。
- 「セッションホスト」は使用しないでください。
- 新しいOSインストール（Windows 10の同じバージョンであっても）を実行しているイメージでマシンカタログを更新しないでください。ベストプラクティスは、マシンカタログの作成時に使用したのと同じマスターイメージ内でOSに更新を適用することです。
- ブート時ドライバーやその他の早期ブートパーソナライゼーションを使用しないでください。
- PvDデータをユーザーパーソナライゼーションレイヤー機能に移行しないでください。
- 既存のユーザーレイヤーを完全なApp Layering製品からユーザーパーソナライゼーションレイヤー機能に移行しないでください。
- 異なるマスターOSイメージを使用して作成されたユーザーレイヤーにアクセスするために、ユーザーレイヤーのSMBパスを変更しないでください。
- ユーザーがセッションからログアウトして再度ログインすると、新しいセッションはプール内の別のマシンで実行されます。VDI環境では、Microsoft Software Centerはアプリケーションを最初のマシンでは**インストール済み**と表示しますが、2番目のマシンでは**利用不可**と表示します。

  アプリケーションの実際の状態を確認するには、ユーザーにSoftware Centerでアプリケーションを選択し、**インストール**をクリックするように指示します。その後、SCCMが状態を実際の値に更新します。

- ユーザーパーソナライゼーションレイヤー機能が有効になっているVDA内でSoftware Centerを起動すると、すぐに停止することがあります。この問題を回避するには、MicrosoftのXenDesktop VDI環境でのSCCMの実装に関する推奨事項に従ってください。また、Software Centerを起動する前に、`ccmexec`サービスが実行されていることを確認してください。
- グループポリシー（コンピューター設定）では、ユーザーレイヤー設定がマスターイメージに適用された設定を上書きします。そのため、GPOを使用してコンピューター設定で行った変更は、次回のセッションログイン時にユーザーに常に適用されるとは限りません。

  この問題を回避するには、次のコマンドを発行するユーザーログオンスクリプトを作成します。

  ```
  gpupdate /force
  ```

  例えば、ある顧客はユーザーがログインするたびに次のコマンドを実行するように設定しました。

  ```
  gpudate /Target:Computer /force
  ```

  最良の結果を得るには、ユーザーがログインした後で、コンピューター設定への変更をユーザーレイヤーに直接適用します。
- ドメインユーザーアカウントは、マスターイメージに最後にログインしたユーザーであってはなりません。そうしないと、そのイメージからプロビジョニングされたマシンで問題が発生する可能性があります。
- 純粋なAzure AD環境でUPLが有効になっている場合、Azure上で実行されているWindowsの根本的な問題により、カスタム証明書は保持されません。Microsoftが将来の機能強化でこの問題を修正した場合、この記事を更新します。

コンポーネントの削除

コンポーネントを削除するには、Citrix®はWindowsのプログラムの削除または変更機能を使用することを推奨します。あるいは、コマンドラインまたはインストールメディア上のスクリプトを使用してコンポーネントを削除することもできます。

コンポーネントを削除しても、前提条件は削除されず、ファイアウォール設定も変更されません。たとえば、Delivery Controller™ を削除しても、SQL Serverソフトウェアとデータベースは削除されません。

Web Interfaceを含む以前の展開からControllerをアップグレードした場合、Web Interfaceコンポーネントは別途削除する必要があります。インストーラーを使用してWeb Interfaceを削除することはできません。

以下に記載されていない機能の削除については、その機能のドキュメントを参照してください。

準備

Controllerを削除する前に、サイトから削除してください。詳しくは、「Controllerを削除する」を参照してください。

StudioとDirectorを削除する前に、それらを閉じます。

Windowsのプログラムの削除または変更機能を使用してコンポーネントを削除する

Windowsのプログラムの削除または変更機能から：

- Controller、Studio、Director、License Server、またはStoreFrontを削除するには、**Citrix Virtual Apps *version*** または **Citrix Virtual Apps and Desktops™ *version*** を右クリックして、**アンインストール**を選択します。インストーラーが起動します。削除するコンポーネントを選択します。

  あるいは、**Citrix StoreFront** を右クリックして **アンインストール** を選択することで、StoreFront™ を削除することもできます。
- VDAを削除するには、**Citrix Virtual Delivery Agent *version*** を右クリックし、**アンインストール**を選択します。インストーラーが起動し、削除するコンポーネントを選択できます。デフォルトでは、削除後にマシンは自動的に再起動します。
- Universal Print Serverを削除するには、**Citrix Universal™ Print Server**を右クリックし、**アンインストール**を選択します。

コマンドラインを使用してコアコンポーネントを削除する

`\x64\XenDesktop Setup`ディレクトリから、`XenDesktopServerSetup.exe`コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove`および`/components`オプションを指定します。
- すべてのコンポーネントを削除するには、`/removeall`オプションを指定します。

コマンドとパラメーターの詳細については、「コマンドラインを使用したインストール」を参照してください。

例えば、次のコマンドはWeb Studioを削除します。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components webstudio
```

コマンドラインを使用してVDAを削除する

`\x64\XenDesktop Setup`ディレクトリから、`XenDesktopVdaSetup.exe`コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove`オプションと`/components`オプションを使用します。例えば、VDAとCitrix Workspaceアプリを削除するには、`/remove /components vda,plugin`を使用します。
- `/removeall`オプションはVDAのみを削除します。Citrix Workspaceアプリは削除しません。

コマンドとパラメーターの詳細については、「コマンドラインを使用したインストール」を参照してください。

デフォルトでは、削除後にマシンは自動的に再起動します。

Active Directoryでスクリプトを使用してVDAを削除するには、「スクリプトを使用したVDAのインストールまたは削除」を参照してください。

アップグレードと移行

はじめに

アップグレードすると、新しいマシンやサイトをセットアップすることなく、展開をCitrix Virtual Apps and Desktops 7 Current Release (CR)に変更できます。これはインプレースアップグレードとして知られています。

アップグレードにより、利用資格のある最新の機能とテクノロジーにアクセスできるようになります。アップグレードには、以前のバージョンからの修正、説明、機能強化も含まれる場合があります。

アップグレードの概要

1. アップグレードを開始する前に、展開のアップグレードの記事を確認してください。これは、アップグレードの準備方法と実装方法を学ぶための主要な情報源です。
2. 現在のCustomer Success Servicesの有効期限が切れていないことを確認してください。詳細については、Customer Success Servicesの更新ライセンスの記事を参照してください。
3. 準備ガイドを完了します。
4. インストーラーを実行してコアコンポーネントをアップグレードします。
5. システムデータベースとサイトをアップグレードします。
6. イメージ上のVDA（またはマシンに直接）をアップグレードします。
7. その他のコンポーネントをアップグレードします。

各準備およびアップグレードの手順は、展開のアップグレードに詳しく記載されています。

アップグレード可能なバージョン

Citrix Virtual Apps and Desktops™ 2203 LTSRへは、以下からアップグレードできます。

- XenApp および XenDesktop 7.15 LTSR CU5 から CU8 まで
- Virtual Apps and Desktops 1912 (CU の有無にかかわらず、CU5 を含む)
- 現在サポートされている Citrix Virtual Apps and Desktops の CR バージョン

アップグレード可能なCitrix Virtual Apps and Desktops（およびXenAppおよびXenDesktop）のバージョンの一覧については、Citrix Upgrade Guideも参照してください。

よくある質問

このセクションでは、Citrix Virtual Apps and Desktops のアップグレードに関するよくある質問に答えます。

- **Virtual Apps and Desktops環境をアップグレードする正しい順序は何ですか？**

  推奨されるアップグレードシーケンスの図と説明については、アップグレードシーケンスおよびアップグレード手順を参照してください。

- **私のサイトには複数の Delivery Controller (異なるゾーン) があります。一部のみをアップグレードした場合、どうなりますか？同じメンテナンス期間中にサイト内のすべての Controller をアップグレードする必要がありますか？**

  各Controller上のさまざまなサービスが相互に通信するため、すべてのDelivery Controllerを同じメンテナンス期間中にアップグレードすることがベストプラクティスです。異なるバージョンを維持すると問題が発生する可能性があります。メンテナンス期間中には、Controllerの半分をアップグレードし、サイトをアップグレードしてから、残りのControllerをアップグレードすることをお勧めします。(詳細については、アップグレード手順を参照してください。)

- **最新バージョンに直接アップグレードできますか、それとも段階的なアップグレードを行う必要がありますか？**

  アップグレード先のバージョンの **新機能** の記事で明示的に記載されていない限り、ほとんどの場合、中間リリースをスキップして最新バージョンにアップグレードできます。Upgrade Guide を参照してください。

- **お客様は Long Term Service Release (LTSR) 環境から Current Release にアップグレードできますか？**

  はい。お客様は長期間 Long Term Service Release を維持する必要はありません。お客様はビジネス要件と機能に基づいて、LTSR 環境を Current Release に移行できます。

- **コンポーネントの混在バージョンは許可されていますか？**

  各サイト内で、Citrixはすべてのコンポーネントを同じバージョンにアップグレードすることを推奨しています。一部のコンポーネントで以前のバージョンを使用することはできますが、最新バージョンのすべての機能が利用できるとは限りません。詳細については、「混在環境に関する考慮事項」を参照してください。

- **Current Releaseはどのくらいの頻度でアップグレードする必要がありますか？**

Current Releaseは、リリース日から6か月後にEnd of Maintenance (EOM) に達します。Citrixは、お客様が最新のCurrent Releaseを採用することを推奨しています。Current Releaseは、リリース日から18か月後にEnd of Life (EOL) に達します。詳細については、「Current Releaseのライフサイクル」を参照してください。

- **推奨されるのは、LTSRへのアップグレードですか、それともCRへのアップグレードですか？**

  Current Release (CR) は、最新かつ最も革新的なアプリ、デスクトップ、およびサーバー仮想化の機能を提供します。これにより、最先端のテクノロジーを維持し、競合他社の一歩先を行くことができます。

  Long Term Service Release (LTSR) は、長期間にわたって同じベースバージョンを維持することを好む大規模なエンタープライズ本番環境に最適です。

  詳細については、サービスオプションを参照してください。

- **ライセンスをアップグレードする必要がありますか？**

  現在のライセンスの有効期限が切れておらず、アップグレード先のリリースで有効であることを確認してください。CTX111618を参照してください。更新については、Customer Success Services renewal licensesを参照してください。

- **アップグレードにはどのくらい時間がかかりますか？**

  展開のアップグレードにかかる時間は、インフラストラクチャとネットワークによって異なります。そのため、正確な時間をお伝えすることはできません。

- **ベストプラクティスは何ですか？**

  「準備ガイド」を理解し、それに従っていることを確認してください。

- **サポートされているオペレーティングシステムは何ですか？**

  アップグレード先のバージョンのシステム要件の記事に、サポートされているOSが記載されています。

  現在の展開でサポート対象外のオペレーティングシステムを使用している場合は、「以前のオペレーティングシステム」を参照してください。

- **サポートされているVMware vSphere (vCenter + ESXi) のバージョンは何ですか？**

  CTX131239 には、サポートされているホストとバージョン、および既知の問題へのリンクが記載されています。

- **私のバージョンはいつEOLになりますか？**

  製品マトリックス を確認してください。

- **最新リリースにおける既知の問題は何ですか？**
  - シトリックス バーチャルアプリおよびデスクトップ
  - StoreFront
  - シトリックス プロビジョニング
  - シトリックス ライセンスサーバー
  - シトリックス ワークスペースアプリ for Windows

詳細情報

Long Term Service Release (LTSR) の展開更新では、累積更新プログラム (CU) が使用されます。CU は LTSR のベースラインコンポーネントを更新し、各 CU には独自のメタインストーラーが含まれています。

各CUには専用のドキュメントがあります。たとえば、7.15 LTSR の場合、その LTSR の **「新機能」** ページで最新の CU へのリンクを確認してください。各 CU ページには、サポートされているバージョン情報、手順、および CU ダウンロードパッケージへのリンクが含まれています。

移行

クラウドへの移行

Citrix Virtual Apps and Desktopsの自動構成ツールを使用して、オンプレミス展開をクラウドに移行できます。詳しくは、「クラウドへの移行」を参照してください。

レガシー移行

移行とは、以前の展開から新しいバージョンにデータを移動することです。このプロセスには、新しいコンポーネントのインストールと新しいサイトの作成、古いファームからのデータのエクスポート、そして新しいサイトへのデータのインポートが含まれます。

XenApp および XenDesktop のバージョン、または以前の Citrix Virtual Apps and Desktops のバージョンを移行するためのサポートされているツールやスクリプトはありません。Citrix Upgrade Guide に記載されている Citrix Virtual Apps and Desktops のバージョンについては、*アップグレード*がサポートされており、この製品ドキュメントで説明されています。

以前のXenApp 6.xの移行コンテンツについては、以下を参照してください。スクリプトも記事もサポートまたは保守されていません。

- XenApp 6.x バージョン用のオープンソース移行スクリプトは `<https://github.com/citrix/xa65migrationtool>` で入手できます。Citrix はこれらの移行スクリプトをサポートまたは保守していません。
- 7.x での変更点
- XenApp 6.5 ワーカーを新しい VDA にアップグレードする
- XenApp 6.x を移行する

展開のアップグレード

> **注:**
>
> この記事では、Web Studioを含む展開のアップグレードについて説明します。Citrix Studioを含むアップグレードについては、Citrix Virtual Apps and Desktops™ 7 2212以前の同等の記事を参照してください。

はじめに

新しいマシンやサイトを最初にセットアップすることなく、特定のデプロイメントを新しいバージョンにアップグレードできます。これはインプレースアップグレードと呼ばれます。アップグレードできる Citrix Virtual Apps and Desktops のバージョンについては、Citrix Upgrade Guide を参照してください。

Citrix Virtual Apps and Desktops のいずれかのリリースにアップグレードする前に、現在の Customer Success Services の日付が有効であり、期限切れになっていないことを確認してください。詳細については、Customer Success Services renewal licenses の記事を参照してください。

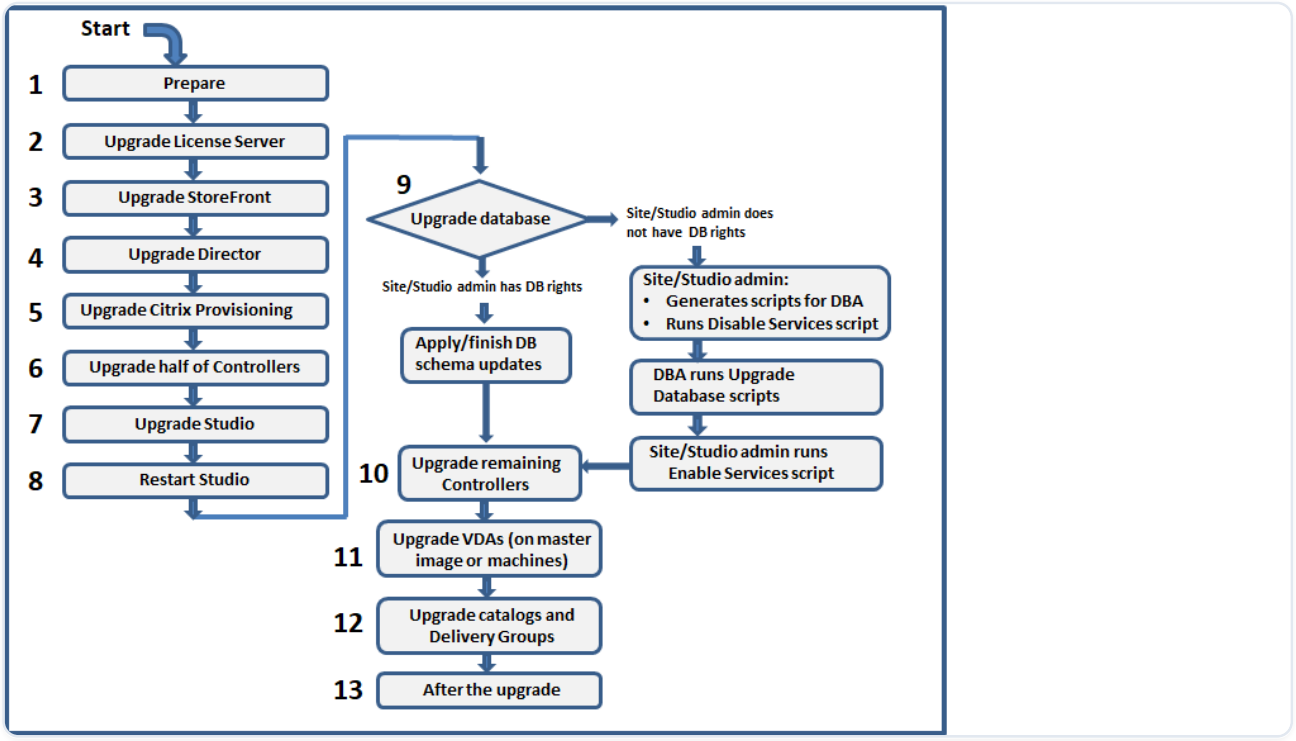
アップグレードを開始するには、新しいバージョンのインストーラーを実行して、以前にインストールされたコアコンポーネント、VDA、およびその他の特定のコンポーネントをアップグレードします。その後、データベースとサイトをアップグレードします。

より新しいバージョンが提供されている場合、フルプロダクトインストーラー（およびスタンドアロン VDA インストーラー）でインストールできる任意のコンポーネントをアップグレードできます。フルプロダクトインストーラーでインストールされないその他のコンポーネント（Citrix Provisioning™ や Profile Management など）については、そのコンポーネントのドキュメントを参照してください。ホストのアップグレードについては、適切なドキュメントを参照してください。

アップグレードを開始する前に、この記事のすべての情報を確認してください。

アップグレードシーケンス

次の図は、アップグレードシーケンスのステップを示しています。Upgrade procedure には、図の各ステップの詳細が含まれています。



注:

障害を回避するため、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

ハイブリッド権限ライセンス

ハイブリッドライツライセンスは、顧客が永続ライセンスからクラウドサービスサブスクリプションに移行またはアップグレードする際に、クラウドサービスサブスクリプションに加えて提供される、期間ベースのサブスクリプションライセンスです。DaaSサブスクリプションでハイブリッドライツアドオンを購入することもできます。

SaaS属性を持つハイブリッドライツライセンスをお持ちの場合、Citrix Virtual Apps and Desktops LTSR 2203以降にアップグレードすると、Citrix Virtual Apps and Desktops LTSR 1912では利用で

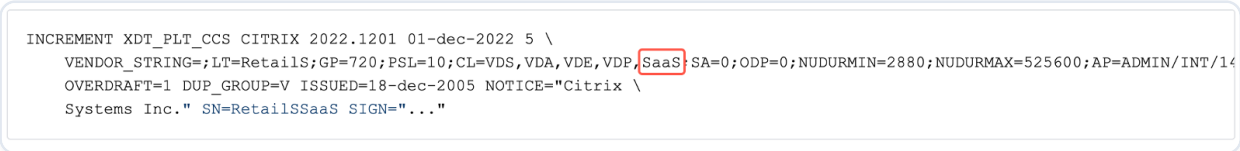
きなかった機能にアクセスできるようになります。これらの機能には、Microsoft Azure、AWS EC2、Google Cloudなどのパブリッククラウドでのワークロードのプロビジョニングとホスティングが含まれます。新しいライセンスファイルを展開する前に、ライセンスサーバーを最新バージョンに更新してください。

SaaS属性のないハイブリッドライツライセンスにアクセスできる場合は、次の手順に従ってSaaS属性を持つ新しいハイブリッドライツライセンスにアクセスしてください。

注：

- 新しいライセンスコードが記載されたメールが届きます。詳しくは、「ライセンスアクセスコードの使用」を参照してください。
- 既存のライセンスは取り消されます。取り消されたライセンスはライセンスサーバーから削除し、その後新しいライセンスをインストールする必要があります。詳しくは、「ライセンスファイルの削除」を参照してください。

1. citrix.comのライセンス管理ポータルにアクセスし、クラウドプロビジョニング権限が有効になっている（SaaS属性を持つ）新しいハイブリッドライツライセンスファイルをダウンロードします。詳細については、「ライセンスのダウンロード」を参照してください。次の図は、インクリメントセクションにあるSaaS属性を持つハイブリッドライツライセンスファイルを示しています。



2. ライセンスサーバーにハイブリッド権限ライセンスファイルをインストールします。詳しくは、「ライセンスのインストール」を参照してください。
3. ライセンスのエディションまたはモデルに変更がある場合は、ブローカーコマンドを実行してエディションとモデルを設定し、インプレースアップグレードを開始してください。ブローカーコマンドの詳細については、「Broker PowerShell SDK」セクションを参照してください。

Citrix Virtual Apps and Desktops Current ReleasesおよびLong Term Service Releasesでのパブリッククラウドサポートの詳細については、CTX270373を参照してください。

アップグレード手順

主要な製品コンポーネントのほとんどは、コンポーネントを含むマシンで製品インストーラーを実行することでアップグレードできます。

1台のマシンに複数のコンポーネント（Studioやライセンスサーバーなど）が含まれている場合、製品メディアにそれらのソフトウェアの新しいバージョンが含まれていれば、そのマシン上のすべてのコンポーネントがアップグレードされます。

インストーラーを使用するには：

- 製品インストーラーのグラフィカルインターフェイスを実行するには、マシンにログオンし、メディアを挿入するか、新しいリリースのISOドライブをマウントします。**AutoSelect**をダブルクリックします。
- コマンドラインインターフェイスを使用するには、適切なコマンドを発行します。(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/install-command.html)を参照してください。

ステップ1：準備

アップグレードを開始する前に、準備が整っていることを確認してください。必要なタスクを読み、完了してください。

- PVD、AppDisks™、およびサポートされていないホストの削除
- PvDまたはAppDiskコンポーネントを持つVDA
- 制限事項
- 混在環境に関する考慮事項
- 以前のオペレーティングシステム
- 準備
- 予備サイトテスト
- SQL Serverのバージョンチェック

ステップ2：ライセンスサーバーのアップグレード

インストールに新しいバージョンのCitrix License Serverソフトウェアが含まれている場合は、他のコンポーネントよりも先にこのコンポーネントをアップグレードしてください。

まだライセンスサーバーが新しいバージョンと互換性があるかどうかを判断していない場合は、他のコアコンポーネントをアップグレードする前に、ライセンスサーバーでインストーラーを実行することが不可欠です。

ステップ3: StoreFront™ のアップグレード

インストールメディアに新しいバージョンのStoreFrontソフトウェアが含まれている場合、StoreFrontサーバーがインストールされているマシンでインストーラーを実行します。

- グラフィカルインターフェイスで、「**展開の拡張**」セクションから「**Citrix StoreFront**」を選択します。
- コマンドラインから、Citrix Virtual Apps and Desktopsインストールメディアの`x64`フォルダーにある`CitrixStoreFront-x64.exe`を実行します。

ステップ4: Director のアップグレード

インストールメディアに新しいバージョンのDirectorソフトウェアが含まれている場合、Directorがインストールされているマシンでインストーラーを実行します。

ステップ5: Citrix Provisioning のアップグレード

Citrix Provisioningのインストールメディアは、Citrix Virtual Apps and Desktopsのインストールメディアとは別に提供されます。Citrix Provisioningサーバーおよびターゲットデバイスソフトウェアのインストールとアップグレードの方法については、Citrix Provisioning製品ドキュメントを参照してください。

ステップ6: Delivery Controller の半分をアップグレードする

たとえば、サイトに4つのControllerがある場合、そのうちの2つでインストーラーを実行します。

Controllerの半分をアクティブなままにしておくことで、ユーザーはサイトにアクセスできます。VDAは残りのControllerに登録できます。Controllerの数が少ないため、サイトの容量が低下する場合があります。アップグレードによって、最終的なデータベースアップグレード手順中に新しいクライアント接続の確立が一時的に中断されるだけです。アップグレードされたControllerは、サイト全体がアップグレードされるまで要求を処理できません。

サイトにControllerが1つしかない場合、アップグレード中は動作しません。

実際のアップグレードが開始される前に、最初のControllerでサイトの事前テストが実行されます。詳細については、サイトの事前テストを参照してください。

ステップ7: Studio のアップグレード

Web Studioをまだアップグレードしていない場合（別のコンポーネントと同じマシンにあったため）、Studioがインストールされているマシンでインストーラーを実行します。

> **注：**

Web Studio をアップグレードした後、バージョン情報がすぐに更新されない場合があります。Web Studio がすでに最新の状態であっても、アップグレードを促されることがあります。この問題に対処するには、Web Studio サーバーに移動し、インターネットインフォメーションサービス (IIS) マネージャーを開き、 > > に移動して、 ペインで を選択します。

ステップ8：Studioを再起動する

アップグレードされたWeb Studioを再起動します。アップグレードプロセスが自動的に再開されます。

ステップ9：データベースとサイトをアップグレードする

注：

障害を避けるため、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

SQL Serverデータベースのスキーマを更新するために必要な権限については、準備を確認してください。

- SQL Serverデータベーススキーマを更新する十分な権限がある場合は、データベースの自動アップグレードを開始できます。データベースとサイトを自動的にアップグレードするに進んでください。
- データベース権限が不十分な場合は、スクリプトを使用する手動アップグレードを開始し、データベース管理者（必要な権限を持つ人）の助けを借りて進めることができます。手動アップグレードの場合、Studioユーザーはスクリプトを生成し、サービスを有効/無効にするスクリプトを実行します。データベース管理者は、SQLCMDユーティリティまたはSQLCMDモードのSQL Server Management Studioを使用して、データベーススキーマを更新する他のスクリプトを実行します。データベースとサイトを手動でアップグレードするに進んでください。
- マルチゾーン展開があり、データベースとサイトを自動的にアップグレードしたい場合は、サイトのSQL Serverデータベースをホストするのと同じゾーンでdbschemaアップグレードを実行することをCitrixは推奨します。そうしないと、データベースとサイトの自動アップグレードが失敗する可能性があります。

Citrixは、アップグレード前にデータベースをバックアップすることを強く推奨します。CTX135207を参照してください。データベースのアップグレード中は、製品サービスが無効になります。その間、Controllerはサイトの新しい接続を仲介できないため、慎重に計画してください。

データベースとサイトを自動的にアップグレードする

1. 新しくアップグレードされたStudioを起動します。
2. サイトのアップグレードを自動的に開始することを示し、準備ができたことを確認します。

データベースとサイトのアップグレードが進行します。

データベースとサイトを手動でアップグレードする

1. 新しくアップグレードされたStudioを起動します。
2. サイトを手動でアップグレードすることを示します。ウィザードはライセンスサーバーの互換性を確認し、確認を求めます。
3. データベースをバックアップしたことを確認します。

   ウィザードは、スクリプトとアップグレード手順のチェックリストを生成して表示します。アップグレード対象の製品バージョン以降、データベースのスキーマが変更されていない場合、そのスクリプトは生成されません。たとえば、ログデータベースのスキーマが変更されない場合、`UpgradeLoggingDatabase.sql` スクリプトは生成されません。
4. 次のスクリプトを記載されている順序で実行します。

   - `DisableServices.ps1`: Studioユーザーは、製品サービスを無効にするために、ControllerでこのPowerShellスクリプトを実行します。
   - `UpgradeSiteDatabase.sql`: データベース管理者は、サイトデータベースを含むサーバーでこのSQLスクリプトを実行します。
   - `UpgradeMonitorDatabase.sql`: データベース管理者は、監視データベースを含むサーバーでこのSQLスクリプトを実行します。
   - `UpgradeLoggingDatabase.sql`: データベース管理者は、構成ログデータベースを含むサーバーでこのSQLスクリプトを実行します。このスクリプトは、このデータベースが変更された場合（たとえば、ホットフィックスを適用した後など）にのみ実行してください。
   - `EnableServices.ps1`: Studioユーザーは、製品サービスを有効にするために、ControllerでこのPowerShellスクリプトを実行します。

データベースのアップグレードが完了し、製品サービスが有効になると、Studioは環境と構成を自動的にテストし、HTMLレポートを生成します。問題が特定された場合は、データベースのバックアップを復元できます。問題を解決した後、データベースを再度アップグレードできます。

5. チェックリストのタスクを完了したら、**Finish upgrade**をクリックします。

手順10: 残りのDelivery Controllerをアップグレードする

新しくアップグレードされたStudioから、ナビゲーションペインで **Citrix Studio** *サイト名* を選択します。**Common Tasks** タブで、**Upgrade remaining Delivery Controllers** を選択します。

> **注:**
>
> **残りのDelivery Controllerをアップグレード**を有効にするには、サイト用に少なくとも1つのマシンカタログと1つのデリバリーグループを作成します。

> アップグレードが完了し、その完了を確認したら、Studioを閉じてから再度開きます。Studioは、Controllerのサービスをサイトに登録するため、またはゾーンIDが存在しない場合にゾーンIDを作成するために、追加のサイトアップグレードを促すことがあります。

手順11: VDAをアップグレードする

> **重要:**
>
> VDAをバージョン1912以降にアップグレードする場合は、「VDAを1912以降にアップグレードする」を参照してください。

> VDAを含むマシンで製品インストーラーを実行します。

Machine Creation Services™とマスターイメージを使用してマシンを作成した場合、ホストに移動し、マスターイメージ上のVDAをアップグレードします。利用可能なVDAインストーラーのいずれかを使用できます。

- グラフィックインターフェイスのガイダンスについては、「VDAをインストールする」を参照してください。
- コマンドラインのガイダンスについては、「コマンドラインを使用してインストールする」を参照してください。

Citrix Provisioningを使用してマシンを作成した場合は、アップグレードに関するガイダンスについて「Citrix Provisioning製品ドキュメント」を参照してください。

ステップ12：マシンカタログとデリバリーグループを更新する

- アップグレードされたVDAを使用するマシンを含むカタログを更新する。
- アップグレードされたVDAを使用するマシンを含むカタログをアップグレードする。
- アップグレードされたVDAを使用するマシンを持つデリバリーグループをアップグレードする](/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/delivery-groups-manage.html#upgrade-a-delivery-group-or-revert-an-upgrade)。

ステップ13：アップグレード後

展開内の他のコンポーネントをアップグレードします。ガイダンスについては、以下の製品ドキュメントを参照してください。

- StoreFront
- AppDNA
- シトリックス App Layering
- HDX リアルタイム最適化パック
- プロファイル管理
- Citrix プロビジョニング
- セッションレコーディング
- ワークスペース環境管理

Microsoft SQL Server Express LocalDBソフトウェアを新しいバージョンに置き換える必要がある場合は、SQL Server Express LocalDBの置き換えを参照してください。

Dbschemaのアップグレード

展開を更新すると、複数のデータベーススキーマをアップグレードできます。次の表に、そのプロセスでアップグレードされるデータベーススキーマを示します。

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203
7.15 RTM or 7.15 CU releases	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 RTM	Config	Site, Config	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU1		Site	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU2			Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU4					Site, Config	Site; Monitor; Config; Logging
1912 CU5						Site; Monitor; Config; Logging
2112						Site; Monitor; Config

用語の定義:

- サイト: サイトデータストア。Dbschemaの更新はサイトデータストアに対して行われます。
- モニター: モニターデータストア。Dbschemaの更新はモニターデータストアに対して行われます。
- 構成: 構成テーブル。構成テーブルでは、Desktop Studioのバージョン、ライセンス情報、またはその両方が更新されます。
- ロギング: ロギングデータストア。Dbschemaの更新はロギングデータストアに対して行われます。

VDAを2203以降にアップグレードする

Personal vDisk (PvD) コンポーネントがVDAにインストールされていた場合、そのVDAはバージョン2203以降にアップグレードできません。新しいVDAを使用するには、現在のVDAをアンインストールしてから、新しいVDAをインストールする必要があります。

この指示は、PvDを一度も使用したことがない場合でも適用されます。

以前のバージョンでPvDコンポーネントがインストールされた可能性のある方法は次のとおりです。

- VDAインストーラーのグラフィカルインターフェイスでは、PvDは**追加コンポーネント**ページでオプションとして提供されていました。7.15 LTSRおよびそれ以前の7.xリリースでは、このオプションがデフォルトで有効になっていました。したがって、デフォルトを受け入れた場合（または、いずれかのリリースでこのオプションを明示的に有効にした場合）、PvDがインストールされていました。
- コマンドラインでは、`/baseimage` オプションでPvDがインストールされました。このオプションを指定した場合、またはこのオプションを含むスクリプトを使用した場合は、PvDがインストールされていました。

VDAにPvDがインストールされているかどうかわからない場合は、マシンまたはイメージで新しいVDA（2203以降）のインストーラーを実行してください。

- PvDがインストールされている場合、互換性のないコンポーネントがあることを示すメッセージが表示されます。
  - グラフィカルインターフェイスから、メッセージが表示されているページで**キャンセル**をクリックし、インストーラーを閉じたいことを確認します。
  - CLIからは、コマンドは表示されたメッセージとともに単に失敗します。
- PvDがインストールされていない場合、アップグレードが続行されます。

実行すること

VDAにPvDがインストールされていない場合は、通常のアップグレード手順に従ってください。

VDAにPvDがインストールされている場合：

1. 現在のVDAをアンインストールします。
2. 新しいVDAをインストールします。

Windows 10（1607以前、更新なし）マシンでPvDの使用を継続したい場合は、VDA 7.15 LTSRが最新のサポート対象バージョンです。

> **注:**

> *XenAppおよびXenDesktop 7.15 LTSRでWindows 7デスクトップとPersonal vDiskを使用できますか？*

> Citrixは、January 2016に発表されたXenAppおよびXenDesktop 7.6 LTSRからPersonal vDisk (PvD) を除外しました。さらに、CitrixはPvDテクノロジーの非推奨を発表し、今後Citrix App Layeringの使用を開始することを推奨しています。Citrix App Layering（バージョン4.4以降）は、XenAppおよびXenDesktop 7.15 LTSRの互換コンポーネントです。しかし、Windows 7で既存のPvD展開を使用しているお客様がCitrix App Layeringテクノロジーに移行できるよう、CitrixはXenAppおよびXenDesktop 7.15 LTSR累積更新プログラム（CU）を通じて、Windows 7デスクトップ向けPvD展開の期間限定サポートをJan 14, 2020まで提供することを決定しました。PvDコンポーネントはLTSR CUから削除され、Jan 14, 2020以降はサポートされません。さらに、Jan 14, 2020以降にWindows 7でPvDを使用すると、LTSRサイトは非準拠となります。また、Windows 10向けPvDは引き続き7.15 LTSRから除外されています。したがって、お客様は7.15 LTSRサイトでこれを使用すべきではありません。

PvD、AppDisks、およびサポートされていないホストを削除する

Citrix Virtual Apps and Desktops 7 Current Release展開では、以下のテクノロジーとホストタイプはサポートされていません。

- カタログ内のユーザーのVMの隣にデータを保存するための**Personal vDisks (PvD)**。ユーザーパーソナライゼーションレイヤー機能がユーザーの永続性を処理するようになりました。
- デリバリーグループで使用されるアプリケーションを管理するための**AppDisks**。
- **ホストタイプ：** Azure Classic、CloudPlatform（元のCitrix製品）。

- このリリースでサポートされているホストの種類については、システム要件を参照してください。
- ARMおよびAWSを引き続き使用できる代替方法については、CTX270373を参照してください。

現在の展開でPvDまたはAppDiskを使用している場合、あるいはサポートされていないホストタイプ（Microsoft Azure Classicなど）への接続がある場合、それらのテクノロジーを使用する項目を削除した後にのみ、バージョン2006（またはそれ以降のサポートされているバージョン）にアップグレードできます。現在の展開でパブリッククラウドホスト接続（AWSなど）を使用している場合は、アップグレードする前にHybrid Rights Licenseがあることを確認してください。インストーラーがサポートされていないテクノロジーまたはHybrid Rights Licenseのないホスト接続を1つ以上検出すると、アップグレードは一時停止または停止し、説明メッセージが表示されます。インストーラーログには詳細が含まれています。

アップグレードを確実に成功させるために、サポートされていない項目を削除するための該当するガイダンスを確認し、それに従ってください。

- PvDの削除
- AppDiskの削除
- サポートされていないホスト項目の削除

展開でPvDまたはAppDiskを使用していなかったとしても、関連するMSIが以前のVDAインストールまたはアップグレードに含まれていた可能性があります。VDAをバージョン2006（またはそれ以降のサポートされているバージョン）にアップグレードする前に、たとえ一度も使用していなくても、そのソフトウェアを削除する必要があります。グラフィカルインターフェイスを使用する場合、その削除は自動的に行われるか、CLIを使用する際に削除オプションを含めることができます。詳細については、PvDまたはAppDiskコンポーネントを持つVDAのアップグレードを参照してください。

PvDを削除する

PvDを使用するように構成されているすべてのマシンを削除するまで、展開のアップグレードは成功しません。これはカタログとデリバリーグループに影響します。

グループとカタログからPvDを削除するには：

1. Studioから、デリバリーグループにPvDを使用するカタログのマシンが含まれている場合、それらのマシンをグループから削除します。
2. Studioから、PvDを使用するマシンを含むすべてのカタログを削除します。

VDAのアップグレード： 展開のアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラーは検出します。詳細については、「PvDまたはAppDiskコンポーネントを持つVDA」(#vdas-that-have-pvd-or-appdisks-components)を参照してください。

PvDの代わりにApp Layeringを使用する予定がある場合は、データの移行に関する情報についてPvDからApp Layeringへの移行を参照してください。

AppDisk を削除する

AppDisk を使用しているすべてのデリバリーグループから AppDisk を削除し、その後 AppDisk 自体を削除するまで、展開のアップグレードは続行できません。

1. Studio ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで をクリックします。
3. グループから AppDisk を削除するアクションをクリックします。
4. AppDisk を使用している各デリバリーグループに対して、手順 2 と 3 を繰り返します。
5. Studio ナビゲーションペインで を選択します。
6. AppDisk を選択し、AppDisk を削除するアクションをクリックします。
7. 各 AppDisk に対して、手順 5 と 6 を繰り返します。

VDA のアップグレード: 展開のアップグレードでは、VDA に AppDisk または PvD コンポーネントがインストールされているかどうかは検出されません。ただし、VDA インストーラーは検出します。詳細については、「PvD または AppDisk コンポーネントがインストールされている VDA」を参照してください。

サポートされていないホストアイテムを削除する

サイトに Citrix CloudPlatform や Microsoft Azure Classic など、サポートされていないホストタイプへの接続がある場合、バージョン 2006 (またはそれ以降のサポートされているバージョン) への展開のアップグレードは続行できません。アップグレードを試行する前に、以下のタスクを完了してください。

Studio から:

- サポートされていないホストへのすべての接続を削除します。
- デリバリーグループに、サポートされていないホストのマスターイメージで作成されたカタログのマシンが含まれている場合は、それらのマシンをグループから削除します。

- サポートされていないホストのマスターイメージを使用して作成されたすべてのカタログを削除(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/machine-catalogs-manage.html#delete-a-catalog)。

PvDまたはAppDisksコンポーネントがインストールされているVDA

PvDおよびAppDisksテクノロジーを有効にするコンポーネントがVDAにインストールされている場合、それらのコンポーネントが削除されるまで、そのVDAはアップグレードできません。

> **注:**
>
> バージョン1912にアップグレードする場合、現在のVDAをアンインストールしてから、新しいVDAをインストールする必要がありました。このバージョンでは、Citrixがコンポーネントを削除してアップグレードを続行するかどうかを尋ねられます。

> AppDiskおよびPvDコンポーネントは、それらのテクノロジーを一度も使用していなかったとしても、以前のVDAバージョンでインストールされている可能性があります。

- グラフィカルインターフェイス：VDAインストーラーでは、**追加コンポーネント**ページに**Citrix AppDisk / Personal vDisk**オプションが含まれていました。7.15 LTSRおよびそれ以前の7.xリリースでは、このオプションがデフォルトで有効になっていました。そのため、デフォルトを受け入れた場合（または、このオプションを提供するリリースで明示的に有効にした場合）、そのコンポーネントがインストールされました。
- CLI：`/baseimage`オプションを指定すると、コンポーネントがインストールされました。

対処法

VDAインストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出しない場合、アップグレードは通常どおり続行されます。

インストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出した場合：

- グラフィカルインターフェイス：アップグレードは一時停止します。サポートされていないコンポーネントを自動的に削除するかどうかを尋ねるメッセージが表示されます。**OK**をクリックすると、コンポーネントが自動的に削除され、アップグレードが続行されます。
- CLI：コマンドの失敗を避けるため、コマンドに次のオプションを含めます：
  - `/remove_appdisk_ack`

- `/remove_pvd_ack`

制限事項

アップグレードには次の制限が適用されます。

- **選択的なコンポーネントのインストール：** 新しいバージョンにコンポーネントをインストールまたはアップグレードしても、アップグレードが必要な他のコンポーネント（別のマシン上）をアップグレードしないことを選択した場合、Studioから通知されます。たとえば、アップグレードにControllerとStudioの新しいバージョンが含まれているとします。Controllerはアップグレードしましたが、Studioがインストールされているマシンでインストーラーを実行しませんでした。Studioは、Studioをアップグレードするまでサイトの管理を続行できません。

  VDAをアップグレードする必要はありませんが、利用可能なすべての機能を使用できるように、すべてのVDAをアップグレードすることをお勧めします。
- **早期リリースまたはテクノロジープレビューバージョン:** 早期リリース、テクノロジープレビュー、またはプレビューバージョンからアップグレードすることはできません。
- **以前のオペレーティングシステム上のコンポーネント:** MicrosoftまたはCitrixによってサポートされなくなったオペレーティングシステムに、現在のVDAをインストールすることはできません。詳しくは、「以前のオペレーティングシステム」を参照してください。
- **混在環境/サイト：** 以前のバージョンのサイトと現在のバージョンのサイトを継続して実行する必要がある場合は、「混在環境に関する考慮事項」を参照してください。
- **製品の選択：** 以前のバージョンからアップグレードする場合、インストール時に設定された製品（Citrix Virtual AppsまたはCitrix Virtual Apps and Desktops）を選択または指定することはありません。

混在環境に関する考慮事項

アップグレード時には、エディションとバージョンに含まれるすべての新しい機能と強化された機能にアクセスできるように、すべてのコンポーネントとVDAをアップグレードすることをお勧めします。

たとえば、以前のControllerバージョンを含む展開で現在のVDAを使用することはできますが、現在のリリースの一部の新機能は利用できない場合があります。また、最新ではないバージョンを使用している場合、VDAの登録に関する問題が発生する可能性もあります。

環境によっては、すべてのVDAを最新バージョンにアップグレードできない場合があります。その場合、マシンカタログを作成するときに、マシンにインストールされているVDAバージョンを指

定できます。（これは機能レベルと呼ばれます。）デフォルトでは、この設定は推奨される最小VDAバージョンを指定します。ほとんどの展開では、デフォルト値で十分です。カタログにデフォルトよりも古いVDAが含まれている場合にのみ、設定を以前のバージョンに変更することを検討してください。マシンカタログでVDAバージョンを混在させることはお勧めしません。

カタログがデフォルトの最小VDAバージョン設定で作成され、1つ以上のマシンにデフォルトバージョンよりも古いVDAがある場合、それらのマシンはControllerに登録できず、機能しません。

詳細については、VDAバージョンと機能レベルを参照してください。

異なるバージョンを持つ複数のサイト

環境に異なる製品バージョンのサイト（例：XenDesktop 7.18サイトとCitrix Virtual Apps and Desktops 1909サイト）が含まれている場合、Citrixでは、異なる製品バージョンのアプリケーションとデスクトップを集約するためにStoreFrontを使用することをお勧めします。詳細については、(/ja-jp/storefront.html)のドキュメントを参照してください。

混在環境では、各リリースに対応するStudioおよびDirectorのバージョンを引き続き使用しますが、異なるバージョンは別々のマシンにインストールされていることを確認してください。

以前のオペレーティングシステム

サポートされているオペレーティングシステム（OS）バージョンを実行しているマシンに、コンポーネントの以前のバージョンをインストールしたとします。現在、より新しいコンポーネントバージョンを使用したいと考えていますが、そのOSは現在のコンポーネントバージョンではサポートされていません。

例えば、Windows Server 2008 R2マシンにサーバーVDAをインストールしたとします。現在、そのVDAを現在のリリースにアップグレードしたいと考えていますが、アップグレード先の現在のリリースではWindows Server 2008 R2はサポートされていません。

サポートされなくなったオペレーティングシステムにコンポーネントをインストールまたはアップグレードしようとすると、「このオペレーティングシステムにはインストールできません」などのエラーメッセージが表示されます。

これらの考慮事項は、Current ReleaseおよびLong Term Service Releaseバージョンのアップグレードに適用されます。（LTSRバージョンにCUを適用することには影響しません。）

サポートされているOSについては、以下のリンクを参照してください。

- Citrix Virtual Apps and Desktops (現在のリリース):
    - デリバリーコントローラー、Studio、Director、VDA、ユニバーサルプリントサーバー

  - (/ja-jp/federated-authentication-service/system-requirements.html)
  - (/ja-jp/storefront.html)、(/ja-jp/self-service-password-reset.html)、および(/ja-jp/session-recording.html)については、現在のリリースのシステム要件の記事を参照してください。

- LTSRについては、お使いのLTSRバージョンとCUのコンポーネントリストを参照してください。（メインの(/ja-jp/citrix-virtual-apps-desktops.html)製品ドキュメントページからLTSRバージョンを選択してください。）

無効なオペレーティングシステム

次の表に、現在のリリースでコンポーネントのインストール/アップグレードに無効な以前のオペレーティングシステムを示します。各OSでサポートされる最新の有効なコンポーネントバージョンと、インストールおよびアップグレードが無効になったコンポーネントバージョンを示します。

表のオペレーティングシステムには、サービスパックとアップデートが含まれます。

オペレーティングシステム	コンポーネント/機能	最新の有効なバージョン	このバージョン以降はインストール/アップグレード不可
Windows 7および Windows 8	VDA	7.15 LTSR	7.16
Windows 7および Windows 8	その他のインストーラーコンポーネント	7.17	7.18
1607より前の Windows 10バージョン	VDA	7.15 LTSR	7.16
Windows 10 x86 バージョン	VDA	1906.2.0	1909
Windows サーバー 2008 R2	VDA	7.15 LTSR	7.16
Windows サーバー 2008 R2	その他のインストーラーコンポーネント	7.17	7.18
Windows サーバー 2012	VDA	7.15 LTSR	7.16

オペレーティングシステム	コンポーネント/機能	最新の有効なバージョン	このバージョン以降はインストール/アップグレード不可
Windows サーバー 2012	その他のインストーラーコンポーネント	7.17	7.18
ウィンドウズ サーバー 2012 R2	その他のインストーラーコンポーネント *	1912 LTSR	2003
ウィンドウズ サーバー 2012 R2	サーバーVDI	7.15 LTSR	7.16

Windows XPおよびWindows Vistaは、7.xのコンポーネントまたはテクノロジーでは無効です。

* Delivery Controller、Studio、Director、およびVDAに適用されます。

実行できること

選択肢があります。次のことができます。

- 現在のOSを継続して使用する(#continue-with-the-current-os)
- マシンを再イメージ化またはアップグレードする(#reimage-or-upgrade-the-machine)
- 新しいマシンを追加してから古いマシンを削除する(#add-new-machines-and-then-remove-old-machines)

現在のOSを継続して使用する

これらの方法はVDAで実行可能です。以前のOSを搭載したマシンの使用を継続する場合は、次のいずれかを選択できます。

- インストールされているコンポーネントバージョンを継続して使用する。
- 最新の有効なコンポーネントバージョンをダウンロードし、そのバージョンにコンポーネントをアップグレードする。（これは、最新の有効なコンポーネントバージョンがまだインストールされていないことを前提としています。）

たとえば、Windows 7 SP1マシンに7.14 VDAがインストールされているとします。Windows 7 OSマシンで有効な最新のVDAバージョンは、XenApp and XenDesktop 7.15 LTSRです。7.14を継続して使用するか、7.15 LTSR VDAをダウンロードしてVDAをそのバージョンにアップグレードすることができます。これらの以前のVDAバージョンは、新しいバージョンのDelivery Controllerを

含む展開で機能します。たとえば、7.15 LTSR VDAはCitrix Virtual Apps and Desktops 7 1808 Controllerに接続できます。

マシンの再イメージ化またはアップグレード

これらの方法は、VDAおよびコアコンポーネント（Delivery Controllerなど）がインストールされていないその他のマシンで実行可能です。次のいずれかを選択してください。

- マシンをサービスから外し（メンテナンスモードをオンにしてすべてのセッションを閉じさせてから）、サポートされているWindows OSバージョンに再イメージ化し、コンポーネントの最新バージョンをインストールします。
- VDAマシンでOSを再イメージ化せずにアップグレードするには、まずアップグレード先のOSでサポートされているVDAバージョンをインストールするか、OSアップグレード後にVDAをアップグレードする必要があります。そうしないと、Citrixソフトウェアはサポートされていない状態になります。

新しいマシンを追加し、古いマシンを削除する

この方法は、Delivery Controller™ またはその他のコアコンポーネントを含むマシンでOSをアップグレードする必要がある場合に実行可能です。

Citrix は、サイト内のすべてのコントローラーが同じ OS を持つことを推奨しています。以下のアップグレードシーケンスは、異なるコントローラーが異なる OS を持つ期間を最小限に抑えます。

1. サイト内のすべてのDelivery Controllerのスナップショットを取得し、サイトデータベースをバックアップします。
2. サポートされているオペレーティングシステムを搭載したクリーンなサーバーに新しいDelivery Controllerをインストールします。たとえば、2台のWindows Server 2016マシンにControllerをインストールします。
3. 新しいControllerをサイトに追加します。
4. 現在のリリースで有効でないオペレーティングシステムで実行されているControllerを削除します。たとえば、2台のWindows Server 2008 R2マシン上の2つのControllerを削除します。Delivery Controllers でControllerを削除するための推奨事項に従ってください。

準備

アップグレードを開始する前に、以下の情報を確認し、必要なタスクを完了してください。

> **注:**

> VDAのアップグレードはアップグレードシーケンス の後半で行われますが、アップグレードを開始する前にインストーラーを選択し、手順を確認して、何が予想されるかを知っておくことをお勧めします。

インストーラーとインターフェイスを選択する

コンポーネントをアップグレードするには、製品ISOからフルプロダクトインストーラーを使用します。VDAは、フルプロダクトインストーラーまたはスタンドアロンVDAインストーラーのいずれかを使用してアップグレードできます。すべてのインストーラーは、グラフィカルインターフェイスとコマンドラインインターフェイスを提供します。

詳細については、インストーラー を参照してください。

インストールの詳細: 準備作業を完了し、インストーラーを起動する準備ができたら、インストール記事には、表示される内容 (グラフィカルインターフェイスを使用している場合) または入力する内容 (コマンドラインインターフェイスを使用している場合) が示されています。

- グラフィカルインターフェイスを使用してコアコンポーネントをインストール/アップグレードする
- コマンドラインを使用してコアコンポーネントをインストール/アップグレードする
- グラフィカルインターフェイスを使用してVDAをインストール/アップグレードする
- コマンドラインを使用してVDAをインストール/アップグレードする

シングルセッションVDAを`VDAWorkstationCoreSetup.exe`インストーラーで最初にインストールした場合、Citrixではそのインストーラーを使用してアップグレードすることをお勧めします。フル製品VDAインストーラーまたは`VDAWorkstationSetup.exe`インストーラーを使用してVDAをアップグレードすると、アップグレードから明示的に除外しない限り、元々除外されていたコンポーネントがインストールされる可能性があります。

VDAを現在のリリースにアップグレードする際、アップグレードプロセス中にマシンの再起動が発生します（この要件は7.17リリースから始まりました）。これは回避できません。再起動後、アップグレードは自動的に再開されます（コマンドラインで`/noresume`を指定しない限り）。

データベース操作

サイト、監視、および構成ログデータベースをバックアップします。CTX135207の手順に従ってください。アップグレード後に問題が発見された場合、バックアップを復元できます。

サポートされなくなったSQL Serverバージョンのアップグレードについては、SQL Serverバージョンチェックを参照してください。(これは、サイト、監視、および構成ログデータベースに使用されるSQL Serverを指します。)

Microsoft SQL Server Express LocalDBは、ローカルホストキャッシュで使用するために自動的にインストールされます。以前のバージョンを置き換える必要がある場合、新しいバージョンはSQL Server Express LocalDB 2019である必要があります。コンポーネントとサイトをアップグレードした後にSQL Server Express LocalDBを新しいバージョンに置き換える方法の詳細については、SQL Server Express LocalDBの置き換えを参照してください。

Citrixライセンスが最新であることを確認する

Citrixライセンスの管理に関する包括的な情報については、Citrixライセンスのアクティブ化、アップグレード、および管理を参照してください。

フル製品インストーラーを使用してライセンスサーバーをアップグレードできます。または、ライセンスコンポーネントを個別にダウンロードしてアップグレードすることもできます。アップグレードを参照してください。

アップグレードする前に、Customer Success Services / Software Maintenance / Subscription Advantageの日付が新しい製品バージョンに対して有効であることを確認してください。日付は2021.11.15以降である必要があります。

Citrixライセンスサーバーが互換性があることを確認してください

Citrixライセンスサーバーが新しいバージョンと互換性があることを確認してください。これを行うには、2つの方法があります。

- 他のCitrixコンポーネントをアップグレードする前に、Delivery Controllerを含むマシンでISOレイアウトから`XenDesktopServerSetup.exe`インストーラーを実行します。互換性の問題がある場合、インストーラーは問題を解決するための推奨手順とともにそれを報告します。
- インストールメディアの`XenDesktop Setup`ディレクトリから、コマンド`.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`を実行します。表示により、ライセンスサーバーが互換性があるかどうかが示されます。ライセンスサーバーに互換性がない場合は、ライセンスサーバーをアップグレードしてください。

StoreFrontの変更をバックアップする

アップグレードを開始する前に、`C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`内のファイル（*default.ica*や*usernamepassword.tfrm*など）に変更を加えている場合は、各ストアについてそれらをバックアップしてください。アップグレード後、それらを復元して変更を元に戻すことができます。

アプリケーションとコンソールを閉じる

アップグレードを開始する前に、管理コンソールやPowerShellセッションなど、ファイルロックを引き起こす可能性のあるすべてのプログラムを閉じます。

マシンを再起動すると、ファイルロックがすべて解除され、保留中のWindowsアップデートがないことが保証されます。

アップグレードを開始する前に、サードパーティの監視エージェントサービスをすべて停止して無効にします。

適切な権限があることを確認する

ドメインユーザーであることに加えて、製品コンポーネントをアップグレードするマシンではローカル管理者である必要があります。

サイトデータベースとサイトは、自動または手動でアップグレードできます。データベースを自動アップグレードする場合、Studioユーザーの権限には、SQL Serverデータベーススキーマを更新する機能（たとえば、`db_securityadmin`または`db_owner`データベースロール）が含まれている必要があります。詳細については、「データベース」を参照してください。

Studioユーザーがこれらの権限を持っていない場合、手動データベースアップグレードを開始すると、スクリプトが生成されます。Studioユーザーは、Studioから一部のスクリプトを実行します。データベース管理者は、SQL Server Management Studioなどのツールを使用して、他のスクリプトを実行します。

その他の準備タスク

- 必要に応じて、テンプレートをバックアップし、ハイパーバイザーをアップグレードします。
- 事業継続計画で定められているその他の準備タスクを完了します。

サイトの事前テスト

Delivery Controllerとサイトをアップグレードすると、実際のアップグレードが開始される前にサイトの事前テストが実行されます。これらのテストでは、次のことを確認します。

- サイトデータベースにアクセスでき、バックアップされていること
- 重要なCitrixサービスへの接続が正しく機能していること
- Citrixライセンスサーバーのアドレスが利用可能であること
- 構成ログデータベースにアクセスできること

- パブリッククラウドホスト接続（AWSなど）を追加する場合は、Hybrid Rights Licenseがあることを確認してください。そうしないと、サイトの事前テストが一時停止または停止し、説明メッセージが表示されます。

テストの実行後、結果のレポートを表示できます。検出された問題を修正し、テストを再度実行できます。サイトの事前テストを実行せず、問題を解決しないと、サイトの動作に影響を与える可能性があります。

テスト結果を含むレポートは、インストールログと同じディレクトリにあるHTMLファイル（`PreliminarySiteTestResult.html`）です。そのファイルが存在しない場合は作成されます。ファイルが存在する場合は、その内容が上書きされます。

テストを実行する

- インストーラーのグラフィカルインターフェイスを使用してアップグレードする場合、ウィザードには、テストを開始してレポートを表示できるページが含まれています。テストが実行され、レポートを確認し、検出された問題を解決した後、テストを再実行できます。テストが正常に完了したら、次へをクリックしてウィザードを続行します。
- コマンドラインインターフェイスを使用してアップグレードする場合、テストは自動的に実行されます。デフォルトでは、テストが失敗した場合、アップグレードは実行されません。レポートを表示して問題を解決した後、コマンドを再実行してください。

Citrixでは、Controllerとサイトのアップグレードを続行する前に、必ずサイトの事前テストを実行し、すべての問題を解決することをお勧めします。テストを実行するのにかかるわずかな時間で得られる潜在的なメリットは十分にあります。ただし、この推奨されるアクションを上書きすることもできます。

- グラフィカルインターフェイスを使用してアップグレードする場合、テストをスキップしてアップグレードを続行することを選択できます。
- コマンドラインからアップグレードする場合、テストをスキップすることはできません。デフォルトでは、サイトテストが失敗すると、アップグレードを実行せずにインストーラーが失敗します。ほとんどの場合、`/ignore_site_test_failure` オプションを含めると、テストの失敗は無視され、アップグレードが続行されます。(例外については、SQL Server のバージョンチェック を参照してください。)

複数のControllerをアップグレードする場合

1つのControllerでアップグレードを開始し、その後、同じサイト内の別のControllerでアップグレードを開始した場合（最初のアップグレードが完了する前）：

- 最初のControllerで予備サイトテストが完了している場合、他のControllerのウィザードには予備サイトテストページは表示されません。
- 他のControllerでアップグレードを開始したときに最初のControllerでのテストが進行中の場合、他のControllerのウィザードにサイトテストページが表示されます。ただし、最初のControllerでのテストが完了すると、最初のControllerからのテスト結果のみが保持されます。

サイトの健全性に関連しないテストの失敗

- 予備サイトテストがメモリ不足で失敗した場合は、より多くのメモリを確保してからテストを再実行してください。
- アップグレードの権限はあるがサイトテストを実行する権限がない場合、予備サイトテストは失敗します。これを解決するには、テストを実行する権限を持つユーザーアカウントでインストーラーを再実行してください。

SQL Server のバージョンチェック

Citrix Virtual Apps and Desktopsの展開を成功させるには、サイト、モニター、および構成ログデータベース用にサポートされているバージョンのMicrosoft SQL Serverが必要です。サポートされなくなったSQL ServerバージョンでCitrix展開をアップグレードすると、機能上の問題が発生し、サイトがサポートされなくなる可能性があります。

アップグレードするCitrixリリースでサポートされているSQL Serverのバージョンを確認するには、そのリリースのシステム要件 の記事を参照してください。

Controllerをアップグレードする際、Citrixインストーラーは、サイト、モニター、および構成ログデータベースに使用されている現在インストールされているSQL Serverのバージョンを確認します。

- チェックの結果、現在インストールされているSQL Serverのバージョンが、アップグレードするCitrixリリースでサポートされているバージョンではないと判断された場合：
  - グラフィカルインターフェイス：アップグレードはメッセージとともに停止します。**I understand** をクリックし、次に **Cancel** をクリックしてCitrixインストーラーを閉じます。（アップグレードを続行することはできません。）
  - コマンドラインインターフェイス: コマンドは失敗します (コマンドに `/ignore_db_check_failure` オプションを含めた場合でも)。

  SQL Serverのバージョンをアップグレードしてから、Citrixのアップグレードを再度開始してください。

- チェックで現在インストールされているSQL Serverのバージョンを特定できない場合は、現在インストールされているバージョンがアップグレード先のバージョンでサポートされているかどうかを確認してください（システム要件）。
    - グラフィカルインターフェイス: アップグレードはメッセージとともに停止します。
        - 現在インストールされているSQL Serverのバージョンがサポートされている場合は、**I understand**をクリックしてメッセージを閉じ、**Next**をクリックしてCitrixのアップグレードを続行します。
        - 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、**I understand**をクリックしてメッセージを閉じ、**Cancel**をクリックしてCitrixのアップグレードを終了します。SQL Serverをサポートされているバージョンにアップグレードしてから、Citrixのアップグレードを再度開始してください。
    - コマンドラインインターフェイス: コマンドはメッセージとともに失敗します。メッセージを閉じた後:
        - 現在インストールされているSQL Serverのバージョンがサポートされている場合は、`/ignore_db_check_failure` オプションを指定してコマンドを再度実行します。
        - 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、SQL Serverをサポートされているバージョンにアップグレードします。コマンドを再度実行してCitrixのアップグレードを開始します。

SQL Serverのアップグレード

新しいSQL Serverを立ち上げてサイトデータベースを移行する場合、接続文字列を更新する必要があります。

サイトが現在、サイトデータベースにSQL Server Expressを使用している場合 (Citrixがサイト作成時に自動的にインストールしたもの):

1. 最新のSQL Server Expressバージョンをインストールします。
2. データベースをデタッチします。
3. データベースを新しいSQL Server Expressにアタッチします。
4. 接続文字列を移行します。

詳しくは、「接続文字列の構成」およびMicrosoft SQL Serverの製品ドキュメントを参照してください。

SQL Server Express LocalDBの置き換え

Microsoft SQL Server Express LocalDB は、Local Host Cache がスタンドアロンで使用する SQL Server Express の機能です。Local Host Cache は、SQL Server Express LocalDB 以外の SQL Server Express のコンポーネントを必要としません。

Citrix は SQL Server Express LocalDB を自動的に更新しません。SQL Server Express LocalDB のバージョンを更新するには、このセクションのガイダンスに従ってください。

- Delivery Controller を Citrix Virtual Apps and Desktops バージョン 2203 LTSR 以降のバージョンにアップグレードする場合、サポートされるバージョンは SQL Server Express LocalDB 2019 または SQL Server Express LocalDB 2022 です。

必要なもの:

- Citrix Virtual Apps and Desktopsのインストールメディア。
- Windows SysinternalsツールボックスのPsExecツール。

手順:

1. Citrix Virtual Apps and Desktopsのコンポーネント、データベース、およびサイトのアップグレードを完了します。（これらのデータベースアップグレードは、サイト、監視、および構成ログデータベースに影響します。SQL Server Express LocalDBを使用するLocal Host Cacheデータベースには影響しません。）
2. SQL Server Express LocalDBを更新したいDelivery Controllerにログオンします。
3. MicrosoftからPsExecをダウンロードし、そのDelivery Controller上のアクセスしやすい場所（例：C:\Temp）に配置します。
4. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを停止します。
5. Delivery Controller でコマンドプロンプトを開き、PsExec がある場所（例: `C:\Temp`）に移動してから、次のコマンドを実行して、Network Service アカウントでコマンドプロンプトを昇格させます。

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
   ```

6. `whoami`を実行して、コマンドプロンプトがNetwork Serviceアカウントとして実行されていることを確認します。次の出力が得られるはずです: `nt authority\networkservice`。
7. コマンドプロンプトを使用して、SQL LocalDBインスタンスに移動します:

- SQL LocalDB 2014からアップグレードする場合:

```
cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
```

- SQL LocalDB 2017からアップグレードする場合:

```
cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
```

- SQL LocalDB 2019からアップグレードする場合:

```
cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
```

8. SQL LocalDBインスタンスを停止して削除します: `CitrixHA`。

```
SqlLocalDB stop CitrixHA



SqlLocalDB delete CitrixHA
```

9. Delivery Controllerから以下のファイルを削除します:

```
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName.*

C:\Windows\ServiceProfiles\NetworkService\HADatabaseName_log.*

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName.* (if
exists)

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName_log.*
(if exists)
```

10. プログラムを削除するためのWindowsのネイティブ機能を使用して、Delivery Controllerから既存のSQL LocalDB SQL Server Expressをアンインストールします。
11. アンインストールが完了したら、Delivery Controllerを再起動します。
12. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを停止します。

13. Citrix Virtual Apps and Desktopsのインストールメディアを Delivery Controllerにマウントします。
14. Delivery Controllerに管理者としてSQL Server Express LocalDB 2019をインストールします。
    a. Citrix Virtual Apps and Desktopsインストールメディアの `Support > SQLLocalDB` フォルダーにある `sqllocaldb.msi` ファイルを使用します。たとえば、インストールメディアが `E drive` ドライブにマウントされている場合、ファイルは `E:\Support\SQLLocalDB\sqllocaldb.msi` にあります。インストールを完了するには再起動が必要です。
    b. 新しいSQL LocalDBは `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` にある必要があります。
15. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを開始します。
16. Delivery Controllerのコマンドプロンプトで、 `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` に移動し、 `SqlLocalDB i` を実行してCitrixHAインスタンスが作成されたことを確認します。返されたインスタンスのリストに `CitrixHA` が含まれている必要があります。

    > **注:**
    >
    > Citrix High Availability Serviceの開始後、CitrixHAデータベースが作成されるまでに最大15分かかる場合があります。

17. ローカルホストキャッシュデータベースファイルが作成されていることを確認し、必要に応じて高可用性サービス（セカンダリブローカー）が引き継ぐことができることを確認します。
    a. Delivery Controllerで、 `C:\Windows\ServiceProfiles\NetworkService` を参照します。
    b. `HaDatabaseName.mdf` と `HaDatabaseName_log.ldf` が作成されていることを確認します。
18. 残りのDelivery Controllerで手順を繰り返します。

VDAアップグレードエージェントのプロキシサポート

VDAアップグレードエージェントのプロキシサポートは、2311 VDAで追加されました。

2311 VDA (バージョン: 7.40) のVDAアップグレードエージェントは、プロキシを介してトラフィックを認識し、送信できます。

VDAアップグレードエージェント (VUA) は、Hostname:Port (IP:Port) およびPACファイルの形式でプロキシをサポートしています。

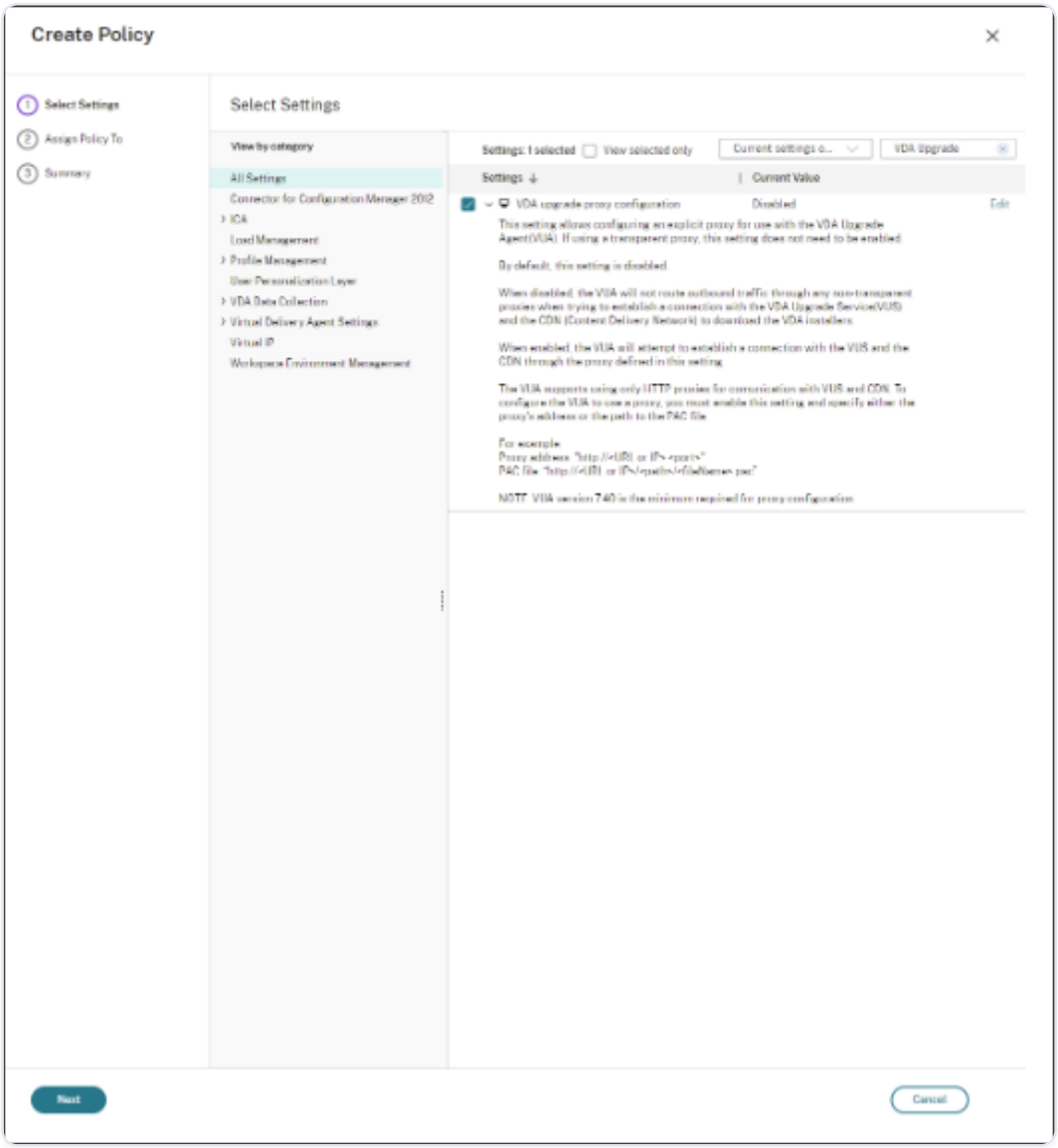
HTTPプロキシのみがサポートされています。 パケットの復号化と検査はサポートされていません。

プロキシ認証はサポートされていません。 SOCKS5はサポートされていません。

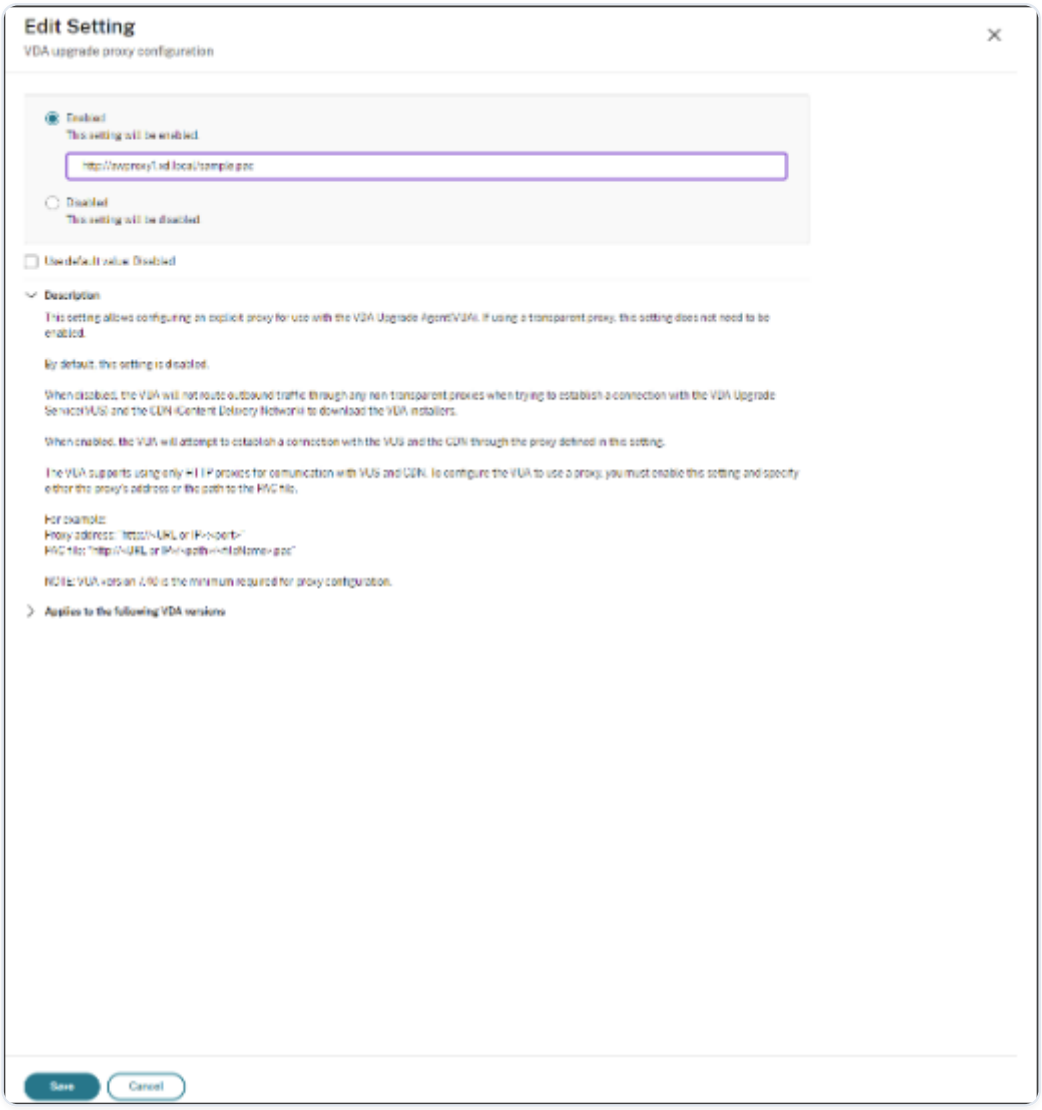
VDAアップグレードエージェントプロキシの構成

VDAアップグレードエージェントプロキシは、次の2つの方法で構成できます。

1. **Webstudioポリシー**を使用して**VDAアップグレードエージェントポリシーを構成**する。
2. **ポリシーの作成**ページで、**設定**から**VDAアップグレードプロキシ構成**を選択します。



3. この設定を有効にします。デフォルトでは、この設定は無効になっています。



4. レジストリキーを使用したVDAアップグレードエージェントの構成。

   レジストリキーは、VDAインストール中にMeta-Installerに設定されます。

   レジストリ:

   キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`

   値の型: 文字列

   値の名前: ProxySettings

   値のデータ: プロキシアドレスまたはPACファイルへのパス。

   例:

   a. プロキシアドレス: `http://<URL or IP>:<port>`

b. PACファイル: `http://<URL or IP>/<path/<filename>.pac`

セキュリティ

FIDO2およびWebAuthn認証

FIDO2およびWebAuthnを使用したローカル認証と仮想認証

ユーザーは、FIDO2セキュリティキー、TPM 2.0およびWindows Hello対応の統合生体認証デバイスを使用して、仮想セッションでFIDO2またはWebAuthnを活用するアプリケーションに認証できます。

FIDO2の詳細については、「FIDO2: WebAuthn & CTAP」を参照してください。

この機能の使用方法については、「FIDO2 redirection」を参照してください。

> **注**
>
> この機能は、WebAuthnまたはFIDO2を使用した仮想セッションへのログオンをサポートしていません。この機能は、仮想セッション内のアプリケーションでこれらの認証方法を使用することのみを許可します。

> この機能は、ダブルホップシナリオではサポートされていません。

サポートマトリックス

セッションホストオペレーティングシステム	WEBアプリケーション認証	UWPアプリケーション認証
Windows サーバー 2016	USBリダイレクト経由でサポート	サポートされていません
ウィンドウズ サーバー 2019	対応	非対応
ウィンドウズ サーバー 2022	対応	対応
ウィンドウズ 10	対応	対応

セッションホストオペレーティングシステム	WEBアプリケーション認証	UWPアプリケーション認証
ウィンドウズ 11	対応	対応

詳細については、以下の要件を確認してください。

Webアプリケーション認証

要件

WebアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

Citrix® コントロールプレーン

- シトリックス Virtual Apps and Desktops™ 2009 以降

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - ウィンドウズ サーバー 2019 以降
- VDA
  - Windows: バージョン2009以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux: Workspace app for Linuxのシステム要件を参照してください。
- Workspaceアプリ
  - Windows: バージョン2009.1以降
  - Linux: 2303以降

Webブラウザーの要件

- 64ビットブラウザーのみ

サポートされている認証方法

- FIDO2セキュリティキー
- ウィンドウズ ハロー
  - TPM 2.0
  - 統合生体認証
    - 顔認証
    - 指紋スキャナー
  - WebAuthn

UWPアプリケーション認証

Citrix Virtual Apps and Desktops 2112のリリースにより、CitrixはUWPアプリケーションでのWebAuthnおよびFIDO2認証をサポートします。

Microsoft Teams、Office 365向けMicrosoft Outlook、OneDriveなどのアプリケーションは、Azure Active Directoryへのリンクとして認証にUWPアプリケーションを使用します。Citrixは現在、FIDO2を使用してこれらのアプリケーションを認証することをサポートしています。

要件

UWPアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

Citrixコントロールプレーン

- シトリックス バーチャルアプリおよびデスクトップ 2112 以降

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - ウィンドウズ サーバー 2022 以降
- VDA
  - Windows: バージョン2112以降

クライアントデバイス

- オペレーティングシステム

- Windows 10 1809以降
- Linux: Workspace app for Linuxのシステム要件を参照してください。

- Workspaceアプリ
  - Windows: バージョン2009.1以降
  - Linux: 2303 以降

サポートされている認証方法

- FIDO2 セキュリティキー
- ウィンドウズ ハロー
  - TPM 2.0
  - 統合された生体認証
    - 顔認証
    - 指紋スキャナー
  - WebAuthn

> **注記:**

> クライアント、VDA、またはオペレーティングシステムで機能がサポートされていないためFIDO2リダイレクトが利用できないシナリオでは、USBベースのFIDO2キーをUSBリダイレクトを使用してリダイレクトできます。 FIDO2リダイレクトが利用可能なシナリオでも、USBリダイレクトを使用してUSBベースのFIDO2キーをリダイレクトすることが可能です。この場合、FIDO2リダイレクトを無効にし、適切なUSBリダイレクトルールを構成する必要があります。 USBリダイレクトルールを使用してFIDO2キーを構成する方法の詳細については、USBリダイレクトデバイスルール のドキュメントを参照してください。

msedgewebview2.exe ベースのアプリケーションの高度な構成

> **注記:**

> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。 レジストリエディターの使用

> は、お客様ご自身の責任で行ってください。編集する前に、必ずレジストリをバックアップしてください。

> msedgewebview2.exe ベースのWebアプリケーションを使用している企業の場合、HDXセッション内でFIDO2リダイレクトが機能するように、VDAに追加のレジストリ値を追加する必要があります。

「AllowedProcesses」レジストリ値にmsedgewebview2.exeのフルパスを追加します。

- キー: HKLM\SOFTWARE\Citrix\WebAuthnAllowedProcesses
- 値の名前: AllowedProcesses
- 値の型: REG_MULTISZ
- 値のデータ: `<add full path of the msedgewebview2.exe here >`

64ビットアプリケーションの場合、以下の値を設定する必要があります。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\msedgewebview2
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: FilePathName
- 値の型: REG_SZ
- 値のデータ: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: Flag
- 値の型: DWORD
- 値のデータ: 00000002

32ビットアプリケーションの場合、以下の値を設定する必要があります。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: FilePathName
- 値の型: REG_SZ
- 値のデータ: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: Flag
- 値の型: DWORD
- 値のデータ: 00000002

msedgewebview2.exeベースのアプリケーションでFIDO2リダイレクトを有効にするためのレジストリ値を設定した後、VDAを再起動します。

シトリックス バーチャル アプリケーションズ アンド デスクトップス™ と シトリックス ゲートウェイ の統合

StoreFront™ サーバーは、公開されたリソースとデータへのアクセスを管理するために展開および構成されます。リモートアクセスの場合、StoreFront の前に Citrix Gateway を追加することをお勧めします。

> **注:**
>
> Citrix Virtual Apps and Desktops と Citrix Gateway を統合する方法の詳細な構成手順については、StoreFront のドキュメントを参照してください。

> 以下の図は、Citrix Gateway を含む簡素化されたCitrix展開の例を示しています。Citrix Gateway は、Citrix Virtual Apps and Desktops によって配信されるアプリとデータを保護するために、StoreFront と通信します。ユーザーデバイスは、安全な接続を作成し、アプリ、デスクトップ、ファイルにアクセスするために、Citrix Workspace™ app を実行します。

Citrix Gateway を含む簡素化された Citrix 展開(/en-us/citrix-virtual-apps-desktops/2311/media/sample-deployment-overview.png)

ユーザーはCitrix Gatewayを使用してログオンし、認証します。Citrix GatewayはDMZに展開され、保護されています。2要素認証が構成されています。ユーザーの資格情報に基づいて、ユーザーには関連するリソースとアプリケーションが提供されます。アプリケーションとデータは適切なサーバー上にあります（図には示されていません）。セキュリティ上機密性の高いアプリケーションとデータには、個別のサーバーが使用されます。

セキュリティに関する考慮事項とベストプラクティス

注:

組織は、規制要件を満たすために特定のセキュリティ標準に準拠する必要がある場合があります。このようなセキュリティ標準は時間とともに変化するため、このドキュメントではこの主題については扱いません。セキュリティ標準とCitrix製品に関する最新情報については、`<http://www.citrix.com/security/>`を参照してください。

セキュリティのベストプラクティス

環境内のすべてのマシンをセキュリティパッチで最新の状態に保ちます。利点の1つは、シンクライアントをターミナルとして使用できるため、このタスクが簡素化されることです。

環境内のすべてのマシンをアンチウイルスソフトウェアで保護します。

プラットフォーム固有のマルウェア対策ソフトウェアの使用を検討してください。

ソフトウェアをインストールする際は、提供されているデフォルトパスにインストールしてください。

- 提供されているデフォルトパス以外のファイル場所にソフトウェアをインストールする場合は、制限付きアクセス許可などの追加のセキュリティ対策をファイル場所に追加することを検討してください。

すべてのネットワーク通信は、セキュリティポリシーに合わせて適切に保護および暗号化する必要があります。IPSecを使用してMicrosoft Windowsコンピューター間のすべての通信を保護できます。これを行う方法の詳細については、オペレーティングシステムのドキュメントを参照してください。さらに、ユーザーデバイスとデスクトップ間の通信は、デフォルトで128ビット暗号化に構成されているCitrix SecureICAを介して保護されます。SecureICAは、デリバリーグループの作成または更新時に構成できます。

注:

Citrix SecureICAはICA/HDXプロトコルの一部ですが、トランスポート層セキュリティ (TLS) のような標準準拠のネットワークセキュリティプロトコルではありません。TLSを使用して、ユーザーデバイスとデスクトップ間のネットワーク通信を保護することもできます。TLSを構成するには、「トランスポート層セキュリティ (TLS)」を参照してください。

アカウント管理にはWindowsのベストプラクティスを適用してください。Machine Creation ServicesまたはProvisioning Servicesによって複製される前に、テンプレートまたはイメージ上にアカウントを作成しないでください。保存されている特権ドメインアカウントを使用してタスクをスケジュールしないでください。共有Active Directoryマシンアカウントを手動で作成しないでください。これらの慣行は、マシン攻撃がローカルの永続的なアカウントパスワードを取得し、それらを使用して他のユーザーに属するMCS/PVS共有イメージにログオンするのを防ぐのに役立ちます。

ファイアウォール

環境内のすべてのマシンを、必要に応じてエンクレーブ境界を含め、境界ファイアウォールで保護します。

環境内のすべてのマシンはパーソナルファイアウォールによって保護されている必要があります。コアコンポーネントとVDAをインストールする際、Windowsファイアウォールサービスが検出された場合（ファイアウォールが有効になっていない場合でも）、コンポーネントと機能の通信に必要なポートを自動的に開くように選択できます。これらのファイアウォールポートを手動で構成することもできます。別のファイアウォールを使用する場合は、手動で構成する必要があります。

従来の環境をこのリリースに移行する場合、既存の境界ファイアウォールの再配置や新しい境界ファイアウォールの追加が必要になる場合があります。たとえば、データセンター内の従来のクライアントとデータベースサーバーの間に境界ファイアウォールがあるとします。このリリースを使用する場合、その境界ファイアウォールは、仮想デスクトップとユーザーデバイスが一方にあり、データセンター内のデータベースサーバーとDelivery Controllerがもう一方にあるように配置する必要があります。したがって、データベースサーバーとControllerを格納するために、データセンター内にエンクレーブを作成することを検討してください。また、ユーザーデバイスと仮想デスクトップの間に保護を設けることも検討してください。

注:

TCPポート1494および2598はICAおよびCGPに使用されるため、データセンター外のユーザーがアクセスできるようにファイアウォールで開かれている可能性が高いです。Citrixは、管理インターフェイスが意図せず攻撃に対して開かれたままになる可能性を避けるため、これらのポートを他の目的で使用しないことを推奨します。ポート1494および2598は、Internet Assigned Number Authority (http://www.iana.org/) に正式に登録されています。

アプリケーションセキュリティ

管理者以外のユーザーが悪意のある操作を実行するのを防ぐため、VDAホストおよびローカルのWindowsクライアントで、インストーラー、アプリケーション、実行可能ファイル、スクリプトに対してWindows AppLockerルールを構成することをお勧めします。

ユーザー権限の管理

ユーザーには必要な機能のみを付与します。Microsoft Windowsの特権は、通常の方法でデスクトップに引き続き適用されます。ユーザー権利の割り当てを通じて特権を構成し、グループポリシーを通じてグループメンバーシップを構成します。このリリースの利点の1つは、デスクトップが保存されているコンピューターの物理的な制御を付与することなく、ユーザーにデスクトップへの管理者権限を付与できることです。

デスクトップの特権を計画する際には、次の点に注意してください。

- デフォルトでは、特権のないユーザーがデスクトップに接続すると、自身のユーザーデバイスのタイムゾーンではなく、デスクトップを実行しているシステムのタイムゾーンが表示されます。ユーザーがデスクトップを使用する際にローカル時間を確認できるようにする方法については、「デリバリーグループの管理」の記事を参照してください。
- デスクトップの管理者であるユーザーは、そのデスクトップを完全に制御できます。デスクトップが専用デスクトップではなくプールされたデスクトップである場合、そのユーザーは、将来のユーザーを含む、そのデスクトップの他のすべてのユーザーに対して信頼される必要があります。デスクトップのすべてのユーザーは、この状況によってデータセキュリティに潜在的に永続的なリスクがあることを認識する必要があります。この考慮事項は、単一のユーザーしか持たない専用デスクトップには適用されません。そのユーザーは、他のどのデスクトップでも管理者であってはなりません。
- デスクトップの管理者であるユーザーは、潜在的に悪意のあるソフトウェアを含むソフトウェアをそのデスクトップにインストールできるのが一般的です。また、ユーザーはデスクトップに接続されている任意のネットワーク上のトラフィックを監視または制御できる可能性もあります。

ログオン権限の管理

ログオン権限は、ユーザーアカウントとコンピューターアカウントの両方に必要です。Microsoft Windowsの特権と同様に、ログオン権限は通常の方法でデスクトップに引き続き適用されます。ユーザー権利の割り当てを通じてログオン権限を構成し、グループポリシーを通じてグループメンバーシップを構成します。

Windowsのログオン権限は、ローカルでログオン、リモートデスクトップサービス経由でログオン、ネットワーク経由でログオン（ネットワークからこのコンピューターにアクセス）、バッチジョブとしてログオン、サービスとしてログオンです。

コンピューターアカウントの場合、コンピューターが必要とするログオン権限のみを付与します。「ネットワーク経由でこのコンピューターにアクセス」というログオン権限が必要です。

- VDAで、Delivery Controllerのコンピューターアカウントに対して
- Delivery Controllerで、VDAのコンピューターアカウントに対して。「Active Directory OUベースのController検出」(/ja-jp/advanced-concepts/implementation-guides/ad-ou-controller-discovery.html)を参照してください。
- StoreFront™サーバーで、同じStoreFrontサーバーグループ内の他のサーバーのコンピューターアカウントに対して

ユーザーアカウントの場合、ユーザーが必要とするログオン権限のみを付与します。

Microsoftによると、デフォルトでは、Remote Desktop Usersグループに「リモートデスクトップサービスを介したログオンを許可」というログオン権限が付与されます (ドメインコントローラーを除く)。

組織のセキュリティポリシーによっては、このグループをそのログオン権限から削除するよう明示的に規定している場合があります。次のアプローチを検討してください。

- マルチセッションOS用Virtual Delivery Agent (VDA) は、Microsoft Remote Desktop Servicesを使用します。Remote Desktop Usersグループを制限付きグループとして構成し、Active Directoryグループポリシーを介してグループのメンバーシップを制御できます。詳細については、Microsoftのドキュメントを参照してください。
- シングルセッションOS用VDAを含むCitrix Virtual Apps and Desktops™のその他のコンポーネントでは、Remote Desktop Usersグループは不要です。したがって、これらのコンポーネントでは、Remote Desktop Usersグループに「リモートデスクトップサービスを介したログオンを許可」というログオン権限は不要であり、削除できます。さらに：
  - Remote Desktop Servicesを介してそれらのコンピューターを管理する場合、そのようなすべての管理者がすでにAdministratorsグループのメンバーであることを確認してください。
  - Remote Desktop Servicesを介してそれらのコンピューターを管理しない場合、それらのコンピューターでRemote Desktop Services自体を無効にすることを検討してください。

「リモートデスクトップサービスを介したログオンを拒否」というログオン権限にユーザーとグループを追加することは可能ですが、ログオン拒否権限の使用は一般的に推奨されません。詳細については、Microsoftのドキュメントを参照してください。

ユーザー権限の構成

Delivery Controller™ のインストールにより、次の Windows サービスが作成されます。

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): VMのMicrosoft Active Directoryコンピューターアカウントを管理します。
- Citrix Analytics (NT SERVICE\CitrixAnalytics): サイト管理者が承認した場合、Citrix が使用するサイト構成の使用状況情報を収集します。その後、この情報を Citrix に送信し、製品の改善に役立てます。
- Citrix App Library (NT SERVICE\CitrixAppLibrary): AppDisk の管理とプロビジョニング、AppDNA 統合、および App-V の管理をサポートします。
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): 管理者がサイトに対して行ったすべての構成変更およびその他の状態変更を記録します。
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): 共有構成のためのサイト全体のリポジトリ。
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): 管理者に付与された権限を管理します。
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): 他の Delivery Controller サービスのセルフテストを管理します。
- Citrix Host Service (NT SERVICE\CitrixHostService): Citrix Virtual Apps または Citrix Virtual Desktops の展開で使用されるハイパーバイザーインフラストラクチャに関する情報を保存し、コンソールがハイパーバイザープール内のリソースを列挙するために使用する機能も提供します。
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): デスクトップ VM の作成をオーケストレーションします。
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Citrix Virtual Apps または Citrix Virtual Desktops のメトリックを収集し、履歴情報を保存し、トラブルシューティングおよびレポートツール用のクエリインターフェイスを提供します。
- Citrix Storefront Service (NT SERVICE\ CitrixStorefront): StoreFront の管理をサポートします。（StoreFront コンポーネント自体の一部ではありません。）
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): StoreFront の特権管理操作をサポートします。（StoreFront コンポーネント自体の一部ではありません。）

- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): メインサイトデータベースからローカルホストキャッシュに構成データを伝播します。
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): メインサイトデータベースが利用できない場合に、ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。

Delivery Controller のインストールでは、以下の Windows サービスも作成されます。これらは、他の Citrix コンポーネントと一緒にインストールされた場合にも作成されます。

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Citrixサポートが使用する診断情報の収集をサポートします。
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Citrixによる分析のために診断情報を収集します。これにより、管理者は分析結果と推奨事項を表示して、サイトの問題の診断に役立てることができます。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これは現在使用されていません。有効になっている場合は、無効にしてください。

- Citrix リモートブローカープロバイダー (NT SERVICE\XaXdCloudProxy)

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは現在使用されていませんが、有効にする必要があります。無効にしないでください。

- Citrix オーケストレーションサービス (NT SERVICE\CitrixOrchestration)
- Citrix トラストサービス (NT SERVICE\CitrixTrust)

Citrix Storefront Privileged Administration Service を除き、これらのサービスには、サービスとしてログオンするログオン権限と、プロセスのメモリクォータの調整、セキュリティ監査の生成、プロセスレベルトークンの置き換えの特権が付与されます。これらのユーザー権限を変更する必要はありません。これらの特権は Delivery Controller では使用されず、自動的に無効になります。

サービス設定の構成

Citrix Storefront Privileged Administration サービスと Citrix Telemetry Service を除き、ユーザー権限の構成 セクションに上記でリストされている Delivery Controller の Windows サービスは、NETWORK SERVICE ID としてログオンするように構成されています。これらのサービス設定を変更しないでください。

Citrix Config Synchronizer Serviceは、Delivery Controller上のローカル管理者グループにNETWORK SERVICEアカウントが属している必要があります。これにより、ローカルホストキャッシュが正しく機能します。

Citrix Storefront Privileged Administrationサービスは、ローカルシステム (NT AUTHORITY\SYSTEM) としてログオンするように構成されています。これは、通常サービスでは利用できないDelivery Controller StoreFront操作 (Microsoft IISサイトの作成を含む) に必要です。そのサービス設定を変更しないでください。

Citrix Telemetry Service は、サービス固有の ID としてログオンするように構成されています。

Citrix Telemetry Serviceは無効にできます。このサービスと、すでに無効になっているサービスを除き、これらのDelivery Controller Windowsサービスの他のサービスを無効にしないでください。

レジストリ設定の構成

VDAファイルシステムで8.3形式のファイル名とフォルダーの作成を有効にする必要はなくなりました。レジストリキー **NtfsDisable8dot3NameCreation** を構成して、8.3形式のファイル名とフォルダーの作成を無効にできます。これは、**fsutil.exe behavior set disable8dot3** コマンドを使用して構成することもできます。

展開シナリオのセキュリティへの影響

ユーザー環境には、組織によって管理されておらず、完全にユーザーの制御下にあるユーザーデバイス、または組織によって管理および運用されているユーザーデバイスのいずれかを含めることができます。これら2つの環境におけるセキュリティ上の考慮事項は、一般的に異なります。

管理対象ユーザーデバイス

管理対象ユーザーデバイスは管理制御下にあります。それらは、お客様自身の制御下にあるか、信頼できる別の組織の制御下にあります。ユーザーデバイスを直接ユーザーに構成して提供することも、単一のデスクトップが全画面モードでのみ実行されるターミナルを提供することもできます。すべての管理対象ユーザーデバイスについて、上記の一般的なセキュリティのベストプラクティスに従ってください。このリリースには、ユーザーデバイスに必要なソフトウェアが最小限であるという利点があります。

管理対象のユーザーデバイスは、全画面表示モードまたはウィンドウモードで使用するように構成できます。

- 全画面表示モード: ユーザーは通常のWindowsログオン画面でログオンします。その後、同じユーザー資格情報を使用して、このリリースに自動的にログオンします。
- ユーザーはデスクトップをウィンドウで表示します: ユーザーはまずユーザーデバイスにログオンし、次にこのリリースに付属のWebサイトを通じてこのリリースにログオンします。

管理対象外のユーザーデバイス

信頼できる組織によって管理および運用されていないユーザーデバイスは、管理制御下にあるとはみなされません。たとえば、ユーザーが自分のデバイスを入手して構成することを許可する場合がありますが、ユーザーは上記の一般的なセキュリティのベストプラクティスに従わない可能性があります。このリリースには、非管理対象ユーザーデバイスにデスクトップを安全に配信できるという利点があります。これらのデバイスには、キーロガーや同様の入力攻撃を防ぐための基本的なウイルス対策保護が依然として必要です。

データストレージに関する考慮事項

このリリースを使用する場合、ユーザーが物理的に制御しているユーザーデバイスにデータを保存することを防ぐことができます。ただし、ユーザーがデスクトップにデータを保存することの影響については、依然として考慮する必要があります。ユーザーがデスクトップにデータを保存することは良い習慣ではありません。データは、ファイルサーバー、データベースサーバー、または適切に保護できるその他のリポジトリに保持する必要があります。

デスクトップ環境は、プールされたデスクトップや専用デスクトップなど、さまざまな種類のデスクトップで構成される場合があります。ユーザーは、プールされたデスクトップなど、ユーザー間で共有されるデスクトップにデータを保存してはなりません。ユーザーが専用デスクトップにデータを保存する場合、そのデスクトップが後で他のユーザーに利用可能になった場合は、そのデータを削除する必要があります。

混在バージョン環境

混在バージョン環境は、一部のアップグレード中に避けられません。ベストプラクティスに従い、異なるバージョンのCitrixコンポーネントが共存する時間を最小限に抑えてください。混在バージョン環境では、たとえばセキュリティポリシーが均一に適用されない場合があります。

注記:

これは他のソフトウェア製品にも共通しており、以前のバージョンのActive Directoryを使用すると、後のバージョンのWindowsではグループポリシーが部分的にしか適用されません。

以下のシナリオでは、特定の混在バージョンのCitrix環境で発生する可能性のあるセキュリティ問題について説明します。Citrix Receiver 1.7を使用して、XenAppおよびXenDesktop 7.6 Feature Pack 2のVDAを実行している仮想デスクトップに接続する場合、ポリシー設定「**デスクトップとクライアント間のファイル転送を許可**」がサイトで有効になっていますが、XenAppおよびXenDesktop 7.1を実行しているDelivery Controllerでは無効にできません。これは、製品の後期バージョンでリリースされたポリシー設定を認識しないためです。

このポリシー設定により、ユーザーはファイルを仮想デスクトップにアップロードおよびダウンロードできるようになり、これがセキュリティ問題となります。この問題を回避するには、Delivery Controller（またはStudioのスタンドアロンインスタンス）をバージョン7.6 Feature Pack 2にアップグレードし、グループポリシーを使用してポリシー設定を無効にします。または、影響を受けるすべての仮想デスクトップでローカルポリシーを使用します。

Remote PCアクセスに関するセキュリティ上の考慮事項

Remote PCアクセスは、以下のセキュリティ機能を実装しています。

- スマートカードの使用がサポートされています。
- リモートセッションが接続されると、オフィスのPCのモニターは空白になります。
- Remote PCアクセスは、CTRL+ALT+DEL、USB対応スマートカード、および生体認証デバイスを除くすべてのキーボードとマウス入力をリモートセッションにリダイレクトします。
- SmoothRoamingは、単一ユーザーのみがサポートされます。
- ユーザーがオフィスPCにリモートセッションを接続している場合、そのユーザーのみがオフィスPCへのローカルアクセスを再開できます。ローカルアクセスを再開するには、ユーザーはローカルPCでCtrl-Alt-Delを押し、リモートセッションで使用したのと同じ資格情報でログオンします。システムに適切なサードパーティの資格情報プロバイダー統合がある場合は、スマートカードを挿入するか、生体認証を利用してローカルアクセスを再開することもできます。このデフォルトの動作は、グループポリシーオブジェクト（GPO）を介して高速ユーザー切り替えを有効にするか、レジストリを編集することでオーバーライドできます。

注記:

Citrixは、VDA管理者権限を一般セッションユーザーに割り当てないことを推奨します。

自動割り当て

デフォルトでは、Remote PCアクセスは複数のユーザーをVDAに自動割り当てすることをサポートしています。XenDesktop 5.6 Feature Pack 1では、管理者はRemotePCAccess.ps1 PowerShellスクリプトを使用してこの動作をオーバーライドできました。このリリースでは、複数の自動Remote PC割り当てを許可または禁止するためにレジストリエントリを使用します。この設定はサイト全体に適用されます。

注意:

> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤用によって生じた問題が解決されることを保証できません。レジストリエディターは、ご自身の責任において使用してください。編集する前に、必ずレジストリをバックアップしてください。

> 自動割り当てを単一ユーザーに制限するには：

サイト内の各Controllerで、次のレジストリエントリを設定します。

```
HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple
user assignment.
```

既存のユーザー割り当てがある場合は、SDKコマンドを使用してそれらを削除し、VDAがその後単一の自動割り当ての対象となるようにします。

- VDAから割り当てられているすべてのユーザーを削除します: `$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- デリバリーグループからVDAを削除します: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

物理的なオフィスPCを再起動します。

XML信頼

XML信頼設定は、以下の展開に適用されます。

- オンプレミスのStoreFront。
- パスワードを必要としないサブスクライバー（ユーザー）認証テクノロジ。このようなテクノロジの例としては、ドメインパススルー、スマートカード、SAML、Veridiumソリューションなどがあります。

XML信頼設定を有効にすると、ユーザーは正常に認証され、アプリケーションを起動できるようになります。Delivery ControllerはStoreFrontから送信された資格情報を信頼します。この設定は、Delivery ControllerとStoreFront間の通信が保護されている場合（ファイアウォール、IPsec、またはその他のセキュリティ推奨事項を使用している場合）にのみ有効にしてください。

この設定はデフォルトで無効になっています。

XML信頼設定の確認、有効化、または無効化には、Citrix Virtual Apps and Desktops PowerShell SDKを使用します。

- XML信頼設定の現在の値を確認するには、`Get-BrokerSite`を実行し、`TrustRequestsSentToTheXMLServicePort`の値を調べます。
- XML信頼を有効にするには、`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true`を実行します。
- XML信頼を無効にするには、`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $false`を実行します。

スマートカード

スマートカードおよび同等のテクノロジーは、この記事で説明されているガイドライン内でサポートされています。Citrix Virtual AppsまたはCitrix Virtual Desktops™でスマートカードを使用するには：

- スマートカードの使用に関する組織のセキュリティポリシーを理解してください。これらのポリシーには、たとえば、スマートカードの発行方法やユーザーがスマートカードを保護する方法が記載されている場合があります。これらのポリシーの一部は、Citrix Virtual Apps™またはCitrix Virtual Desktops環境で再評価する必要がある場合があります。
- スマートカードで使用するユーザーデバイスの種類、オペレーティングシステム、および公開アプリケーションを決定します。
- スマートカードテクノロジーと、選択したスマートカードベンダーのハードウェアおよびソフトウェアに精通してください。
- 分散環境でデジタル証明書を展開する方法を理解してください。

> **注:**
>
> 高速スマートカードでは、スマートカードの登録はサポートされていません。高速スマートカードが無効になっている場合、スマートカードの登録は機能する可能性がありますが、ス

> マートカードとミドルウェアの種類によって異なります。Citrix Virtual Apps and Desktopsとの統合、および仮想セッションを介したスマートカード登録のサポートについては、スマートカードおよびミドルウェアベンダーにお問い合わせください。

スマートカードの種類

企業向けスマートカードと消費者向けスマートカードは、同じ寸法、電気コネクタを持ち、同じスマートカードリーダーに適合します。

企業向けスマートカードにはデジタル証明書が含まれています。これらのスマートカードはWindowsログオンをサポートし、ドキュメントやメールのデジタル署名および暗号化のためのアプリケーションでも使用できます。Citrix Virtual Apps and Desktops™はこれらの用途をサポートしています。

コンシューマー用途のスマートカードにはデジタル証明書は含まれていません。共有シークレットが含まれています。これらのスマートカードは、支払い（チップと署名またはチップとPINのクレジットカードなど）をサポートできます。Windowsログオンや一般的なWindowsアプリケーションはサポートしていません。これらのスマートカードを使用するには、特殊なWindowsアプリケーションと適切なソフトウェアインフラストラクチャ（たとえば、決済カードネットワークへの接続を含む）が必要です。Citrix Virtual AppsまたはCitrix Virtual Desktopsでこれらの特殊なアプリケーションをサポートする方法については、Citrix担当者にお問い合わせください。

企業向けスマートカードには、同様の方法で使用できる互換性のある同等品があります。

- スマートカードと同等のUSBトークンは、USBポートに直接接続します。これらのUSBトークンは通常、USBフラッシュドライブと同じくらいのサイズですが、携帯電話で使用されるSIMカードと同じくらい小さい場合もあります。これらは、スマートカードとUSBスマートカードリーダーの組み合わせとして表示されます。
- Windows Trusted Platform Module (TPM) を使用する仮想スマートカードは、スマートカードとして表示されます。これらの仮想スマートカードは、Citrix Workspaceアプリ（最小バージョンCitrix Receiver 4.3）を使用して、Windows 8およびWindows 10でサポートされています。
    - XenAppおよびXenDesktop 7.6 FP3より前のCitrix Virtual Apps and Desktopsのバージョン（旧称 XenAppおよびXenDesktop）は、仮想スマートカードをサポートしていません。
    - 仮想スマートカードの詳細については、仮想スマートカードの概要を参照してください。

> **注:** 「仮想スマートカード」という用語は、ユーザーコンピューターに保存されているデジタル証明書を指す場合もあります。これらのデジタル証明書は、スマートカードと厳密には同等ではありません。

Citrix Virtual Apps and Desktopsのスマートカードサポートは、Microsoft Personal Computer/Smart Card (PC/SC) 標準仕様に基づいています。最低要件として、スマートカードおよびスマートカードデバイスは、基盤となるWindowsオペレーティングシステムによってサポートされ、Microsoft Windows Hardware Quality Labs (WHQL) によって認定されている必要があります。これにより、対象となるWindowsオペレーティングシステムを実行しているコンピューターで使用できます。ハードウェアのPC/SC準拠に関する追加情報については、Microsoftのドキュメントを参照してください。その他の種類のユーザーデバイスもPS/SC標準に準拠している場合があります。詳細については、Citrix Readyプログラムを参照してください。

通常、各ベンダーのスマートカードまたは同等のものには、個別のデバイスドライバーが必要です。ただし、スマートカードがNIST Personal Identity Verification (PIV) 標準などの標準に準拠している場合、さまざまなスマートカードに対して単一のデバイスドライバーを使用できる可能性があります。デバイスドライバーは、ユーザーデバイスとVirtual Delivery Agent (VDA) の両方にインストールする必要があります。デバイスドライバーは、Citrixパートナーから入手できるスマートカードミドルウェアパッケージの一部として提供されることがよくあります。スマートカードミドルウェアパッケージは、高度な機能を提供します。デバイスドライバーは、Cryptographic Service Provider (CSP)、Key Storage Provider (KSP)、またはミニドライバーとも呼ばれることがあります。

Windowsシステム用の以下のスマートカードとミドルウェアの組み合わせは、Citrixによってその種類の代表的な例としてテストされています。ただし、他のスマートカードとミドルウェアも使用できます。Citrix互換のスマートカードとミドルウェアの詳細については、`<http://www.citrix.com/ready>`を参照してください。

ミドルウェア	対応カード
Gemalto .NETカード用ミニドライバー	ジェムアルト ドットネット v2以降

他の種類のデバイスでのスマートカードの使用に関する情報については、そのデバイスのCitrix Workspace™アプリのドキュメントを参照してください。

リモートPCアクセス

スマートカードは、Windows 10、Windows 8、またはWindows 7を実行している物理的なオフィスPCへのリモートアクセスでのみサポートされています。

以下のスマートカードは、Remote PC Accessでテストされました。

ミドルウェア	対応カード
Gemalto .NET ミニドライバー	ジェマルト .NET v2+

高速スマートカード

高速スマートカードは、既存のHDX PC/SCベースのスマートカードリダイレクトを改善したものです。高遅延のWAN環境でスマートカードを使用する場合にパフォーマンスが向上します。遅延が大きい場合、パフォーマンスの向上は大幅なものになります（例えば、Windowsの高速スマートカードログオンでは15秒、PC/SCベースのスマートカードリダイレクトでは1分以上）。

高速スマートカードは、現在サポートされているWindows VDAを搭載したホストマシンでデフォルトで有効になっています。ホスト側で高速スマートカードを無効にするには（例えば診断目的で）、'Disable Cryptographic Redirection' レジストリ設定をゼロ以外の値に設定します。

```
HKLM\SOFTWARE\Citrix\SmartCard

CryptographicRedirectionDisable (DWORD)
```

クライアント側で高速スマートカードを有効にするには、関連するStoreFrontサイトの*default.ica*ファイルにSmartCardCryptographicRedirection ICAパラメーターを含めます。

```
[WFClient]

SmartCardCryptographicRedirection=On
```

さらに、クライアント側では、次のレジストリ設定を使用して、高速スマートカードを強制的に有効または無効にできます (例: 診断目的で)。

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (ゼロ以外のDWORDとして)

または

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (ゼロ以外のDWORDとして)

クライアントマシンが64ビットの場合、32ビットレジストリハイブを指定する必要があります（`WOW6432Node`を使用）。

制限事項:

- Windows版Citrix Workspaceアプリのみが高速スマートカードをサポートしています。default.icaファイルで高速スマートカードを構成した場合でも、Windows版ではないCitrix Workspaceアプリは、引き続き既存のPC/SCリダイレクトを使用します。
- 高速スマートカードがサポートする唯一のダブルホップシナリオは、両方のホップで高速スマートカードが有効になっているICA® > ICAです。高速スマートカードはICA > RDPダブルホップシナリオをサポートしていないため、これらのシナリオは機能しません。
- 高速スマートカードは次世代暗号化をサポートしていません。そのため、高速スマートカードは楕円曲線暗号 (ECC) スマートカードをサポートしていません。
- 高速スマートカードは、読み取り専用キーコンテナ操作のみをサポートしています。
- 高速スマートカードは、スマートカードPINの変更をサポートしていません。

VDAバージョン2203およびCitrix Workspaceアプリバージョン2202 for Windows（またはそれ以降）以降、高速スマートカードは次世代暗号化 (CNG) と互換性があります。さらに、楕円曲線暗号 (ECC) スマートカードは、P-256、P-384、P-521ビットの曲線で、ECDSAとECDHの両方でサポートされています。

VDAバージョン2203以降、高速スマートカードは、同じユーザーのログオンセッション内のアプリケーション間でスマートカードPINをキャッシュする機能を追加します。たとえば、**セッションPINキャッシュ**が有効になっており、エンドユーザーが以前にOutlookにスマートカードPINを提供している場合、その後Wordを使用してドキュメントに署名すると、Wordはすでにキャッシュされているスマートカード PIN（Outlookに送信されたもの）を使用します。**セッションPINキャッシュ**は、ユーザーがスマートカードPINを入力する回数を減らすことで、ユーザーエクスペリエンスを向上させます。さらに、スマートカードがVDAへのログオンに使用される場合、Windowsスマートカードログオン PINは、オプションで**セッションPINキャッシュ**に保存できます。これにより、ユーザーエクスペリエンスがさらに向上します。

セッションPINキャッシュはデフォルトで無効になっています。VDAで以下のレジストリ設定を使用して有効にし、制御できます。

HKLM\SOFTWARE\Citrix\SmartCardで:

- `EnablePinSessionCache` をDWORDとして (有効にするにはゼロ以外)
- `EnableLogonPinSessionCache` をDWORDとして (有効にするにはゼロ以外)
- `PinSessionCacheEntryStaleTimeout` をDWORDとして (エントリが古くなるまでの秒数、デフォルトは1時間)

スマートカードリーダーの種類

スマートカードリーダーは、ユーザーデバイスに内蔵されている場合もあれば、ユーザーデバイスに別途接続されている場合もあります（通常はUSBまたはBluetooth経由）。USBチップ/スマートカードインターフェースデバイス (CCID) 仕様に準拠する接触型カードリーダーがサポートされています。これらには、ユーザーがスマートカードを挿入するスロットまたはスワイプがあります。ドイツ信用経済 (DK) 規格は、接触型カードリーダーの4つのクラスを定義しています。

- クラス1スマートカードリーダーは最も一般的で、通常はスロットを備えています。クラス1スマートカードリーダーは、通常、オペレーティングシステムに付属の標準CCIDデバイスドライバーでサポートされています。
- クラス2スマートカードリーダーには、ユーザーデバイスからアクセスできないセキュアなキーパッドも含まれています。クラス2スマートカードリーダーは、統合されたセキュアなキーパッドを備えたキーボードに組み込まれている場合があります。クラス2スマートカードリーダーについては、Citrix担当者にお問い合わせください。セキュアなキーパッド機能を有効にするには、リーダー固有のデバイスドライバーが必要になる場合があります。
- クラス3スマートカードリーダーには、セキュアなディスプレイも含まれています。クラス3スマートカードリーダーはサポートされていません。
- クラス4のスマートカードリーダーには、セキュアトランザクションモジュールも含まれています。クラス4のスマートカードリーダーはサポートされていません。

> **注:**
>
> スマートカードリーダーのクラスは、USBデバイスクラスとは関係ありません。

> スマートカードリーダーは、ユーザーデバイスに適切なデバイスドライバーをインストールする必要があります。

サポートされているスマートカードリーダーについては、使用しているCitrix Workspaceアプリのドキュメントを参照してください。Citrix Workspaceアプリのドキュメントでは、サポートされているバージョンはスマートカードに関する記事またはシステム要件の記事に記載されています。

ユーザーエクスペリエンス

スマートカードのサポートは、Citrix Virtual Apps and Desktopsに統合されており、特定のICA/HDXスマートカード仮想チャネルを使用します。これはデフォルトで有効になっています。

重要: スマートカードリーダーに汎用USBリダイレクトを使用しないでください。これはスマートカードリーダーではデフォルトで無効になっており、有効にしてもサポートされません。

同じユーザーデバイスで複数のスマートカードと複数のリーダーを使用できますが、パススルー認証を使用している場合は、ユーザーが仮想デスクトップまたはアプリケーションを起動するときに、スマートカードを1枚だけ挿入する必要があります。アプリケーション内でスマートカードを使用する場合（デジタル署名や暗号化機能など）、スマートカードの挿入やPINの入力が再度求められることがあります。これは、複数のスマートカードが同時に挿入されている場合に発生する可能性があります。

- スマートカードがすでにリーダーに挿入されているにもかかわらず、スマートカードの挿入を求められた場合は、［キャンセル］を選択する必要があります。
- PINの入力を求められた場合は、PINを再度入力する必要があります。

カード管理システムまたはベンダーユーティリティを使用してPINをリセットできます。

> **重要:**

> Citrix Virtual AppsまたはCitrix Virtual Desktopsセッション内で、Microsoft Remote Desktop Connectionアプリケーションとスマートカードを使用することはサポートされていません。これは「ダブルホップ」の使用と呼ばれることがあります。

スマートカードを展開する前に

- スマートカードリーダー用のデバイスドライバーを入手し、ユーザーデバイスにインストールします。多くのスマートカードリーダーは、Microsoftが提供するCCIDデバイスドライバーを使用できます。
- スマートカードベンダーからデバイスドライバーと暗号化サービスプロバイダー (CSP) ソフトウェアを入手し、ユーザーデバイスと仮想デスクトップの両方にインストールします。ドライバーとCSPソフトウェアは、Citrix Virtual Apps and Desktopsと互換性がある必要があります。互換性については、ベンダーのドキュメントを確認してください。ミニドライバーモデルをサポートおよび使用するスマートカードを使用する仮想デスクトップの場合、スマートカードミニドライバーは自動的にダウンロードされますが、http://catalog.update.microsoft.com またはベンダーから入手することもできます。また、PKCS#11ミドルウェアが必要な場合は、カードベンダーから入手してください。
- 重要: Citrixソフトウェアをインストールする前に、物理コンピューターにドライバーとCSPソフトウェアをインストールしてテストすることをお勧めします。

- Windows 10でInternet Explorerを使用してスマートカードを使用するユーザー向けに、Citrix Receiver™ for WebのURLを信頼済みサイトリストに追加します。Windows 10では、Internet Explorerは信頼済みサイトに対してデフォルトで保護モードで実行されません。
- 公開鍵インフラストラクチャ (PKI) が適切に構成されていることを確認してください。これには、Active Directory環境で証明書からアカウントへのマッピングが正しく構成されていること、およびユーザー証明書の検証が正常に実行できることを確認することが含まれます。
- 展開が、スマートカードで使用される他のCitrixコンポーネント（Citrix Workspaceアプリと StoreFrontを含む）のシステム要件を満たしていることを確認してください。
- サイト内の以下のサーバーへのアクセスを確保してください:
  - スマートカード上のログオン証明書に関連付けられているユーザーアカウント用のActive Directoryドメインコントローラー
  - デリバリーコントローラー™
  - シトリックス ストアフロント
  - シトリックス ゲートウェイ/シトリックス アクセス ゲートウェイ 10.x
  - VDA
  - (Remote PC Accessの場合、オプション): Microsoft Exchange Server

スマートカードの使用を有効にする

ステップ1. カード発行ポリシーに従って、ユーザーにスマートカードを発行します。

ステップ2. (オプション) ユーザーがRemote PC Accessを利用できるようにスマートカードを設定します。

ステップ3. スマートカードのリモート処理のために、Delivery ControllerとStoreFrontをインストールして構成します（まだインストールされていない場合）。

ステップ4. スマートカードの使用のためにStoreFrontを有効にします。詳細については、StoreFrontドキュメントの「スマートカード認証の構成」を参照してください。

ステップ5. スマートカードの使用のためにCitrix Gateway/Access Gatewayを有効にします。詳細については、NetScalerドキュメントの「認証と承認の構成」および「Web Interfaceを使用したスマートカードアクセスの構成」を参照してください。

ステップ6. スマートカードの使用のためにVDAを有効にします。

- VDA に必要なアプリケーションと更新プログラムがあることを確認します。
- ミドルウェアをインストールします。

- スマートカードのリモート処理を設定し、ユーザーデバイス上のCitrix Workspaceアプリと仮想デスクトップセッション間のスマートカードデータの通信を有効にします。

ステップ7. ユーザーデバイス（ドメイン参加済みまたは非ドメイン参加済みのマシンを含む）でスマートカードを使用できるようにします。詳細については、StoreFrontドキュメントの「スマートカード認証の構成」を参照してください。

- 証明機関のルート証明書と発行証明機関の証明書をデバイスのキーストアにインポートします。
- ベンダーのスマートカードミドルウェアをインストールします。
- Windows版Citrix Workspaceアプリをインストールして構成します。その際、グループポリシー管理コンソールを使用してicaclient.admをインポートし、スマートカード認証を有効にしてください。

ステップ8. 展開をテストします。テストユーザーのスマートカードを使用して仮想デスクトップを起動し、展開が正しく構成されていることを確認します。可能なすべてのアクセスメカニズム（例：Internet ExplorerおよびCitrix Workspaceアプリを介したデスクトップへのアクセス）をテストします。

スマートカードリーダーの挿入回数を追跡する

スマートカードのリモート処理を使用すると、SCardGetStatusChange関数を使用して、スマートカードがリーダーに挿入または取り外された回数を追跡できます。この関数は、監視するリーダーごとに1つずつ、SCARD_READERSTATEデータ構造の配列を更新します。各SCARD_READERSTATEのdwEventStateフィールドの上位ワード（16ビット）には、リーダーのカウントが含まれます。詳細については、Microsoftの記事「SCardGetStatusChangeA function」および「SCARD_READERSTATEA structure」を参照してください。

リーダー挿入回数レポート設定は、デフォルトで無効になっています。追跡を有効にするには、次のレジストリキーを追加します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

名前: EnableReaderInsertCountReporting

種類: DWORD

値: ゼロ以外の任意の値

セッションが切断されると、カウントはゼロにリセットされます。

リーダー挿入回数レポートは、サードパーティのスマートカードミドルウェアと互換性があります。

スマートカードの展開

この製品バージョンおよびこのバージョンを含む混在環境では、以下の種類のスマートカード展開がサポートされています。その他の構成も動作する可能性がありますが、サポートされていません。

種類	STOREFRONT™ 接続
ローカルのドメイン参加済みコンピューター	直接接続
ドメイン参加済みコンピューターからのリモートアクセス	Citrix Gateway 経由で接続
ドメインに参加していないコンピューター	直接接続
ドメインに参加していないコンピューターからのリモートアクセス	Citrix Gateway 経由で接続
ドメインに参加していないコンピューターおよびシンクライアントがデスクトップアプライアンスサイトにアクセスする場合	デスクトップアプライアンスサイト経由で接続
ドメイン参加済みコンピューターおよびシンクライアントが XenApp® Services URL を介して StoreFront にアクセスする場合	XenApp Services URL経由で接続

展開の種類は、スマートカードリーダーが接続されているユーザーデバイスの特性によって定義されます。

- デバイスがドメイン参加済みか、非ドメイン参加済みか。
- デバイスがStoreFrontにどのように接続されているか。
- 仮想デスクトップとアプリケーションを表示するためにどのソフトウェアが使用されているか。

さらに、Microsoft WordやMicrosoft Excelなどのスマートカード対応アプリケーションをこれらの展開で使用できます。これらのアプリケーションを使用すると、ユーザーはドキュメントにデジタル署名したり、暗号化したりできます。

バイモーダル認証

これらの各展開において可能な場合、Receiverはスマートカードの使用とユーザー名およびパスワードの入力のいずれかを選択できるようにすることで、バイモーダル認証をサポートします。これは、スマートカードが使用できない場合（たとえば、ユーザーが自宅に忘れた場合やログオン証明書の有効期限が切れた場合）に役立ちます。

非ドメイン参加デバイスのユーザーはReceiver for Windowsに直接ログオンするため、ユーザーが明示的な認証にフォールバックできるようにすることができます。バイモーダル認証を構成すると、ユーザーは最初にスマートカードとPINを使用してログオンするように求められますが、スマートカードに問題が発生した場合は明示的な認証を選択するオプションがあります。

Citrix Gatewayを展開する場合、ユーザーはデバイスにログオンし、Receiver for WindowsによってCitrix Gatewayへの認証を求められます。これは、ドメイン参加済みデバイスと非ドメイン参加済みデバイスの両方に適用されます。ユーザーは、スマートカードとPIN、または明示的な資格情報を使用してCitrix Gatewayにログオンできます。これにより、Citrix Gatewayログオンに対してバイモーダル認証をユーザーに提供できます。Citrix GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報検証をCitrix Gatewayに委任することで、ユーザーはStoreFrontにサイレント認証されます。

複数のActive Directoryフォレストに関する考慮事項

Citrix環境では、スマートカードは単一のフォレスト内でサポートされます。フォレストをまたがるスマートカードログオンには、すべてのユーザーアカウントへの直接的な双方向フォレスト信頼が必要です。スマートカードを含むより複雑なマルチフォレスト展開（つまり、信頼が一方通行であるか、異なるタイプである場合）はサポートされていません。

リモートデスクトップを含むCitrix環境でスマートカードを使用できます。この機能は、ローカル（スマートカードが接続されているユーザーデバイス上）またはリモート（ユーザーデバイスが接続するリモートデスクトップ上）にインストールできます。

スマートカード取り外しポリシー

製品に設定されているスマートカード取り外しポリシーは、セッション中にリーダーからスマートカードを取り外した場合に何が起こるかを決定します。スマートカード取り外しポリシーは、Windowsオペレーティングシステムによって構成および処理されます。

ポリシー設定	デスクトップの動作
アクションなし	アクションなし。

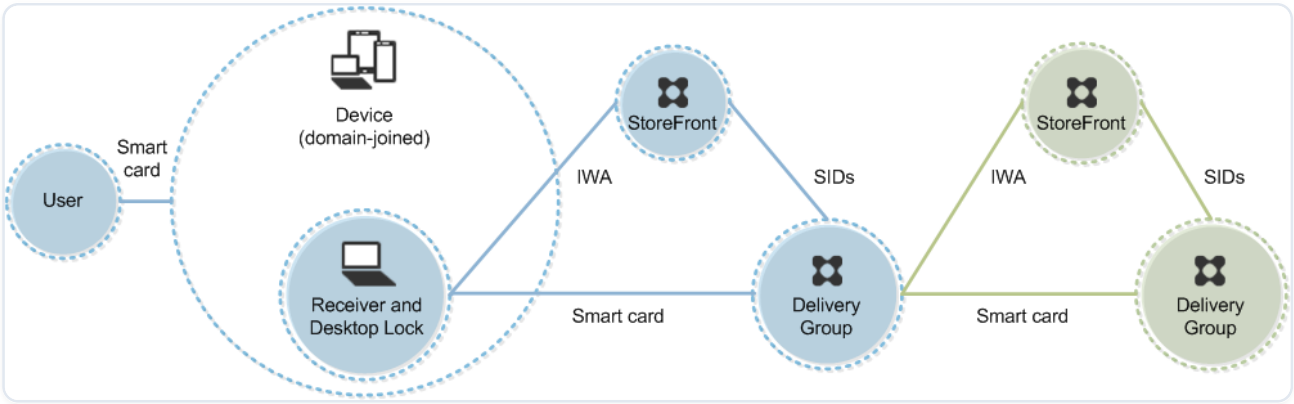
ポリシー設定	デスクトップの動作
ワークステーションをロック	デスクトップセッションが切断され、仮想デスクトップがロックされます。
強制ログオフ	ユーザーは強制的にログオフされます。ネットワーク接続が失われ、この設定が有効になっている場合、セッションがログオフされ、ユーザーはデータを失う可能性があります。
リモートターミナルサービスセッションの場合に切断	セッションが切断され、仮想デスクトップがロックされます。

証明書失効チェック

証明書失効チェックが有効になっており、ユーザーが無効な証明書を含むスマートカードをカードリーダーに挿入した場合、ユーザーは認証できず、その証明書に関連するデスクトップまたはアプリケーションにアクセスできません。たとえば、無効な証明書がメールの復号化に使用されている場合、メールは暗号化されたままになります。認証に使用されるものなど、カード上の他の証明書がまだ有効である場合、それらの機能はアクティブなままになります。

展開例：ドメイン参加済みコンピューター

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン参加済みユーザーデバイスを使用します。



ユーザーはスマートカードとPINを使用してデバイスにログオンします。Receiverは、統合Windows認証 (IWA) を使用して、ユーザーをStoreFrontサーバーに認証します。StoreFrontは、ユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、シングルサインオン機能がReceiverで構成されているため、PINの入力を再度求められることはありません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに認証します。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン参加済みコンピューターからのリモートアクセス

この展開には、Desktop Viewerを実行し、Citrix Gateway/Access Gatewayを介してStoreFrontに接続するドメイン参加済みのユーザーデバイスが含まれます。

展開例: ドメイン参加済みコンピューターからのリモートアクセス(/en-us/citrix-virtual-apps-desktops/2311/media/smartcard2_1.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンし、その後Citrix Gateway/Access Gatewayに再度ログオンします。この2回目のログオンは、Receiverがこの展開でバイモーダル認証を許可しているため、スマートカードとPIN、またはユーザー名とパスワードのいずれかで行うことができます。

ユーザーはStoreFrontに自動的にログオンし、StoreFrontはユーザーセキュリティ識別子 (SID) をCitrix Virtual Apps™またはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、シングルサインオン機能がReceiverで構成されているため、PINの入力を再度求められることはありません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに認証します。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン非参加コンピューター

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン非参加ユーザーデバイスが関与します。

展開例: ドメイン非参加コンピューター(/en-us/citrix-virtual-apps-desktops/2311/media/smartcard3_1.png)

ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能であるため、Receiverはユーザーにスマートカードと PIN、また

はユーザー名とパスワードのいずれかを要求します。その後、ReceiverはStoreFrontに認証します。

StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、PINの再入力を求められます。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに認証します。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン非参加コンピューターからのリモートアクセス

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメインに参加していないユーザーデバイスが使用されます。

ドメインに参加していないコンピューターからのリモートアクセス展開例(/en-us/citrix-virtual-apps-desktops/2311/media/smartcard4_1.png)

ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能であるため、Receiver はユーザーにスマートカードと PIN、またはユーザー名とパスワードのいずれかを要求します。その後、Receiver は StoreFront に対して認証を行います。

StoreFront はユーザーセキュリティ識別子 (SID) を Citrix Virtual Apps または Citrix Virtual Desktops に渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、ユーザーは再度 PIN の入力を求められます。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメインに参加していないコンピューターとシンクライアントがDesktop Applianceサイトにアクセスする

この展開では、Desktop Lock を実行し、Desktop Appliance サイトを通じて StoreFront に接続するドメインに参加していないユーザーデバイスが使用される場合があります。

Desktop Lock は、Citrix Virtual Apps、Citrix Virtual Desktops、および VDI-in-a-Box とともにリリースされる別のコンポーネントです。これは Desktop Viewer の代替であり、主に再利用された Windows コンピューターと Windows シンクライアント向けに設計されています。Desktop Lock は、これらのユーザーデバイスの Windows シェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスするのを防ぎます。Desktop Lock を使用すると、ユーザーは Windows Server Machine デスクトップと Windows Desktop Machine デスクトップにアクセスできます。Desktop Lock のインストールはオプションです。

展開例：ドメインに参加していないコンピューターとシンクライアントがDesktop Applianceサイトにアクセスする(/en-us/citrix-virtual-apps-desktops/2311/media/smartcard5_1.png)

ユーザーはスマートカードを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、デバイスはキオスクモードで実行されているInternet Explorerを介してDesktop Applianceサイトを起動するように構成されます。サイト上のActiveXコントロールがユーザーにPINを要求し、それをStoreFrontに送信します。StoreFrontはユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。割り当てられたデスクトップグループのアルファベット順リストで最初に利用可能なデスクトップが起動します。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメインに参加しているコンピューターとシンクライアントがXenApp Services URLを通じてStoreFrontにアクセスする

この展開では、Desktop Lock を実行し、XenApp Services URL を通じて StoreFront に接続するドメインに参加しているユーザーデバイスが使用されます。

Desktop Lock は、Citrix Virtual Apps、Citrix Virtual Desktops、および VDI-in-a-Box とともにリリースされる別のコンポーネントです。これは Desktop Viewer の代替であり、主に再利用された Windows コンピューターと Windows シンクライアント向けに設計されています。Desktop Lock は、これらのユーザーデバイスの Windows シェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスするのを防ぎます。Desktop Lock を使用すると、ユーザーは

Windows Server Machine デスクトップと Windows Desktop Machine デスクトップにアクセスできます。Desktop Lock のインストールはオプションです。

展開例：ドメインに参加しているコンピューターとシンクライアントがXenApp Services URLを通じてStoreFrontにアクセスする(/en-us/citrix-virtual-apps-desktops/2311/media/smartcard6.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、統合Windows認証（IWA）を使用してユーザーをStorefrontサーバーに認証します。StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップを起動すると、Receiverでシングルサインオン機能が構成されているため、ユーザーは再度PINを要求されません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

スマートカードによるパススルー認証とシングルサインオン

パススルー認証

スマートカードによる仮想デスクトップへのパススルー認証は、Windows 10、Windows 8、Windows 7 SP1 EnterpriseおよびProfessional Editionを実行しているユーザーデバイスでサポートされています。

スマートカードによるホストされたアプリケーションへのパススルー認証は、Windows Server 2016、Windows Server 2012 R2、Windows Server 2012、および Windows Server 2008 R2 SP1 を実行しているサーバーでサポートされています。

スマートカードホスト型アプリケーションでパススルー認証を使用するには、サイトの認証方法としてスマートカードによるパススルーを構成する際に、Kerberosの使用を有効にしてください。

注：スマートカードによるパススルー認証の可用性は、以下を含むがこれに限定されない多くの要因に依存します。

- パススルー認証に関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

スマートカードによるパススルー認証はCitrix StoreFrontで構成されます。詳細については、StoreFrontのドキュメントを参照してください。

シングルサインオン

シングルサインオンは、仮想デスクトップおよびアプリケーションの起動時にパススルー認証を実装するCitrixの機能です。この機能は、ドメイン参加型、StoreFrontへの直接接続、およびドメイン参加型、NetScalerからStoreFrontへのスマートカード展開で使用して、ユーザーがPINを入力する回数を減らすことができます。これらの展開タイプでシングルサインオンを使用するには、StoreFrontサーバーにあるdefault.icaファイルで次のパラメーターを編集します。

- ドメイン参加型、StoreFrontへの直接接続スマートカード展開 — DisableCtrlAltDelをOffに設定
- ドメイン参加型、NetScalerからStoreFrontへのスマートカード展開 — UseLocalUserAndPasswordをOnに設定

これらのパラメーターの設定に関する詳細な手順については、StoreFrontまたはCitrix Gatewayのドキュメントを参照してください。

シングルサインオン機能の可用性は、以下を含む（ただしこれらに限定されない）多くの要因に依存します。

- シングルサインオンに関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

注:

スマートカードリーダーが接続されたマシンでユーザーがVirtual Delivery Agent (VDA)にログオンすると、スマートカードやパスワードなど、以前に成功した認証モードを表すWindowsタイルが表示されることがあります。その結果、シングルサインオンが有効になっている場合、シングルサインオンタイルが表示されることがあります。ログオンするには、シングルサインオンタイルは機能しないため、ユーザーは**ユーザーの切り替え**を選択して別のタイルを選択する必要があります。

トランスポート層セキュリティ (TLS)

Citrix Virtual Apps and Desktopsは、コンポーネント間のTCPベースの接続にTransport Layer Security (TLS) プロトコルをサポートしています。Citrix Virtual Apps and Desktopsは、アダプティブトランスポートを使用して、UDPベースのICA/HDX接続にDatagram Transport Layer Security (DTLS) プロトコルもサポートしています。

TLSとDTLSは似ており、同じデジタル証明書をサポートしています。Citrix Virtual AppsまたはCitrix Virtual Desktops™サイトをTLSを使用するように構成すると、DTLSを使用するようにも構成されます。次の手順を使用してください。記載されている箇所を除き、手順はTLSとDTLSの両方に共通です。

- すべてのDelivery Controllerでサーバー証明書を取得、インストール、登録し、TLS証明書でポートを構成します。詳しくは、ControllerにTLSサーバー証明書をインストールするを参照してください。

  必要に応じて、ControllerがHTTPおよびHTTPSトラフィックをリッスンするために使用するポートを変更できます。
- Citrix Workspace™アプリとVirtual Delivery Agent (VDA) 間でTLS接続を有効にするには、次のタスクを完了します。
  - VDAがインストールされているマシンでTLSを構成します。（便宜上、VDAがインストールされているマシンへの以降の参照は、単に「VDA」と呼びます。）一般情報については、VDAのTLS設定を参照してください。TLS/DTLSの構成には、Citrixが提供するPowerShellスクリプトを使用することを強くお勧めします。詳しくは、PowerShellスクリプトを使用してVDAでTLSを構成するを参照してください。ただし、TLS/DTLSを手動で構成する場合は、VDAでTLSを手動で構成するを参照してください。
  - VDAを含むデリバリーグループでTLSを構成するには、Studioで一連のPowerShellコマンドレットを実行します。詳しくは、デリバリーグループでTLSを構成するを参照してください。

    要件と考慮事項:

    - ユーザーとVDA間のTLS接続を有効にすることは、XenApp 7.6およびXenDesktop 7.6サイト、およびそれ以降のサポート対象リリースでのみ有効です。
    - デリバリーグループとVDAでTLSを構成するのは、コンポーネントのインストール、サイトの作成、マシンカタログの作成、およびデリバリーグループの作成後に行います。
    - デリバリーグループでTLSを構成するには、Controllerのアクセスルールを変更する権限が必要です。フル管理者にはこの権限があります。

- VDAでTLSを構成するには、VDAがインストールされているマシンでWindows管理者である必要があります。
- Machine Creation Services™またはProvisioning Servicesによってプロビジョニングされたプールされ たVDAでは、VDAマシンイメージは再起動時にリセットされ、以前のTLS設定が失われます。VDAが再起動されるたびにPowerShellスクリプトを実行して、TLS設定を再構成してください。

> **警告:**
>
> Windowsレジストリでの作業を含むタスクの場合—レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になる深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターは自己責任で使用してください。編集する前にレジストリを必ずバックアップしてください。

> サイトデータベースへのTLSを有効にする方法については、CTX137556を参照してください。

Controller に TLS サーバー証明書をインストールする

HTTPSの場合、XMLサービスはクライアント証明書ではなくサーバー証明書を使用してTLS機能をサポートします。このセクションでは、Delivery ControllerにTLS証明書を取得してインストールする方法について説明します。同じ手順をCloud Connectorに適用して、STAおよびXMLトラフィックを暗号化できます。

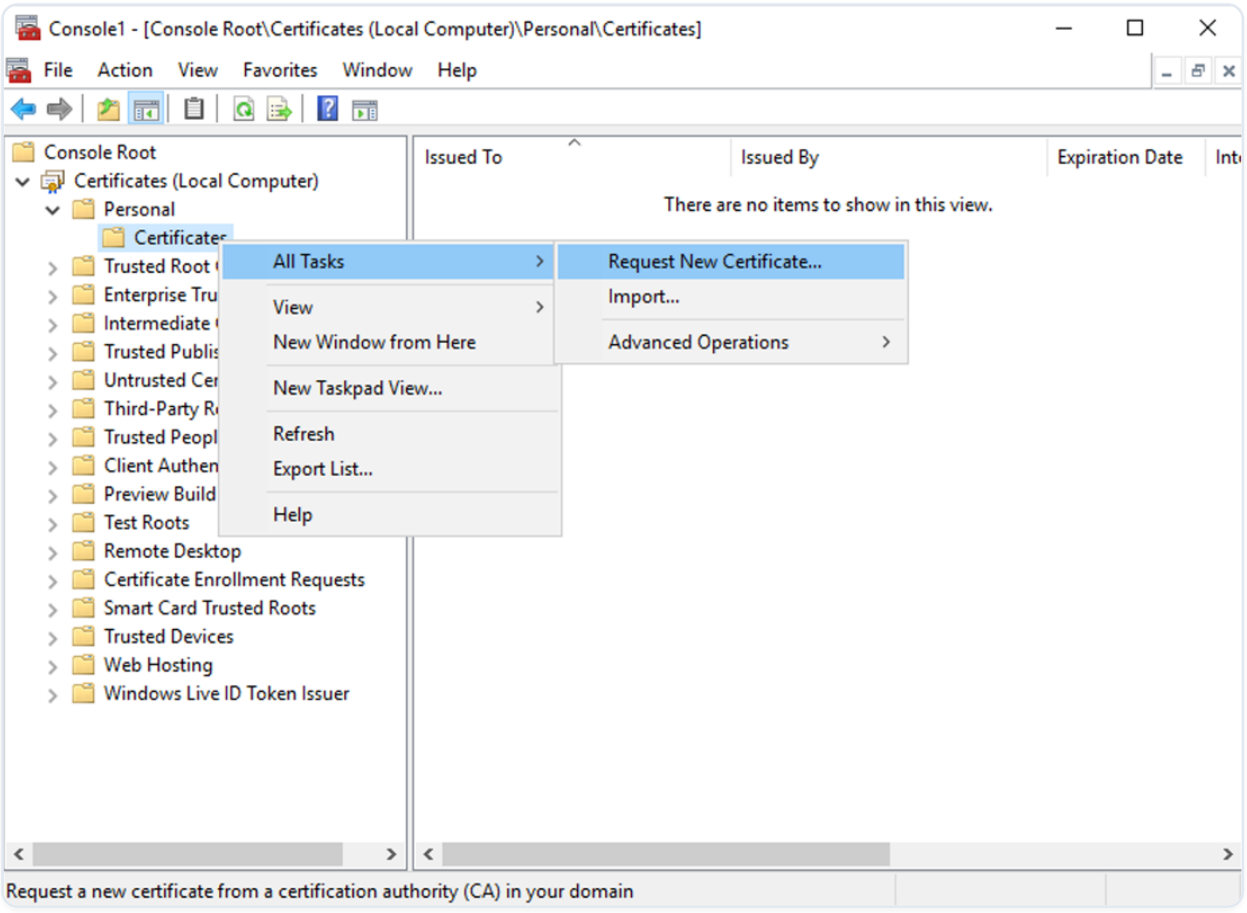
証明機関にはさまざまな種類があり、そこから証明書を要求する方法もさまざまですが、この記事では Microsoft 証明機関について説明します。Microsoft 証明機関には、サーバー認証の目的で公開された証明書テンプレートが必要です。

Microsoft 証明機関が Active Directory ドメインまたは Delivery Controller が参加している信頼されたフォレストに統合されている場合、証明書 MMC スナップインの証明書登録ウィザードから証明書を取得できます。

証明書の要求とインストール

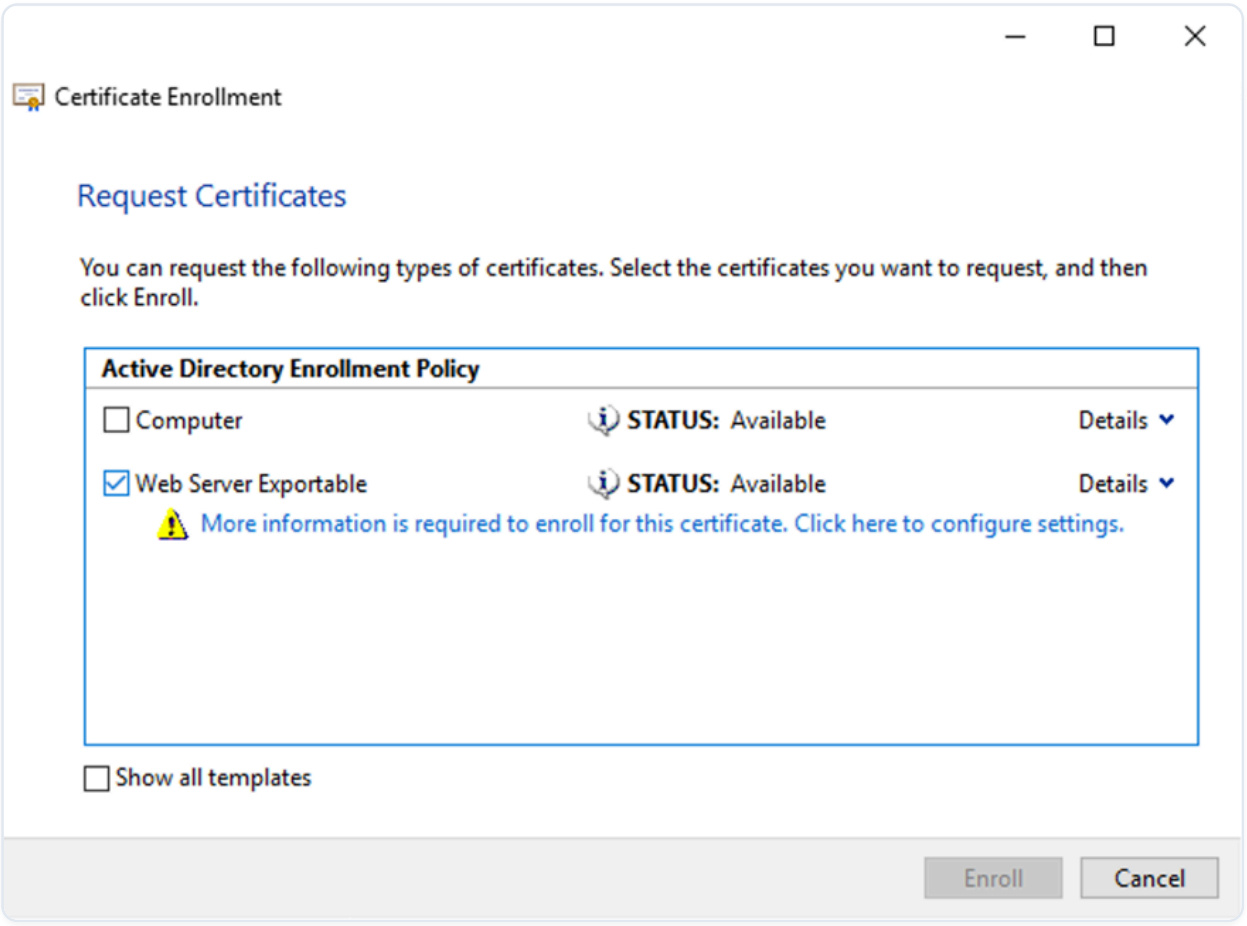
1. Delivery Controller™ で、MMC コンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、 を選択します。

2. **個人 > 証明書**を展開し、**すべてのタスク > 新しい証明書の要求**コンテキストメニューコマンドを使用します。



3. 開始するには**次へ**をクリックし、Active Directory登録から証明書を取得することを確認するには**次へ**をクリックします。

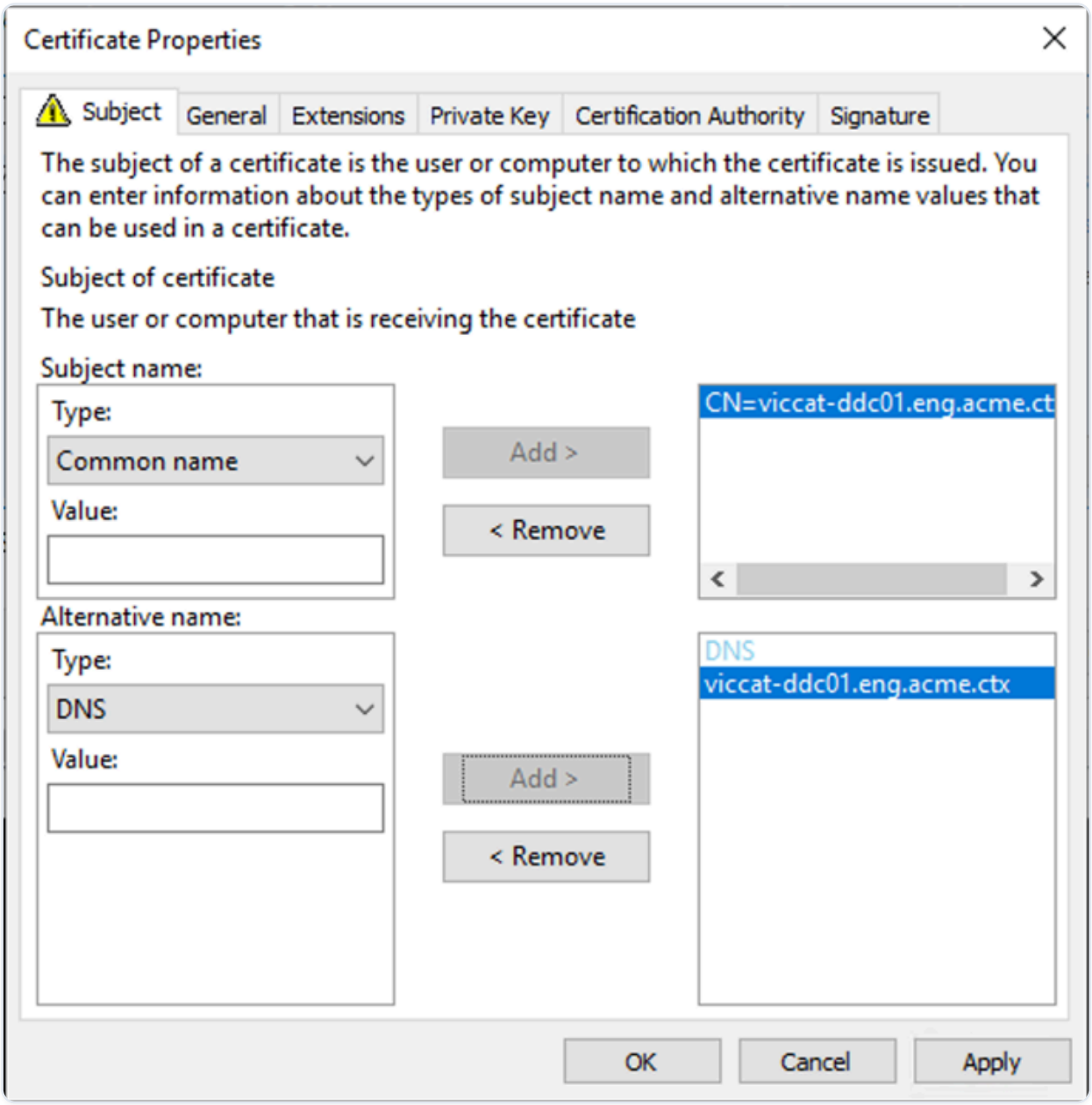
4. サーバー認証証明書のテンプレートを選択します。テンプレートがSubjectの値を自動的に提供するように設定されている場合は、詳細を指定せずに**登録**をクリックできます。



5. 証明書テンプレートの詳細を指定するには、**詳細**の矢印ボタンをクリックして、以下を構成します。

   サブジェクト名: 共通名を選択し、Delivery Controller の FQDN を追加します。

   代替名: DNSを選択し、Delivery ControllerのFQDNを追加します。



SSL/TLSリスナーポートの構成

Web StudioおよびDirectorの一部としてインストールされるIIS Windowsコンポーネントが同じサーバーにインストールされている場合、IISを使用してTLSを構成できます。詳細については、「Web StudioおよびDirectorでTLSを有効にする」を参照してください。それ以外の場合、PowerShellを使用して証明書を構成するには、次の手順を実行します。

1. 既存の証明書がバインドされているか確認するには、コマンドプロンプトを開き、`netsh http show sslcert`を実行します。

   ```
   netsh http show sslcert
   ```

2. 既存のバインドがある場合は、それを削除します。

```
netsh http delete sslcert ipport=0.0.0.0:443
```

既存のバインドで指定されていた場合は、`0.0.0.0:443`を特定のIPアドレスとポートに置き換えます。

3. 以前にインストールした証明書のサムプリントを見つけます。サムプリントを表示するには、**コンピューター証明書の管理**を開き、証明書を参照して開き、**詳細**タブに移動します。

   サムプリントを示す証明書のプロパティのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/certificate-thumbprint.png)

   または、PowerShellを使用することもできます。たとえば、次のスクリプトは、共通名がサーバーのホスト名と一致する証明書を検索し、サムネイルを出力します。

   ```
   $HostName =
   ([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

   $Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
   {$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

   Write-Host -Object "Certificate Thumbprint for $($HostName): $
   ($Thumbprint)" -Foreground Yellow
   ```

   証明書の共通名がホスト名と一致しない場合、これは失敗します。ホスト名に対して複数の証明書がある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

   次の例は、フレンドリ名で証明書を検索します。

   ```
   $friendlyName = "My certificate name"

   $Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
   {$_.FriendlyName -eq $friendlyNam}).Thumbprint -join ';'

   Write-Host -Object "Certificate Thumbprint for $friendlyName: $
   ($Thumbprint)" -Foreground Yellow
   ```

   指定されたフレンドリ名を持つ複数の証明書がある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

4. 証明書をポートにバインドするには、`netsh http add sslcert`コマンドを使用します。

```
netsh http add sslcert ipport=[IP address]:443 certhash=[certificate
hash] appid=[application GUID] disablelegacytls=enable
```

- `ipport`: IPアドレスとポート。0.0.0.0:443を使用すると、すべてのIPアドレスに適用されます。代わりに特定のIPアドレスを指定することもできます。
- `certhash`: 前の手順で特定した証明書のサムプリント。
- `appid`: シトリックス ブローカー サービスの GUID。

> **注:**
>
> 証明書を更新または再バインドする際は、任意の GUID ではなく、Broker Service に関連付けられている特定の `appid` を使用してください。
>
> Citrix Broker Service の正しい `appid` を見つけるには:

a. 管理者として PowerShell コマンドウィンドウを開き、次のコマンドを実行します:

```
Get-WmiObject -Class Win32_Product | Select-String -Pattern
"broker"
```

b. 出力でCitrix Broker ServiceのIdentifyingNumber (GUID) を見つけます (例: `{D333C884-187F-447C-8C67-463F33989C8F}`)。このGUIDを`appid`パラメーターに使用します。

- `disablelegacytls=enable`: レガシーバージョンの TLS を無効にします。このパラメーターは Windows 2022 以降で利用可能です。Windows 2022 では TLS 1.0 および 1.1 を無効にします。Windows 2025 では、TLS 1.0 および 1.1 はデフォルトで無効になっているため、これは不要です。

たとえば、すべてのIPアドレスで、サムプリント`bc96f958848639fd101a793b87915d5f2829b0b6`の証明書をポート`443`にバインドするには、次のコマンドを実行します。

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=bc96f958848639fd101a793b87915d5f2829b0b6 appid={91fe7386-
e0c2-471b-a252-1e0a805febac} disablelegacytls=enable
```

HTTPS が有効になったら、StoreFront の展開 および Netscaler Gateway を構成して、HTTP の代わりに HTTPS を使用してデリバリーコントローラーに接続するようにする必要があります。

> **注:**
>
> Controller が Windows Server 2016 にインストールされ、StoreFront が Windows Server 2012 R2 にインストールされている場合、TLS 暗号スイートの順序を変更するために、Controller で構成変更が必要です。この構成変更は、他の Windows Server バージョンの組み合わせの Controller と StoreFront では必要ありません。

> 暗号スイートの順序リストには、`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` の暗号スイート (あるいはその両方) を含める必要があります。また、これらの暗号スイートは、`TLS_DHE_` の暗号スイートよりも前に配置する必要があります。

1. Microsoft グループポリシーエディターを使用して、**コンピューターの構成 > 管理用テンプレート > ネットワーク > SSL 構成設定** に移動します。
2. 「SSL 暗号スイートの順序」ポリシーを編集します。デフォルトでは、このポリシーは「未構成」に設定されています。このポリシーを「有効」に設定します。
3. スイートを正しい順序に並べます。使用しない暗号スイートは削除します。

`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` が、`TLS_DHE_` の暗号スイートの前に来るようにしてください。

Microsoft MSDNで、Schannel 暗号スイートの優先順位付けも参照してください。

HTTPまたはHTTPSポートを変更する

デフォルトでは、Controller上のXML Serviceは、HTTPトラフィックにはポート80を、HTTPSトラフィックにはポート443をリッスンします。デフォルト以外のポートを使用することもできますが、Controllerを信頼できないネットワークに公開することによるセキュリティリスクに注意してください。デフォルトを変更するよりも、スタンドアロンのStoreFrontサーバーを展開する方が望ましいです。

Controllerで使用されるデフォルトのHTTPまたはHTTPSポートを変更するには、Studioから次のコマンドを実行します。

```
BrokerService.exe -WIPORT \<http-port> -WISSLPORT \<https-port>
```

ここで、`<http-port>`はHTTPトラフィックのポート番号、`<https-port>`はHTTPSトラフィックのポート番号です。

> **注：**
>
> ポートを変更した後、Studioでライセンスの互換性とアップグレードに関するメッセージが表示されることがあります。この問題を解決するには、次のPowerShellコマンドレットシーケンスを使用してサービスインスタンスを再登録します。

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS
|

Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |

Register-ConfigServiceInstance
```

HTTPSトラフィックのみを強制する

XML ServiceでHTTPトラフィックを無視させる場合は、Controller上のHKLM\Software\Citrix\DesktopServer\に次のレジストリ設定を作成し、Broker Serviceを再起動します。

HTTPトラフィックを無視するには、DWORD XmlServicesEnableNonSslを作成し、0に設定します。

HTTPSトラフィックを無視するために作成できる対応するレジストリDWORD値があります：DWORD XmlServicesEnableSsl。これが0に設定されていないことを確認してください。

VDA上のTLS設定

デリバリーグループには、TLSが構成されているVDAとTLSが構成されていないVDAを混在させることはできません。デリバリーグループにTLSを構成する前に、そのデリバリーグループ内のすべてのVDAにTLSが構成されていることを確認してください。

VDAでTLSを構成すると、インストールされているTLS証明書の権限が変更され、ICA®サービスに証明書の秘密キーへの読み取りアクセス権が付与され、ICAサービスに次の情報が通知されます。

- **TLSに使用する証明書ストア内の証明書。**
- **TLS接続に使用するTCPポート番号。**

  Windows ファイアウォール（有効な場合）は、この TCP ポートでの受信接続を許可するように構成する必要があります。この構成は、PowerShell スクリプトを使用すると自動的に行われます。
- **許可するTLSプロトコルのバージョン。**

  > **重要:**
  >
  > Citrixでは、SSLv3の使用状況を確認し、必要に応じてSSLv3のサポートを削除するように展開を再構成することをお勧めします。CTX200238を参照してください。
  >
  > サポートされているTLSプロトコルバージョンには階層があります（低い順から高い順）：SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3。許可される最小バージョンを指定すると、そのバージョン以上を使用するすべてのプロトコル接続が許可されます。

  たとえば、TLS 1.1 を最小バージョンとして指定した場合、TLS 1.1 および TLS 1.3 プロトコル接続が許可されます。SSL 3.0 を最小バージョンとして指定した場合、サポートされているすべてのバージョンの接続が許可されます。TLS 1.3 を最小バージョンとして指定した場合、TLS 1.3 接続のみが許可されます。

  DTLS 1.0はTLS 1.1に、DTLS 1.3はTLS 1.3に対応します。
- **許可するTLS暗号スイート。**

  暗号スイートは、接続に使用される暗号化を選択します。クライアントとVDAは、異なる暗号スイートのセットをサポートできます。クライアント（Citrix Workspaceアプリまたは StoreFront）が接続し、サポートされているTLS暗号スイートのリストを送信すると、VDAはクライアントの暗号スイートの1つを、自身の構成済み暗号スイートのリストにある暗号スイートの1つと照合し、接続を受け入れます。一致する暗号スイートがない場合、VDAは接続を拒否します。

  VDAは、3つの暗号スイートセット（コンプライアンスモードとも呼ばれます）をサポートしています：GOV（政府）、COM（商用）、およびALL。許容される暗号スイートは、Windows FIPSモードにも依存します。Windows FIPSモードについては、`<http://support.microsoft.com/kb/811833>`を参照してください。次の表に、各セットの暗号スイートを示します。

TLS/DTLS暗号スイート	すべて	COM	GOV	すべて	COM	GOV
FIPSモード	オフ	オフ	オフ	オン	オン	オン
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X	X		X	X	

* Windows Server 2012 R2ではサポートされていません。

注:

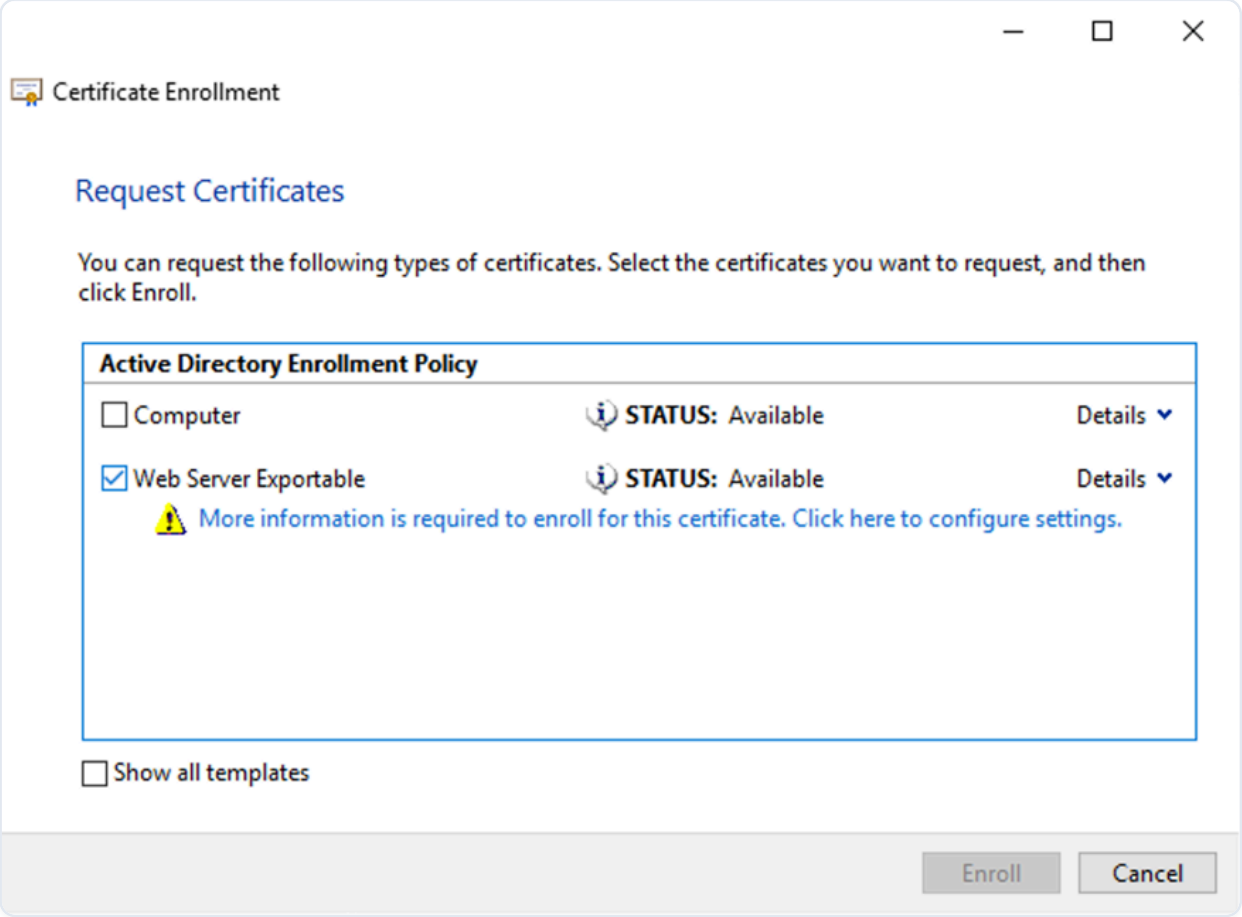
VDAはDHE暗号スイート（例：TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_256_CBC_SHA、TLS_DHE_RSA_WITH_AES_128_GCM_SHA256、TLS_DHE_RSA_WITH_AES_128_CBC_SHA）をサポートしていません。Windowsによって選択された場合でも、Receiverでは使用されない可能性があります。

Citrix Gatewayを使用している場合は、バックエンド通信の暗号スイートサポートに関する情報について、Citrix ADCのドキュメントを参照してください。TLS暗号スイートのサポー

> トについては、Citrix ADCアプライアンスで利用可能な暗号を参照してください。DTLS暗号スイートのサポートについては、DTLS暗号のサポートを参照してください。

証明書のリクエストとインストール

1. VDAで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、コンピューターアカウントを選択します。
2. **個人 > 証明書**を展開し、コンテキストメニューコマンド**すべてのタスク > 新しい証明書のリクエスト**を使用します。
3. **次へ**をクリックして開始し、**次へ**をクリックして、Active Directory登録から証明書を取得することを確認します。
4. サーバー認証証明書のテンプレートを選択します。デフォルトのWindows **コンピューター**または**Webサーバーエクスポート可能**のいずれも使用できます。テンプレートが件名の値を自動的に提供するように設定されている場合は、詳細を指定せずに**登録**をクリックできます。



5. 証明書テンプレートの詳細を指定するには、**詳細**をクリックして以下を構成します。

   サブジェクト名 — タイプ**共通名**を選択し、VDAのFQDNを追加します

   代替名 — タイプ**DNS**を選択し、VDAのFQDNを追加します

証明書のプロパティ(/en-us/citrix-virtual-apps-desktops/2311/media/tls-certificate-properties.png)

> **注：**
>
> Active Directory証明書サービス証明書の自動登録を使用して、VDAへの証明書の発行と展開を自動化します。これについては`<https://support.citrix.com/article/CTX205473>`で説明されています。
>
> ワイルドカード証明書を使用して、単一の証明書で複数のVDAを保護できます。

サブジェクト名 — タイプ **共通名** を選択し、VDA の *.primary.domain を入力します。

代替名 — タイプ **DNS** を選択し、VDA の *.primary.domain を追加します。

ワイルドカード証明書要求ダイアログ(/en-us/citrix-virtual-apps-desktops/2311/media/tls-request-certificates-wildcard.png)

SAN 証明書を使用して、単一の証明書で複数の特定の VDA を保護できます。

サブジェクト名 — タイプ **共通名** を選択し、証明書の使用状況を識別するのに役立つ文字列を入力します。

代替名 — タイプ **DNS** を選択し、各 VDA の FQDN のエントリを追加します。最適な TLS ネゴシエーションを確保するために、代替名の数を最小限に抑えてください。

「証明書要求」ダイアログ(/en-us/citrix-virtual-apps-desktops/2311/media/tls-request-certificates-san.png)

> **注:**
>
> ワイルドカード証明書とSAN証明書の両方で、秘密キーのタブで**秘密キーをエクスポート可能にする**が選択されている必要があります。
>
> 「証明書要求」ダイアログ(/en-us/citrix-virtual-apps-desktops/2311/media/tls-certificate-properties-private-key.png)

PowerShellスクリプトを使用してVDAでTLSを構成する

TLS証明書を証明書ストアのローカルコンピューター > 個人 > 証明書の領域にインストールします。その場所に複数の証明書がある場合は、証明書のサムプリントをPowerShellスクリプトに提供します。

> **注:**
>
> XenAppおよびXenDesktop 7.16 LTSR以降、PowerShellスクリプトはVDAのFQDNに基づいて正しい証明書を見つけます。VDAのFQDNに対して単一の証明書のみが存在する場合、サムプリントを提供する必要はありません。

> Enable-VdaSSL.ps1スクリプトは、VDA上のTLSリスナーを有効または無効にします。このスクリプトは、インストールメディアの*Support* > *Tools* > *SslSupport*フォルダーにあります。

TLSを有効にすると、DHE暗号スイートは無効になります。ECDHE暗号スイートは影響を受けません。

TLSを有効にすると、スクリプトは指定されたTCPポートの既存のWindowsファイアウォール規則をすべて無効にします。次に、ICAサービスがTLS TCPポートとUDPポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。また、次のWindowsファイアウォール規則も無効にします。

- Citrix ICA（デフォルト：1494）
- Citrix CGP（デフォルト：2598）
- Citrix WebSocket（デフォルト：8008）

その結果、ユーザーはTLSまたはDTLSを使用してのみ接続できるようになります。TLSまたはDTLSなしでは、ICA/HDX、セッションの信頼性を備えたICA/HDX、またはWebSocket経由のHDXを使用できません。

> **注：**
>
> DTLSは、UDPリアルタイムトランスポート経由のICA/HDXオーディオ、またはICA/HDX Framehawkではサポートされていません。

「ネットワークポート」を参照してください。

スクリプトには、以下の構文の説明と追加の例が含まれています。Notepad++などのツールを使用して、この情報を確認できます。

重要：

EnableまたはDisableパラメーターと、CertificateThumbPrintパラメーターのいずれかを指定します。その他のパラメーターはオプションです。

構文

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint "<thumbprint>" [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]
```

パラメーター	説明
有効	VDAにTLSリスナーをインストールして有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効	VDA上のTLSリスナーを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。このパラメーターを指定した場合、他のパラメーターは無効になります。
証明書サムプリント "<thumbprint>"	引用符で囲まれた、証明書ストア内のTLS証明書のサムプリント。スクリプトは指定されたサムプリントを使用して、使用する証明書を選択します。このパラメーターを省略すると、誤った証明書が選択されます。
SSLポート <port>	TLSポート。デフォルト: 443
SSL最小バージョン "<version>"	引用符で囲まれた最小TLSプロトコルバージョン。有効な値: “TLS_1.0”（デフォルト）、“TLS_1.1”、および“TLS_1.3”。
SSL暗号スイート "<suite>"	TLS暗号スイート。引用符で囲みます。有効な値: "GOV"、"COM"、および "ALL" (デフォルト)。

例

次のスクリプトは、TLS プロトコルバージョン値をインストールして有効にします。サムプリント（この例では「12345678987654321」として表されています）は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

以下のスクリプトは、TLSリスナーをインストールして有効にし、TLSポート400、GOV暗号スイート、および最小TLS 1.2プロトコル値を指定します。サムプリント（この例では「12345678987654321」として表されています）は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable

-CertificateThumbPrint "12345678987654321"

-SSLPort 400 -SSLMinVersion "TLS_1.3"

-SSLCipherSuite "All"
```

次のスクリプトは、VDA上のTLSリスナーを無効にします。

```
Enable-VdaSSL -Disable
```

VDAでTLSを手動で構成する

VDAでTLSを手動で構成する場合、各VDA上の適切なサービス（WindowsシングルセッションOS用VDAの場合はNT SERVICE\PorticaService、WindowsマルチセッションOS用VDAの場合はNT SERVICE\TermService）のTLS証明書の秘密キーに一般的な読み取りアクセス権を付与します。VDAがインストールされているマシンで、次の手順を実行します。

ステップ1。Microsoft管理コンソール（MMC）を起動します： > > 。

ステップ2。MMCに証明書スナップインを追加します。

1. > を選択します。
2. を選択し、 をクリックします。
3. 「このスナップインは常に次の証明書を管理します:」というプロンプトが表示されたら、「コンピューターアカウント」を選択し、 をクリックします。

4. 「このスナップインで管理するコンピューターを選択してください」というプロンプトが表示されたら、「ローカルコンピューター」を選択し、 をクリックします。

ステップ3。 > > の下で、証明書を右クリックし、 > を選択します。

ステップ4。アクセス制御リストエディターに「(FriendlyName) の秘密キーのアクセス許可」が表示されます。(FriendlyName) はTLS証明書の名前です。以下のいずれかのサービスを追加し、読み取りアクセス権を付与します。

- WindowsシングルセッションOS用VDAの場合、「PORTICASERVICE」
- Windows Multi-session OS 用 VDA の場合、「TERMSERVICE」

ステップ5。インストールされているTLS証明書をダブルクリックします。証明書ダイアログで、タブを選択し、一番下までスクロールします。 をクリックします。

ステップ 6. regedit を実行し、HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd に移動します。

1. SSL Thumbprint キーを編集し、TLS 証明書のサムプリントの値をこのバイナリ値にコピーします。バイナリ値の編集ダイアログボックスの不明な項目（「0000」や特殊文字など）は無視しても問題ありません。
2. SSLEnabled キーを編集し、DWORD 値を 1 に変更します。（後で SSL を無効にするには、DWORD 値を 0 に変更します。）
3. デフォルト設定を変更する場合（オプション）は、同じレジストリパスで以下を使用します。

   SSLPort DWORD – SSL ポート番号。デフォルト: 443。

   SSLMinVersion DWORD – 1 = SSL 3.0、2 = TLS 1.0、3 = TLS 1.1、4 = TLS 1.3。デフォルト: 2 (TLS 1.0)。

   SSLCipherSuite DWORD – 1 = GOV、2 = COM、3 = ALL。デフォルト: 3 (ALL)。

ステップ 7. TLS の TCP および UDP ポートがデフォルトの 443 ではない場合、Windows ファイアウォールで開いていることを確認します。（Windows ファイアウォールで受信規則を作成する際は、そのプロパティで「接続を許可する」と「有効」が選択されていることを確認してください。）

ステップ 8. 他のアプリケーションやサービス（IIS など）が TLS TCP ポートを使用していないことを確認します。

ステップ 9. Windows Multi-session OS 用 VDA の場合、変更を有効にするためにマシンを再起動します。（Windows Single-session OS 用 VDA を含むマシンを再起動する必要はありません。）

重要:

VDA が Windows Server 2012 R2、Windows Server 2016、または Windows 10 Anniversary Edition 以降のサポート対象リリース上にある場合、追加の手順が必要です。これは、Citrix Receiver for Windows (バージョン 4.6 から 4.9)、Citrix Workspace app for HTML5、および Citrix Workspace app for Chrome からの接続に影響します。これには、Citrix Gateway を使用する接続も含まれます。

Citrix Gateway と VDA 間の TLS が構成されている場合、すべての VDA バージョンにおいて、Citrix Gateway を使用するすべての接続でこの手順も必要です。これは、すべての Citrix Receiver™ バージョンに影響します。

VDA (Windows Server 2012 R2、Windows Server 2016、または Windows 10 Anniversary Edition 以降) で、グループポリシーエディターを使用して、Computer Configuration > Policies > Administrative Templates > Network > SSL Configuration Settings > SSL Cipher Suite Order に移動します。次の順序を選択します。

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

注:

最初の6つの項目では、楕円曲線（P384またはP256）も指定されています。
「curve25519」が選択されていないことを確認してください。FIPSモードは
「curve25519」の使用を妨げません。

> このグループポリシー設定が構成されている場合、VDAは、グループポリシーリストと選択されたコンプライアンスモード（COM、GOV、またはALL）のリストの両方に表示される場合にのみ、暗号スイートを選択します。暗号スイートは、クライアント（Citrix Workspaceアプリまたは StoreFront）によって送信されるリストにも表示されている必要があります。

このグループポリシー構成は、VDA上の他のTLSアプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合、それらをこのグループポリシーリストに追加する必要がある場合があります。

> **重要:**
>
> グループポリシーの変更は適用時に表示されますが、TLS構成のグループポリシーの変更は、オペレーティングシステムの再起動後にのみ有効になります。したがって、プールされたデスクトップの場合、TLS構成のグループポリシーの変更をベースイメージに適用してください。

デリバリーグループでのTLSの構成

TLS接続用に構成したVDAを含む各デリバリーグループについて、この手順を完了してください。

1. StudioからPowerShellコンソールを開きます。
2. Citrix製品のコマンドレットを読み込むには、**asnp Citrix.***を実行します。
3. **Get-BrokerAccessPolicyRule -DesktopGroupName '\<*delivery-group-name*>' \| Set-BrokerAccessPolicyRule -HdxSslEnabled $true**を実行します。
4. **Set-BrokerSite -DnsResolutionEnabled $true**を実行します。

トラブルシューティング

接続エラーが発生した場合は、VDAのシステムイベントログを確認してください。

Windows向けCitrix Workspaceアプリを使用しているときに、TLSエラーを示す接続エラーが表示された場合は、Desktop Viewerを無効にしてから、もう一度接続を試してください。接続は引き続き失敗しますが、基になるTLS問題の説明が提供される場合があります。（たとえば、証明機関から証明書を要求する際に誤ったテンプレートを指定したなど。）

HDX™ Adaptive Transportを使用するほとんどの構成は、Citrix Workspaceアプリ、Citrix Gateway、およびVDAの最新バージョンを使用するものを含め、DTLSで正常に動作します。Citrix

WorkspaceアプリとCitrix Gatewayの間、およびCitrix GatewayとVDAの間でDTLSを使用する一部の構成では、追加の操作が必要です。

次の場合、追加の操作が必要です。

- Citrix ReceiverのバージョンがHDX Adaptive TransportとDTLSをサポートしている場合：Receiver for Windows (4.7, 4.8, 4.9)、Receiver for Mac (12.5, 12.6, 12.7)、Receiver for iOS (7.2, 7.3.x)、またはReceiver for Linux (13.7)

かつ、以下のいずれかが当てはまる場合：

- Citrix GatewayのバージョンはVDAへのDTLSをサポートしているが、VDAのバージョンはDTLSをサポートしていない（バージョン7.15以前）。
- VDAのバージョンがDTLSをサポートしているが（バージョン7.16以降）、Citrix GatewayのバージョンがVDAへのDTLSをサポートしていない場合。

Citrix Receiverからの接続が失敗するのを避けるには、以下のいずれかを実行してください。

- Citrix Receiverを、Receiver for Windowsバージョン4.10以降、Receiver for Mac 12.8以降、またはReceiver for iOSバージョン7.5以降に更新する。
- Citrix Gatewayを、VDAへのDTLSをサポートするバージョンに更新する。
- VDAをバージョン7.16以降に更新する。
- VDAでDTLSを無効にする。
- HDX Adaptive Transportを無効にする。

> **注:**
>
> Receiver for Linuxの適切なアップデートはまだ利用できません。Receiver for Android (バージョン3.12.3) は、Citrix Gateway経由のHDX Adaptive TransportおよびDTLSをサポートしていないため、影響を受けません。

> VDAでDTLSを無効にするには、VDAファイアウォール設定を変更してUDPポート443を無効にします。(/ja-jp/tech-zone/build/tech-papers/citrix-communication-ports.html#citrix-virtual-apps-and-desktops)を参照してください。

ControllerとVDA間の通信

Windows Communication Framework (WCF) メッセージレベル保護は、Controller と VDA 間の通信を保護します。TLS を使用した追加のトランスポートレベル保護は必要ありません。WCF 構成では、Controller と VDA 間の相互認証に Kerberos を使用します。暗号化には、256 ビットキーの CBC モードで AES を使用します。メッセージの整合性には SHA-1 を使用します。

Microsoftによると、WCFで使用されるセキュリティ プロトコル は、WS-SecurityPolicy 1.2を含むOASIS（Organization for the Advancement of Structured Information Standards）の標準に準拠しています。さらに、Microsoftは、WCFが Security Policy 1.2 に記載されているすべてのアルゴリズムスイートをサポートしていると述べています。

Controller と VDA 間の通信には、上記で述べたアルゴリズムを持つ basic256 アルゴリズムスイートが使用されます。

TLS と HTML5 ビデオリダイレクト、およびブラウザコンテンツリダイレクト

HTML5 ビデオリダイレクトとブラウザコンテンツリダイレクトを使用して、HTTPS Web サイトをリダイレクトできます。これらの Web サイトに挿入された JavaScript は、VDA で実行されている Citrix HDX HTML5 ビデオリダイレクトサービスへの TLS 接続を確立する必要があります。これを実現するために、HTML5 ビデオリダイレクトサービスは、VDA の証明書ストアに 2 つのカスタム証明書を生成します。サービスを停止すると、証明書は削除されます。

HTML5 ビデオリダイレクトポリシーは、デフォルトで無効になっています。

ブラウザコンテンツリダイレクトは、デフォルトで有効になっています。

HTML5 ビデオリダイレクトの詳細については、「マルチメディアポリシー設定」を参照してください。

ユニバーサルプリントサーバーにおけるトランスポート層セキュリティ (TLS)

仮想デリバリーエージェント (VDA) とユニバーサルプリントサーバー間のTCPベースの接続では、トランスポート層セキュリティ (TLS) プロトコルがサポートされています。

> **警告:**
>
> Windowsレジストリでの作業を含むタスクの場合、レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決できる

> ことを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

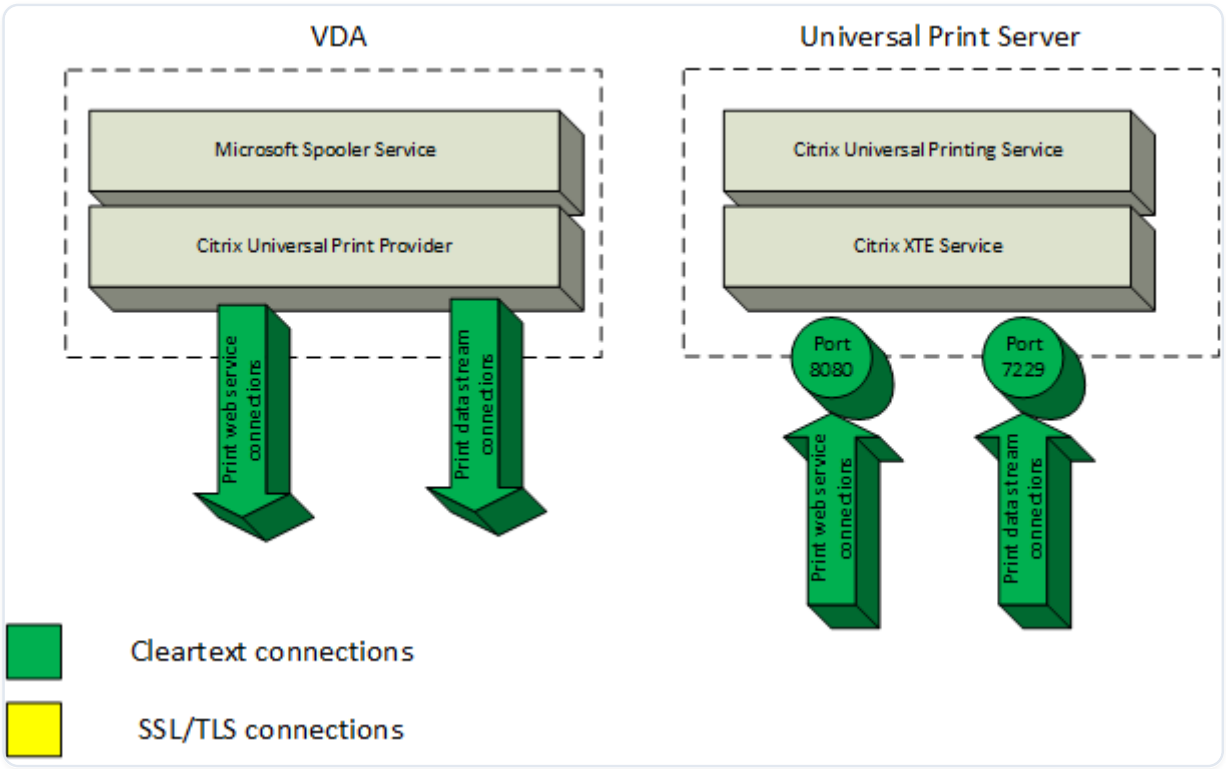
VDAとユニバーサルプリントサーバー間の印刷接続の種類

クリアテキスト接続

以下の印刷関連の接続はVDAから発信され、ユニバーサルプリントサーバー上のポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Disabled** (デフォルト) に設定されている場合にのみ行われます。

- クリアテキスト印刷Webサービス接続 (TCPポート 8080)
- クリアテキスト印刷データストリーム (CGP) 接続 (TCPポート 7229)

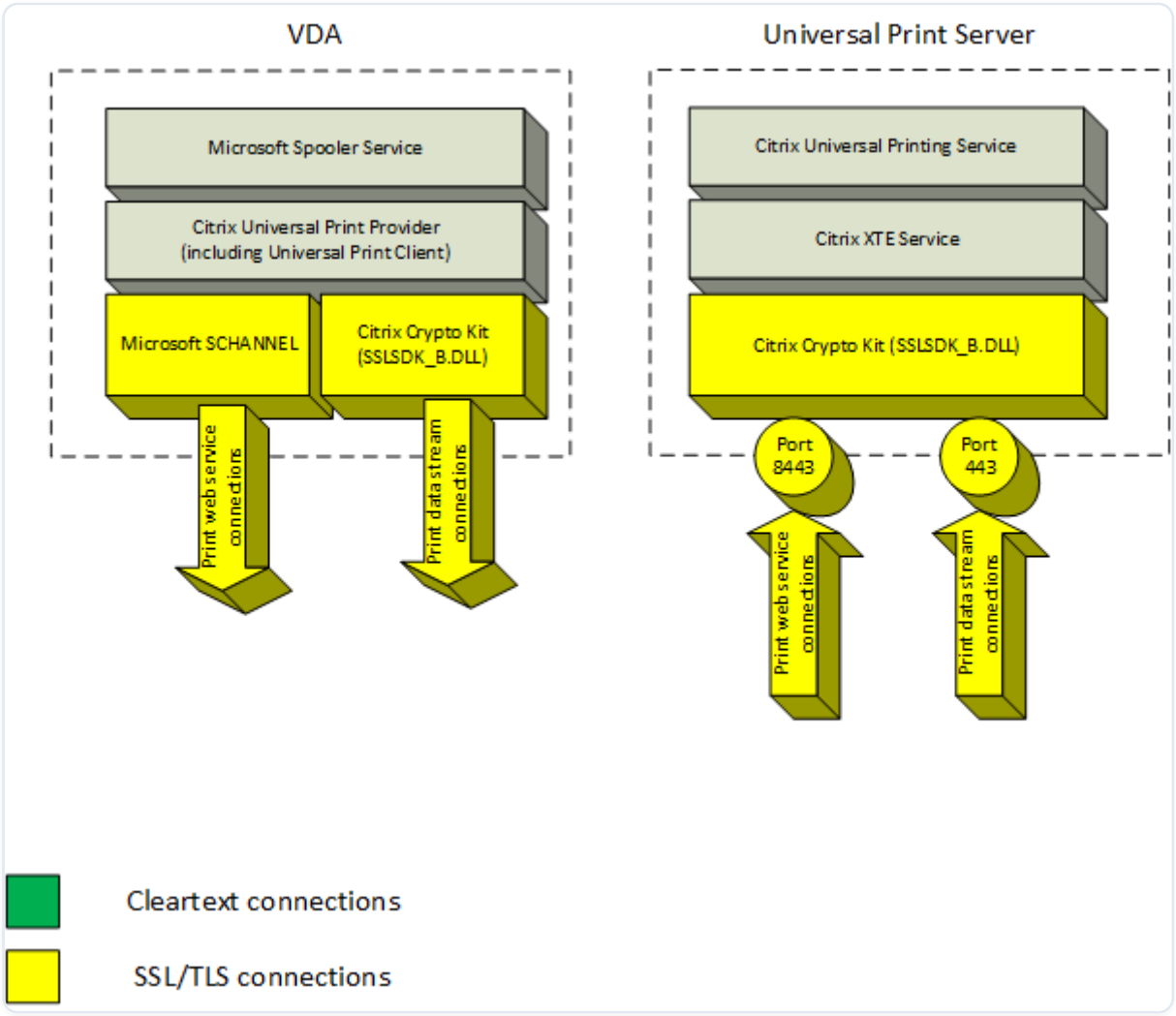
Microsoftサポート記事「Service overview and network port requirements for Windows」では、Microsoft Windows Print Spoolerサービスが使用するポートについて説明しています。このドキュメントのSSL/TLS設定は、Windows Print Spoolerサービスによって行われるNetBIOSおよびRPC接続には適用されません。**Universal Print Server enable** ポリシー設定が **Enabled with fallback to Windows' native remote printing** に設定されている場合、VDAはWindows Network Print Provider (win32spl.dll) をフォールバックとして使用します。



暗号化された接続

これらの印刷関連のSSL/TLS接続はVDAから発信され、ユニバーサルプリントサーバー上のポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Enabled** に設定されている場合にのみ行われます。

- 暗号化された印刷Webサービス接続 (TCPポート 8443)
- 暗号化された印刷データストリーム (CGP) 接続 (TCPポート 443)



SSL/TLS クライアント構成

VDA は SSL/TLS クライアントとして機能します。

Microsoft Group Policy とレジストリを使用して、暗号化された印刷 Web サービス接続 (TCP ポート 8443) 用に Microsoft SCHANNEL SSP を構成します。Microsoft サポート記事の TLS Registry Settings には、Microsoft SCHANNEL SSP のレジストリ設定が記載されています。

VDAでグループポリシーエディターを使用し、**Computer Configuration > Administrative Templates > Network > SSL Configuration Settings > SSL Cipher Suite Order**に移動します。TLS 1.3が設定されている場合は、次の順序を選択します。

TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256

TLS 1.2 が設定されている場合は、次の順序を選択します。

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

注:

このグループポリシー設定が構成されている場合、VDA は、暗号化された印刷 Web サービス接続 (デフォルトポート: 8443) の暗号スイートを、接続が両方の SSL 暗号スイートリストに表示されている場合にのみ選択します。

- グループポリシーSSL暗号スイート順序リスト
- 選択されたSSL Cipher Suiteポリシー設定（COM、GOV、またはALL）に対応するリスト

このグループポリシー構成は、VDA 上の他の TLS アプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合、それらをこのグループポリシー暗号スイート順序リストに追加する必要がある場合があります。

重要:

TLS構成のグループポリシー変更は、オペレーティングシステムの再起動後にのみ有効になります。

Citrixポリシーを使用して、暗号化された印刷データストリーム (CGP) 接続 (TCPポート443) のSSL/TLS設定を構成します。

SSL/TLS サーバー構成

ユニバーサルプリントサーバーはSSL/TLSサーバーとして機能します。

`Enable-UpsSsl.ps1` PowerShellスクリプトを使用して、SSL/TLS設定を構成します。

Universal Print ServerにTLSサーバー証明書をインストールする

HTTPSの場合、Universal Print Serverはサーバー証明書を使用してTLS機能をサポートします。クライアント証明書は使用されません。Microsoft Active Directory証明書サービスまたは別の認証局を使用して、Universal Print Serverの証明書を要求します。

マイクロソフト Active Directory 証明書サービスを使用して証明書を登録または要求する際は、以下の考慮事項に留意してください。

1. 証明書をローカルコンピューターの**個人**証明書ストアに配置します。
2. 証明書のサブジェクト識別名 (Subject DN) の**共通名**属性を、Universal Print Serverの完全修飾ドメイン名 (FQDN) に設定します。これは証明書テンプレートで指定します。
3. 証明書要求と秘密鍵の生成に使用される暗号化サービスプロバイダー (CSP) を、**Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)** に設定します。これは証明書テンプレートで指定します。
4. キーサイズを2048ビット以上に設定します。これは証明書テンプレートで指定します。

Universal Print ServerでのSSLの構成

Universal Print Server上のXTEサービスは、受信接続をリッスンします。SSLが有効な場合、SSLサーバーとして機能します。受信接続には、印刷コマンドを含む印刷Webサービス接続と、印刷ジョブを含む印刷データストリーム接続の2種類があります。これらの接続でSSLを有効にできます。SSLは、これらの接続の機密性と整合性を保護します。デフォルトでは、SSLは無効になっています。

SSLの構成に使用されるPowerShellスクリプトは、インストールメディアにあり、ファイル名は次のとおりです: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1.`.

Universal Print Serverでのリスニングポート番号の構成

XTEサービス のデフォルトポートは次のとおりです。

- クリアテキスト印刷Webサービス（HTTP）TCPポート: 8080
- クリアテキスト印刷データストリーム (CGP) TCPポート: 7229
- 暗号化された印刷Webサービス (HTTPS) TCPポート: 8443
- 暗号化された印刷データストリーム (CGP) TCPポート: 443

Universal Print Server でXTEサービスが使用するポートを変更するには、管理者として PowerShellで次のコマンドを実行します（Enable-UpsSsl.ps1 PowerShellスクリプトの使用方法については、後のセクションを参照してください）。

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` または `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

ユニバーサル プリント サーバーのTLS設定

負荷分散構成で複数のUniversal Print Serverを使用している場合は、すべてのUniversal Print Serverで **TLS** 設定が一貫して構成されていることを確認してください。

Universal Print Server でTLSを構成すると、インストールされているTLS証明書のアクセス許可が変更され、Universal Printing Serviceに証明書の秘密キーへの読み取りアクセス権が付与され、Universal Printing Serviceに次の情報が通知されます。

- TLSに使用する証明書ストア内の証明書。
- TLS接続に使用するTCPポート番号。

Windowsファイアウォール (有効な場合) は、これらのTCPポートでの受信接続を許可するように構成する必要があります。この構成は、Enable-UpsSsl.ps1 PowerShellスクリプトを使用すると自動的に行われます。

- 許可するTLSプロトコルのバージョン。

Universal Print ServerはTLSプロトコルバージョン1.3および1.2をサポートしています。許可される最小バージョンを指定します。

デフォルトのTLSプロトコルバージョンは1.2です。

> **注:**
>
> TLS 1.1および1.0は、Citrix Virtual Apps and Desktopsバージョン2311以降サポートされなくなりました。

- 許可するTLS暗号スイート。

暗号スイートは、接続に使用される暗号化アルゴリズムを選択します。VDAとUniversal Print Serverは、異なる暗号スイートのセットをサポートできます。VDAが接続し、サポートされているTLS暗号スイートのリストを送信すると、Universal Print Serverはクライアントの暗号スイートの1つを、自身の構成済み暗号スイートのリストにある暗号スイートの1つと照合し、接続を受け入れます。一致する暗号スイートがない場合、Universal Print Serverは接続を拒否します。

Universal Print Serverは、OPEN、FIPS、およびSP800-52ネイティブCrypto Kitモードに対して、GOV(ernment)、COM(mercial)、およびALLという名前の以下の暗号スイートセットをサポートしています。許容される暗号スイートは、**SSL FIPS Mode**ポリシー設定とWindows FIPS Modeにも依存します。Windows FIPSモードの詳細については、このMicrosoftサポート記事を参照してください。

暗号スイート（優先順位の降順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_	X		X	X		X	X		X

暗号スイート（優先順位の降順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
SHA384									
TLS_ECDHE_RSA_AES256_CBC_SHA	X	X		X	X		X	X	

PowerShellスクリプトを使用してUniversal Print ServerでTLSを構成する

証明書ストアの**ローカルコンピューター > 個人 > 証明書**領域にTLS証明書をインストールします。その場所に複数の証明書がある場合は、証明書のサムプリントを`Enable-UpsSsl.ps1` PowerShellスクリプトに指定します。

> **注:**
>
> PowerShellスクリプトは、Universal Print ServerのFQDNに基づいて正しい証明書を検索します。Universal Print ServerのFQDNに対して単一の証明書のみが存在する場合、証明書のサムプリントを指定する必要はありません。

> `Enable-UpsSsl.ps1` スクリプトは、VDAからUniversal Print ServerへのTLS接続を有効または無効にします。このスクリプトは、インストールメディアの**Support > Tools > SslSupport**フォルダーにあります。

TLSを有効にすると、スクリプトはUniversal Print ServerのTCPポートに対する既存のすべてのWindowsファイアウォールルールを無効にします。その後、XTEサービスがTLS TCPおよびUDPポートでのみ受信接続を受け入れることを許可する新しいルールを追加します。また、以下のWindowsファイアウォールルールも無効にします。

- クリアテキスト印刷Webサービス接続 (デフォルト: 8080)
- クリアテキスト印刷データストリーム (CGP) 接続 (デフォルト: 7229)

その結果、VDAはTLSを使用している場合にのみこれらの接続を行うことができます。

> **注：**
>
> TLSを有効にしても、VDAからUniversal Print ServerへのWindows Print Spooler RPC/SMB接続には影響しません。

> **重要：**
>
> 最初のパラメーターとして、**Enable**または**Disable**のいずれかを指定します。ローカルコンピューターの個人証明書ストアにUniversal Print ServerのFQDNを持つ証明書が1つしかない場合、CertificateThumbprintパラメーターはオプションです。その他のパラメーターはオプションです。

構文

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort &lt;port&gt;] [-CGPPort &lt;port&gt;] [-HTTPSPort &lt;port&gt;] [-CGPSSLPort &lt;port&gt;] [-SSLMinVersion &lt;version&gt;] [-SSLCipherSuite &lt;name&gt;] [-CertificateThumbprint &lt;thumbprint&gt;] [-FIPSMode &lt;Boolean&gt;] [-ComplianceMode &lt;mode&gt;]

Enable-UpsSSL.ps1 -Disable [-HTTPPort &lt;portnum&gt;] [-CGPPort &lt;portnum&gt;]
```

パラメーター	説明
有効にする	XTEサーバーでSSL/TLSを有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。

パラメーター	説明
無効にする	XTEサーバーでSSL/TLSを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。
CertificateThumbprint `"<thumbprint>"`	ローカルコンピューターの個人証明書ストアにあるTLS証明書のサムプリントを引用符で囲んで指定します。スクリプトは、指定されたサムプリントを使用して、使用する証明書を選択します。
HTTPポート `<port>`	クリアテキスト印刷Webサービス (HTTP/SOAP) ポート。デフォルト: 8080
CGPポート `<port>`	クリアテキスト印刷データストリーム (CGP) ポート。デフォルト: 7229
HTTPSポート `<port>`	暗号化された印刷Webサービス (HTTPS/SOAP) ポート。デフォルト: 8443
CGPSSLポート `<port>`	暗号化された印刷データストリーム (CGP) ポート。デフォルト: 443
SSLMinVersion `"<version>"`	引用符で囲まれた最小TLSプロトコルバージョン。有効な値: 「TLS_1.2」および「TLS_1.3」。デフォルト: TLS_1.2。
SSLCipherSuite `"<name>"`	引用符で囲まれたTLS暗号スイートパッケージの名前。有効な値: 「GOV」、「COM」、および「ALL」(デフォルト)。
FIPSモード `<Boolean>`	XTEサーバーでFIPS 140モードを有効または無効にします。有効な値: FIPS 140モードを有効にする場合は$true、FIPS 140モードを無効にする場合は$false。

例

次のスクリプトはTLSを有効にします。サムプリント（この例では「12345678987654321」として表されています）は、使用する証明書を選択するために使用されます。

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

次のスクリプトはTLSを無効にします。

```
Enable-UpsSsl.ps1 –Disable
```

FIPSモードの構成

米国連邦情報処理標準（FIPS）モードを有効にすると、Universal Print Serverの暗号化された接続にはFIPS 140準拠の暗号化のみが使用されるようになります。

クライアントでFIPSモードを構成する前に、サーバーでFIPSモードを構成してください。

WindowsのFIPSモードを有効または無効にする方法については、マイクロソフトのドキュメントサイトを参照してください。

クライアントでのFIPSモードの有効化

Delivery Controller™でWeb Studioを実行し、Citrixポリシー設定の**SSL FIPS Mode**を**Enabled**に設定します。Citrixポリシーを有効にします。

各VDAで以下を実行します。

1. Windows FIPSモードを有効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの有効化

各Universal Print Serverで以下を実行します。

1. Windows FIPSモードを有効にします。
2. 管理者として次のPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
3. `-Enable -FIPSMode $true` パラメーターを指定して、`Enable-UpsSsl.ps1` スクリプトを実行します。
4. Universal Print Serverを再起動します。

クライアントでのFIPSモードの無効化

Web Studioで、**SSL FIPSモード** Citrixポリシー設定を**無効**に設定します。Citrixポリシーを有効にします。**SSL FIPSモード** Citrixポリシー設定を削除することもできます。

各VDAで以下を実行します:

1. Windows FIPSモードを無効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの無効化

各Universal Print Serverで以下を実行します:

1. Windows FIPSモードを無効にします。
2. 管理者として次のPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
3. `-Enable -FIPSMode $false` パラメーターを指定して、`Enable-UpsSsl.ps1` スクリプトを実行します。
4. Universal Print Serverを再起動します。

> **注:**
>
> SSLプロトコルバージョンがTLS 1.3に設定されている場合、FIPSモードはサポートされません。

SSL/TLSプロトコルバージョンの構成

デフォルトのSSL/TLSプロトコルバージョンはTLS 1.2です。TLS 1.2およびTLS 1.3は、実稼働環境での使用が推奨されるSSL/TLSプロトコルバージョンです。トラブルシューティングのために、非実稼働環境でSSL/TLSプロトコルバージョンを一時的に変更する必要がある場合があります。

SSL 2.0およびSSL 3.0はUniversal Print Serverではサポートされていません。

サーバーでのSSL/TLSプロトコルバージョンの設定

各Universal Print Serverで次の操作を行います。

1. 管理者として次のPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
2. `-Enable -SSLMinVersion` バージョンパラメーターを指定して`Enable-UpsSsl.ps1` スクリプトを実行します。テストが完了したら、これをTLS 1.2またはTLS 1.3に戻すことを忘れないでください。
3. Universal Print Serverを再起動します。

クライアントでのSSL/TLSプロトコルバージョンの設定

各VDAで次の操作を行います。

1. Delivery Controllerで、**SSLプロトコルバージョン**ポリシー設定を目的のプロトコルバージョンに設定し、ポリシーを有効にします。

2. Microsoftサポート記事「TLS Registry Settings」には、Microsoft SCHANNEL SSPのレジストリ設定が記載されています。レジストリ設定を使用して、クライアント側の**TLS 1.2またはTLS 1.3**を有効にします。

   > **重要:**
   >
   > テストが完了したら、レジストリ設定を元の値に復元することを忘れないでください。

3. VDAを再起動します。

トラブルシューティング

接続エラーが発生した場合は、Universal Print Server上のC:\Program Files (x86)\Citrix\XTE\logs\error.logファイルを確認してください。

SSL/TLSハンドシェイクが失敗した場合、このログファイルにエラーメッセージ「**SSL handshake from client failed**」が表示されます。このような失敗は、VDAとUniversal Print ServerのSSL/TLSプロトコルバージョンが一致しない場合に発生する可能性があります。

Universal Print Serverのホスト名を含む以下のポリシー設定で、Universal Print ServerのFQDNを使用します。

- セッションプリンター
- プリンターの割り当て
- 負荷分散用のUniversal Print Server

Universal Print ServerとVDAで、システムクロック（日付、時刻、タイムゾーン）が正しいことを確認してください。

仮想チャネルのセキュリティ

デフォルトでは、仮想チャネル許可リスト機能が有効になっています。その結果、Citrix®仮想チャネルのみが仮想アプリおよびデスクトップセッションで開くことが許可されます。自社製であろうとサードパーティ製であろうと、カスタム仮想チャネルを使用する必要がある場合は、仮想チャネルを明示的に許可リストに追加してください。

仮想チャネルを許可リストに追加する

仮想チャネルを許可リストに追加するには、以下が必要です。

1. コードで定義されている仮想チャネル名。最大7文字です。例: `CTXCVC1`。
2. VDAマシン上で仮想チャネルを開くプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。リストに仮想チャネルを追加するには、仮想チャネル名の後にコンマを入力し、次に仮想チャネルにアクセスするプロセスのパスを入力します。複数のプロセスがある場合は、コンマで区切って追加できます。

前の例を使用すると、以下をリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスがある場合は、次をリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名または実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次の項目にはワイルドカードを使用できます。

- ディレクトリ名全体を置き換えるため。例: `C:\Program Files\Application*\run1.exe`
- ディレクトリ名の一部を置き換えるため。例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイルの名前を置き換えるため。例: `C:\Program Files\Application\v1.2*.exe`
- 実行可能ファイル名の一部を置き換えるため。例: `C:\Program Files\Application\v1.2\run*.exe`

以下の制限が適用されます:

- ワイルドカードは単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\Application\v1.2\run1.exe` にある場合
  - 許可されるもの: `C:\Program Files\Application*\run1.exe`
  - 許可されないもの: `C:\Program Files*\run1.exe`

- エントリにはファイル拡張子を含める必要があります。
  - 許可されるもの: `C:\Program Files\Application\v1.2*.exe`
  - 許可されないもの: `C:\Program Files\Application\v1.2*`
- すべてのパスはローカルである必要があります。

> **注:**
>
> Citrix Virtual Apps and Desktops™ 2109リリース以降、ネットワークパスは許可されません。

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加設定なしで開くことが許可されています。ただし、外部依存関係のため、許可リストに明示的なエントリを必要とする機能が2つあります。

- マルチメディアリダイレクト
- HDX™ リアルタイム最適化パック for スカイプ・フォー・ビジネス

マルチメディアリダイレクト

許可リストエントリには、次の情報が必要です。

- 仮想チャネル名: CTXMM
- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX リアルタイム最適化パック for スカイプ・フォー・ビジネス

許可リストエントリには、次の情報が必要です。

- 仮想チャネル名: CTXRMEP
- プロセス: VDAマシン内のSkype for Business実行可能ファイルへのパス。Skype for Businessのバージョンやカスタムインストールパスの使用状況によって異なる場合があります。例: C:\Program Files\Microsoft Office\root\Office16\lync.exe。

- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

仮想チャネル名とプロセスを取得する

仮想チャネル名と、VDAマシン上でそれを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を入手することです。

または、この情報は機能のログを適用し、以下の手順に従うことで取得できます。

1. カスタム仮想チャネルのクライアントおよびサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDAマシンのシステムイベントログで、カスタム仮想チャネルの名前と、それを開こうとしたプロセスを以下のイベントで探します。
   - シングルセッションVDAでは、ソースPicaddからのイベントID 2002。
   - マルチセッションVDAでは、ソースRpmからのイベントID 14。
3. セッションからログオフします。
4. 識別された仮想チャネルとプロセスに対して、仮想チャネル許可リストポリシー設定にエントリを追加します。
5. 仮想アプリケーションまたは仮想デスクトップを起動して、カスタム仮想チャネルが正常に開くことを検証します。

仮想チャネル許可リストのログ記録

シングルセッションVDAマシンのイベントログには、以下のイベントが記録されます。

ログ名	システム
ID	2001
ソース	ピックアップド
レベル	情報
説明	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開かれました

ログ名	システム

ID	2002
ソース	ピキャッド
レベル	警告
説明	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開けません

ログ名	システム
ID	2003
送信元	ピカッド
レベル	情報
説明	`<username>` がカスタム仮想チャネル `<vcName>` を開きました

ログ名	システム
ID	2004
送信元	ピカッド
レベル	警告
説明	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました

以下のイベントが、マルチセッション VDA マシンのイベントログに記録されます。

ログ名	システム
ID	13
送信元	Rpm
レベル	情報

説明	プロセス `<processName>` によってカスタム仮想チャネル `<vcName>` が開かれました

ログ名	システム
ID	14
送信元	Rpm
レベル	警告
説明	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開くことができません

ログ名	システム
ID	15
送信元	Rpm
レベル	情報
説明	`<username>` がカスタム仮想チャネル `<vcName>` を開きました

ログ名	システム
ID	16
送信元	Rpm
レベル	警告
説明	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました

既知のサードパーティ仮想チャネル

以下は、カスタムCitrix仮想チャネルを使用する既知のサードパーティソリューションです。このリストには、カスタムCitrix仮想チャネルを使用するすべてのソリューションが含まれているわけではありません。

- カーナー
- シスコ WebEx Teams
- シスコ WebEx Meetings バーチャルデスクトップソフトウェア
- エピック スリングショット
- エピック ワープドライブ
- ミッドマーク IQPath クライアント拡張機能
- ニュアンス PowerMic クライアント拡張機能
- ニュアンス Dragon Medical Network Edition 360 vSync
- VDI 用 ズームミーティング
- アルティマ IA-Connect

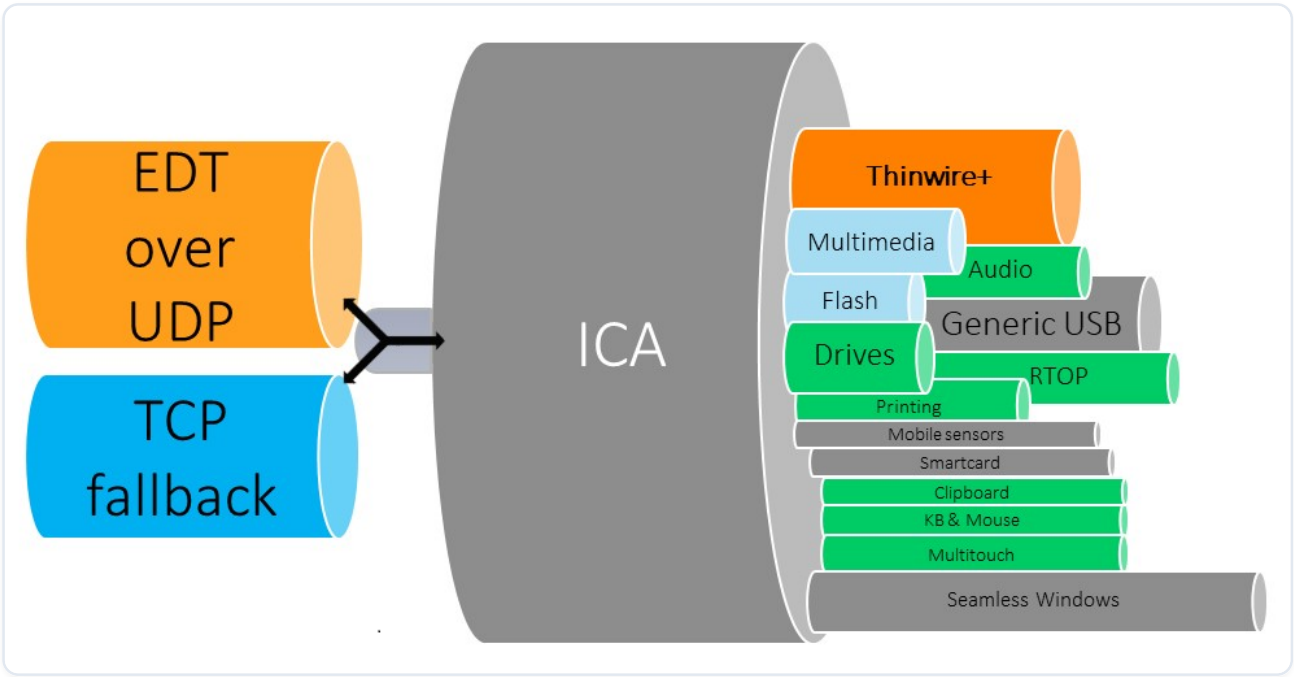
関連する仮想チャネルを許可リストに追加するための詳細については、ソリューションのベンダーにお問い合わせください。または、仮想チャネル名とプロセスの取得セクションに記載されている手順に従ってください。

HDXトランスポート

アダプティブトランスポート

アダプティブトランスポートは、Citrix Virtual Apps and Desktops™におけるメカニズムであり、ICA接続のトランスポートプロトコルとしてEnlightened Data Transport (EDT)を使用する機能を提供します。EDTが利用できない場合、アダプティブトランスポートはTCPに切り替わります。

EDTは、User Datagram Protocol (UDP)上に構築されたCitrix独自のトランスポートプロトコルです。サーバーのスケーラビリティを維持しながら、困難な長距離接続において優れたユーザーエクスペリエンスを提供します。EDTは、信頼性の低いネットワーク上のすべてのICA®仮想チャネルのデータスループットを向上させ、より良く、より一貫したユーザーエクスペリエンスを提供します。

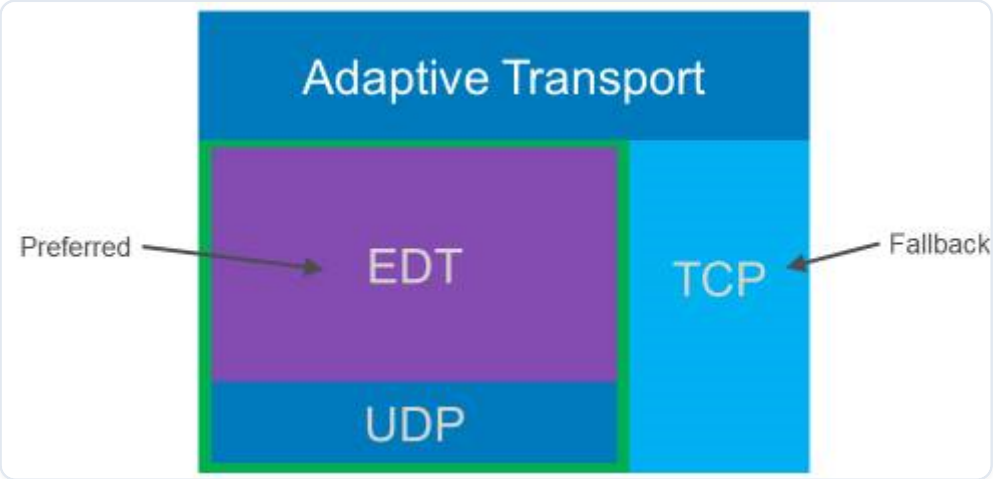


アダプティブトランスポートが**Preferred**に設定されている場合、EDTがプライマリトランスポートプロトコルとして使用され、TCPがフォールバックに使用されます。デフォルトでは、アダプティブトランスポートは**Preferred**に設定されています。テスト目的でアダプティブトランスポートを**Diagnostic mode**に設定できます。このモードではEDTのみが許可され、TCPへのフォールバックは無効になります。

Windows、Mac、およびiOS向けのCitrix Workspace™ appでは、初期接続、セッションの信頼性の再接続、および自動クライアント再接続中に、EDTとTCP接続が並行して試行されます。これに

より、基盤となるUDPトランスポートが利用できない場合にTCPを使用する必要があるときの接続時間が短縮されます。アダプティブトランスポートが**Preferred**に設定されており、TCPを使用して接続が確立された場合、アダプティブトランスポートは5分ごとにEDTへの切り替えを試行し続けます。

LinuxおよびAndroid向けのCitrix Workspace appでは、まずEDT接続が試行されます。接続が失敗した場合、Citrix Workspace appはEDT要求がタイムアウトした後、TCPを使用して接続を試みます。



システム要件

アダプティブトランスポートとEDTを使用するための要件は次のとおりです。

- コントロールプレーン
  - シトリックス DaaS（旧称：シトリックス バーチャル アプリケーションズ アンド デスクトップ サービス）
  - シトリックス バーチャル アプリケーションズ アンド デスクトップ 1912以降
- 仮想配信エージェント
  - バージョン1912以降 (2203以降を推奨)
  - Citrix Gateway ServiceでEDTを使用するには、バージョン2012が最低限必要です。
- StoreFront™
  - バージョン3.12.x
  - バージョン1912.0.x
- Citrix Workspace アプリ

  - Windows: バージョン 2105 以降
  - Linux: バージョン 2109 以降
  - Mac: バージョン 2108 以降
  - iOS: Apple App Storeで入手可能な最新バージョン
  - Android: Google Playで入手可能な最新バージョン
- Citrix ゲートウェイ (ADC)
  - 13.1.17.42 以降 (推奨)
  - 13.0.52.24 以降
  - 12.1.56.22 以降
- ファイアウォール（VDAの観点から）
  - UDP 1494 インバウンド – セッションの信頼性が無効になっている場合
  - UDP 2598 インバウンド – セッションの信頼性が有効になっている場合
  - UDP 443 インバウンド – ICA暗号化（DTLS）のためにVDA SSLが有効になっている場合
  - UDP 443 アウトバウンド – Citrix Gateway Serviceを使用している場合。詳しくは、Citrix Gateway serviceのドキュメントを参照してください。

考慮事項

- EDT MTU Discovery を使用し、Citrix Gateway および Citrix Gateway service で EDT を使用するには、セッションの信頼性を有効にします。
- EDT MTU が適切に設定され、フラグメンテーションを回避していることを確認してください。そうしないと、パフォーマンスに影響が出たり、状況によってはセッションが起動に失敗したりする可能性があります。詳細については、EDT MTU Discover セクションを参照してください。
- Citrix Gateway service で EDT を使用するための要件と考慮事項の詳細については、HDX Adaptive Transport with EDT support for Citrix Gateway service を参照してください。
- EDT をサポートするための Citrix Gateway の構成の詳細については、Configure Citrix Gateway to support Enlightened Data Transport and HDX Insight を参照してください。
- IPv6 は現在サポートされていません。

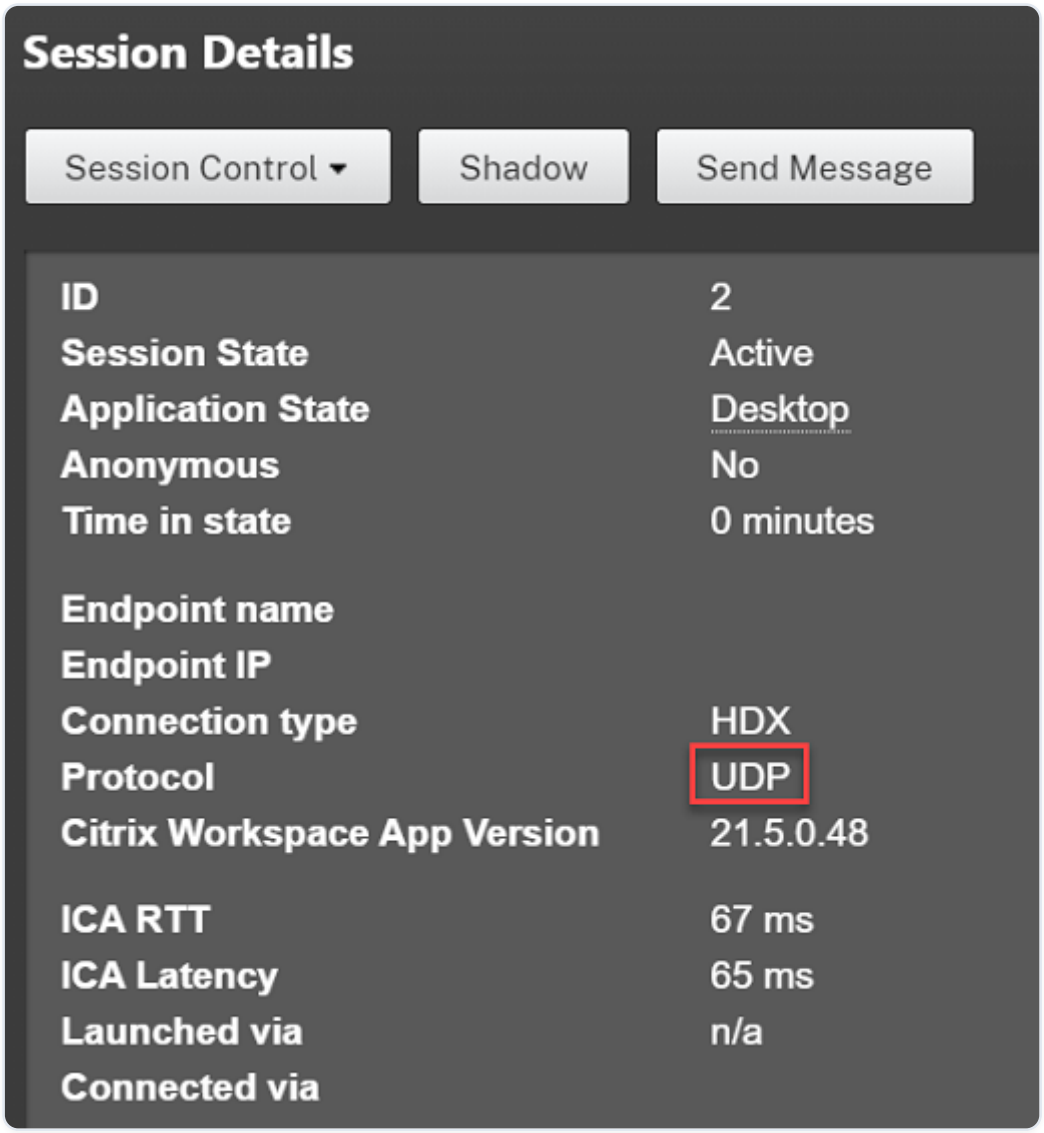
構成

アダプティブトランスポートはデフォルトで有効になっています。CitrixポリシーのHDX™ Adaptive Transport設定を使用して、次のオプションを構成できます。

- **優先**。これがデフォルト設定です。アダプティブトランスポートが有効になり、EDT を優先トランスポートプロトコルとして使用し、TCP へのフォールバックが行われます。
- **診断モード**。アダプティブトランスポートが有効になり、EDT の使用が強制されます。TCP へのフォールバックは無効になります。この設定は、テストとトラブルシューティングのみに推奨されます。
- **オフ**。アダプティブトランスポートは無効になり、トランスポートには TCP のみが使用されます。

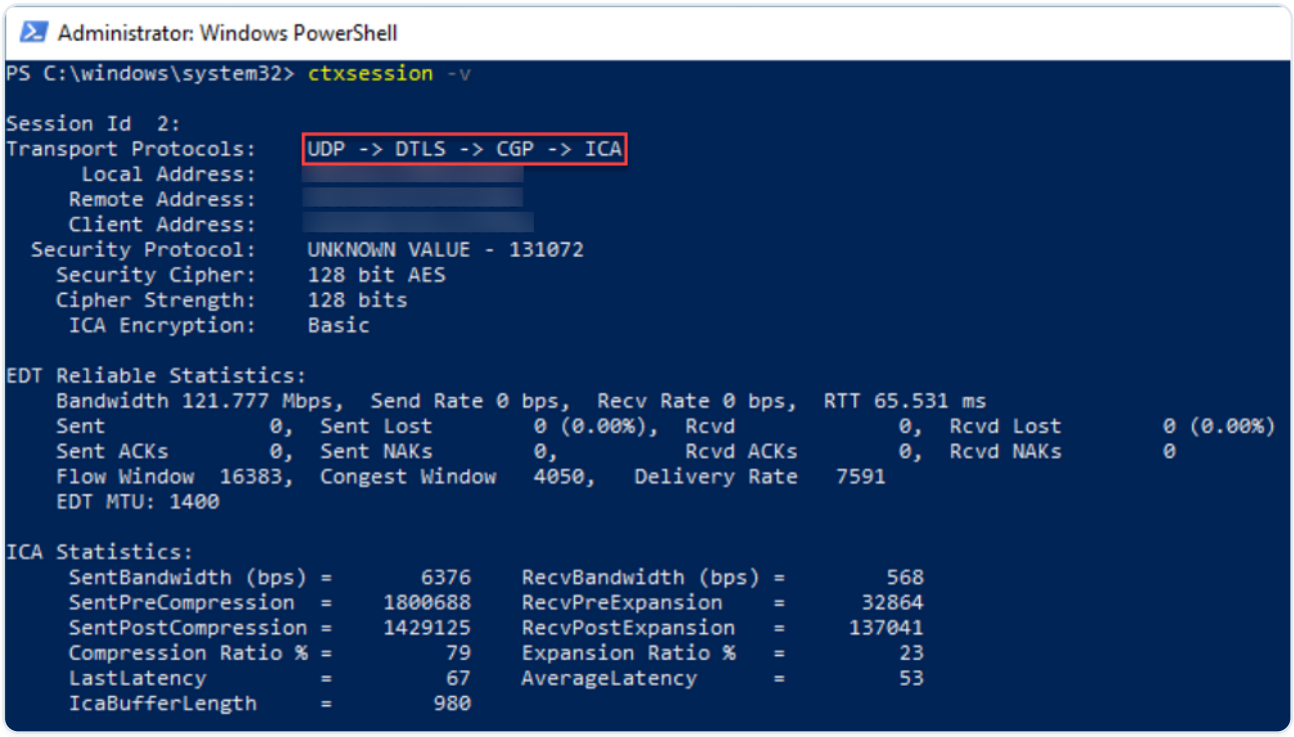
セッションのトランスポートプロトコルとしてEDTが使用されていることを確認するには、DirectorまたはVDA上のCtxSession.exeコマンドラインユーティリティを使用します。

Directorでセッションを検索し、**詳細**を選択します。**接続の種類**が**HDX**で**プロトコル**が**UDP**の場合、EDTがセッションのトランスポートプロトコルとして使用されています。**接続の種類**が**RDP**の場合、ICAは使用されておらず、**プロトコル**はN/Aと表示されます。詳細については、「セッションの監視」を参照してください。



CtxSession.exeユーティリティを使用するには、セッション内でコマンドプロンプトまたはPowerShellを起動し、`ctxsession.exe`を実行します。詳細な統計情報を表示するには、`ctxsession.exe -v`を実行します。EDTが使用されている場合、トランスポートプロトコルは次のいずれかを表示します。

- **UDP > ICA**（セッションの信頼性が無効）
- **UDP > CGP > ICA** (セッションの信頼性が有効)
- **UDP > DTLS > CGP > ICA** (ICAはDTLSでエンドツーエンド暗号化されています)



EDT MTU検出

MTU検出により、EDTはセッション確立時に最大転送単位（MTU）を自動的に決定できます。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットの断片化を防ぎます。

重要:

- MTU検出を機能させるには、セッションの信頼性を有効にする必要があります。
- マルチストリームICAでのMTU検出は、VDAバージョン2209以降で利用可能です。

VDAでEDT MTU検出を制御するには

MTU検出はデフォルトで有効になっています。この機能を無効にするには、**EDT MTU Discovery**レジストリ値を削除し、VDAを再起動します。詳細については、レジストリで管理されるHDX機能のリストにあるEDT MTU Discovery設定を参照してください。

警告：

レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使

> 用によって生じた問題が解決されることを保証できません。レジストリエディターは、ご自身の責任において使用してください。編集する前に、必ずレジストリをバックアップしてください。

システム要件

- シトリックス バーチャル デリバリー エージェント (VDA) 2003
- Windows向けCitrix Workspaceアプリ 2002
- セッションの信頼性が有効になっていること。セッションの信頼性について詳しくは、「セッションの信頼性ポリシー設定」を参照してください。

既知の問題

アダプティブトランスポートとEDTには、次の問題があります。

- パケットの断片化により、パフォーマンスが低下したり、セッションの起動に失敗したりする可能性があります。これを回避するには、EDT MTUを調整できます。MTU検出を使用するか、「CTX231821」に記載されている回避策を使用してください。
- MTU検出が有効になっている場合、Windowsクライアントからセッションを起動すると、グレースクリーンまたはブラックスクリーンが表示されることがあります。この問題に対処するには、Windows向けWorkspaceアプリ2105以降、またはWindows向けWorkspaceアプリ1912 CU4以降にアップグレードしてください。
- Citrix GatewayまたはCitrix Gateway Service経由で接続する場合、LinuxおよびAndroidクライアントでTCPへのフォールバックが失敗することがあります。これは、クライアントとGateway間でEDTネゴシエーションが成功し、GatewayとVDA間でEDTネゴシエーションが失敗した場合に発生します。この問題に対処するには、Linux向けWorkspaceアプリ2104以降、およびAndroid向けWorkspaceアプリ21.5以降にアップグレードしてください。
- 非対称ネットワークパスでは、Citrix GatewayまたはCitrix Gateway Serviceを経由しない接続でMTU検出が失敗する可能性があります。この問題に対処するには、VDAバージョン2103以降にアップグレードしてください。
- Citrix Gatewayを使用している場合、非対称ネットワークパスが原因でMTU検出が失敗することがあります。これは、Gatewayの問題により、EDTパケットヘッダーのDon't Fragment（DF）ビットが伝播されないために発生します。この問題の修正は、ファームウェアリリース13.1ビルド17.42以降で利用可能です。修正を有効にする方法の詳細については、「Citrix Gatewayのドキュメント」を参照してください。

- DS-Liteネットワーク経由で接続するユーザーの場合、MTU Discoveryが失敗する可能性があります。一部のモデムでは、パケット処理が有効になっている場合にDFビットを尊重せず、MTU Discoveryがフラグメンテーションを検出できないことがあります。このような状況では、以下のオプションが利用可能です。
  - ユーザーのモデムでパケット処理を無効にする。
  - MTU検出を無効にし、CTX231821に記載されているようにハードコードされたMTUを使用します。
  - Adaptive Transportを無効にして、セッションがTCPを使用するように強制します。一部のユーザーのみが影響を受ける場合は、他のユーザーがEDTを引き続き使用できるように、クライアント側で無効にすることを検討してください。

トラブルシューティング

Adaptive TransportとEDTのトラブルシューティングには、以下をお勧めします。

1. (/ja-jp/citrix-virtual-apps-desktops/2311/technical-overview/hdx/adaptive-transport.html#system-requirements)、(/ja-jp/citrix-virtual-apps-desktops/2311/technical-overview/hdx/adaptive-transport.html#considerations)、および(/ja-jp/citrix-virtual-apps-desktops/2311/technical-overview/hdx/adaptive-transport.html#known-issues)を徹底的に確認し、検証します。
2. StudioまたはGPOに、目的の**HDX Adaptive Transport**設定を上書きするCitrixポリシーがないか確認します。
3. クライアントに、目的のHDX Adaptive Transport設定を上書きする設定がないか確認します。これは、GPO設定、オプションのWorkspaceアプリ管理テンプレートを使用して構成された設定、またはレジストリまたはクライアントの構成ファイルでの**HDXoverUDP**設定の手動構成である可能性があります。
4. マルチセッションVDAマシンで、UDPリスナーがアクティブであることを確認します。VDAマシンでコマンドプロンプトを開き、`netstat -a -p udp`を実行します。詳しくは、HDX Enlightened Data Transport プロトコルを確認する方法を参照してください。
5. Citrix Gatewayをバイパスして内部で直接セッションを起動し、使用中のプロトコルを確認します。セッションがEDTを使用している場合、VDAはCitrix Gatewayを介した外部接続にEDTを使用する準備ができています。
6. EDTが直接内部接続では機能するが、Citrix Gatewayを介するセッションでは機能しない場合：
   - セッションの信頼性が有効になっていることを確認する
   - GatewayでDTLSが有効になっていることを確認する

7. ネットワークファイアウォールとVDAマシンで実行されているファイアウォールの両方で、適切なファイアウォールルールが構成されていることを確認します。
8. ユーザーの接続に非標準のMTUが必要かどうかを確認します。実効MTUが1500バイト未満の接続では、EDTパケットの断片化が発生し、パフォーマンスに影響を与えたり、セッション起動の失敗を引き起こしたりする可能性があります。この問題は、VPN、一部のWi-Fiアクセスポイント、および4Gや5Gなどのモバイルネットワークを使用している場合に一般的です。この問題の対処方法については、「(/ja-jp/citrix-virtual-apps-desktops/2311/technical-overview/hdx/adaptive-transport.html#edt-mtu-discovery)」セクションを参照してください。

Citrix SD-WAN™ との相互運用性

Citrix SD-WAN WAN最適化 (WANOP) は、URLベースのビデオキャッシュを含むセッション間トークン化圧縮 (データ重複排除) を提供し、大幅な帯域幅削減を実現します。この削減は、オフィス拠点で2人以上のユーザーが同じクライアント取得ビデオを視聴したり、同じファイルやドキュメントの大部分を転送または印刷したりする場合に発生します。さらに、WANOPは、ICAデータ削減および印刷ジョブ圧縮のプロセスを支社アプライアンスで実行することにより、VDAサーバーのCPUオフロードを提供し、Citrix Virtual Apps and Desktopsサーバーの拡張性を向上させます。

現在、SD-WAN WANOPはEDTをサポートしていません。ただし、SD-WAN WANOPを使用している場合でも、アダプティブトランスポートを無効にする必要はありません。ユーザーがWANOPが有効なSD-WANを介してセッションを起動すると、セッションは自動的にトランスポートプロトコルとしてTCPを使用するように設定されます。WANOP以外のセッションは、可能な限りEDTを引き続き使用します。

HDX™ Direct (プレビュー)

Citrixが提供するリソースにアクセスする場合、HDX Directにより、直接通信が可能な場合、内部および外部のクライアントデバイスの両方がセッションホストと安全な直接接続を確立できます。

> **重要:**
>
> HDX Directは現在プレビュー版です。この機能はサポートなしで提供されており、本番環境での使用はまだ推奨されていません。フィードバックの送信または問題の報告には、こちらのフォームをご利用ください。

システム要件

HDX Directを使用するためのシステム要件は以下のとおりです。

- コントロールプレーン
  - シトリックス DaaS™
  - シトリックス Virtual Apps and Desktops™ 2311 以降
- バーチャル デリバリー エージェント (VDA)
  - Windows: バージョン 2311 以降
- Workspaceアプリ
  - Windows: バージョン 2311 以降
- アクセス層
  - シトリックス Workspace™ と シトリックス Gateway Service
  - NetScaler® Gateway を使用した Citrix Workspace
- その他
  - 外部からの直接接続の場合、アダプティブトランスポートを有効にする必要があります

ネットワーク要件

HDX Directを使用するためのネットワーク要件は以下のとおりです。

セッションホスト

セッションホストにWindows Defender ファイアウォールなどのファイアウォールがある場合、内部接続のために以下のインバウンドトラフィックを許可する必要があります。

説明	送信元	プロトコル	ポート
直接内部接続	クライアント	TCP	443
直接内部接続	クライアント	UDP	443

> 注:

> VDAインストーラーは、適切な受信規則をWindows Defender ファイアウォールに追加します。別のファイアウォールを使用する場合は、上記の規則を追加する必要があります。

クライアントネットワーク

以下の表は、内部および外部ユーザー向けのクライアントネットワークについて説明しています。

内部ユーザー

説明	プロトコル	ソース	ソースポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
STUN (外部ユーザーのみ)	UDP	クライアントネットワーク	1024–65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	クライアントネットワーク	1024–65535	データセンターのパブリックIPアドレス	1024–65535

データセンターネットワーク

以下の表は、内部ユーザーと外部ユーザー向けのデータセンターネットワークについて説明しています。

内部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	送信元	送信元ポート	宛先	宛先ポート
STUN (外部ユーザーのみ)	UDP	VDAネットワーク	1024–65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	DMZ / 内部ネットワーク	1024–65535	VDAネットワーク	55000–55250
外部ユーザー接続	UDP	VDAネットワーク	55000–55250	クライアントのパブリックIP	1024–65535

注:

VDAとWorkspaceアプリの両方が、以下のサーバーに同じ順序でSTUNリクエストを送信しようとします。

- stunserver.stunprotocol.org:3478
- employees.org:3478
- stun.l.google.com:19302

> **HDX Direct port range**ポリシー設定を使用して外部ユーザー接続のデフォルトポート範囲を変更した場合、対応するファイアウォールルールはカスタムポート範囲と一致する必要があります。

構成

HDX Directはデフォルトで無効になっています。この機能は、CitrixポリシーのHDX Direct設定を使用して構成できます。

- **HDX Direct**：機能を有効または無効にする。
- **HDX Direct mode**：**HDX Direct**が内部クライアントのみに利用可能か、内部クライアントと外部クライアントの両方に利用可能かを決定します。
- **HDX Direct port range**：VDAが外部クライアントからの接続に使用するポート範囲を定義します。

考慮事項

HDX Directを使用する際の考慮事項は次のとおりです。

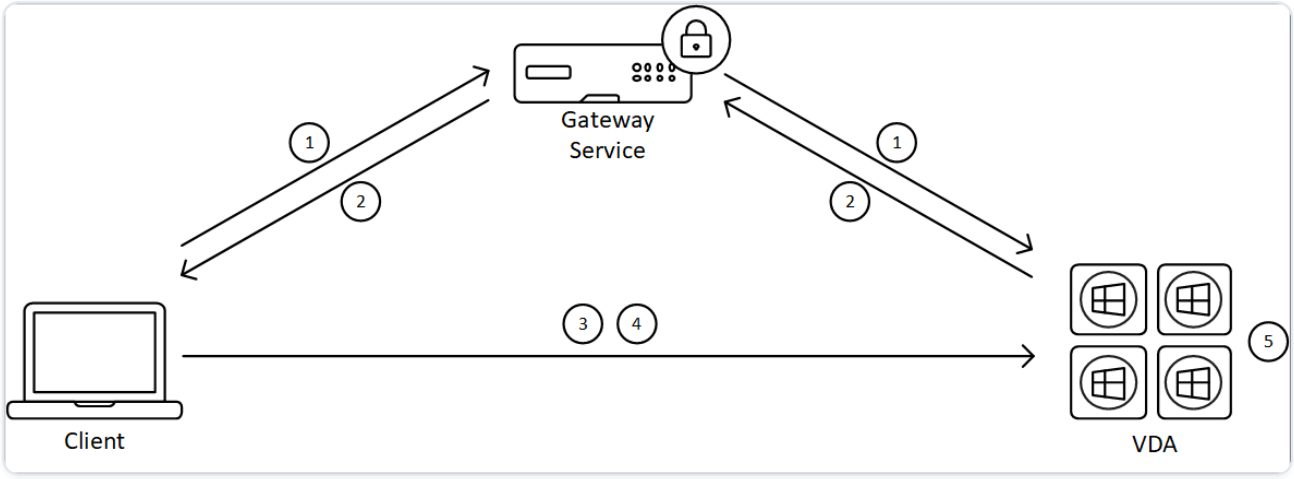
- 外部ユーザー向けのHDX Directは、トランスポートプロトコルとしてEDT (UDP) を使用する場合にのみ利用可能です。したがって、**Adaptive Transport**を有効にする必要があります。
- **HDX Insight**を使用している場合、**HDX Direct**を使用すると、セッションがNetScaler Gatewayを介してプロキシされなくなるため、HDX Insightのデータ収集が妨げられることに注意してください。
- 仮想アプリおよびデスクトップに非永続マシンを使用する場合、Citrixは、各マシンが独自の証明書を生成するように、マスター/テンプレートイメージではなくセッションホストで**HDX Direct**を有効にすることを推奨します。
- HDX Directで独自の証明書を使用することは現在サポートされていません。

動作の仕組み

HDX Directを使用すると、直接通信が可能な場合、クライアントはセッションホストへの直接接続を確立できます。HDX Directを使用して直接接続が行われる場合、ネットワークレベルの暗号化 (TLS/DTLS) で直接接続を保護するために自己署名証明書が使用されます。

内部ユーザー

次の図は、内部ユーザーのHDX Direct接続プロセスの概要を示しています。

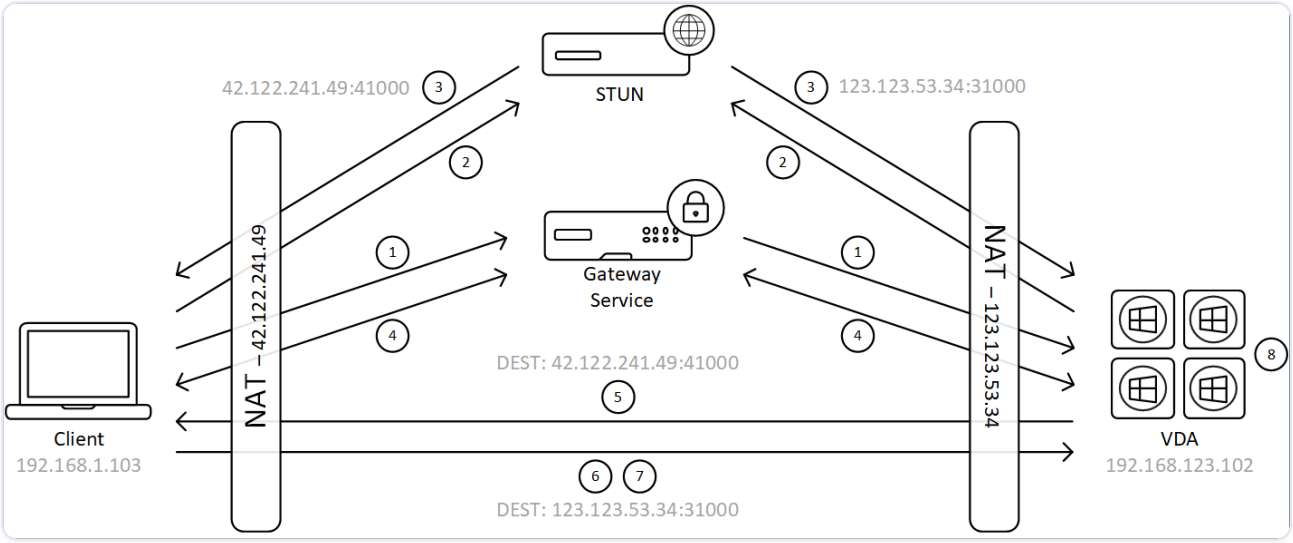


1. クライアントはGateway Serviceを介してHDXセッションを確立します。
2. 接続が成功すると、VDAはHDX接続を介して、VDAマシンのFQDN、そのIPアドレスのリスト、およびVDAマシンの証明書をクライアントに送信します。
3. クライアントはIPアドレスをプローブし、VDAに直接到達できるかどうかを確認します。
4. クライアントが共有されたいずれかのIPアドレスでVDAに直接到達できる場合、クライアントはVDAとの直接接続を確立し、ステップ(2)で交換された証明書と一致する証明書を使用して(D)TLSで保護します。
5. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

> **注:**
>
> 上記のステップ2で接続を確立した後、セッションはアクティブになります。その後のステップは、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅らせたり、妨げたりすることはありません。その後のステップのいずれかが失敗した場合でも、Gatewayを介した接続はユーザーのセッションを中断することなく維持されます。

外部ユーザー

次の図は、外部ユーザー向けのHDX Direct接続プロセスの概要を示しています。



1. クライアントはGateway Serviceを介してHDXセッションを確立します。
2. 接続が成功すると、クライアントとVDAの両方がSTUNリクエストを送信して、それぞれのパブリックIPアドレスとポートを検出します。
3. STUNサーバーは、クライアントとVDAにそれぞれのパブリックIPアドレスとポートで応答します。
4. HDX接続を介して、クライアントとVDAはそれぞれのパブリックIPアドレスとUDPポートを交換し、VDAはその証明書をクライアントに送信します。
5. VDAはクライアントのパブリックIPアドレスとUDPポートにUDPパケットを送信します。クライアントはVDAのパブリックIPアドレスとUDPポートにUDPパケットを送信します。
6. VDAからのメッセージを受信すると、クライアントはセキュアな接続要求で応答します。
7. DTLSハンドシェイク中に、クライアントは証明書がステップ(4)で交換された証明書と一致することを確認します。検証後、クライアントは認証トークンを送信します。これでセキュアな直接接続が確立されます。
8. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

注：

上記のステップ2で接続を確立した後、セッションはアクティブになります。その後のステップは、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅らせたり、妨げたりすることはありません。その後のステップのいずれかが失敗した場合でも、Gatewayを介した接続はユーザーのセッションを中断することなく維持されます。

証明書管理

セッションホスト

VDA マシン上の次の 2 つのサービスは証明書の作成と管理を処理します。どちらもマシンの起動時に自動的に実行されるように設定されています。

- Citrix ClxMtp Service: CA 証明書キーの生成とローテーションを担当します。
- Citrix Certificate Manager Service: 自己署名ルート CA 証明書とマシン証明書の生成および管理を担当します。

次の手順は証明書管理プロセスを示しています。

1. サービスはマシンの起動時に開始します。
2. まだキーが作成されていない場合、`Citrix ClxMtp Service`がキーを作成します。
3. Citrix Certificate Manager Serviceは、**HDX Direct**が有効になっているかを確認します。有効になっていない場合、サービスは自身を停止します。
4. **HDX Direct**が有効になっている場合、Citrix Certificate Manager Serviceは自己署名ルートCA証明書が存在するかを確認します。存在しない場合、自己署名ルート証明書が作成されます。
5. ルートCA証明書が利用可能になると、Citrix Certificate Manager Serviceは自己署名マシン証明書が存在するかを確認します。存在しない場合、サービスはキーを生成し、マシンのFQDNを使用して新しい証明書を作成します。
6. Citrix Certificate Manager Serviceによって作成された既存のマシン証明書があり、そのサブジェクト名がマシンのFQDNと一致しない場合、新しい証明書が生成されます。

> **注:**
>
> Citrix Certificate Manager Serviceは、2048ビットキーを利用するRSA証明書を生成します。

クライアントデバイス

安全な**HDX Direct**接続を正常に確立するには、クライアントはセッションを保護するために使用される証明書を信頼する必要があります。これを容易にするため、クライアントはICA®ファイル（Workspaceによって提供）を介してセッション用のCA証明書を受け取るため、CA証明書をクライアントデバイスの証明書ストアに配布する必要はありません。

NAT互換性

外部ユーザーデバイスとセッションホスト間の直接接続を確立するために、HDX™ Directは、NATトラバーサルのためにホールパンチングを、クライアントデバイスとセッションホストのパブリックIPアドレスとポートマッピングの交換を容易にするためにSTUNを利用します。これは、VoIP、ユニファイドコミュニケーション、P2Pソリューションの仕組みと同様です。

ファイアウォールやその他のネットワークコンポーネントが、STUNリクエストとHDXセッションのUDPトラフィックを許可するように構成されている限り、外部ユーザー向けのHDX Directは機能すると予想されます。ただし、ユーザーとセッションホストのネットワークのNATタイプが互換性のない組み合わせになり、HDX Directが失敗する特定のシナリオがあります。

検証

STUNTMANのSTUNクライアントユーティリティを使用して、クライアントとセッションホストのNATタイプを検証できます。

1. stunprotocol.orgからターゲットプラットフォームに適したパッケージをダウンロードし、内容を抽出します。
2. ターミナルプロンプトを開き、内容が抽出されたディレクトリに移動します。
3. 次のコマンドを実行します: `.\stunclient.exe stunserver.stunprotocol.org --mode behavior`
4. 出力を記録します。

バインディングテストと動作テストが成功した場合、**バインディングテスト**と**動作テスト**の両方が成功を報告し、NAT動作が指定されます。



テストが失敗した場合、**バインディングテスト**と**動作テスト**の両方が失敗を報告します。



クライアントとセッションホストの両方のテスト結果に基づいて、外部ユーザー向けのHDX Directが機能するかどうかを判断するには、次の表を参照してください。

クライアントデバイス	セッションホスト	動作が期待されますか？
エンドポイント独立マッピング	エンドポイント独立マッピング	はい
エンドポイント独立マッピング	エンドポイント依存マッピング	はい
エンドポイント依存マッピング	エンドポイント独立マッピング	はい
エンドポイント依存マッピング	エンドポイント依存マッピング	いいえ
失敗	任意のNATタイプ	いいえ
任意のNATタイプ	失敗	いいえ
失敗	失敗	いいえ

トラブルシューティング

HDX Direct が直接接続を正常に確立したことを確認するには、VDA マシンで `CtxSession.exe` ユーティリティを使用します。

`CtxSession.exe` ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を起動し、`ctxsession.exe -v` を実行します。**HDX Direct** 接続が正常に確立されている場合、**HDX Direct Status** は `Connected` となります。

HDX Direct のトラブルシューティング(/en-us/citrix-virtual-apps-desktops/2311/media/hdx-direct-troubleshooting.png)

セッションホストのイベントログで、HDX™ Direct 接続が正常に確立されたか、または失敗したかに関する情報を確認することもできます。詳細については、**イベントログ**のセクションを参照してください。

> 注:
>
> 環境およびセッションホストで利用可能な IP アドレスの数によっては、HDX Direct 接続が確立されるまでに最大 5 分かかる場合があります。

HDX Direct が直接接続の確立に失敗した場合

HDX Direct が直接接続の確立に失敗している場合は、次の手順を確認してください。

1. 使用している VDA バージョンと Workspace app バージョンが、システム要件に従ってこの機能をサポートしていることを確認してください。
2. HDX Direct を有効にするポリシーが VDA に適用されており、この機能を無効にする優先度の高い他のポリシーがないことを確認してください。
3. 目的の HDX Direct モードを設定するポリシーが VDA に適用されており、この構成を上書きする優先度の高い他のポリシーがないことを確認してください。
4. Citrix ClxMtp Service がセッションホストで実行されていることを確認してください。
5. Citrix Certificate Manager Service がセッションホストで実行されていることを確認してください。実行されていない場合は、手動で開始してみてください。HDX Direct が無効になっている場合、このサービスは自動的に停止します。
6. セッションホストに自己署名 Root CA 証明書があるか確認してください。
    a. 発行先: `CA-<hostname>` (例: CA-FTLW11-001)
    b. 発行元: `CA-<hostname>` (例: CA-FTLW11-001)
    c. 発行者の詳細: 組織はCitrix Systems, Inc.です。
7. セッションホストに自己署名サーバー証明書があるか確認します:
    a. 発行先: `<host FQDN>` (例: FTLW11-001.ctxlab.net)
    b. 発行元: `CA-<hostname>` (例: CA-FTLW11-001)
    c. 発行者の詳細: 組織はCitrix Systems, Inc.です。
8. 証明書がない場合は、Citrixテクニカルサポートにお問い合わせください。
9. 証明書が存在する場合:
    a. セッションホストでCitrix Certificate Manager Serviceを停止します。
    b. 自己署名ルートCA証明書と自己署名サーバー証明書の両方を削除します。
    c. セッションホストでCitrix Certificate Manager Serviceを開始します。サービスは開始されると新しい証明書を作成します。
10. 内部ユーザーの場合:

a. セッションホストのファイアウォールが、HDX over EDTおよびHDX over TCPのそれぞれについて、UDP 443またはTCP 443のインバウンドトラフィックをブロックしていないことを確認します。

b. ネットワークファイアウォールが、クライアントネットワークとセッションホストネットワーク間のUDP 443およびTCP 443のトラフィックをブロックしていないことを確認します。

11. 外部ユーザーの場合：

a. クライアントとセッションホストのNATタイプを確認し、その組み合わせが機能すると予想されることを確認してください。詳細については、「NAT互換性」セクションを参照してください。

b. クライアントまたはセッションホストのいずれかでNATテストが失敗した場合：

i. システムでファイアウォールが実行されている場合は、UDP 3478での送信トラフィックをブロックしていないことを確認してください。

ii. ネットワークファイアウォールがUDP 3478での送信トラフィックをブロックしていないことを確認してください。

iii. ファイアウォールがSTUNサーバーの応答をブロックしていないことを確認してください。

c. ネットワークファイアウォールに、必要なすべてのトラフィックを許可するための適切なルールが構成されていることを確認してください。詳細については、「ネットワーク要件」セクションを参照してください。

d. HDX Directポート範囲ポリシー設定を使用してデフォルトのポート範囲を変更する場合は、ファイアウォールルールがカスタムポート範囲に設定されていることを確認してください。

イベントログ

以下のイベントがVDAマシンのイベントログに記録されます：

ログ	ID	送信元	レベル	説明
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/ Operational	1	HDX ダイレクト	情報	内部ユーザー `<username>` のHDX Direct接続が確立されました。

ログ	ID	送信元	レベル	説明
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/ Operational	2	HDX ダイレクト	情報	外部ユーザー `<username>` のHDX Direct接続が確立されました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/ Operational	3	HDX ダイレクト	情報	ユーザー `<username>` のHDX Direct接続に失敗しました。

既知の問題

HDX Direct が有効になっているマシンでVDAのインプレースアップグレードを実行すると、HDX Directが動作しなくなることがあります。 この問題を解決するには、次の手順を実行します。

1. セッションホストでCitrix Certificate Manager Serviceを停止します。
2. 自己署名ルートCA証明書と自己署名サーバー証明書を削除します。
3. レジストリを開きます。
4. `HKLM\Software\Citrix\HDX-Direct` キーを削除します。
5. `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd` にアクセスします。
6. **SSLEnabled** の値を `0` に設定します。
7. **SSLThumbprint** の値の内容を削除します。
8. **Citrix Certificate Manager Service** を開始します。

デバイス

HDX™は、あらゆるデバイスで、あらゆる場所で、高精細なユーザーエクスペリエンスを提供します。「デバイス」セクションの記事では、以下のデバイスについて説明します。

- クライアントドライブマッピング
- 汎用USBデバイス
- モバイルおよびタッチスクリーンデバイス
- シリアルデバイス
- 特殊キーボード
- TWAINデバイス
- Webカメラ
- WIAデバイス

最適化されたUSBデバイスと汎用USBデバイス

最適化されたUSBデバイスとは、Citrix Workspace™アプリが特定のサポートを提供するデバイスです。たとえば、HDX Multimedia仮想チャネルを使用してWebカメラをリダイレクトする機能などです。汎用デバイスとは、Citrix Workspaceアプリで特定のサポートがないUSBデバイスです。

デフォルトでは、汎用USBリダイレクトは、汎用モードに設定しない限り、最適化された仮想チャネルサポートを持つUSBデバイスをリダイレクトできません。

一般的に、USBデバイスは汎用モードよりも最適化モードの方がパフォーマンスが向上します。ただし、最適化モードではUSBデバイスが完全な機能を持たない場合があります。その機能に完全にアクセスするには、汎用モードに切り替える必要があるかもしれません。

USB大容量記憶装置の場合、Citrix®ポリシーによって制御されるクライアントドライブマッピングまたは汎用USBリダイレクト、あるいはその両方を使用できます。主な違いは次のとおりです。

汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっており、セッション開始前または開始後にマスストレージデバイスが挿入された場合、クライアントドライブマッピングを使用してリダイレクトされます。

これらの条件が満たされている場合、マスストレージデバイスは汎用USBリダイレクトを使用してリダイレクトされます。

- 汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっている。
- デバイスが自動リダイレクト用に構成されている。
- マスストレージデバイスがセッション開始前または開始後に挿入される。

詳細については、`<http://support.citrix.com/article/CTX123015>`を参照してください。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセス設定可能	はい	いいえ
暗号化されたデバイスアクセス	はい、仮想セッションでデバイスにアクセスする前に暗号化が解除されている場合。	Citrix Virtual Desktops™ に限定されます

クライアントドライブマッピング

クライアントドライブマッピングにより、クライアントエンドポイント上のストレージドライブがCitrix HDX™セッション内で利用可能になり、ファイルやフォルダーをクライアントからセッションホストへ、またはその逆に転送できるようになります。この機能は、読み取りおよび書き込みの両方の権限でデフォルトで有効になっています。マップされたクライアントデバイス上のファイルやフォルダーをユーザーが追加または変更できないようにするには、**読み取り専用クライアントドライブアクセス**ポリシー設定を有効にします。この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が**許可**に設定されており、かつポリシーにも追加されていることを確認してください。

セキュリティ上の予防措置として、エンドポイントドライブはデフォルトで実行権限なしでマップされます。ユーザーがマップされたクライアントドライブから実行可能ファイルを直接実行できるようにするには、セッションホストで**ExecuteFromMappedDrive**レジストリ値を編集します。詳細については、**レジストリで管理されるHDX機能**セクションのマップされたクライアントドライブを参照してください。

要件

CDMを使用するための要件は次のとおりです。

Citrixコントロールプレーン

- シトリックス Virtual Apps and Desktops™ 1912以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows Server 2016 以降のバージョン
  - Linux: Linux VDAのシステム要件を参照してください
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 以降のバージョンであること
  - Linux: Linux VDAのドキュメントを参照してください。

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux: Workspace app for Linuxのシステム要件を参照してください。

関連ポリシー

CDM設定については、ポリシー設定リファレンスセクションを参照してください。

ダブルホップシナリオ

CDMはダブルホップシナリオでサポートされています。デフォルトでは、クライアントエンドポイントのドライブはセカンドホップセッションにマップされ、ファーストホップのドライブは利用できません。ただし、クライアントエンドポイントのドライブの代わりに、ファーストホップのドライブがセカンドホップセッションにマップされるように設定することも可能です。

この機能を構成するには、以下のレジストリ値を編集します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive\
- 値の名前: NativeDriveMapping
- 値の型: REG_SZ
- 値のデータ:
  - True - ファーストホップセッションのドライブをセカンドホップセッションにマップします
  - 無効 - セカンドホップセッションでクライアントエンドポイントのドライブをマップします

> **注:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような重大な問題を引き起こす可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターの使用は、お客様ご自身の責任において行ってください。編集する前に、必ずレジストリをバックアップしてください。

汎用USBデバイス

HDX™テクノロジーは、ほとんどの一般的なUSBデバイスに対して**最適化されたサポート**を提供します。これらのデバイスには以下が含まれます:

- モニター
- マウス
- キーボード
- ボイス・オーバー・インターネット・プロトコル電話
- ヘッドセット
- Webカメラ
- スキャナー
- カメラ
- プリンタ
- ドライブ

- スマートカードリーダー
- ペンタブレット
- 署名パッド

最適化されたサポートは、WAN経由でパフォーマンスと帯域幅の効率を向上させ、ユーザーエクスペリエンスを改善します。最適化されたサポートは、特に高遅延またはセキュリティに敏感な環境において、通常は最良の選択肢です。

HDXテクノロジーは、最適化されたサポートがない、または不適切な特殊デバイス向けに**汎用USBリダイレクト**を提供します。汎用USBリダイレクトの詳細については、「汎用USBリダイレクト」を参照してください。

USBデバイスとCitrix Workspaceアプリ for Windowsの詳細については、「複合USBデバイスリダイレクトの構成」および「USBサポートの構成」を参照してください。

USB診断ツール

`CtxUsbDiagnostics.exe` は、Citrix管理者がクライアントで発生するUSBデバイスのリダイレクトの問題を迅速に診断し、解決するのに役立つVDA上のコマンドラインツールです。このユーティリティツールは、HDXセッション内でリダイレクトに失敗するクライアントに接続されたUSBデバイスに関連する構成の問題を解決するために必要な重要な情報を収集します。

```
> **Note :**

>

> Running Command Prompt or Powershell as an administrator is required to
ensure the tool has the necessary permissions to perform system-level
operations.
```

要件

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows 11 21H2以降
  - Windows Server 2016年以降
- VDA

- Windows版: Citrix Virtual Apps and Desktops™ バージョン2311 以降

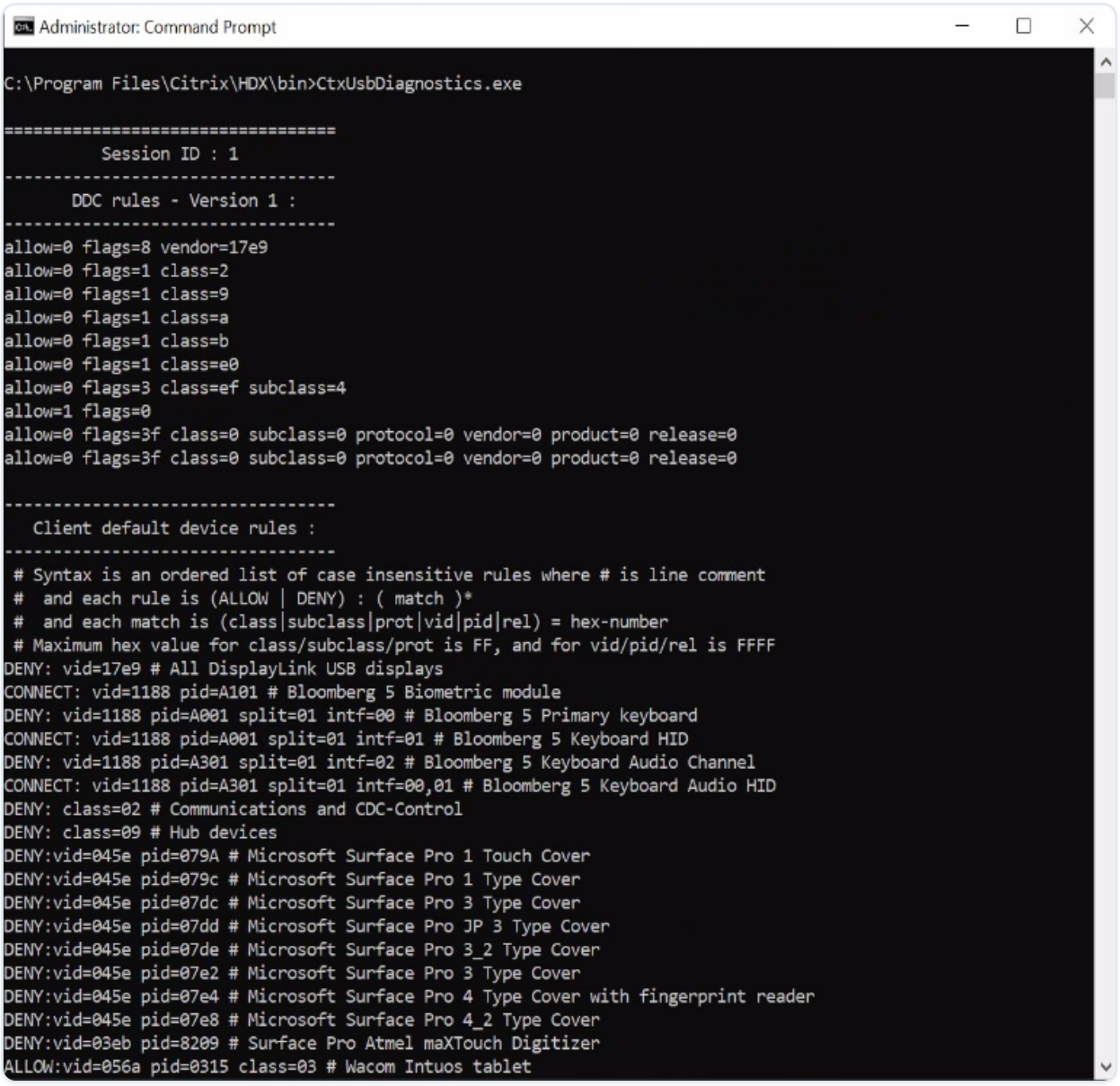
クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
- ワークスペースアプリ
  - Windows: バージョン 2311 以降

ツールは何をしますか?

このツールは現在、以下を提供します。

- VDAデバイスポリシー（Studioで設定されたデバイスルール）
- クライアントデバイスとクライアントデバイスポリシー（デバイスルール）
- デバイスのリスト、そのリダイレクト状態、および許可または拒否された理由



> **注記：**
>
> 管理者は、すべてのアクティブなセッションのデバイス情報を確認できます。

表示される情報

- **DDCルール - バージョン1/2**
  - DDCルールは、Studioにおけるレガシーな「**クライアントUSBデバイスリダイレクトルール**」または「**クライアントUSBデバイスリダイレクトルール (バージョン 2)**」ポリシーの使用を示します。このセクションに記載されている情報は、Citrix®管理者が構成したすべてのルールを一覧表示します。

```
C:\Program Files\Citrix\HDX\bin>CtxUsbDiagnostics.exe

==================================
          Session ID : 1
----------------------------------
       DDC rules - Version 1 :
----------------------------------
allow=0 flags=8 vendor=17e9
allow=0 flags=1 class=2
```

- **クライアントのデフォルトデバイスルール**
  - このセクションには、クライアントのレジストリに設定されているルールが一覧表示されます。

```
--------------------------------
   Client default device rules :
--------------------------------
 # Syntax is an ordered list of case insensitive rules where # is line comment
 #   and each rule is (ALLOW | DENY) : ( match )*
 #   and each match is (class|subclass|prot|vid|pid|rel) = hex-number
 # Maximum hex value for class/subclass/prot is FF, and for vid/pid/rel is FFFF
DENY: vid=17e9 # All DisplayLink USB displays
CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID
DENY: class=02 # Communications and CDC-Control
DENY: class=09 # Hub devices
DENY:vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY:vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07dd # Microsoft Surface Pro JP 3 Type Cover
DENY:vid=045e pid=07de # Microsoft Surface Pro 3_2 Type Cover
DENY:vid=045e pid=07e2 # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
DENY:vid=045e pid=07e8 # Microsoft Surface Pro 4_2 Type Cover
DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer
ALLOW:vid=056a pid=0315 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=0314 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=00fb class=03 # Wacom DTU tablet
DENY: class=03 subclass=01 prot=01 # HID Boot keyboards
DENY: class=03 subclass=01 prot=02 # HID Boot mice
DENY: class=0a # CDC-Data
DENY: class=0b # Smartcard
DENY: class=e0 # Wireless controller
DENY: class=ef subclass=04 # Miscellaneous network devices
ALLOW: # Otherwise allow everything else
```

デバイスリスト

このセクションには、クライアントエンドポイントに接続されている各デバイスに関する貴重な情報、ハードウェア情報、リダイレクトされているかどうか、正しいデバイスリダイレクトルールが設定されているかどうかなどが一覧表示されます。

タグ名	説明
displayName	デバイスの一般名を一覧表示します。
ベンダーID	ベンダーID
プロダクトID	プロダクトID
インターフェイス	このサブセクションには、複合デバイスが複数の子デバイスに分割されている場合のすべてのインターフェイスが一覧表示されます。
redirectionState	**Local** は、デバイスがICA®セッションでリダイレクトされていないことを示します。**ThisSession** は、デバイスがICAセッションでリダイレクトされていることを示します。**OtherSession** は、デバイスが別のICAセッションでリダイレクトされていることを示します。
optiEnabled	**true** はデバイスが最適化されていることを示します。**false** はデバイスが最適化されておらず、データ転送がUSB仮想チャネル経由で行われることを示します。
deviceType	**generic** は、デバイスに最適化された仮想チャネルがなく、トラフィックがUSB仮想チャネルを介して流れていることを示します。**optimized** は、デバイスに関連付けられたデータ転送が専用の仮想チャネルを介して行われていることを意味します。
isDenied	**true** は、管理者が設定したポリシー規則によりデバイスがリダイレクトされていないことを示します。**false** は、適用されたポリシーによりデバイスがリダイレクトされていることを示します。
denyRule	このフィールドは、isDenied が **true** に設定されている場合に役立ちます。これにより、デバイスがリダイレクトされない原因となっているポリシー内の特定の規則セットを管理者に伝えます。

モバイルデバイスとタッチスクリーンデバイス

Citrix Virtual Apps and Desktops™ を使用すると、ユーザーは公開されたアプリケーションやデスクトップにモバイルおよびタッチスクリーンクライアントデバイスからアクセスできます。

要件

Citrix® コントロールプレーン

- シトリックス バーチャル アプリケーションズ アンド デスクトップス 7.15 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
  - Windows Server 2016 またはそれ以降のバージョン
- VDA
  - Windows: Citrix Virtual Apps and Desktops のバージョン 7.15 またはそれ以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- Windows 用 Citrix Workspace™ アプリ バージョン 1808 以降

Windows Continuum を使用するタッチスクリーンデバイスのタブレットモード

Continuum は、クライアントデバイスの使用方法に適応する Windows 10 の機能です。VDA は、タッチ対応クライアントでキーボードまたはマウスの存在を検出すると、クライアントをデスクトップモードにします。キーボードまたはマウスが存在しない場合、VDA はクライアントをタブレット/モバイルモードにします。この検出は、セッションの接続時および再接続時、ならびにセッション中にキーボードまたはマウスが接続または切断されたときに発生します。

この機能はデフォルトで有効になっています。この機能を無効にするには、ポリシー設定 タブレットモード切り替えポリシー設定 を構成します。

上記のタッチスクリーンデバイスの要件に加えて、Windows Continuumには以下が必要です。

ゼノサーバー (旧 シトリックス ハイパーバイザー™)

- シトリックス ハイパーバイザー 8.2 以降
- ラップトップ/タブレットの切り替えを許可するには、XenServer CLIコマンドを実行します。
  xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1

> **重要:**

> メタデータ設定を変更した後に既存のマシンカタログのベースイメージを更新しても、以前にプロビジョニングされたVMには影響しません。XenServer VMのベースイメージを変更した後、カタログを作成し、ベースイメージを選択して、新しいMachine Creation Services™ (MCS) マシンをプロビジョニングします。

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA
  - Windows: バージョン 7.16 以降
  - **現在のオペレーティングシステム構成の制限により、ユーザーは最初のICA®セッションを開始してVDAを再起動した後、ドロップダウンメニューから以下のオプションを設定する必要があります。**
    - **設定 > システム > タブレットモード**
      - ハードウェアに適したモードを使用する
      - 常に切り替える（確認しない）

    タブレットモード設定の画像(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/tablet-mode-settings.png)

タブレットモードは、タッチスクリーンにより適したユーザーインターフェイスを提供します。

- ボタンが少し大きくなります。
- スタート画面と起動するすべてのアプリが全画面で開きます。
- タスクバーに「戻る」ボタンが含まれます。
- タスクバーからアイコンが削除されます。

ファイルエクスプローラーにアクセスできます。

タブレットモードの画像(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/tablet-mode.png)

Windows 10 は、この更新された BIOS に基づいて、ターゲット仮想マシンに GPIO ドライバーをロードします。これは、仮想マシン内でタブレットモードとデスクトップモードを切り替えるために使用されます。

HTML5 用 Citrix Workspace アプリは、Windows Continuum 機能をサポートしていません。

デスクトップモードは、PC とキーボード、マウスを使用するのと同じ方法で操作する従来のユーザーインターフェイスを提供します。

マイクロソフト Surface Pro および Surface Book ペン

Windows Inkベースのアプリケーションで標準のペン機能をサポートしています。サポートには、ポインティング、消去、ペン圧、Bluetooth信号、およびオペレーティングシステムのファームウェアとペンモデルに応じたその他の機能が含まれます。例えば、ペン圧は最大4096レベルまで可能です。この機能はデフォルトで有効になっています。

ペン機能のサポートに関する要件は次のとおりです。

Citrixコントロールプレーン

- シトリックス バーチャル アプリケーションズ アンド デスクトップス 1903 以降
- シトリックス DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows 11 21H2 以降
  - Windows Server 2016 またはそれ以降

- VDA
  - Windows: シトリックス バーチャル アプリケーションズ アンド デスクトップス 1903 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- Windows 版 Citrix Workspace アプリ バージョン 1902 以降

Windows Ink とペンの機能のデモンストレーションについては、このグラフィックをクリックしてください:



この機能を無効または有効にするには、レジストリで管理される機能のリストにある Microsoft Surface Pro および Surface Book のペン を参照してください。

既知の問題

ペンサポートに関する既知の問題は次のとおりです:

- Windows Server 2k22 の OS 制限により、ユーザーは 2k22 サーバーアプリケーションまたはデスクトップに接続している場合、コントロールパネルでペンのショートカットを設定したり、ペン/インクの設定を調整したりすることはできません。
- OS の制限により、ペン対応の Windows 11 クライアントからのペンのショートカットは尊重されません。

シリアルポート

ほとんどの新しいPCには、シリアル（COM）ポートが内蔵されていません。USBコンバーターを使用すると、これらのポートを簡単に追加できます。シリアルポートに適したアプリケーションには、センサー、コントローラー、古いチェックリーダー、パッドなどがよく含まれます。一部のUSB仮想COMポートデバイスは、Windows提供のドライバー（usbser.sys）の代わりにベンダー固有のドライバーを使用します。これらのドライバーを使用すると、USBデバイスの仮想COMポートを強制的に設定できるため、異なるUSBソケットに接続しても変更されません。これは、**デバイスマネージャー > ポート (COM と LPT) > プロパティ**から、またはデバイスを制御するアプリケーションから行うことができます。

クライアントCOMポートマッピングを使用すると、ユーザーのエンドポイントのCOMポートに接続されたデバイスを仮想セッション中に使用できます。これらのマッピングは、他のネットワークマッピングと同様に使用できます。

各COMポートについて、オペレーティングシステムのドライバーはCOM1やCOM2などのシンボリックリンク名を割り当てます。アプリケーションは、そのリンクを使用してポートにアクセスします。

> **重要:**

> デバイスがUSBを直接使用してエンドポイントに接続できるからといって、汎用USBリダイレクトを使用してリダイレクトできるとは限りません。一部のUSBデバイスは仮想COMポートとして機能し、アプリケーションは物理シリアルポートと同じ方法でアクセスできます。オペレーティングシステムはCOMポートを抽象化し、ファイル共有のように扱うことができます。仮想COMの一般的なプロトコルはCDC ACMまたはMCTの2つです。RS-485ポートを介して接続した場合、アプリケーションがまったく機能しない可能性があります。RS-485をCOMポートとして使用するには、RS-485-to-RS232コンバーターを入手してください。 **重要:**

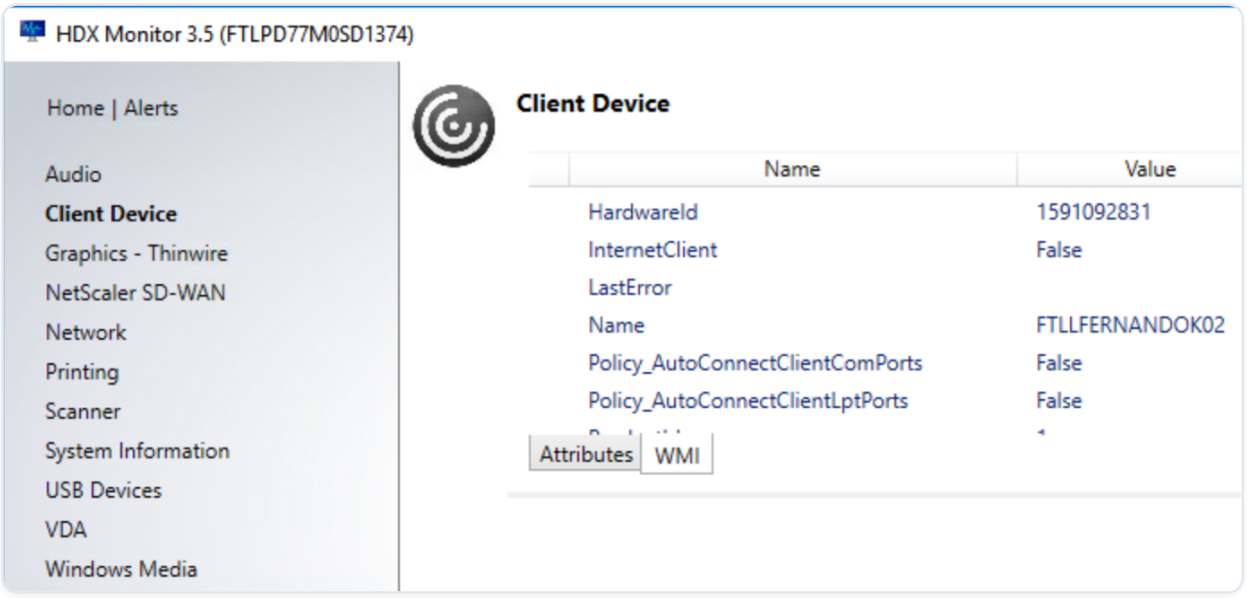
> 一部のアプリケーションは、クライアントワークステーションのCOM1またはCOM2に接続されている場合にのみ、デバイス（たとえば、署名パッド）を一貫して認識します。

クライアントCOMポートをサーバーCOMポートにマッピングする

クライアントCOMポートをCitrix®セッションにマッピングする方法は3つあります。

- Studioポリシー。ポリシーの詳細については、「ポートリダイレクトポリシー設定」を参照してください。
- VDAコマンドプロンプト。
- リモートデスクトップ（ターミナルサービス）構成ツール。

1. **クライアントCOMポートリダイレクト**ポリシーと**クライアントCOMポートの自動接続Studio**ポリシーを有効にします。適用後、HDX™ Monitorで一部の情報を確認できます。



2. **クライアントCOMポートの自動接続**がポートのマッピングに失敗した場合は、手動でポートをマッピングするか、ログオンスクリプトを使用できます。VDAにログオンし、コマンドプロンプトウィンドウで次のように入力します。

   NET USE COMX: `\CLIENT\COMZ`:

   または

   NET USE COMX: `\CLIENT\CLIENTPORT:COMZ`:

   X は VDA 上の COM ポートの番号です (マッピングにはポート 1 から 9 が利用可能です)。**Z** はマッピングしたいクライアント COM ポートの番号です。

   操作が成功したことを確認するには、VDA コマンドプロンプトで **NET USE** と入力します。表示されるリストには、マップされたドライブ、LPT ポート、およびマップされた COM ポートが含まれます。

```
C:\Windows\system32>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
             COM3      \\Client\COM3:            Citrix Client Network
```

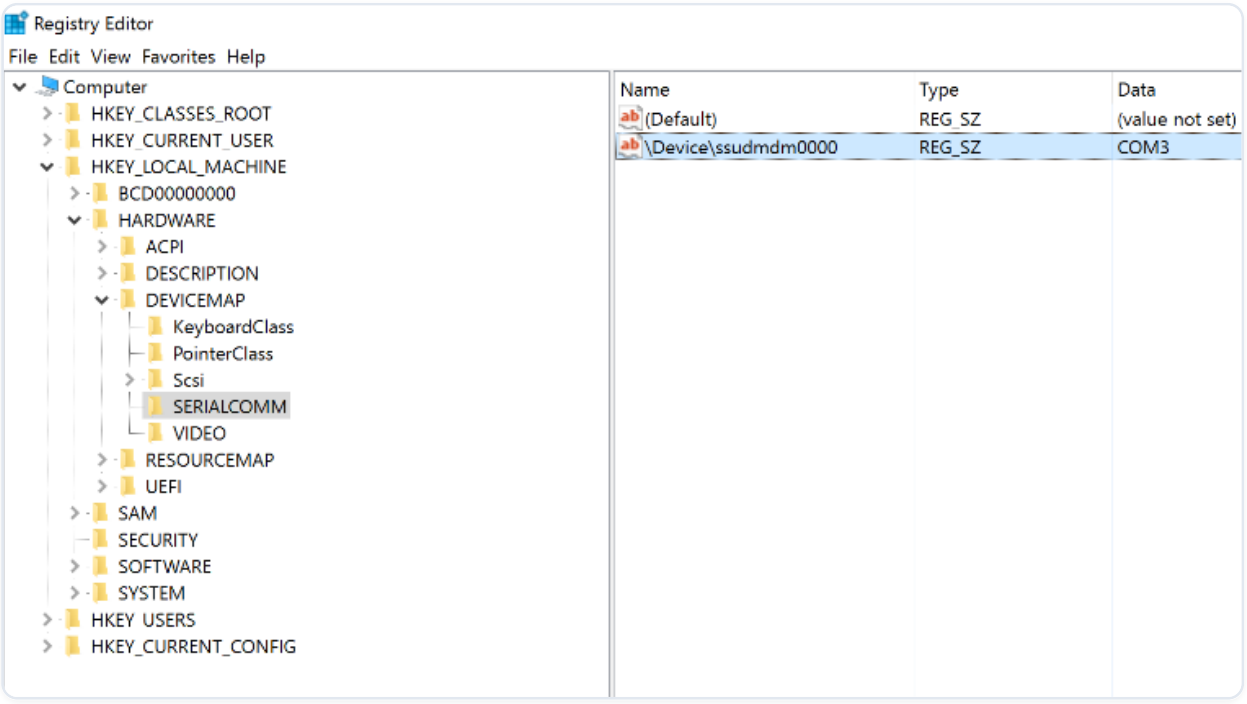
3. 仮想デスクトップまたはアプリケーションでこの COM ポートを使用するには、ユーザーデバイスアプリケーションをインストールし、マップされた COM ポート名を指定します。たとえば、クライアント上の COM1 をサーバー上の COM3 にマップする場合、VDA に COM ポートデバイスアプリケーションをインストールし、セッション中に COM3 を指定します。このマップされた COM ポートは、ユーザーデバイス上の COM ポートと同様に使用します。

重要:

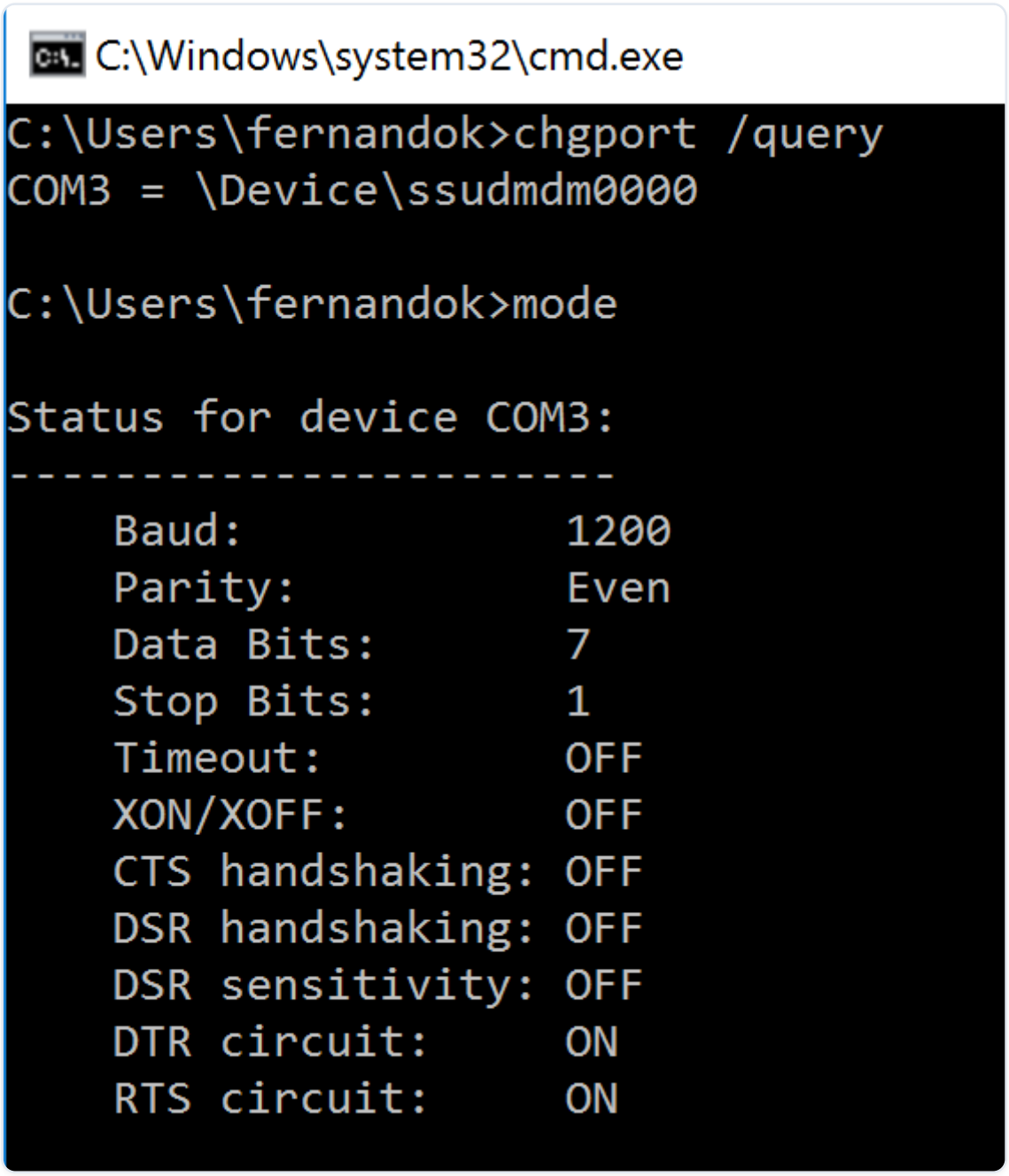
COM ポートマッピングは TAPI と互換性がありません。Windows Telephony Application Programming Interface (TAPI) デバイスをクライアント COM ポートにマップすることはできません。TAPI は、アプリケーションがデータ、FAX、音声通話の電話機能を制御するための標準的な方法を定義します。TAPI は、ダイヤル、応答、通話終了などのシグナリングを管理します。また、保留、転送、会議通話などの補足サービスも管理します。

トラブルシューティング

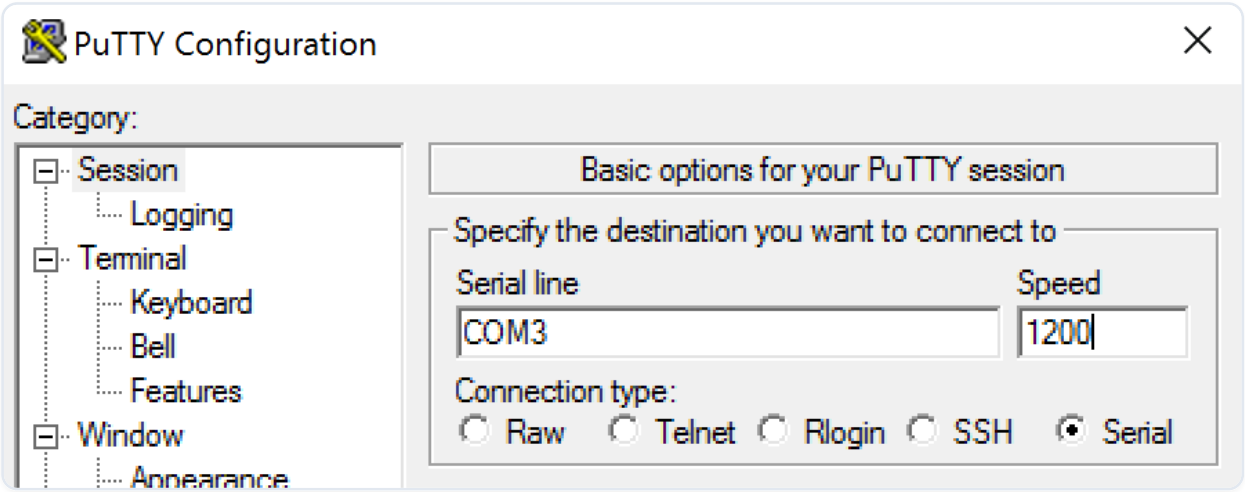
1. Citrix をバイパスして、エンドポイントから直接デバイスにアクセスできることを確認してください。ポートが VDA にマップされていない間は、Citrix セッションに接続されていません。デバイスに付属のトラブルシューティング手順に従い、まずローカルで動作することを確認してください。 シリアル COM ポートにデバイスが接続されると、ここに示されているハイブにレジストリキーが作成されます:



この情報は、コマンドプロンプトで **chgport /query** を実行することでも確認できます。



デバイスのトラブルシューティング手順が利用できない場合は、PuTTY セッションを開いてみてください。**Session** を選択し、**Serial line** で COM ポートを指定します。



ローカルコマンドウィンドウで **MODE** を実行できます。出力には、使用中のCOMポートと、PuTTYセッションで必要となるBaud/Parity/Data Bits/Stop Bitsが表示される場合があります。PuTTY接続が成功した場合は、**Enter** を押してデバイスからのフィードバックを確認します。入力した文字は画面に繰り返されたり、応答されたりする場合があります。この手順が失敗した場合、仮想セッションからデバイスにアクセスすることはできません。

2. ローカルのCOMポートをVDAにマッピングし（ポリシーまたは **NET USE COMX: \\\CLIENT\COMZ:** を使用）、前の手順と同じPuTTYの手順を繰り返しますが、今回はVDAのPuTTYから行います。PuTTYがエラー **Unable to open connection to COM1. Unable to open serial port** を表示しない場合、別のデバイスがCOM1を使用している可能性があります。
3. **chgport /query** を実行します。VDA上の組み込みWindowsシリアルドライバーが、\Device\Serial0 をVDAのCOM1ポートに自動割り当てしている場合は、次の操作を行います。
   A. VDAでCMDを開き、**NET USE.** と入力します。

   B. VDA上の既存のマッピング（例：COM1）を削除します。

   NET USE COM1 /DELETE

   C. デバイスをVDAにマッピングします。

   NET USE COM1: `\CLIENT\COM3` :

   D. VDA上のアプリケーションをCOM3に指定します。

   最後に、ローカルのCOMポート（例: COM3）をVDA上の別のCOMポート（COM1以外、例: COM3）にマッピングしてみてください。アプリケーションがそれを指していることを確認してください。 **NET USE COM3: \\\CLIENT\COM3**
4. ポートがマッピングされているのにPuTTYは動作しているがデータが通過しない場合、それは競合状態である可能性があります。アプリケーションがマッピングされる前にポートに接続して開いてしまい、マッピングをロックしている可能性があります。次のいずれかを試してください。

   - 同じサーバーで公開されている2番目のアプリケーションを開きます。ポートがマッピングされるまで数秒待ってから、ポートを使用しようとする実際のアプリケーションを開きます。
   - Studioではなく、Active DirectoryのグループポリシーエディターからCOMポートリダイレクトポリシーを有効にします。これらのポリシーは、**Client COM port redirection** と **Auto connect client COM ports** です。この方法で適用されたポリシーは、Studioポリシーよりも前に処理され、COMポートがマッピングされることを保証する場合がありま

す。Citrixポリシーは VDA にプッシュされ、次の場所に保存されます。
`HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`

- ユーザーにこのログオンスクリプトを使用するか、アプリケーションを公開する代わりに、まず VDA 上のマッピングを削除し、仮想 COM ポートを再マッピングしてからアプリケーションを起動する.bat スクリプトを公開します。

@echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: `\CLIENT\COM1`: NET USE COM2: `\CLIENT\COM2`: MODE COM1: BAUD=1200 (または必要な値) MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (または必要な値) START `C:\Program Files\<Your Software Path>\<your_software.exe>`

5. SysinternalsのProcess Monitorは、最後の手段となるツールです。VDAでこのツールを実行する際、COM3、picaser.sys、CdmRedirectorなどのオブジェクト、特に\<your_app\>.exe を見つけてフィルターします。エラーは「アクセス拒否」または類似の形で表示される場合があります。

特殊キーボード

Bloombergキーボード

> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターの使用は、お客様ご自身の責任において行ってください。編集する前に、必ずレジストリをバックアップしてください。

> Citrix Virtual Apps and Desktops™は、Bloombergモデル5、モデル4 Starboardキーボード（およびそれ以前のモデル3）をサポートしています。このキーボードにより、金融業界のお客様は、キーボードの特殊機能を使用して金融市場データにアクセスし、迅速な取引を実行できます。

> **重要:**

> Bloombergキーボードは1つのセッションでのみ使用することをお勧めします。複数の同時セッション（1つのクライアントから複数のセッションへ）でキーボードを使用することはお勧めしません。

> Bloombergキーボードは、1つの物理シェルに複数のUSBデバイスを搭載したUSB複合デバイスです。

- キーボード。
- 指紋リーダー。
- 音量を上げ下げするキー、およびスピーカーとマイクをミュートするキーを備えたオーディオデバイス。このデバイスには、オンボードスピーカー、マイク、およびマイクとヘッドセット用のジャックが含まれています。
- これらすべてのデバイスをシステムに接続するためのUSBハブ。

要件:

- Citrix Workspace™ app for Windows が接続するセッションは、USB デバイスをサポートしている必要があります。
- Bloomberg キーボード モデル 5 をサポートするには、Linux 用 Citrix Workspace アプリ 2207 以降が必要です。
- Bloomberg キーボード モデル 5 をサポートするには、Windows 用 Citrix Workspace アプリ 2109 以降が必要です。
- Bloomberg キーボード モデル 3 および 4 をサポートするには、Windows 用 Citrix Workspace アプリ 1808 以降、または Windows 用 Citrix Receiver 4.8 以降が必要です。
- モデル 4 で KVM モード (KVM を介してルーティングされた 1 本を含む 2 本の USB ケーブル) を使用するには、Windows 用 Citrix Workspace アプリ 1808 以降、または Windows 用 Citrix Receiver 4.12 以降が必要です。

Windows 用 Citrix Workspace アプリでの Bloomberg キーボードの構成については、「Bloomberg キーボードの構成」を参照してください。

Bloomberg キーボードのサポートを有効にするには、レジストリで管理される機能のリストにある「Bloomberg キーボード」を参照してください。

サポートを確認する:

Citrix Workspace アプリで Bloomberg キーボードのサポートが有効になっているかどうかを確認するには、Desktop Viewer が Bloomberg キーボードのデバイスを正しく報告しているかどうかを確認します。

デスクトップシナリオ:

Desktop Viewer を開きます。Bloomberg キーボードのサポートが有効になっている場合、Desktop Viewer には USB アイコンの下に 3 つのデバイスが表示されます。

Bloomberg 5 キーボードの場合:

- Bloomberg LP Bloomberg バイオメトリックモジュール
- Bloomberg LP Keyboard (2つのインターフェイスを持つ複合デバイス)
- Bloomberg LP Keyboard Audio (3つのインターフェイスを持つ複合デバイス)

Bloomberg 3 および 4 キーボードの場合:

- Bloomberg 指紋スキャナー
- Bloomberg キーボードの機能
- Bloomberg LP キーボード 2013

シームレスアプリケーションのみのシナリオ:

Citrix Workspaceアプリの通知領域アイコンから、**接続センター**メニューを開きます。Bloombergキーボードのサポートが有効になっている場合、3つのデバイスが**デバイス**メニューに表示されます。

これらの各デバイスの横にあるチェックマークは、それらがセッションにリモート接続されていることを示します。

TWAINデバイス

要件

- スキャナーはTWAIN準拠である必要があります。
- TWAINドライバーをローカルデバイスにインストールします。サーバーには必要ありません。
- スキャナーをローカルに接続します（例：USB経由）。
- スキャナーがローカルのTWAINドライバーを使用しており、Windowsイメージ取得サービスを使用していないことを確認してください。

- テストに使用されるユーザーアカウントに、ICA®セッション内の帯域幅を制限するポリシーが適用されていないことを確認してください。たとえば、クライアントUSBリダイレクト帯域幅制限などです。

ポリシー設定については、TWAINデバイスのポリシー設定を参照してください。

Webカメラ

高解像度Webカメラストリーミング

Webカメラは、仮想セッション内で実行されているビデオ会議アプリケーションで使用できます。サーバー上のアプリケーションは、サポートされているフォーマットタイプに基づいてWebカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはWebカメラ情報をサーバーに送信します。ビデオ会議アプリケーションからWebカメラを選択します。Webカメラとアプリケーションの両方が高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。Webカメラの解像度は最大1920x1080までサポートしています。

この機能には、Citrix Receiver for Windows バージョン4.10以降が必要です。HDXウェブカメラリダイレクトをサポートするCitrix Workspaceアプリプラットフォームのリストについては、「Citrix Workspace app feature matrix」を参照してください。

高解像度ウェブカメラストリーミングの詳細については、「HDX video conferencing and webcam video compression」を参照してください。

レジストリキーを使用してこの機能を無効または有効にし、特定の解像度を設定できます。詳細については、レジストリで管理される機能のリストにある「High-definition webcam streaming and High-definition webcam resolution」を参照してください。

WIA デバイス

要件

- スキャナーはWIA準拠である必要があります。
- ローカルデバイスにWIAドライバーをインストールします。サーバーには必要ありません。
- スキャナーをローカルに接続します（例：USB経由）。
- スキャナーがTWAINドライバーではなく、ローカルのWindows Image Acquisitionサービスを使用していることを確認してください。

- テストに使用されるユーザーアカウントに、ICA®セッション内の帯域幅を制限するポリシーが適用されていないことを確認してください。たとえば、クライアントUSBリダイレクトの帯域幅制限などです。

Windows Image Acquisitionアプリケーションの許可リスト

許可リストを使用すると、VDA上のどのアプリケーションがWindows Image Acquisitionスキャナーリダイレクトにアクセスできるかを制御できます。レジストリエディターは、Windows Image Acquisitionを含む各VDAの許可リスト設定からの入力を使用します。デフォルトでは、どのアプリケーションもWindows Image Acquisitionにアクセスできません。

VDA上のアプリケーション向けにWindows Image Acquisitionを調整するには、レジストリを介して管理される機能のリストにあるWindows Image Acquisitionアプリケーションの許可リスト設定を参照してください。

ポリシー設定の詳細については、WIAデバイスのポリシー設定を参照してください。

グラフィックス

Citrix HDXグラフィックスには、Citrix Virtual Apps and Desktopsからのリッチグラフィックアプリケーションの配信を最適化する、広範なグラフィックアクセラレーションおよびエンコード技術が含まれています。これらのグラフィック技術は、グラフィックを多用する仮想アプリケーションをリモートで操作する際に、物理デスクトップを使用するのと同じエクスペリエンスを提供します。

グラフィックレンダリングには、ソフトウェアまたはハードウェアを使用できます。ソフトウェアレンダリングには、ソフトウェアラスタライザーと呼ばれるサードパーティ製ライブラリが必要です。たとえば、WindowsにはDirectXベースのグラフィック用のWARPラスタライザーが含まれています。場合によっては、代替のソフトウェアレンダラーを使用したいこともあるでしょう。ハードウェアレンダリング（ハードウェアアクセラレーション）には、グラフィックプロセッサ（GPU）が必要です。

HDX™ Graphicsは、最も一般的なユースケース向けに最適化されたデフォルトのエンコード構成を提供します。Citrixポリシーを使用することで、IT管理者はさまざまな要件を満たし、望ましいユーザーエクスペリエンスを提供するために、さまざまなグラフィック関連設定を構成できます。

シンワイヤー

Thinwireは、Citrix Virtual Apps and Desktopsで使用されるCitrixのデフォルトのディスプレイリモートテクノロジーです。

ディスプレイリモートテクノロジーにより、あるマシンで生成されたグラフィックを、通常はネットワーク経由で別のマシンに送信して表示できます。グラフィックは、たとえばキーストロークやマウス操作などのユーザー入力の結果として生成されます。

エイチディーエックス スリーディー プロ

Citrix Virtual Apps and DesktopsのHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションのためにグラフィック処理ユニット（GPU）を使用して最高のパフォーマンスを発揮するデスクトップとアプリケーションを配信できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックアプリケーションが含まれます。標準VDAはDirectXのGPUアクセラレーションのみをサポートします。

WindowsシングルセッションOSのGPUアクセラレーション

HDX 3D Proを使用することで、ホスト型デスクトップまたはシングルセッションOSマシン上のアプリケーションの一部として、グラフィックを多用するアプリケーションを配信できます。HDX 3D Proは、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションを含む）と、XenServer®、vSphere、Hyper-V（パススルーのみ）ハイパーバイザーが提供するGPUパススルーおよびGPU仮想化テクノロジーをサポートします。

GPUパススルーを使用すると、専用のグラフィックス処理ハードウェアに排他的にアクセスできるVMを作成できます。ハイパーバイザーに複数のGPUをインストールし、これらのGPUのそれぞれにVMを1対1で割り当てることができます。

GPU仮想化を使用すると、複数の仮想マシンが単一の物理GPUのグラフィックス処理能力に直接アクセスできます。

WindowsマルチセッションOSのGPUアクセラレーション

HDX 3D Proを使用すると、WindowsマルチセッションOSセッションで実行されているグラフィックを多用するアプリケーションをサーバーのグラフィック処理ユニット（GPU）でレンダリングできます。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation（WPF）のレンダリングをサーバーGPUに移行することで、グラフィックレンダリングがサーバーCPUの速度を低下させることはありません。また、ワークロードがCPUとGPUの間で分割されるため、サーバーはより多くのグラフィックを処理できます。

フレームホーク

> **重要:**
>
> Citrix Virtual Apps and Desktops 7 1903以降、Framehawkはサポートされなくなりました。代わりに、Thinwireをアダプティブトランスポートを有効にして使用してください。

> Framehawkは、ブロードバンドワイヤレス接続（Wi-Fiおよび4G/LTEセルラーネットワーク）を使用するモバイルワーカー向けのディスプレイリモートテクノロジーです。Framehawkは、スペクトル干渉やマルチパス伝播の課題を克服し、仮想アプリおよびデスクトップのユーザーにスムーズでインタラクティブなユーザーエクスペリエンスを提供します。

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への

抑止力として、セッションデスクトップに表示されます。テキストのレイヤーであるウォーターマークを指定できます。ウォーターマークは、元のドキュメントの内容を変更することなく、セッション画面全体に表示できます。テキストベースのセッションウォーターマークには、VDAのサポートが必要です。

アダプティブ リフレッシュ レート

新しいスケーラビリティの改善により、HDXは仮想モニターのリフレッシュレートをターゲットFPSポリシー設定に合わせます。アダプティブ リフレッシュ レート（ARR）は、シングルセッションVDAとマルチセッションVDAの両方で利用でき、GPUアクセラレーションシナリオと非GPUシナリオの両方で機能します。

ロス耐性モード

ロス耐性モードは、パケット損失が検出されたときにセッションがインタラクティブな状態を維持するように徹底的に再設計されています。

関連情報

- エイチディーエックス 3D プロ
- WindowsシングルセッションOS向けGPUアクセラレーション
- WindowsマルチセッションOS向けGPUアクセラレーション
- フレームホーク
- シンワイヤー
- テキストベースのセッションウォーターマーク(/ja-jp/citrix-virtual-apps-desktops/2311/graphics/session-watermark.html)

10ビット ハイダイナミックレンジ (HDR)

10ビット ハイダイナミックレンジ (HDR) 仮想デスクトップセッションを使用すると、強化されたエンコードおよびデコード機能を利用して、拡張された色域、より高いコントラストと輝度を備えた高品質の画像とビデオをレンダリングできます。また、白色輝度レベル、Extended Display Identification Data (EDID)、および視覚品質をカスタマイズして、ユーザーエクスペリエンスを向上させることができます。

システム要件

エンドポイント:

- Citrix Workspace™ アプリ for Windows 2209以降 (NVIDIA GPU向け)
- エンドポイント上で10ビット HEVC (H.265) 444デコードをサポートするNVIDIA GPU
- 10ビットHDR対応モニター。ディスプレイ設定を使用して、すべてのモニターで10ビットHDRを有効にする必要があります。

サーバー:

- WindowsシングルセッションOS VDA 2209以降 (NVIDIA GPU向け)、およびVDA 2308以降 (Intel GPU向け)
- VDA上で10ビット HEVC 444エンコードをサポートするNVIDIA GPU

必要なポリシー

エンドポイント:

- グラフィックのH.265デコードを有効にする

サーバー:

- 3Dグラフィックワークロード向けに最適化する
- グラフィックステータスインジケーター (オプション)

サーバー構成

10ビットHDR対応のエンドポイントモニターでCitrix®セッションを起動すると、HDRセッションはデフォルトで有効になります。マルチモニターHDRセッションでは、すべてのエンドポイントモニターで10ビットHDRが有効になっている必要があります。HDRセッションは、ウィンドウモードと全画面モードの両方でサポートされています。

リファレンスホワイトレベル

この設定は、ニト値で白色輝度レベルを定義します。セッション内の相対的なHDR画面の明るさを制御します。デフォルト値は80ニトです。異なるニト値を定義するには、以下のレジストリキーを設定します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- タイプ: REG_DWORD
- 名前: RefWhiteLevel

設定を有効にするには、セッションのサイズを変更するか、セッションを切断して再起動する必要があります。

EDIDオーバーライド

HDRセッションでエンドポイントモニターのEDIDを使用するようにVDAを構成できます。これにより、色域と輝度範囲を一致させることで、モニターの表示機能を最大限に活用できます。デフォルトでは、HDRセッションはHDR1000対応ディスプレイを想定しています。 NVIDIAまたはその他のツールを使用して、エンドポイントモニターのEDIDをエクスポートできます。次のレジストリキーを使用してVDAに適用します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- タイプ: REG_BINARY
- 名前: EDIDオーバーライド

EDIDをレジストリに保存する際、コンマ、スペース、特殊文字を含めてはなりません。オーバーライドEDIDを有効にするには、サインアウトして新しいセッションを起動してください。

視覚的にロスレスなエクスペリエンス

視覚的にロスレスなエクスペリエンスを実現するには、次のポリシーを有効にします。

- 視覚的にロスレスな圧縮を許可する
- 視覚品質: 常にロスレスまたはロスレスに構築

ポリシーが設定された後、グラフィックステータスインジケーターを使用して、イメージ品質スライダーを使用するか、ピクセルパーフェクトモードに切り替えることで、HDRセッションの品質を制御できます。

その他の考慮事項

- 仮想GPUでは、最大4台のモニターで10ビットHDRセッションを起動できます。
- Citrixセッションは、次のインスタンスで8ビットの非HDRモードに戻ります。
    - いずれかのエンドポイントモニターで10ビットHDRが有効になっていない場合
    - 画面共有を有効にする
    - VDA上で仮想ディスプレイレイアウトを設定する
    - 「視覚的にロスレスな圧縮を許可する」ポリシーを設定せずにピクセルパーフェクトモードに切り替える

HDX™ 3D プロ

Citrix Virtual Apps and Desktops™のHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションのためにグラフィックス処理ユニット (GPU) を使用して最高のパフォーマンスを発揮するデスクトップとアプリケーションを提供できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックスアプリケーションが含まれます。標準VDAはDirectXのGPUアクセラレーションのみをサポートします。

HDX 3D Proポリシー設定については、3Dグラフィックワークロードの最適化を参照してください。

サポートされているすべてのCitrix Workspaceアプリは3Dグラフィックスで使用できます。複雑な3Dワークロード、高解像度モニター、マルチモニター構成、および高フレームレートアプリケーションで最高のパフォーマンスを得るには、Citrix Workspace app for WindowsおよびCitrix Workspace app for Linuxの最新バージョンをお勧めします。サポートされているCitrix Workspaceアプリのバージョンに関する詳細については、Citrix Workspaceアプリのライフサイクルマイルストーンを参照してください。

3Dプロフェッショナルアプリケーションの例を次に示します。

- コンピューター支援設計、製造、エンジニアリング (CAD/CAM/CAE) アプリケーション
- 地理情報システム (GIS) ソフトウェア
- 医用画像処理通信システム (PACS)
- 最新のOpenGL、DirectX、NVIDIA CUDA、OpenCL、およびWebGLバージョンを使用するアプリケーション
- 並列コンピューティングにNVIDIA Compute Unified Device Architecture (CUDA) GPUを使用する計算集約型の非グラフィカルアプリケーション

HDX 3D Proは、あらゆる帯域幅で最高のユーザーエクスペリエンスを提供します。

- WAN接続の場合：1.5 Mbpsという低い帯域幅のWAN接続でも、インタラクティブなユーザーエクスペリエンスを提供します。
- LAN接続の場合：LAN接続でローカルデスクトップと同等のユーザーエクスペリエンスを提供します。

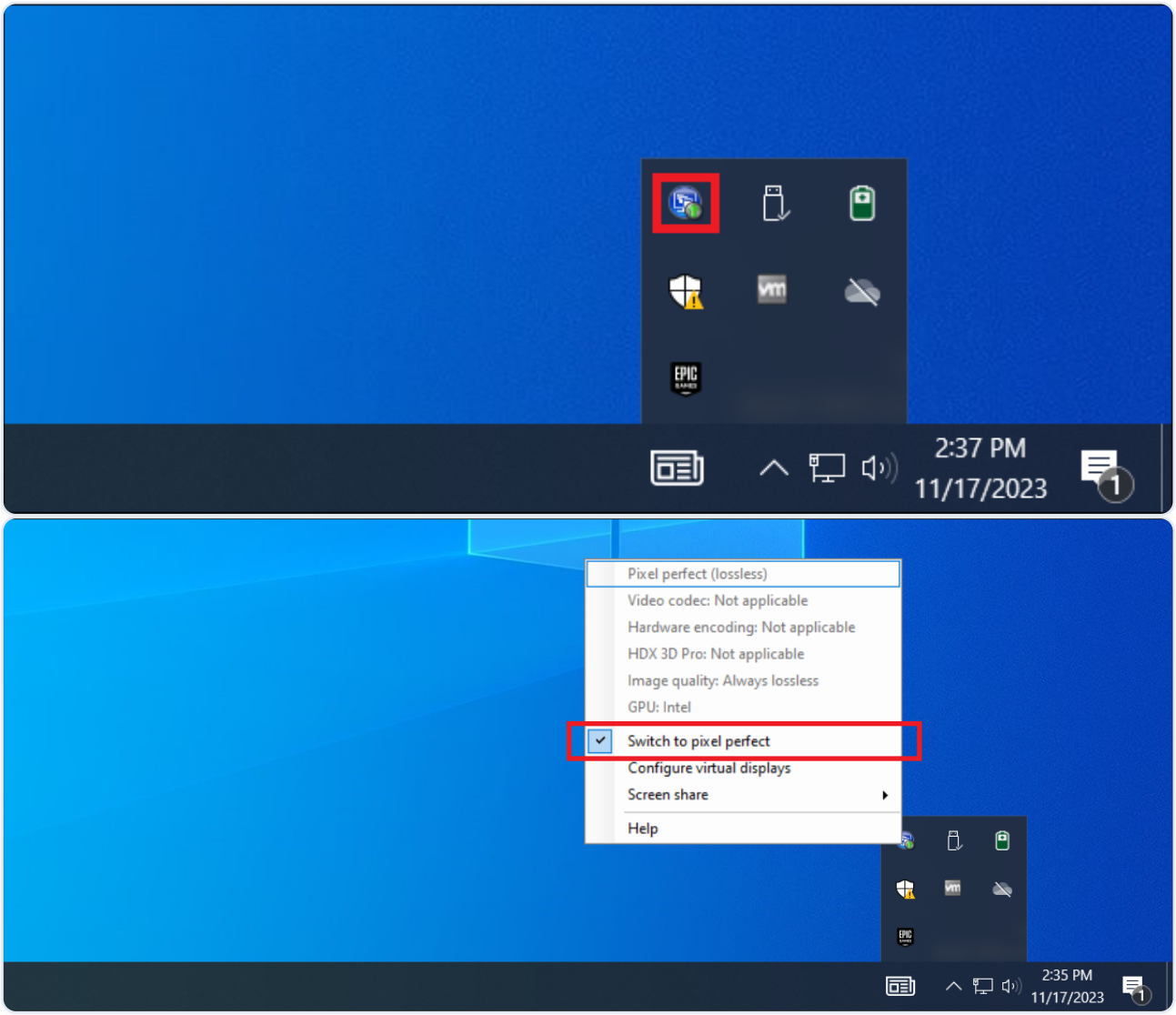
  グラフィックス処理をデータセンターに移動して一元管理することで、複雑で高価なワークステーションをよりシンプルなユーザーデバイスに置き換えることができます。

特殊なユースケース向けのロスレス圧縮オプション

HDX 3D Pro も、医療画像処理など、ピクセルパーフェクトなグラフィックが必要なアプリケーションをサポートするために、CPUベースのロスレスコーデックを提供します。真のロスレス圧縮は、より多くのネットワークリソースと処理リソースを消費するため、特殊なユースケースでのみ推奨されます。

ロスレス圧縮を使用する場合：

- 通知領域アイコンであるグラフィックステータスインジケーターのロスレスインジケーターは、表示されている画面がロッシーフレームかロスレスフレームかをユーザーに通知します。このアイコンは、**視覚品質**ポリシー設定で**ロスレスにビルド**が指定されている場合に役立ちます。送信されるフレームがロスレスの場合、ロスレスインジケーターは緑色に変わります。



- ロスレススイッチを使用すると、セッション中にいつでも**常にロスレス**モードに変更できます。セッション内で**ロスレス**を選択または解除するには、アイコンを右クリックして**ピクセルパーフェクトに切り替え**をクリックするか、ショートカットALT+SHIFT+1を使用します。

- ロスレス圧縮の場合：HDX 3D Proは、ポリシーで選択されたコーデックに関係なく、ロスレスコーデックを圧縮に使用します。
- ロッシー圧縮の場合：HDX 3D Proは、デフォルトまたはポリシーによって選択された元のコーデックを使用します。 ロスレススイッチの設定は、以降のセッションでは保持されません。すべての接続でロスレスコーデックを使用するには、**視覚品質ポリシー**設定で**常にロスレス**を選択します。

セッション内でロスレスを選択または選択解除するためのデフォルトのショートカットALT+SHIFT+1を上書きできます。
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`で新しいレジストリ設定を構成します。

- 名前：HKEY_LOCAL_MACHINE_HotKey、種類：文字列
- ショートカットの組み合わせを構成する形式は、C=0|1, A=0|1, S=0|1, W=0|1, K=val です。キーはコンマ「,」で区切る必要があります。キーの順序は関係ありません。
- A、C、S、W、Kはキーであり、C=Control、A=ALT、S=SHIFT、W=Win、K=有効なキーです。Kに許可される値は、0〜9、a〜z、および任意の仮想キーコードです。
- 例： F10の場合、K=0x79と設定します Ctrl + F10の場合、C=1, K=0x79と設定します Alt + Aの場合、A=1, K=a または A=1, K=A または K=A, A=1と設定します Ctrl + Alt + 5の場合、C=1, A=1, K=5 または A=1, K=5, C=1と設定します Ctrl + Shift + F5の場合、A=1, S=1, K=0x74と設定します

HDX 3D Proのユーザーエクスペリエンスを最適化する

複数のユーザーが限られた帯域幅の接続を共有している場合（たとえば、支店など）、各ユーザーが利用できる帯域幅を制限するために、全体的なセッション帯域幅制限ポリシー設定を使用することをお勧めします。この設定を使用すると、ユーザーがログオンおよびログオフする際に利用可能な帯域幅が大きく変動しないようにすることができます。HDX 3D Proは利用可能なすべての帯域幅を使用するように自動的に調整されるため、ユーザーセッション全体で利用可能な帯域幅が大きく変動すると、パフォーマンスに悪影響を及ぼす可能性があります。 たとえば、20人のユーザーが60 Mbpsの接続を共有している場合、各ユーザーが利用できる帯域幅は、同時ユーザー数に応じて3 Mbpsから60 Mbpsの間で変動する可能性があります。このシナリオでユーザーエクスペリエンスを最適化するには、ピーク時にユーザーごとに必要な帯域幅を決定し、常にこの量にユーザーを制限します。 3Dマウスのユーザーの場合、汎用USBリダイレクト仮想チャネルの優先度を0に上げることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Centerの記事CTX128190を参照してください。 HDX Monitorツールを使用して、HDX視覚化テクノロジーの動作と構成を検証し、HDXの問題を診断およびトラブルシューティングし

ます。このツールは、Citrix Virtual Apps and Desktopsインストールメディアの**Support**フォルダーにあります。

Windows マルチセッション OS 向け GPU アクセラレーション

Citrix Virtual Apps and Desktops™は、WindowsマルチセッションOSセッションで実行されるグラフィック負荷の高いアプリケーションが、サーバーのグラフィック処理ユニット（GPU）でレンダリングされることをサポートします。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation（WPF）のレンダリングをサーバーのGPUに移行することで、サーバーのCPUをより効率的に使用できます。

Windows Serverはマルチユーザーオペレーティングシステムであるため、複数のユーザーがGPU仮想化（vGPU）を必要とせずに、Citrix Virtual Apps™によってアクセスされるGPUを共有できます。

レジストリの編集を伴う手順については、注意してください。レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

GPU 共有

GPU共有により、リモートデスクトップセッションでOpenGLおよびDirectXアプリケーションのGPUハードウェアレンダリングが可能になります。これには次の特徴があります。

- アプリケーションのスケーラビリティとパフォーマンスを向上させるために、ベアメタルまたは仮想マシンで使用できます。
- 複数の同時セッションでGPUリソースを共有できます（ほとんどのユーザーは専用GPUのレンダリングパフォーマンスを必要としません）。
- 特別な設定は不要です。

GPUは、ハイパーバイザーおよびGPUベンダーの要件に従って、フルパススルーモードまたは仮想GPU（vGPU）モードのいずれかでWindows Server仮想マシンに割り当てることができます。物理Windows Serverマシンへのベアメタル展開もサポートされています。

GPU共有は、特定のグラフィックカードに依存しません。

- 仮想マシンの場合、使用中のハイパーバイザーと互換性のあるグラフィックカードを選択してください。XenServerのハードウェア互換性リストについては、ハイパーバイザーハードウェア互換性リストを参照してください。

- ベアメタルで実行する場合、オペレーティングシステムによって有効化された単一のディスプレイアダプターを使用することをお勧めします。複数のGPUがハードウェアにインストールされている場合は、デバイスマネージャーを使用して1つを除くすべてを無効にしてください。

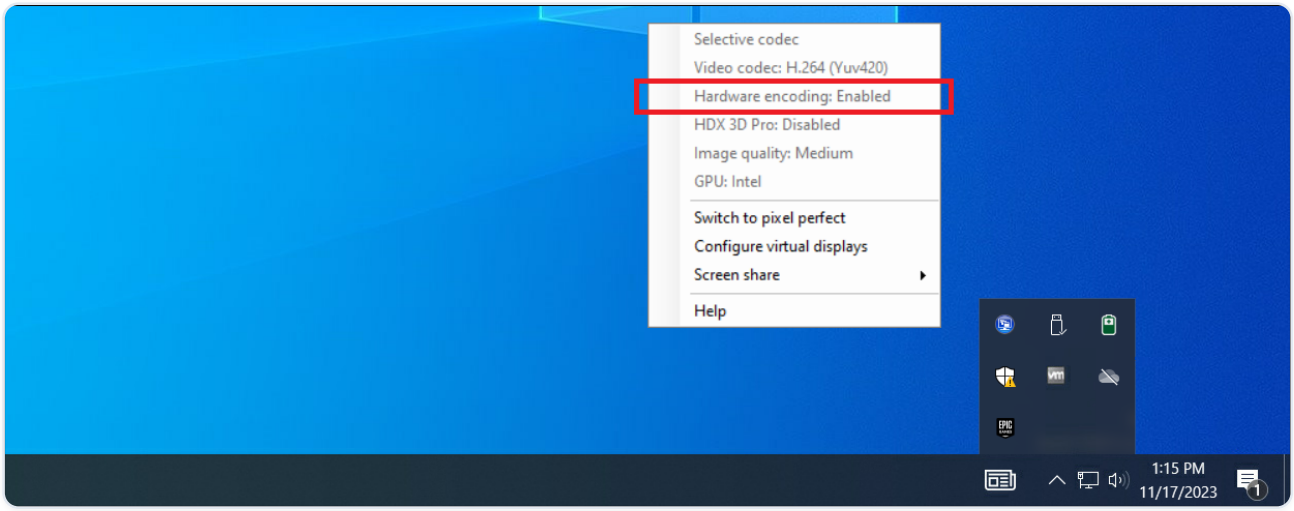
GPU Sharing を使用したスケーラビリティは、いくつかの要因によって異なります。

- 実行されているアプリケーション
- 消費するビデオ RAM の量
- グラフィックカードの処理能力

アプリケーションによっては、ビデオRAMの不足を他のものよりうまく処理するものがあります。ハードウェアが過負荷になると、グラフィックカードドライバーの不安定化やクラッシュが発生する可能性があります。このような問題を避けるため、同時実行ユーザー数を制限してください。

- NVIDIA GPU および Intel Iris Pro グラフィックプロセッサ用の高性能ビデオエンコーダーへのアクセス。ポリシー設定（デフォルトで有効）がこの機能を制御し、H.264 エンコード（利用可能な場合）にハードウェアエンコードの使用を許可します。このようなハードウェアが利用できない場合、VDA はソフトウェアビデオコーデックを使用した CPU ベースのエンコードにフォールバックします。詳しくは、「グラフィックポリシー設定」を参照してください。

GPU アクセラレーションが機能していることを確認するには、グラフィックステータスインジケーターを使用できます。



DirectX、Direct3D、および WPF レンダリング

DirectX、Direct3D、および WPF レンダリングは、ディスプレイドライバーインターフェイス（DDI）バージョン 9ex、10、または 11 をサポートする GPU を搭載したサーバーでのみ利用できます。

- Windows Server 2016以降では、RDセッションホストサーバー上のRemote Desktop Services（RDS）セッションは、Microsoft Basic Render Driverをデフォルトのアダプターとして使用します。Windows Server 2016以降のRDSセッションでGPUを使用するには、グループポリシーの**ローカルコンピューターポリシー** \> **コンピューターの構成** \> **管理用テンプレート** \> **Windowsコンポーネント** \> **Remote Desktop Services** \> **リモートデスクトップセッションホスト** \> **リモートセッション環境**で、**すべてのRemote Desktop Servicesセッションにハードウェアのデフォルトグラフィックアダプターを使用する**設定を有効にします。
- WPFアプリケーションがサーバーのGPUを使用してレンダリングできるようにするには、Windows Multi-session OSセッションを実行しているサーバーのレジストリに設定を作成します。レジストリ設定の詳細については、レジストリで管理される機能のリストにある「Windows Presentation Foundation (WPF) レンダリング」を参照してください。

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDA アクセラレーション機能を使用するには、レジストリ設定を有効にします。詳細については、レジストリで管理される機能のリストにある「CUDA または OpenCL アプリケーションの GPU アクセラレーション」を参照してください。

Windowsシングルセッション OS向けGPUアクセラレーション

HDX 3D Proを使用すると、グラフィックを多用するアプリケーションを、ホストされたデスクトップまたはシングルセッションOSマシン上のアプリケーションの一部として配信できます。HDX 3D Proは、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションを含む）と、XenServer®、vSphere、Nutanix、Hyper-V（パススルーのみ）ハイパーバイザーが提供するGPUパススルーおよびGPU仮想化テクノロジーをサポートします。

HDX™ 3D Proは、以下の機能を提供します。

- WANおよびワイヤレスパフォーマンスを最適化するための、適応型H.264ベースまたはH.265ベースのディープ圧縮。HDX 3D Proは、エンコードのデフォルト圧縮技術としてCPUベースの全画面H.264圧縮を使用します。H.264によるハードウェアエンコードは、NVENCをサポートするNVIDIA、Intel、およびAMDのカードで使用されます。H.265によるハードウェアエンコードは、NVENCをサポートするNVIDIAのカードで使用されます。
- 特殊なユースケース向けのロスレス圧縮オプション。HDX 3D Proは、医療画像処理など、ピクセルパーフェクトなグラフィックが必要なアプリケーションをサポートするために、CPU

ベースのロスレスコーデックも提供します。真のロスレス圧縮は、より多くのネットワークおよび処理リソースを消費するため、特殊なユースケースでのみ推奨されます。

ロスレス圧縮を使用する場合：

- ロスレスインジケーター（通知領域アイコン）は、表示されている画面がロッシーフレームかロスレスフレームかをユーザーに通知します。このアイコンは、**Visual Quality**ポリシー設定で**Build to lossless**が指定されている場合に役立ちます。送信されるフレームがロスレスの場合、ロスレスインジケーターは緑色に変わります。
- ロスレススイッチを使用すると、ユーザーはセッション中にいつでも「常にロスレス」モードに変更できます。**セッション中にいつでもロスレス**を選択または選択解除するには、アイコンを右クリックして**Switch to pixel perfect**をクリックするか、ショートカットALT+SHIFT+1を使用します。

  ロスレス圧縮の場合：HDX 3D Proは、ポリシーで選択されたコーデックに関係なく、ロスレスコーデックを圧縮に使用します。

  ロッシー圧縮の場合：HDX 3D Proは、デフォルトまたはポリシーで選択された元のコーデックを使用します。

  ロスレススイッチの設定は、以降のセッションでは保持されません。すべての接続でロスレスコーデックを使用するには、**Visual quality**ポリシー設定で**Always lossless**を選択します。

- セッション内でロスレスを選択または選択解除するためのデフォルトのショートカットALT+SHIFT+1を上書きできます。
  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`で新しいレジストリ設定を構成します。
  - 名前：HKEY_LOCAL_MACHINE_HotKey、種類：String
  - ショートカットの組み合わせを構成する形式は、C=0`|`1, A=0`|`1, S=0`|`1, W=0`|`1, K=valです。キーはコンマ「,」で区切る必要があります。キーの順序は問いません。
  - A、C、S、W、Kはキーであり、C=Control、A=ALT、S=SHIFT、W=Win、K=有効なキーです。Kに許可される値は、0〜9、a〜z、および任意の仮想キーコードです。
  - 例:
    - F10の場合、K=0x79を設定します
    - Ctrl + F10の場合、C=1, K=0x79を設定します
    - Alt + Aの場合、A=1, K=a または A=1, K=A または K=A, A=1を設定します

    - Ctrl + Alt + 5の場合、C=1, A=1, K=5 または A=1, K=5, C=1を設定します
    - Ctrl + Shift + F5の場合、A=1, S=1, K=0x74を設定します

注意:

レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターの使用は、お客様ご自身の責任において行ってください。編集する前に必ずレジストリをバックアップしてください。

- 複数および高解像度モニターのサポート。シングルセッションOSマシンでは、最大8台の4Kモニターがサポートされます。ユーザーは、モニターを任意の構成で配置でき、異なる解像度や向きのモニターを混在させることができます。モニターの数は、ホストコンピューターのGPU、ユーザーデバイス、および利用可能な帯域幅の機能によって制限されます。HDX 3D Proはすべてのモニター解像度をサポートしており、ホストコンピューターのGPUの機能によってのみ制限されます。
- 動的解像度。仮想デスクトップまたはアプリケーションウィンドウを任意の解像度にリサイズできます。**注:** 解像度を変更する唯一のサポートされている方法は、VDAセッションウィンドウのサイズを変更することです。VDAセッション内から解像度を変更すること（**コントロールパネル > デザイン**と**パーソナル設定 > ディスプレイ > 画面の解像度**を使用）はサポートされていません。
- NVIDIA vGPUアーキテクチャのサポート。HDX 3D ProはNVIDIA vGPUカードをサポートしています。詳細については、GPUパススルーおよびGPU共有に関するNVIDIA vGPUを参照してください。NVIDIA vGPUを使用すると、非仮想化オペレーティングシステムに展開されているものと同じNVIDIAグラフィックドライバーを使用して、複数のVMが単一の物理GPUに同時に直接アクセスできるようになります。
- Virtual Direct Graphics Acceleration (vDGA) を使用したVMware vSphereおよびVMware ESXのサポート - RDSワークロードとVDIワークロードの両方で、vDGAとHDX 3D Proを使用できます。
- VMware vSphere/ESX のサポート。
- Windows Server 2016のDiscrete Device Assignmentを使用したMicrosoft HyperVのサポート。
- Intel Xeon Processor E3ファミリーおよびIntel Data Center GPU Flexシリーズを使用したデータセンターグラフィックスのサポート。詳細については、`<https://www.intel.com/`

`content/www/us/en/products/details/discrete-gpus/data-center-gpu/flex-series.html>`を参照してください。

- AMD GPUのサポート。

> 注：
>
> AMD MxGPU（GPU仮想化）のサポートは、VMware vSphere vGPUでのみ機能します。Citrix HypervisorおよびHyper-Vは、GPUパススルーでサポートされます。詳細については、`<https://www.amd.com/en/graphics/workstation-virtual-graphics>`を参照してください。

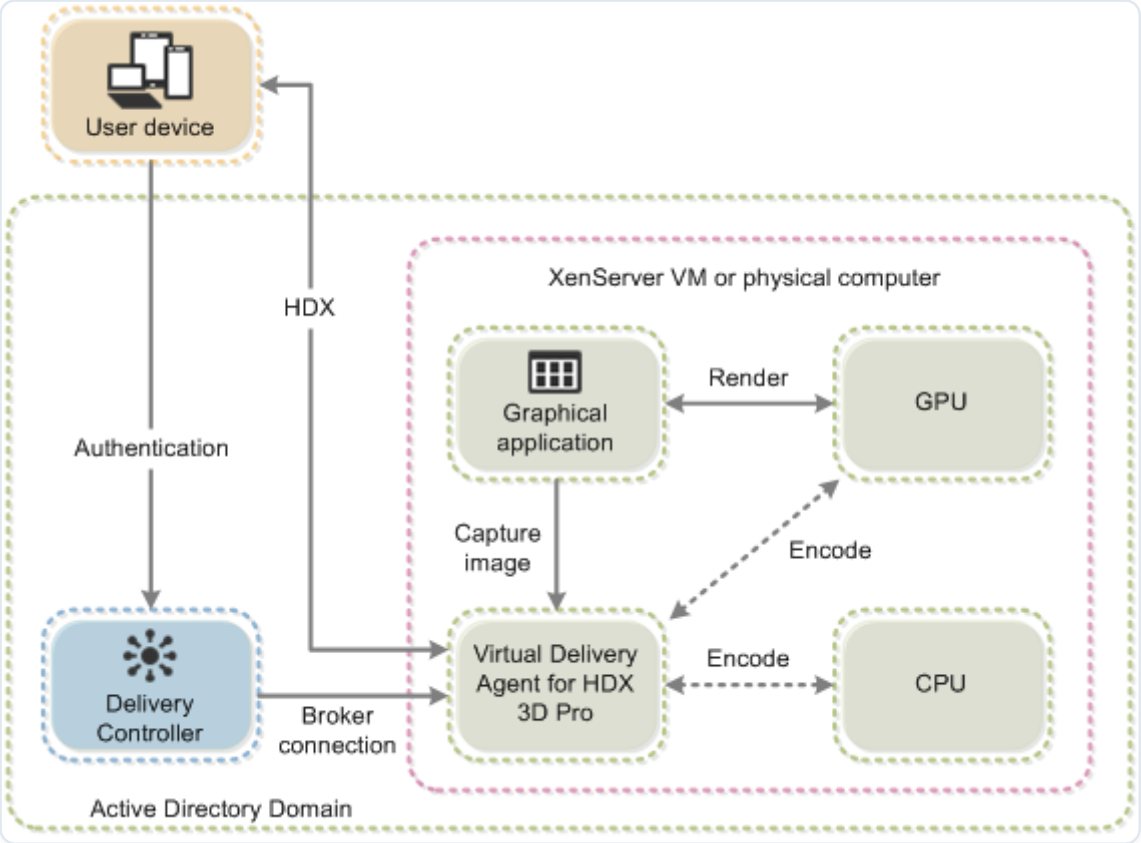
- NVIDIA GPU、AMD GPU、Intel GPU向けの高性能ビデオエンコーダーへのアクセス。ポリシー設定（デフォルトで有効）がこの機能を制御します。この機能により、H.264、H.265、またはAV1エンコーディング（利用可能な場合）にハードウェアエンコーディングを使用できます。このようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。詳細については、「グラフィックポリシー設定」を参照してください。

次の図に示すように：

- ユーザーがCitrix Workspace™アプリにログオンし、仮想アプリケーションまたはデスクトップにアクセスすると、Controllerがユーザーを認証します。その後、ControllerはHDX 3D Pro用VDAに接続し、グラフィックアプリケーションをホストするコンピューターへの接続を仲介します。

HDX 3D Pro用VDAは、ホスト上の適切なハードウェアを使用して、デスクトップ全体またはグラフィックアプリケーションのみのビューを圧縮します。

- デスクトップまたはアプリケーションのビューと、それらに対するユーザーの操作は、ホストコンピューターとユーザーデバイス間で送信されます。この送信は、Citrix WorkspaceアプリとHDX 3D Pro用VDA間の直接HDX接続を介して行われます。



HDX 3D Proのユーザーエクスペリエンスを最適化する

複数のユーザーが限られた帯域幅の接続（たとえば、支店など）を共有している場合、各ユーザーが利用できる帯域幅を制限するために、**セッション全体の帯域幅制限**ポリシー設定を使用することをお勧めします。この設定を使用すると、ユーザーがログオンおよびログオフする際に、利用可能な帯域幅が大きく変動しないようにできます。HDX 3D Proは利用可能なすべての帯域幅を使用するように自動的に調整されるため、ユーザーセッション中に利用可能な帯域幅が大きく変動すると、パフォーマンスに悪影響を及ぼす可能性があります。

たとえば、20人のユーザーが60 Mbpsの接続を共有している場合、各ユーザーが利用できる帯域幅は、同時ユーザー数に応じて3 Mbpsから60 Mbpsの間で変動する可能性があります。このシナリオでユーザーエクスペリエンスを最適化するには、ピーク時にユーザーごとに必要な帯域幅を決定し、常にその量にユーザーを制限します。

3Dマウスのユーザーの場合、汎用USBリダイレクト仮想チャネルの優先度を0に上げることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Centerの記事CTX128190を参照してください。

シンワイヤ

はじめに

Citrix HDXテクノロジーの一部であるThinwireは、Citrix Virtual Apps and Desktopsで使用されるCitrixのデフォルトのディスプレイリモートテクノロジーです。

ディスプレイリモートテクノロジーにより、あるマシンで生成されたグラフィックを、通常はネットワーク経由で別のマシンに送信して表示できます。

成功したディスプレイリモートソリューションは、ローカルPCと同様の高度にインタラクティブなユーザーエクスペリエンスを提供します。Thinwireは、さまざまな複雑で効率的な画像分析および圧縮技術を使用することで、このエクスペリエンスを実現します。Thinwireは、サーバーのスケーラビリティを最大化し、他のディスプレイリモートテクノロジーよりも少ない帯域幅を消費します。

このバランスにより、Thinwireはほとんどの一般的なビジネスユースケースに対応し、Citrix Virtual Apps and Desktopsのデフォルトのディスプレイリモートテクノロジーとして使用されています。

HDX™ スリーディープロ

デフォルト構成では、Thinwireは3Dまたは高度にインタラクティブなグラフィックを提供し、GPU（グラフィック処理ユニット）が存在する場合はそれを使用できます。ただし、GPUが存在するシナリオでは、**3Dグラフィックワークロード向けに最適化**または**視覚品質 > ロスレスビルド**ポリシーを使用してHDX 3D Proモードを有効にすることをお勧めします。これらのポリシーは、GPUが存在する場合に、ビデオコーデック（H.264、H.265、またはAV1）を使用して画面全体をハードウェアアクセラレーションでエンコードするようにThinwireを構成します。これにより、3Dプロフェッショナルグラフィックの操作がよりスムーズになります。詳細については、H.264 ロスレスビルド、HDX 3D Pro、およびWindowsシングルセッションOSのGPUアクセラレーションを参照してください。

要件

Thinwireは、Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows Server 2012 R2、Windows 10、Windows 7などの最新のオペレーティングシステム向けに最適化されています。Windows Server 2008 R2の場合、レガシーグラフィックモードが推奨されます。これらのユースケースに対してCitrixが推奨するポリシー設定の組み合わせを提供するには、組み込みのCitrixポリシーテンプレート、High Server Scalability-Legacy OSおよびOptimized for WAN-Legacy OSを使用してください。

注:

このリリースでは、レガシーグラフィックモードはサポートされていません。これは、XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、および以前のVDAリリースをWindows 7およびWindows 2008 R2で使用する場合の後方互換性のために含まれています。

- Thinwireの動作を制御するポリシー設定 - **圧縮にビデオコーデックを使用**は、Citrix Virtual Apps and Desktops 7 1808以降、およびXenApp and XenDesktop 7.6 FP3以降のVDAバージョンで利用可能です。**優先時にビデオコーデックを使用**オプションは、Citrix Virtual Apps and Desktops 7 1808以降、およびXenApp and XenDesktop 7.9以降のVDAバージョンでデフォルト設定です。
- すべてのCitrix Workspace™アプリはThinwireをサポートしています。一部のCitrix Workspaceアプリは、帯域幅使用量を削減するための8ビットまたは16ビットグラフィックなど、他のアプリではサポートされていないThinwireの機能をサポートしている場合があります。このような機能のサポートは、Citrix Workspaceアプリによって自動的にネゴシエートされます。
- Thinwireは、マルチモニターおよび高解像度のシナリオで、より多くのサーバーリソース（CPU、メモリ）を使用します。Thinwireが使用するリソースの量を調整することは可能ですが、結果として帯域幅の使用量が増加する可能性があります。
- 低帯域幅または高遅延のシナリオでは、インタラクティブ性を向上させるために8ビットまたは16ビットのグラフィックを有効にすることを検討してください。特に8ビットの色深度では、視覚的な品質が影響を受ける可能性があります。

エンコード方法

Thinwireは、ポリシーとクライアントの機能に応じて、2つの異なるエンコードモードで動作できます。

- Adaptive JPEGを使用したThinwire **圧縮にビデオコーデックを使用する**ポリシー設定: **ビデオコーデックを使用しない**
- Selective H.264、H.265、またはAV1を使用したThinwire **圧縮にビデオコーデックを使用する**ポリシー設定: **優先される場合はビデオコーデックを使用する** または **アクティブに変化する領域の場合**
- フルスクリーンH.264、H.265、またはAV1を使用したThinwire **圧縮にビデオコーデックを使用する**ポリシー設定: **画面全体の場合**

H.265

H.265としても知られるHigh Efficiency Video Coding (HEVC) は、H.264の後継です。 H.265ビデオコーデックを使用したハードウェアエンコードは、以下のGPUでサポートされています。

- NVIDIA MaxwellベースのGPU以降
- Intel 第6世代GPU以降
- AMD RavenベースのGPU以降

AV1

CitrixはAV1ビデオコーデックのサポートを追加しました。AV1の利点は、H.264およびH.265と比較して、優れた画像圧縮、より良い画質、および低い帯域幅使用量を持つことです。

AV1の以下の要件を満たす必要があります。

- NVIDIA GPUの場合はVDA 2305以降、または
- Intel GPUの場合はVDA 2308以降

以下のGPUがエンコードに対応しています。

- NVIDIA Ada LovelaceベースのGPU
- インテル ARC または インテル データセンター GPU Flex シリーズ GPU

NVIDIAのAda Lovelace GPUの詳細については、「ADA architecture」を参照してください。

IntelのARCワークステーションおよびデータセンターFlex Series GPUの詳細については、「Flex series」と「Overview」を参照してください。

自動ビデオコーデック選択

圧縮ポリシーの**Use video codec**が有効になっている場合、またはVDAで「3Dグラフィックワークロード用に最適化」が有効になっている場合、使用する最適なビデオコーデックを自動的に検出できます。Citrix Workspaceアプリfor Windowsのインストール中に、エンドポイントのデコード機能が評価されます。この情報に基づいて、Citrix Workspaceアプリfor Windowsは、接続時にVDAと使用する最適なコーデックをネゴシエートします。ビデオコーデックが評価される順序は次のとおりです。

- AV1
- H.265
- H.264

自動選択は、これらのコーデックの4:2:0バリアントにのみ適用されます。**Visual Quality**設定が「Build-to-Lossless」または「Always Lossless」に設定されており、かつAllow Visually Losslessが「enabled」に設定されている場合、ビデオコーデックの自動選択は無効になります。

リソースに接続すると、Citrix WorkspaceアプリはエンドポイントのH.265およびAV1のデコード機能をテストし、その機能をレジストリに保存します。その後、Citrix Workspaceアプリは使用する最適なビデオコーデックを自動的に選択し、VDAとネゴシエートします。VDAとクライアントの両方がH.265とAV1を使用できる場合、AV1がビデオコーデックとして選択されます。VDAまたはクライアントのいずれかでAV1が利用できない場合、H.265がネゴシエートされます。H.265もどちらでも利用できない場合、セッションはH.264をビデオコーデックとして使用します。

> **注:**
>
> この機能はデフォルトで有効になっています。この動作は、新しいクライアント側のレジストリ設定`DisableDecoderCaps`を設定することで変更できます。

> ビデオコーデックの自動選択を無効にするには、「DisableDecoderCaps」を`HKLM\Software\WOW6432Node\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1`または`HKCU\Software\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1`として設定します。

これらの値のいずれかが1に設定されている場合、ビデオコーデックの自動選択は使用されません。 グラフィックステータスインジケーターとHDXモニターでビデオコーデックを監視できます。

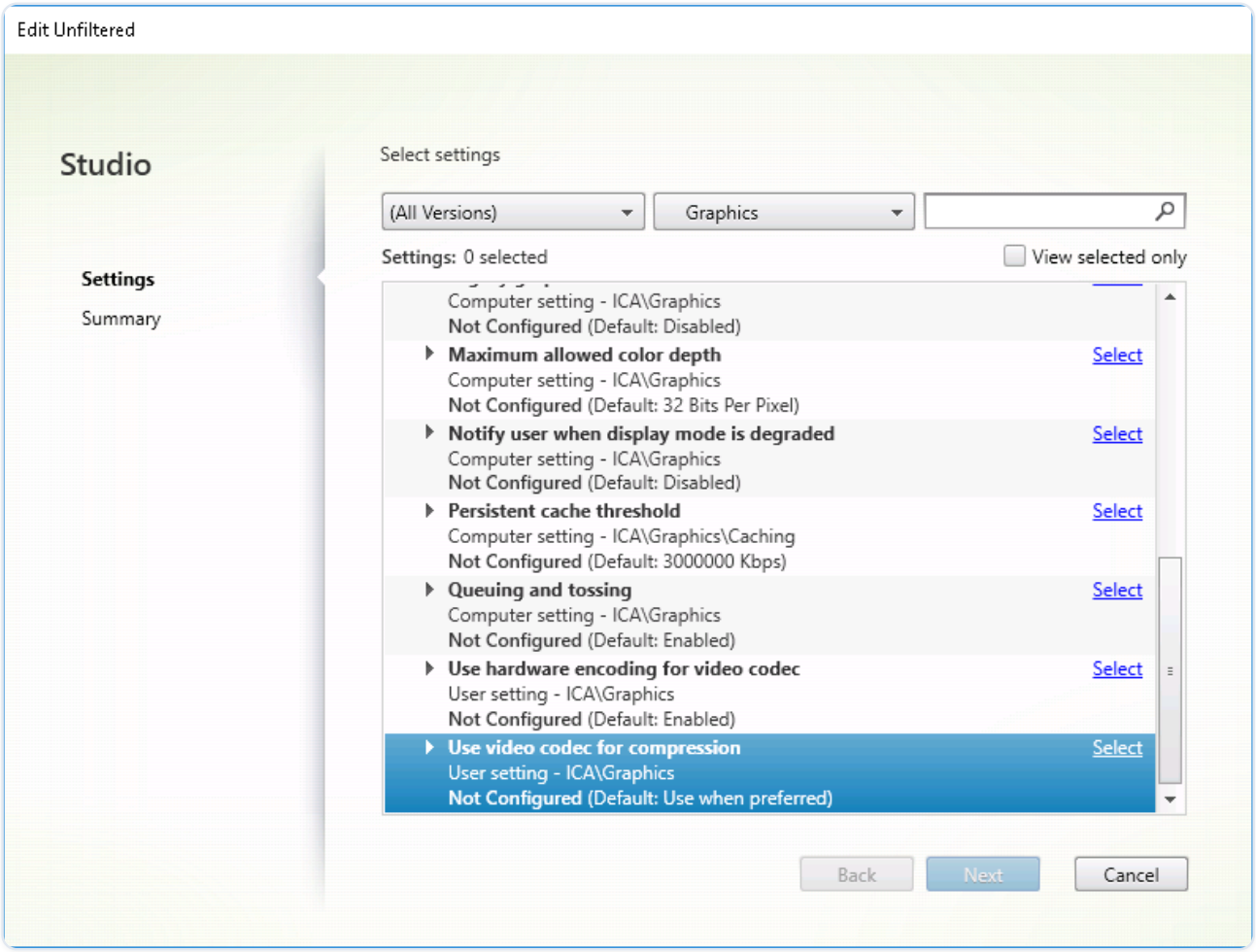
構成

Thinwireは、デフォルトのディスプレイリモートテクノロジーです。

次のグラフィックポリシー設定は、デフォルトを設定し、さまざまなユースケースの代替手段を提供します。

- 圧縮にビデオコーデックを使用する
  - **優先される場合はビデオコーデックを使用する**。これはデフォルト設定です。追加の構成は必要ありません。この設定をデフォルトのままにすることで、すべてのCitrix接続でThinwireが選択され、スケーラビリティ、帯域幅、および一般的なデスクトップワークロードの優れた画質のために最適化されます。これは、**アクティブに変化する領域の場合**と機能的に同等です。

- このポリシー設定の他のオプションは、さまざまなユースケースで他のテクノロジーとThinwireを引き続き使用します。例:
  - **アクティブに変化する領域の場合**。Thinwireのアダプティブディスプレイテクノロジーは、移動する画像（ビデオ、移動中の3D）を識別し、画像が移動している画面の一部でのみH.264、H.265、またはAV1を使用します。
  - **画面全体の場合**。3Dグラフィックを多用するケースで、ユーザーエクスペリエンスと帯域幅を向上させるために、H.264、H.265、またはAV1を使用したフルスクリーンでThinwireを提供します。H.264 4:2:0の場合（**視覚的にロスレス**ポリシーが無効になっている場合）、最終画像はピクセルパーフェクト（ロスレス）ではなく、特定のシナリオには適さない可能性があります。そのような場合は、代わりにH.264 Build to losslessまたはH.265 Build to losslessの使用を検討してください。



次の視覚表示ポリシー設定を含む、さまざまな他のポリシー設定を使用して、ディスプレイリモートテクノロジーのパフォーマンスを微調整できます。Thinwireはそれらすべてをサポートします。

- 単純なグラフィックの優先色深度
- ターゲットフレームレート

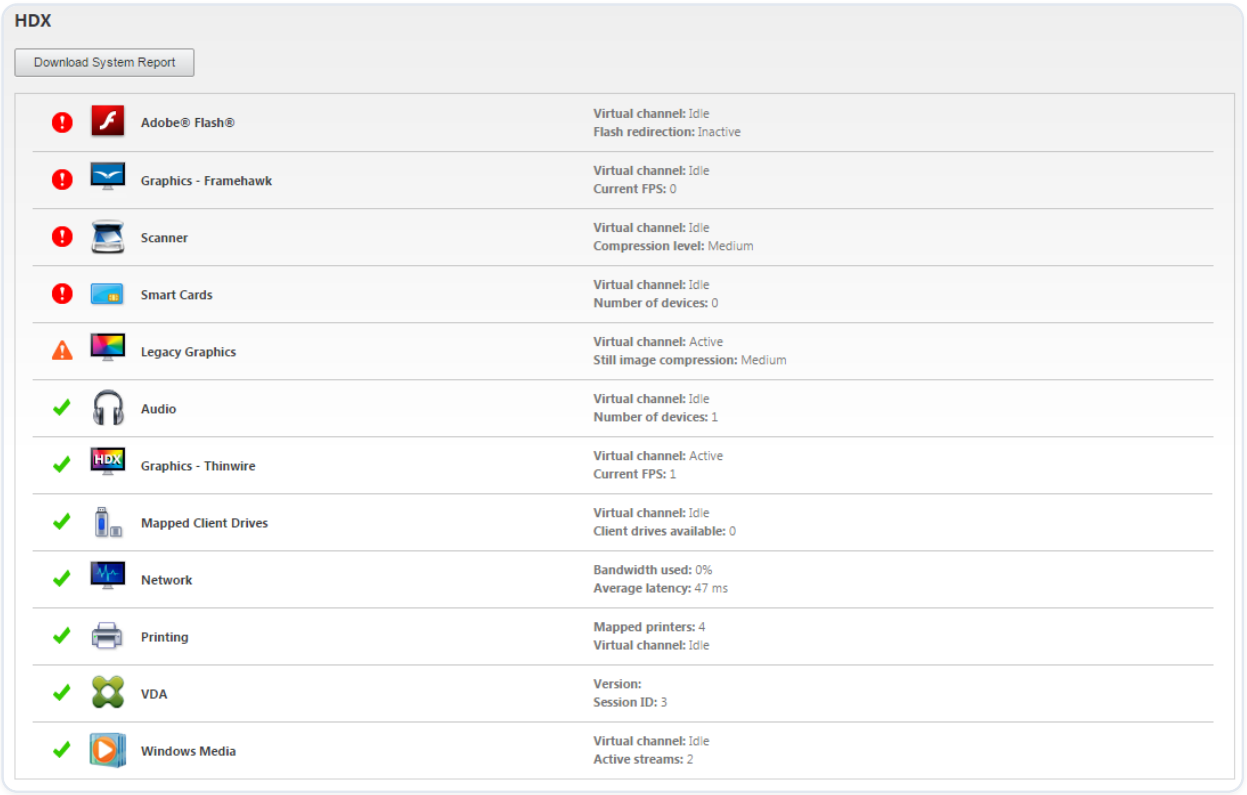
- 視覚品質

さまざまなビジネスユースケースに対応するCitrix推奨のポリシー設定の組み合わせを取得するには、組み込みの(/ja-jp/citrix-virtual-apps-desktops/2311/policies/policies-templates.html)を使用します。**High Server Scalability**および**Very High Definition User Experience**テンプレートは、組織の優先順位とユーザーの期待に最適なポリシー設定の組み合わせでThinwireを使用します。

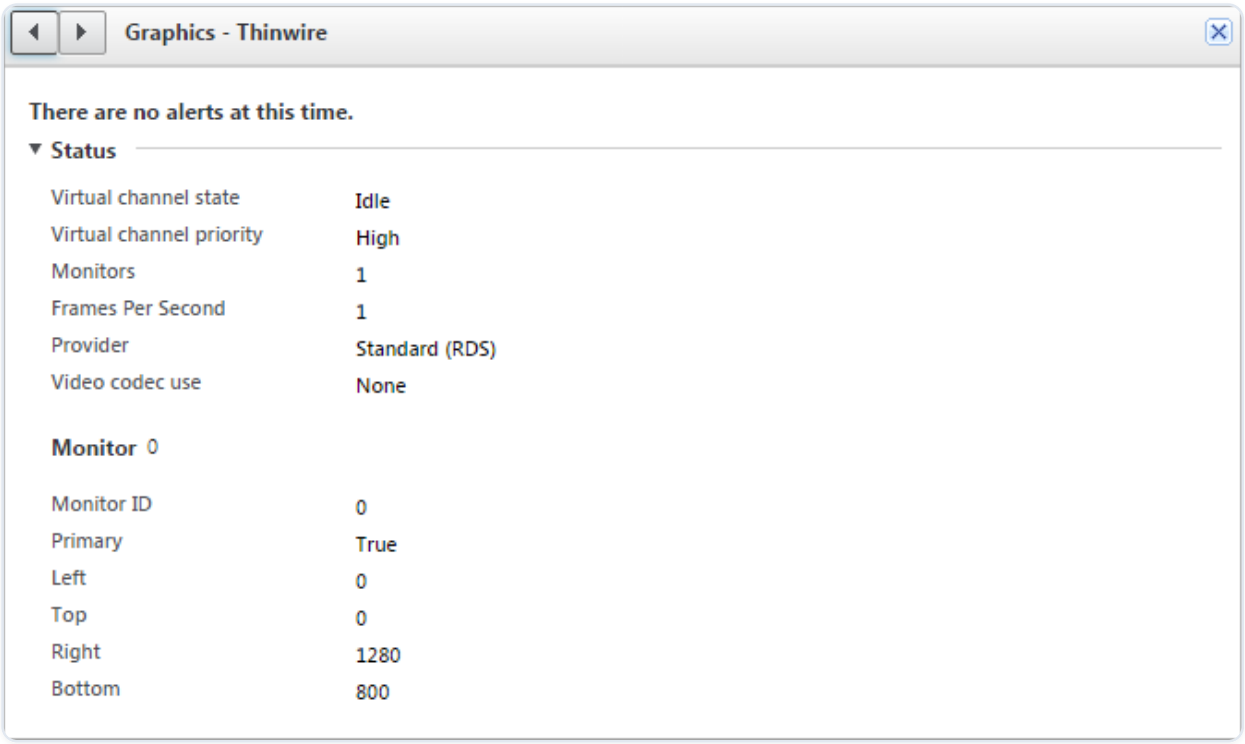
Thinwireの監視

Citrix DirectorからThinwireの使用状況とパフォーマンスを監視できます。HDX仮想チャネルの詳細ビューには、任意のセッションでThinwireのトラブルシューティングと監視に役立つ情報が含まれています。Thinwire関連のメトリックを表示するには:

1. Directorで、ユーザー、マシン、またはエンドポイントを検索し、アクティブなセッションを開いて**Details**をクリックします。または、**Filters** > **Sessions** > **All Sessions**を選択し、アクティブなセッションを開いて**Details**をクリックします。
2. **HDX**パネルまでスクロールします。



3. **グラフィック - Thinwire**を選択します。



ロスレス圧縮コーデック (MDRLE)

一般的なデスクトップセッションでは、ほとんどの画像は単純なグラフィックまたはテキスト領域です。Thinwireはこれらの領域を特定し、2DRLEコーデックを使用してロスレスエンコーディングのためにこれらの領域を選択します。Citrix Workspaceアプリのクライアント側では、これらの要素はセッション表示のためにCitrix Workspaceアプリ側の2DRLEデコーダーを使用してデコードされます。

XenAppおよびXenDesktop 7.17では、2DRLEコーデックよりも一般的なデスクトップセッションで消費帯域幅が少ない、より高い圧縮率のMDRLEコーデックを追加しました。この新しいコーデックは、サーバーのスケーラビリティに影響を与えません。

帯域幅が低いということは、通常、セッションの対話性が向上し（特に共有または制約のあるリンクで）、コストが削減されることを意味します。たとえば、MDRLEコーデックを使用した場合の予想帯域幅消費量は、一般的なOfficeのようなワークロードの場合、XenAppおよびXenDesktop 7.15 LTSRと比較して約10～15%少なくなります。

MDRLEコーデックには構成は不要です。Citrix WorkspaceアプリがMDRLEデコードをサポートしている場合、VDAはVDA MDRLEエンコーディングとCitrix WorkspaceアプリMDRLEデコードを使用します。Citrix WorkspaceアプリがMDRLEデコードをサポートしていない場合、VDAは自動的に2DRLEエンコーディングにフォールバックします。

MDRLEの要件:

- Citrix Virtual Apps and Desktopsの最小バージョン7 1808 VDA

- XenAppおよびXenDesktopの最小バージョン7.17 VDA
- Windows向けCitrix Workspaceアプリの最小バージョン1808
- Windows向けCitrix Receiverの最小バージョン4.11

プログレッシブモード

Citrix Virtual Apps and Desktops 1808では、プログレッシブモードが導入され、デフォルトで有効になりました。ネットワーク条件が制限されている場合（デフォルト：帯域幅 < 2 Mbps、または遅延 > 200 ms）、Thinwireは画面アクティビティ中のインタラクティブ性を向上させるために、テキストと静止画像の圧縮を強化しました。画面アクティビティが停止すると、高度に圧縮されたテキストと画像は、ランダムなブロック方式で段階的にシャープ化されます。このように圧縮とシャープ化を行うことで、全体的なインタラクティブ性は向上しますが、キャッシュ効率が低下し、帯域幅の使用量が増加します。

Citrix Virtual Apps and Desktops 1906以降、プログレッシブモードはデフォルトで無効になっています。現在、別の方法を使用しています。静止画の品質は、ネットワーク条件に基づいており、各**視覚品質**設定の事前定義された最小値と最大値の間で変動します。明示的なシャープ化ステップがないため、Thinwireは画像配信を最適化し、キャッシュ効率を維持しながら、プログレッシブモードのほぼすべての利点を提供します。

プログレッシブモードの動作を変更する

レジストリキーを使用してプログレッシブモードの状態を変更できます。詳しくは、レジストリで管理される機能の一覧にあるプログレッシブモードを参照してください。

ロスレスへのビルド

Build to losslessは、対話性と最終的な画質のためにグラフィック配信を最適化する特別なThinwire構成です。この設定は、**視覚品質**ポリシーを**Build to lossless**に設定することで有効にできます。

ビルドトゥロスレスは、画面アクティビティ中にH.264、H.265、またはAV1を使用して画面を圧縮し、アクティビティが停止するとピクセルパーフェクト（ロスレス）にシャープ化します。非可逆圧縮の画質は、利用可能なリソースに合わせて調整され、可能な限り最高のフレームレートを維持します。シャープ化のステップは段階的に実行されます。たとえば、モデルを選択して回転させる場合などです。

ビルドトゥロスレスは、ハードウェアアクセラレーションを含む画面全体にビデオコーデックを使用するすべての利点を提供しますが、最終的に保証されたロスレス画面という追加の利点があります。これは、最終的なピクセルパーフェクトな画像を必要とする3Dタイプのワークロードにとって重要です。たとえば、医療画像の操作などです。また、H.264の**ビルドトゥロスレス**は、フ

ルスクリーンH.264 4:4:4よりも少ないリソースを使用します。その結果、**ビルドトゥロスレス**を使用すると、通常、視覚的にロスレスなH.264 4:4:4よりも高いフレームレートが得られます。

> **注：**
>
> ビルドトゥロスレスを使用している場合、ビデオコーデックの使用を無効にできます。**ビデオコーデックの使用**ポリシーを`Do not use video codec`に設定するだけです。これにより、動画は代わりにAdaptive JPEGでエンコードされます。

視覚的にロスレスなエンコード

視覚的にロスレスなエンコーディングは、ビデオコーデック圧縮にクロマサブサンプリングされたYUV 4:2:0カラースペースの代わりにYUV 4:4:4カラースペースを使用します。これにより、カラースペース変換中に色情報が失われることがなく、デコード後には元のRGB画像と視覚的に区別できなくなります。

次の例を考えてみましょう。ビデオコーデックを使用して画面全体を圧縮する場合、4:2:0の色圧縮はテキストのような高コントラストの詳細を劣化させ、ぼやけて読みにくくする可能性があります。対照的に、4:4:4はほぼすべての色情報を保持し、視覚的に認識できる劣化を示しません。



ピクセルパーフェクトな品質や正確な色表示を必要とするワークロードは、視覚的にロスレスなエンコーディングの恩恵を受けることができます。

視覚的にロスレスなエンコーディングは、H.264とH.265の両方で利用可能です。H.264 4:4:4エンコーディングは純粋にソフトウェアベースのソリューションであるため、VDAとクライアントの両方でCPU使用率に大きな影響を与える可能性があります。これにより、フレームレートにも影響が出る場合があります。

H.265 4:4:4のサポートはCitrix Workspaceアプリ2305のリリースで追加され、ThinwireがH.265 4:4:4エンコーディングのためにVDAとクライアントの両方でGPUを使用できるようになり、パフォーマンスが大幅に向上しました。

視覚的にロスレスな4:4:4エンコーディングを許可するには、2つのポリシーを有効にする必要があります。

- **視覚品質**: `Build to Lossless`または`Always Lossless`に設定します。
- **視覚的にロスレスを許可**: `Enabled`に設定します。

> **注:**
>
> **視覚的にロスレスを許可**が有効になっていない場合、Thinwireエンコーダーは`Build to lossless`または`Always Lossless`のいずれかに切り替わります。

> H.265 4:4:4の視覚的にロスレスには、追加の要件があります。

- NVIDIA GPUにはVDAバージョン2209以降が必要です。
- Intel GPUにはVDAバージョン2308以降が必要です。

次の例を考えてみましょう。ビデオコーデックを使用して画面全体を圧縮する場合、4:2:0の色圧縮は、テキストのような高コントラストの詳細を劣化させ、ぼやけて読みにくくする可能性があります。対照的に、4:4:4はほぼすべての色情報を保持し、視覚的に認識できる劣化を示しません。



クライアントには、Citrix Workspaceアプリ for Windows バージョン2305が必要です（バージョン2309.1を推奨）。

H.265 4:4:4のハードウェアデコードは、以下のクライアントデバイスGPUで可能です。

H.265 4:4:4のサポートは、Citrix Workspaceアプリ2305のリリースで追加され、ThinwireがVDAとクライアントの両方のGPUをH.265 4:4:4エンコードに使用できるようになり、パフォーマンスが大幅に向上しました。

視覚的にロスレスな4:4:4エンコードを許可するには、2つのポリシーを有効にする必要があります。

- **視覚品質**: `Build to Lossless`または`Always Lossless`に設定します
- **視覚的にロスレスを許可**: `Enabled`に設定します

> **注:**
>
> **視覚的にロスレスを許可**が有効になっていない場合、Thinwireエンコーダーは`Build to lossless`または`Always Lossless`に切り替わります。

> H.265 4:4:4 視覚的にロスレスには、追加の要件があります。

- NVIDIA GPU には、VDA バージョン 2209 以降が必要です
- Intel GPU には、VDA バージョン 2308 以降が必要です

H.265 4:4:4 は、以下の GPU でサポートされています。

- NVIDIA Pascal世代以降のGPU
- Intel 第10世代以降のGPU

クライアントには、Citrix Workspace app for Windows バージョン 2305 が必要です（バージョン 2309.1 を推奨）。

H.265 4:4:4 のハードウェアデコードは、以下のクライアントデバイスGPUで可能です。

- NVIDIA Turing世代以降のGPU
- Intel 第10世代以降のGPU

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。元のドキュメントの内容を変更することなく、セッション画面全体に表示されるテキストのレイヤーであるウォーターマークを指定できます。テキストベースのセッションウォーターマークにはVDAのサポートが必要です。

> **重要:**
>
> テキストベースのセッションウォーターマークはセキュリティ機能ではありません。このソリューションはデータ盗難を完全に防ぐものではありませんが、ある程度の抑止力と追跡可能性を提供します。この機能を使用した場合の完全な情報追跡可能性を保証するものではありませんが、必要に応じて他のセキュリティソリューションと組み合わせて使用することをお勧めします。

> セッションウォーターマークはテキストであり、ユーザーに配信されるセッションに適用されます。セッションウォーターマークには、データ盗難を追跡するための情報が含まれています。最も重要なデータは、スクリーンイメージが取得された現在のセッションのログオンユーザーのIDです。データ漏洩をより効果的に追跡するために、サーバーまたはクライアントのインターネットプロトコルアドレスや接続時間などの他の情報を含めます。

ユーザーエクスペリエンスを調整するには、セッションウォーターマークポリシー設定 を使用して、画面上の配置とウォーターマークの外観を構成します。

要件:

仮想デリバリーエージェント:

マルチセッションOS 7.17 シングルセッションOS 7.17

制限事項:

- セッションウォーターマークは、ローカルアプリアクセス、Windowsメディアリダイレクト、MediaStream、ブラウザコンテンツリダイレクト、およびHTML5ビデオリダイレクトが使用されているセッションではサポートされていません。セッションウォーターマークを使用するには、これらの機能が無効になっていることを確認してください。
- セッションが全画面ハードウェアアクセラレーションモード（全画面H.264またはH.265エンコーディング）で実行されている場合、セッションウォーターマークはサポートされず、表示されません。
- これらのHDX™ポリシーを設定すると、ウォーターマーク設定は有効にならず、セッション表示にウォーターマークは表示されません。

ビデオコーデックにハードウェアエンコーディングを使用 を **有効 圧縮にビデオコーデックを使用** に **画面全体**

- これらのHDXポリシーを設定すると、動作は未定義となり、ウォーターマークが表示されない場合があります。

  ビデオコーデックにハードウェアエンコーディングを使用 を **有効 圧縮にビデオコーデックを使用** を **優先する場合にビデオコーデックを使用**

  ウォーターマークが表示されるようにするには、「**ビデオコーデックにハードウェアエンコードを使用する**」を「**無効**」に設定するか、「**圧縮にビデオコーデックを使用する**」を「**アクティブに変更される領域の場合**」または「**ビデオコーデックを使用しない**」に設定します。
- セッションウォーターマークは、Thinwireグラフィックモードのみをサポートします。

- セッションレコーディングを使用している場合、記録されたセッションにはウォーターマークは含まれません。
- Windowsリモートアシスタンスを使用している場合、ウォーターマークは表示されません。
- ユーザーが画面をキャプチャするために **Print Screen** キーを押した場合、VDA側でキャプチャされた画面にはウォーターマークは含まれません。キャプチャされた画像がコピーされるのを防ぐための対策を講じることをお勧めします。

画面共有

画面共有を使用すると、ユーザーは画面コンテンツ、キーボード、マウスコントロールを含むCitrix Virtual Desktopセッションを他のユーザーと共有できます。

システム要件

- Windows: シングルセッションまたはマルチセッションOS VDA
- Linux: Linuxセッションの共有に関する詳細については、Linux VDAドキュメントを参照してください。
- デスクトップセッションのみを共有できます。
- セッションをホストするVDAと、共有セッションに接続するマシンとの間にネットワーク接続が必要です。ネットワークポート要件は、使用中のICAポート（TCP/UDP 1494または2598）と、画面共有ポリシーの構成（デフォルトではTCP 52525〜52625）に基づいています。

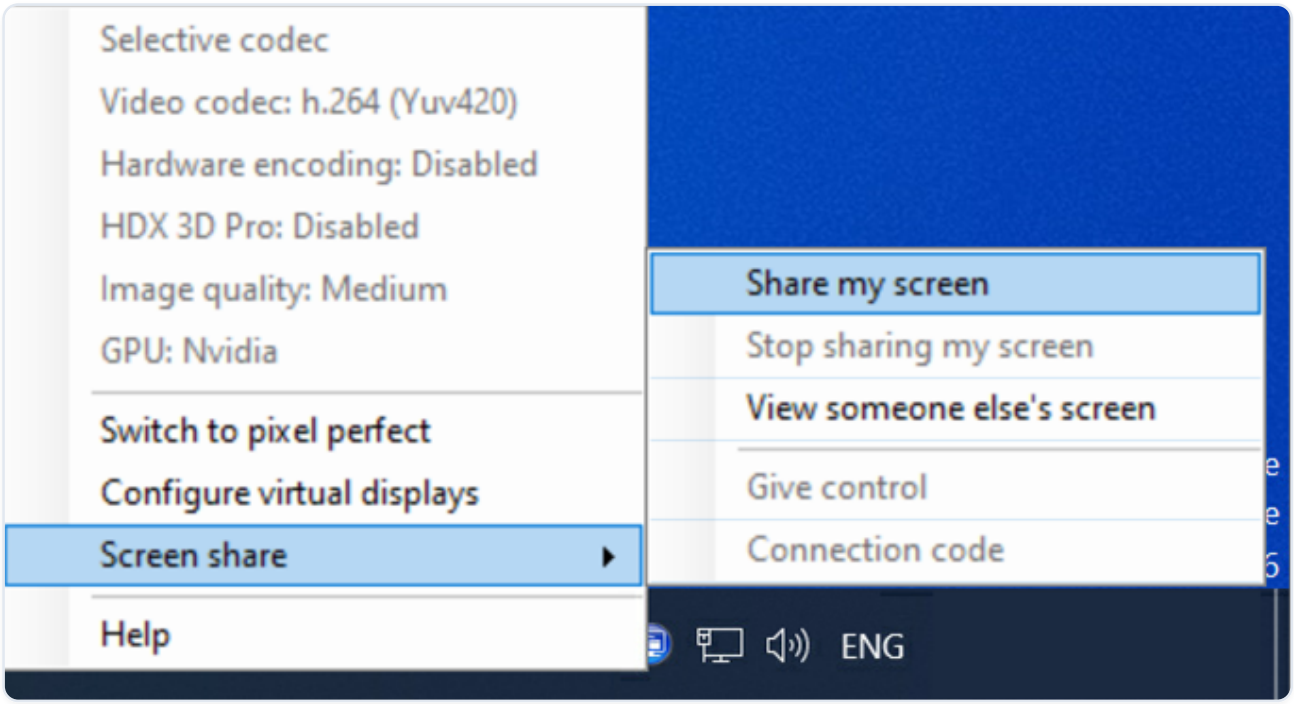
構成

画面共有はCitrixポリシーを使用して有効にする必要があります。画面共有はデフォルトで無効になっています。画面共有ポリシーを構成して、この機能を有効または無効にし、使用可能なネットワークポート範囲を割り当てます。

グラフィックステータスインジケーターポリシーを有効にして、セッションの共有と接続の制御を含むユーザーインターフェイスを表示します。

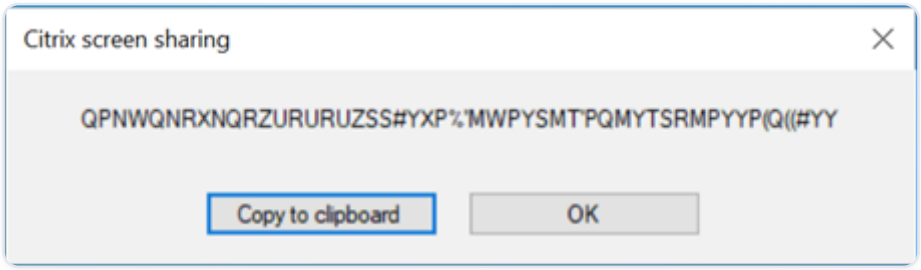
セッションの共有

セッションを共有するには、Windowsの通知領域にあるHDX™グラフィックステータスインジケーターアイコンを探します。アイコンを右クリックしてメニューを表示し、**画面共有 > 自分の画面を共有**を選択します。



クリップボードにコピーをクリックするか、ダイアログボックスに表示されている文字列全体を手動で選択してコピーします。その文字列は、電子メールやIMクライアントなど、選択したアプリケーションに貼り付けて、他のユーザーに配布できます。

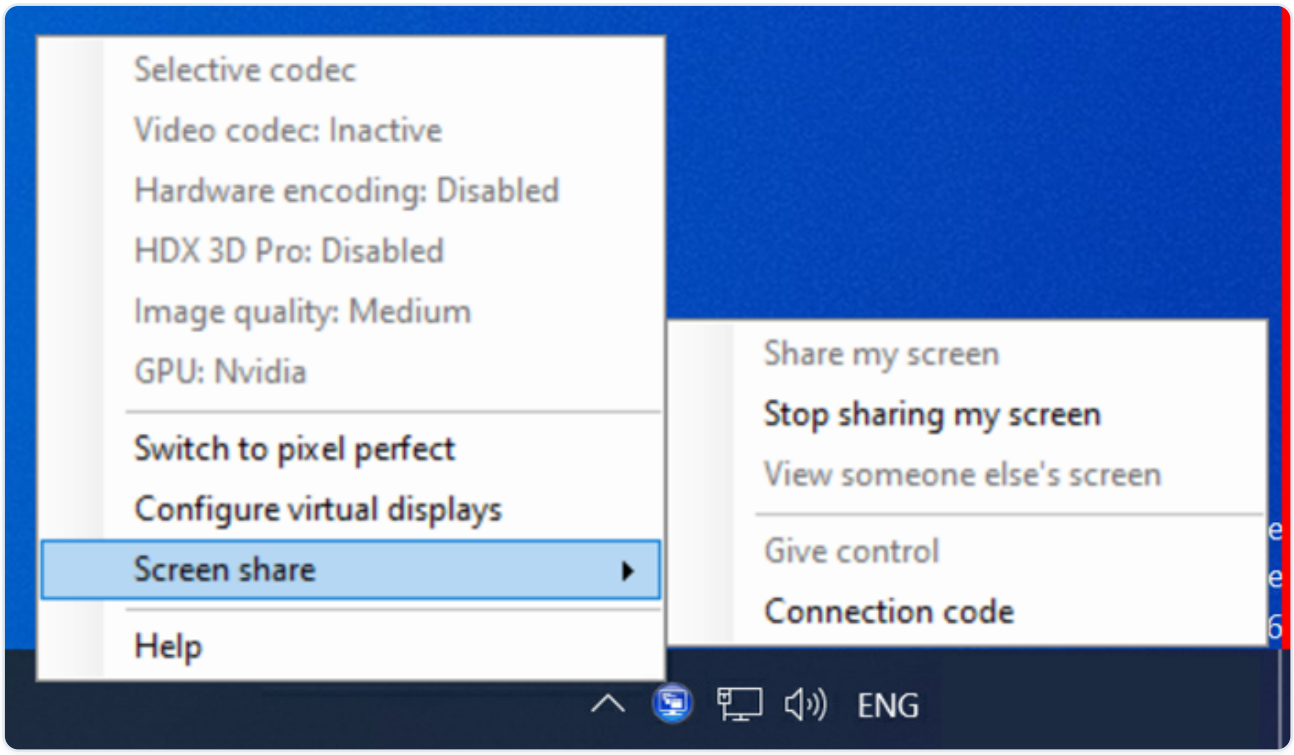
OKまたは**x**をクリックしてダイアログボックスを閉じます。セッションが共有されている間はいつでも、**画面共有 > 接続コード**メニューオプションから接続コードを取得できます。



画面の周りに赤い枠線が表示され、セッションが共有されており、他のユーザーから見える状態であることを示します。

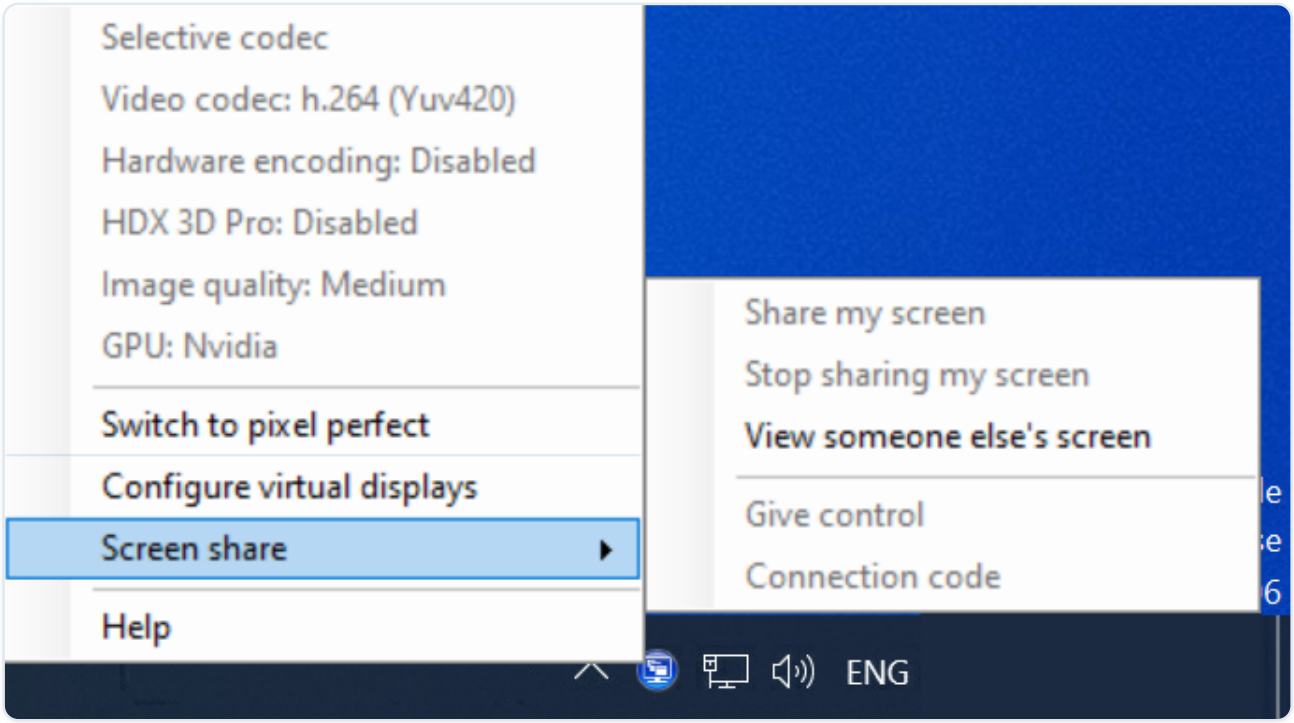
画面共有 > 制御を付与 メニューオプションを使用して、キーボードとマウスの制御を他のユーザーと共有することもできます。

画面共有 > 画面共有を停止 メニューオプションを使用して、セッションの共有を停止し、すべてのユーザーを切断します。

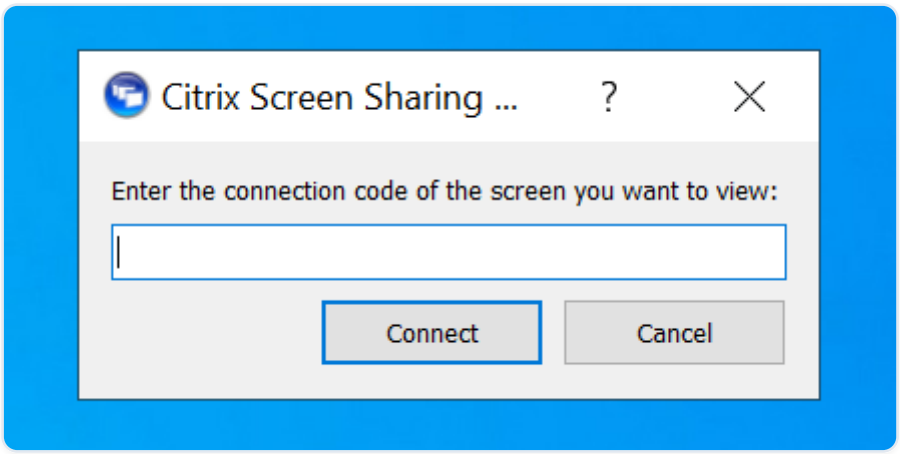


共有セッションへの接続

他のユーザーのセッションに接続するには、Windows の通知領域にある HDX グラフィックステータスインジケーターアイコンを探します。それを右クリックしてメニューを表示し、**画面共有 > 他のユーザーの画面を表示** を選択します。

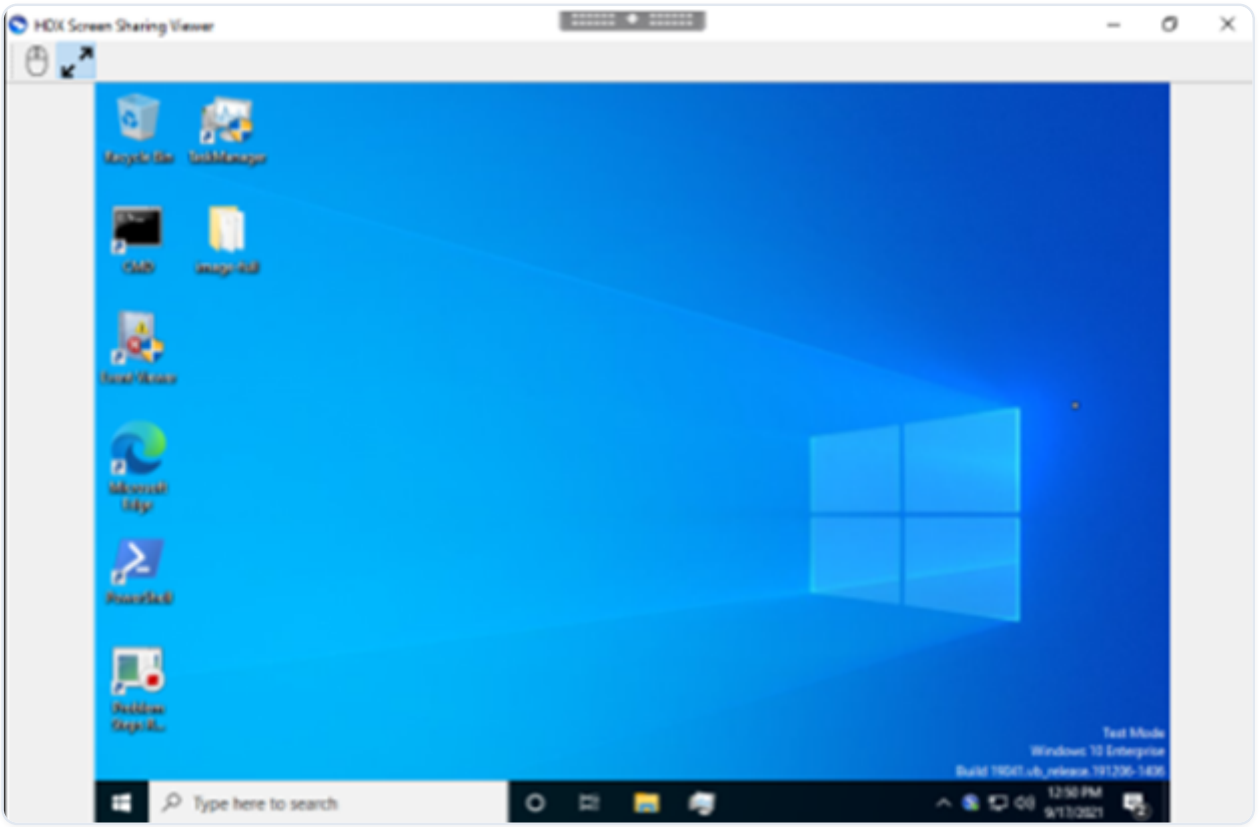


セッションを共有しているユーザーから提供された接続文字列をテキストボックスに入力または貼り付けます。**接続** をクリックして接続を確立します。



HDX 画面共有ビューア ウィンドウの左上隅にあるマウスアイコンをクリックすると、キーボードとマウスの制御を要求できます。

HDX 画面共有ビューア ウィンドウを閉じると、いつでも共有セッションから切断できます。



その他の考慮事項

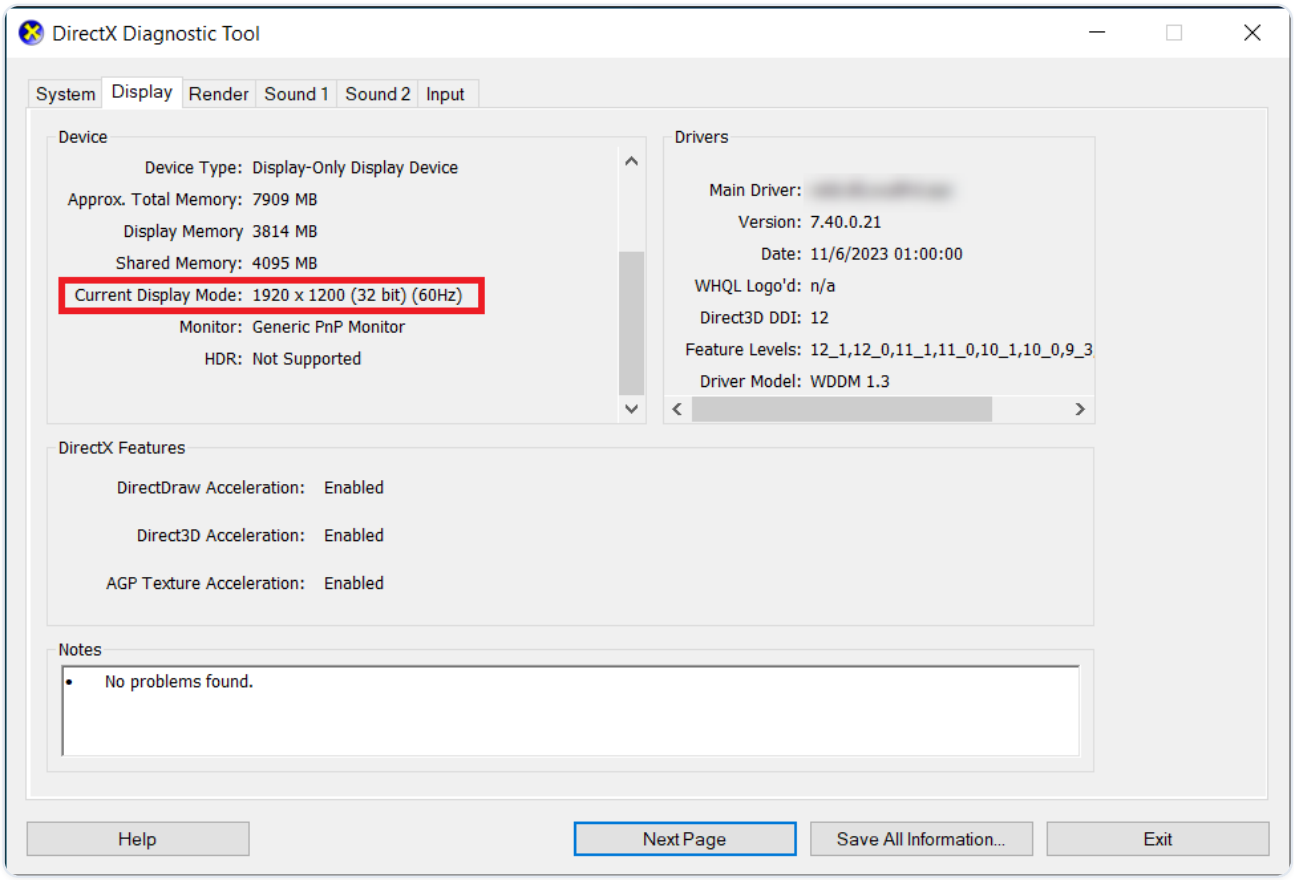
- 画面共有ビューアアプリケーションは、VDA に *C:\Program Files\Citrix\HDX\bin\TwPlayer.exe* として含まれており、Virtual Apps Server を使用して 公開アプリケーション として展開される場合があります。この代替展開モデルにより、仮想デスクトップにアクセスできないユーザーとのコラボレーションが可能になります。

- 画面共有ポリシーのネットワークポート範囲を使用して、共有セッションに接続できるユーザー数を制限できます。ユーザーごとに1つのポートが必要です。デフォルトの範囲では、最大100人のユーザーが許可されます。
- セッションに接続されているすべてのモニターが共有されます。個々のモニターを選択することはできません。
- H.265ビデオコーデックはサポートされていません。

アダプティブ リフレッシュレート

新しいスケーラビリティの向上により、HDX™ は仮想モニターのリフレッシュ レートを設定されたターゲット FPS ポリシーに一致させます。アダプティブ リフレッシュ レート (ARR) は、シングルセッション VDA とマルチセッション VDA の両方で利用でき、GPU アクセラレーションシナリオと非 GPU シナリオの両方で機能します。

ターゲットフレームレート(/en-us/citrix-virtual-apps-desktops/2311/media/targetframerate_60.png)



> **注**

アダプティブ リフレッシュ レートは、Citrix Indirect Display または IDD が使用されている場合 (Citrix Virtual Apps and Desktops™ のデフォルト通り) にのみ利用可能であり、ベンダー提供のディスプレイアダプターを使用している場合は利用できません。

マルチメディア

HDX™ テクノロジースタックは、2つの補完的なアプローチを通じてマルチメディアアプリケーションの配信をサポートします。

- サーバー側レンダリングによるマルチメディア配信
- クライアント側レンダリングによるマルチメディアリダイレクト

この戦略により、優れたユーザーエクスペリエンスで幅広いマルチメディア形式を配信できると同時に、サーバーのスケーラビリティを最大化してユーザーあたりのコストを削減できます。

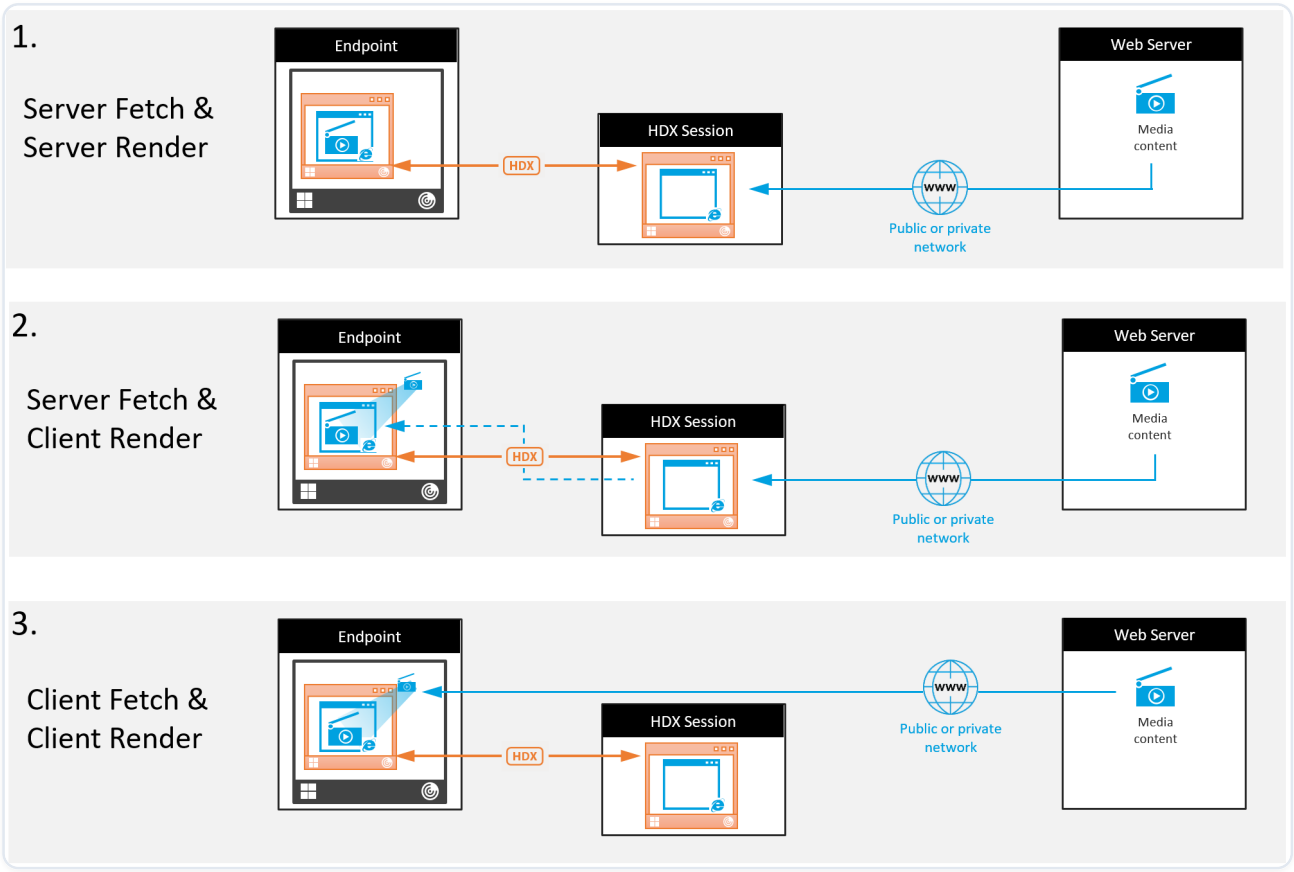
サーバーレンダリングによるマルチメディア配信では、オーディオおよびビデオコンテンツは、アプリケーションによってCitrix Virtual Apps and Desktopsサーバー上でデコードおよびレンダリングされます。その後、コンテンツは圧縮され、ICAプロトコルを使用してユーザーデバイス上のCitrix Workspaceアプリに配信されます。この方法は、さまざまなアプリケーションやメディア形式との互換性を最大限に高めます。ビデオ処理は計算負荷が高いため、サーバーレンダリングによるマルチメディア配信は、オンボードのハードウェアアクセラレーションから大きな恩恵を受けます。たとえば、DirectX Video Acceleration (DXVA) のサポートにより、H.264デコードを別のハードウェアで実行することでCPUの負荷を軽減します。Intel Quick Sync、AMD RapidFire、およびNVIDIA NVENCテクノロジーは、ハードウェアアクセラレーションによるH.264エンコーディングを提供します。

ほとんどのサーバーはビデオ圧縮用のハードウェアアクセラレーションを提供しないため、すべてのビデオ処理がサーバーCPUで行われると、サーバーのスケーラビリティに悪影響が及びます。多くのマルチメディア形式をローカルレンダリングのためにユーザーデバイスにリダイレクトすることで、高いサーバーのスケーラビリティを維持できます。

- Windows Mediaリダイレクトは、通常Windows Media Playerに関連付けられているさまざまなメディア形式について、サーバーの負荷を軽減します。
- HTML5ビデオは普及しており、Citrix®はこの種のコンテンツ向けにリダイレクトテクノロジーを導入しました。HTML5、HLS、DASH、またはWebRTCを使用するWebサイトには、ブラウザーコンテンツリダイレクトをお勧めします。
- 一般的なコンテンツリダイレクトテクノロジーであるホストからクライアントへのリダイレクトとローカルアプリアクセスをマルチメディアコンテンツに適用できます。

これらのテクノロジーを組み合わせると、リダイレクトを構成しない場合、HDXはサーバー側レンダリングを実行します。 リダイレクトを構成すると、HDXはサーバーフェッチとクライアントレンダリング、またはクライアントフェッチとクライアントレンダリングのいずれかを使用します。これらの方法が失敗した場合、HDXは必要に応じてサーバー側レンダリングにフォールバックし、フォールバック防止ポリシーの対象となります。

シナリオ例



シナリオ1. (サーバーフェッチとサーバーレンダリング):

1. サーバーはソースからメディアファイルを取得し、デコードし、その後、コンテンツをオーディオデバイスまたはディスプレイデバイスに提示します。
2. サーバーは、表示デバイスまたはオーディオデバイスから、それぞれ提示された画像またはサウンドを抽出します。
3. サーバーは、必要に応じてそれを圧縮し、クライアントに送信します。

このアプローチでは、高いCPUコスト、高い帯域幅コスト（抽出された画像/音声が効率的に圧縮されていない場合）、および低いサーバー拡張性が発生します。

Thinwireおよびオーディオ仮想チャネルがこのアプローチを処理します。このアプローチの利点は、クライアントのハードウェアおよびソフトウェア要件を軽減することです。このアプローチを

使用すると、デコードはサーバーで行われ、より幅広い種類のデバイスとフォーマットで動作します。

シナリオ2. (サーバーフェッチとクライアントレンダリング):

このアプローチは、メディアコンテンツがデコードされてオーディオまたはディスプレイデバイスに提示される前に、それを傍受できることに依存します。圧縮されたオーディオ/ビデオコンテンツは代わりにクライアントに送信され、そこでローカルでデコードおよび提示されます。このアプローチの利点は、それらがクライアントデバイスにオフロードされ、サーバーのCPUサイクルを節約できることです。

しかし、これはクライアントに追加のハードウェアおよびソフトウェア要件ももたらします。クライアントは、受信する可能性のある各フォーマットをデコードできる必要があります。

シナリオ3. (クライアントフェッチとクライアントレンダリング):

このアプローチは、メディアコンテンツのURLがソースからフェッチされる前に、それを傍受できることに依存します。URLはクライアントに送信され、そこでメディアコンテンツがローカルでフェッチ、デコード、および提示されます。このアプローチは概念的にシンプルです。その利点は、サーバーが制御コマンドのみを送信するため、サーバーのCPUサイクルと帯域幅の両方を節約できることです。ただし、メディアコンテンツが常にクライアントからアクセスできるとは限りません。

フレームワークとプラットフォーム:

シングルセッションオペレーティングシステム（Windows、Mac OS X、Linux）は、マルチメディアアプリケーションのより迅速な開発を可能にするマルチメディアフレームワークを提供します。この表は、より一般的なマルチメディアフレームワークの一部をリストしています。各フレームワークは、メディア処理をいくつかの段階に分割し、パイプラインベースのアーキテクチャを使用します。

フレームワーク	プラットフォーム
DirectShow	Windows (98以降)
メディアファンデーション	ウィンドウズ (Vista 以降)
Gストリーマー	リナックス
クイックタイム	マックオーエスエックス

メディアリダイレクト技術によるダブルホップサポート

オーディオリダイレクト	いいえ
ブラウザコンテンツリダイレクト	いいえ
HDX Webカメラリダイレクト	はい
HTML5ビデオのリダイレクト	はい
Windows Media リダイレクト	はい

オーディオ機能

HDXオーディオ機能を最適化するポリシーに、以下のCitrixポリシー設定を構成して追加できます。使用方法の詳細、および他のポリシー設定との関係と依存関係については、「オーディオポリシー設定」、「帯域幅ポリシー設定」、および「マルチストリーム接続ポリシー設定」を参照してください。

アダプティブオーディオ

アダプティブオーディオを使用すると、VDAでオーディオ品質ポリシーを手動で構成する必要がありません。アダプティブオーディオは、環境に合わせて設定を最適化し、古いオーディオ圧縮形式を置き換えて、優れたユーザーエクスペリエンスを提供します。

アダプティブオーディオはデフォルトで有効になっています。アダプティブオーディオを無効にするには、「オーディオポリシー設定」を参照してください。

重要:

リアルタイムオーディオアプリケーションが必要な場合は、TCPではなくUser Datagram Protocol (UDP) を使用してオーディオを配信することをお勧めします。Windows Virtual Delivery Agent (VDA) のみがUDP経由のオーディオをサポートしています。

DTLSを使用したUDPオーディオ暗号化は、Citrix GatewayとCitrix Workspace™アプリの間でのみ利用可能です。そのため、TCPトランスポートを使用する方が望ましい場合があります。TCPは、VDAからCitrix Workspaceアプリへのエンドツーエンドの TLS暗号化をサポートしています。

アダプティブオーディオとUDPオーディオの詳細については、「UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲」を参照してください。

損失許容モードでのオーディオのサポート (プレビュー)

損失許容モードはオーディオをサポートします。この機能は、高遅延およびパケット損失のあるネットワークを介してユーザーが接続している場合に、リアルタイムストリーミングのユーザーエクスペリエンスを向上させ、EDTと比較してオーディオ品質を改善します。

パブリックプレビュー

この機能は2308ではデフォルトで無効になっています。パブリックプレビューに参加するには、「オーディオプレビュー用損失許容モードフォーム」に記入してください。

システム要件

以下の製品が、損失許容モードをサポートする最小バージョンであることを確認してください。

- シトリックス バーチャル デリバリー エージェント (VDA) 2308
- シトリックス Workspace アプリ (Windows向け) 2309

さらに、以下の機能を有効にする必要があります。

- HDX Adaptive Transportポリシー。
- (オプション) リモート接続の場合、Citrix Gateway Service が必要です。

注:

上記の条件が満たされない場合、オーディオはEDT Reliableトランスポート経由で送信されます。

追加情報

損失許容モードは、マルチメディアコンテンツを再送信せずに伝送中のパケット損失を許容する損失許容トランスポートプロトコルであり、ユーザーによりリアルタイムなエクスペリエンスを提供します。

Enlightened Data Transport (EDT) は、Citrix独自のトランスポートプロトコルであり、サーバーのスケーラビリティを維持しながら、困難な長距離接続で優れたユーザーエクスペリエンスを提供します。損失許容モードは、Citrix Gatewayサービスの一機能であり、ネットワークの混雑時でも安

定した接続を維持するために、損失許容モードをトランスポートプロトコルとして使用します。これにより、リモートワーカーに一貫した安定したエクスペリエンスが保証されます。通常の状況では、EDTと損失許容モードの両方が同様の結果を提供します。しかし、パケット損失のあるネットワーク状況では、損失許容モードはEDTと比較してより良いオーディオエクスペリエンスを提供します。このため、リアルタイムマルチメディアに依存するリモートワーカーにとって不可欠な機能となります。

オーディオ品質

一般的に、音質が高いほど、より多くのオーディオデータをユーザーデバイスに送信するため、より多くの帯域幅とサーバーCPU使用率を消費します。サウンド圧縮を使用すると、音質とセッション全体のパフォーマンスのバランスを取ることができます。Citrixポリシー設定を使用して、サウンドファイルに適用する圧縮レベルを構成します。

デフォルトでは、TCPトランスポートが使用される場合、**オーディオ品質ポリシー**設定は「高 - 高精細オーディオ」に設定されています。UDPトランスポート（推奨）が使用される場合、ポリシーは「中 - 音声に最適化」に設定されます。**高精細オーディオ**設定は、高忠実度のステレオオーディオを提供しますが、他の品質設定よりも多くの帯域幅を消費します。最適化されていない音声チャットまたはビデオチャットアプリケーション（ソフトフォンなど）には、このオーディオ品質を使用しないでください。その理由は、リアルタイム通信に適さない遅延をオーディオパスに導入する可能性があるためです。選択されたトランスポートプロトコルに関係なく、リアルタイムオーディオには「音声に最適化」ポリシー設定を推奨します。

帯域幅が制限されている場合（例えば、衛星接続やダイヤルアップ接続など）は、オーディオ品質を**低**に下げることで、可能な限り少ない帯域幅を消費します。この状況では、低帯域幅接続のユーザー向けに個別のポリシーを作成し、高帯域幅接続のユーザーが悪影響を受けないようにします。

設定の詳細については、オーディオポリシー設定 を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

オーディオ再生と録音の帯域幅ガイドライン：

- アダプティブオーディオ（デフォルト）
  - ビットレート: 可変アダプティブ
  - チャンネル数: 再生用2（ステレオ）、マイクキャプチャ用1（モノラル）
  - 周波数: 48000 Hz
  - ビット深度: 16ビット

- 高音質
  - ビットレート：再生で約100 kbps（最小75、最大175 kbps）/マイクキャプチャで約70 kbps
  - チャンネル数：再生で2（ステレオ）、マイクキャプチャで1（モノラル）
  - 周波数：44100 Hz
  - ビット深度: 16ビット
- 中品質 (VoIPに推奨)
  - ビットレート: 再生時 ~16 kbps (最小20 kbps、最大40 kbps)、マイクキャプチャ時 ~16 kbps
  - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
  - 周波数: 16000 Hz (ワイドバンド)
  - ビット深度: 16ビット
- 低品質
  - ビットレート: 再生時約11 kbps (最小10; 最大25 kbps)、マイクキャプチャ時約11 kbps
  - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
  - 周波数: 8000 Hz (ナローバンド)
  - ビット深度: 16ビット

クライアントオーディオリダイレクト

ユーザーデバイス上のスピーカーまたはその他のサウンドデバイスを介して、サーバー上のアプリケーションからオーディオを受信できるようにするには、**クライアントオーディオリダイレクト**設定を**許可**のままにします。これはデフォルトです。

クライアントオーディオマッピングは、サーバーとネットワークに余分な負荷をかけます。ただし、クライアントオーディオリダイレクトを禁止すると、すべてのHDX™オーディオ機能が無効になります。

設定の詳細については、オーディオポリシー設定を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

クライアントマイクのリダイレクト

ユーザーデバイス上のマイクなどの入力デバイスを使用してユーザーがオーディオを録音できるようにするには、**クライアントマイクのリダイレクト**設定をデフォルト（許可）のままにします。

セキュリティのため、ユーザーデバイスは、信頼できないサーバーがマイクにアクセスしようとすると、ユーザーに警告します。ユーザーは、マイクを使用する前にアクセスを許可または拒否できます。ユーザーは、Citrix Workspaceアプリでこの警告を無効にできます。

設定の詳細については、オーディオポリシー設定を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

オーディオプラグアンドプレイ

オーディオプラグアンドプレイポリシー設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。この設定は、デフォルトで**有効**になっています。オーディオプラグアンドプレイにより、オーディオデバイスが認識されるようになります。ユーザーセッションが開始されるまで接続されていなくても、デバイスは認識されます。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

設定の詳細については、「オーディオポリシー設定」を参照してください。

オーディオリダイレクト帯域幅制限とオーディオリダイレクト帯域幅制限の割合

オーディオリダイレクト帯域幅制限ポリシー設定は、セッションでのオーディオの再生と録音のために、最大帯域幅（キロビット/秒単位）を指定します。

オーディオリダイレクト帯域幅制限の割合設定は、利用可能な総帯域幅の割合として、オーディオリダイレクトの最大帯域幅を指定します。

デフォルトでは、両方の設定でゼロ（最大なし）が指定されています。両方の設定が構成されている場合、帯域幅制限が最も低い方が使用されます。

設定の詳細については、「帯域幅ポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲

デフォルトでは、ユーザーデータグラムプロトコル（UDP）リアルタイムトランスポート経由のオーディオは許可されています（インストール時に選択した場合）。これは、UDPリアルタイムトランスポート経由のオーディオを使用する接続のために、サーバー上にUDPポートを開きます。ネットワークの輻輳やパケット損失がある場合は、可能な限り最高のユーザーエクスペリエンスを確保するために、オーディオにUDP/RTPを構成することをお勧めします。ソフトフォンアプリケーションなどのリアルタイムオーディオの場合、EDTよりもUDPオーディオが推奨されます。

UDPは再送信なしでパケット損失を許容するため、パケット損失が多い接続で遅延が追加されることはありません。

重要:

Citrix Gatewayが経路にない場合、UDPで送信されるオーディオデータは暗号化されません。Citrix GatewayがCitrix Virtual Apps and Desktops™リソースにアクセスするように構成されている場合、エンドポイントデバイスとCitrix Gateway間のオーディオトラフィックはDTLSプロトコルを使用して保護されます。

オーディオUDPポート範囲は、Windows VDAがユーザーデバイスとオーディオパケットデータを交換するために使用するポート番号の範囲を指定します。

デフォルトでは、範囲は16500から16509です。

注:

アダプティブオーディオにUDPリアルタイムトランスポート経由のオーディオが必要ない場合、Citrixはポリシー設定を「無効」に構成することを推奨します。これにより、Citrix Workspaceアプリクライアントが UDP接続の開放を要求したり、不要なCitrix Workspaceアプリクライアントのファイアウォール構成ダイアログウィンドウが表示されたりするのを防ぐことができます。

UDPリアルタイムトランスポート経由のオーディオの設定の詳細については、「オーディオポリシー設定」を参照してください。オーディオUDPポート範囲の詳細については、「マルチストリーム接続ポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDP経由のオーディオにはWindows VDAが必要です。Linux VDAでサポートされているポリシーについては、「ポリシーサポートリスト」を参照してください。

ユーザーデバイス向けオーディオ設定ポリシー

1. 「グループポリシーオブジェクト管理用テンプレートの構成」に従って、グループポリシーテンプレートをロードします。
2. グループポリシーエディターで、**管理用テンプレート > Citrix Components > Citrix Workspace > ユーザーエクスペリエンス**を展開します。

3. **クライアントオーディオ設定**で、**未構成**、**有効**、または**無効**を選択します。
   - **未構成**。デフォルトでは、オーディオリダイレクトは高品質オーディオまたは以前に構成されたカスタムオーディオ設定を使用して有効になります。
   - **有効**。選択したオプションを使用してオーディオリダイレクトを有効にします。
   - **無効**。オーディオリダイレクトを無効にします。
4. **有効**を選択した場合、音質を選択します。UDPオーディオの場合は、**中**（デフォルト）を使用します。
5. UDPオーディオの場合のみ、**リアルタイムトランスポートを有効にする**を選択し、ローカルのWindowsファイアウォールで開く受信ポートの範囲を設定します。
6. Citrix GatewayでUDPオーディオを使用するには、**ゲートウェイ経由のリアルタイムトランスポートを許可**を選択します。Citrix GatewayをDTLSで構成します。詳細については、こちらの記事を参照してください。

管理者として、これらの変更を行うためのエンドポイントデバイスを制御できない場合は、StoreFrontのdefault.ica属性を使用してUDPオーディオを有効にします。たとえば、BYODデバイスや家庭用コンピューターの場合などです。

1. StoreFrontマシンで、C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.icaをメモ帳などのエディターで開きます。
2. セクションに以下のエントリを作成します。

   ; このテキストはリアルタイムトランスポートを有効にします

   RTPオーディオを有効にする=true

   ; このテキストはゲートウェイ経由のリアルタイムトランスポートを許可します

   ゲートウェイ経由のUDPを有効にする=true

   ; このテキストはオーディオ品質を「中」に設定します

   AudioBandwidthLimit=1

   ; UDP ポート範囲

   RtpAudioLowestPort=16500

   RtpAudioHighestPort=16509

default.ica を編集してユーザーデータグラムプロトコル (UDP) オーディオを有効にすると、そのストアを使用しているすべてのユーザーに対して UDP オーディオが有効になります。

マルチメディア会議中のエコーを回避する

オーディオ会議やビデオ会議のユーザーは、エコーを聞くことがあります。エコーは通常、スピーカーとマイクが互いに近すぎるときに発生します。そのため、オーディオ会議やビデオ会議にはヘッドセットの使用をお勧めします。

HDX は、エコーを最小限に抑えるエコーキャンセルオプション (デフォルトで有効) を提供します。エコーキャンセルの有効性は、スピーカーとマイクの間の距離に影響されます。デバイスが互いに近すぎたり遠すぎたりしないようにしてください。

レジストリ設定を変更して、エコーキャンセルを無効にすることができます。詳細については、レジストリで管理される機能のリストにある マルチメディア会議中のエコーを回避する を参照してください。

ソフトフォン

ソフトフォンは、電話インターフェースとして機能するソフトウェアです。ソフトフォンを使用すると、コンピューターやその他のスマートデバイスからインターネット経由で通話できます。ソフトフォンを使用することで、画面を使って電話番号をダイヤルしたり、その他の電話関連機能を実行したりできます。

Citrix Virtual Apps and Desktopsは、ソフトフォンを配信するためのいくつかの代替手段をサポートしています。

- **コントロールモード**。ホストされているソフトフォンが物理的な電話機を制御します。このモードでは、Citrix Virtual Apps and Desktopsサーバーを介してオーディオトラフィックが流れることはありません。
- **HDX RealTime最適化ソフトフォンサポート (推奨)**。メディアエンジンはユーザーデバイス上で実行され、Voice over Internet Protocolトラフィックはピアツーピアで流れます。例については、以下を参照してください。
  - Microsoft Teams 用 HDX 最適化(/ja-jp/citrix-virtual-apps-desktops/2311/multimedia/opt-ms-teams.html)
  - HDX RealTime Optimization Pack は、Microsoft Skype for Businessの配信を最適化します
  - VDI 用 Cisco Jabber ソフトフォン (旧称 VXME)
  - シスコ Webex Meetings VDI用(https://www.cisco.com/c/en/us/td/docs/collaboration/meeting_center/wvdi/wvdi-b-admin-guide/wvdi-b-admin-guide_chapter_010.html)

  - Avaya VDI Equinox (以前はVDI Communicatorとして知られていた)
  - Zoom VDI プラグイン
  - ジェネシス ピュアエンゲージ クラウド
  - Nuance Dragon PowerMic ディクテーションデバイス

- **ローカルアプリアクセス**。Citrix Virtual Apps and Desktopsの機能で、ソフトフォンなどのアプリケーションをWindowsユーザーデバイス上でローカルに実行しながら、仮想/公開デスクトップとシームレスに統合されているように見せることができます。この機能は、すべてのオーディオ処理をユーザーデバイスにオフロードします。詳細については、「ローカルアプリアクセスとURLリダイレクト」を参照してください。
- **HDX RealTime汎用ソフトフォンサポート。** ICA経由のVoice over Internet Protocol。

汎用ソフトフォンサポート

汎用ソフトフォンサポートにより、データセンターのXenAppまたはXenDesktop上で未変更のソフトフォンをホストできます。音声トラフィックは、Citrix ICAプロトコル（できればUDP/RTPを使用）を介して、Citrix Workspaceアプリを実行しているユーザーデバイスに送信されます。

汎用ソフトフォンサポートはHDX RealTimeの機能です。このソフトフォン配信アプローチは、特に次の場合に役立ちます。

- ソフトフォンを配信するための最適化されたソリューションが利用できず、ユーザーがLocal App Accessを使用できるWindowsデバイスを使用していない場合。
- ソフトフォンの最適化された配信に必要なメディアエンジンがユーザーデバイスにインストールされていないか、ユーザーデバイスで実行されているオペレーティングシステムのバージョンで利用できない場合。このシナリオでは、汎用HDX RealTimeが貴重なフォールバックソリューションを提供します。

Citrix Virtual Apps and Desktopsを使用する場合、ソフトフォンの配信には次の2つの考慮事項があります。

- 仮想/公開デスクトップにソフトフォンアプリケーションがどのように配信されるか。
- ユーザーのヘッドセット、マイク、スピーカー、またはUSB電話機との間で音声がどのように配信されるか。

Citrix Virtual Apps and Desktopsには、汎用ソフトフォン配信をサポートするための多数のテクノロジーが含まれています。

- リアルタイムオーディオの高速エンコードと帯域幅効率のためのOptimized-for-Speechコーデック。

- 低遅延オーディオスタック。
- ネットワーク遅延が変動するときに音声をスムーズにするための、サーバー側のジッターバッファ。
- サービス品質（QoS）のためのパケットタグ付け（DSCPおよびWMM）。
    - RTPパケット（レイヤー3）用のDSCPタグ付け
    - Wi-Fi用のWMMタグ付け

Windows、Linux、Chrome、Mac 用の Citrix Workspace アプリのバージョンも、Voice over Internet Protocol に対応しています。Windows 用 Citrix Workspace アプリには、次の機能があります。

- クライアント側ジッターバッファ - ネットワーク遅延が変動する場合でも、スムーズなオーディオを保証します。
- エコーキャンセル - ヘッドセットを使用しない作業者向けに、マイクとスピーカー間の距離の変動をより大きく許容します。
- オーディオプラグアンドプレイ - セッションを開始する前にオーディオデバイスを接続する必要はありません。いつでも接続できます。
- オーディオデバイスルーティング - ユーザーは着信音をスピーカーに、音声パスをヘッドセットに送ることができます。
- マルチストリーム ICA - ネットワークを介した柔軟なQuality of Serviceベースのルーティングを可能にします。
- ICA は 4 つの TCP ストリームと 2 つの UDP ストリームをサポートします。UDP ストリームの 1 つは、RTP を介したリアルタイムオーディオをサポートします。

Citrix Workspace アプリの機能の概要については、「Citrix Receiver Feature Matrix」を参照してください。

システム構成の推奨事項

クライアントハードウェアとソフトウェア: 最適なオーディオ品質を得るには、最新バージョンの Citrix Workspace アプリと、音響エコーキャンセル (AEC) 機能を備えた高品質のヘッドセットをお勧めします。Windows、Linux、Mac 用の Citrix Workspace アプリのバージョンは、Voice over Internet Protocol をサポートしています。また、Dell Wyse は ThinOS (WTOS) 用の Voice over Internet Protocol サポートを提供しています。

CPU に関する考慮事項: VDA の CPU 使用率を監視し、各仮想マシンに 2 つの仮想 CPU を割り当てる必要があるかどうかを判断します。リアルタイムの音声とビデオはデータ集約型です。2 つの

仮想 CPU を構成すると、スレッド切り替えの遅延が減少します。そのため、Citrix Virtual Desktops™ VDI 環境では 2 つの vCPU を構成することをお勧めします。

2 つの仮想 CPU を持つことは、物理 CPU がセッション間で共有できるため、物理 CPU の数を 2 倍にすることを必ずしも意味しません。

セッションの信頼性機能に使用される Citrix Gateway Protocol (CGP) も、CPU 消費量を増加させます。高品質のネットワーク接続では、この機能を無効にして VDA の CPU 消費量を削減できます。強力なサーバーでは、上記のいずれのステップも必要ない場合があります。

UDP オーディオ: UDP を介したオーディオは、ネットワークの輻輳とパケット損失に対して優れた耐性を提供します。利用可能な場合は、TCP の代わりに UDP をお勧めします。

LAN/WAN 構成: 良好なリアルタイムオーディオ品質には、ネットワークの適切な構成が不可欠です。通常、過剰なブロードキャストパケットがジッターを引き起こす可能性があるため、仮想 LAN (VLAN) を構成する必要があります。IPv6 対応デバイスは多くのブロードキャストパケットを生成する可能性があります。IPv6 サポートが不要な場合は、これらのデバイスで IPv6 を無効にできます。Quality of Service をサポートするように構成してください。

WAN接続の使用設定: LANおよびWAN接続で音声チャットを使用できます。WAN接続では、オーディオ品質は接続の遅延、パケット損失、ジッターに依存します。WAN接続のユーザーにソフトフォンを配信する場合、データセンターとリモートオフィス間でNetScaler® SD-WANを使用することをお勧めします。これにより、高いサービス品質が維持されます。NetScaler SD-WANは、UDPを含むMulti-Stream ICAをサポートしています。また、単一のTCPストリームの場合、さまざまなICA仮想チャネルの優先順位を区別して、優先度の高いリアルタイムオーディオデータが優先的に処理されるようにすることが可能です。

DirectorまたはHDX Monitorを使用して、HDX構成を検証します。

リモートユーザー接続: Citrix Gatewayは、UDP/RTPトラフィックをネイティブに（TCPでのカプセル化なしで）配信するためにDTLSをサポートしています。 ポート443経由のUDPトラフィックに対して、ファイアウォールを双方向に開きます。

コーデックの選択と帯域幅の消費: ユーザーデバイスとデータセンター内のVDA間では、Medium Qualityオーディオとも呼ばれる**Optimized-for-Speech**コーデック設定を使用することをお勧めします。VDAプラットフォームとIP-PBX間では、ソフトフォンは構成またはネゴシエートされたコーデックを使用します。例：

- G711は良好な音声品質を提供しますが、1コールあたり80キロビット/秒から100キロビット/秒の帯域幅要件があります（ネットワークレイヤー2のオーバーヘッドに依存）。

- G729は良好な音声品質を提供し、1コールあたり30キロビット/秒から40キロビット/秒の低い帯域幅要件があります（ネットワークレイヤー2のオーバーヘッドに依存）。

仮想デスクトップへのソフトフォンアプリケーションの配信

XenDesktop®仮想デスクトップにソフトフォンを配信するには、2つの方法があります。

- アプリケーションは仮想デスクトップイメージにインストールできます。
- アプリケーションはMicrosoft App-Vを使用して仮想デスクトップにストリーミングできます。このアプローチには、仮想デスクトップイメージが整理された状態に保たれるため、管理上の利点があります。仮想デスクトップにストリーミングされた後、アプリケーションは通常の方法でインストールされたかのようにその環境で実行されます。すべてのアプリケーションがApp-Vと互換性があるわけではありません。

ユーザーデバイスとの間のオーディオ配信

汎用HDX RealTimeは、ユーザーデバイスとの間でオーディオを配信する2つの方法をサポートしています。

- **Citrixオーディオ仮想チャネル**。Citrixオーディオ仮想チャネルはオーディオ転送専用に設計されているため、通常はこちらをお勧めします。
- **汎用USBリダイレクト**。ユーザーデバイスがCitrix Virtual Apps and Desktopsサーバーへの LANまたはLANに類似した接続上にある場合、ボタンまたはディスプレイ（あるいはその両方）を持つオーディオデバイス、ヒューマンインターフェイスデバイス（HID）をサポートします。

Citrix オーディオ仮想チャネル

双方向のCitrixオーディオ仮想チャネル（CTXCAM）により、オーディオをネットワーク経由で効率的に配信できます。汎用HDX RealTimeは、ユーザーのヘッドセットまたはマイクからのオーディオを取得して圧縮します。その後、ICA経由で仮想デスクトップ上のソフトフォンアプリケーションに送信します。同様に、ソフトフォンのオーディオ出力も圧縮され、逆方向にユーザーのヘッドセットまたはスピーカーに送信されます。この圧縮は、ソフトフォン自体が使用する圧縮（G.729やG.711など）とは独立しています。これは、Optimized-for-Speechコーデック（中品質）を使用して行われます。その特性は、Voice over Internet Protocolに最適です。エンコード時間が短く、ネットワーク帯域幅はピーク時で約56キロビット/秒（各方向28 Kbps）しか消費しません。このコーデックはデフォルトのオーディオコーデックではないため、Studioコンソールで明示的に選択する必要があります。デフォルトはHDオーディオコーデック（高品質）です。このコーデックは高忠実度のステレオサウンドトラックに優れていますが、Optimized-for-Speechコーデックと比較してエンコードが遅いです。

汎用 USB リダイレクト

Citrixの汎用USBリダイレクトテクノロジー（CTXGUSB仮想チャネル）は、複合デバイス（オーディオとHID）やアイソクロナスUSBデバイスを含むUSBデバイスをリモートで利用するための汎用的な手段を提供します。このアプローチは、LAN接続されたユーザーに限定されます。その理由は、USBプロトコルがネットワーク遅延に敏感であり、かなりのネットワーク帯域幅を必要とする傾向があるためです。アイソクロナスUSBリダイレクトは、一部のソフトフォンを使用する場合にうまく機能します。このリダイレクトは、優れた音声品質と低遅延を提供します。ただし、Citrixオーディオ仮想チャネルはオーディオトラフィックに最適化されているため、こちらが推奨されます。主な例外は、ボタン付きのオーディオデバイスを使用する場合です。たとえば、データセンターにLAN接続されたユーザーデバイスに接続されたUSB電話などです。この場合、汎用USBリダイレクトは、ソフトフォンに信号を送り返すことで機能を制御する電話機またはヘッドセットのボタンをサポートします。デバイス上でローカルに機能するボタンには問題ありません。

オーディオ診断コマンドラインツール

VDA上のオーディオ診断コマンドラインツールは、オーディオポリシー、構成、データ転送に関連するセッションデータを照会するために使用できます。

使用方法

コマンドプロンプトを開き、`C:\Program Files\Citrix\HDX\bin`フォルダーから`CtxAudio.exe`を実行します。

- 管理者としてツールを実行すると、すべてのアクティブなICAセッションのオーディオ情報が表示されます。
- 非管理者としてツールを実行すると、現在ユーザーのICAセッションオーディオ情報が表示されます。

出力

このツールは、セッション内のオーディオ関連の問題の診断に役立つさまざまな構成設定を出力します。

セクション	説明
ポリシー情報	現在のセッションに適用されるオーディオポリシー。

セクション	説明
設定情報	レジストリに保存されているオーディオ関連の構成設定。
状態情報	現在のセッションに適用されているオーディオの状態、バージョン、コーデック、およびトランスポート。
デバイス情報	セッションで使用されるデバイス名、その役割、およびステータス。

注:

出力は、マルチセッション (TS) VDA またはシングルセッション VDA (WSVDA) のどちらでツールを実行するかによって異なります。

制限事項

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にして、RDSセッションを開始します。オーディオファイルが再生に失敗し、エラーメッセージが表示されることがあります。

回避策として、RDSマシンにレジストリキーを追加し、マシンを再起動します。詳細については、レジストリを介して管理される機能のリストにあるオーディオの制限を参照してください。

ブラウザコンテンツリダイレクト

ブラウザコンテンツリダイレクトは、VDA側での許可リスト内のWebページのレンダリングを防ぎます。この機能は、Citrix Workspace™アプリ for WindowsまたはCitrix Workspaceアプリ for Linuxを使用して、クライアント側で対応するレンダリングエンジンをインスタンス化し、URLからHTTPおよびHTTPSコンテンツをフェッチします。

注:

ブロックリストを使用することで、WebページをVDA側にリダイレクトするよう指定できます（クライアント側ではリダイレクトされません）。

> このオーバーレイウェブレイアウトエンジンは、VDA上ではなくエンドポイントデバイス上で実行され、エンドポイントのCPU、GPU、RAM、およびネットワークを使用します。

ブラウザのビューポートのみがリダイレクトされます。ビューポートとは、ブラウザ内でコンテンツが表示される長方形の領域です。ビューポートには、アドレスバー、**お気に入り**ツールバー、ステータスバーのようなものは含まれません。これらの項目はユーザーインターフェイスにあり、VDA内のブラウザで引き続き実行されます。

ビューポートの例(/en-us/citrix-virtual-apps-desktops/2311/media/viewport.png)

1. リダイレクト用の許可リスト内のURL、または特定のURLパスのリダイレクトを無効にするブロックリストを含むアクセス制御リストを指定するStudioポリシーを構成します。VDA上のブラウザが、ユーザーがアクセスしているURLが許可リストと一致するか、ブロックリストと一致しないことを検出するために、ブラウザ拡張機能が比較を実行します。Internet Explorer 11用のブラウザ拡張機能は、インストールメディアに含まれており、自動的にインストールされます。Chromeの場合、ブラウザ拡張機能はChromeウェブストアで入手でき、グループポリシーとADMXファイルを使用して展開できます。Chrome拡張機能はユーザーごとにインストールされます。拡張機能を追加または削除するためにゴールデンイメージを更新する必要はありません。
2. 許可リスト内で一致が見つかり（例: `https://www.mycompany.com/`）、ブロックリスト内のURLと一致しない場合（例: `https://www.mycompany.com/engineering`）、仮想チャネル（CTXCSB）がCitrix Workspaceアプリにリダイレクトが必要であることと、URLを中継するよう指示します。その後、Citrix Workspaceアプリはローカルレンダリングエンジンをインスタンス化し、ウェブサイトを表示します。
3. その後、Citrix Workspaceアプリはウェブサイトを仮想デスクトップのブラウザコンテンツ領域にシームレスにブレンドし直します。

> **注:**
>
> ブラウザコンテンツリダイレクト拡張機能の新機能と修正に関する詳細については、Chromeウェブストアにアクセスし、「citrix® bcr」を検索して拡張機能を見つけてください。

> ロゴの色はChrome拡張機能のステータスを示します。以下の3色のいずれかです。

- 緑: アクティブで接続済み。
- 灰色: 現在のタブでは非アクティブ/アイドル状態。

- 赤: 破損/動作していません。

拡張機能メニューの**オプション**を使用して、ログのデバッグを行うことができます。

ブラウザビューポートリダイレクトの例の画像(/en-us/citrix-virtual-apps-desktops/2311/media/browser-viewport-redirection-example.png)

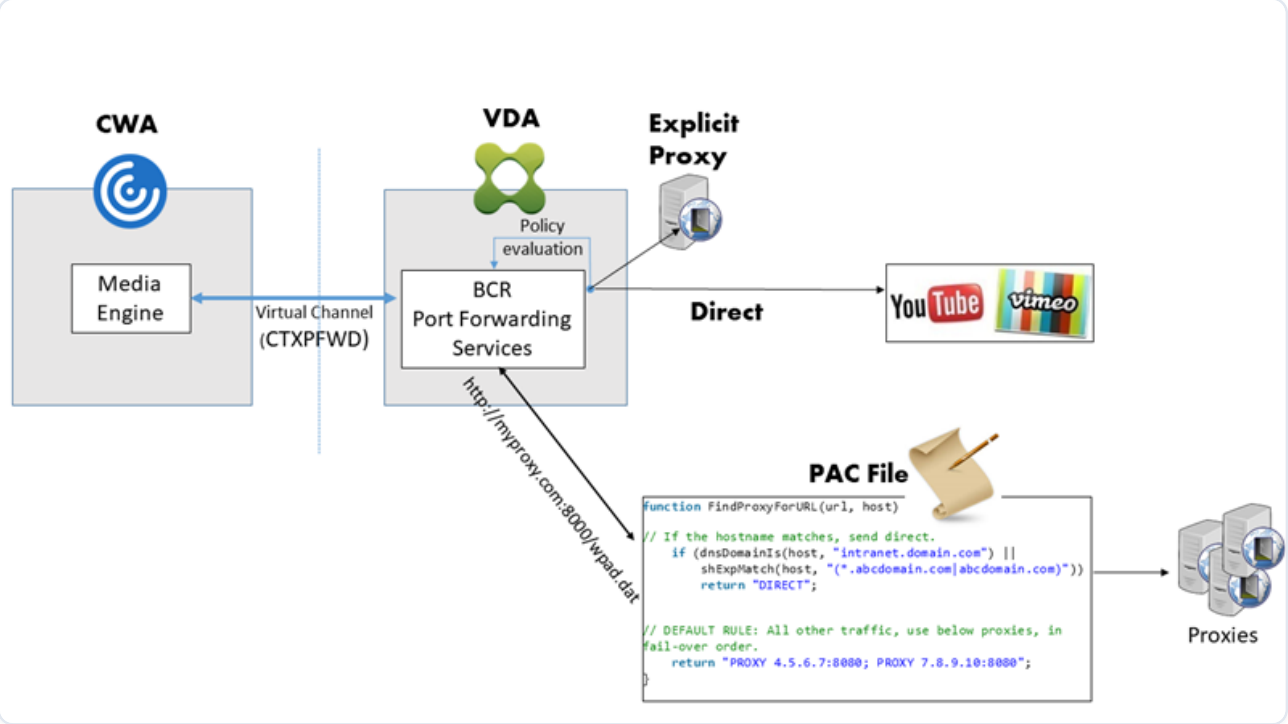
Citrix Workspaceアプリがコンテンツを取得するシナリオは次のとおりです。

- **サーバーフェッチとサーバーレンダリング**: サイトを許可リストに追加しなかったか、リダイレクトが失敗したため、リダイレクトは行われません。VDAでウェブページをレンダリングし、Thinwireを使用してグラフィックをリモート処理します。フォールバック動作を制御するにはポリシーを使用します。VDAでのCPU、RAM、帯域幅の消費量が高くなります。
- **サーバーフェッチとクライアントレンダリング**: Citrix Workspaceアプリは、仮想チャネル（CTXPFWD）を使用してVDA経由でWebサーバーに接続し、コンテンツを取得します。このオプションは、クライアントがインターネットアクセスを持たない場合（シンクライアントなど）に役立ちます。VDAでのCPUとRAMの消費量は低いですが、ICA®仮想チャネルで帯域幅が消費されます。

  このシナリオには3つの動作モードがあります。プロキシという用語は、VDAがインターネットアクセスを得るためにアクセスするプロキシデバイスを指します。

  選択するポリシーオプション：

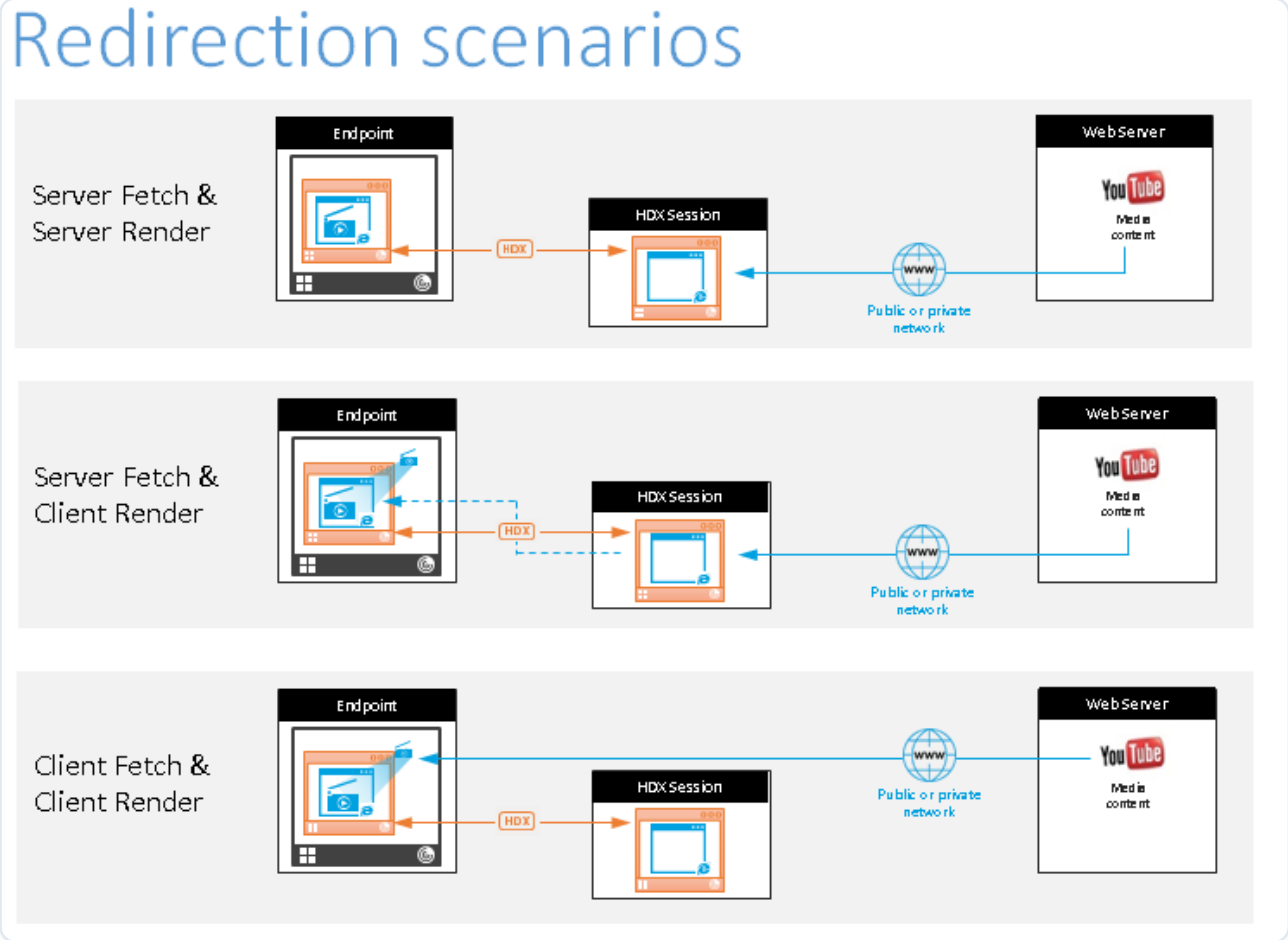
  - Explicit Proxy - データセンターに単一の明示的なプロキシがある場合。
  - Direct or Transparent - プロキシがない場合、または透過プロキシを使用している場合。
  - PAC files - VDA内のブラウザが指定されたURLを取得するために適切なプロキシサーバーを自動的に選択できるように、PACファイルに依存している場合。



- **クライアントフェッチとクライアントレンダリング**: Citrix WorkspaceアプリがWebサーバーに直接接続するため、インターネットアクセスが必要です。このシナリオでは、XenApp and XenDesktop®サイトからのすべてのネットワーク、CPU、およびRAMの使用量をオフロードします。

  利点:

  - より良いエンドユーザーエクスペリエンス（アダプティブビットレート（ABR））
  - VDAリソース使用量の削減（CPU/RAM/IO）
  - 帯域幅消費量の削減



フォールバックメカニズム：

クライアントリダイレクトが失敗する場合があります。たとえば、クライアントマシンがインターネットに直接アクセスできない場合、エラー応答がVDAに戻される可能性があります。そのような場合、VDA上のブラウザはページを再読み込みし、サーバー上でレンダリングできます。

既存の**Windows Mediaフォールバック防止**ポリシーを使用して、ビデオ要素のサーバーレンダリングを抑制できます。このポリシーを**すべてのコンテンツをクライアントでのみ再生**または**クライアントでアクセス可能なコンテンツのみをクライアントで再生**に設定します。これらの設定は、クライアントリダイレクトに失敗した場合に、ビデオ要素がサーバーで再生されるのをブロックします。このポリシーは、ブラウザコンテンツリダイレクトを有効にし、**アクセスコントロールリスト**ポリシーにフォールバックするURLが含まれている場合にのみ有効になります。URLはブロックリストポリシーに含まれていてはなりません。

システム要件:

Windowsエンドポイント:

- ウィンドウズ 10
- Citrix Workspaceアプリ 1809 for Windows以降

> **注:**
>
> ブラウザコンテンツリダイレクトは、Citrix Workspaceアプリ for WindowsのCurrent Releaseでのみサポートされており、Citrix WorkspaceアプリLTSRリリース（1912および2203.1）ではサポートされていません。

> Linuxエンドポイント:

- Citrix Workspaceアプリ 1808 for Linux以降
- シンクライアント端末にはWebKitGTK+が含まれている必要があります

Citrix Virtual Apps and Desktops 7 1808以降、およびXenApp and XenDesktop 7.15 CU5以降:

- VDAオペレーティングシステム: Windows 10 (最小バージョン 1607)、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019
- VDA 上のブラウザ:
  - Google Chrome v66 以降 (Chrome を使用するには、ユーザーエンドポイントに Citrix Workspace app 1809 for Windows 以降、Citrix Virtual Apps and Desktops™ 7 1808 VDA 以降、およびブラウザコンテンツリダイレクト拡張機能が必要です)
  - Internet Explorer 11 と、以下のオプションを構成します:
    - **インターネットオプション** > **詳細設定 > セキュリティ** の下にある **拡張保護モード** をクリアします
    - **インターネットオプション > 詳細設定 > 閲覧** の下にある **サードパーティのブラウザ拡張機能を有効にする** をオンにします

トラブルシューティング

トラブルシューティング情報については、Knowledge Centerの記事https://support.citrix.com/article/CTX230052をご覧ください。

ブラウザコンテンツリダイレクト Chrome 拡張機能

Chrome でブラウザコンテンツリダイレクトを使用するには、Chrome ウェブストアからブラウザコンテンツリダイレクト拡張機能を追加します。Citrix Virtual Apps and Desktops 環境で **Chrome に追加** をクリックします。

この拡張機能は、ユーザーのクライアントマシンには **不要** です。VDA のみに必要です。

システム要件

- Chrome v66 以降
- ブラウザコンテンツリダイレクト拡張機能
- Citrix Virtual Apps and Desktops のバージョン 7 1808 以降
- Citrix Workspaceアプリ 1809 for Windows 以降

> **注：**
>
> ブラウザコンテンツリダイレクトは、Citrix Workspaceアプリ for Windows のCurrent Releaseでのみサポートされており、Citrix WorkspaceアプリのLTSRリリース（1912および2203.1）ではサポートされていません。

> ブラウザコンテンツリダイレクト拡張機能(/en-us/citrix-virtual-apps-desktops/2311/media/bcr_extension.png)

この方法は個々のユーザーに有効です。組織内の大規模なユーザーグループに拡張機能を展開するには、グループポリシーを使用して拡張機能を展開します。

グループポリシーを使用して拡張機能を展開する

1. Google Chrome ADMXファイルを環境にインポートします。ポリシーテンプレートのダウンロード、およびグループポリシーエディターへのテンプレートのインストールと構成については、「管理対象PCでChromeブラウザポリシーを設定する」を参照してください。
2. グループポリシー管理コンソールを開き、**ユーザーの構成 \ 管理用テンプレート\従来の管理用テンプレート (ADM) \ Google\ Google Chrome \ 拡張機能**に移動します。「**強制的にインストールするアプリと拡張機能のリストを構成する**」設定を有効にします。

   ブラウザコンテンツリダイレクト拡張機能(/en-us/citrix-virtual-apps-desktops/2311/media/bcr_extension_gpo.png)
3. **表示**をクリックし、拡張機能IDに対応する次の文字列を入力します。ブラウザコンテンツリダイレクト拡張機能のURLを更新します。

   `hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx`

   ブラウザコンテンツリダイレクトの表示(/en-us/citrix-virtual-apps-desktops/2311/media/bcr_extension_show.png)

4. 設定を適用し、**gpupdate**で更新すると、ユーザーは自動的に拡張機能を受け取ります。ユーザーのセッションでChromeブラウザを起動すると、拡張機能はすでに適用されており、ユーザーはそれを削除できません。

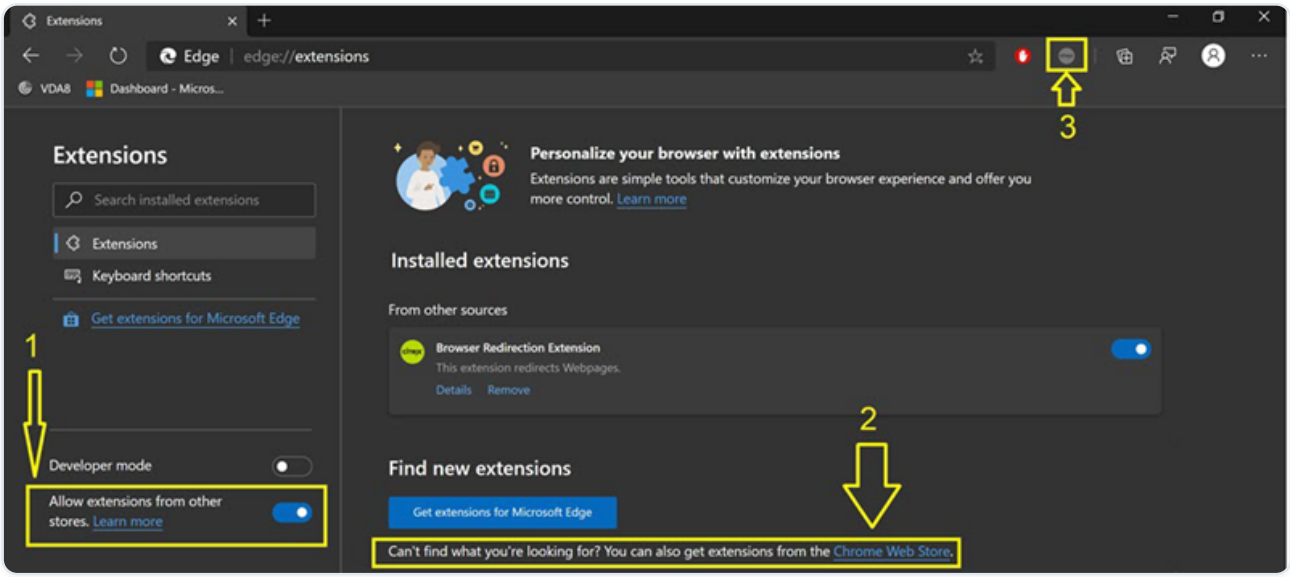
   拡張機能への更新は、設定で指定した更新URLを介して、ユーザーのマシンに自動的にインストールされます。

   「**強制インストールされるアプリと拡張機能のリストを構成する**」設定が**無効**に設定されている場合、拡張機能はすべてのユーザーのChromeから自動的に削除されます。

ブラウザーコンテンツリダイレクトEdge Chromium拡張機能

Edgeにブラウザーコンテンツリダイレクト拡張機能をインストールするには、Edgeブラウザーのバージョン**83.0.478.37**以降がインストールされていることを確認してください。

1. **拡張機能**オプションをクリックします。「**拡張機能の管理**」を選択します。「**他のストアからの拡張機能を許可する**」をオンにします。
2. **Chromeウェブストア**リンクをクリックすると、拡張機能が右上のバーに表示されます。Microsoft Edgeの拡張機能の詳細については、「拡張機能」を参照してください。



ブラウザーコンテンツリダイレクトとDPI

ユーザーのマシンでDPI（スケーリング）が100%を超えて設定されている状態でブラウザーコンテンツリダイレクトを使用すると、リダイレクトされたブラウザーコンテンツ画面が正しく表示されません。この問題を回避するには、ブラウザーコンテンツリダイレクトを使用する際にDPIを設定しないでください。この問題を回避するもう1つの方法は、ユーザーのマシンにレジストリキーを作成して、Chromeのブラウザーコンテンツリダイレクト GPUアクセラレーションを無効に

することです。詳細については、レジストリで管理される機能のリストにある「ブラウザーコンテンツリダイレクトとDPI」を参照してください。

統合Windows認証によるシングルサインオン

ブラウザーコンテンツリダイレクトは、VDAと同じドメイン内で統合Windows認証（IWA）が構成されているWebサーバーへの認証にNegotiateスキームを使用するようにオーバーレイを強化します。

デフォルトでは、ブラウザーコンテンツリダイレクトは、ユーザーがWebサーバーにアクセスするたびにVDA資格情報で認証する必要がある基本認証スキームを使用します。シングルサインオンの場合、**ブラウザーコンテンツリダイレクトの統合Windows認証サポート**ポリシー設定を有効にするか、VDAにレジストリキーを作成できます。

シングルサインオンを有効にする前に、以下を完了してください。

- ホスト名から構築されたサービスプリンシパル名（SPN）のチケットを発行するようにKerberosインフラストラクチャを構成します。例：`HTTP/serverhostname.com`。
- サーバーフェッチの場合：サーバーフェッチモードでブラウザーコンテンツリダイレクトを使用する場合は、VDAでDNSが適切に構成されていることを確認してください。
- クライアントフェッチの場合：クライアントフェッチモードでブラウザーコンテンツリダイレクトを使用する場合は、クライアントデバイスでDNSが適切に構成されており、オーバーレイからWebサーバーのIPアドレスへのTCP接続を許可していることを確認してください。

Browser content redirectionポリシーを使用してシングルサインオンを構成するには、Browser content redirection Integrated Windows Authentication support設定を参照してください。

または、VDAにレジストリキーを追加することで、Webサーバーへのシングルサインオンを有効にできます。詳細については、レジストリで管理される機能のリストにあるSingle sign-on with Integrated Windows Authentication for browser content redirectionを参照してください。

ユーザーエージェント要求ヘッダー

ユーザーエージェントヘッダーは、ブラウザコンテンツリダイレクトから送信されたHTTP要求を識別するのに役立ちます。この設定は、プロキシおよびファイアウォールルールを構成する際に役立ちます。たとえば、サーバーがブラウザコンテンツリダイレクトから送信された要求をブロックする場合、ユーザーエージェントヘッダーを含むルールを作成して、特定の要件をバイパスできます。

Windowsデバイスのみがユーザーエージェント要求ヘッダーをサポートします。

デフォルトでは、ユーザーエージェント要求ヘッダーストリングは無効になっています。クライアントレンダリングされたコンテンツのユーザーエージェントヘッダーを有効にするには、レジストリエディターを使用します。詳細については、レジストリで管理される機能のリストにあるUser-agent request headerを参照してください。

ブラウザコンテンツリダイレクトクライアントの互換性

WMIを使用して、クライアントがブラウザコンテンツリダイレクトと互換性があるかどうかを確認できます。WMIにアクセスするための任意の方法を使用できます。以下はPowerShellを使用した例です。

1. PowerShellを開きます。
2. `Get-WmiObject -Class CTXBCRStatus`を実行します。
3. `BCR_Capable`パラメーターを確認します。
   - `True`の場合、クライアントはブラウザコンテンツリダイレクトと互換性があります。
   - `False`の場合、クライアントはブラウザコンテンツリダイレクトと互換性がありません。

追加情報

- `CtxBrowserSvc`が利用できない場合、コマンドの実行時に結果は表示されません。
- `CtxBrowserSvc`が一度も実行されていない場合、結果は無効なクラスエラーを返します。

HDX™ビデオ会議とウェブカメラビデオ圧縮

> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤用によって生じた問題が解決できることを保証できません。レジストリエディターはご自身の責任において使用してください。編集する前に必ずレジストリをバックアップしてください。

> ウェブカメラは、HDXウェブカメラビデオ圧縮またはHDXプラグアンドプレイ汎用USBリダイレクトを使用して、仮想セッション内で実行されているアプリケーションによって使用できます。モードを切り替えるには、**Citrix Workspace™アプリ > 環境設定 > デバイス**を使用します。Citrixは、可能な限り常にHDXウェブカメラビデオ圧縮を使用することを推奨します。HDX汎用USBリダイレクトは、HDXビデオ圧縮とのアプリケーション互換性の問題があ

> る場合、またはウェブカメラの高度なネイティブ機能が必要な場合にのみ推奨されます。パフォーマンスを向上させるために、CitrixはVirtual Delivery Agentに少なくとも2つの仮想CPUを搭載することを推奨します。

ユーザーがHDXウェブカメラビデオ圧縮から切り替えるのを防ぐには、**ICA®ポリシー設定 > USBデバイスポリシー**設定の下にあるポリシー設定を使用してUSBデバイスリダイレクトを無効にします。Citrix Workspaceアプリのユーザーは、Desktop Viewerの［マイクとウェブカメラ］設定で**マイクまたはウェブカメラを使用しない**を選択することで、デフォルトの動作を上書きできます。

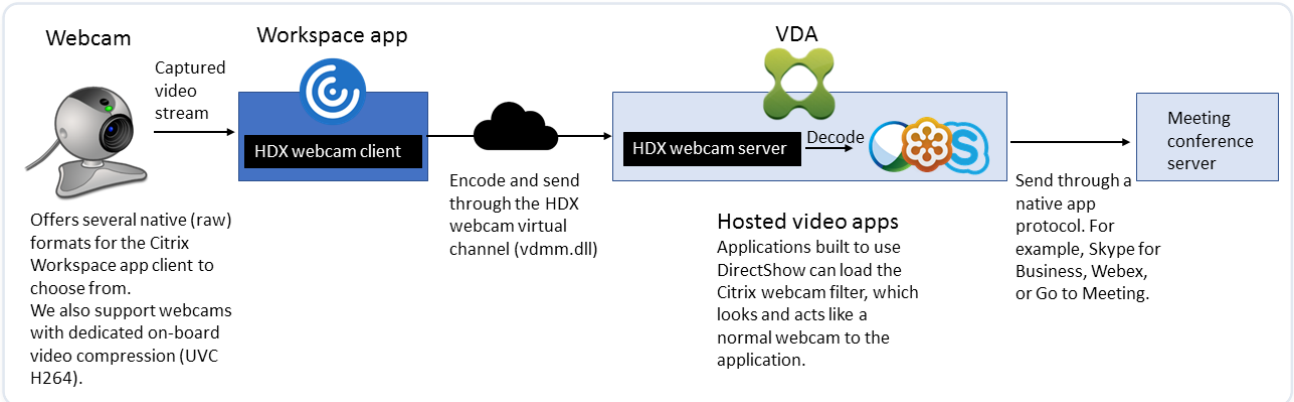
HDXウェブカメラビデオ圧縮

HDXウェブカメラビデオ圧縮は、**最適化された**ウェブカメラモードとも呼ばれます。この種類のウェブカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するため、HDXウェブカメラ圧縮はウェブカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAでレジストリキーを0に設定します。詳しくは、レジストリで管理される機能のリストにあるウェブカメラビデオ圧縮を参照してください。

ビデオストリーミングリソースのデフォルト機能を無効にすると、HDXウェブカメラビデオ圧縮は、クライアントオペレーティングシステムの一部であるマルチメディアフレームワークテクノロジーを使用して、キャプチャデバイスからのビデオをインターセプトし、トランスコードして圧縮します。キャプチャデバイスの製造元は、OSカーネルストリーミングアーキテクチャに接続するドライバーを提供します。

クライアントはウェブカメラとの通信を処理します。その後、クライアントはビデオを適切に表示できるサーバーにのみ送信します。サーバーはウェブカメラを直接処理しませんが、その統合によりデスクトップで同じエクスペリエンスが得られます。Workspaceアプリは、帯域幅を節約し、WANシナリオでの回復力を向上させるためにビデオを圧縮します。



HDXウェブカメラビデオ圧縮には、**マルチメディア会議**ポリシーを有効にする必要があります。このポリシーはデフォルトで有効になっています。

ウェブカメラがハードウェアエンコードをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコードを使用します。ハードウェアエンコードは、ソフトウェアエンコードよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントでレジストリキーを編集します。詳しくは、レジストリで管理される機能のリストにあるウェブカメラソフトウェア圧縮を参照してください。

HDXウェブカメラビデオ圧縮の要件

HDXウェブカメラビデオ圧縮は、Citrix Workspaceアプリの次のバージョンをサポートしています。

プラットフォーム	プロセッサ
Windows向けCitrix Workspaceアプリ	Citrix Workspace app for Windows は、XenApp および XenDesktop 7.17 以降の 32 ビットおよび 64 ビットアプリの Web カメラビデオ圧縮をサポートします。以前のバージョンでは、Citrix Workspace app for Windows は 32 ビットアプリのみをサポートします。
Mac向けCitrix Workspaceアプリ	Citrix Workspace app for Mac 2006 以降は、XenApp および XenDesktop 7.17 以降の 64 ビットアプリの Web カメラビデオ圧縮をサポートします。以前のバージョンでは、Citrix Workspace app for Mac は 32 ビットアプリのみをサポートします。
Linux向けCitrix Workspaceアプリ	Citrix Workspace app for Linux は、仮想デスクトップ上の 32 ビットおよび 64 ビットアプリの両方をサポートします。
Chrome向けCitrix Workspaceアプリ	一部の ARM Chromebook は H.264 エンコードをサポートしていないため、最適化された HDX Web カメラビデオ圧縮を使用できるのは 32 ビットアプリのみです。

Media Foundation ベースのビデオアプリケーションは、Windows 8.x 以降および Windows Server 2012 R2 以降で HDX Web カメラビデオ圧縮をサポートします。詳細については、Knowledge Center の記事 CTX132764 を参照してください。

その他のユーザーデバイスの要件：

- サウンドを生成するための適切なハードウェア。
- DirectShow 互換の Web カメラ（Web カメラのデフォルト設定を使用）。ハードウェアエンコード対応の Web カメラは、クライアント側の CPU 使用率を削減します。
- HDX Web カメラビデオ圧縮の場合、可能であれば、カメラメーカーから入手した Web カメラドライバーをクライアントにインストールします。デバイスドライバーのインストールはサーバーでは不要です。

異なるWebカメラは異なるフレームレートを提供し、明るさやコントラストのレベルも異なります。Webカメラのコントラストを調整すると、アップストリームトラフィックを大幅に削減できます。Citrixは、初期機能検証のために以下のWebカメラを使用しています。

- Microsoft LifeCam VXモデル（2000、3000、5000、7000）
- クリエイティブ ライブ！カム オプティア プロ
- ロジクール クイックカム メッセンジャー
- ロジクール C600、C920
- HP デラックス ウェブカメラ

優先するビデオフレームレートを調整するには、クライアントのレジストリキーを編集します。詳しくは、レジストリで管理される機能のリストにあるWebカメラビデオ圧縮フレームレートを参照してください。

高解像度Webカメラストリーミング

サーバー上のビデオ会議アプリケーションは、サポートされているフォーマットタイプに基づいてWebカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはWebカメラ情報をサーバーに送信します。アプリケーションからWebカメラを選択します。Webカメラとビデオ会議アプリケーションが高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。すべてのWebカメラ解像度をサポートしています。

この機能には、Citrix Workspaceアプリ for Windows（最小バージョン1808）またはCitrix Receiver for Windows（最小バージョン4.10）が必要です。

レジストリキーを使用して、この機能を無効化および有効化できます。詳しくは、レジストリで管理される機能のリストにある高解像度Webカメラストリーミングを参照してください。

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度（640 x 480 ピクセル）にフォールバックします。クライアントのレジストリキーを使用して、デフォルトの解像度を構成できます。カメラが指定された解像度をサポートしていることを確認してください。詳

しくは、レジストリで管理される機能のリストにある高解像度Webカメラ解像度を参照してください。

HDX Webカメラビデオ圧縮は、プラグアンドプレイの汎用USBリダイレクトと比較して帯域幅を大幅に少なく使用し、WAN接続でも良好に機能します。帯域幅を調整するには、クライアントのレジストリキーを設定します。詳しくは、レジストリで管理される機能のリストにある高解像度Webカメラ帯域幅を参照してください。

ビット/秒単位で値を入力します。帯域幅を指定しない場合、ビデオ会議アプリケーションはデフォルトで350000 bpsを使用します。

HDXプラグアンドプレイ汎用USBリダイレクト

HDX plug-n-play generic USB リダイレクト（アイソクロナス）は、**Generic** ウェブカメラモードとも呼ばれます。HDX plug-n-play generic USB リダイレクトの利点は、シンクライアント/エンドポイントにドライバーをインストールする必要がないことです。USB スタックは仮想化されているため、ローカルクライアントに接続したものはすべてリモート VM に送信されます。リモートデスクトップは、ネイティブに接続したかのように動作します。Windows デスクトップは、ハードウェアとのすべてのやり取りを処理し、プラグアンドプレイロジックを通じて適切なドライバーを見つけます。ほとんどのウェブカメラは、ドライバーがサーバーに存在し、ICA 経由で動作できる場合に機能します。Generic ウェブカメラモードは、非圧縮ビデオを USB プロトコルでネットワーク経由で送信するため、はるかに多くの帯域幅（毎秒数メガビット）を使用します。

HTML5 マルチメディアリダイレクト

HTML5 マルチメディアリダイレクトは、HDX™ MediaStream のマルチメディアリダイレクト機能を拡張し、HTML5 オーディオとビデオを含めます。マルチメディアコンテンツのオンライン配信、特にモバイルデバイスへの配信が増加しているため、ブラウザ業界はオーディオとビデオを提示するより効率的な方法を開発してきました。

Flash は標準でしたが、プラグインが必要で、すべてのデバイスで動作せず、モバイルデバイスではバッテリー消費量が多くなります。YouTube、Netflix、および Mozilla、Google、Microsoft の新しいブラウザバージョンなどの企業は、HTML5 に移行しており、これが新しい標準となっています。

HTML5 ベースのマルチメディアには、独自のプラグインに比べて以下のような多くの利点があります。

- 企業に依存しない標準 (W3C)
- 簡素化されたデジタル著作権管理 (DRM) ワークフロー

- プラグインによって引き起こされるセキュリティ問題なしにパフォーマンスが向上

HTTP プログレッシブダウンロード

HTTP プログレッシブダウンロードは、HTML5 をサポートする HTTP ベースの疑似ストリーミング方式です。プログレッシブダウンロードでは、ブラウザは HTTP Web サーバーからダウンロード中に単一のファイル（単一の品質でエンコードされたもの）を再生します。ビデオは受信時にドライブに保存され、ドライブから再生されます。ビデオを再視聴する場合、ブラウザはキャッシュからビデオを読み込むことができます。

プログレッシブダウンロードの例については、HTML5 ビデオリダイレクトテストページ を参照してください。Web ページ内のビデオ要素を検査し、HTML5 ビデオタグ内のソース（mp4 コンテナ形式）を見つけるには、ブラウザの開発者ツールを使用します。

HTML5 と Flash の比較

機能	HTML5	フラッシュ
独自のプレーヤーが必要	いいえ	はい
モバイルデバイスで動作	はい	一部
さまざまなプラットフォームでの実行速度	高い	遅い
iOSでサポート	はい	いいえ
リソース使用量	少ない	多い
より速くロード	はい	いいえ

要件

mp4形式のプログレッシブダウンロードのリダイレクトのみをサポートしています。WebMやDASH/HLSのようなアダプティブビットレートストリーミング技術はサポートしていません。

以下をサポートしており、ポリシーを使用して制御します。詳細については、「マルチメディアポリシー設定」を参照してください。

- サーバー側レンダリング
- サーバーフェッチクライアントレンダリング
- クライアント側フェッチとレンダリング

Citrix Workspace™アプリおよびCitrix Receiver™の最小バージョン:

- Windows用Citrix Workspaceアプリ1808
- Windows用シトリックス レシーバー 4.5
- Linux用Citrix Workspaceアプリ1808
- Linux版 Citrix レシーバー 13.5

最小VDAブラウザーバージョン	WINDOWS オペレーティングシステムのバージョン、ビルド、サービスパック
インターネット エクスプローラー 11.0	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1)；ウィンドウズ 7 x86 および x64；ウィンドウズ Server 2016 RTM 14393 (1607)；ウィンドウズ Server 2012 R2
Firefox 47 証明書を手動でFirefox証明書ストアに追加するか、Windowsの信頼された証明書ストアから証明書を検索するようにFirefoxを設定します。詳細については、`https://wiki.mozilla.org/CA:AddRootToFirefox`を参照してください。	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1); ウィンドウズ 7 x86 および x64; ウィンドウズ サーバー 2016 RTM 14393 (1607); ウィンドウズ サーバー 2012 R2
クローム 51	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1); ウィンドウズ 7 x86 および x64; ウィンドウズ サーバー 2016 RTM 14393 (1607); ウィンドウズ サーバー 2012 R2

HTML5ビデオリダイレクトソリューションのコンポーネント

- **HdxVideo.js** - ウェブサイト上のビデオコマンドを傍受するJavaScriptフック。HdxVideo.jsは、セキュアWebSocket（SSL/TLS）を使用してWebSocketServiceと通信します。
- **WebSocket SSL証明書**
  - CA（ルート）の場合：**Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA) 場所：**証明書（ローカルコンピューター） > 信頼されたルート証明機関 > 証明書**。
  - エンドエンティティ（リーフ）の場合：**Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and

XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service) 場所：**証明書（ローカルコンピューター） > 個人 > 証明書**。

- **WebSocketService.exe** - ローカルシステムで実行され、SSL終端とユーザーセッションマッピングを実行します。127.0.0.1のポート9001でTLSセキュアWebSocketがリッスンしています。
- **WebSocketAgent.exe** - ユーザーセッションで実行され、WebSocketServiceコマンドの指示に従ってビデオをレンダリングします。

HTML5ビデオのリダイレクトを有効にするにはどうすればよいですか?

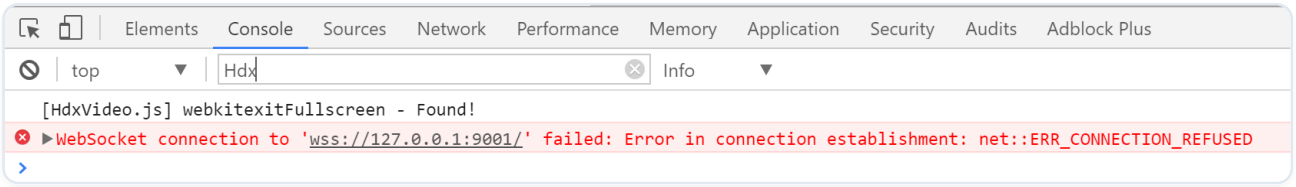
このリリースでは、この機能は制御されたウェブページでのみ利用可能です。HTML5マルチメディアコンテンツが利用可能なウェブページに、HdxVideo.js JavaScript（Citrix Virtual Apps and Desktopsインストールメディアに含まれています）を追加する必要があります。例えば、社内トレーニングサイトのビデオなどです。

youtube.comのような、アダプティブビットレート技術（例：HTTPライブストリーミング（HLS）やHTTP経由のダイナミックアダプティブストリーミング（DASH））に基づいたウェブサイトはサポートされていません。

詳細については、「*マルチメディアポリシー設定*」を参照してください。

トラブルシューティングのヒント

ウェブページがHdxVideo.jsを実行しようとすると、エラーが発生する可能性があります。JavaScriptの読み込みに失敗すると、HTML5リダイレクトメカニズムが機能しません。ブラウザの開発者ツールウィンドウでコンソールを検査し、HdxVideo.jsに関連するエラーがないことを確認してください。例：



Microsoft Teams の最適化

> **注:**
>
> 新しい Microsoft Teams 2.1 は、VDA で一般提供されるようになりました。この Microsoft Teams バージョンは、WebRTC (VDI 1.0) を使用した Citrix Microsoft Teams Optimization と

> 互換性があります。これには、新しい Microsoft Teams が Citrix 仮想チャネルにアクセスできるように、VDA で新しいレジストリ構成設定が必要です。 Microsoft Teams 2.1 の最適化を有効にするには、VDA で次のレジストリキーを構成します。

> 場所: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`

> キー (REG_Multi_SZ): `ProcessWhitelist`

> 値: `msedgewebview2.exe`

> 詳細については、Microsoftドキュメントを参照してください。

> Citrixは、Citrix Virtual Apps and Desktops™およびCitrix Workspace™アプリを使用して、デスクトップベースのMicrosoft Teams向けに最適化を提供します。デフォルトでは、必要なすべてのコンポーネントをCitrix WorkspaceアプリとVirtual Delivery Agent (VDA) にバンドルしています。

Microsoft Teams の最適化には、VDA 側の HDX™ サービスと、コマンドを受信するために Microsoft Teams ホスト型アプリとインターフェースする API が含まれています。これらのコンポーネントは、制御仮想チャネル (CTXMTOP) を Citrix Workspace アプリ側のメディアエンジンに開きます。エンドポイントはマルチメディアをローカルでデコードして提供し、Citrix Workspace アプリのウィンドウをホストされている Microsoft Teams アプリに戻します。

認証とシグナリングは、他のMicrosoft Teamsサービス (チャットやコラボレーションなど) と同様に、Microsoft Teamsホスト型アプリでネイティブに発生します。オーディオ/ビデオのリダイレクトはこれらに影響しません。

`CTXMTOP`はコマンドおよび制御仮想チャネルです。これは、Citrix WorkspaceアプリとVDAの間でメディアが交換されないことを意味します。

クライアントフェッチ/クライアントレンダリングのみが利用可能です。

このビデオデモンストレーションでは、Citrix 仮想環境で Microsoft Teams がどのように機能するかを理解できます。



Microsoft Teamsのインストール

CitrixとMicrosoftは、Microsoft Teamsの最新バージョンを利用し、常に最新の状態に保つことを推奨しています。 現在のバージョンのリリース日から90日以上古いリリース日のMicrosoft Teamsデスクトップアプリのバージョンはサポートされていません。 サポートされていないMicrosoft Teamsデスクトップアプリのバージョンは、ユーザーにブロックページを表示し、アプリの更新を要求します。

最新の利用可能なバージョンについては、「Update history for Microsoft Teams App (Desktop and Mac)」を参照してください。

Microsoft Teamsのコンピューター全体へのインストールガイドラインに従うことをお勧めします。Microsoft Teamsを`AppData`にインストールする.exeインストーラーの使用は避けてください。代わりに、コマンドラインから`ALLUSER=1`フラグを使用して`C:\Program Files (x86)\Microsoft\Teams`にインストールしてください。

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

この例では、`ALLUSERS=1`パラメーターも使用しています。このパラメーターを設定すると、Microsoft Teams Machine-Wide Installerが**コントロールパネル**の**プログラムと機能**に表示されます。また、コンピューターのすべてのユーザーに対して、Windowsの設定の**アプリと機能**にも表示されます。管理者資格情報を持つすべてのユーザーは、Microsoft Teamsをアンインストールできます。

`ALLUSERS=1`と`ALLUSER=1`の違いを理解することが重要です。`ALLUSERS=1`パラメーターは、非VDI環境とVDI環境の両方で使用できます。`ALLUSER=1`パラメーターは、マシンごとのインストールを指定するためにVDI環境でのみ使用してください。

`ALLUSER=1`モードでは、新しいバージョンがリリースされてもMicrosoft Teamsアプリケーションは自動更新されません。このモードは、Windows ServerまたはWindows 10のランダム/プールされたカタログからのホスト型共有アプリやデスクトップなど、非永続的な環境に推奨されます。詳細については、「Install Microsoft Teams using MSI」(VDIインストールセクション)を参照してください。

Windows 10専用の永続VDI環境があるとします。Microsoft Teamsアプリケーションを自動更新し、Microsoft Teamsを`Appdata/Local`の下にユーザーごとにインストールしたい場合は、`.exe`インストーラーまたは`ALLUSER=1`なしのMSIを使用してください。

> **注:**

Citrixでは、ゴールデンイメージにMicrosoft Teamsをインストールする前にVDAをインストールすることを推奨しています。このインストール順序は、`ALLUSER=1`フラグを有効にするために必要です。VDAをインストールする前に仮想マシンにMicrosoft Teamsをインストールした場合は、Microsoft Teamsをアンインストールして再インストールしてください。

Remote PC Accessの場合

Citrixは、VDAのインストール後にMicrosoft Teamsバージョン1.4.00.22472以降をインストールすることを推奨しています。そうしないと、Microsoft TeamsがVDAを期待どおりに検出するために、サインアウトして再度サインインする必要があります。バージョン1.4.00.22472以降には、VDA検出のためにMicrosoft Teamsの起動時およびサインイン時に実行される拡張ロジックが含まれています。これらのバージョンには、アクティブなセッションタイプ識別（HDX、RDP、またはクライアントマシンにローカル接続）も含まれています。ローカル接続している場合、以前のバージョンのMicrosoft Teamsは、特定の機能やUI要素（ブレイクアウトルーム、会議やチャットのポップアウトウィンドウ、会議のリアクションなど）を検出して無効にできない場合があります。

重要:

ローカルセッションからHDXセッションにローミングし、Microsoft Teamsがバックグラウンドで開いたまま実行されている場合、HDXで正しく最適化するには、Microsoft Teamsを終了して再起動する必要があります。 逆に、最適化されたHDXセッションを介してMicrosoft Teamsをリモートで使用している場合、HDXセッションを切断し、デバイスで同じWindowsセッションにローカルで再接続します。オフィスで作業している場合は、Microsoft TeamsがRemote PC Accessの状態（HDXまたはローカル）を正しく検出できるように、Microsoft Teamsを再起動する必要があります。これは、Microsoft TeamsがVDIモードを評価できるのはアプリの起動時のみであり、バックグラウンドで既に実行されている間は評価できないためです。再起動しないと、Microsoft Teamsはポップアウトウィンドウ、ブレイクアウトルーム、会議のリアクションなどの機能をロードできない場合があります。

App Layeringの場合

Citrix App Layering を使用して、異なるレイヤーで VDA と Microsoft Teams のインストールを管理している場合、コマンドラインから `ALLUSER=1` フラグを指定して Microsoft Teams をインストールする前に、Windows VDA 上にレジストリキーを作成する必要があります。詳細については、マルチメディア の「*Citrix App Layering を使用した Microsoft Teams の最適化*」セクションを参照してください。

プロファイル管理の推奨事項

Windows ServerおよびプールされたVDI Windows 10環境には、マシン全体のインストーラーを使用することをお勧めします。

コマンドラインから MSI に **ALLUSER=1** フラグが渡されると（マシン全体のインストーラー）、Microsoft Teams アプリは `C:\Program Files (x86)`（約 300 MB）にインストールされます。このアプリは、ログに `AppData\Local\Microsoft\TeamsMeetingAddin` を使用し、ユーザー固有の構成、ユーザーインターフェイスの要素のキャッシュなどに `AppData\Roaming\Microsoft\Teams`（約 600〜700 MB）を使用します。

> **重要:**

> **ALLUSER=1**フラグを渡さない場合、MSIはTeams.exeインストーラーと`setup.json`を`C:\Program Files (x86)\Teams Installer`に配置します。レジストリキー（TeamsMachineInstaller）は`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`の下に追加されます。

> その後のユーザーログオンにより、代わりに **AppData** に最終インストールがトリガーされます。

マシン全体のインストーラー

以下は、Windows Server 2016 64ビットVMにMicrosoft Teamsマシンワイドインストーラーをインストールすることによって作成されるフォルダー、デスクトップショートカット、およびレジストリの例です。

フォルダー:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

レジストリ:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- 名前: `Teams`
- 種類: `REG_SZ`
- 値: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **注:**
>
> レジストリの場所は、基盤となるオペレーティングシステムとビット数によって異なります。

推奨事項

- Microsoft Teams のレジストリキーを削除して、自動起動を無効にすることをお勧めします。これにより、同時に発生する多数のログオン（たとえば、勤務開始時など）による VM の CPU スパイクを防ぐことができます。
- 仮想デスクトップに GPU/vGPU がない場合は、パフォーマンスを向上させるために、Microsoft Teams の で を設定することをお勧めします。この設定 (`"disableGpu":true`) は、`desktop-config.json` の `%Appdata%\Microsoft\Teams` に保存されます。ログオンスクリプトを使用してそのファイルを編集し、値を `true` に設定できます。
- Citrix Workspace Environment Management™ (WEM) を使用している場合は、Microsoft Teams のプロセッサ消費を管理するために を有効にします。

ユーザーごとのインストーラー

`.exe` インストーラーを使用する場合、インストールプロセスが異なります。すべてのファイルは AppData に配置されます。

フォルダー:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`

- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

レジストリ:

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

ベストプラクティス

ベストプラクティスの推奨事項は、ユースケースシナリオに基づいています。 非永続的な設定でMicrosoft Teamsを使用する場合、効率的なMicrosoft Teamsランタイムデータ同期のためにプロファイルキャッシュマネージャーが必要です。プロファイルキャッシュマネージャーを使用すると、ユーザーセッション中に適切なユーザー固有の情報がキャッシュされます。たとえば、ユーザー固有の情報には、ユーザーデータ、プロファイル、設定が含まれます。これら2つのフォルダーのデータを同期します。

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

非永続的セットアップ向けの Microsoft Teams キャッシュコンテンツ除外リスト

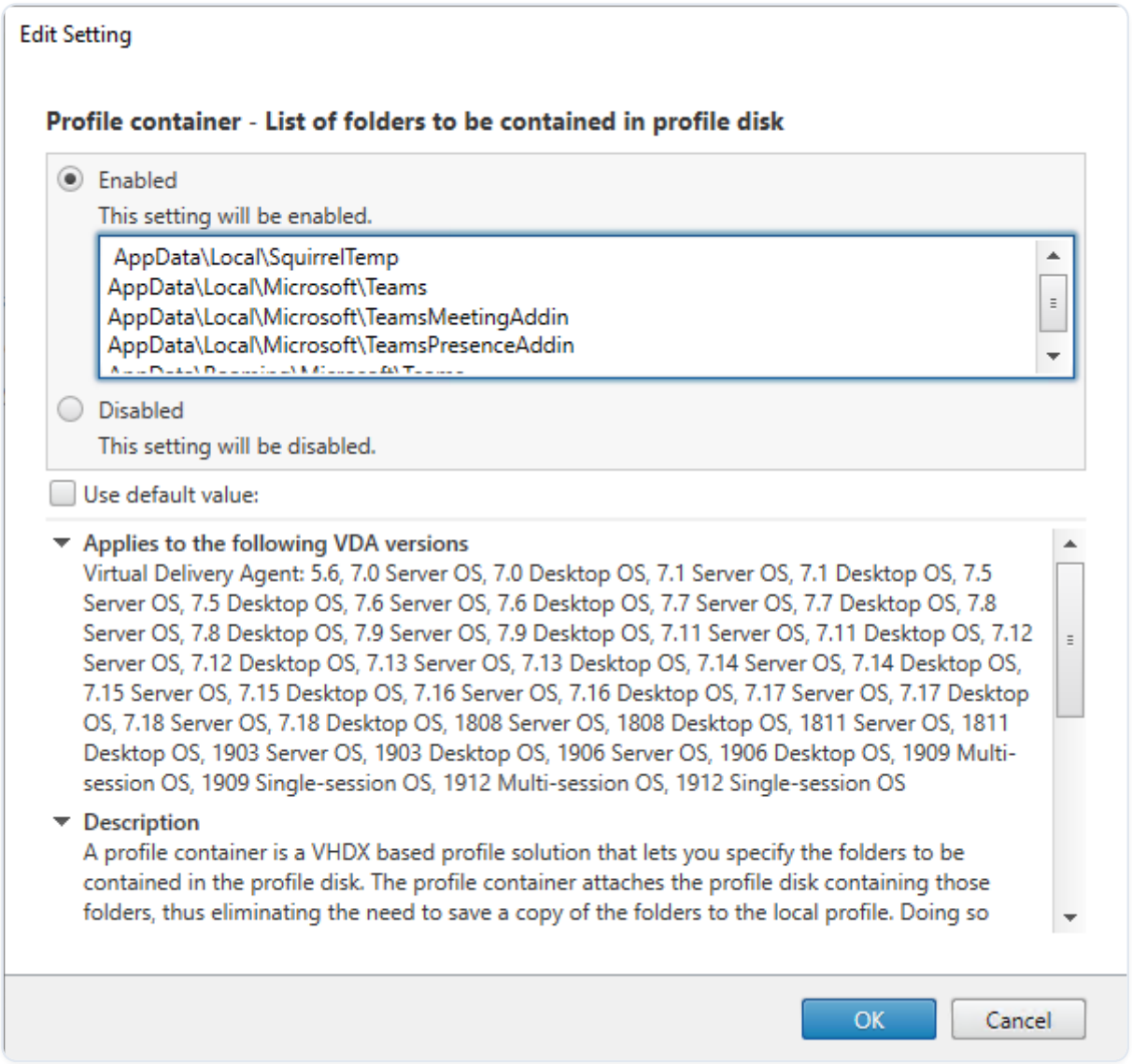
Microsoftドキュメントに記載されているように、Microsoft Teamsのキャッシュフォルダーからファイルとディレクトリを除外します。この操作は、ユーザーキャッシュサイズを削減し、非永続的なセットアップをさらに最適化するのに役立ちます。

ユースケース: シングルセッションシナリオ

このシナリオでは、エンドユーザーは一度に1つの場所でMicrosoft Teamsを使用します。同時に2つのWindowsセッションでMicrosoft Teamsを実行する必要はありません。一般的な仮想デスクトップ展開では、各ユーザーに1つのデスクトップが割り当てられ、Microsoft Teamsは仮想デスクトップに1つのアプリケーションとして展開されます。 Citrix Profileコンテナを有効にし、ユーザーごとのインストーラーにリストされているユーザーごとのディレクトリをコンテナにリダイレクトすることをお勧めします。

1. ゴールデンイメージにMicrosoft Teamsのコンピューター全体インストーラー (**ALLUSER=1**) を展開します。
2. Citrix Profile Managementを有効にし、適切な権限でユーザープロファイルストアを設定します。

3. 次のProfile Managementポリシー設定を有効にします: **ファイルシステム > 同期 > プロファイルコンテナ – プロファイルディスクに含めるフォルダーのリスト。**



この構成で、すべてのユーザーごとのディレクトリをリストします。これらの設定は、Citrix Workspace Environment Management (WEM) サービスを使用して構成することもできます。

4. 設定を正しいデリバリーグループに適用します。
5. ログインして展開を検証します。

システム要件

推奨される最小バージョン - Delivery Controller (DDCs) 1906.2

以前のバージョンを使用している場合は、Microsoft Teamsの最適化を有効にするを参照してください:

サポートされているオペレーティングシステム:

- Windows Server 2022、2019、2016、2012R2 StandardおよびDatacenter Edition、およびServer Coreオプション付き

最小バージョン - Virtual Delivery Agents (VDA) 1906.2

サポートされているオペレーティングシステム:

- ウィンドウズ 11
- Windows 10 64ビット、バージョン1607以降。VMホスト型アプリは、Citrix Workspaceアプリ 2109.1 for Windows以降でサポートされています
- Windows Server 2022、2019、2016、および2012 R2 (StandardおよびData Centerエディション)

要件:

- BCR_x64.msi - Microsoft Teamsの最適化コードを含み、GUIから自動的に起動するMSI。VDAインストールのコマンドラインインターフェイスを使用している場合は、除外しないでください。

推奨バージョン – Citrix Workspaceアプリ for Windows 最新CR、および最小バージョン – Citrix Workspaceアプリ 1907 for Windows

- Windows 11です。
- Windows 10 (32ビットおよび64ビットエディション、Embeddedエディションを含む) (Windows 7のサポートはバージョン2006で終了) (Windows 8.1のサポートはバージョン2204.1で終了)。
- Windows 10 IoT Enterprise 2016 LTSB (バージョン 1607) および 2019 LTSC (バージョン 1809)。
- サポートされているプロセッサ (CPU) アーキテクチャ: x86およびx64 (ARMはサポートされていません)。
- エンドポイント要件: ピアツーピアビデオ会議中に720p HD解像度をサポートできる約2.2～2.4 GHzのデュアルコアCPU。
- Intel Turbo BoostまたはAMD Turbo Coreを搭載し、少なくとも2.4 GHzまでブーストできる、ベース速度が低い（約1.5 GHz）デュアルコアまたはクアッドコアCPU。
- 検証済みHPシンクライアント: t630/t640、t730/t740、mt44/mt45。
- 検証済みDellシンクライアント: 5070、5470 Mobile TCおよびAIO。
- 10ZiG Thin Client の検証済みモデル: 4510 および 5810q。
- 検証済みエンドポイントの完全なリストについては、Thin Clients を参照してください。

- Citrix Workspaceアプリには、最低600 MBの空きディスク容量と1 GBのRAMが必要です。
- Microsoft .NET Framework の最小要件はバージョン 4.8 です。Citrix Workspaceアプリは、システムに.NET Frameworkが存在しない場合、自動的にダウンロードしてインストールします。

管理者は、Microsoft Teams Optimization policy を変更することで、最適化モードでMicrosoft Teamsを有効/無効にできます。Citrix Workspaceアプリで最適化モードを開始したユーザーは、Microsoft Teamsを無効にできません。

最小バージョン - Linux向けCitrix Workspaceアプリ 2006

詳細については、Linux向けCitrix Workspaceアプリのドキュメントにある Optimization for Microsoft Teams を参照してください。

ソフトウェア:

- `GStreamer` 1.0以降、またはCairo 2
- `libc++-9.0` 以降
- `libgdk` 3.22以降
- OpenSSL 1.1.1d
- `libnsl`
- Ubuntu 20.04 以降

認証の強化:

- Libsecretライブラリ
- libunwind-12ライブラリ。詳しくは、llvm-12のlibunwind-12ライブラリ依存関係の追加を参照してください。

ハードウェア:

- ピアツーピアのビデオ会議通話中に720p HD解像度をサポートできる、最低1.8 GHzのデュアルコアCPU
- ベース速度1.8 GHz、Intel Turbo Boostの最大速度2.9 GHz以上のデュアルコアまたはクアッドコアCPU

動作確認済みエンドポイントの完全なリストについては、「シンクライアント」を参照してください。

詳細については、Citrix Workspaceアプリをインストールするための前提条件を参照してください。

`/opt/Citrix/ICAClient/config/module.ini`ファイルで**VDWEBRTC**フィールドの値をOffに更新すると、Microsoft Teamsの最適化を無効にできます。デフォルトはVDWEBRTC=Onです。更新が完了したら、セッションを再起動してください。(ルート権限が必要です)。

最小バージョン - Mac用Citrix Workspaceアプリ2012

サポートされているオペレーティングシステム:

- macOS Catalina (バージョン 10.15)。
- macOS Big Sur 11.0.1以降。
- macOS モントレー。

サポートされている機能:

- オーディオ
- ビデオ
- 画面共有の最適化（受信および送信）

> **注：**

> 画面共有を機能させるには、Citrix Viewerアプリがmacosの「セキュリティとプライバシー」設定へのアクセスを必要とします。ユーザーは、**Appleメニュー > システム環境設定 > セキュリティとプライバシー > プライバシー > 画面収録**でこの設定を構成し、**Citrix Viewer**を選択します。

> Microsoft Teamsの最適化は、Citrix Workspaceアプリ2012以降およびmacOS 10.15でデフォルトで動作します。

Microsoft Teamsの最適化を無効にする場合は、ターミナルでこのコマンドを実行し、Citrix Workspaceアプリを再起動してください。

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

最小バージョン - 最新バージョンのChromeOSで実行されているChromeOS用Citrix Workspaceアプリの最新バージョン

ハードウェア：

- Intel i3、クアッドコア2.4 GHzと同等以上の性能を持つプロセッサ。

サポートされる機能：

- オーディオ
- ビデオ
- 画面共有の最適化（受信および送信） - デフォルトで無効。有効にする方法については、これらの設定を参照してください。

シングルサーバーのスケーラビリティ

このセクションでは、単一の物理ホストでサポートできるユーザー数または仮想マシン (VM) 数を推定するための推奨事項とガイダンスを提供します。これは一般的に、Citrix Virtual Apps and Desktops シングルサーバー スケーラビリティ (SSS) と呼ばれます。Citrix Virtual Apps (CVA) またはセッション仮想化のコンテキストでは、ユーザー密度としても一般的に知られています。その目的は、主要なハイパーバイザーを実行している単一のハードウェアで、どのくらいのユーザーまたはVMを実行できるかを特定することです。

> **注:**
>
> このセクションには、SSSを推定するためのガイダンスが含まれています。このガイダンスは大まかなものであり、お客様固有の状況や環境に必ずしも特化したものではない可能性があります。Citrix Virtual Apps and Desktops SSSを真に理解する唯一の方法は、Login VSIのようなスケーラビリティまたは負荷テストツールを使用することです。Citrixは、SSSを迅速に推定するためだけに、このガイダンスとこれらの簡単なルールを使用することを推奨します。ただし、Citrixは、特にハードウェアを購入したり、財務上の決定を下したりする前に、結果を検証するためにLogin VSIまたは選択した負荷テストツールを使用することを推奨します。

ハードウェア (テスト対象システム)

- デル PowerEdge R740
- Intel Xeon (Gold) 6126 @ 2.60 GHz (最大ターボ 3.70 GHz)、ソケットあたり12コア、ハイパースレッディング有効のデュアルソケット
- 382 GBのRAM
- ローカルSSD RAID 0ストレージ (11ディスク) 6 TB

ソフトウェア

Windows 2019 (TSVDA) を実行する単一の仮想マシン (40論理プロセッサ) とCitrix Virtual Apps and Desktops 2106 VMware ESXi 6.7

用語

- ナレッジワーカーのワークロード: Acrobat Reader、Freemind/Java、フォトビューアー、Edge、およびExcel、Outlook、PowerPoint、WordなどのMS Officeアプリが含まれます。
- ベースライン: ナレッジワーカーのワークロード (Microsoft Teamsなし) で実行されるサーバースケーラビリティ テスト。
- Microsoft Teamsワークロード: ナレッジワーカーの一般的なワークロード + Microsoft Teams。

Microsoft Teams のストレステスト方法

- Microsoft Teams は HDX で最適化されています。そのため、すべてのマルチメディア処理はエンドポイントまたはクライアントにオフロードされ、測定には含まれません。
- ワークロードが開始される前に、すべての Microsoft Teams プロセスが停止または終了されます。
- Microsoft Teams を開く（コールドスタート）。
- Microsoft Teams がロードされ、Microsoft Teams のプライマリウィンドウがフォーカスを取得するまでにかかる時間を測定します。
- キーボードショートカットを使用してチャットウィンドウに切り替えます。
- キーボードショートカットを使用してカレンダーウィンドウに切り替えます。
- キーボードショートカットを使用して、特定のユーザーにチャットメッセージを送信します。
- キーボードショートカットを使用してMicrosoft Teamsウィンドウに切り替える。

結果

- ベースライン（137ユーザー）と比較して、Microsoft Teamsワークロード（81ユーザー）ではスケーラビリティに40%の影響があります。
- サーバー容量を約40%（CPUで）増やすと、ベースラインワークロードの場合と同じユーザー数に戻ります。
- ベースラインと比較して、Microsoft Teamsワークロードでは20%の追加メモリが必要です。
- ユーザーあたりのストレージサイズを512～1024 MB増やします。

- IOPS書き込みが約50%増加し、IOPS読み取りが約100%増加します。Microsoft Teamsは、ストレージが遅い環境では大きな影響を与える可能性があります。

機能マトリックスとバージョンサポート

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	CITRIX WORKSPACEアプリ FOR MAC（最小バージョン）	CITRIX WORKSPACEアプリ FOR LINUX（最小バージョン）	CITRIX WORKSPACEアプリ FOR CHROME OS（最小バージョン）
オーディオ/ビデオ (P2P および会議)	現在のバージョンから90日前	1906	1907	2009	2004	2105.5
画面共有	現在のバージョンから90日前	1906	1907	2012	2006	2105.5
i. 画面インジケーターの赤い枠線	現在のバージョンから90日前	1906	2002	2012	2006	いいえ
ii. キャプチャをDesktop Viewerに限定する	現在のバージョンから90日前	1906	2009.5	2012	2006	なし
iii. マルチモニター	現在のバージョンより90日前	1912 CU6+	2106 (1)	2106	2106	なし
DTMF	現在のバージョ	該当なし	2102	2101	2101	2111.1

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	CITRIX WORKSPACEアプリ FOR MAC（最小バージョン）	CITRIX WORKSPACEアプリ FOR LINUX（最小バージョン）	CITRIX WORKSPACEアプリ FOR CHROME OS（最小バージョン）
	ンより90日前					
プロキシサーバーのサポート	現在のバージョンから90日前	該当なし	2012 (2)	2104 (3)	2101 (3)	2305
アプリ共有	現在のバージョンから90日前	2109	2109.1	2203.1	2209	いいえ
ライブキャプション	現在のバージョンから90日前	N/A (4)	2109.1	2109	2109	2303
動的e911	現在のバージョンから90日前	N/A	2112.1	2112	2112	2112
制御を付与	現在のバージョンから90日前	該当なし	2112.1	2203.1	いいえ	いいえ
制御を要求	現在のバージョンから90日前	該当なし	2112.1	2203.1	2203	2303

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	CITRIX WORKSPACEアプリ FOR MAC（最小バージョン）	CITRIX WORKSPACEアプリ FOR LINUX（最小バージョン）	CITRIX WORKSPACEアプリ FOR CHROME OS（最小バージョン）
マルチウィンドウ	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
会議の文字起こし	現在のバージョンから90日遡ったもの	2112.1, 1912 CU6+	2112	2203.1	2203	2303
背景ぼかし	現在のバージョンから90日遡ったもの	2112, 1912 CU6+	2207	2301	2212	2303

1. CD Viewerは全画面モードのみ。SHIFT+F2はサポートされていません。
2. Negotiate/Kerberos、NTLM、Basic、およびDigest。`Pac`ファイルもサポートされています。
3. 匿名のみ。
4. VDAが2112以降の場合、ライブキャプションは、Citrix Workspaceアプリのバージョンが MAC用2203.1、Linux用2203、またはWindows用2112の場合にのみ機能します。これは、Microsoft Teamsがシングルウィンドウ UIモードまたはマルチウィンドウモードの場合、ライブキャプションの動作が異なるためです。
5. MultiWindowは2112 VDAで導入されましたが、VDA 1912 LTSR CU6リリースにバックポートされました。

> **注:**

- **Citrix Workspace app for Windows 1912 CU6 (またはそれ以降)**に記載されているすべての機能は、Citrix Workspace app for Windows 2203.1 LTSR CU1に適用されます。
- Microsoftは、Microsoft Teamsにおけるシングルウィンドウモードのサポートを非推奨としました。これに対応するため、VDAを1912 CU6+ LTSRに、Citrix Workspaceアプリを2203 CU2+以降にアップグレードする必要があります。これらはマルチウィンドウモードをサポートしています。

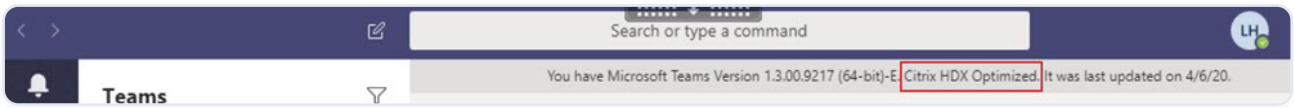
Microsoft Teamsの最適化を有効にする

Microsoft Teams の最適化を有効にするには、Microsoft Teams リダイレクト ポリシーで説明されている管理コンソールポリシーを使用します。このポリシーはデフォルトで**オン**になっています。このポリシーが有効になっていることに加えて、HDX は Citrix Workspace アプリのバージョンが最小要件バージョン以上であることを確認します。ポリシーを有効にし、Citrix Workspace アプリのバージョンがサポートされている場合、VDA 上で **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** が自動的に **1** に設定されます。Microsoft Teams は、VDI モードでロードするためにこのキーを読み取ります。

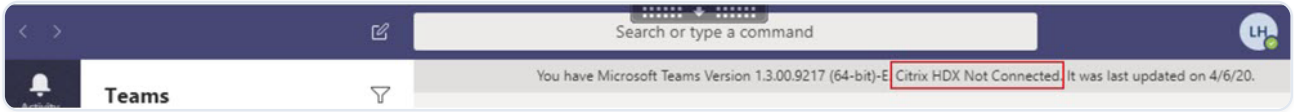
注:

バージョン1906.2以降のVDA、またはManageコンソール（Studio）でポリシーが利用できない古いコントローラーバージョン（バージョン7.15など）を使用している場合でも、VDAを最適化できます。Microsoft TeamsのHDX最適化は、VDAでデフォルトで有効になっています。

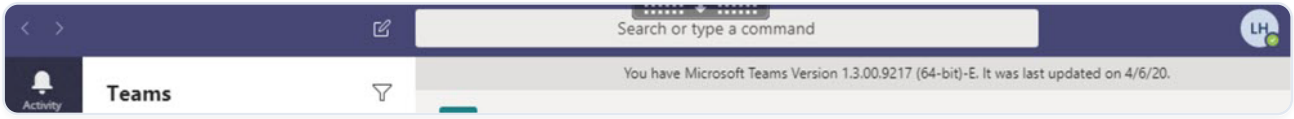
About > Versionをクリックすると、**Citrix HDX Optimized**の凡例が表示されます。



Citrix HDX Not Connected と表示される場合、Citrix API は Microsoft Teams にロードされています。API のロードはリダイレクトへの最初のステップです。しかし、スタックの後続の部分でエラーが発生しています。エラーは VDA サービスまたは Citrix Workspace アプリにある可能性が最も高いです。



凡例が表示されない場合、Microsoft Teams は Citrix API のロードに失敗しました。通知領域のアイコンを右クリックして Microsoft Teams を終了し、再起動してください。管理コンソールポリシーが**禁止**に設定されておらず、Citrix Workspace アプリのバージョンがサポートされていることを確認してください。



重要: セッションの再接続

- 接続が変更された場合、HDX 最適化セッションを取得するために Microsoft Teams を再起動する必要がある場合があります。たとえば、サポートされていないエンドポイント (iOS、Android 用 Workspace アプリ、または Windows/Linux/Mac の古いバージョン) からサポートされているエンドポイント (Windows/Linux/Mac/ChromeOS/HTML5 用 Workspace アプリ) にローミングする場合、またはその逆の場合です。
- VDA に Microsoft Teams .exe インストーラーを使用してアプリをインストールした場合も、Microsoft Teams の再起動が必要です。.exe インストーラーは、永続的な VDI 展開に推奨されます。そのような場合、HDX セッションが切断状態にある間に Microsoft Teams が自動更新されることがあります。そのため、HDX セッションに再接続するユーザーは、Microsoft Teams が最適化されて実行されていないことに気づきます。
- ローカルセッションから HDX セッションにローミングする場合、HDX で最適化するために Microsoft Teams を再起動する必要があります。この操作は、リモート PC アクセスシナリオで必要です。

ネットワーク要件

Microsoft Teamsは、会議や多人数通話のためにMicrosoft 365のメディアプロセッササーバーに依存しています。また、Microsoft Teamsは以下のシナリオでMicrosoft 365トランスポートリレーに依存しています。

- ポイントツーポイント通話の2つのピアが直接接続されていない
- 参加者がメディアプロセッサに直接接続されていない。

したがって、ピアとMicrosoft 365クラウド間のネットワークの状態が通話のパフォーマンスを決定します。ネットワーク計画に関する詳細なガイドラインについては、Microsoft 365 network connectivity principlesを参照してください。

クラウド音声およびビデオの全体的な展開に影響を与える可能性のあるリスクと要件を特定するために、環境を評価することをお勧めします。 ネットワークがMicrosoft Teamsに対応しているかどうかをテストするには、Skype for Business Network Assessment Toolを使用してください。サポート情報については、Supportを参照してください。

リアルタイムプロトコル (RTP) トラフィックに関する主要なネットワーク推奨事項の概要

- 支社からMicrosoft 365ネットワークに可能な限り直接接続してください。
- 支社で十分な帯域幅を計画し、提供してください。
- 各支社のネットワーク接続と品質を確認してください。
- 支社で以下のいずれかを使用する必要がある場合は、RTP/UDPトラフィック (Citrix WorkspaceアプリのHdxRtcEngine.exeによって処理されます) が妨げられないことを確認してください。
  - プロキシサーバーのバイパス
  - ネットワークSSLインターセプト
  - ディープパケットインスペクションデバイス
  - VPNヘアピン (可能であればスプリットトンネリングを使用)

> **重要: VPNスプリットトンネル構成**

> HdxRtcEngine.exe トラフィックは VPN トンネルから迂回させ、ユーザーのローカルインターネット接続を使用してサービスに直接接続できるようにする必要があります。これを実現する方法は、使用する VPN 製品とマシンプラットフォームによって異なりますが、ほとんどの VPN ソリューションでは、このロジックを適用するためのポリシーの簡単な設定が可能です。VPN プラットフォーム固有の分割トンネルガイダンスの詳細については、こちらの Microsoft の記事を参照してください。

> Workspace アプリの WebRTC メディアエンジン (HdxRtcEngine.exe) は、クライアントにオフロードされるマルチメディアストリームに Secure Real-time Transport Protocol (SRTP) を使用します。SRTP は RTP に機密性と認証を提供します。この機能では、対称鍵 (DTLS とネゴシエート) を使用して、AES 暗号化方式でメディアと制御メッセージを暗号化します。

良好なユーザーエクスペリエンスのために、以下のメトリックが推奨されます。

メトリック	エンドポイントからMICROSOFT 365まで
遅延 (片道)	50 ミリ秒未満
遅延 (RTT)	100 ミリ秒未満
パケット損失	15 秒間隔で 1% 未満
パケット到着間隔ジッター	15 秒間隔で 30 ミリ秒未満

詳細については、Microsoft Teams 用に組織のネットワークを準備するを参照してください。

帯域幅要件については、Microsoft Teams の最適化では、オーディオ (OPUS/G.722/PCM G711) およびビデオ (H264) にさまざまなコーデックを使用できます。

ピアは、セッション記述プロトコル (SDP) のオファー/アンサーを使用して、通話確立プロセス中にこれらのコーデックをネゴシエートします。 ユーザーあたりのCitrixの最小推奨事項は次のとおりです。

タイプ	帯域幅	コーデック
オーディオ (双方向)	約 90 kbps	G.722
オーディオ (双方向)	約 60 kbps	オーパス*
ビデオ (双方向)	約 700 kbps	H.264 360p、30フレーム/秒、16:9
画面共有	約 300 kbps	H264 1080p で 15 fps

* Opus は、6 kbps から 510 kbps までの定数および可変ビットレートエンコーディングをサポートしています。

OpusとH264は、ピアツーピアおよび電話会議に推奨されるコーデックです。

重要:

パフォーマンスに関して、クライアントマシンでのCPU使用量では、エンコードはデコードよりもコストがかかります。LinuxおよびWindows版Citrix Workspaceアプリで、最大エンコード解像度をハードコードできます。「エンコーダーパフォーマンス見積もり」および「Microsoft Teamsの最適化」を参照してください。

プロキシサーバー

プロキシの場所に応じて、以下を考慮してください。

- VDAでのプロキシ構成:

  VDAで明示的なプロキシサーバーを構成し、localhostへの接続をプロキシ経由でルーティングすると、リダイレクトは失敗します。プロキシを正しく構成するには、 **>>>** で 設定を選択し、`127.0.0.1:9002`をバイパスする必要があります。

  PACファイルを使用する場合、PACファイルからのVDAプロキシ構成スクリプトは、`wss://127.0.0.1:9002`に対して **DIRECT** を返す必要があります。そうでない場合、最適化は失敗します。スクリプトが **DIRECT** を返すことを確認するには、`shExpMatch(url, "wss://127.0.0.1:9002/*")`を使用します。

- Citrix Workspaceアプリでのプロキシ構成:

  支社がプロキシ経由でインターネットにアクセスするように構成されている場合、これらのバージョンはプロキシサーバーをサポートします。

  - Windows版Citrix Workspaceアプリバージョン2012 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac`ファイルもサポートされています)
  - Windows版Citrix Workspaceアプリバージョン1912 CU5 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac`ファイルもサポートされています)
  - Linux版Citrix Workspaceアプリバージョン2101 (匿名認証)
  - Citrix Workspace app for Mac バージョン 2104 (匿名認証)

以前のバージョンのCitrix Workspaceアプリを搭載したクライアントデバイスは、プロキシ構成を読み取ることができません。これらのデバイスは、トラフィックをMicrosoft 365 TURNサーバーに直接送信します。

重要:

- クライアントデバイスがDNS解決を行うためにDNSサーバーに接続できることを確認してください。クライアントデバイスは、以下のMicrosoft Teamsリレーサーバーの FQDN を解決できる必要があります。

- `worldaz.relay.teams.microsoft.com`
- `inaz.relay.teams.microsoft.com`
- `uaeaz.relay.teams.microsoft.com`
- `euaz.relay.teams.microsoft.com`
- `usaz.relay.teams.microsoft.com`
- `turn.dod.teams.microsoft.us`
- `turn.gov.teams.microsoft.us`

DNS要求が失敗した場合、外部ユーザーとのP2P通話およびメディア確立を伴う会議通話は失敗します。

- 会議サーバーの場所は、最初の参加者の仮想デスクトップの場所に基づいて選択されます（クライアントではありません）。

通話の確立とメディアフローパス

可能な場合、Citrix WorkspaceアプリのHDX WebRTCメディアエンジン (HdxRtcEngine.exe) は、ピアツーピア通話でUser Datagram Protocol (UDP) を介して直接ネットワークSecure Real-time Transport Protocol (SRTP) 接続を確立しようとします。UDPハイポートがブロックされている場合、メディアエンジンはTCP/TLS 443にフォールバックします。

HDXメディアエンジンは、候補の検出と接続の確立のために、ICE、NAT用セッショントラバーサルユーティリティ（STUN）、およびNAT周辺リレーを使用したトラバーサル（TURN）をサポートしています。このサポートは、エンドポイントがDNS解決を実行できる必要があることを意味します。

2つのピア間、またはピアと会議サーバー間に直接パスがなく、多人数通話または会議に参加しているシナリオを検討してください。HdxRtcEngine.exeは、Microsoft 365のMicrosoft Teamsトランスポートリレーサーバーを使用して、他のピアまたはメディアプロセッサ（会議がホストされている場所）に到達します。クライアントマシンは、3つのMicrosoft 365サブネットIPアドレス範囲と4つのUDPポート（UDPがブロックされている場合はフォールバックとしてTCP/TLS 443）にアクセスできる必要があります。詳細については、通話設定 および Office 365 URLとIPアドレス範囲 ID 11 のアーキテクチャ図を参照してください。

ID	カテゴリ	アドレス	宛先ポート
11	最適化が必要	13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (フォールバック)

これらの範囲には、トランスポートリレーとメディアプロセッサの両方が含まれており、Azure Load Balancerによってフロントエンド化されています。 Microsoft Teamsトランスポートリレーは STUNおよびTURN機能を提供しますが、ICEエンドポイントではありません。また、Microsoft Teamsトランスポートリレーは、メディア、TLSを終端したり、トランスコーディングを行ったりしません。HdxRtcEngine.exeがTCPを使用する場合、他のピアまたはメディアプロセッサにトラフィックを転送する際に、TCPをUDPにブリッジできます。

WorkspaceアプリのWebRTCメディアエンジンは、Microsoft 365クラウドで最も近いMicrosoft Teamsトランスポートリレーに接続します。メディアエンジンは、エニーキャストIPとポート3478～3481 UDP（ワークロードごとに異なるUDPポートですが、多重化が発生する可能性があります）、またはフォールバックとして443 TCP/TLSを使用します。通話品質は基盤となるネットワークプロトコルに依存します。UDPは常にTCPよりも推奨されるため、ブランチオフィスでUDPトラフィックに対応できるようにネットワークを設計することをお勧めします。

Microsoft Teamsが最適化モードでロードされ、HdxRtcEngine.exeがエンドポイントで実行されている場合、ICEの障害により、通話設定の失敗や片方向のみのオーディオ/ビデオが発生する可能性があります。通話が完了できない場合やメディアストリームが全二重でない場合は、まずエンドポイントで **Wiresharkトレース** を確認してください。ICE候補収集プロセスに関する詳細については、サポート セクションの「ログの収集」を参照してください。

> **注:**
>
> エンドポイントがインターネットにアクセスできない場合でも、両方のユーザーが同じLAN上にいる場合は、ピアツーピア通話を行うことができる可能性があります。会議は失敗します。この場合、通話設定が開始される前に30秒のタイムアウトが発生します。

通話設定

このアーキテクチャ図を、通話フローシーケンスの視覚的な参照として使用してください。対応する手順は図に示されています。

アーキテクチャ

Microsoft Teams の最適化の仕組み(/en-us/citrix-virtual-apps-desktops/2311/media/teams-description.png)

1. Microsoft Teams を起動します。
2. Microsoft Teams は O365 に対して認証を行います。テナントポリシーは Microsoft Teams クライアントにプッシュされ、関連する TURN およびシグナリングチャネル情報がアプリに中継されます。
3. Microsoft Teams は VDA で実行されていることを検出し、Citrix JavaScript API に対して API 呼び出しを行います。
4. Microsoft Teams 内の Citrix JavaScript は、VDA で実行されている WebSocketService.exe へのセキュアな WebSocket 接続を開き、これによりユーザーセッション内で WebSocketAgent.exe が起動されます。
5. WebSocketAgent.exe は、Citrix HDX Microsoft Teams Redirection Service (CtxSvcHost.exe) を呼び出すことにより、汎用仮想チャネルをインスタンス化します。
6. Citrix Workspace アプリの wfica32.exe (HDX エンジン) は、HdxRtcEngine.exe と呼ばれる新しいプロセスを起動します。これは、Microsoft Teams の最適化に使用される新しい WebRTC エンジンです。
7. Citrix メディアエンジンと Teams.exe は双方向の仮想チャネルパスを持ち、マルチメディア要求の処理を開始できます。

   -----ユーザー通話------

8. **ピア A** が **通話** ボタンをクリックします。Teams.exe は Microsoft 365 の Microsoft Teams サービスと通信し、**ピア B** とのエンドツーエンドのシグナリングパスを確立します。Microsoft Teams は HdxRtcEngine に、サポートされている一連の通話パラメーター（コーデック、解像度など。これらはセッション記述プロトコル (SDP) オファーとして知られています）を要求します。これらの通話パラメーターは、シグナリングパスを使用して Microsoft 365 の Microsoft Teams サービスに中継され、そこからもう一方のピアに中継されます。
9. SDP オファー/アンサー（シングルパスネゴシエーション）はシグナリングチャネルを介して行われ、ICE 接続チェック（STUN バインド要求を使用した NAT およびファイアウォールトラバーサル）が完了します。その後、Secure Real-time Transport Protocol (SRTP) メディアは HdxRtcEngine.exe ともう一方のピア（会議の場合は Microsoft 365 会議サーバー）との間で直接流れます。

マイクロソフト フォンシステム

Phone Systemは、Microsoft Teamsを使用してMicrosoft 365クラウドで通話制御とPBXを可能にするMicrosoftのテクノロジーです。Microsoft Teamsの最適化は、Microsoft 365 Calling PlansまたはDirect Routingを使用してPhone Systemをサポートします。Direct Routingを使用すると、追加のオンプレミスソフトウェアなしで、サポートされている独自のセッションボーダーコントローラーをMicrosoft Phone Systemに直接接続できます。 通話キュー、転送、フォワード、保留、ミュート、通話再開がサポートされています。

DTMF

デュアルトーン多周波（DTMF）機能は、以下のバージョンのCitrix Workspaceアプリ（およびそれ以降）でサポートされています。

- Citrix Workspace アプリ for Windows バージョン 2102
- Citrix Workspaceアプリ Windows版 LTSR 1912 CU5 (Windows 10 OSのみ)
- Citrix Workspaceアプリ for Linux バージョン 2101
- Citrix Workspaceアプリ for Mac バージョン 2101
- ChromeOS向けCitrix Workspaceアプリ バージョン2111.1

動的e911のサポート

バージョン 2112 以降、Citrix Workspace アプリは動的緊急通話をサポートしています。Microsoft Calling Plans、Operator Connect、および Direct Routing で使用する場合、次のことが可能になります。

- 緊急通報の設定とルーティング。
- セキュリティ担当者への通知。

通知は、VDAで実行されているMicrosoft Teamsクライアントではなく、エンドポイントで実行されているCitrix Workspaceアプリの現在の場所に基づいて提供されます。

Ray Baum法では、911通報者の派遣可能な位置情報を適切な公共安全応答拠点（PSAP）に送信することが義務付けられています。HDXによるMicrosoft Teamsの最適化は、以下のバージョンのCitrix Workspaceアプリで使用する場合、Ray Baum法に準拠しています。

- Windows 版 Citrix Workspace アプリ バージョン 2112.1 以降
- Citrix Workspaceアプリ for Linux バージョン2112以降
- Citrix Workspaceアプリ for Mac バージョン2112以降
- Citrix Workspaceアプリ for ChromeOS バージョン2112以降

動的な緊急通報を有効にするには、管理者はMicrosoft Teams管理センターを使用して、ネットワークまたは緊急ロケーションマップを作成するために以下を構成する必要があります。

- ネットワーク設定
- ロケーション情報サービス (LIS)

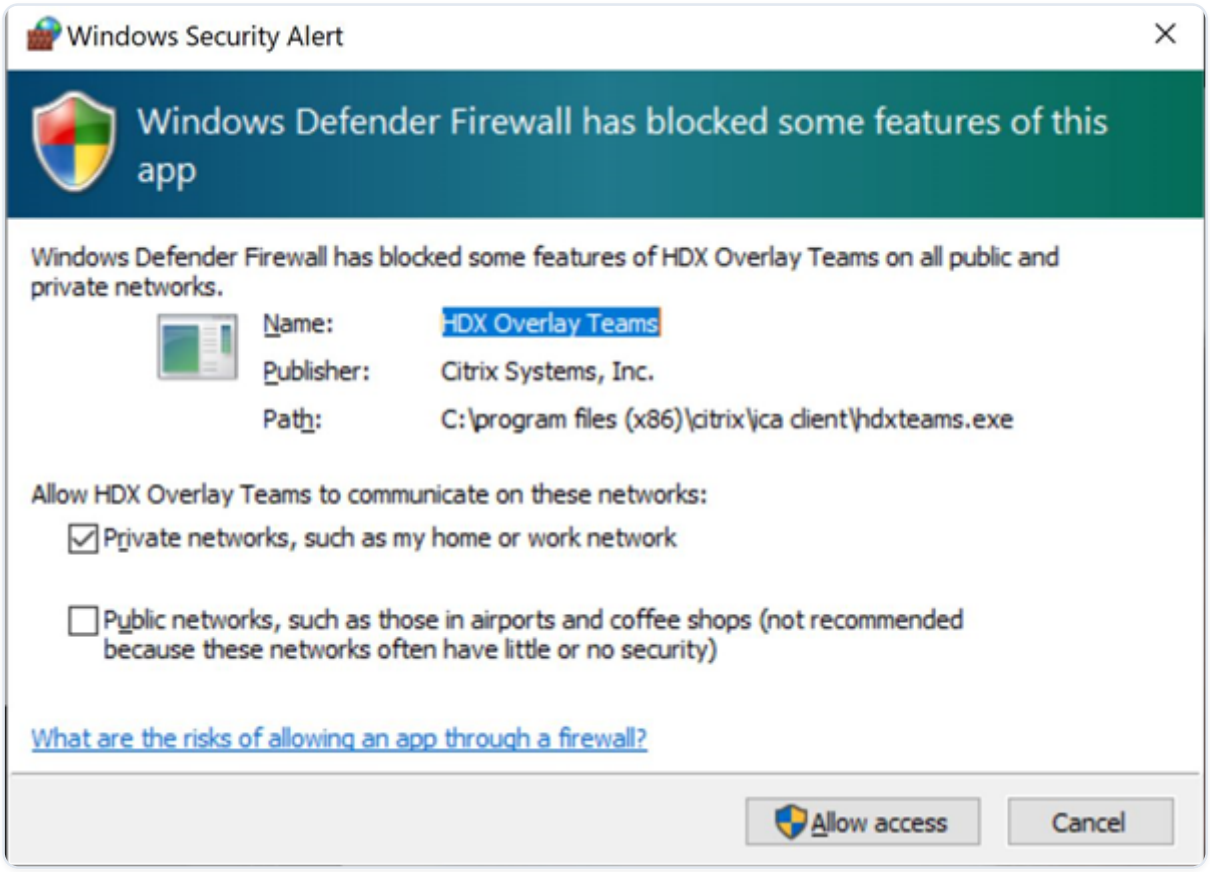
動的緊急通報の詳細については、Microsoft のドキュメントを参照してください。

Citrix Workspaceアプリ がMicrosoft Teamsに中継するディスパッチ可能な位置情報は次のとおりです。

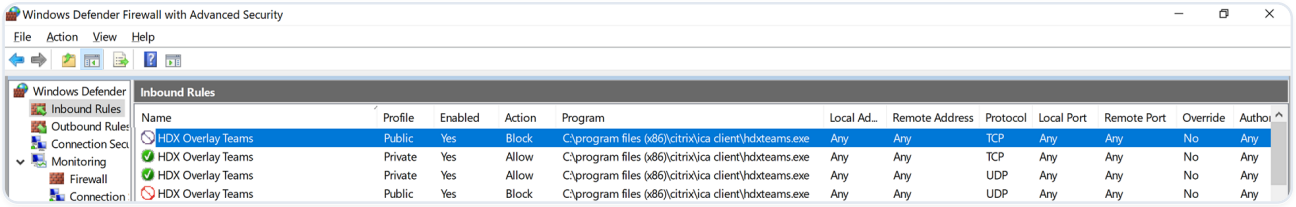
- イーサネット/スイッチ接続用のリンク層検出プロトコル (LLDP) を使用したシャーシ ID / ポート ID。イーサネット/スイッチ (LLDP) は以下でサポートされています。
  - Windowsバージョン8.1および10
  - LLDP有効化ソフトウェアを必要とするmacOS。LLDP有効化ソフトウェアをダウンロードするには、`www.microsoft.com`にアクセスして「LLDP enablement software」を検索してください。
  - LLDPライブラリがシンクライアントのオペレーティングシステム (OS) ディストリビューションに含まれている必要があるLinux。
- Citrix Workspaceアプリがインストールされているエンドポイントの WLAN BBSIDおよび {IPv4-IPv6; サブネット; MACアドレス}。
  - サブネットおよびWiFiベースのロケーションは、Windows、Linux、Mac版のWorkspaceアプリでサポートされています。
- Citrix Workspaceアプリがインストールされている OSレベルでユーザー権限が付与されている場合 (権限はHDX RTC Engineに設定されています) の緯度と経度
  - すべてのWorkspaceアプリプラットフォームでサポートされています。ただし、Citrix Workspace for Linuxの場合、シンクライアントのOSディストリビューションに`libgps`ライブラリを含める必要があります(>sudo apt-get install libgps23 gpsd lldpd)。

ファイアウォールの考慮事項

ユーザーがMicrosoft Teamsクライアントを使用して最適化された通話を初めて開始すると、**Windowsファイアウォール**の設定に関する警告が表示されることがあります。この警告は、HdxTeams.exeまたはHdxRtcEngine.exe（HDX Overlay Microsoft Teams）の通信を許可するようにユーザーに求めます。



Windows Defender Firewall > Advanced Securityコンソールで、**受信の規則**の下に次の4つのエントリが追加されます。必要に応じて、より制限の厳しい規則を適用できます。

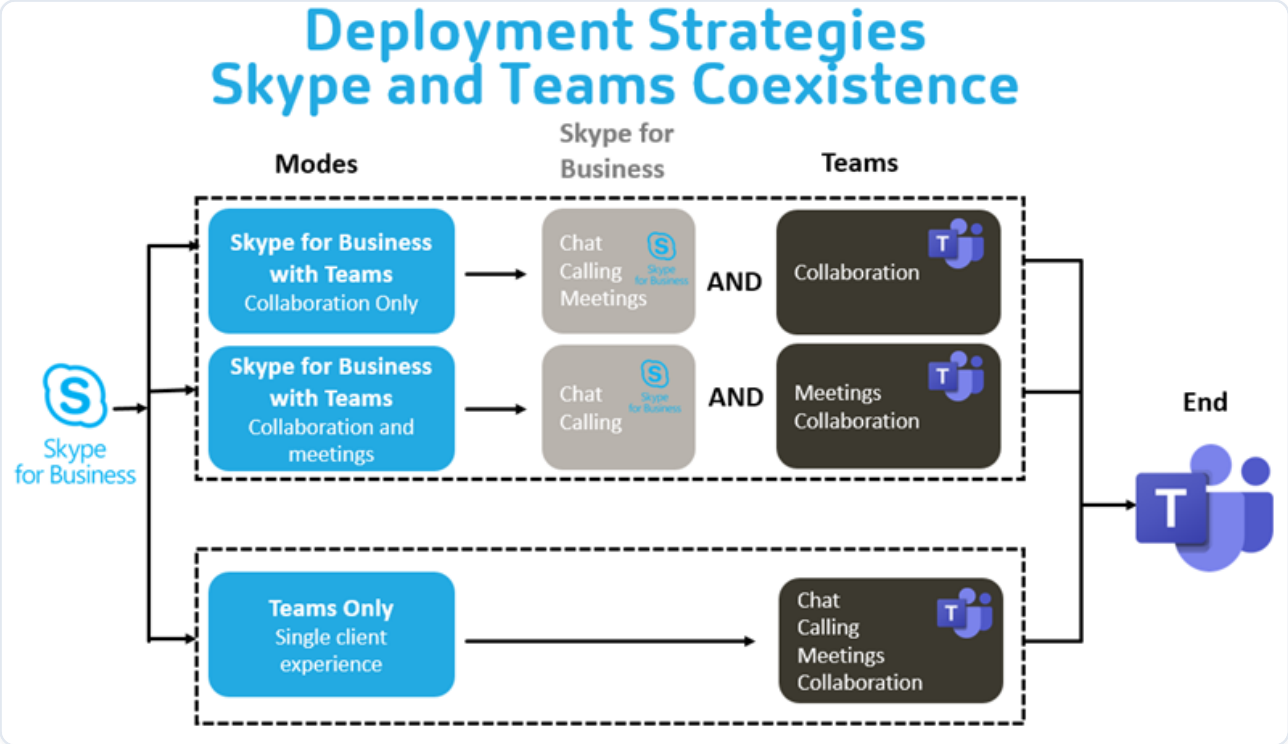


マイクロソフト チームズ と スカイプ フォー ビジネス の共存

Microsoft TeamsとSkype for Businessは、重複する機能を備えた2つの個別のソリューションとして並行して展開できます。 詳細については、Understand Microsoft Teams and Skype for Business coexistence and interoperabilityを参照してください。

Citrix RealTime Optimization PackとMicrosoft Teamsマルチメディアエンジン用のHDX最適化は、環境で設定された構成を尊重します。例としては、アイランドモードや、Microsoft TeamsとのSkype for Businessコラボレーションなどがあります。また、Microsoft TeamsとのSkype for Businessコラボレーションと会議も含まれます。

周辺機器へのアクセスは、一度に1つのアプリケーションにのみ許可されます。たとえば、通話中にRealTime Media EngineによるWebカメラアクセスは、通話中にイメージングデバイスをロックします。デバイスが解放されると、Microsoft Teamsで利用可能になります。



Citrix SD-WAN™: Microsoft Teams向けに最適化されたネットワーク接続

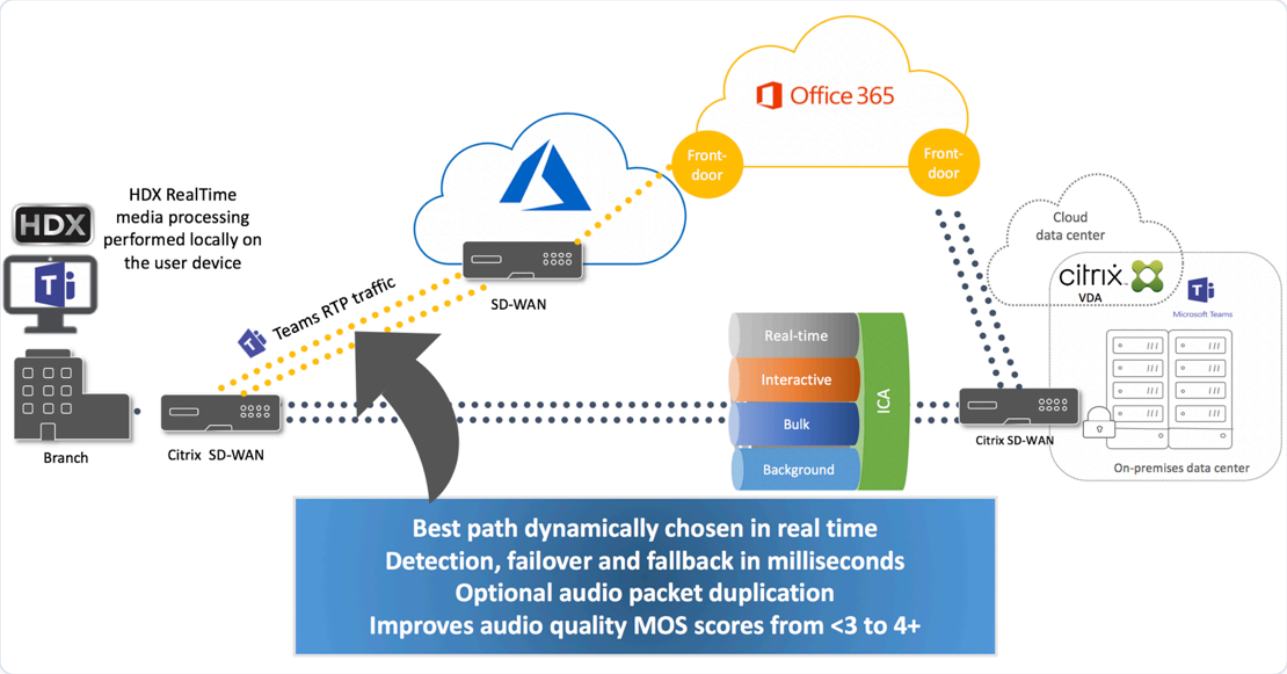
最適なオーディオおよびビデオ品質には、低遅延、低ジッター、低パケット損失のMicrosoft 365クラウドへのネットワーク接続が必要です。支店拠点のCitrix Workspaceアプリユーザーからの Microsoft Teamsオーディオビデオ RTPトラフィックを、インターネットに接続する前にデータセンターにバックホールすると、過剰な遅延が発生する可能性があります。また、WANリンクの輻輳を引き起こす可能性もあります。Citrix SD-WANは、Microsoft 365ネットワーク接続の原則に従ってMicrosoft Teamsの接続を最適化します。Citrix SD-WANは、Microsoft RESTベースの Microsoft 365 IPアドレスとWebサービス、および近接DNSを使用して、Microsoft Teamsトラフィックを識別、分類、および誘導します。

多くの地域で、ビジネスブロードバンドインターネット接続は、断続的なパケット損失、過剰なジッター期間、および停止に悩まされています。

Citrix SD-WANは、ネットワークの状態が不安定または劣化している場合に、Microsoft Teamsのオーディオ/ビデオ品質を維持するための2つのソリューションを提供します。

- Microsoft Azureを使用している場合、Azure VNETに展開されたCitrix SD-WAN仮想アプライアンス（VPX）は、高度な接続最適化を提供します。これらの最適化には、シームレスなリンクフェイルオーバーとオーディオパケットレーシングが含まれます。
- Citrix SD-WANのお客様は、Citrix Cloud™ Directサービスを介してMicrosoft 365に接続できます。このサービスは、すべてのインターネット向けトラフィックに対して信頼性と安全性の高い配信を提供します。

支社のインターネット接続の品質が問題にならない場合、遅延を最小限に抑えるだけで十分な場合があります。遅延を最小限に抑えるには、Microsoft TeamsのトラフィックをCitrix SD-WANブランチアプライアンスから最寄りのMicrosoft 365フロントドアに直接誘導します。詳細については、「Citrix SD-WAN Office 365の最適化」を参照してください。



マルチウィンドウ会議とチャット

Windows版Microsoft Teamsでは、複数の会議またはチャットウィンドウを使用できます。ポップアウト機能の詳細については、Microsoft 365サイトの「Microsoft Teamsのチャットと会議のポップアウトウィンドウ」を参照してください。

注:

この機能は、Citrix Workspaceアプリ for Windows 2112.1、Mac 2203、Linux 2203、ChromeOS 2303でサポートされています。VDA 2112以降が必要で、1912 CU6+ LTSRにバックポートされました。

背景のぼかしと背景効果

Citrix Workspaceアプリ for Windows、Mac、Linux、ChromeOS/HTML5は、HDXによるMicrosoft Teamsの最適化で背景のぼかしと背景効果をサポートしています。

背景をぼかすか、デフォルトの画像に置き換えることで、会話がシルエット（体と顔）に集中し続けるようにし、予期せぬ邪魔を避けることができます。この機能は、P2Pまたは電話会議で使用できます。

> **注:**
>
> この機能は、Microsoft Teams の UI/ボタンと統合されています。マルチウィンドウのサポートは、VDA を 2112 以降に更新する必要がある前提条件です。詳細については、「マルチウィンドウ会議とチャット」を参照してください。

> 背景のぼかしと効果に関する Microsoft Teams UI コントロールには、以下の最小バージョンが必要です。

- Citrix Workspace アプリ Windows 用 2207
- Mac 2301 用 Citrix Workspace アプリ
- Citrix Workspaceアプリ Linux向け 2307
- ChromeOS 2303 用 Citrix Workspace アプリ

制限事項:

- クライアントは、背景画像を Microsoft Teams のデフォルト画像に置き換える際に、インターネットに接続されている必要があります。
- 管理者およびユーザー定義の背景画像の置き換えは、Microsoft Teams UI ではサポートされていません。カスタム背景画像は、画像がクライアントにも保存されている場合、クライアントの構成設定を使用して構成できます。

カスタム背景画像の設定

以下のレジストリキーは、Microsoft Teams UIを使用してこの機能を制御する予定がない場合、または管理者がデフォルトの動作を上書きしたい場合にのみ必要です。たとえば、エンドポイントの性能が十分でないため、背景のぼかしを無効にする場合などです。

Windowsの場合

カスタム背景画像を設定するには、管理者またはエンドユーザーがクライアントまたはエンドポイントで以下のレジストリキーを構成する必要があります。

場所: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- 名前: VideoBackgroundEffect

- 種類: DWORD
- 値: 0 (無効), 1 (有効), 2 (背景画像の置き換え)

値を 1 に設定すると、背景がぼかされます。この値はエンドユーザーまたは管理者が設定できます。

値が2に設定されている場合、**VideoBackgroundImage**キーも存在する必要があります。この値は管理者のみが設定できます。背景画像を置き換える場合のみ、以下のキーが必要です（ぼかしには不要です）。

- 名前: VideoBackgroundImage
- 種類: REG_SZ
- 値: my_image_name.jpeg

ビデオの背景画像は`C:\Program Files (x86)\Citrix\ICA Client`ディレクトリに存在する必要があります。

このレジストリ設定は、Microsoft Teams UIセレクターなしでCitrix Workspaceアプリ2206での背景ぼかしまたは画像置換を有効にするためにも使用できます。言い換えれば、環境またはVDAがマルチウィンドウをサポートしていない場合でも、Citrix Workspaceアプリ2206以降でHKCUレジストリの回避策を適用して同様の結果を得ることができます。ただし、ユーザーはHDXセッション中またはMicrosoft Teams通話中に機能を制御することはできません。

レジストリキーの変更は、HDXセッションが接続したときにのみ有効になります。

Macの場合

ユーザーがダウンロードした画像の場所: */Users/username/Downloads/any_image.png*

カスタム画像をデフォルト画像として設定するには、次のコマンドを実行します。

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "/Users/username/Downloads/any_image.png"
```

Linuxの場合

ユーザーがダウンロードした画像の場所: */home/username/Downloads/any_image.jpg*

ファイル*/var/.config/citrix/hdx_rtc_engine/config.json*を作成し、以下の設定キーをJSON形式で追加します。例:

```
{


"VideoBackgroundEffect":2,


"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"


}
```

HTML5の場合

1. **HTML5Client**フォルダーにある**configuration.js**ファイルに移動します。
2. **backgroundEffects**属性を追加し、属性を**true**に設定します。例：

```
'features' : {

    'msTeamsOptimization' :

    {

        'backgroundEffects' : true

    }

}
```

3. 変更を保存します。

クライアントCPU消費に関する考慮事項

ぼかし機能はCPUへの負荷が低いですが、消費量の増加が予想されます。たとえば、4コア、1.5 GHz、TurboBoostで最大2.8 GHzのIntel® Pentium® Silverチップを搭載したシンクライアントでは、背景のぼかしによりCPU使用率が約2%増加します。平均CPU使用率は20%未満です。

Microsoft Teamsのギャラリービューとアクティブスピーカー

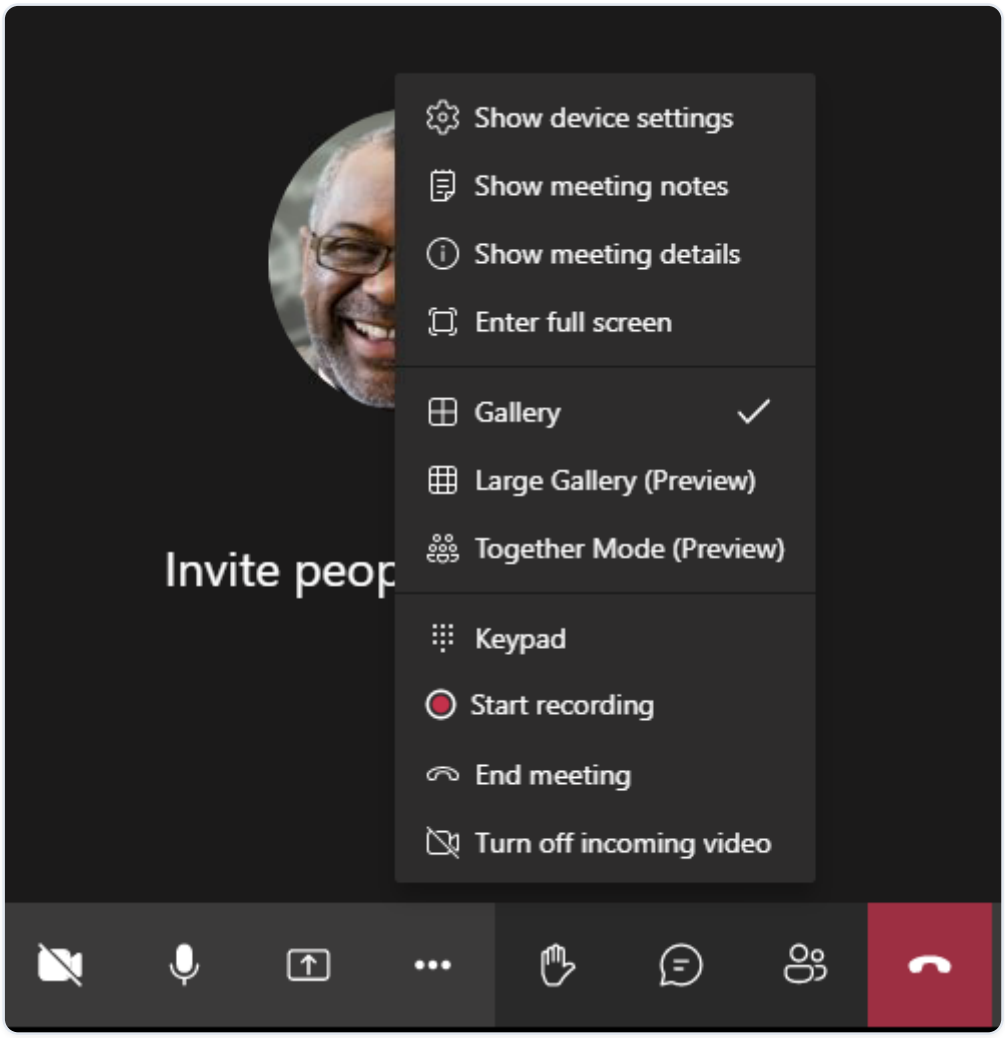
Microsoft Teamsは、**ギャラリー**、**大規模ギャラリー**、および**Togetherモード**のレイアウトをサポートしています。

Microsoft Teamsは、4人の参加者のビデオストリームを2x2のグリッドで表示します（**ギャラリー**として知られています）。この場合、Microsoft Teamsは4つのビデオストリームをクライアントデバイスに送信してデコードします。4人を超える参加者がビデオを共有している場合、画面には最後に最もアクティブだった4人の話者のみが表示されます。

Microsoft Teamsは、最大7x7のグリッドを持つ大規模ギャラリービューも提供します。その結果、Microsoft Teams会議サーバーは単一のビデオフィードを合成し、デコードのためにクライアントデバイスに送信するため、CPU消費量が低減されます。この単一のマトリックス形式のフィードには、ユーザー自身のプレビュービデオも含まれる場合があります。

最後に、Microsoft Teamsは新しい会議エクスペリエンスの一部である**Togetherモード**をサポートしています。AIセグメンテーション技術を使用して参加者を共有背景にデジタル配置することで、Microsoft Teamsはすべての参加者を同じ講堂に配置します。

ユーザーは、会議中に省略記号メニューで**ギャラリー**、**大規模ギャラリー**、または**Togetherモード**のレイアウトを選択することで、これらのモードを制御できます。



ビデオアスペクト比の制約のサポート（Citrix Workspaceアプリ for Windows 2102、Citrix Workspaceアプリ for Linux 2106、Citrix Workspaceアプリ for MAC 2106以降）：

- ギャラリー/大規模ギャラリービューで**フレームに合わせる**オプションが利用可能です。このオプションは、サブウィンドウに収まるようにビデオサイズをトリミングします。一方、**フレームにフィット**は、ビデオの側面に黒いバー（レターボックス）を表示するため、トリミングは行われません。

以下の表は、ギャラリーとラージギャラリーのレイアウトを比較したものです。

	ギャラリービュー 2X2 (デフォルト)	ラージギャラリービュー
レイアウト / グリッド	4人の参加者のビデオストリームを含む2x2グリッドを表示します。画面には直近で最もアクティブな4人の発言者のみが表示され、他の参加	49人の参加者のビデオストリームを含む7x7グリッドを表示します。

	ギャラリービュー 2X2 (デフォルト)	ラージギャラリービュー
	者はグリッドに表示されません。	
ミキシング技術	メディアルーターは、各参加者からの個々のストリームをすべてのユーザーに転送します。	中央の会議サーバーがすべてのオーディオまたはビデオをミキシングおよびトランスコードし、各参加者向けに調整された複合レイアウトを作成します。この処理により、追加の遅延が発生する場合があります。
アクティブスピーカー	新しいアクティブスピーカーが、グリッド内で最もアクティブでないスピーカーと入れ替わります。	アクティブか非アクティブかに関わらず、すべての参加者を表示します。
エンドポイントでのエンコード	Simulcastが有効になっている場合、1つ以上のビデオストリームがエンドポイントでエンコードされることがあります。Simulcastのサポートに関する詳細については、Simulcastを参照してください。	Simulcastが有効になっている場合、1つ以上のビデオストリームがエンドポイントでエンコードされることがあります。Simulcastのサポートに関する詳細については、Simulcastを参照してください。
エンドポイントでのデコード	各参加者は最大4つの個別のメディアストリームを受け取ります。これにより、HdxRtcEngine.exeによるエンドポイントでのCPU消費量が増加します（デコード/レンダリングのため）。	各参加者はオーディオとビデオに対して単一のストリームのみを受け取ります。この設定により、エンドポイントでのCPU消費量が削減されます。
最大解像度	720p。4人の参加者がビデオを共有している場合、ビデオフィードあたりの最大解像度は360pです。4人未満の参加者がビデオを共有している場合、ビデオフィードあたりの	複合レイアウトまたはミキシングの場合は720p。複合レイアウトでは、参加者ごとに高品質のビデオストリームは必要ありません。この条件により、各送信者は解像度または

	ギャラリービュー 2X2 (デフォルト)	ラージギャラリービュー
	解像度は高くなる可能性があります。	アップロードビットレートを削減します。
「低速ユーザー」の問題	送信者は、各モダリティ（オーディオ/ビデオ/画面共有）の品質を、参加者間の最低共通ネットワーク品質に合わせます。このマルチメディアストリームは、その後、他のすべての参加者に転送されます。結果として、ネットワーク状態の悪い参加者が、通話中の他の全員の品質に影響を与えます。	最低共通ネットワーク品質のシナリオの影響を受けにくい。会議サーバーは、個々の参加者のネットワーク状況に基づいて異なる品質を提供します。
セルフプレビュー	リアルタイムで自分自身を小さなサムネイルで表示します。	自分自身をサムネイルで表示し、他のビデオフィードと混合します。結果として、メインのビデオレイアウトに自分自身が追加の遅延を伴って含まれているのを目にするかもしれません。

Microsoft Teamsでの画面共有

Microsoft Teamsは、ビデオベースの画面共有（VBSS）に依存しており、H264などのビデオコーデックで共有されているデスクトップを効率的にエンコードし、高解像度ストリームを作成します。HDX最適化により、受信する画面共有はビデオストリームとして扱われます。

Windows、Linux、Mac向けのCitrix Workspaceアプリ2109以降、およびChromeOS向けのCitrix Workspaceアプリ2303以降では、ユーザーは画面とビデオカメラを同時に共有できます。

以前のバージョンでは、ビデオ通話中に相手がデスクトップの共有を開始すると、元のカメラビデオフィードは一時停止されます。代わりに、画面共有ビデオフィードが表示されます。その後、相手は手動でカメラ共有を再開する必要があります。

> **PowerPoint Liveに関する注意**

PowerPoint Liveからコンテンツを共有している場合、この制限はありません。その場合、他の参加者は引き続きあなたのウェブカメラとコンテンツを見ることができ、他のスライドを確認するために前後に移動できます。このシナリオでは、スライドはVDAでレンダリングされます。PowerPoint Liveのスライドデッキにアクセスするには、「共有トレイ」ボタンをクリックして提案されたPowerPointスライドのいずれかを選択するか、「参照」をクリックしてコンピューターまたはOneDriveでPowerPointファイルを見つけます。

送信画面共有も最適化され、Citrix Workspaceアプリにオフロードされます。この場合、メディアエンジンは、赤い枠線が描かれたCitrix Desktop Viewer (CDViewer.exe) ウィンドウのみをキャプチャして送信します。Desktop Viewerと重なるローカルアプリケーションはキャプチャされません。

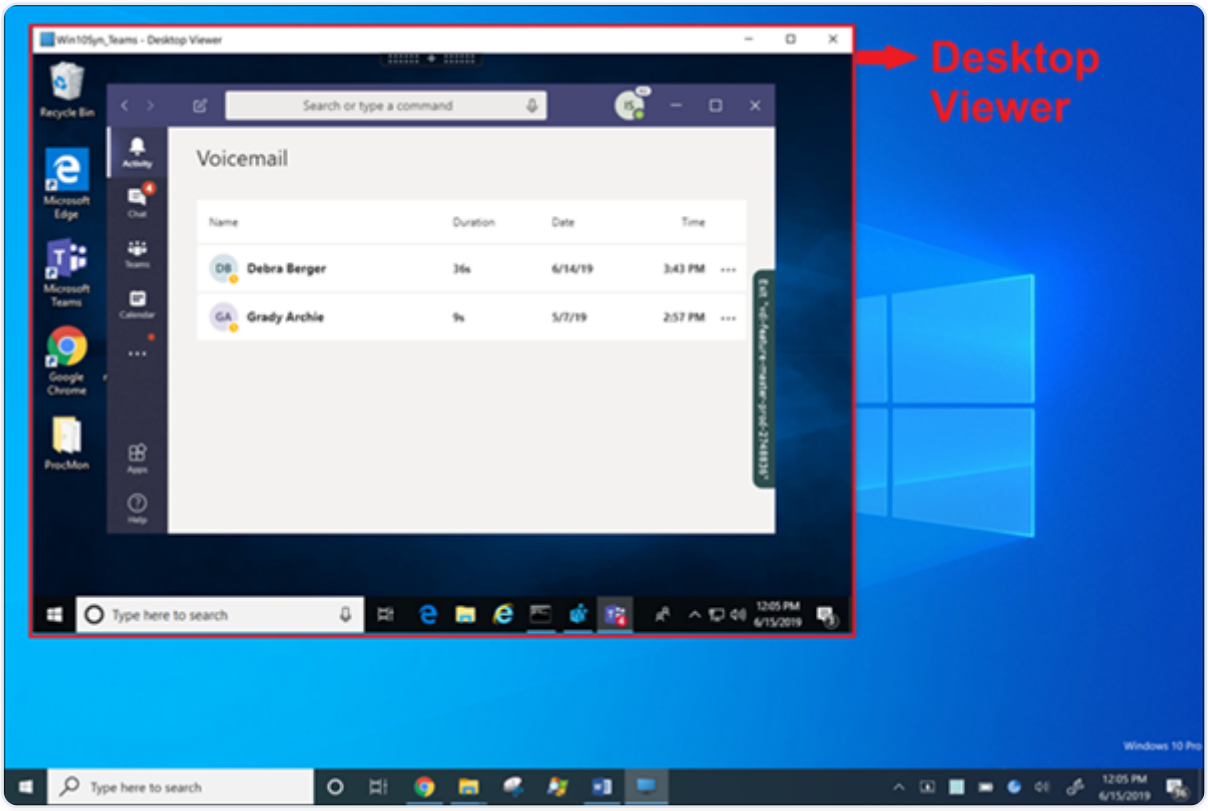
注

Mac版Citrix Workspaceアプリで画面共有を有効にするには、特定の権限を設定してください。詳細については、システム要件を参照してください。

既知の制限:

- Desktop Viewerが無効になっている場合、またはDesktop Lockが使用されている場合、Microsoft Teamsの画面ピッカーでマルチモニター選択は利用できません。Desktop Viewerは、`.ICA`ファイルテンプレートを編集するか、`StoreFront web.config`によって無効にすることができます。SHIFT+F2ホットキーはマルチモニター画面共有と互換性がありません。
- Workspaceアプリのバージョン2106より古い場合、プライマリモニターのみが共有されます。通話中の他の参加者に見せるには、仮想デスクトップ内のアプリケーションをプライマリモニターにドラッグしてください。
- 仮想モニターレイアウト機能（単一の物理モニターの論理パーティション）でCitrix Workspaceアプリを設定した場合、マルチモニター画面共有が機能しないことがあります。この場合、すべての仮想モニターは複合画像として共有されます。
- Windows版Citrix Workspaceアプリの古いバージョン（1907から2008まで）では、クライアントマシンで実行されているローカルアプリケーションも共有されます。この共有は、ローカルアプリがDesktop Viewerの上に重ねて表示されている場合にのみ可能です。この動作は、2009.6以降および1912 CU5以降で削除されました。
- 画面共有中に、ウィンドウモードから全画面表示に切り替えると、画面共有が停止します。画面共有を機能させるには、一度停止して再度共有する必要があります。

- Optimized Microsoft Teamsでは、共有コントロールを特定の場所にピン留めすることはできません。
- 最小化されたアプリを共有すると、そのアプリのタイトルバーも共有される場合があります。



シームレスアプリケーションからの画面共有:

Microsoft Teamsをスタンドアロンのシームレスアプリケーションとして公開している場合、画面共有は物理エンドポイントのローカルデスクトップをキャプチャします。Citrix Workspaceアプリの最小バージョン1909が必要です。

アプリ共有

Citrix Workspaceアプリ for Windows 2112.1およびVDA 2112以降、Microsoft Teamsはアプリ共有をサポートしています。

Citrix Workspace アプリ for Windows 2109、Mac 2203、Linux 2209 および VDA 2109 以降、Microsoft Teams は、仮想セッションで実行されている特定のアプリの画面共有をサポートしています。最適化された Microsoft Teams を使用して、Java などのカスタム社内アプリケーションを共有することもできます。特定のアプリを共有するには:

1. リモートセッション内でMicrosoft Teamsアプリに移動します。
2. Microsoft Teams UIで**コンテンツを共有**をクリックします。
3. 会議で共有するアプリを選択します。選択したアプリの周囲に赤い枠が表示され、通話中のピアは共有されたアプリを見ることができます。

別のアプリを共有するには、もう一度「**コンテンツを共有**」をクリックし、新しいアプリを選択します。

アプリ共有を無効にする場合は、VDA の `HKLM\SOFTWARE\Citrix\Graphics` に次のレジストリキーを作成します。 名前: `UseWsProvider` 種類: `DWORD` 値: 0

> **注:**

> - アプリを最小化すると、Microsoft Teams は共有アプリの最後の画像を表示します。画面共有を再開するには、ウィンドウを最大化します。
> - 画面共有は、VDA 側でのウィンドウのキャプチャに依存します。その後、コンテンツは最大速度で Citrix Workspace アプリに中継されます。最大速度は 1 秒あたり 30 フレームです。Citrix Workspace アプリは、コンテンツをピアまたは会議サーバーに転送します。

> Microsoft Teamsのアプリ共有](/en-us/citrix-virtual-apps-desktops/2311/media/ms-teams-app-sharing.png)

特定のアプリの画面共有に関する既知の制限事項:

- アプリを画面共有している間は、マウス ポインターは表示されません。
- アプリを共有中に最小化すると、スクリーン ピッカーにはアプリのアイコンのみが表示されます。アプリのサムネイルはスクリーン ピッカーにプレビューされません。アプリを最大化するまで、コンテンツを共有できず、赤い枠も表示されません。
- LAAアプリは、VDAの最適化されたMicrosoft Teamsでデスクトップアプリと共有できるアプリのリストを表示します。ただし、リストからアプリを選択しても、期待どおりの結果が得られない場合があります。

アプリ保護との互換性 特定のアプリの画面共有は、HDX最適化されたMicrosoft Teamsのアプリ保護機能と互換性があります。アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動した場合、特定のアプリを画面共有できます。

Microsoft Teams UIで**コンテンツを共有**をクリックすると、スクリーン ピッカーから**デスクトップ**オプションが削除されます。開いているアプリを共有するには、**ウィンドウ**オプションのみを選択できます。

> **注：**

> アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動した場合、Citrix Workspaceアプリ for Windows 2202以前を使用していると、受信ビデオまたは画面共有を表示できません。

Microsoft Teamsでの制御の付与と要求

この機能は、Citrix Workspaceアプリの以下のバージョンでサポートされています（VDAバージョンやオペレーティングシステム、シングルセッションまたはマルチセッションには依存しません）。

- Citrix Workspaceアプリ for Windows バージョン 2112.1以降
- Citrix Workspaceアプリ for Mac バージョン 2203.1以降
- Citrix Workspaceアプリ for Linux バージョン 2203以降
- Citrix Workspaceアプリ for ChromeOS バージョン 2303以降

Microsoft Teams通話中に参加者が画面を共有している場合、制御を要求できます。制御を取得すると、共有画面に対して選択、編集、その他のキーボードおよびマウス操作を行うことができます。

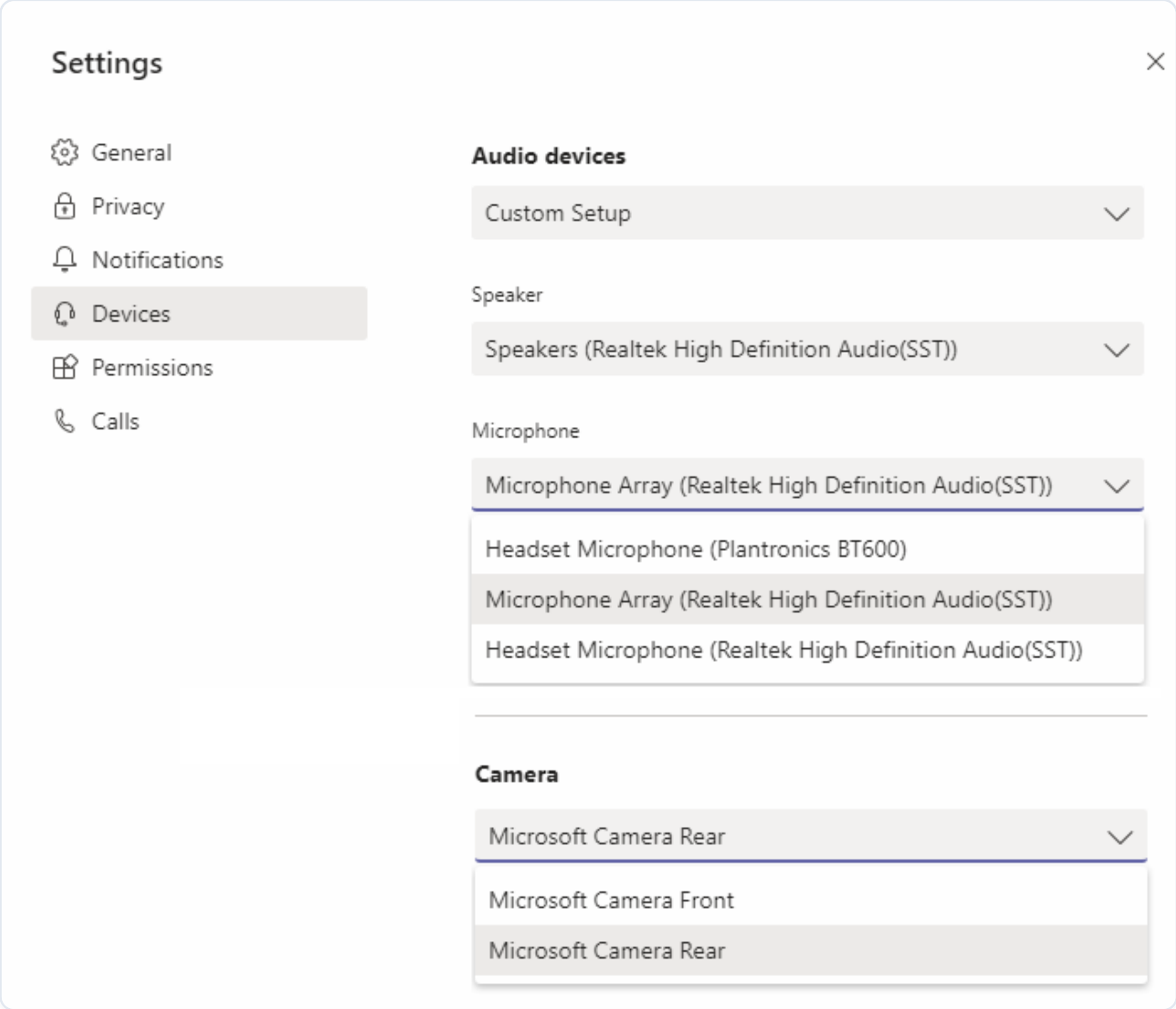
画面が共有されているときに制御を取得するには、Microsoft Teams UIの**制御を要求**ボタンをクリックします。画面を共有している会議参加者は、要求を許可または拒否できます。

制御権がある間は、共有画面の選択、編集、その他の変更を行うことができます。これらの操作には、キーボードとマウスの両方を使用できます。完了したら、 をクリックします。

> **制限事項:**
>
> - ユーザーが単一のアプリ（アプリ共有とも呼ばれる）を共有している場合、制御の付与と要求は利用できません。デスクトップ全体またはモニターを共有する必要があります。
> - コントロールバーを特定の場所に固定する機能は利用できません。

Microsoft Teamsでの周辺機器

Microsoft Teamsの最適化が有効な場合、Citrix Workspaceアプリは周辺機器（ヘッドセット、マイク、カメラ、スピーカーなど）にアクセスします。その後、周辺機器はMicrosoft Teams UI（**>**）に適切に表示されます。



Microsoft Teamsはデバイスに直接アクセスしません。代わりに、メディアの取得、キャプチャ、処理のためにWorkspaceアプリのWebRTCメディアエンジンに依存します。Microsoft Teamsは、ユーザーが選択できるようにデバイスを一覧表示します。

Microsoft Teamsがアクティブな間に挿入された周辺機器は、デフォルトでは選択されません。Microsoft Teams UIの**** > 画面から周辺機器を手動で選択する必要があります。周辺機器が選択されると、Microsoft Teamsは周辺機器の情報をキャッシュします。その結果、同じエンドポイントからセッションに再接続すると、周辺機器が自動的に選択されます。

推奨事項:

- エコーキャンセレーション内蔵のMicrosoft Teams認定ヘッドセット。マイクとスピーカーが別々のデバイスにある追加の周辺機器を使用するセットアップでは、エコーが発生する可能性があります。例としては、マイク内蔵のWebカメラとスピーカー付きモニターがあります。外部スピーカーを使用する場合は、マイクからできるだけ離して配置してください。また、音をマイクに屈折させる可能性のある表面からも離して配置してください。詳細については、`www.microsoft.com` にアクセスし、Microsoft Teams認定ヘッドセットを検索してください。
- Microsoft Teams認定カメラ。ただし、Skype for Business認定周辺機器はMicrosoft Teamsと互換性があります。詳細については、<www.microsoft.com> にアクセスし、Microsoft Teams認定カメラとSkype for Business認定周辺機器を検索してください。
- Citrix Workspaceアプリのメディアエンジンは、オンボードH.264エンコーディング（UVC 1.1および1.5）を実行するWebカメラでのCPUオフロードを利用できません。

注:

Windows用Workspaceアプリ2009.6は、24ビットまたは96 kHzを超える周波数のオーディオ形式を持つ周辺機器を取得できるようになりました。

HdxTeams.exe (Citrix Workspace app for Windows 2009以前のバージョン) は、以下の特定のオーディオデバイス形式 (チャンネル、ビット深度、サンプルレート) のみをサポートしています。

- 再生デバイス: 最大2チャンネル、16ビット、最大96,000 Hzの周波数
- 録音デバイス: 最大4チャンネル、16ビット、最大96,000 Hzの周波数

スピーカーまたはマイクのいずれかが予期される設定と一致しない場合でも、Microsoft Teamsでのデバイス列挙は失敗し、**設定 > デバイス**の下に**なし**と表示されます。

HdxTeams.exeの**Webrpc**ログには、この種類の情報が表示されます。

`Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...`.

> `Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!`!

> 回避策として、特定のデバイスを無効にするか、次のいずれかを実行します。

> 1. **サウンドコントロールパネル** (mmsys.cpl) を開きます。
> 2. 再生デバイスまたは録音デバイスを選択します。
> 3. **プロパティ > 詳細設定**に移動し、設定をサポートされているモードに変更します。

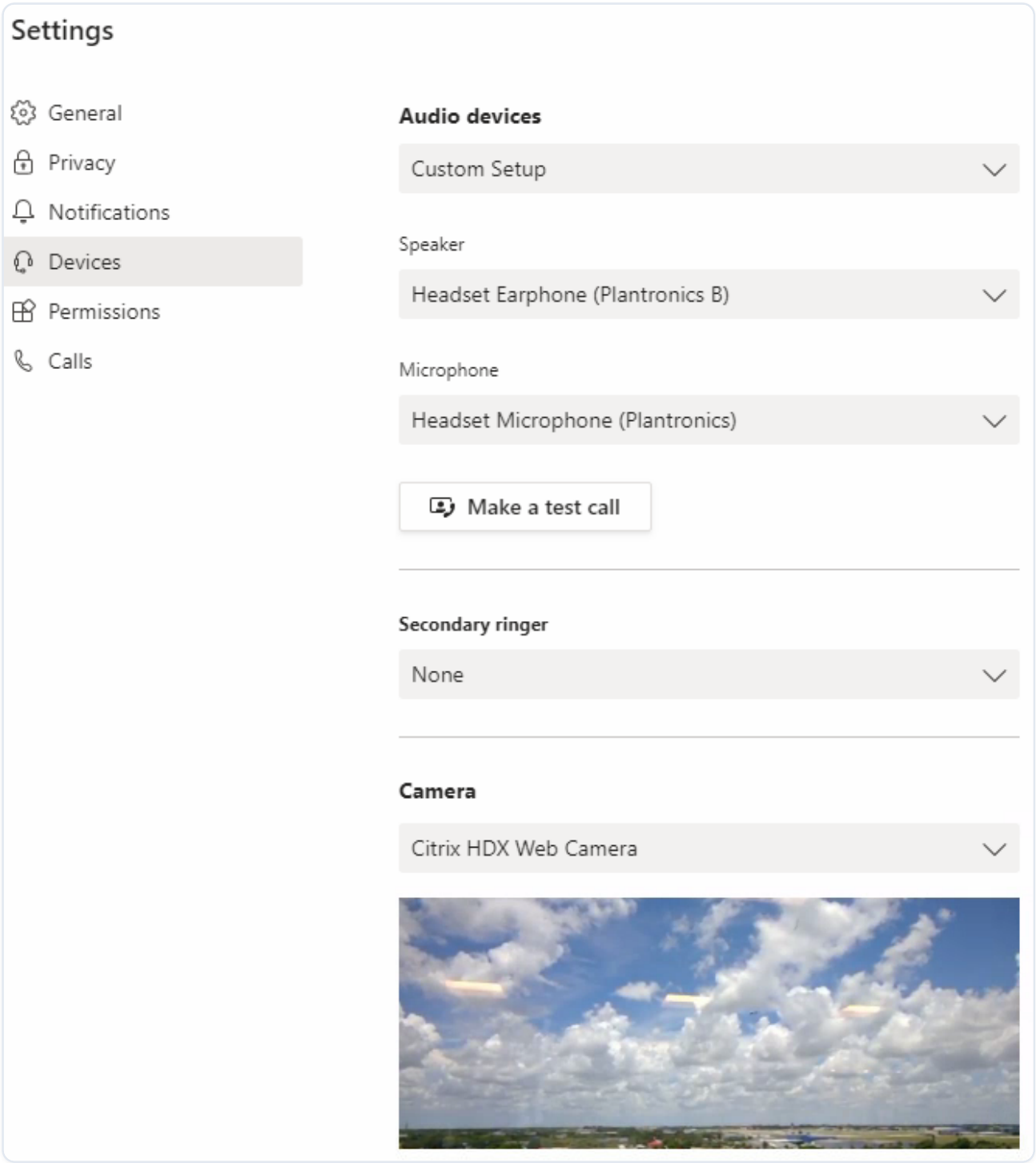
フォールバックモード

Microsoft Teamsが最適化されたVDIモードでロードに失敗した場合 (Microsoft Teams/バージョン情報/バージョンで「Citrix HDX Not Connected」と表示される場合)、VDAはレガシーHDXテクノロジーにフォールバックします。レガシーHDXテクノロジーには、Webカメラリダイレクト、クライアントオーディオ、マイクのリダイレクトが含まれる場合があります。Microsoft Teamsの最適化をサポートしていないWorkspaceアプリのバージョン/プラットフォームOSを使用している場合、フォールバックレジストリキーは適用されません。 フォールバックモードでは、周辺機器はVDAにマッピングされます。周辺機器は、仮想デスクトップにローカルで接続されているかのようにMicrosoft Teamsアプリに表示されます。

VDA でレジストリキーを設定することで、フォールバックメカニズムをきめ細かく制御できるようになりました。詳細については、レジストリで管理される機能のリストにある Microsoft Teams フォールバックモード を参照してください。

この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。

Microsoft Teamsアプリの**設定 > デバイス**タブで、最適化モードか非最適化モードかを確認するには、カメラ名が主な違いです。Microsoft Teamsが非最適化モードでロードされている場合、レガシーHDXテクノロジーが起動します。ウェブカメラ名には、次の図に示すように**Citrix HDX**のサフィックスが付いています。スピーカーとマイクのデバイス名は、最適化モードと比較してわずかに異なる（または切り詰められている）場合があります。



レガシー HDX テクノロジーが使用されている場合、Microsoft Teams はオーディオ、ビデオ、画面共有の処理をエンドポイントの Citrix Workspace アプリ WebRTC メディアエンジンにオフロードしません。代わりに、HDX テクノロジーはサーバー側レンダリングを使用します。ビデオをオンにすると、VDA で高い CPU 消費が予想されます。リアルタイムオーディオのパフォーマンスは最適ではない可能性があります。

既知の制限事項

Citrixの制限事項

Citrix Workspaceアプリの制限事項：

- HIDボタン - 通話の応答と終了はサポートされていません。音量の上げ下げはサポートされています。
- Microsoft Teamsの管理センターのQoS設定は、VDIユーザーには適用されません。
- VDAでSnipping Toolを使用している間は、Microsoft Teamsのコンテンツのスクリーンショットを撮ることはできません。ただし、クライアント側でSnipping Toolを使用すると、コンテンツをキャプチャできます。

VDAの制限事項：

- **Citrix Workspace アプリの高 DPI** 設定を `Yes` に構成すると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターの DPI スケーリング係数が 100% を超える値に設定されている場合に発生します。

Citrix Workspace アプリと VDA の制限事項:

- 最適化された通話の音量は、VDAではなく、クライアントマシンの音量バーを使用してのみ制御できます。

サイマルキャスト

WindowsおよびMac上の最適化されたMicrosoft Teamsビデオ会議通話でサイマルキャストがサポートされています。Linuxについては、シンクライアントベンダーにお問い合わせください。 サイマルキャストを使用すると、すべての発信者にとって最適な通話エクスペリエンスのために適切な解像度に調整することで、さまざまなエンドポイントでのビデオ会議通話の品質とエクスペリエンスが向上します。

この改善されたエクスペリエンスにより、各ユーザーは、エンドポイントの機能、ネットワークの状態など、いくつかの要因に応じて、異なる解像度（たとえば、720p、360pなど）で複数のビデオストリームを配信できます。受信側のエンドポイントは、処理できる最大品質の解像度を要求し、それによってすべてのユーザーに最適なビデオエクスペリエンスを提供します。

> **注:**
>
> この機能は、Microsoft Teamsからの更新プログラムが展開された後にのみ利用可能になります。ETAについては、`<https://www.microsoft.com/>` にアクセスし、Microsoft 365ロー

> ドマップを検索してください。Microsoftによって更新プログラムが展開されたら、ドキュメントの更新と発表についてはCTX253754を確認してください。

Microsoftの制限事項

- 3x3ギャラリービューはサポートされていません。Microsoft Teamsの依存関係 – 3x3グリッドの提供時期についてはMicrosoftにお問い合わせください。
- Skype for Businessとの相互運用性は音声通話に限定されており、ビデオモダリティは利用できません。
- 送受信ビデオストリームの最大解像度は720pです。
- PSTN通話の呼び出し音はサポートされていません。
- ダイレクトルーティングのメディアバイパスはサポートされていません。
- ブロードキャストおよびライブイベントのプロデューサーとプレゼンターの役割はサポートされていません。参加者ロールはサポートされていますが、最適化されていません（代わりにVDAでレンダリングされます）。
- Microsoft Teamsのズームインおよびズームアウト機能はサポートされていません。
- ロケーションベースルーティングとメディアバイパスはサポートされていません。
- 通話のマージはサポートされていません（ユーザーインターフェイスにオプションが表示されません）。

CitrixとMicrosoftの制限事項

- 画面共有を行う際、**システムオーディオを含める**オプションは利用できません。
- サイマルキャストはChromeOSではサポートされていません。

今後のMicrosoft Teamsシングルウィンドウのサポート終了

On January 31, 2024, Microsoftは、VDI Microsoft Teams最適化を使用する際のシングルウィンドウUIに対するMicrosoft Teamsのサポートを終了し、マルチウィンドウエクスペリエンスのみをサポートします。Microsoftは、この非推奨化について、9/8/2023にM365管理者センター（投稿ID: MC674419）で通知しました。 マルチウィンドウ機能に関する公開されている詳細は、Tech Communityの記事「New Meeting and Calling Experience in Microsoft Teams」で確認できます。

> **注：**

Citrixは、ビデオおよび画面共有のために最適化モードでMicrosoft Teamsを引き続き使用するには、VDAおよびCitrix Workspaceアプリをサポートされているバージョンにアップグレードすることを推奨します。インフラストラクチャとエンドポイントをマルチウィンドウをサポートするようにアップグレードしない場合、通話、ビデオ通話、および画面共有は最適化されなくなります。これにより、通話品質の問題、遅延の増加、およびサーバーへの負荷の増加が発生する可能性があります。

次の表は、Citrix VDIでMicrosoft Teamsの最適化された通話を継続して使用するために必要なVDAおよびCitrix Workspaceアプリの最小バージョン、LTSRバージョン、推奨バージョンを示しています。

コンポーネント	最小バージョン (1)	LTSRサポートバージョン (2)	推奨バージョン (3)
マイクロソフト チームズ	1.5.00.11865	該当なし	最新
VDA	1912 CU6 LTSR, 2109 CR, 2203 LTSR	1912 CU8+, 2203 LTSR CU2+ (4)	2308 CR+
Windows版 Citrix Workspaceアプリ	2112.1 CR	2203 CU2+ (4)	2309 CR以降
Mac向けCitrix Workspaceアプリ	2203 CR	該当なし	2308 CR+
Linux向けCitrix Workspaceアプリ	2202 CR	該当なし	2308 CR+
Citrix Workspaceアプリ for ChromeOS または HTML5	2303 CR	該当なし	2309 CR+

注:

1. 最小バージョン: これは、マルチウィンドウが初めて導入されたバージョンです。ここに記載されている最小バージョンの一部は、サポート終了となっている場合があります。

2. LTSRサポート対象バージョン: これは、Citrixがマルチウィンドウ向けにサポートしているLTSRバージョンです。これらのLTSRリリースの古いバージョンは動作する可能性がありますが、新しいLTSR CUバージョンがリリースされると、それらのバージョンに対するサポートは利用できなくなります。LTSRサポートポリシーの詳細については、`<https://support.citrix.com/article/CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr>`を参照してください。
3. 推奨バージョン: これは、ユーザー/顧客がソフトウェアのアップグレードを選択した場合にCitrixが推奨するソフトウェアのバージョンです。これらはすべてCRバージョンです。
4. VDAおよびCWAのベースバージョンであるバージョン2203 LTSRには、マルチウィンドウ機能が含まれています。これらのバージョンは、正式にサポートされている最新のCUに置き換えられています。お客様は、自己責任でこれらのサポートされていないバージョンを引き続き使用できます。Citrixは、LTSRリリースをご利用のお客様に最新のCUへのアップグレードを推奨します。

WebRTCからのSDP形式（プランB）の非推奨化のお知らせ

Citrixは、将来のリリースでWebRTCからの現在のSDP形式 (プランB) のサポートを廃止する予定です。最適化されたMicrosoft Teamsの機能に対応するには、WebRTCでUnified Planを使用する必要があります。

影響を受ける製品

Citrix Workspaceアプリケーションの今後のリリースでは、Citrix Workspaceアプリの今後のリリースを使用するエンドポイントと、Citrix Workspaceアプリ2108以前のバージョンを使用するエンドポイント間の通話はサポートされません。この通話の非互換性には、1912 LTSR Citrix Workspaceアプリクライアント（CWA）が含まれます。影響を受けるCWAクライアントは次のとおりです。

- Citrix Workspace アプリ Windows用
- Citrix Workspace アプリ Linux用
- Mac用Citrix Workspaceアプリ
- Chrome用Citrix Workspaceアプリ

Plan Bの代替

Citrix Workspaceアプリのバージョン2109より古いものを使用している場合は、サポートされているバージョン（できれば最新のCRリリース）にアップグレードする必要があります。そうしないと、将来のリリースまたは新しいエンドポイントとの通話は接続に失敗します。フェデレーションパートナーがCitrix Workspaceをアップグレードしていない場合、将来のリリースとフェデレーション通信パートナー間の通話も完了しない可能性があります。

Citrix Workspaceアプリバージョン2108は2023年3月にサポート期限が終了しており、新しいバージョンにアップグレードする必要があります。詳細については、Citrix Workspaceアプリのバージョンサポートに関するWorkspace Appを参照してください。

Plan Bの廃止に関する詳細については、WebRTCドキュメントを参照してください。

追加情報

- Microsoft Teams の監視、トラブルシューティング、サポート
- VM への Microsoft Teams デスクトップアプリの展開
- MSI を使用した Microsoft Teams のインストール (VDI インストールセクション)
- シンクライアント
- Skype for Business ネットワーク評価ツール
- Microsoft Teams と Skype for Business の共存と相互運用性を理解する

Microsoft Teamsの監視、トラブルシューティング、サポート

Teamsの監視

このセクションでは、HDX を使用した Microsoft Teams の最適化を監視するためのガイドラインを提供します。 最適化モードで実行しており、`HdxRtcEngine.exe` がクライアントマシンで実行されている場合、VDA 上の `WebSocketAgent.exe` というプロセスがセッションで実行されています。アプリケーションを表示するには、Director の **アクティビティマネージャー** を使用します。

](/en-us/citrix-virtual-apps-desktops/2311/media/teams-activity-manager.png)

Microsoft Teams の最適化ステータスは、Director の **ユーザー詳細** ページ > **セッション詳細** パネル > **MS Teams Optimization** フィールドで確認できます。Microsoft Teams が最適化されていることは、クリアなオーディオとビデオなど、より良いユーザーエクスペリエンスのために不可欠です。この機能は、VDA バージョン 2311 以降で利用可能です。サポートされている Citrix Workspace™ アプリのバージョンは、「Microsoft Teams の最適化」に記載されています。

Director は、Microsoft Teams が公開アプリケーションとして、または公開デスクトップ内で実行されている場合にのみ、Microsoft Teams の最適化ステータスを表示します。 詳細については、「Microsoft Teams の最適化ステータス」を参照してください。

VDA バージョン 1912 以降では、Citrix HDX Monitor (バージョン 3.11 以降) を使用してアクティブな Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品 ISO には、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。VDA バージョン 1912 以降では、Citrix HDX Monitor (バージョン 3.11 以降) を使用してアクティブな Microsoft Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品 ISO には、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。

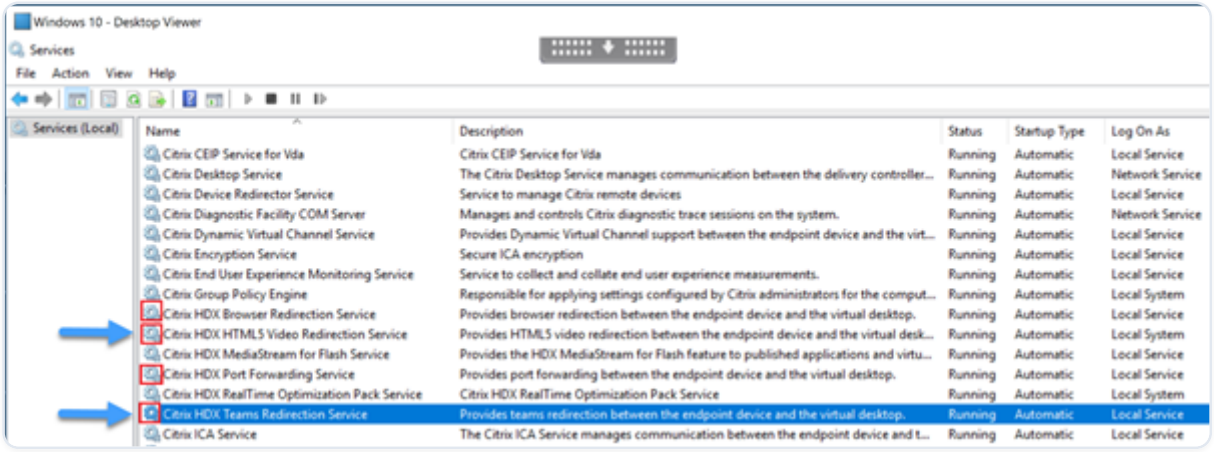
詳しくは、Knowledge Centerの記事「CTX253754」の「*監視*」を参照してください。

トラブルシューティング

このセクションでは、Microsoft Teamsの最適化を使用する際に発生する可能性のある問題のトラブルシューティングのヒントを提供します。詳しくは、「CTX253754」を参照してください。

バーチャル デリバリー エージェント上で

BCR_x64.msi によって4つのサービスがインストールされます。VDA での Microsoft Teams リダイレクトを担当するのはそのうちの2つだけです。



- **Citrix HDX Teams Redirection Service**は、Microsoft Teamsで使用される仮想チャネルを確立します。このサービスはCtxSvcHost.exeに依存しています。
- **Citrix HDX HTML5 Video Redirection Service** は、127.0.0.1:9002 TCP でリッスンする WebSocketService.exe として実行されます。WebSocketService.exe は、主に次の2つの機能を実行します。

i. **セキュアな WebSocket の TLS 終端** は、Microsoft Teams アプリ内のコンポーネントである vdiCitrixPeerConnection.js からセキュアな WebSocket 接続を受信します。Process Monitor で追跡できます。証明書の詳細については、「Controller と VDA 間の通信」の「TLS と HTML5 ビデオのリダイレクト、およびブラウザコンテンツのリダイレクト」セクションを参照してください。

一部のアンチウイルスソフトウェアおよびデスクトップセキュリティソフトウェアは、`WebSocketService.exe`とその証明書の正常な機能に干渉します。Citrix HDX HTML5 Video Redirectionサービスが`services.msc`コンソールで実行されている場合でも、netstatで確認すると、localhost `127.0.0.1:9002` TCPソケットがリスニングモードになっていません。サービスを再起動しようとすると、ハングアップします（「停止中...」）。`WebSocketService.exe`プロセスに適切な除外設定を適用してください。

「プロセスモニター」(/en-us/citrix-virtual-apps-desktops/2311/media/team-process-monitor.png)

ii. **ユーザーセッションマッピング。** Microsoft Teamsアプリケーションが起動すると、WebSocketService.exeはVDAのユーザーセッションでWebSocketAgent.exeプロセスを開始します。WebSocketService.exeはLocalSystemアカウントとしてセッション0で実行されます。

「WebSocketAgent.exeサービス」(/en-us/citrix-virtual-apps-desktops/2311/media/websocketservice-websocketagent.png)

VDAでWebSocketService.exeサービスがアクティブなリスニング状態にあるかどうかを確認するには、`netstat`を使用できます。

昇格されたコマンドプロンプトウィンドウから`netstat -anob -p tcp`を実行します。

「netstatの例を実行」(/en-us/citrix-virtual-apps-desktops/2311/media/teams-netstat.png)

接続が成功すると、状態はESTABLISHEDに変わります。

「netstatの成功例」(/en-us/citrix-virtual-apps-desktops/2311/media/teams-netstat-success.png)

> **重要:**
>
> WebSocketService.exeは、127.0.0.1:9001と127.0.0.1:9002の2つのTCPソケットでリッスンします。ポート9001はブラウザコンテンツリダイレクトとHTML5ビデオのリダイレクトに使用されます。ポート9002はMicrosoft Teamsのリダイレクトに使用されます。Teams.exeとWebSocketService.exe間の直接通信を妨げる可能性のあるプロキシ設定がVDAのWindows

OSにないことを確認してください。Internet Explorer 11で明示的なプロキシ（**インターネットオプション > 接続 > LANの設定 > プロキシサーバー**）を設定すると、接続が割り当てられたプロキシサーバーを経由する場合があります。手動および明示的なプロキシ設定を使用する場合は、**ローカルアドレスにはプロキシサーバーを使用しない**がチェックされていることを確認してください。

サービスの位置と説明

サービス	WINDOWS SERVER OSでの実行可能ファイルへのパス	ログオンアカウント	説明
Citrix HTML5ビデオリダイレクトサービス	実行ファイルパス: "C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service	ローカルシステムアカウント	仮想デスクトップとエンドポイントデバイス間でメディアリダイレクトを実行するために必要な初期フレームワークを、複数のHDXマルチメディアサービスに提供します。
Citrix HDXブラウザリダイレクトサービス	実行ファイルパス: "C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	このアカウント（ローカルサービス）	エンドポイントデバイスと仮想デスクトップ間でブラウザコンテンツリダイレクトを提供します。
Citrixポートフォワーディングサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs	このアカウント（ローカルサービス）	ブラウザコンテンツリダイレクトのために、エンドポイントデバイスと仮想デスクトップ間でポートフォワーディングを提供します。
Citrix HDX Teamsリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs	ローカルシステムアカウント	エンドポイントデバイスと仮想デスクトップ間のMicrosoft Teamsリダイレクトを提供します。

シトリックス ワークスペース アプリ

ユーザーのエンドポイントで、Windows用Citrix Workspaceアプリは、HdxTeams.exeまたはHdxRtcEngine.exeという新しいサービスをインスタンス化します。これは、VDAでMicrosoft Teamsが起動し、ユーザーがセルフプレビューで周辺機器を呼び出したりアクセスしようとしたときに発生します。このサービスが表示されない場合は、以下を確認してください。

1. Windows用Workspaceアプリバージョン1905以降がインストールされていることを確認してください。WorkspaceアプリのインストールパスにHdxTeams.exeまたはHdxRtcEngine.exeとwebrpc.dllバイナリが表示されますか？
2. ステップ1を検証した場合は、HdxTeams.exeまたはHdxRtcEngine.exeが起動しているかどうかを確認するために、以下を実行してください。
    a. VDAでMicrosoft Teamsを終了します。
    b. VDAでservices.mscを開始します。
    c. Citrix HDX Teamsリダイレクトサービスを停止します。
    d. ICA®セッションを切断します。
    e. ICAセッションに接続します。
    f. Citrix HDX Teamsリダイレクトサービスを開始します。
    g. Citrix HDX HTML5ビデオリダイレクトサービスを再起動します。
    h. VDAでMicrosoft Teamsを起動します。
3. クライアントエンドポイントでHdxTeams.exeまたはHdxRtcEngine.exeがまだ起動していない場合は、以下を実行してください。
    a. VDAを再起動します。
    b. クライアントエンドポイントを再起動します。

サポート

CitrixとMicrosoftは、Microsoft Teamsの最適化を使用して、Citrix Virtual Apps and Desktops™からMicrosoft Teamsの提供を共同でサポートしています。この共同サポートは、両社の緊密な連携の結果です。有効なサポート契約があり、このソリューションで問題が発生した場合は、問題の原因となっていると思われるコードのベンダーにサポートチケットを提出してください。つまり、TeamsについてはMicrosoftに、最適化コンポーネントについてはCitrixに提出します。 CitrixまたはMicrosoftがチケットを受け取り、問題をトリアージし、必要に応じてエスカレートします。各社のサポートチームに連絡する必要はありません。

問題が発生した場合は、Teams UIで **>** をクリックすることをお勧めします。技術的な問題をより迅速に解決するために、VDA側のログはCitrixとMicrosoft間で自動的に共有されます。

ログの収集

HDXメディアエンジンログはユーザーのマシン上（VDA上ではない）にあります。問題が発生した場合は、サポートケースにログを添付してください。

Windowsログ：

Windowsログは、%TEMP%内の **HDXTeams** フォルダー（AppData/Local/Temp/HDXTeamsまたはAppData/Local/Temp/HdxRtcEngine）にあります。webrpc_Day_Month_timestamp_Year.txtという名前の.txtファイルを探してください。Citrix Workspaceアプリ2009.5以降などの新しいバージョンを使用している場合は、ログをAppData\Local\Temp\HdxRtcEngineに保存します。

各セッションはログ用に個別のフォルダーを作成します。

Macログ：

1. VDWEBRTCログ - 仮想チャネルの実行を記録します。

   場所：`/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`

2. HdxRtcEngineログ - HdxRtcEngine上のプロセスの実行を記録します。

   場所: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

   HdxRtcEngineログはデフォルトで有効になっています。

3. Webrpcログ - webrtcライブラリのラップアップの実行を記録する最も重要なログです。

   場所: `/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

Linuxログ：

Linuxログは`/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/`フォルダーにあります。 Webrtcログ：`/tmp/webrpc/<current date>/webrtc.log` カーネルログ：`/var/log/syslog`

ICE/STUN/TURN/ログ：

通話確立時には、次の4つのICEフェーズが必要です。

- 候補収集
- 候補交換

- 接続チェック (STUNバインド要求)
- 候補昇格

HdxRtcEngine.exe ログには、関連するInteractive Connectivity Establishment (ICE) エントリが含まれています。これらのエントリは、通話設定が成功するために必要です。収集段階のサンプルスニペットを以下に示します。

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =



webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering



[…]

>>> begin:sdp

candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
generation 0 ufrag oVk6 network-id 1

<<< end:sdp

[…]
```

```
>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

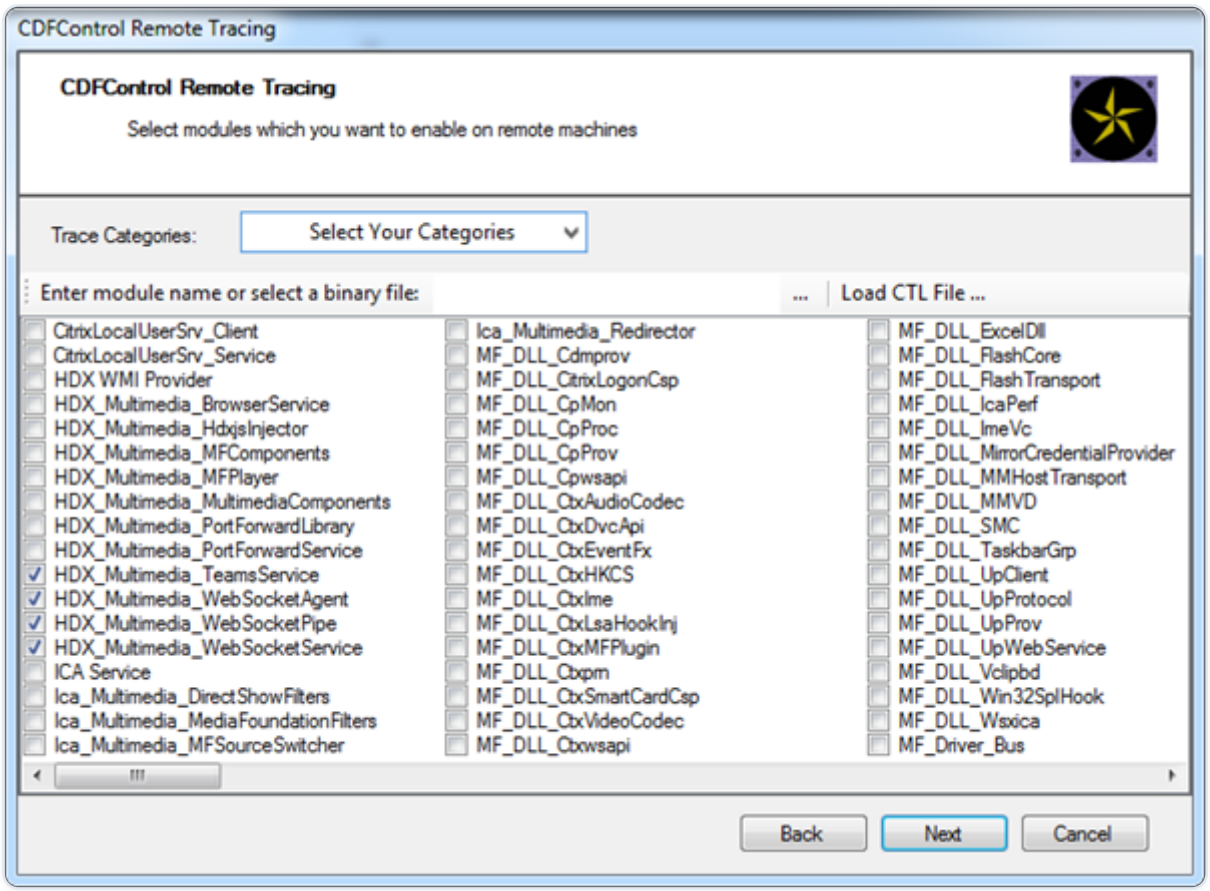
複数のICE候補がある場合、優先順位は次のとおりです。

1. ホスト
2. ピアリフレクシブ
3. サーバーリフレクシブ
4. トランスポートリレー

問題が発生し、それを一貫して再現できる場合は、Microsoft Teams で **ヘルプ > 問題の報告** をクリックすることをお勧めします。Microsoft にケースをオープンした場合、技術的な問題を解決するためにログは Citrix と Microsoft の間で共有されます。 Citrix サポートに問い合わせる前に CDF トレースをキャプチャすることも有益です。詳細については、Knowledge Center の記事 CDFcontrol を参照してください。

CDF トレース収集の推奨事項については、Knowledge Center の記事 Recommendations for Collecting the CDF Traces を参照してください。

VDA側CDFトレース - 次のCDFトレースプロバイダーを有効にします。



Workspaceアプリ側CDFトレース - 次のCDFトレースプロバイダーを有効にします。

Workspace App 側の CDF トレース(/en-us/citrix-virtual-apps-desktops/2311/media/team-cwa-cdf-traces.png)

- IcaClient_DriversVd_TeamsRedir (オプション)
- IcaClient_Multimedia_HdxTeams (Citrix Workspace app 2012 以降が必要)

Windows Media リダイレクト

Windows Media リダイレクトは、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御し、最適化します。メディアのランタイムファイルをサーバーではなくクライアントデバイスで再生することで、Windows Media リダイレクトは、マルチメディアファイルの再生に必要な帯域幅を削減します。Windows Media リダイレクトは、仮想Windowsデスクトップで実行されているWindows Media Playerおよび互換性のあるプレーヤーのパフォーマンスを向上させます。

Windows Media クライアント側コンテンツフェッチの要件が満たされない場合、メディア配信は自動的にサーバー側フェッチを使用します。この方法はユーザーには透過的です。Citrix Scoutを使用して、HostMMTransport.dllからCitrix Diagnosis Facility (CDF) トレースを実行し、使用されている方法を特定できます。詳しくは、Citrix Scoutを参照してください。

Windows Media リダイレクトは、ホストサーバーでメディアパイプラインをインターセプトし、メディアデータをネイティブの圧縮形式でキャプチャし、コンテンツをクライアントデバイスにリダイレクトします。その後、クライアントデバイスはメディアパイプラインを再構築して、ホストサーバーから受信したメディアデータを解凍およびレンダリングします。Windows Media リダイレクトは、Windowsオペレーティングシステムを実行しているクライアントデバイスでうまく機能します。これらのデバイスには、ホストサーバーに存在していたメディアパイプラインを再構築するために必要なマルチメディアフレームワークがあります。Linuxクライアントは、同様のオープンソースメディアフレームワークを使用してメディアパイプラインを再構築します。

ポリシー設定の**Windows Media Redirection**は、この機能を制御し、デフォルトで**Allowed**になっています。通常、この設定は、サーバーからレンダリングされるオーディオおよびビデオの品質を、クライアントデバイスでローカルに再生されるコンテンツに匹敵するレベルまで向上させます。まれに、Windows Media リダイレクトを使用して再生されるメディアが、基本的なICA®圧縮と通常のオーディオを使用してレンダリングされるメディアよりも品質が劣って見えることがあります。この機能を無効にするには、ポリシーに**Windows Media Redirection**設定を追加し、その値を**Prohibited**に設定します。

ポリシー設定の詳細については、マルチメディアポリシー設定を参照してください。

制限事項:

セッション内でWindows Media PlayerとRemote Audio & Video Extensions (RAVE) を有効にしている場合、黒い画面が表示されることがあります。この黒い画面は、ビデオコンテンツを右クリックして**再生中を常に手前に表示**を選択した場合に表示されることがあります。

一般的なコンテンツリダイレクト

コンテンツリダイレクトを使用すると、ユーザーがサーバーで公開されているアプリケーションを使用するか、ユーザーデバイスでローカルに実行されているアプリケーションを使用するかによって、情報にアクセスする方法を制御できます。

クライアントフォルダーリダイレクト(/ja-jp/citrix-virtual-apps-desktops/2311/general-content-redirection/client-folder-redirection.html)

クライアントフォルダーリダイレクトは、ホスト側のセッションでクライアント側のファイルにアクセスする方法を変更します。

- サーバーでクライアントドライブマッピングのみを有効にすると、クライアント側のフルボリュームは、Universal Naming Convention (UNC) リンクとしてセッションに自動的にマッピングされます。
- サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがWindowsデスクトップデバイスでそれを構成すると、ユーザーによって指定されたローカルボリュームの一部がリダイレクトされます。

ホストからクライアントへのリダイレクト(/ja-jp/citrix-virtual-apps-desktops/2311/general-content-redirection/host-to-client-redirection.html)

特定のまれなユースケースでは、ホストからクライアントへのリダイレクトの使用を検討してください。通常、他の形式のコンテンツリダイレクトの方が優れている場合があります。このタイプのリダイレクトは、マルチセッションOS VDAでのみサポートされており、シングルセッションOS VDAではサポートされていません。

ローカルアプリアクセスとURLリダイレクト(/ja-jp/citrix-virtual-apps-desktops/2311/general-content-redirection/laa-url-redirect.html)

ローカルアプリアクセスは、ローカルにインストールされたWindowsアプリケーションをホストされたデスクトップ環境にシームレスに統合します。これは、コンピューターを切り替えることなく行われます。

HDX™テクノロジーは、最適化されたサポートがない、または不適切な特殊デバイス向けに**汎用USBリダイレクト**を提供します。

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセス可能になる方法を変更します。サーバーでクライアントドライブマッピングのみを有効にすると、クライアント側の完全なボリュームは、ユニバーサルネーミング規則 (UNC) リンクとしてセッションに自動的にマップされます。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ユーザーが指定したフォルダーのみが、セッション内でUNCリンクとして表示されます。つまり、ユーザーデバイス上の完全なファイルシステムではなく、指定されたフォルダーのみが表示されます。レジストリを介してUNCリンクを無効にすると、クライアントフォルダーはセッション内でマップされたドライブとして表示されます。

クライアントフォルダーリダイレクトは、WindowsシングルセッションOSマシンでのみサポートされています。

外部USBドライブのクライアントフォルダーリダイレクトは、デバイスの取り外しと再接続時に保存されません。

サーバーでクライアントフォルダーリダイレクトを有効にします。次に、クライアントデバイスで、リダイレクトするフォルダーを指定します。クライアントフォルダーオプションを指定するために使用するアプリケーションは、このリリースに付属のCitrix Workspace™アプリに含まれています。

要件:

サーバーの場合:

- ウィンドウズ サーバー 2022
- Windows Server 2019 StandardおよびDatacenterエディション
- Windows Server 2016 StandardおよびDatacenterエディション
- Windows Server 2012 R2 StandardおよびDatacenterエディション

クライアントの場合:

- Windows 10、32ビットおよび64ビットエディション (最小バージョン1607)
- Windows 8.1、32ビットおよび64ビットエディション (Embeddedエディションを含む)
- Windows 7、32ビット版および64ビット版（Embedded版を含む）

サーバーでクライアントフォルダーリダイレクトを有効にするには、レジストリで管理される機能の一覧にある「クライアントフォルダーリダイレクト」(/ja-jp/citrix-virtual-apps-desktops/2311/policies/reference/hdx-registry-settings.html)を参照してください。

ユーザーデバイスで、リダイレクトするフォルダーを指定します:

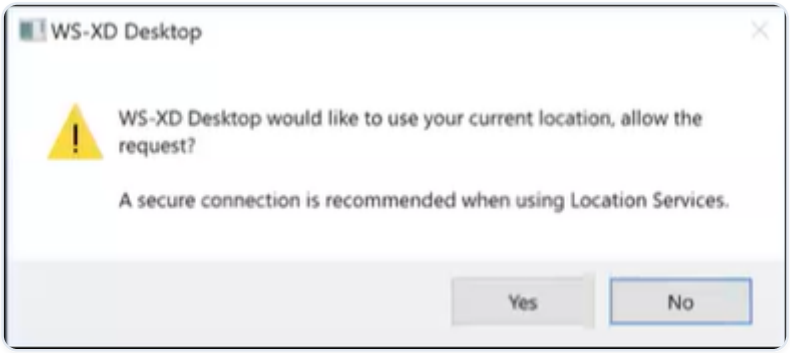
1. Citrix Workspaceアプリの最新バージョンがインストールされていることを確認してください。
2. Citrix Workspaceアプリのインストールディレクトリから、CtxCFRUI.exeを起動します。
3. **カスタム**ラジオボタンを選択し、フォルダーを追加、編集、または削除します。
4. 設定を有効にするには、セッションを切断して再接続します。

クライアント位置情報リダイレクト

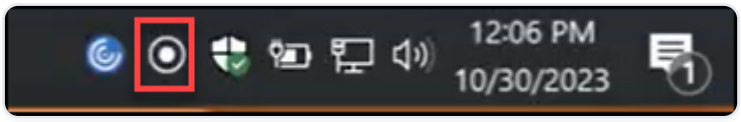
クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリとデスクトップセッションが、クライアントの現在の位置情報にシームレスにアクセスできるようになります。マルチセッションオペレーティングシステム（TS VDAまたはマルチセッションWS VDA）では、各セッションは、接続されているクライアントによって提供される独自の場所を持ちます。この機能を使用すると、位置情報に依存するVDA上のアプリケーションは、クライアントの正確な位置情報を取得できます。

詳細については、Microsoftドキュメントを参照してください。

クライアント位置情報リダイレクトが有効になり、サーバー側とクライアント側の両方で位置情報へのアクセスが許可されると、位置情報にアクセスするアプリケーションまたはデスクトップを起動したときに、クライアントは次のダイアログボックスで現在の位置情報を共有するように求めます。



クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリまたはデスクトップが現在の位置情報を照会した場合に、クライアントのタスクバーに次のアイコンが表示されます。



システム要件

サーバーの場合:

- シングルセッション（Win10/11）またはマルチセッション（Win 11 22H2およびServer 2022 23H2以降）OS VDA
- Citrix Workspace™ アプリ（Windows、iOS、またはAndroid用）

構成

この機能が動作するには、Citrix®ポリシーを使用してクライアント位置情報リダイレクトを有効にする必要があります。クライアント位置情報リダイレクトはデフォルトで無効になっています。

クライアント位置情報リダイレクトを有効にするには、次の手順を実行します。

Windows VDAおよびクライアント側で:

1. 「**設定 > プライバシー > 位置情報**」で、次のオプションを有効にします。
   - **このデバイスの位置情報へのアクセスを許可する**
   - **アプリが位置情報にアクセスすることを許可する**
   - **デスクトップアプリが位置情報にアクセスすることを許可する**
2. マルチセッションOSの場合、「**Location Override**」設定を有効にします。

Controller/DDC側で:

Studio > ポリシー > 位置情報 > 設定 > アプリケーションがクライアントデバイスの物理的な位置情報を使用することを許可するポリシーを有効にします。 詳細については、クライアントセンサーポリシー設定を参照してください。

ホストからクライアントへのリダイレクト

ホストからクライアントへのリダイレクトにより、Citrix®セッションで実行されているアプリケーションにハイパーリンクとして埋め込まれたURLを、ユーザーのエンドポイントデバイス上の対応するアプリケーションを使用して開くことができます。ホストからクライアントへのリダイレクトの一般的なユースケースには、次のようなものがあります。

- Citrixサーバーがソースへのインターネットまたはネットワークアクセスを持たない場合のWebサイトのリダイレクト。
- セキュリティ、パフォーマンス、互換性、またはスケーラビリティの理由から、Citrixセッション内でWebブラウザを実行することが望ましくない場合のWebサイトのリダイレクト。
- URLを開くために必要なアプリケーションがCitrixサーバーにインストールされていない場合の、特定のURLタイプのリダイレクト。

ホストからクライアントへのリダイレクトは、Citrixセッションで実行されているWebブラウザのWebページでアクセスしたり、アドレスバーに入力したりするURLを対象としていません。Webブラウザでのリダイレクトについては、双方向URLリダイレクトまたはブラウザコンテンツリダイレクトを参照してください。

システム要件

- マルチセッションOS VDA
- サポートされているクライアント:
  - Windows 用 Citrix Workspace™ アプリ
  - Mac 用 Citrix Workspace アプリ
  - Linux 用 Citrix Workspace アプリ
  - HTML5 用 Citrix Workspace アプリ
  - Chrome 用 Citrix Workspace アプリ

クライアントデバイスには、URLタイプのリダイレクトを処理するために、アプリケーションがインストールされ、構成されている必要があります。

構成

この機能を有効にするには、ホストからクライアントへのリダイレクト Citrixポリシーを使用します。**ホストからクライアントへのリダイレクト**はデフォルトで無効になっています。ホストからクライアントへのリダイレクトポリシーを有効にすると、Citrix Launcherアプリケーションが Windowsサーバーに登録され、URLをインターセプトしてクライアントデバイスに送信できるようになります。

次に、必要なURLタイプのデフォルトアプリケーションとしてCitrix Launcherを使用するように Windowsグループポリシーを構成する必要があります。CitrixサーバーVDAで、ServerFTAdefaultPolicy.xmlファイルを作成し、次のXMLコードを挿入します。

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>



<Association Identifier="http" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



</DefaultAssociations>
```

グループポリシー管理コンソールから、**コンピューターの構成 > 管理用テンプレート > Windows コンポーネント > エクスプローラー > 既定の関連付け構成ファイルの設定** に移動し、ServerFTAdefaultPolicy.xmlファイルを保存します。

注:

Citrixサーバーにグループポリシー設定がない場合、WindowsはURLを開くためのアプリケーションを選択するようユーザーに促します。

デフォルトでは、次のURLタイプのリダイレクトをサポートしています。

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

リダイレクトのリストに追加の標準またはカスタムURLタイプを含めるには、前述のServerFTAdefaultPolicy.xmlファイルに新しい**関連付け識別子**の行を作成します。例：

```
<Association Identifier="ftp" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />

<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />

<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />

<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

リストにURLタイプを追加するには、クライアント構成も必要です。Windowsクライアントで以下のレジストリキーと値を作成します。

> **注:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような重大な問題が発生する可能性があります。レジストリエディターの誤った使用によって生じた問題が解決できることをCitrixは保証できません。レジストリエディターの使用は、お客様ご自身の責任において行ってください。編集する前に必ずレジストリをバックアップしてください。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 値の名前: ExtraURLProtocols
- 値の型: REG_SZ
- 値のデータ: 必要なURLタイプをセミコロンで区切って指定します。URLのオーソリティ部分より前のすべてを含めます。例： `ftp://;mailto:;customtype1://;custometype2://`

URLタイプはWindowsクライアントにのみ追加できます。上記のレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLタイプを処理するようにインストールおよび構成されたアプリケーションが必要です。

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: DisableServerFTA
- 値の型: DWORD
- 値のデータ: 1
- 値の名前: NoRedirectClasses
- 値の型: REG_MULTI_SZ
- 値のデータ: 次の値の任意の組み合わせを指定します: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または `mms`。複数の値を別々の行に入力します。例:

`http`

`https`

`rtsp`

特定のWebサイトのホストからクライアントへのリダイレクトを有効にするには、サーバーVDAにレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: ValidSites
- 値の型: REG_MULTI_SZ
- 値のデータ: 完全修飾ドメイン名 (FQDN) の任意の組み合わせを指定します。複数のFQDNを別々の行に入力します。プロトコル (`http://` または `https://`) を含めず、FQDNのみを含めます。FQDNには、左端の位置にのみアスタリスク (`*`) をワイルドカード文字として含めることができます。このワイルドカードは、RFC 6125のルールに準拠した単一レベルのドメインに一致します。例:

`www.exmaple.com`

`*.example.com`

> **注:**
>
> 「**ValidSites**」キーを「**DisableServerFTA**」キーおよび「**NoRedirectClasses**」キーと組み合わせて使用することはできません。

サーバーVDAのデフォルトブラウザ構成

このセクションで参照されているホストからクライアントへのリダイレクトを有効にすると、サーバーVDA上の以前のデフォルトブラウザ構成はすべて上書きされます。Web URLがリダイレクトされない場合、Citrix Launcherは、`command_backup`レジストリキーで構成されているブラウザにURLを渡します。このキーはデフォルトでInternet Explorerを指していますが、別のブラウザへのパスを含むように変更できます。詳細については、レジストリを介して管理される機能のリストにあるサーバーVDAのデフォルトブラウザ構成を参照してください。

双方向コンテンツリダイレクト

双方向コンテンツリダイレクトにより、Webブラウザ内のHTTPまたはHTTPS URL、あるいはアプリケーションに埋め込まれたURLを、Citrix VDAセッションとクライアントエンドポイント間で双方向に転送できます。Citrixセッションで実行されているブラウザに入力されたURLは、クライアントのデフォルトブラウザを使用して開くことができます。逆に、クライアントで実行されているブラウザに入力されたURLは、公開アプリケーションまたはデスクトップを使用してCitrixセッションで開くことができます。双方向コンテンツリダイレクトの一般的なユースケースには、次のものがあります。

- 開始ブラウザーがソースへのネットワークアクセスを持たない場合のWeb URLのリダイレクト。
- ブラウザーの互換性およびセキュリティ上の理由によるWeb URLのリダイレクト。
- CitrixセッションまたはクライアントでWebブラウザーを実行したくない場合に、アプリケーションに埋め込まれたWeb URLのリダイレクト。

システム要件

- シングルセッションまたはマルチセッションOS VDA
- シトリックス ワークスペース アプリ (Windows版) 2311以降
- シトリックス ワークスペース アプリ (Linux版) 2503以降
- シトリックス ワークスペース アプリ (Mac版) 2607以降

ブラウザー：

- シトリックス ブラウザ リダイレクション エクステンション を搭載した グーグル クローム
    - グーグル クローム エクステンション
- シトリックス ブラウザ リダイレクション エクステンション を搭載した マイクロソフト エッジ

- マイクロソフト エッジ エクステンション

構成

Citrix Virtual Apps and Desktops™ バージョン 2311 以降、双方向コンテンツリダイレクトは Citrix Studio を介してのみ構成されます。以前のリリースでは、クライアントエンドポイントと Studio の両方でポリシー設定が構成されていました。双方向コンテンツリダイレクトはデフォルトで無効になっています。

VDAの構成については、**ICAポリシー**設定の「双方向コンテンツリダイレクト」(/ja-jp/citrix-virtual-apps-desktops/2311/policies/reference/ica-policy-settings/bidirectional-content-redirection.html) を参照してください。

ブラウザリダイレクトを機能させるには、示されているコマンドを使用して、元のブラウザ（URLがリダイレクトされる場所）にブラウザ拡張機能を登録する必要があります。使用しているブラウザに基づいて、必要に応じてVDAとクライアントでコマンドを実行してください。

ブラウザ	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regChrome
マイクロソフト エッジ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regEdge
すべての利用可能なブラウザ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regall	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regall コマンド

ブラウザ拡張機能を登録解除するには：

ブラウザ	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregChrome

ブラウザ	VDA	クライアント
マイクロソフト エッジ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregEdge
利用可能なすべてのブラウザ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregall コマンド	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregall コマンド

注:

- これらのコマンドは、管理者権限でコマンドプロンプト（CMD）ウィンドウで実行します。
- 登録コマンドを実行すると、ChromeおよびEdgeブラウザーは、初回起動時にCitrix Browser Redirection Extensionを有効にするようユーザーに促します。
- 登録コマンドは、Browser Redirection Extensionをネイティブメッセージングホストにリンクさせ、これにより拡張機能がネイティブコードと通信できるようになります。これがないと、ブラウザーは通信をブロックします。
- ブラウザー拡張機能は、Google Chromeウェブストアから手動でインストールすることもできます。Microsoft EdgeアドオンストアからBrowser Redirection Extensionを使用するには、Virtual Delivery Agent (VDA) バージョン2503以降が必要です。古いVDAバージョンの場合は、Microsoft Edgeブラウザー内でGoogle Chromeウェブストアから拡張機能をインストールしてください（ChromeウェブストアからMicrosoft Edgeに拡張機能を追加するを参照）。
- システム要件に記載されているCitrix Workspaceアプリのバージョンは、双方向コンテンツリダイレクトとOAuthリダイレクトの両方をサポートするために必要な最小バージョンです。
- Macの場合：公証済みアプリケーションに関するmacOSのセキュリティ要件により、カスタムOAuthコールバックURLスキームはCitrixに事前登録する必要があり、インストール後に動的に変更することはできません。デフォルトでは`citrix-oauth-redir`のみがサポートされています。URLスキームを登録するには、Citrix製品チームにお問い合わせください。

Citrix VDAからクライアントへのワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトするURLを定義する際にワイルドカードの使用をサポートします。双方向コンテンツリダイレクトを構成するには、構成の手順を参照してください。

VDAからクライアントへのカスタムプロトコルリダイレクト

双方向コンテンツリダイレクトは、Citrix VDAからクライアントへのカスタムプロトコルのリダイレクトをサポートします。HTTPまたはHTTPS以外のプロトコルがサポートされています。双方向コンテンツリダイレクトを構成するには、構成の手順を参照してください。

Web Studioで、**双方向コンテンツリダイレクト**のカスタムプロトコルを設定します。

> **注:**
>
> - これらのコマンドを実行するには、管理者権限が必要です。
> - クライアントには、プロトコルを処理するために登録されたアプリケーションが必要です。そうでない場合、URLはクライアントにリダイレクトされますが、起動に失敗します。
> - ChromeおよびEdgeブラウザーで入力または起動するカスタムプロトコルURLはサポートされておらず、リダイレクトされません。
> - 以下のプロトコルはサポートされていません: `rtsp://, rtspu://, pnm://, mms://`。

その他の考慮事項

- ブラウザの要件と構成は、リダイレクトを開始するブラウザにのみ適用されます。リダイレクトが成功した後にURLが開かれる宛先ブラウザは、サポートの対象とはなりません。VDAからクライアントにURLをリダイレクトする場合、サポートされるブラウザ構成はVDA上でのみ必要です。逆に、クライアントからVDAにURLをリダイレクトする場合、サポートされるブラウザ構成はクライアント上でのみ必要です。リダイレクトされたURLは、方向に応じて、クライアントまたはVDAのいずれかの宛先マシンで構成されたデフォルトのブラウザに渡されます。VDAとクライアントで同じブラウザタイプを使用する必要はありません。
- リダイレクトルールがループ構成にならないことを確認してください。たとえば、VDAポリシーが`https://www.citrix.com`をリダイレクトするように設定されており、クライアント

ポリシーが同じURLをリダイレクトするように設定されている場合、無限ループが発生します。

- URL短縮サービスはサポートされていません。
- クライアントからVDAへのリダイレクトには、Windowsクライアントが管理者権限でインストールされている必要があります。
- 宛先ブラウザーがすでに開いている場合、リダイレクトされたURLは新しいタブで開きます。そうでない場合、URLは新しいブラウザーウィンドウで開きます。
- 双方向コンテンツリダイレクトは、ローカルアプリアクセス（LAA）が有効になっている場合は機能しません。

ローカルアプリアクセスとURLリダイレクト

はじめに

ローカルアプリアクセスは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。ローカルアプリアクセスを使用すると、次のことができます。

- 物理的なラップトップ、PC、またはその他のデバイスにローカルにインストールされているアプリケーションに、仮想デスクトップから直接アクセスできます。
- 柔軟なアプリケーション配信ソリューションを提供します。仮想化できないローカルアプリケーションや、IT部門が保守していないローカルアプリケーションがある場合でも、それらのアプリケーションは仮想デスクトップにインストールされているかのように動作します。
- アプリケーションが仮想デスクトップとは別にホストされている場合のダブルホップ遅延を解消します。これを行うには、公開されたアプリケーションへのショートカットをユーザーのWindowsデバイスに配置します。
- 次のようなアプリケーションを使用します。
    - GoToMeetingなどのビデオ会議ソフトウェア。
    - まだ仮想化されていない特殊なアプリケーションやニッチなアプリケーション。
    - ユーザーデバイスからサーバーへ、そしてサーバーからユーザーデバイスへ大量のデータを転送する可能性のあるアプリケーションや周辺機器。たとえば、DVDバーナーやTVチューナーなどです。

Citrix Virtual Apps and Desktops™では、ホストされたデスクトップセッションはURLリダイレクトを使用してローカルアプリアクセスアプリケーションを起動します。URLリダイレクトにより、アプリケーションは複数のURLアドレスで利用可能になります。デスクトップセッション内のブ

ラウザに埋め込まれたリンクを選択することで、ローカルブラウザ（ブラウザのURLブロックリストに基づいて）が起動します。ブロックリストにないURLに移動すると、そのURLはデスクトップセッションで再度開かれます。

URLリダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。アプリケーションセッションで使用できる唯一のリダイレクト機能は、ホストからクライアントへのコンテンツリダイレクトであり、これはサーバーFTA（ファイルタイプ関連付け）リダイレクトの一種です。このFTAは、HTTP、HTTPS、RTSP、MMSなどの特定のプロトコルをクライアントにリダイレクトします。たとえば、埋め込みリンクをHTTPでのみ開く場合、リンクはクライアントアプリケーションで直接開かれます。URLブロックリストや許可リストのサポートはありません。

ローカルアプリアクセスが有効になっている場合、ローカルで実行されているアプリケーション、ユーザーがホストするアプリケーションからのリンクとして、またはデスクトップ上のショートカットとしてユーザーに表示されるURLは、次のいずれかの方法でリダイレクトされます。

- ユーザーのコンピューターからホストされたデスクトップへ
- Citrix Virtual Apps and Desktopsサーバーからユーザーのコンピューターへ
- 起動された環境でレンダリングされる（リダイレクトされない）

特定のWebサイトからのコンテンツのリダイレクトパスを指定するには、Virtual Delivery AgentでURL許可リストとURLブロックリストを構成します。これらのリストには、URLリダイレクトポリシー設定を指定する複数文字列のレジストリキーが含まれています。詳細については、ローカルアプリアクセス ポリシー設定を参照してください。

次の例外を除き、URLはVDAでレンダリングできます。

- 地域/ロケール情報 — msn.comやnews.google.comなど、ロケール情報を必要とするWebサイト（地域に基づいて国固有のページを開く）。たとえば、VDAが英国のデータセンターからプロビジョニングされ、クライアントがインドから接続している場合、ユーザーはin.msn.comが表示されることを期待します。しかし、実際にはuk.msn.comが表示されます。
- マルチメディアコンテンツ — リッチメディアコンテンツを含むWebサイトは、クライアントデバイスでレンダリングされると、エンドユーザーにネイティブなエクスペリエンスを提供し、高遅延ネットワークでも帯域幅を節約します。この機能は、Silverlightなどの他のメディアタイプを含むサイトをリダイレクトします。このプロセスは安全な環境で行われます。つまり、管理者が承認したURLはクライアントで実行され、残りのURLはVDAにリダイレクトされます。

URLリダイレクトに加えて、FTAリダイレクトを使用できます。FTAは、セッションでファイルが検出されたときにローカルアプリケーションを起動します。ローカルアプリが起動された場合、

ローカルアプリはそのファイルを開くためにファイルへのアクセス権を持っている必要があります。したがって、ネットワーク共有またはクライアントドライブ（クライアントドライブマッピングを使用）にあるファイルのみをローカルアプリケーションを使用して開くことができます。たとえば、PDFファイルを開くときに、PDFリーダーがローカルアプリである場合、そのPDFリーダーを使用してファイルが開きます。ローカルアプリはファイルに直接アクセスできるため、ファイルを開くためにICA®を介したファイルのネットワーク転送は発生しません。

要件、考慮事項、および制限事項

WindowsマルチセッションOS用VDAおよびWindowsシングルセッションOS用VDAの有効なオペレーティングシステムで、ローカルアプリアクセスをサポートしています。ローカルアプリアクセスには、Citrix Workspaceアプリ for Windowsバージョン4.1（最小）が必要です。以下のブラウザがサポートされています。

- Edge、最新バージョン
- Firefox、最新バージョンおよび延長サポートリリース
- Chrome、最新バージョン

ローカルアプリアクセスとURLリダイレクトを使用する際の以下の考慮事項と制限事項を確認してください。

- ローカルアプリアクセスは、すべてのモニターにまたがる全画面の仮想デスクトップ向けに設計されています。
    - ウィンドウモードで実行される仮想デスクトップや、すべてのモニターをカバーしない仮想デスクトップでローカルアプリアクセスを使用すると、ユーザーエクスペリエンスが混乱する可能性があります。
    - 複数モニター — 1つのモニターが最大化されると、そのセッションで起動されたすべてのアプリケーションのデフォルトデスクトップになります。このデフォルトは、後続のアプリケーションが通常別のモニターで起動される場合でも発生します。
    - この機能は1つのVDAをサポートします。複数の同時VDAとの統合はありません。
- 一部のアプリケーションは予期せぬ動作をする可能性があり、ユーザーに影響を与えます。
    - ドライブ文字はユーザーを混乱させる可能性があります。たとえば、仮想デスクトップのC:ドライブではなく、ローカルのC:ドライブなどです。
    - 仮想デスクトップで利用可能なプリンターは、ローカルアプリケーションでは利用できません。

- 昇格された権限を必要とするアプリケーションは、クライアントホスト型アプリケーションとして起動できません。
- シングルインスタンスアプリケーション（Windows Media Playerなど）に対する特別な処理はありません。
- ローカルアプリケーションは、ローカルマシンのWindowsテーマで表示されます。
- 全画面表示アプリケーションはサポートされていません。これには、PowerPointのスライドショーやデスクトップ全体を覆うフォトビューアーなど、全画面で開くアプリケーションが含まれます。
- ローカルアプリアクセスは、ローカルアプリケーションのプロパティ（クライアントのデスクトップやスタートメニューのショートカットなど）をVDAにコピーします。ただし、ショートカットキーや読み取り専用属性などの他のプロパティはコピーしません。
- 重なり合うウィンドウの順序の処理方法をカスタマイズするアプリケーションは、予期せぬ結果をもたらす可能性があります。たとえば、一部のウィンドウが非表示になることがあります。
- ショートカットはサポートされていません。これには、マイコンピュータ、ごみ箱、コントロールパネル、ネットワークドライブのショートカット、フォルダーのショートカットが含まれます。
- 次のファイルの種類とファイルはサポートされていません。カスタムファイルの種類、関連付けられたプログラムがないファイル、zipファイル、隠しファイル。
- 32ビットと64ビットが混在するクライアントホスト型またはVDAアプリケーションでは、タスクバーのグループ化はサポートされていません。つまり、32ビットのローカルアプリケーションと64ビットのVDAアプリケーションをグループ化することです。
- COMを使用してアプリケーションを起動することはできません。たとえば、Officeアプリケーション内から埋め込みOfficeドキュメントをクリックした場合、プロセスの起動が検出されず、ローカルアプリケーションの統合が失敗します。

- ダブルホップシナリオ（ユーザーが別の仮想デスクトップセッション内から仮想デスクトップを起動するケース）はサポートされていません。
- URLリダイレクトは明示的なURL（つまり、ブラウザのアドレスバーに表示されるURL、またはブラウザに応じてブラウザ内ナビゲーションを使用して見つかるURL）のみをサポートします。
- URLリダイレクトは、アプリケーションセッションではなく、デスクトップセッションでのみ機能します。
- VDAセッションのローカルデスクトップフォルダーでは、ユーザーはファイルを作成できません。

- ローカルで実行されているアプリケーションの複数のインスタンスは、仮想デスクトップ用に確立されたタスクバー設定に従って動作します。ただし、ローカルで実行されているアプリケーションへのショートカットは、それらのアプリケーションの実行中のインスタンスとグループ化されません。また、ホストされたアプリケーションの実行中のインスタンスや、ホストされたアプリケーションへのピン留めされたショートカットともグループ化されません。ユーザーは、タスクバーからローカルで実行されているアプリケーションのウィンドウのみを閉じることができます。ユーザーはローカルアプリケーションのウィンドウをデスクトップのタスクバーやスタートメニューにピン留めできますが、これらのショートカットを使用するとアプリケーションが常に起動するとは限りません。
- **Allow Local App Access** ポリシー設定を **Enabled** に設定した場合、ブラウザコンテンツリダイレクトはサポートされません。デフォルトでは、Local App Access は禁止されています。

Windowsとの連携

Local App AccessとWindowsとの連携には、次の動作が含まれます。

- Windows 8およびWindows Server 2012のショートカットの動作
  - クライアントにインストールされているWindowsストアアプリケーションは、Local App Accessショートカットの一部として列挙されません。
  - 画像ファイルとビデオファイルは、デフォルトでWindowsストアアプリケーションを使用して開かれます。ただし、Local App AccessはWindowsストアアプリケーションを列挙し、デスクトップアプリケーションでショートカットを開きます。
- ローカルプログラム
  - Windows 7の場合、フォルダーはスタートメニューで利用できます。
  - Windows 8の場合、ローカルプログラムは、ユーザーがスタート画面からカテゴリとして **すべてのアプリ** を選択した場合にのみ利用できます。すべてのサブフォルダーがローカルプログラムに表示されるわけではありません。
- アプリケーション向けのWindows 8グラフィック機能
  - デスクトップアプリケーションはデスクトップ領域に制限されており、スタート画面およびWindows 8スタイルのアプリケーションによって覆われます。
  - ローカルアプリアクセスアプリケーションは、マルチモニターモードではデスクトップアプリケーションのように動作しません。マルチモニターモードでは、スタート画面とデスクトップが異なるモニターに表示されます。
- Windows 8とローカルアプリアクセスのURLリダイレクト

- Windows 8のInternet Explorerではアドオンが有効になっていないため、URLリダイレクトを有効にするにはデスクトップ版のInternet Explorerを使用してください。
- Windows Server 2012では、Internet Explorerはデフォルトでアドオンを無効にします。URLリダイレクトを実装するには、Internet Explorerの拡張構成を無効にします。その後、Internet Explorerのオプションをリセットして再起動し、標準ユーザー向けにアドオンが有効になっていることを確認してください。

ローカルアプリアクセスとURLリダイレクトの構成

Citrix Workspace™アプリでローカルアプリアクセスとURLリダイレクトを使用するには：

- ローカルクライアントマシンにCitrix Workspaceアプリをインストールします。Citrix Workspaceアプリのインストール中に両方の機能を有効にするか、グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にすることができます。
- **Allow Local App Access**ポリシー設定を**Enabled**に設定します。URLリダイレクトのURL許可リストおよびブロックリストポリシー設定も構成できます。詳しくは、「ローカルアプリアクセスのポリシー設定」を参照してください。

ローカルアプリアクセスとURLリダイレクトを有効にする

すべてのローカルアプリケーションでローカルアプリアクセスを有効にするには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**Policies**をクリックします。
2. アクションバーで、**Create Policy**をクリックします。
3. Create Policyウィンドウで、検索ボックスに「Allow Local App Access」と入力し、**Select**をクリックします。
4. Edit Settingウィンドウで、**Allowed**を選択します。デフォルトでは、**Allow local app access**ポリシーは禁止されています。この設定が許可されている場合、VDAはエンドユーザーが公開アプリケーションとローカルアプリアクセスのショートカットをセッションで有効にするかどうかを決定できるようにします（この設定が禁止されている場合、公開アプリケーションとローカルアプリアクセスのショートカットはVDAでは機能しません）。このポリシー設定は、マシン全体とURLリダイレクトポリシーに適用されます。
5. Create Policyウィンドウで、検索ボックスに「URL redirection allow list」と入力し、**Select**をクリックします。URLリダイレクト許可リストは、リモートセッションのデフォルトブラウザで開くURLを指定します。
6. 「設定の編集」ウィンドウで、「**追加**」をクリックしてURLを追加し、「**OK**」をクリックします。

7. 「ポリシーの作成」ウィンドウで、検索ボックスに「URL redirection block list」と入力し、「**選択**」をクリックします。URLリダイレクトブロックリストは、エンドポイントで実行されているデフォルトのブラウザーにリダイレクトされるURLを指定します。
8. 「設定の編集」ウィンドウで、「**追加**」をクリックしてURLを追加し、「**OK**」をクリックします。
9. 「設定」ページで、「**次へ**」をクリックします。
10. 「ユーザーとマシン」ページで、該当するデリバリーグループにポリシーを割り当て、「**次へ**」をクリックします。
11. 「概要」ページで、設定を確認し、「**完了**」をクリックします。

Citrix Workspaceアプリのインストール中にすべてのローカルアプリケーションでURLリダイレクトを有効にするには、次の手順に従います。

1. マシン上のすべてのユーザーに対してCitrix Workspaceアプリをインストールするときに、URLリダイレクトを有効にします。これにより、URLリダイレクトに必要なブラウザーアドオンも登録されます。
2. コマンドプロンプトから、次のいずれかのオプションを使用してCitrix Workspaceアプリをインストールするための適切なコマンドを実行します。
   - CitrixReceiver.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。
   - CitrixReceiverWeb.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。

グループポリシーエディターを使用してローカルアプリアクセス テンプレートを有効にする

注:

- グループポリシーエディターを使用してローカルアプリアクセス テンプレートを有効にする前に、receiver.admx/admlテンプレートファイルをローカルGPOに追加します。
- Citrix Workspaceアプリ for Windowsのテンプレートファイルは、CitrixBase.admx/CitrixBase.admlを%systemroot%\policyDefinitionsフォルダーに追加した場合のみ、ローカルGPOの「**管理用テンプレート > Citrix Components > Citrix Workspace**」フォルダーにあります。

> グループポリシーエディターを使用してローカルアプリアクセス テンプレートを有効にするには、次の手順に従います。

1. **gpedit.msc**を実行します。
2. **> > > > >** の順に移動します。
3. をクリックします。
4. を選択し、次に を選択します。URLリダイレクトについては、この記事の後半にある「*ブラウザアドオンの登録*」セクションで説明されているコマンドラインを使用して、ブラウザアドオンを登録してください。

公開アプリケーションのみにアクセスを提供する

レジストリエディターまたはPowerShell SDKを使用して、公開アプリケーションへのアクセスを提供できます。

レジストリエディターについては、レジストリを介して管理される機能のリストにある公開アプリケーションのローカルアプリアクセスを参照してください。

PowerShell SDKを使用するには：

1. Delivery Controller™が実行されているマシンでPowerShellを開きます。
2. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

クラウドサービス展開で にアクセスするには、Citrix DaaS Remote PowerShell SDKを使用します。詳細については、Citrix DaaS Remote PowerShell SDKを参照してください。

1. インストーラーをダウンロードします:

   `<https://download.apps.cloud.com/CitrixPoshSdk.exe>`
2. 次のコマンドを実行します:

   a. `asnp citrix.*`.

   b. `Get-XdAuthentication`
3. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

該当する前の手順を完了したら、以下の手順に従って続行します。

1. Web Studioにサインインし、左側のペインで**アプリケーション**を選択します。

2. 上部中央のペインで、空白の領域を右クリックし、コンテキストメニューから**ローカルアプリアクセスアプリケーションの追加**を選択します。アクションバーで**ローカルアプリアクセスアプリケーションの追加**をクリックすることもできます。アクションバーにローカルアプリアクセスアプリケーションの追加オプションを表示するには、**更新**をクリックします。
3. ローカルアプリアクセスアプリケーションを公開します。

    - ローカルアプリケーションアクセスウィザードが「はじめに」ページとともに起動します。このページは、今後のウィザードの起動時に表示しないように設定できます。
    - ウィザードは、以下に説明する「グループ」、「場所」、「識別」、「配信」、「概要」の各ページを案内します。各ページの作業が完了したら、**次へ**をクリックして「概要」ページに進みます。
    - 「グループ」ページで、新しいアプリケーションを追加するデリバリーグループを1つ以上選択し、**次へ**をクリックします。
    - 「場所」ページで、ユーザーのローカルマシン上のアプリケーションの完全な実行可能パスを入力し、アプリケーションが配置されているフォルダーへのパスを入力します。Citrixでは、システム環境変数パスを使用することをお勧めします。例: %ProgramFiles(x86)%\Internet Explorer\iexplore.exe。
    - 「識別」ページで、デフォルト値を受け入れるか、必要な情報を入力して**次へ**をクリックします。
    - 「配信」ページで、このアプリケーションをユーザーに配信する方法を構成し、**次へ**をクリックします。選択したアプリケーションのアイコンを指定できます。また、仮想デスクトップ上のローカルアプリケーションへのショートカットを、スタートメニュー、デスクトップ、またはその両方に表示するかどうかも指定できます。
    - 「概要」ページで設定を確認し、**完了**をクリックしてローカルアプリケーションアクセスウィザードを終了します。

ブラウザアドオンを登録する

> **注:**
>
> コマンドラインからCitrix Workspaceアプリを/ALLOW_CLIENTHOSTEDAPPSURL=1オプションを使用してインストールすると、URLリダイレクトに必要なブラウザアドオンが自動的に登録されます。

1つまたはすべてのアドオンを登録および登録解除するには、次のコマンドを使用します。

- クライアントデバイスにアドオンを登録するには：\<*client-installation-folder*>\redirector.exe /reg\<*browser*>
- クライアントデバイスからアドオンを登録解除するには：\<*client-installation-folder*>\redirector.exe /unreg\<*browser*>
- VDAにアドオンを登録するには：\<*VDAinstallation-folder*>\VDARedirector.exe /reg\<*browser*>
- VDAからアドオンを登録解除するには：\<*VDAinstallation-folder*>\VDARedirector.exe /unreg\<*browser*>

ここで、\<*browser*> はInternet Explorer、Firefox、Chrome、またはAllです。

たとえば、次のコマンドは、Citrix Workspaceアプリを実行しているデバイスにInternet Explorerアドオンを登録します。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

次のコマンドは、WindowsマルチセッションOS VDAにすべてのアドオンを登録します。

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

ブラウザ間のURLインターセプト

- デフォルトでは、Internet Explorerは指定されたURLをリダイレクトします。URLがブロックリストにないが、ブラウザまたはWebサイトが別のURLにリダイレクトする場合、最終的なURLはリダイレクトされません。ブロックリストにある場合でもリダイレクトされません。

URLリダイレクトが正しく機能するには、ブラウザからプロンプトが表示されたときにアドオンを有効にします。インターネットオプションを使用しているアドオン、またはプロンプトに表示されるアドオンが無効になっている場合、URLリダイレクトは正しく機能しません。

- Firefoxのアドオンは常にURLをリダイレクトします。

アドオンがインストールされると、Firefoxは新しいタブページにアドオンのインストールを許可するか、または防止するかを促します。機能が動作するようにアドオンを許可してください。

- Chromeのアドオンは、入力されたURLではなく、常にナビゲートされた最終URLをリダイレクトします。

拡張機能は外部からインストールされています。拡張機能を無効にすると、ChromeではURLリダイレクト機能が動作しません。シークレットモードでURLリダイレクトが必要な場合は、ブラウザ設定でそのモードでの拡張機能の実行を許可してください。

ログオフ時および切断時のローカルアプリケーションの動作を構成する

注:

これらの手順に従って設定を構成しない場合、デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは引き続き実行されます。再接続後、仮想デスクトップで利用可能な場合、ローカルアプリケーションは再統合されます。

ログオフ時および切断時のローカルアプリケーションの動作を構成するには、レジストリを介して管理される機能のリストにあるログオフ時および切断時のローカルアプリケーションの動作を参照してください。

汎用USBリダイレクトとクライアントドライブに関する考慮事項

HDX™テクノロジーは、ほとんどの一般的なUSBデバイスに対して**最適化されたサポート**を提供します。最適化されたサポートは、WAN経由でのパフォーマンスと帯域幅効率を向上させ、ユーザーエクスペリエンスを改善します。最適化されたサポートは、特に高遅延またはセキュリティに敏感な環境において、通常は最良の選択肢です。

HDXテクノロジーは、最適化されたサポートがない、または不適切な特殊なデバイスに対して**汎用USBリダイレクト**を提供します。たとえば、次のような場合です。

- USBデバイスに、最適化されたサポートに含まれていないより高度な機能がある場合（たとえば、マウスやWebカメラにボタンが多い場合など）。
- ユーザーが最適化されたサポートに含まれていない機能を必要とする場合。
- USBデバイスが特殊なデバイスである場合（たとえば、テストおよび測定機器や産業用コントローラーなど）。
- アプリケーションがUSBデバイスとしてデバイスに直接アクセスを必要とする場合。
- USBデバイスにWindowsドライバーしか利用できない場合。たとえば、スマートカードリーダーには、Android版Citrix Workspace™アプリ用のドライバーが利用できない場合があります。
- Citrix Workspaceアプリのバージョンが、この種のUSBデバイスに対して最適化されたサポートを提供しない場合。

汎用USBリダイレクトを使用する場合：

- ユーザーはユーザーデバイスにデバイスドライバーをインストールする必要がありません。
- USBクライアントドライバーはVDAマシンにインストールされます。

重要：

- 汎用USBリダイレクトは、最適化されたサポートと組み合わせて使用できます。汎用USBリダイレクトを有効にする場合は、汎用USBリダイレクトと最適化されたサポートの両方に対してCitrixのUSBデバイスポリシー設定を構成します。
- クライアントUSBデバイス最適化ルールのCitrixポリシー設定は、特定のUSBデバイスに対する汎用USBリダイレクトの固有の設定です。ここで説明されている最適化されたサポートには適用されません。

USBデバイスのパフォーマンスに関する考慮事項

一部の種類のUSBデバイスで汎用USBリダイレクトを使用する場合、ネットワークの遅延と帯域幅がユーザーエクスペリエンスとUSBデバイスの動作に影響を与える可能性があります。たとえば、タイミングに敏感なデバイスは、高遅延で低帯域幅のリンクでは正しく動作しない場合があります。可能な場合は、代わりに最適化されたサポートを使用してください。

一部のUSBデバイスは、使用するために高い帯域幅を必要とします。たとえば、3Dマウス（通常、高い帯域幅を必要とする3Dアプリで使用されます）などです。帯域幅を増やすことができない場合、帯域幅ポリシー設定を使用して他のコンポーネントの帯域幅使用量を調整することで、問題を軽減できる可能性があります。詳細については、クライアントUSBデバイスリダイレクトの帯域幅ポリシー設定と、マルチストリーム接続ポリシー設定を参照してください。

USBデバイスのセキュリティに関する考慮事項

スマートカードリーダー、指紋リーダー、署名パッドなど、一部のUSBデバイスは本質的にセキュリティに敏感です。USBストレージデバイスなどの他のUSBデバイスは、機密データを送信するために使用される可能性があります。

USBデバイスはマルウェアを配布するためによく使用されます。Citrix WorkspaceアプリとCitrix Virtual Apps and Desktops™の設定により、これらのUSBデバイスからのリスクを軽減できますが、完全に排除することはできません。この状況は、汎用USBリダイレクトを使用する場合でも、最適化されたサポートを使用する場合でも当てはまります。

重要:

セキュリティに敏感なデバイスとデータの場合、常にTLSまたはIPsecのいずれかを使用してHDX接続を保護してください。

必要なUSBデバイスのサポートのみを有効にしてください。このニーズを満たすように、汎用USBリダイレクトと最適化されたサポートの両方を構成してください。

USBデバイスを安全に使用するためのガイダンスをユーザーに提供してください。

- 信頼できる情報源から入手したUSBデバイスのみを使用してください。
- オープンな環境でUSBデバイスを放置しないでください。たとえば、インターネットカフェでのフラッシュドライブなどです。
- 複数のコンピューターでUSBデバイスを使用するリスクを説明してください。

汎用USBリダイレクトとの互換性

汎用USBリダイレクトは、USB 2.0以前のデバイスでサポートされています。汎用USBリダイレクトは、USB 2.0またはUSB 3.0ポートに接続されたUSB 3.0デバイスでもサポートされています。汎用USBリダイレクトは、スーパースピードなど、USB 3.0で導入されたUSB機能はサポートしていません。

次のCitrix Workspaceアプリは、汎用USBリダイレクトをサポートしています。

- Windows向けCitrix Workspaceアプリ。詳細については、アプリケーション配信の構成を参照してください。
- Mac向けCitrix Workspaceアプリ。詳細については、Citrix Workspace app for Macを参照してください。
- Linux向けCitrix Workspaceアプリ。詳細については、最適化を参照してください。
- Chrome OS向けCitrix Workspaceアプリ。詳細については、Citrix Workspace app for Chromeを参照してください。

Citrix Workspaceアプリのバージョンについては、Citrix Workspaceアプリの機能マトリックスを参照してください。

以前のバージョンのCitrix Workspaceアプリを使用している場合は、Citrix Workspaceアプリのドキュメントを参照して、汎用USBリダイレクトがサポートされていることを確認してください。サポートされているUSBデバイスの種類に関する制限については、Citrix Workspaceアプリのドキュメントを参照してください。

汎用USBリダイレクトは、VDA for Single-session OSバージョン7.6以降のデスクトップセッションでサポートされています。

汎用USBリダイレクトは、VDA for Multi-session OSバージョン7.6以降のデスクトップセッションでサポートされていますが、次の制限があります。

- VDAは、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、またはWindows Server 2022を実行している必要があります。
- USBデバイスドライバーは、完全な仮想化サポートを含め、VDA OS（Windows 2012 R2）のRemote Desktop Session Host（RDSH）と完全に互換性がある必要があります。

一部の種類のUSBデバイスは、リダイレクトしても有用ではないため、汎用USBリダイレクトではサポートされていません。

- USBモデム。
- USBネットワークアダプター。
- USBハブ。USBハブに接続されたUSBデバイスは個別に処理されます。
- USB仮想COMポート。汎用USBリダイレクトではなく、COMポートリダイレクトを使用してください。

汎用USBリダイレクトでテスト済みのUSBデバイスについては、Citrix Ready Marketplaceを参照してください。一部のUSBデバイスは、汎用USBリダイレクトで正しく動作しません。

汎用USBリダイレクトの構成

汎用USBリダイレクトを使用するUSBデバイスの種類は、個別に制御および構成できます。

- VDA上で、Citrixポリシー設定を使用します。詳しくは、ポリシー設定リファレンスのクライアントドライブとユーザーデバイスのリダイレクトおよびUSBデバイスポリシー設定を参照してください。
- Citrix Workspaceアプリで、Citrix Workspaceアプリに依存するメカニズムを使用します。たとえば、管理用テンプレートは、Windows向けCitrix Workspaceアプリを構成するレジストリ設定を制御します。デフォルトでは、特定のクラスのUSBデバイスに対してUSBリダイレクトが許可され、その他のデバイスに対しては拒否されます。詳しくは、Windows向けCitrix Workspaceアプリのドキュメントの構成を参照してください。

この個別の構成により、柔軟性が向上します。例：

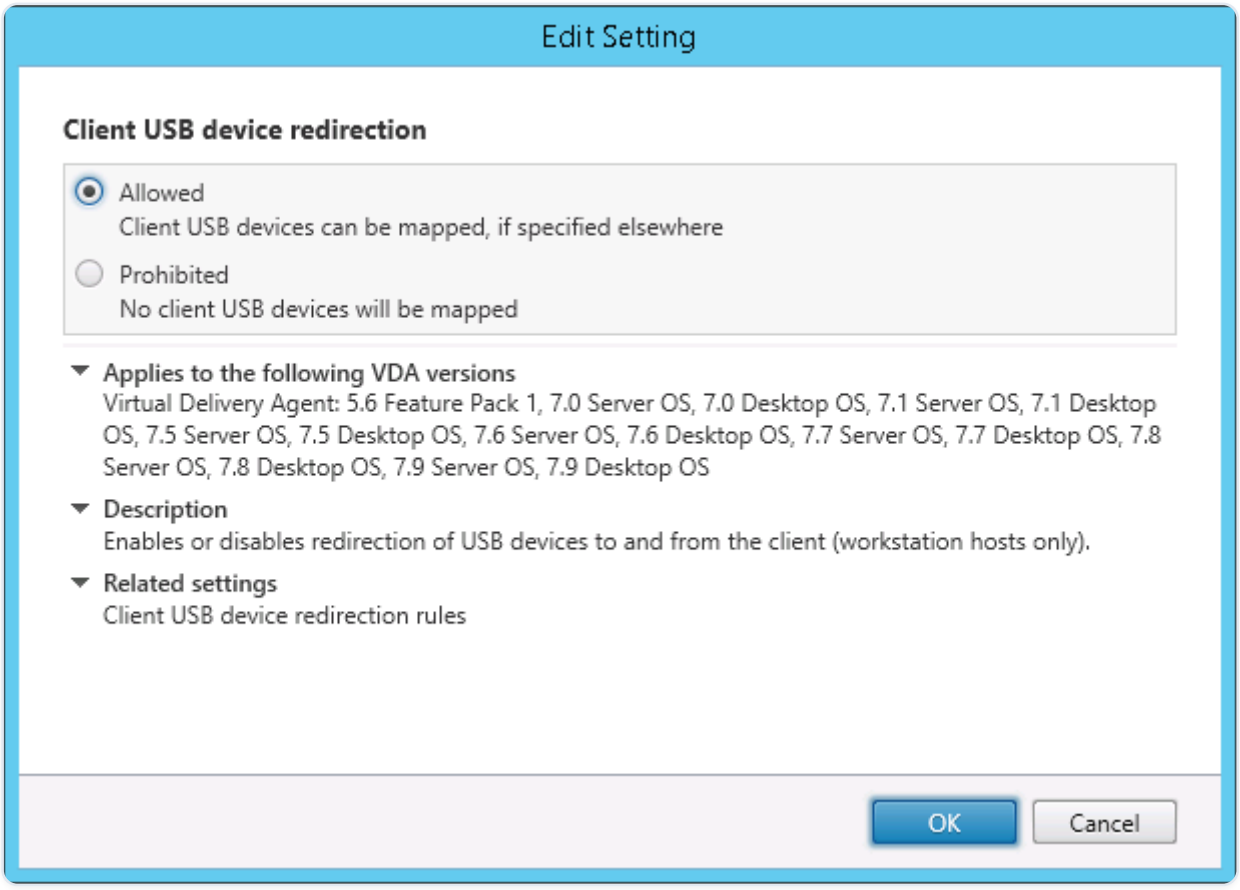
- 2つの異なる組織または部門がCitrix WorkspaceアプリとVDAを担当している場合、それぞれが個別に制御を適用できます。この構成は、ある組織のユーザーが別の組織のアプリケーションにアクセスする場合に適用されます。
- Citrixポリシー設定は、特定のユーザーのみ、またはLAN経由でのみ接続するユーザー（Citrix Gatewayを使用しない場合）に許可されるUSBデバイスを制御できます。

汎用USBリダイレクトを有効にする

汎用USBリダイレクトを有効にし、ユーザーによる手動リダイレクトを不要にするには、Citrixポリシー設定とCitrix Workspaceアプリの接続設定の両方を構成します。

Citrixポリシー設定で：

1. クライアントUSBデバイスリダイレクトをポリシーに追加し、その値を**許可**に設定します。



2. （オプション）リダイレクトに利用可能なUSBデバイスのリストを更新するには、クライアントUSBデバイスリダイレクト規則設定をポリシーに追加し、USBポリシー規則を指定します。

   ポリシー設定が完了したら、Citrix Workspaceアプリで:

3. デバイスが手動リダイレクトなしで自動的に接続されるように指定します。これは、管理テンプレートを使用するか、Citrix Workspaceアプリの **Windows > Preferences > Connections** で行うことができます。

   接続画像(/en-us/citrix-virtual-apps-desktops/2311/media/connections-generic-usb-devices-receiver.png)

前のステップでVDAのUSBポリシー規則を指定した場合は、Citrix Workspaceアプリにも同じポリシー規則を指定します。

シンクライアントについては、USBサポートの詳細と必要な構成について製造元にお問い合わせください。

汎用USBリダイレクトで利用可能なUSBデバイスの種類を構成する

USBサポートが有効で、USBユーザー設定がUSBデバイスを自動的に接続するように設定されている場合、USBデバイスは自動的にリダイレクトされます。接続バーが存在しない場合も、USBデバイスは自動的にリダイレクトされます。

ユーザーは、USBデバイスリストからデバイスを選択することで、自動的にリダイレクトされないデバイスを明示的にリダイレクトできます。詳細については、Citrix Workspaceアプリ for Windowsのユーザーヘルプ記事「Desktop Viewerでデバイスを表示する」を参照してください。

デバイス画像(/en-us/citrix-virtual-apps-desktops/2311/media/usb-device-list-receiver.png)

最適化されたサポートではなく、汎用USBリダイレクトを使用するには、次のいずれかの方法があります。

- Citrix Workspaceアプリで、汎用USBリダイレクトを使用するUSBデバイスを手動で選択し、環境設定ダイアログボックスの タブから を選択します。
- USBデバイスタイプ（例: AutoRedirectStorage=1）の自動リダイレクトを構成し、USBユーザー設定でUSBデバイスを自動的に接続するように設定することで、汎用USBリダイレクトを使用するUSBデバイスを自動的に選択します。詳しくは、「USBデバイスの自動リダイレクトを構成する」を参照してください。

> **注:**
>
> ウェブカメラがHDXマルチメディアリダイレクトと互換性がないと判明した場合にのみ、ウェブカメラでの使用のために汎用USBリダイレクトを構成してください。

> USBデバイスがリストされたりリダイレクトされたりするのを完全に防ぐには、Citrix WorkspaceアプリとVDAにデバイス規則を指定できます。

汎用USBリダイレクトの場合、少なくともUSBデバイスクラスとサブクラスを知る必要があります。すべてのUSBデバイスが、その明白なUSBデバイスクラスとサブクラスを使用するわけではありません。例：

- ペンはマウスデバイスクラスを使用します。
- スマートカードリーダーは、ベンダー定義またはHIDデバイスクラスを使用できます。

より正確な制御のためには、ベンダーID、製品ID、およびリリースIDを知る必要があります。この情報はデバイスベンダーから入手できます。

> **重要:**
>
> 悪意のあるUSBデバイスは、意図された用途と一致しないUSBデバイス特性を示す可能性があります。デバイスルールは、この動作を防ぐことを目的としていません。

> 汎用USBリダイレクトで利用可能なUSBデバイスは、デフォルトのUSBポリシー規則を上書きするために、USBデバイスリダイレクト規則を指定することで制御します。

シトリックス DaaS（旧シトリックス バーチャルアプリ＆デスクトップサービス）：

- ほとんどの場合、Citrix Group Policy Management Console MSI（`CitrixGroupPolicyManagement_x64.msi`）をダウンロードしてActive Directoryシステムにインストールし、ADグループポリシーを管理します。（VDAにはMSIをインストールしないでください。）
- Citrix Workspace app for Windowsの場合、ユーザーデバイスのレジストリを編集します。Active Directoryグループポリシーを通じてユーザーデバイスを変更できるように、管理用テンプレート（ADMファイル）がインストールメディアに含まれています：dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

オンプレミス版Citrix Virtual Apps and Desktops：

- VDAの場合、グループポリシー規則を通じて、マルチセッションOSマシンの管理者上書き規則を編集します。Group Policy Management Consoleはインストールメディアに含まれています：

  - x64: DVDルート `\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86: DVD ルート `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`

- Citrix Workspace app for Windowsの場合、ユーザーデバイスのレジストリを編集します。Active Directoryグループポリシーを通じてユーザーデバイスを変更できるように、管理用テンプレート（ADMファイル）がインストールメディアに含まれています：dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

> **警告：**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。レジストリエディターの誤った使用によって発生した問題が解決されることを、Citrixは保証できません。レジストリエディターは、ご自身の責任において使用してください。編集する前に、必ずレジストリをバックアップしてください。

> 製品のデフォルトルールは、HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\GenericUSB に保存されています。これらの製品のデフォルトルールは編集しないでください。代わりに、この記事の後半で説明する管理者オーバーライドルールを作成するためのガイドとして使用してください。GPOオーバーライドは、製品のデフォルトルールよりも前に評価されます。

管理者オーバーライドルールは、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules に保存されています。GPOポリシーのルールは、**{Allow: | Deny:}** の形式で、その後に空白で区切られた *tag=value* 式のセットが続きます。

次のタグがサポートされています。

タグ	説明
VID	デバイス記述子からのベンダーID
PID	デバイス記述子からの製品ID
REL	デバイス記述子からのリリースID

タグ	説明
クラス	デバイス記述子またはインターフェイス記述子のいずれかからのクラス。利用可能なUSBクラスコードについては、`<http://www.usb.org/>` のUSB Webサイトを参照してください
サブクラス	デバイス記述子またはインターフェイス記述子のいずれかからのサブクラス
プロトコル	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル

ポリシー規則を作成する際は、次の点に注意してください。

- 規則では大文字と小文字は区別されません。
- 規則には、`#` で始まるオプションのコメントを末尾に含めることができます。区切り文字は不要で、コメントは照合目的では無視されます。
- 空白行と純粋なコメント行は無視されます。
- 空白は区切り文字として使用されますが、数値または識別子の中央に表示することはできません。たとえば、Deny: Class = 08 SubClass=05 は有効な規則ですが、Deny: Class=0 Sub Class=05 は無効です。
- タグは一致演算子 = を使用する必要があります。例：VID=1230。
- 各規則は新しい行で開始するか、セミコロン区切りのリストの一部を形成する必要があります。

注：

- Citrix Virtual Apps and Desktopsバージョン2212以降、一部のUSBデバイスは汎用USBリダイレクト機能の使用が無効になっています。これらのデバイスは、それぞれのベンダーID（VID）と製品ID（PID）を使用して明示的に追加する必要があります。
- ADMテンプレートファイルを使用している場合は、セミコロン区切りのリストとして、単一行で規則を作成する必要があります。

例：

- 以下は、ベンダーおよび製品識別子に対する管理者定義のUSBポリシー規則の例です。

  ```
  Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products
  ```

- 以下は、定義されたクラス、サブクラス、およびプロトコルに対する管理者定義のUSBポリシー規則の例です。

  ```
  Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices
  ```

USBデバイスの使用と削除

ユーザーは、仮想セッションを開始する前または後にUSBデバイスを接続できます。

Windows向けCitrix Workspaceアプリを使用する場合、以下が適用されます。

- セッション開始後に接続されたデバイスは、Desktop ViewerのUSBメニューにすぐに表示されます。
- USBデバイスが適切にリダイレクトされない場合は、仮想セッションが開始されるまでデバイスの接続を待つことで問題を解決できる場合があります。
- データ損失を避けるため、USBデバイスを取り外す前にWindowsの「ハードウェアを安全に取り外す」アイコンを使用してください。

USBマスストレージデバイスのセキュリティ制御

USB大容量記憶装置には最適化されたサポートが提供されます。このサポートは、Citrix Virtual Apps and Desktopsのクライアントドライブマッピングの一部です。ユーザーがログオンすると、ユーザーデバイス上のドライブは仮想デスクトップ上のドライブ文字に自動的にマッピングされます。ドライブは、マッピングされたドライブ文字を持つ共有フォルダーとして表示されます。クライアントドライブマッピングを構成するには、**Client removable drives**設定を使用します。この設定は、ICAポリシー設定のファイルリダイレクトポリシー設定セクションにあります。

USB大容量記憶装置では、クライアントドライブマッピング、汎用USBリダイレクト、またはその両方を使用できます。これらはCitrixポリシーを使用して制御します。主な違いは次のとおりです。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセス設定可能	はい	いいえ
暗号化デバイスアクセス	はい、デバイスにアクセスする前に暗号化が解除されている場合	はい
BitLocker To Goデバイス	いいえ	いいえ
セッション中にデバイスを安全に削除できる	いいえ	はい、ユーザーがオペレーティングシステムの安全な取り外しに関する推奨事項に従う場合。

汎用USBリダイレクトとクライアントドライブマッピングの両方のポリシーが有効になっており、セッション開始前または開始後にマスストレージデバイスが挿入された場合、クライアントドライブマッピングを使用してリダイレクトされます。汎用USBリダイレクトとクライアントドライブマッピングの両方のポリシーが有効になっており、デバイスが自動リダイレクト用に構成されていて、セッション開始前または開始後にマスストレージデバイスが挿入された場合、汎用USBリダイレクトを使用してリダイレクトされます。詳細については、Knowledge Centerの記事CTX123015を参照してください。

注:

USBリダイレクトは、50 Kbpsなどの低帯域幅接続でもサポートされます。ただし、大きなファイルのコピーは機能しません。

印刷

環境でプリンターを管理するには、複数の段階があります。

1. まだ慣れていない場合は、印刷の概念を理解してください。
2. 印刷アーキテクチャを計画します。これには、ビジネスニーズ、既存の印刷インフラストラクチャ、ユーザーとアプリケーションが現在印刷とどのようにやり取りしているか、およびどの印刷管理モデルが環境に最適であるかを分析することが含まれます。
3. プリンタープロビジョニング方法を選択し、印刷設計を展開するためのポリシーを作成して、印刷環境を構成します。新しい従業員やサーバーが追加されたときにポリシーを更新します。
4. パイロット印刷構成をユーザーに展開する前にテストします。
5. プリンタードライバーを管理し、印刷パフォーマンスを最適化することで、Citrix® 印刷環境を維持します。
6. 発生する可能性のある問題をトラブルシューティングします。

印刷の概念

展開の計画を開始する前に、印刷に関する次の主要な概念を理解していることを確認してください。

- 利用可能なプリンタープロビジョニングの種類
- 印刷ジョブのルーティング方法
- プリンタードライバー管理の基本

印刷の概念は、Windowsの印刷の概念に基づいています。環境内で印刷を構成し、正常に管理するには、Windowsのネットワーク印刷とクライアント印刷がどのように機能し、それがこの環境での印刷動作にどのように変換されるかを理解する必要があります。

印刷プロセス

この環境では、すべての印刷はアプリケーションをホストするマシン上で（ユーザーによって）開始されます。印刷ジョブは、ネットワークプリントサーバーまたはユーザーデバイスを介して印刷デバイスにリダイレクトされます。

仮想デスクトップおよびアプリケーションのユーザーには、永続的なワークスペースはありません。セッションが終了するとユーザーのワークスペースは削除されるため、すべての設定は各セッションの開始時に再構築する必要があります。その結果、ユーザーが新しいセッションを開始するたびに、システムはユーザーのワークスペースを再構築しなければなりません。

ユーザーが印刷する場合：

- ユーザーに提供するプリンターを決定します。これはプリンタープロビジョニングとして知られています。
- ユーザーの印刷設定を復元します。
- セッションのデフォルトプリンターを決定します。

プリンタープロビジョニング、印刷ジョブのルーティング、プリンタープロパティの保持、ドライバー管理のオプションを構成することで、これらのタスクの実行方法をカスタマイズできます。さまざまなオプション設定が、環境での印刷パフォーマンスとユーザーエクスペリエンスにどのように影響するかを必ず評価してください。

プリンタープロビジョニング

セッションでプリンターを利用可能にするプロセスは、プロビジョニングとして知られています。プリンタープロビジョニングは通常、動的に処理されます。つまり、セッションに表示されるプリンターは事前に決定されて保存されるわけではありません。代わりに、ログオン時および再接続時にセッションが構築される際に、ポリシーに基づいてプリンターが組み立てられます。その結果、ポリシーに反映されていれば、プリンターはポリシー、ユーザーの場所、およびネットワークの変更に応じて変化する可能性があります。したがって、異なる場所にローミングするユーザーは、ワークスペースの変更を確認する場合があります。

システムはまた、クライアント側のプリンターを監視し、クライアント側のプリンターの追加、削除、変更に基づいて、セッション内で自動作成されるプリンターを動的に調整します。この動的なプリンター検出は、さまざまなデバイスから接続するモバイルユーザーにメリットをもたらします。

プリンタープロビジョニングの最も一般的な方法は次のとおりです。

- **Universal Print Server** - Citrix Universal Print Server は、ネットワークプリンターのユニバーサル印刷をサポートします。Universal Print Server は、ユニバーサル印刷ドライバーを使用します。このソリューションにより、マルチセッションOSマシンで単一のドライバーを使用して、任意のデバイスからネットワーク印刷を行うことができます。

Citrix は、リモートプリントサーバーのシナリオで Citrix Universal™ Print Server を推奨しています。Universal Print Server は、最適化され圧縮された形式で印刷ジョブをネットワーク経由で転送するため、ネットワーク使用量を最小限に抑え、ユーザーエクスペリエンスを向上させます。

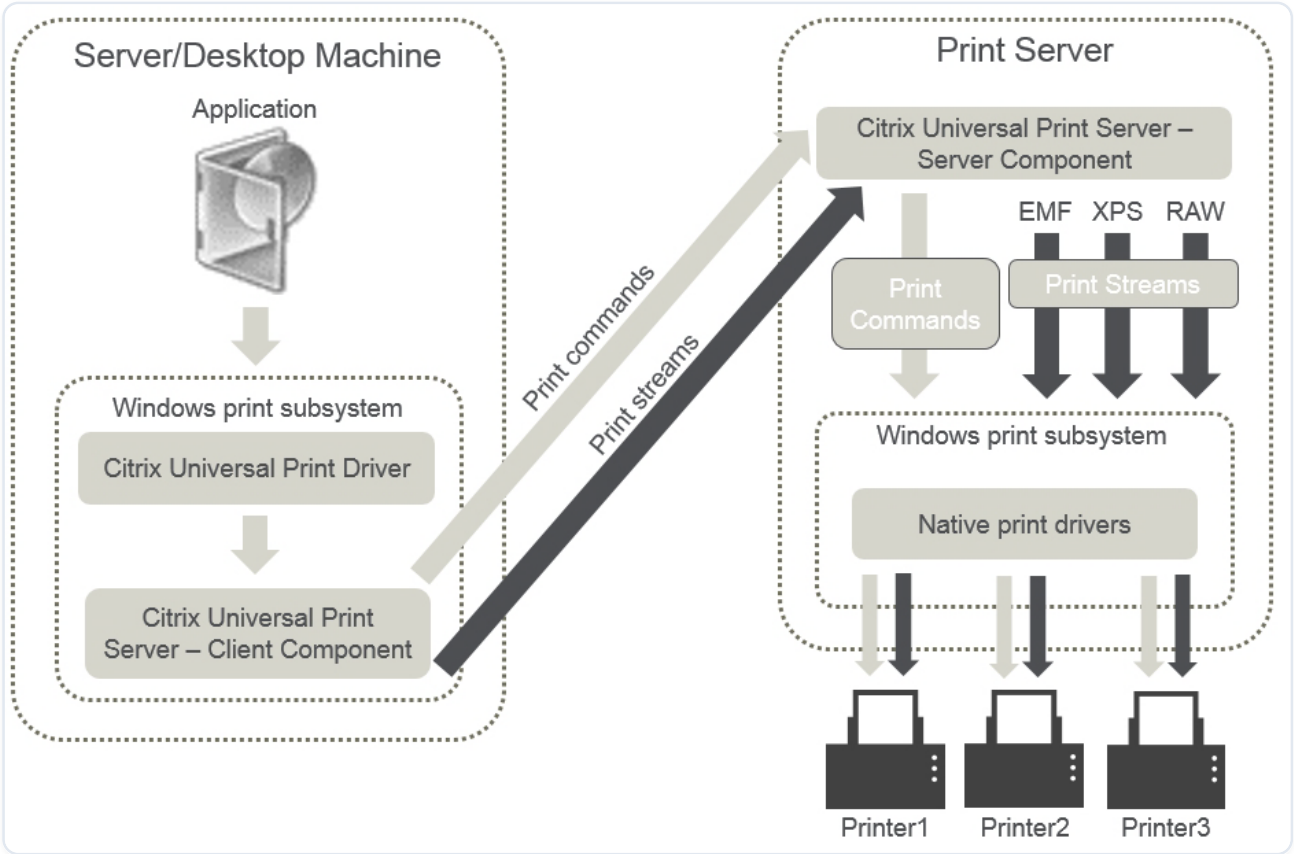
Universal Print Server の機能は次のとおりです。

クライアントコンポーネントである **UPClient** - セッションネットワークプリンターをプロビジョニングし、ユニバーサル印刷ドライバーを使用する各マルチセッションOSマシンで UPClient を有効にします。

サーバーコンポーネントである**UPServer** - セッションネットワークプリンターをプロビジョニングし、セッションプリンターにユニバーサルプリントドライバーを使用する各プリントサーバーにUPServerをインストールします（セッションプリンターが集中管理されているかどうかにかかわらず）。

Universal Print Serverの要件とセットアップの詳細については、システム要件とインストールの記事を参照してください。

次の図は、Universal Print Serverを使用する環境におけるネットワークベースのプリンターの一般的なワークフローを示しています。



Citrix Universal Print Serverを有効にすると、接続されているすべてのネットワークプリンターが自動検出によって自動的にそれを活用します。

- **自動作成** - *自動作成*とは、各セッションの開始時に自動的に作成されるプリンターを指します。リモートネットワークプリンターとローカルに接続されたクライアントプリンターの両方を自動作成できます。ユーザーあたりのプリンター数が多い環境では、デフォルトのクライアントプリンターのみを自動作成することを検討してください。自動作成するプリンターの数を減らすと、マルチセッションOSマシンでのオーバーヘッド（メモリとCPU）が少なくなります。自動作成されるプリンターを最小限に抑えることで、ユーザーのログオン時間を短縮することもできます。

  自動作成されるプリンターは、以下に基づいています。

  - ユーザーデバイスにインストールされているプリンター。
  - セッションに適用されるポリシー。

    自動作成ポリシー設定により、自動作成されるプリンターの数または種類を制限できます。デフォルトでは、ユーザーデバイス上のすべてのプリンター（ローカル接続プリンターとネットワークプリンターを含む）を自動的に構成すると、プリンターはセッションで利用可能になります。

  ユーザーがセッションを終了すると、そのセッションのプリンターは削除されます。

  クライアントおよびネットワークプリンターの自動作成には、関連するメンテナンスが必要です。たとえば、プリンターを追加するには、次の操作が必要です。

  - セッションプリンターポリシー設定を更新します。
  - プリンタードライバーマッピングと互換性ポリシー設定を使用して、すべてのマルチセッションOSマシンにドライバーを追加します。

印刷ジョブのルーティング

「印刷経路」という用語は、印刷ジョブがルーティングされるパスと、印刷ジョブがスプールされる場所の両方を指します。この概念の両方の側面が重要です。ルーティングはネットワークトラフィックに影響を与えます。スプーリングは、ジョブを処理するデバイス上のローカルリソースの利用に影響を与えます。

この環境では、印刷ジョブは印刷デバイスに到達するために2つのパスを取ることができます。クライアント経由か、ネットワークプリントサーバー経由かです。これらのパスは、クライアント印刷経路およびネットワーク印刷経路と呼ばれます。デフォルトでどちらのパスが選択されるかは、使用されるプリンターの種類によって異なります。

ローカル接続プリンター

システムは、Multi-session OSマシンからクライアントを介して、ローカル接続プリンターにジョブをルーティングし、その後印刷デバイスにルーティングします。ICA®プロトコルは、印刷ジョブのトラフィックを最適化および圧縮します。印刷デバイスがユーザーデバイスにローカルに接続されている場合、印刷ジョブはICA仮想チャネル経由でルーティングされます。

ローカル接続プリンターへの印刷ジョブのルーティング図(/en-us/citrix-virtual-apps-desktops/2311/media/cds-print-local-attached.png)

ネットワークベースのプリンター

デフォルトでは、ネットワークプリンター宛てのすべての印刷ジョブは、Multi-session OSマシンからネットワーク経由で直接プリントサーバーにルーティングされます。ただし、以下の状況では、印刷ジョブはICA接続経由で自動的にルーティングされます。

- 仮想デスクトップまたはアプリケーションがプリントサーバーに接続できない場合。
- Multi-session OSマシンでネイティブプリンタードライバーが利用できない場合。

Universal Print Serverが有効になっていない場合、ネットワーク印刷用にクライアント印刷経路を構成することは、ICA接続経由でジョブを送信することによって得られる最適化とトラフィック圧縮の恩恵を受けることができる、広域ネットワークなどの低帯域幅接続に役立ちます。

クライアント印刷経路を使用すると、トラフィックを制限したり、印刷ジョブに割り当てられる帯域幅を制限したりすることもできます。印刷機能のないシンクライアントのように、ユーザーデバイスを介したジョブのルーティングが不可能な場合は、ICA/HDXトラフィックを優先し、良好なセッション内ユーザーエクスペリエンスを確保するために、Quality of Serviceを構成する必要があります。

ネットワーク接続プリンターへの印刷ジョブのルーティング図(/en-us/citrix-virtual-apps-desktops/2311/media/cds-print-network-attached.png)

印刷ドライバー管理

Citrix Universal Printer Driver (UPD) は、ほとんどのプリンターと互換性のあるデバイス非依存の印刷ドライバーです。Citrix UPDは2つのコンポーネントで構成されています。

サーバーコンポーネント。Citrix UPDは、Citrix Virtual Apps and Desktops™ VDAのインストールの一部としてインストールされます。VDAは、Citrix UPDとともに以下のドライバーをインストールします。「Citrix Universal Printer」（EMFドライバー）と「Citrix XPS Universal Printer」（XPSドライバー）。

印刷ドライバー(/en-us/citrix-virtual-apps-desktops/2311/media/print-drivers.png)

VDAインストーラーは、Universal Print Server PDFプリンタードライバーのインストールを制御するオプションを提供しなくなりました。PDFプリンタードライバーは、常に自動的にインストールされるようになりました。7.17 VDA（またはそれ以降のサポートされるバージョン）にアップグレードすると、以前にインストールされていたCitrix PDFプリンタードライバーは自動的に削除され、最新バージョンに置き換えられます。

印刷ジョブが開始されると、ドライバーはアプリケーションの出力を記録し、変更せずにエンドポイントデバイスに送信します。

クライアントコンポーネント。Citrix UPD は、Citrix Workspace™ アプリのインストールの一部としてインストールされます。Citrix Virtual Apps and Desktops セッションの受信印刷ストリームを取得します。その後、印刷ストリームをローカル印刷サブシステムに転送し、そこでデバイス固有のプリンタードライバーを使用して印刷ジョブがレンダリングされます。

Citrix UPD は、次の印刷形式をサポートしています。

- 拡張メタファイル形式（**EMF**）、デフォルト。EMFは、Windowsメタファイル（WMF）形式の32ビットバージョンです。EMFドライバーは、Windowsベースのクライアントでのみ使用できます。
- XML Paper Specification（**XPS**）。XPSドライバーはXMLを使用して、Adobe PDF形式に似たプラットフォームに依存しない「電子ペーパー」を作成します。
- プリンターコマンド言語（**PCL5c**および**PCL4**）。PCLは、元々ヒューレット・パッカードがインクジェットプリンター向けに開発した印刷プロトコルです。基本的なテキストとグラフィックの印刷に使用され、HP LaserJetおよび多機能周辺機器で広くサポートされています。
- PostScript（**PS**）。PostScriptは、テキストとベクターグラフィックの印刷に使用できるコンピューター言語です。このドライバーは、低コストのプリンターや多機能周辺機器で広く使用されています。

PCLおよびPSドライバーは、MacやUNIXクライアントなどのWindows以外のデバイスを使用する場合に最適です。Citrix UPDがドライバーを使用しようとする順序は、Universal driver preferenceポリシー設定を使用して変更できます。

Citrix UPD（EMFおよびXPSドライバー）は、ステープルや給紙トレイ選択などの高度な印刷機能をサポートしています。これらの機能は、ネイティブドライバーがMicrosoft Print Capabilityテクノロジーを使用して利用可能にしている場合に利用できます。ネイティブドライバーは、Print Capabilities XMLで標準化されたPrint Schema Keywordsを使用する必要があります。非標準の

キーワードが使用されている場合、Citrix Universal Print Driverでは高度な印刷機能は利用できません。

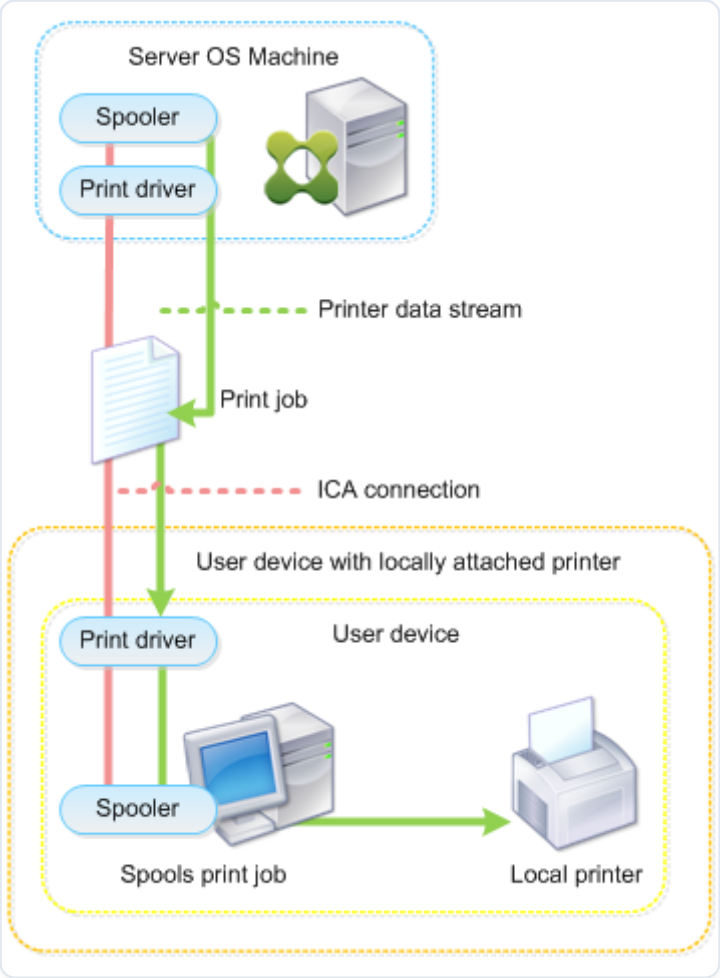
次の図は、Universal Print Driverのコンポーネントと、デバイスにローカル接続されたプリンターの一般的なワークフローを示しています。

Universal Print Driverのコンポーネントとワークフローの図(/en-us/citrix-virtual-apps-desktops/2311/media/cds-print-univ-printer-driver-flow.png)

ドライバー管理戦略を計画する際には、Universal Print Driver、デバイス固有のドライバー、またはその両方をサポートするかどうかを決定します。標準ドライバーをサポートする場合、以下を決定する必要があります。

プリンターの自動作成中に、システムがユーザーデバイスに接続された新しいローカルプリンターを検出した場合、必要なプリンタードライバーをMulti-session OSマシンで確認します。デフォルトでは、Windowsネイティブドライバーが利用できない場合、システムはUniversal Print Driverを使用します。

印刷を成功させるには、マルチセッションOSマシン上のプリンタードライバーとユーザーデバイス上のドライバーが一致している必要があります。以下の図は、クライアント印刷でプリンタードライバーが2か所でどのように使用されるかを示しています。



- サポートするドライバーの種類。
- マルチセッションOSマシンにプリンタードライバーがない場合に、自動的にインストールするかどうか。
- ドライバー互換性リストを作成するかどうか。

関連コンテンツ

- 印刷構成の例
- ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作
- 印刷ポリシーと設定
- プリンターのプロビジョニング
- 印刷環境の維持

印刷構成の例

ニーズと環境に最も適した印刷構成オプションを選択することで、管理を簡素化できます。デフォルトの印刷構成はほとんどの環境でユーザーが印刷できるようにしますが、そのデフォルト設定では、期待されるユーザーエクスペリエンスや、環境にとって最適なネットワーク使用量および管理オーバーヘッドが提供されない場合があります。

印刷構成は、以下によって異なります。

- ビジネスニーズと既存の印刷インフラストラクチャ。

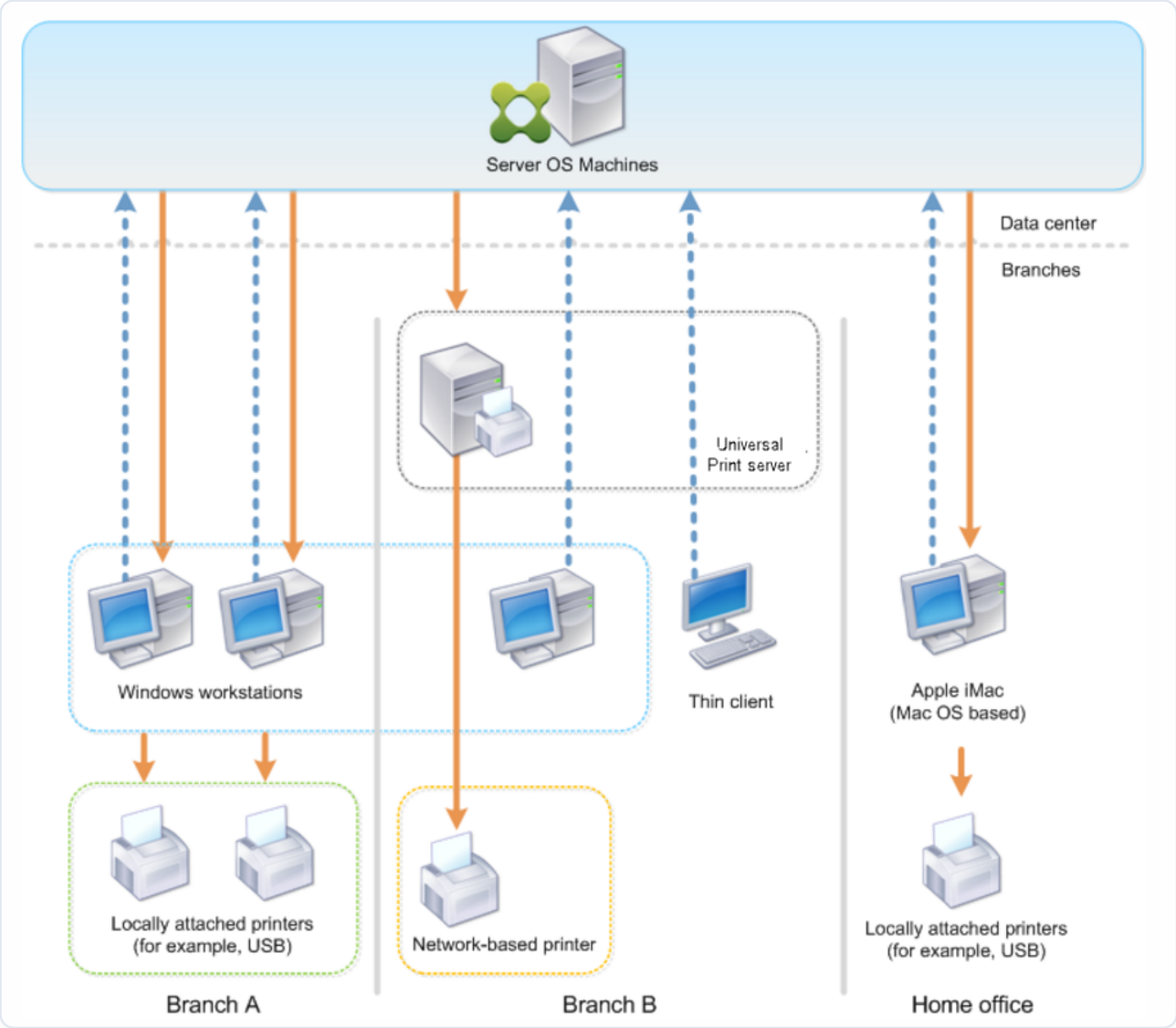
  組織のニーズに合わせて印刷構成を設計してください。既存の印刷実装（ユーザーがプリンターを追加できるかどうか、どのユーザーがどのプリンターにアクセスできるかなど）は、印刷構成を定義する際に役立つガイドとなる場合があります。
- 組織に、特定のユーザー（たとえば、人事部や給与計算用のプリンター）のためにプリンターを予約するセキュリティポリシーがあるかどうか。
- ユーザーが主要な作業場所から離れているときに印刷する必要があるかどうか（たとえば、ワークステーション間を移動する作業者や出張中の作業者など）。

印刷構成を設計する際には、ローカルユーザーデバイスから印刷する場合と同じエクスペリエンスをセッション内でユーザーに提供するように努めてください。

印刷展開の例

次の図は、これらのユースケースの印刷展開を示しています。

- **支店A** - 数台のWindowsワークステーションがある小規模な海外支店。各ユーザーワークステーションには、ローカルに接続されたプライベートプリンターがあります。
- **支店B** - シンクライアントとWindowsベースのワークステーションがある大規模な支店。効率を高めるため、この支店のユーザーはネットワークベースのプリンター（フロアごとに1台）を共有しています。支店内に設置されたWindowsベースのプリントサーバーが印刷キューを管理します。
- **ホームオフィス** - 会社のCitrix®インフラストラクチャにアクセスするMac OSベースのユーザーデバイスがあるホームオフィス。ユーザーデバイスにはローカルに接続されたプリンターがあります。



以下のセクションでは、環境の複雑さを最小限に抑え、管理を簡素化する構成について説明します。

自動作成されたクライアントプリンターとCitrix Universal™ プリンタードライバー

支店Aでは、すべてのユーザーがWindowsベースのワークステーションで作業するため、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーが使用されます。これらのテクノロジーは以下の利点を提供します。

- パフォーマンス - 印刷ジョブはICA®印刷チャネルを介して配信されるため、印刷データを圧縮して帯域幅を節約できます。

  大容量のドキュメントを印刷する単一のユーザーが他のユーザーのセッションパフォーマンスを低下させないように、Citrixポリシーが構成され、最大印刷帯域幅が指定されます。

代替ソリューションとして、マルチストリームICA接続を活用する方法があります。この接続では、印刷トラフィックが個別の低優先度TCP接続内で転送されます。マルチストリームICAは、WAN接続でQuality of Service (QoS) が実装されていない場合のオプションです。

- 柔軟性 - Citrix Universalプリンタードライバーを使用すると、データセンターに新しいプリンタードライバーを統合することなく、クライアントに接続されているすべてのプリンターを仮想デスクトップまたはアプリケーションセッションから使用できます。

Citrix ユニバーサル印刷サーバー

支店Bでは、すべてのプリンターがネットワークベースであり、そのキューはWindowsプリントサーバーで管理されているため、Citrix Universal Print Serverが最も効率的な構成となります。

必要なすべてのプリンタードライバーは、ローカル管理者によってプリントサーバーにインストールおよび管理されます。仮想デスクトップまたはアプリケーションセッションへのプリンターのマッピングは次のとおりです。

- Windowsベースのワークステーションの場合 - ローカルITチームは、ユーザーが適切なネットワークベースのプリンターをWindowsワークステーションに接続するのを支援します。これにより、ユーザーはローカルにインストールされたアプリケーションから印刷できるようになります。

  仮想デスクトップまたはアプリケーションセッション中、ローカルで構成されたプリンターは自動作成によって列挙されます。その後、仮想デスクトップまたはアプリケーションは、可能であれば直接ネットワーク接続としてプリントサーバーに接続します。

  Citrix Universal Print Serverコンポーネントがインストールされ、有効になっているため、ネイティブプリンタードライバーは不要です。ドライバーが更新されたり、プリンターキューが変更されたりしても、データセンターでの追加構成は不要です。
- シンクライアントの場合 - シンクライアントユーザーの場合、プリンターは仮想デスクトップまたはアプリケーションセッション内で接続されている必要があります。ユーザーに最もシンプルな印刷エクスペリエンスを提供するために、管理者はフロアごとに単一のCitrixセッションプリンターポリシーを構成し、そのフロアのプリンターをデフォルトプリンターとして接続します。

  ユーザーがフロア間を移動しても正しいプリンターが接続されるようにするため、ポリシーはサブネットまたはシンクライアントの名前に基づいてフィルター処理されます。この構成は近接印刷と呼ばれ、ローカルプリンタードライバーのメンテナンスを可能にします（委任された管理モデルに従って）。

プリンターキューを変更または追加する必要がある場合、Citrix管理者は環境内の該当するセッションプリンターポリシーを変更する必要があります。

ネットワーク印刷トラフィックはICA仮想チャネル外に送信されるため、QoSが実装されます。ICA/HDXトラフィックで使用されるポートのインバウンドおよびアウトバウンドネットワークトラフィックは、他のすべてのネットワークトラフィックよりも優先されます。この構成により、ユーザーセッションが大規模な印刷ジョブによって影響を受けることはありません。

自動作成されたクライアントプリンターとCitrixユニバーサルプリンタードライバー

ユーザーが標準外のワークステーションで作業し、管理されていない印刷デバイスを使用するホームオフィスの場合、最も簡単なアプローチは、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーを使用することです。

展開の概要

要約すると、サンプルの展開は次のように構成されています。

- マルチセッションOSマシンにはプリンタードライバーはインストールされていません。Citrixユニバーサルプリンタードライバーのみが使用されます。ネイティブ印刷へのフォールバックとプリンタードライバーの自動インストールは無効になっています。
- すべてのユーザーに対してすべてのクライアントプリンターを自動作成するようにポリシーが構成されています。マルチセッションOSマシンは、デフォルトで印刷サーバーに直接接続します。必要な構成は、ユニバーサルプリントサーバーコンポーネントを有効にすることだけです。
- 支店Bの各フロアにセッションプリンターポリシーが構成され、各フロアのすべてのシンクライアントに適用されます。
- 優れたユーザーエクスペリエンスを保証するために、支店BにはQoSが実装されています。

ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作

ベストプラクティス

特定の環境に最適な印刷ソリューションを決定する要因は多数あります。これらのベストプラクティスの一部は、お客様のサイトには適用されない場合があります。

- Citrix Universal™ Print Serverを使用します。

- ユニバーサルプリンタードライバーまたはWindowsネイティブドライバーを使用します。
- マルチセッションOSマシンにインストールされているプリンタードライバーの数を最小限に抑えます。
- ネイティブドライバーへのドライバーマッピングを使用します。
- テストされていないプリンタードライバーを本番サイトにインストールしないでください。
- ドライバーの更新は避けてください。常にドライバーをアンインストールし、プリントサーバーを再起動してから、交換用ドライバーをインストールするようにしてください。
- 使用されていないドライバーをアンインストールするか、プリンタードライバーマッピングおよび互換性ポリシーを使用して、そのドライバーでプリンターが作成されないようにします。
- バージョン2のカーネルモードドライバーの使用は避けてください。
- プリンターモデルがサポートされているかどうかを確認するには、製造元に問い合わせるか、www.citrix.com/readyにあるCitrix Ready製品ガイドを参照してください。

  一般に、Microsoftが提供するすべてのプリンタードライバーはTerminal Servicesでテストされており、Citrixで動作することが保証されています。ただし、サードパーティ製プリンタードライバーを使用する前に、Windows Hardware Quality Labs（WHQL）プログラムによってTerminal Services向けにドライバーが認定されていることをプリンタードライバーベンダーに確認してください。Citrixはプリンタードライバーを認定していません。

セキュリティに関する考慮事項

Citrixの印刷ソリューションは、設計上安全です。

- Citrix Print Manager Service は、ログオンとログオフ、切断、再接続、セッション終了などのセッションイベントを常に監視し、対応します。実際のセッションユーザーを偽装してサービス要求を処理します。
- Citrix印刷では、各プリンターにセッション内で一意の名前空間を割り当てます。
- Citrix印刷では、自動作成されたプリンターのデフォルトのセキュリティ記述子を設定し、あるセッションで自動作成されたクライアントプリンターが、他のセッションで実行されているユーザーからアクセスできないようにします。デフォルトでは、管理ユーザーは、他のセッションのクライアントプリンターの権限を表示したり手動で調整したりできる場合でも、誤ってそのプリンターに印刷することはできません。

デフォルトの印刷操作

デフォルトでは、ポリシー規則を構成しない場合、印刷動作は次のとおりです。

- ユニバーサルプリントサーバーは無効になっています。

- ユーザーデバイスで構成されているすべてのプリンターは、各セッションの開始時に自動的に作成されます。

  この動作は、Citrixポリシー設定「クライアントプリンターの自動作成」を「すべてのクライアントプリンターを自動作成」オプションで構成することと同じです。
- システムは、ユーザーデバイスにローカルに接続されたプリンターにキューイングされたすべての印刷ジョブを、クライアント印刷ジョブとして（つまり、ICA®チャネル経由でユーザーデバイスを介して）ルーティングします。
- システムは、ネットワークプリンターにキューイングされたすべての印刷ジョブを、Multi-session OSマシンから直接ルーティングします。システムがネットワーク経由でジョブをルーティングできない場合、ユーザーデバイスを介してリダイレクトされたクライアント印刷ジョブとしてルーティングします。

  この動作は、Citrixポリシー設定「プリントサーバーへの直接接続」を無効にすることと同じです。
- システムは、ユーザーの印刷設定と印刷デバイス固有の設定の組み合わせである印刷プロパティを、ユーザーデバイスに保存しようとします。クライアントがこの操作をサポートしていない場合、システムは印刷プロパティをマルチセッションOSマシンのユーザープロファイルに保存します。

  この動作は、Citrixポリシー設定「プリンタープロパティの保持」を「クライアントに保存されていない場合のみプロファイルに保持」オプションで構成することと同じです。
- VDAバージョン7.16以降では、V3インボックスプリンタードライバーがオペレーティングシステムに含まれていないため、Citrixポリシー設定「インボックスプリンタードライバーの自動インストール」はWindows 8以降のWindowsオペレーティングシステムバージョンには影響しません。
- VDA 7.16より前のバージョンでは、マルチセッションOSマシンで利用可能な場合、システムはプリンタードライバーのWindowsバージョンを使用します。プリンタードライバーが利用できない場合、システムはWindowsオペレーティングシステムからドライバーをインストールしようとします。Windowsでドライバーが利用できない場合、Citrixユニバーサルプリントドライバーを使用します。

  この動作は、Citrixポリシー設定の「インボックスプリンタードライバーの自動インストール」を有効にし、ユニバーサル印刷設定を「要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する」で構成することと同等です。

  「インボックスプリンタードライバーの自動インストール」を有効にすると、多数のネイティブプリンタードライバーがインストールされる可能性があります。

注:

印刷の出荷時デフォルト設定が不明な場合は、新しいポリシーを作成し、すべての印刷ポリシー規則を「有効」に設定して表示します。表示されるオプションがデフォルトです。

常時オンロギング

VDA上のプリントサーバーおよび印刷サブシステムで、常時オンロギング機能が利用可能です。

ログをZIP形式でまとめてメール送信したり、Citrix Insight Servicesに自動的にアップロードしたりするには、**Start-TelemetryUpload** PowerShellコマンドレットを使用します。

印刷ポリシーと設定

ユーザーが公開アプリケーションからプリンターにアクセスする場合、Citrix®ポリシーを構成して、以下を指定できます。

- プリンターがプロビジョニングされる方法（またはセッションに追加される方法）
- 印刷ジョブがルーティングされる方法
- プリンタードライバーが管理される方法

ユーザーデバイス、ユーザー、またはポリシーがフィルターされるその他のオブジェクトごとに異なる印刷構成を設定できます。

ほとんどの印刷機能は、Citrixの印刷ポリシー設定を通じて構成されます。印刷設定は、標準のCitrixポリシーの動作に従います。

ユーザーのネットワークアカウントに十分な権限がある場合、システムはセッションの終了時にプリンター設定をプリンターオブジェクトに書き込むか、クライアント印刷デバイスに書き込むことができます。デフォルトでは、Citrix Workspace™アプリは、他の場所で設定や環境設定を探す前に、セッション内のプリンターオブジェクトに保存されている設定を使用します。

デフォルトでは、システムはプリンターのプロパティをユーザーデバイス上（デバイスがサポートしている場合）またはMulti-session OSマシンのユーザープロファイルに保存または保持します。ユーザーがセッション中にプリンターのプロパティを変更すると、それらの変更はマシンのユーザープロファイルに更新されます。ユーザーが次回ログオンまたは再接続するときに、ユーザーデバイスは保持されているそれらの設定を継承します。つまり、ユーザーデバイスでのプリンタープロパティの変更は、ユーザーがログオフして再度ログオンするまで、現在のセッションには影響しません。

印刷設定の場所

Windowsの印刷環境では、印刷設定への変更はローカルコンピューターまたはドキュメントに保存できます。この環境では、ユーザーが印刷設定を変更すると、設定は次の場所に保存されます。

- **ユーザーデバイス自体** - Windowsユーザーは、コントロールパネルでプリンターを右クリックし、を選択することで、ユーザーデバイス上のデバイス設定を変更できます。たとえば、ページ方向として「横」が選択されている場合、「横」はそのプリンターのデフォルトのページ方向設定として保存されます。
- **ドキュメント内** - ワープロプログラムやデスクトップパブリッシングプログラムでは、ページ方向などのドキュメント設定は、多くの場合ドキュメント内に保存されます。たとえば、ドキュメントを印刷キューに入れると、Microsoft Wordは通常、指定した印刷設定（ページ方向やプリンター名など）をドキュメント内に保存します。これらの設定は、次回そのドキュメントを印刷するときにデフォルトで表示されます。
- **ユーザーがセッション中に行った変更から** - システムは、自動作成されたプリンターの印刷設定に対する変更がセッション内のコントロールパネルで行われた場合、つまりMulti-session OSマシンで行われた場合にのみ、その変更を保持します。
- **Multi-session OSマシン上** - これらは、マシン上の特定のプリンタードライバーに関連付けられているデフォルト設定です。

Windowsベースの環境で保持される設定は、ユーザーが変更を行った場所によって異なります。これは、スプレッドシートプログラムなどのある場所に表示される印刷設定が、ドキュメントなどの他の場所の印刷設定とは異なる場合があることも意味します。その結果、特定のプリンターに適用される印刷設定は、セッション中に変更される可能性があります。

ユーザーの印刷設定の階層

印刷設定は複数の場所に保存できるため、システムは特定の優先順位に従ってそれらを処理します。また、デバイス設定はドキュメント設定とは明確に区別され、通常はドキュメント設定よりも優先されることに注意することが重要です。

デフォルトでは、システムは常に、ユーザーがセッション中に変更した印刷設定（つまり、保持された設定）を、他の設定を考慮する前に適用します。ユーザーが印刷すると、システムはMulti-session OSマシンに保存されているデフォルトのプリンター設定と、保持されているクライアントプリンター設定を結合して適用します。

ユーザーの印刷設定の保存

Citrixは、プリンタープロパティの保存場所を変更しないことを推奨します。ユーザーデバイスにプリンタープロパティを保存するデフォルト設定は、一貫した印刷プロパティを確保する最も簡単な方法です。システムがユーザーデバイスにプロパティを保存できない場合、Multi-session OSマシンのユーザープロファイルに自動的にフォールバックします。

次のシナリオが適用される場合は、プリンタープロパティ保持ポリシー設定を確認してください。

- ユーザーがユーザーデバイスにプリンタープロパティを保存することを許可しないレガシープラグインを使用している場合。
- Windowsネットワークで強制プロファイルを使用しており、ユーザーのプリンタープロパティを保持したい場合。

プリンターのプロビジョニング

シトリックス ユニバーサル™ プリントサーバー

環境に最適な印刷ソリューションを決定する際には、次の点を考慮してください。

- Universal Print Serverは、Windows Print Providerでは利用できない機能（画像とフォントのキャッシュ、高度な圧縮、最適化、QoSサポート）を提供します。
- Universal Print Driverは、Microsoftによって定義されたパブリックなデバイス非依存設定をサポートします。ユーザーが特定のプリンタードライバーメーカーに固有のデバイス設定にアクセスする必要がある場合、Universal Print ServerとWindowsネイティブドライバーを組み合わせるのが最適なソリューションとなる可能性があります。この構成により、Universal Print Serverの利点を維持しつつ、ユーザーに特殊なプリンター機能へのアクセスを提供できます。考慮すべきトレードオフとして、Windowsネイティブドライバーにはメンテナンスが必要です。
- Citrix Universal Print Serverは、ネットワークプリンターに対するユニバーサル印刷サポートを提供します。Universal Print Serverは、Multi-session OSマシン上の単一ドライバーであるUniversal Print Driverを使用し、シンクライアントやタブレットを含むあらゆるデバイスからのローカルまたはネットワーク印刷を可能にします。

Universal Print ServerをWindowsネイティブドライバーとともに使用するには、Universal Print Serverを有効にします。デフォルトでは、Windowsネイティブドライバーが利用可能な場合はそれが使用されます。そうでない場合は、Universal Print Driverが使用されます。Windowsネイティブドライバーのみを使用するか、Universal Print Driverのみを使用するかなど、この動作の変更を指定するには、Universal Print Driverの使用ポリシー設定を更新します。

Universal Print Serverのインストール

Universal Print Serverを使用するには、インストールドキュメントに記載されているとおり、プリントサーバーにUpsServerコンポーネントをインストールして構成します。詳細については、「コアコンポーネントのインストール」および「コマンドラインを使用したインストール」を参照してください。

UPClientコンポーネントを個別に展開したい環境（例: **XenApp 6.5**を使用する場合）の場合：

1. Windows Single-session OSまたはWindows Multi-session OS用のCitrix Virtual Apps and Desktops™ Virtual Delivery Agent (VDA) スタンドアロンパッケージをダウンロードします。
2. 「コマンドラインを使用したインストール」に記載されているコマンドラインの指示に従ってVDAを抽出します。
3. \\Image-Full\\Support\\VcRedist_2013_RTM から前提条件をインストールします。
    - Vcredist_x64 / vcredist_x86
        - 32ビットのみの場合はx86を実行し、64ビット展開の場合は両方を実行します。
4. \\Image-Full\\x64\\Virtual Desktop Components または \\Image-Full\\x86\\Virtual Desktop Components から cdf の前提条件をインストールします。
    - Cdf_x64 / Cdf_x86
        - x86 は 32 ビット用、x64 は 64 ビット用
5. \\Image-Full\\x64\\Virtual Desktop Components または \\Image-Full\\x86\\Virtual Desktop Components で UPClient コンポーネントを見つけます。
6. UPClient コンポーネントを抽出し、コンポーネントの MSI を起動してインストールします。
7. UPClient コンポーネントのインストール後、再起動が必要です。

ユニバーサルプリントサーバーのCEIPをオプトアウトする

ユニバーサルプリントサーバーをインストールすると、Citrix Customer Experience Improvement Program (CEIP) に自動的に登録されます。最初のデータアップロードは、インストール日時から7日後に実行されます。

CEIPをオプトアウトするには、レジストリキー `HKLM\Software\Citrix\Universal Print Server\CEIPEnabled` を編集し、**DWORD** 値を **0** に設定します。

再度オプトインするには、DWORD値を1に設定します。

注意: レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターの使用は自己責任で行ってください。編集する前に必ずレジストリをバックアップしてください。

詳細については、「Citrix Insight Services」を参照してください。

ユニバーサルプリントサーバーの構成

以下の Citrix ポリシー設定を使用して、Universal Print Server を構成します。詳細については、画面上のポリシー設定ヘルプを参照してください。

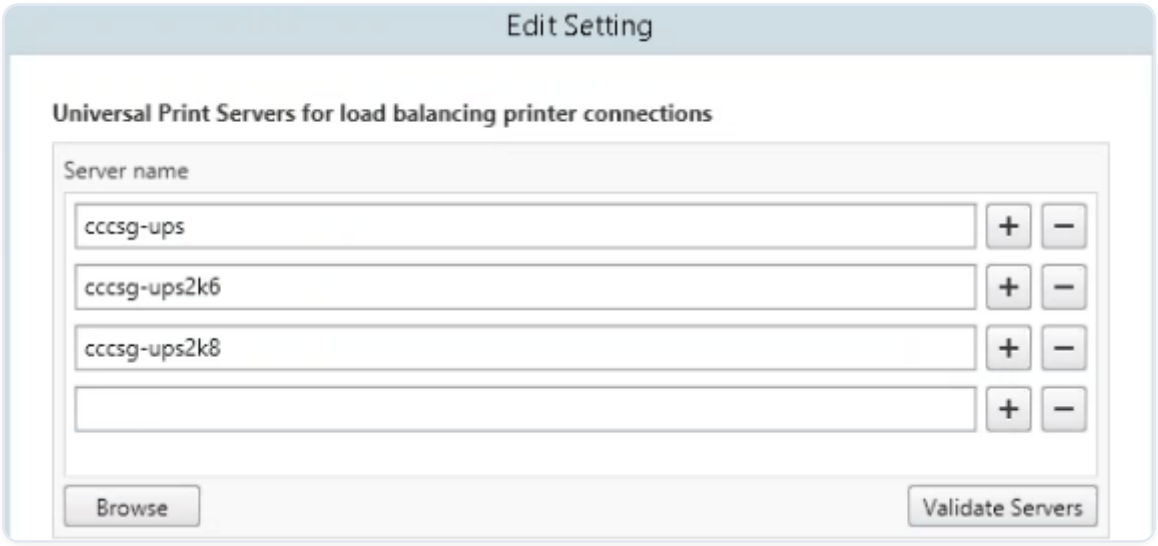
- **Universal Print Server enable**. Universal Print Server is disabled by default. When you enable Universal Print Server, you choose whether to use the Windows Print Provider if the Universal Print Server is unavailable. After you enable the Universal Print Server, a user can add and enumerate network printers through the Windows Print Provider and Citrix Provider interfaces.
- **Universal Print Server印刷データストリーム (CGP) ポート**。Universal Print Server印刷データストリームCGP (Common Gateway Protocol) リスナーが使用するTCPポート番号を指定します。デフォルトは**7229**です。
- **ユニバーサルプリントサーバーWebサービス (HTTP/SOAP) ポート**。ユニバーサルプリントサーバーリスナーが受信HTTP/SOAP要求に使用するTCPポート番号を指定します。デフォルトは**8080**です。

Citrix Virtual Apps and Desktops VDAへのUniversal Print Server通信のデフォルトポートであるHTTP 8080を変更するには、Universal Print Serverコンピューターで以下のレジストリを作成し、ポート番号の値を変更する必要があります。

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies`
"UpsHttpPort"=DWORD:\<portnumber\>

このポート番号は、StudioのHDXポリシー、Universal Print Server Webサービス (HTTP/SOAP) ポートと一致している必要があります。

- **Universal Print Server印刷ストリーム入力帯域幅制限 (kbps)**。CGPを使用して各印刷ジョブからUniversal Print Serverに配信される印刷データの転送速度の上限 (キロビット/秒) を指定します。デフォルトは0 (無制限) です。
- **負荷分散のためのUniversal Print Server**。この設定は、他のCitrix印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用されるUniversal Print Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべての印刷サーバーが同じ共有プリンターセットを持つことを推奨します。



- **Universal Print Serverサービス停止しきい値**。負荷分散機能が、利用できない印刷サーバーが回復するまで待機する時間を指定します。この時間を過ぎると、サーバーが恒久的にオフラインであると判断され、その負荷が他の利用可能な印刷サーバーに再分散されます。デフォルトは180 (秒) です。

Delivery Controller™で印刷ポリシーが変更されると、ポリシーの変更がVDAに適用されるまでに数分かかる場合があります。

他のポリシー設定との相互作用 - Universal Print Serverは、他のCitrix印刷ポリシー設定を尊重し、以下の表に示すようにそれらと相互作用します。提供される情報は、Universal Print Serverポリシー設定が有効になっており、Universal Print Serverコンポーネントがインストールされ、ポリシー設定が適用されていることを前提としています。

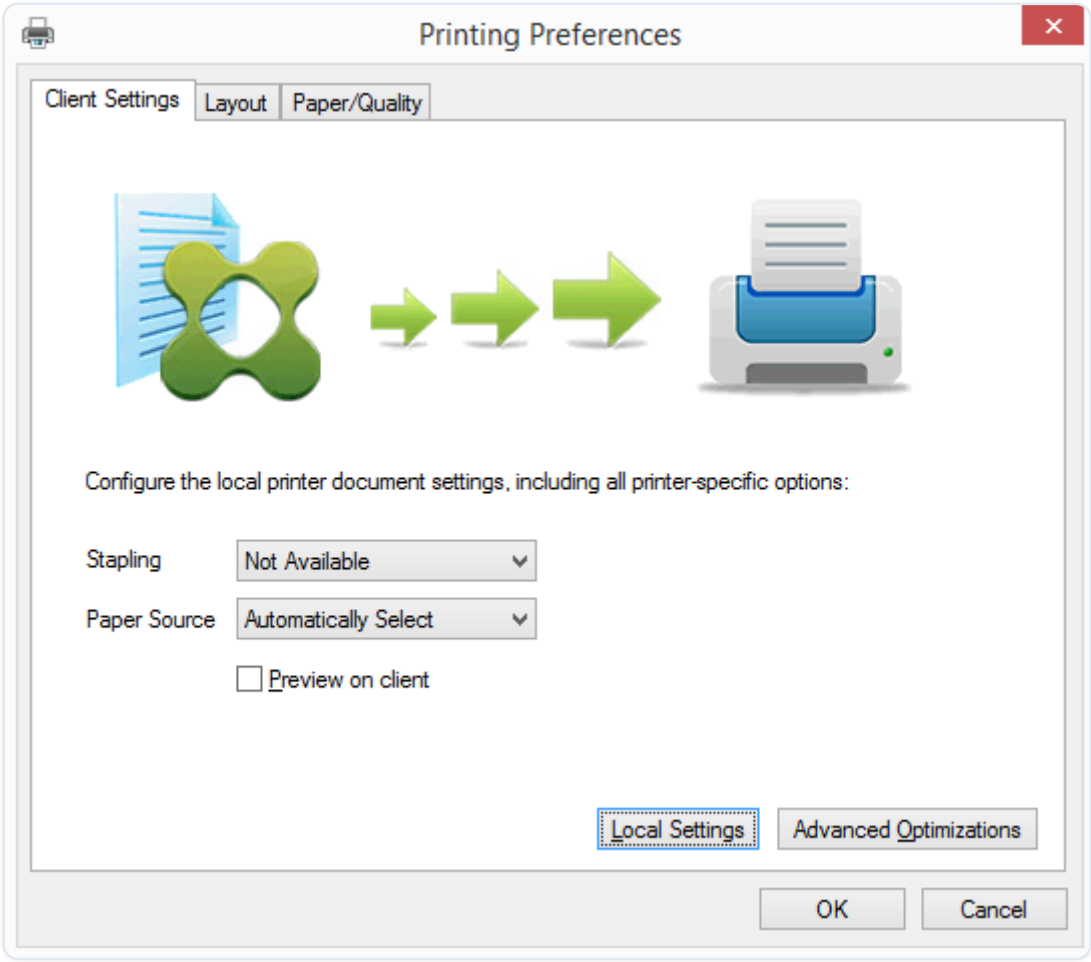
ポリシー設定	相互作用
クライアントプリンターリダイレクト、クライアントプリンターの自動作成	Universal Print Serverが有効になると、クライアントネットワークプリンターはネイティブドライバーではなくUniversal print driverを使用して作成されます。ユーザーには以前と同じプリンター名が表示されます。
セッションプリンター	Citrix Universal Print Serverソリューションを使用する場合、ユニバーサルプリントドライバーのポリシー設定が適用されます。
プリントサーバーへの直接接続	Universal Print Serverが有効で、ユニバーサルプリントドライバーの使用ポリシー設定がユニバーサル印刷のみを使用するように構成されている場合、ユニバーサルプリントドライ

	バーを使用して、プリントサーバーへの直接ネットワークプリンター接続を作成できます。
UPDの優先設定	EMFおよびXPSドライバーをサポートします。

ユーザーインターフェイスへの影響 - Universal Print Serverで使用されるCitrix Universal Print Driverは、以下のユーザーインターフェイスコントロールを無効にします。

- プリンターのプロパティダイアログボックスのボタン
- ドキュメントのプロパティダイアログボックスのボタンとボタン

Citrix Universal Print Driver（EMFおよびXPSドライバー）は、ステープルや給紙元などの高度な印刷機能をサポートしています。セッション内でUPDにマップされているクライアントプリンターまたはネットワークプリンターがこれらの機能をサポートしている場合、ユーザーはカスタムUPD印刷ダイアログからまたはオプションを選択できます。



ステープルやセキュアPINなどの非標準のプリンター設定を行うには、Citrix UPD EMFまたはXPSドライバーを使用するクライアントマッププリンターのカスタムUPD印刷ダイアログで**を選択します。マップされたプリンターの**ダイアログがセッション外のクライアントに表示され、ユー

ザーは任意のプリンターオプションを変更できます。変更されたプリンター設定は、そのドキュメントを印刷する際にアクティブなセッションで使用されます。

これらの機能は、ネイティブドライバーがMicrosoft Print Capabilityテクノロジーを使用して利用可能にしている場合に利用できます。ネイティブドライバーは、Print Capabilities XMLで標準化されたPrint Schema Keywordsを使用する必要があります。非標準のキーワードが使用されている場合、Citrix Universal Print Driverを使用しても高度な印刷機能は利用できません。

Universal Print Serverを使用する場合、Citrix Print Providerのプリンターの追加ウィザードは、Windows Print Providerのプリンターの追加ウィザードと同じですが、以下の例外があります。

- 名前またはアドレスでプリンターを追加する場合、プリントサーバーのHTTP/SOAPポート番号を指定できます。そのポート番号はプリンター名の一部となり、表示されます。
- Citrix Universal Print Driver使用ポリシー設定でユニバーサル印刷を使用する必要がある場合、プリンターを選択する際にユニバーサルプリントドライバー名が表示されます。Windows Print Providerはユニバーサルプリントドライバーを使用できません。

Citrix Print Providerはクライアント側レンダリングをサポートしていません。

Universal Print Serverについて詳しくは、CTX200328を参照してください。

自動作成されたクライアントプリンター

クライアントプリンターには、次のユニバーサル印刷ソリューションが提供されます。

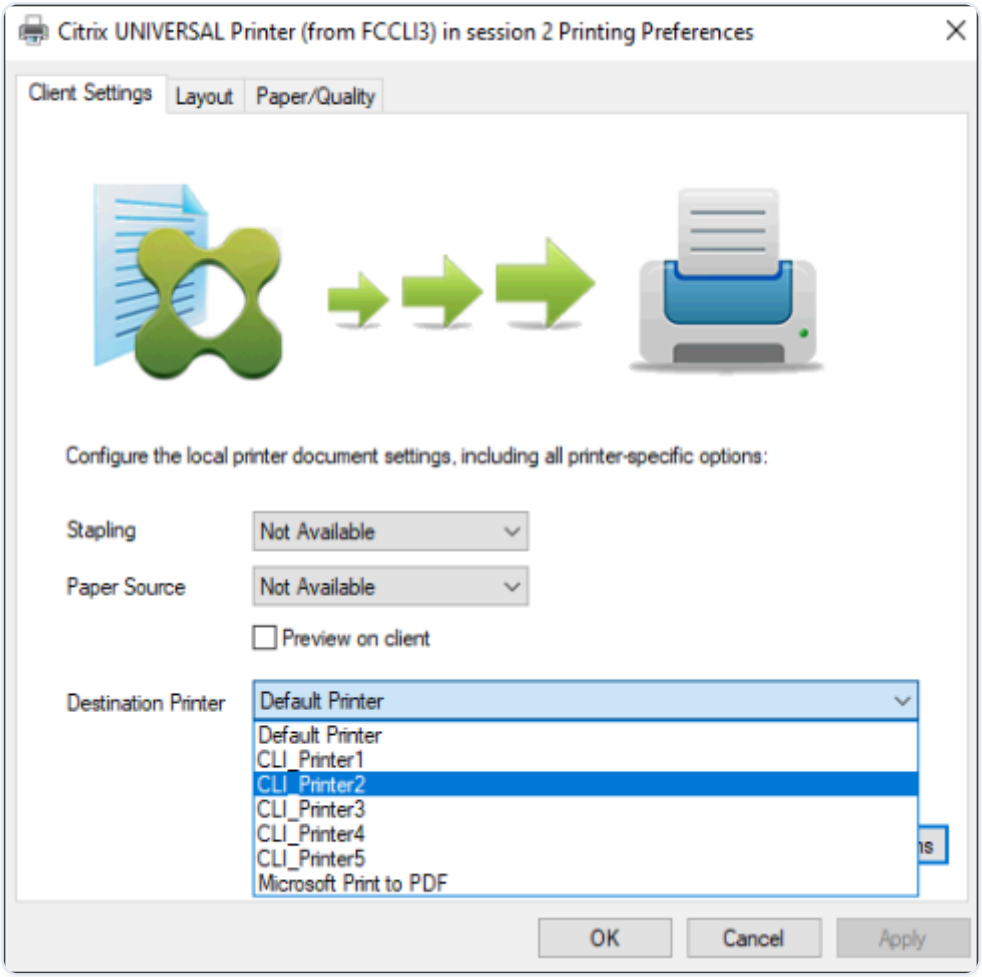
- **Citrix Universal Printer** - セッションの開始時に作成される汎用プリンターで、印刷デバイスに接続されていません。Citrix Universal Printerのみを自動作成して使用すると、リソース使用量とユーザーサインイン時間が短縮される場合があります。Universal Printerは、任意のクライアント側印刷デバイスに印刷できます。

  Citrix Universal Printerは、お使いの環境のすべてのユーザーデバイスまたはCitrix Workspace™アプリで動作しない場合があります。Citrix Universal PrinterにはWindows環境が必要であり、Citrix Offline Plug-inやクライアントにストリーミングされるアプリケーションはサポートしていません。このような環境では、自動作成されたクライアントプリンターとUniversal Print Driverの使用を検討してください。

  Windows以外のCitrix Workspaceアプリでユニバーサル印刷ソリューションを使用するには、PostscriptまたはPCLベースの他のUniversal Print Driverのいずれかを使用します。

  Citrix Universal Printerを使用すると、クライアントのデフォルトプリンターまたは特定のクライアントプリンターを印刷先として選択できます。印刷ジョブの特定のプリンターを選択するには、**［印刷設定］**ダイアログボックスを開きます。**［宛先プリンター］**ドロップダウンを

選択します。［デフォルトプリンター］**オプションは、印刷ジョブをクライアントのデフォルトプリンターに送信します。セッションを実行しているエンドポイントに接続されているクライアントリダイレクトプリンターもすべて一覧表示されます。選択したプリンターは、今後の印刷ジョブの宛先プリンターとして保存されます。



- **Citrix Universal Print Driver** - デバイスに依存しないプリンタードライバーです。Citrix Universal Print Driverを構成すると、システムはデフォルトでEMFベースのUniversal Print Driverを使用します。

  Citrix Universal Print Driverは、古いまたは高度でないプリンタードライバーよりも小さい印刷ジョブを作成する可能性があります。ただし、特殊なプリンターの印刷ジョブを最適化するには、デバイス固有のドライバーが必要になる場合があります。

ユニバーサル印刷の構成 - ユニバーサル印刷を構成するには、次のCitrixポリシー設定を使用します。詳しくは、画面上のポリシー設定ヘルプを参照してください。

- Universal Print Driverの使用。ユニバーサル印刷を使用するタイミングを指定します。
- 汎用Universal Printerの自動作成。Universal Printingと互換性のあるユーザーデバイスが使用されているセッションで、汎用Citrix Universal Printerオブジェクトの自動作成を有効または無効にします。デフォルトでは、汎用Universal Printerオブジェクトは自動作成されません。

- ユニバーサルドライバーの優先順位。システムがユニバーサルプリントドライバーを使用しようとする順序を、リストの最初のエントリから指定します。ドライバーの追加、編集、削除、およびリスト内のドライバーの順序変更が可能です。
- ユニバーサル印刷プレビューの優先順位。自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して、印刷プレビュー機能を使用するかどうかを指定します。
- ユニバーサル印刷EMF処理モード。Windowsユーザーデバイス上のEMFスプールファイルの処理方法を制御します。デフォルトでは、EMFレコードはプリンターに直接スプールされます。プリンターに直接スプールすることで、スプーラーはレコードをより速く処理し、CPUリソースの使用量を削減できます。

その他のポリシーについては、印刷パフォーマンスの最適化を参照してください。用紙サイズ、印刷品質、色、両面印刷、部数などの設定のデフォルトを変更するには、CTX113148を参照してください。

ユーザーデバイスからのプリンターの自動作成 - セッションの開始時に、システムはデフォルトでユーザーデバイス上のすべてのプリンターを自動作成します。ユーザーにプロビジョニングされるプリンターの種類を制御したり、自動作成を防止したりできます。

Citrixポリシー設定の クライアントプリンターの自動作成を使用して自動作成を制御します。以下を指定できます。

- ネットワークプリンターおよびローカル接続プリンターを含む、ユーザーデバイスに表示されるすべてのプリンターが、各セッションの開始時に自動的に作成されます（デフォルト）。
- ユーザーデバイスに物理的に接続されているすべてのローカルプリンターが自動的に作成されます。
- ユーザーデバイスのデフォルトプリンターのみが自動的に作成されます。
- すべてのクライアントプリンターで自動作成が無効になります。

「クライアントプリンターの自動作成」設定では、「クライアントプリンターのリダイレクト」設定が「許可」（デフォルト）である必要があります。

ユーザーへのネットワークプリンターの割り当て

デフォルトでは、ユーザーデバイス上のネットワークプリンターはセッションの開始時に自動的に作成されます。システムは、各セッション内で作成するネットワークプリンターを指定することで、列挙およびマップされるネットワークプリンターの数を減らすことができます。このようなプリンターはセッションプリンターと呼ばれます。

IPアドレスでセッションプリンターポリシーをフィルタリングして、近接印刷を提供できます。近接印刷により、指定されたIPアドレス範囲内のユーザーは、同じ範囲内に存在するネットワーク印刷デバイスに自動的にアクセスできます。近接印刷はCitrix Universal Print Serverによって提供され、このセクションで説明されている構成は必要ありません。

近接印刷には、次のシナリオが含まれる場合があります。

- 会社の内部ネットワークは、ユーザーにIPアドレスを自動的に割り当てるDHCPサーバーで運用されています。
- 社内のすべての部署には、一意に割り当てられたIPアドレス範囲があります。
- ネットワークプリンターは、各部署のIPアドレス範囲内に存在します。

近接印刷が構成されており、従業員がある部署から別の部署に移動した場合、追加の印刷デバイス構成は必要ありません。ユーザーデバイスが新しい部署のIPアドレス範囲内で認識されると、その範囲内のすべてのネットワークプリンターにアクセスできるようになります。

セッションでリダイレクトされる特定のプリンターを構成する - 管理者によって割り当てられたプリンターを作成するには、Citrixポリシー設定のSession printersを構成します。次のいずれかの方法を使用して、そのポリシーにネットワークプリンターを追加します。

- プリンターのUNCパスを「\\servername\\printername」の形式で入力します。
- ネットワーク上のプリンターの場所を参照します。
- 特定のサーバー上のプリンターを参照します。「\\servername」の形式でサーバー名を入力し、「参照」をクリックします。

重要: サーバーは、適用されているすべてのポリシーの有効なセッションプリンター設定を、最も高い優先度から最も低い優先度までマージします。プリンターが複数のポリシーオブジェクトで構成されている場合、カスタムのデフォルト設定は、そのプリンターが構成されている最も優先度の高いポリシーオブジェクトからのみ取得されます。

Session printers設定で作成されたネットワークプリンターは、サブネットなどのオブジェクトでフィルタリングすることにより、セッションが開始された場所に応じて異なる場合があります。

セッションのデフォルトネットワークプリンターを指定する - デフォルトでは、ユーザーのメインプリンターがセッションのデフォルトプリンターとして使用されます。Citrixポリシー設定のDefault printerを使用して、セッションでユーザーデバイスのデフォルトプリンターがどのように確立されるかを変更します。

1. 「デフォルトプリンター設定」ページで、「クライアントのデフォルトプリンターを選択」の設定を選択します。

- ネットワークプリンター名。Session printersポリシー設定で追加されたプリンターがこのメニューに表示されます。このポリシーのデフォルトとして使用するネットワークプリンターを選択します。
- ユーザーのデフォルトプリンターを調整しない。デフォルトプリンターには、現在のターミナルサービスまたはWindowsユーザープロファイル設定を使用します。詳細については、画面上のポリシー設定ヘルプを参照してください。

2. 影響を与えたいユーザーグループ（またはその他のフィルターされたオブジェクト）にポリシーを適用します。

近接印刷の構成 - 近接印刷はCitrix Universal Print Serverによっても提供されており、ここで説明する構成は必要ありません。

1. 各サブネットに対して個別のポリシーを作成します（またはプリンターの場所に合わせます）。
2. 各ポリシーで、そのサブネットの地理的な場所にあるプリンターをセッションプリンター設定に追加します。
3. デフォルトプリンター設定を「ユーザーのデフォルトプリンターを調整しない」に設定します。
4. クライアントIPアドレスでポリシーをフィルターします。DHCP IPアドレス範囲の変更を反映するように、これらのポリシーを必ず更新してください。

印刷環境の維持

印刷環境の維持には、次のものが含まれます。

- プリンタードライバーの管理
- 印刷パフォーマンスの最適化
- プリンターの表示と印刷キューの管理

プリンタードライバーの管理

管理オーバーヘッドとプリンタードライバーの問題の可能性を最小限に抑えるため、Citrixでは Citrix Universal™プリンタードライバーの使用を推奨しています。

自動作成が失敗した場合、デフォルトでは、Windowsに付属のWindowsネイティブプリンタードライバーがシステムにインストールされます。ドライバーが利用できない場合、システムはユニバーサルプリントドライバーにフォールバックします。プリンタードライバーのデフォルトにつ

いて詳しくは、「ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作」を参照してください。

Citrix Universalプリンタードライバーがすべてのシナリオでオプションではない場合、マルチセッションOSマシンにインストールされるドライバーの数を最小限に抑えるためにプリンタードライバーをマップします。さらに、プリンタードライバーをマップすると、次のことが可能になります。

- 指定されたプリンターでCitrix Universalプリンタードライバーのみを使用できるようにする
- 指定されたドライバーでプリンターを作成することを許可または禁止する
- 古くなったドライバーや破損したドライバーを適切なプリンタードライバーに置き換える
- クライアントドライバー名に対して、Windowsサーバーで利用可能なドライバーを置き換える

プリンタードライバーの自動インストールを防止する - マルチセッションOSマシン全体で一貫性を確保するために、プリンタードライバーの自動インストールを無効にする必要があります。これは、Citrix®ポリシー、Microsoftポリシー、またはその両方を通じて実現できます。Windowsネイティブプリンタードライバーの自動インストールを防止するには、Citrixポリシー設定の「Automatic installation of in-box printer drivers」を無効にします。

クライアントプリンタードライバーをマップする - 各クライアントは、ログオン時にクライアント側プリンターに関する情報（プリンタードライバー名を含む）を提供します。クライアントプリンターの自動作成中に、クライアントから提供されたプリンターモデル名に対応するWindowsサーバープリンタードライバー名が選択されます。その後、自動作成プロセスは、識別された利用可能なプリンタードライバーを使用して、リダイレクトされたクライアント印刷キューを構築します。

マップされたクライアントプリンタードライバーのドライバー置換ルールを定義し、印刷設定を編集するための一般的なプロセスは次のとおりです。

1. 自動作成されたクライアントプリンターのドライバー置換ルールを指定するには、Citrixポリシー設定の「プリンタードライバーマッピングと互換性」を構成し、クライアントプリンタードライバー名を追加して、「プリンタードライバーの検索」メニューからクライアントプリンタードライバーの代わりに置換するサーバードライバーを選択します。この設定ではワイルドカードを使用できます。たとえば、すべてのHPプリンターに特定のドライバーを使用させるには、ポリシー設定で「HP*」と指定します。
2. プリンタードライバーを禁止するには、ドライバー名を選択し、「作成しない」設定を選択します。
3. 必要に応じて、既存のマッピングを編集したり、マッピングを削除したり、リスト内のドライバーエントリの順序を変更したりします。

4. マップされたクライアントプリンタードライバーの印刷設定を編集するには、プリンタードライバーを選択し、「設定」をクリックして、印刷品質、向き、色などの設定を指定します。プリンタードライバーがサポートしない印刷オプションを指定した場合、そのオプションは無効になります。この設定は、ユーザーが以前のセッションで設定した保持されているプリンター設定を上書きします。
5. 特定のドライバーでのみ利用可能なプリンター機能があるため、Citrixではドライバーをマッピングした後、プリンターの動作を詳細にテストすることをお勧めします。

ユーザーがログオンすると、システムはクライアントプリンターを設定する前に、クライアントプリンタードライバーの互換性リストをチェックします。

印刷パフォーマンスの最適化

印刷パフォーマンスを最適化するには、ユニバーサルプリントサーバーとユニバーサルプリントドライバーを使用します。以下のポリシーは、印刷の最適化と圧縮を制御します。

- ユニバーサル印刷の最適化のデフォルト。セッション用にユニバーサルプリンターが作成される際のデフォルト設定を指定します。
    - 目的の画質は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、「標準品質」が有効になっており、ユーザーは標準または低品質の圧縮を使用してのみ画像を印刷できることを意味します。
    - ヘビーウェイト圧縮を有効にするは、画質を損なうことなく、目的の画質で設定された圧縮レベルを超えて帯域幅を削減することを有効または無効にします。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
    - 画像とフォントのキャッシュ設定は、印刷ストリームに複数回出現する画像とフォントをキャッシュするかどうかを指定し、各固有の画像またはフォントがプリンターに一度だけ送信されるようにします。デフォルトでは、埋め込み画像とフォントはキャッシュされます。
    - 非管理者によるこれらの設定の変更を許可するは、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。
- ユニバーサル印刷の画像圧縮制限。ユニバーサルプリントドライバーで印刷される画像の最大品質と最小圧縮レベルを定義します。デフォルトでは、画像圧縮制限は「最高品質（ロスレス圧縮）」に設定されています。
- ユニバーサル印刷の印刷品質制限。セッションで印刷出力を生成するために利用できる最大ドット/インチ (dpi) を指定します。デフォルトでは、制限は指定されていません。

デフォルトでは、ネットワークプリンター宛てのすべての印刷ジョブは、マルチセッションOSマシンからネットワーク経由で直接印刷サーバーにルーティングされます。ネットワークにかなりの遅延や帯域幅の制限がある場合は、ICA®接続経由で印刷ジョブをルーティングすることを検討してください。そのためには、Citrixポリシー設定「印刷サーバーへの直接接続」を無効にします。ICA接続経由で送信されるデータは圧縮されるため、WANを介してデータが転送される際の帯域幅の消費が少なくなります。

印刷帯域幅を制限してセッションパフォーマンスを向上させる - マルチセッションOSマシンからユーザープリンターにファイルを印刷している間、特にユーザーが低速なネットワーク経由でサーバーにアクセスしている場合、帯域幅の競合により、他の仮想チャネル（ビデオなど）のパフォーマンスが低下する可能性があります。このような劣化を防ぐために、ユーザー印刷で使用される帯域幅を制限できます。印刷のデータ転送速度を制限することで、HDX™データストリームでビデオ、キーストローク、マウスデータの転送により多くの帯域幅を利用できるようになります。

> **重要:**
>
> プリンターの帯域幅制限は、他のチャネルが使用されていない場合でも常に適用されます。

以下のCitrixポリシーの帯域幅プリンター設定を使用して、印刷帯域幅のセッション制限を構成します。サイトの制限を設定するには、Studioを使用してこのタスクを実行します。個々のサーバーの制限を設定するには、各マルチセッションOSマシンでローカルにWindowsのグループポリシー管理コンソールを使用してこのタスクを実行します。

- 「プリンターリダイレクト帯域幅制限」設定は、印刷に利用できる帯域幅をキロビット/秒 (kbps) で指定します。
- 「プリンターリダイレクト帯域幅制限（パーセント）」設定は、印刷に利用できる帯域幅を、利用可能な全体帯域幅のパーセンテージに制限します。

  注：プリンターリダイレクト帯域幅制限（パーセント）設定を使用して帯域幅をパーセンテージで指定するには、「セッション全体の帯域幅制限」も有効にする必要があります。

  両方の設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

印刷帯域幅に関するリアルタイム情報を取得するには、Citrix Directorを使用します。

ユニバーサルプリントサーバーの負荷分散

ユニバーサルプリントサーバーソリューションは、負荷分散ソリューションにさらに多くの印刷サーバーを追加することで拡張できます。各VDAには、すべての印刷サーバーに印刷負荷を分散するための独自のロードバランサーがあるため、単一障害点はありません。

負荷分散ソリューション内のすべての印刷サーバーに印刷負荷を分散するには、ポリシー設定「負荷分散用ユニバーサルプリントサーバー」と「ユニバーサルプリントサーバーのサービス停止しきい値」を使用します。

プリントサーバーに予期せぬ障害が発生した場合、各VDAのロードバランサーのフェイルオーバーメカニズムは、障害が発生したプリントサーバーに割り当てられていたプリンター接続を、他の利用可能なプリントサーバーに自動的に再分散します。これにより、既存および新規のすべてのセッションは、ユーザーエクスペリエンスに影響を与えることなく、また管理者の即時介入を必要とすることなく、正常に機能します。

管理者は、一連のパフォーマンスカウンターを使用してロードバランスされたプリントサーバーのアクティビティを監視し、VDA上で以下を追跡できます。

- VDA上の負荷分散されたプリントサーバーのリストとその状態（利用可能、利用不可）
- 各プリントサーバーが受け入れたプリンター接続の数
- 各プリントサーバーで失敗したプリンター接続の数
- 各プリントサーバーでのアクティブなプリンター接続の数
- 各プリントサーバーでの保留中のプリンター接続の数

印刷キューの表示と管理

次の表は、環境内でプリンターを表示し、印刷キューを管理できる場所をまとめたものです。

	印刷経路	場所
クライアントプリンター（ユーザーデバイスに接続されたプリンター）	クライアント印刷経路	UACが有効な場合: Microsoft管理コンソールにある印刷の管理スナップイン; UACが無効な場合: Windows 8より前: コントロールパネル, Windows 8: 印刷の管理スナップイン

	印刷経路	場所
ネットワークプリンター（ネットワークプリントサーバー上のプリンター）	ネットワーク印刷経路	UAC有効時: 印刷サーバー \> Microsoft Management Console にある印刷の管理スナップイン; UAC無効時: 印刷サーバー \> コントロールパネル
ネットワークプリンター (ネットワーク印刷サーバー上のプリンター)	クライアント印刷経路	UAC有効時: 印刷サーバー \> Microsoft Management Console にある印刷の管理スナップイン; UAC無効時: Windows 8より前: コントロールパネル, Windows 8: 印刷の管理スナップイン
ローカルネットワークサーバープリンター (マルチセッションOSマシンに追加されたネットワーク印刷サーバーからのプリンター)	ネットワーク印刷経路	UAC有効時: 印刷サーバー \> コントロールパネル; UAC無効時: 印刷サーバー \> コントロールパネル

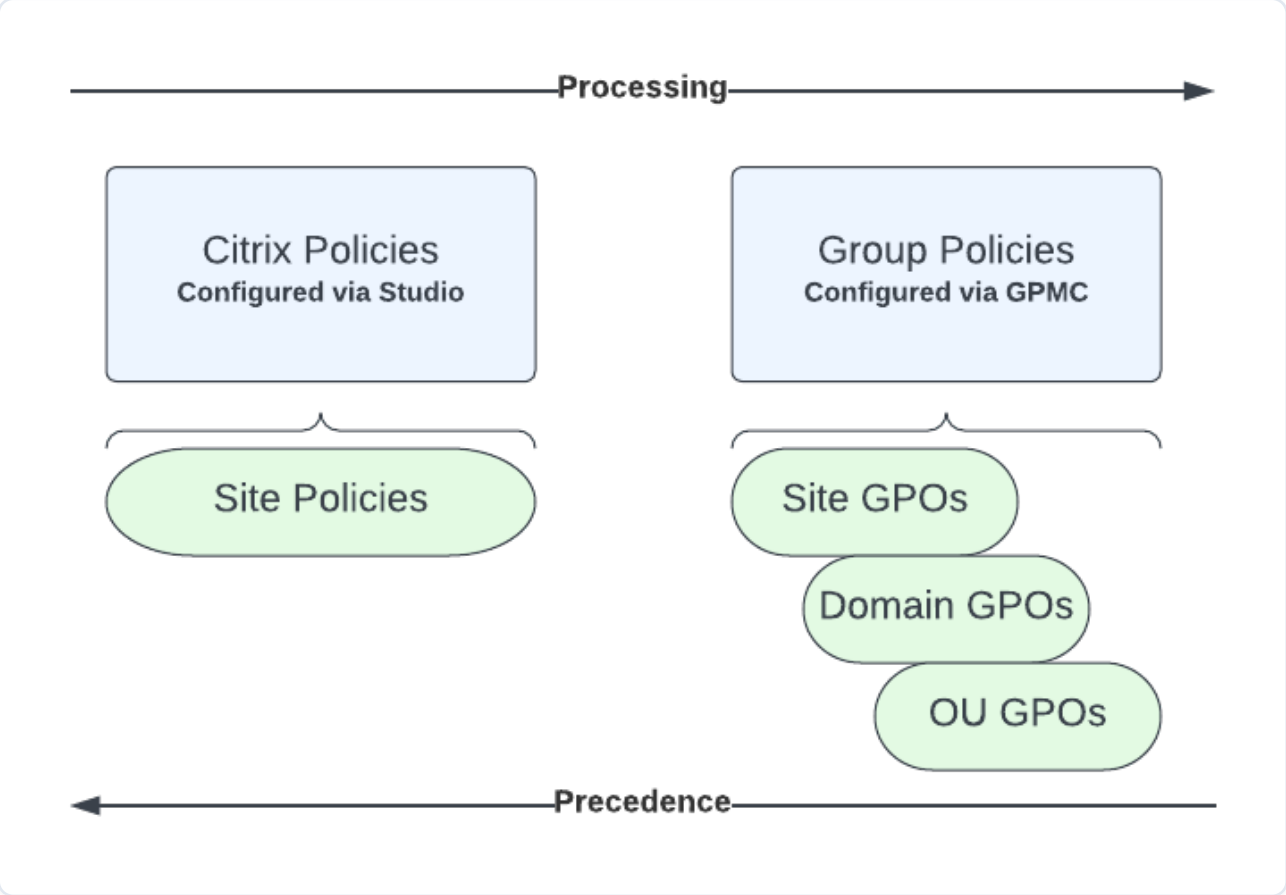
注:

ネットワーク印刷経路を使用するネットワークプリンターの印刷キューはプライベートであり、システムを通じて管理できません。

ポリシー

ポリシーとは、ユーザー、デバイス、または接続の種類グループに対して、セッション、帯域幅、およびセキュリティがどのように管理されるかを定義する設定の集まりです。

ポリシー設定は、物理マシン、仮想マシン、またはユーザーに適用できます。設定は、ローカルレベルの個々のユーザー、またはActive Directoryのセキュリティグループに適用できます。構成は特定の基準とルールを定義します。ポリシーを明示的に割り当てない場合、設定はすべての接続に適用されます。



ポリシーはネットワークのさまざまなレベルで適用できます。組織単位GPOレベルに配置されたポリシー設定は、ネットワーク上で最も高い優先順位を持ちます。ドメインGPOレベルのポリシーは、サイトグループポリシーオブジェクトレベルのポリシーを上書きします。サイトグループポリシーオブジェクトレベルは、MicrosoftおよびCitrixローカルポリシーレベルの両方における競合するポリシーを上書きします。

すべてのCitrixローカルポリシーは、Web Studioコンソールで作成および管理され、サイトデータベースに保存されます。グループポリシーは、Microsoftグループポリシー管理コンソール（GPMC）を使用して作成および管理され、Active Directoryに保存されます。Microsoftローカルポリシーは、Windowsオペレーティングシステムで作成され、レジストリに保存されます。

Studioは、モデリングウィザードを使用して、管理者がテンプレートとポリシー内の構成設定を比較し、競合する設定や冗長な設定を排除するのに役立ちます。管理者はGPMCを使用してGPOを設定し、設定を構成できます。また、それらをネットワークのさまざまなレベルのターゲットユーザーセットに適用することもできます。

これらのGPOはActive Directoryに保存されます。これらの設定の管理へのアクセスは、セキュリティ上の理由からほとんどのIT担当者に対して制限されています。

設定は優先順位とその条件に従ってマージされます。無効な設定は、下位の有効な設定を上書きします。未構成のポリシー設定は無視され、下位の設定を上書きしません。

ローカルポリシーは、Active Directory内のグループポリシーと競合することもあり、状況によっては互いに上書きし合う可能性があります。

すべてのポリシーは次の順序で処理されます。

1. エンドユーザーはドメイン資格情報を使用してマシンにログオンします。
2. 資格情報はドメインコントローラーに送信されます。
3. Active Directoryはすべてのポリシー（エンドユーザー、エンドポイント、組織単位、ドメイン）を適用します。
4. エンドユーザーはCitrix Workspace™アプリにログオンし、アプリケーションまたはデスクトップにアクセスします。
5. CitrixおよびMicrosoftのポリシーは、エンドユーザーとリソースをホストするマシンに対して処理されます。
6. Active Directoryはポリシー設定の優先順位を決定します。その後、それらをエンドポイントデバイスのレジストリと、リソースをホストするマシンに適用します。
7. エンドユーザーがリソースからログオフします。エンドユーザーおよびエンドポイントデバイスに対するCitrixポリシーは、アクティブではなくなります。
8. エンドユーザーがユーザーデバイスからログオフすると、GPOユーザーポリシーが解放されます。
9. エンドユーザーがデバイスの電源を切ると、GPOマシンポリシーが解放されます。

ユーザー、デバイス、マシンのグループに対してポリシーを作成する場合、一部のメンバーは異なる要件を持つ可能性があり、一部のポリシー設定に対して例外が必要になる場合があります。例外は、ポリシーが誰または何に影響するかを決定するStudioおよびGPMCのフィルターによって作成されます。

> **注：**

> 同じGPO内でWindowsポリシーとCitrixポリシーを混在させることはサポートされていません。

ポリシーの操作

> **注:**

> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> ユーザーアクセスとセッション環境を制御するようにCitrixポリシーを構成します。Citrixポリシーは、接続、セキュリティ、および帯域幅の設定を制御する最も効率的な方法です。特定のユーザーグループ、デバイス、または接続タイプに対してポリシーを作成できます。各ポリシーには複数の設定を含めることができます。

Citrixポリシーを操作するためのツール

Citrixポリシーでは、次のツールを使用できます。

- **Web Studio。** グループポリシーを管理する権限がないCitrix管理者の場合は、Web Studioを使用してサイトのポリシーを作成します。Web Studioを使用して作成されたポリシーはサイトデータベースに保存され、更新はVDAがブローカーに登録されたとき、またはユーザーがそのVDAに接続したときにVDAにプッシュされます。
- **ローカルグループポリシーエディター** (Microsoft 管理コンソールスナップイン)。ネットワーク環境でActive Directoryを使用しており、グループポリシーを管理する権限がある場合は、ローカルグループポリシーエディターを使用してサイトのポリシーを作成できます。構成した設定

は、グループポリシー管理コンソールで指定したグループポリシーオブジェクト (GPO) に影響します。

重要:

一部のポリシー設定を構成するには、ローカルグループポリシーエディターを使用することをお勧めします。例としては、VDAをコントローラーに登録する設定や、Microsoft App-Vサーバーに関連する設定などがあります。 追加のポリシー検証が追加されます。その結果、無効なポリシー設定が存在する場合、インプレースアップグレードを行うとポリシーデータが失われる可能性があります。Web Studio以外の方法でポリシーを作成または編集する場合は、最新バージョンのSDKとスナップインを使用することをお勧めします。

ポリシーの処理順序と優先順位

グループポリシー設定は、次の順序で処理されます。

1. ローカルGPO
2. Virtual Apps and DesktopsサイトGPO (サイトデータベースに保存)
3. サイトレベルのGPO
4. ドメインレベルのGPO
5. 組織単位

ただし、競合が発生した場合、最後に処理されたポリシー設定が以前に処理された設定を上書きします。ポリシー設定の優先順位は次のとおりです。

1. 組織単位
2. ドメインレベルのGPO
3. サイトレベルのGPO
4. Virtual Apps and Desktops サイト GPO (サイトデータベースに保存)
5. ローカル GPO

例えば、Citrix管理者はWeb Studioを使用して、会社の営業担当者向けにクライアントファイルリダイレクトを有効にするポリシー（ポリシーA）を作成します。一方、別の管理者はグループポリシーエディターを使用して、営業担当者向けにクライアントファイルリダイレクトを無効にするポリシー（ポリシーB）を作成します。営業担当者が仮想デスクトップにログオンすると、ポリシー

Bが適用され、ポリシーAは無視されます。その理由は、ポリシーBがドメインレベルで処理され、ポリシーAがVirtual Apps and DesktopsサイトGPOレベルで処理されたためです。

ただし、ユーザーがICA®またはリモートデスクトッププロトコル（RDP）セッションを起動すると、Citrixセッション設定は、Active Directoryポリシーで構成された設定、またはリモートデスクトップセッションホスト構成を使用して構成された設定を上書きします。この設定には、一般的なRDPクライアント接続設定に関連する設定が含まれます。RDPクライアント接続設定の例としては、デスクトップの壁紙、メニューアニメーション、ドラッグ中のウィンドウコンテンツの表示などがあります。

複数のポリシーを使用する場合、競合する設定を含むポリシーに優先順位を付けることができます。詳細については、「ポリシーの比較、優先順位付け、モデル化、トラブルシューティング」を参照してください。

Citrixポリシーのワークフロー

ポリシーを構成するプロセスは次のとおりです。

1. ポリシーを作成します。
2. ポリシー設定を構成します。
3. ポリシーをマシンおよびユーザーオブジェクトに割り当てます。
4. ポリシーに優先順位を付けます。
5. Citrixグループポリシーモデリングウィザードを実行して、有効なポリシーを確認します。

> **注:**
>
> Citrixグループポリシーモデリングウィザードを開くには、**ポリシー > モデリング**タブに移動し、アクションバーで**モデリングウィザードの起動**をクリックします。**モデリング**タブは、お客様の要望に応じてWeb Studioで利用できます。

Citrixポリシーと設定のナビゲート

ローカルグループポリシーエディターでは、ポリシーと設定は「コンピューターの構成」と「ユーザーの構成」の2つのカテゴリに表示されます。各カテゴリにはCitrixポリシーノードがあります。このスナップインのナビゲートと使用に関する詳細については、Microsoftのドキュメントを参照してください。

Web Studioでは、ポリシー設定は、影響を与える機能または特徴に基づいてカテゴリに分類されます。例えば、**プロファイル管理**セクションには、プロファイル管理のポリシー設定が含まれています。

- コンピューター設定（マシンに適用されるポリシー設定）は、仮想デスクトップの動作を定義し、仮想デスクトップの起動時に適用されます。これらの設定は、仮想デスクトップ上でアクティブなユーザーセッションがない場合でも適用されます。
- ユーザー設定は、ICAを使用して接続する際のユーザーエクスペリエンスを定義します。ユーザーポリシーは、ユーザーがICAを使用して接続または再接続するときに適用されます。ユーザーがRDPを使用して接続したり、コンソールに直接ログオンしたりする場合は、ユーザーポリシーは適用されません。

  ポリシー、設定、またはテンプレートにアクセスするには、Web Studioの左ペインで**ポリシー**を選択します。

  - **ポリシー**タブには、すべてのポリシーが一覧表示されます。ポリシーを選択すると、下部に次のタブが表示されます。
    - 概要 - 名前、優先度、有効/無効の状態、および説明を一覧表示します
    - 設定 - 構成済みのすべての設定を一覧表示します
    - 割り当て先 - ポリシーが割り当てられているユーザーオブジェクトとマシンオブジェクトを一覧表示します。 詳細については、「ポリシーの作成」を参照してください。
  - 「**テンプレート**」タブには、作成したCitrix提供のカスタムテンプレートが一覧表示されます。テンプレートを選択すると、下部にタブが表示されます。
    - 説明 (テンプレートを使用する理由)
    - 設定 (構成された設定のリスト)。詳細については、「ポリシーテンプレート」を参照してください。
  - 「**比較**」タブを使用すると、ポリシーまたはテンプレートの設定を、他のポリシーまたはテンプレートの設定と比較できます。たとえば、ベストプラクティスへの準拠を確実にするために、設定値を検証したい場合があります。詳細については、「ポリシーの比較、優先順位付け、モデル化、トラブルシューティング」を参照してください。

  ポリシーまたはテンプレートで設定を検索するには：

  a. ポリシーまたはテンプレートを選択します。
  b. アクションバーで、 または を選択します。
  c. ページで、 フィールドに設定の名前を入力します。

検索を絞り込むには、以下を選択します。

- 特定の製品バージョン
- カテゴリ（例：帯域幅）
- 設定名に含まれるキーワード
- チェックボックス
- 選択したポリシーに追加された設定のみを検索する場合。

フィルタリングされていない検索の場合は、 を選択します。

- ポリシー内の設定を検索するには：

a. ポリシーを選択します。

b. **設定**タブを選択し、設定名を入力します。

特定の製品バージョンを選択するか、カテゴリを選択して検索を絞り込むことができます。フィルタリングされていない検索の場合は、**すべての設定**を選択します。

ポリシーは、一度作成されると、使用されたテンプレートとは独立します。新しいポリシーの**説明**フィールドを使用して、使用されたソーステンプレートを追跡できます。

グループポリシーエディターでは、コンピューター設定とユーザー設定は、両方の種類の設定を含むテンプレートから作成された場合でも、個別に適用する必要があります。この例では、コンピューター構成で「非常に高精細なユーザーエクスペリエンス」を使用することを選択した場合：

- レガシーグラフィックモードは、このテンプレートから作成されたポリシーで使用されるコンピューター設定です。
- グレー表示されているユーザー設定は、このテンプレートから作成されたポリシーでは使用されません。

ローカルグループポリシーエディター(/en-us/citrix-virtual-apps-desktops/2311/media/group-policy-editor-template-example.png)

ポリシーテンプレート

> **注:**

> Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> テンプレートは、特定の結果を達成するためのポリシー作成に使用することが推奨される設定の集合です。たとえば、エンドユーザーに高精細なユーザーエクスペリエンスを提供するためのポリシーを作成する場合、**Very High Definition User Experience**テンプレートで定義されている設定を、そのようなポリシーを作成するための参照点および開始点として使用できます。

テンプレートはポリシーではありません。テンプレートはCitrixポリシー設定の補足ドキュメントです。これらは、特定のユーザー関連設定の集合的な機能を示します。

テンプレートの使用は任意です。管理者はテンプレートを使用せずにポリシーを作成できます。テンプレートは、サイトをどのように構成すべきかについて大まかなアイデアを持っているものの、目的の構成を達成するためにどの設定を使用すべきか不明な管理者にとって役立ちます。

管理者は、既存のテンプレート、既存のポリシー、またはゼロからテンプレートを作成できます。

ADMX/ADML

ここで説明するCitrixグループポリシーテンプレートは、Windowsポリシーテンプレートとは関係ありません。ここで説明するテンプレートとWindowsポリシーテンプレートは2つの異なる概念です。CitrixグループポリシーテンプレートはADMXファイルではありません。

組み込みのCitrixテンプレート

以下のポリシーテンプレートが利用可能です。

- **Very High Definition User Experience**。このテンプレートは、ユーザーエクスペリエンスを最大化するデフォルト設定を適用します。複数のポリシーが優先順位に従って処理されるシナリオでこのテンプレートを使用します。
- **High Server Scalability**。このテンプレートを適用して、サーバーリソースを節約します。このテンプレートは、ユーザーエクスペリエンスとサーバーのスケーラビリティのバランスを取ります。単一サーバーでホストできるユーザー数を増やしながら、良好なユーザーエクスペリエンスを提供します。このテンプレートは、グラフィックの圧縮にビデオコーデックを使用せず、サーバー側のマルチメディアレンダリングを防止します。

- **High Server Scalability-Legacy OS**。このHigh Server Scalabilityテンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにより効率的なレガシーグラフィックモードに依存しています。
- **Optimized for NetScaler SD-WAN**。Citrix Virtual Desktopsの配信を最適化するために、NetScaler SD-WANを使用して支社から作業するユーザーにこのテンプレートを適用します。(NetScaler SD-WANはCloudBridgeの新しい名称です)。
- **WAN向けに最適化**。このテンプレートは、共有WAN接続を使用する支社のタスクワーカー、またはグラフィックがシンプルなユーザーインターフェイスとマルチメディアコンテンツが少ないアプリケーションにアクセスする低帯域幅接続のリモートロケーション向けです。このテンプレートは、帯域幅効率を最適化するために、ビデオ再生エクスペリエンスと一部のサーバー拡張性を犠牲にします。
- **WAN向けに最適化 - レガシーOS**。この*WAN向けに最適化*テンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにとってより効率的なレガシーグラフィックモードに依存しています。
- **セキュリティと制御**。リスク許容度が低い環境でこのテンプレートを使用し、Citrix Virtual Apps and Desktopsでデフォルトで有効になっている機能を最小限に抑えます。このテンプレートには、ユーザーデバイスでの印刷、クリップボード、周辺機器、ドライブマッピング、ポートリダイレクト、およびFlashアクセラレーションへのアクセスを無効にする設定が含まれています。このテンプレートを適用すると、より多くの帯域幅を使用し、サーバーあたりのユーザー密度が低下する可能性があります。

組み込みのCitrixテンプレートをデフォルト設定で使用することをお勧めしますが、一部の設定には特定の推奨値がありません。たとえば、WAN向けに最適化テンプレートに含まれる**セッション全体の帯域幅制限**などです。この場合、テンプレートは設定を公開し、管理者がこの設定がシナリオに適用される可能性が高いことを理解できるようにします。

テンプレートのデフォルト設定画像(/en-us/citrix-virtual-apps-desktops/2311/media/template-default-settings.png)

XenAppおよびXenDesktop 7.6 FP3より前の展開（ポリシー管理およびVDA）を使用しており、高サーバー拡張性とWAN最適化テンプレートが必要な場合は、該当する場合にこれらのテンプレートのレガシーOSバージョンを使用してください。

> **注:**

> Citrixは組み込みテンプレートを作成および更新します。これらのテンプレートは変更または削除できません。

Web Studioを使用してテンプレートを作成および管理する

テンプレートに基づいてテンプレートを作成するには：

1. Web Studioにサインインし、左側のペインで**ポリシー**を選択します。
2. **テンプレート**タブを選択し、テンプレートを作成する元のテンプレートを選択します。
3. **テンプレートの作成**タブを選択します。**設定の選択**画面が表示されます。
4. テンプレートに含めるポリシー設定を選択して構成します。
5. 「**次へ**」をクリックします。「**概要**」画面が表示されます。
6. テンプレートの名前を入力します。
7. **完了**をクリックします。新しいテンプレートが**テンプレート**タブに表示されます。

ポリシーに基づいてテンプレートを作成するには：

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **ポリシー**タブを選択し、テンプレートを作成するポリシーを選択します。
3. **その他**タブをクリックします。
4. **テンプレートとして保存**を選択します。**設定の選択**画面が表示されます。
5. テンプレートに含める新しいポリシー設定を選択して構成します。
6. **次へ**をクリックします。**概要**画面が表示されます。
7. テンプレートの名前と説明を入力し、**完了**をクリックします。

テンプレートと委任管理

Web Studioのテンプレートはサイトデータベースに保存されますが、Citrix Studioのテンプレートは、現在の管理者のユーザープロファイルフォルダーに`.gpt`拡張子を持つファイルとして保存されます。ある管理者が作成したCitrix Studioテンプレートは、他の管理者や、別のマシン上の同じ管理者には表示されません。Web Studioテンプレートは、権限と委任管理の対象となるすべての管理者に表示されます。

ポリシーの作成

> **注：**

> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> ポリシーを作成する前に、それが影響を与える可能性のあるユーザーまたはデバイスのグループを決定します。ユーザーの職務、接続の種類、ユーザーデバイス、または地理的な場所に基づいてポリシーを作成することができます。Windows Active Directoryグループポリシーに使用するのと同じ基準を使用することもできます。

すでにグループに適用されるポリシーを作成している場合は、別のポリシーを作成するのではなく、そのポリシーを編集することを検討してください。ポリシーを編集した後、適切な設定を構成します。特定の機能を有効にするためだけ、または特定のユーザーにポリシーが適用されないようにするためだけにポリシーを作成することは避けてください。

ポリシーを作成する際、ポリシーテンプレートの設定に基づいて作成し、必要に応じて設定をカスタマイズできます。テンプレートを使用せずに、必要なすべての設定を追加して作成することもできます。

Web Studioでは、**ポリシーを有効にする**チェックボックスが明示的にオンにされていない限り、新しく作成されたポリシーは無効に設定されます。

ポリシー作成時および設定構成時に、システムは設定の種類を表示するオプションを提供します。次の設定の種類を表示できます。

- すべての設定 - すべてのVDAバージョンに適用可能なすべてを表示
- 現在の設定のみ - 現在のVDAバージョンに固有の設定を表示
- レガシー設定のみ - 非推奨のVDAバージョンにのみ適用可能な設定を表示

設定を構成しながら設定を表示するには：

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **ポリシー**タブで、**ポリシーの作成**をクリックします。
3. **設定の選択**テーブルで、**設定**の横にあるドロップダウンをクリックします。
4. ドロップダウンから以下のいずれかのオプションを選択します。

- すべての設定 - すべてのVDAバージョンのすべての設定を表示します
- 現在の設定のみ - 現在のVDAバージョンの設定のみを表示します

- レガシー設定のみ - 非推奨のVDAバージョンの設定のみを表示します

1. 「**設定**」テーブルには、前の手順に基づいて利用可能な設定が一覧表示されます。

ポリシー設定

ポリシー設定は、有効、無効、または未構成にすることができます。デフォルトでは、ポリシー設定は構成されていません。つまり、ポリシーに追加されていません。設定は、ポリシーに追加された場合にのみ適用されます。

一部のポリシー設定は、次のいずれかの状態になります。

- 許可または禁止は、設定によって制御されるアクションを許可または防止します。ユーザーがセッションで設定のアクションを管理することを許可または防止される場合があります。たとえば、メニューアニメーション設定が「許可」に設定されている場合、ユーザーはクライアント環境でメニューアニメーションを制御できます。
- 有効または無効は、設定をオンまたはオフにします。設定を無効にすると、下位ランクのポリシーでは有効になりません。

さらに、一部の設定は、依存する設定の有効性を制御します。たとえば、クライアントドライブリダイレクトは、ユーザーがデバイス上のドライブにアクセスできるかどうかを制御します。ユーザーがネットワークドライブにアクセスできるようにするには、この設定と「**クライアントネットワークドライブ**」設定の両方をポリシーに追加する必要があります。「**クライアントドライブリダイレクト**」設定が無効になっている場合、「**クライアントネットワークドライブ**」設定が有効になっていても、ユーザーはネットワークドライブにアクセスできません。

一般に、マシンに影響を与えるポリシー設定の変更は、仮想デスクトップが再起動したとき、またはユーザーがログオンしたときに有効になります。ユーザーに影響を与えるポリシー設定の変更は、ユーザーが次回ログオンしたときに有効になります。Active Directoryを使用している場合、ポリシー設定はActive Directoryが90分間隔でポリシーを再評価するときに更新されます。そして、ポリシー設定は、仮想デスクトップが再起動したとき、またはユーザーがログオンしたときに適用されます。

一部のポリシー設定では、設定をポリシーに追加するときに値を入力または選択できます。「デフォルト値を使用」を選択することで、設定の構成を制限できます。この選択により、設定の構成が無効になり、ポリシーが適用されるときに設定のデフォルト値のみが使用されるようになります。「デフォルト値を使用」を選択する前に入力された値に関係なく、この選択が適用されます。

セキュアデフォルト設定が有効になっている場合、VDAインストール中に、ポリシー設定の優先順位は次のように影響を受けます。

- カスタマイズされた設定が最優先されます
- セキュアなデフォルト設定は2番目の優先順位になります
- デフォルト設定は最も低い優先順位になります

ポリシーのセキュアデフォルト設定を表示するには：

1. Web Studioにログオンします。
2. 左側のナビゲーションで、「**ポリシー**」をクリックします。
3. 「**ポリシー**」タブで、「**ポリシーの作成**」をクリックします。
4. 「**設定の選択**」テーブルで、現在の値が「**許可済み ?**」である設定にマウスカーソルを合わせると、「**セキュリティ保護されたデフォルト値: 禁止**」が表示されます。

   セキュアなデフォルト設定(en-us/citrix-virtual-apps-desktops/2311/media/secure-default-setting.png)

ベストプラクティスとして：

- 個々のユーザーではなく、グループにポリシーを割り当てます。グループにポリシーを割り当てると、グループへのユーザーの追加または削除時に割り当てが自動的に更新されます。
- リモートデスクトップセッションホスト構成で、競合する設定や重複する設定を有効にしないでください。リモートデスクトップセッションホスト構成は、Citrixポリシー設定と同様の機能を提供することがあります。トラブルシューティングを容易にするため、可能な限りすべての設定を一貫性のある状態（有効または無効）に保ってください。
- 使用されていないポリシーは無効にしてください。設定が追加されていないポリシーは、不要な処理を発生させます。

ポリシーの割り当て

ポリシーを作成する際、特定のユーザーおよびマシンオブジェクトに割り当てます。そのポリシーは、特定の基準またはルールに従って接続に適用されます。一般的に、基準の組み合わせに基づいて、ポリシーに好きなだけ割り当てを追加できます。

割り当てを指定しない場合、または割り当てを指定しても無効にする場合、ポリシーは**すべて**の接続に適用されます。

> **注:**

ポリシーの割り当ては、ポリシーフィルターとも呼ばれます。詳細については、以下のトピックを参照してください。

- ポリシーのフィルターを作成、変更、または削除する
- フィルターはどのように適用されますか？

次の表に、利用可能な割り当てを示します。

割り当て名	ポリシーの適用基準
アクセスコントロール	クライアントが接続しているアクセスコントロール条件。*接続タイプ* - NetScaler® Gateway を使用して行われた接続、または使用せずに行われた接続にポリシーを適用するかどうか。*NetScaler Gateway ファーム名* - NetScaler Gateway 仮想サーバーの名前。*アクセス条件* - 使用するエンドポイント分析ポリシーまたはセッションポリシーの名前。
NetScaler SD-WAN	ユーザーセッションが NetScaler SD-WAN を介して起動されるかどうか。**注:** 1つのポリシーには、NetScaler SD-WAN 割り当てを1つだけ追加できます。
クライアントIPアドレス	セッションへの接続に使用されるユーザーデバイスのIPアドレス：IPv4の例：12.0.0.0、12.0.0.*、12.0.0.1-12.0.0.70、12.0.0.1/24。IPv6の例：2001:0db8:3c4d:0015:0:0:abcd:ef12、2001:0db8:3c4d:0015::/54
クライアント名	ユーザーデバイスの名前。完全一致：ClientABCName。ワイルドカードを使用：Client*Name。
デリバリーグループ	デリバリーグループのメンバーシップ。
デリバリーグループの種類	デスクトップまたはアプリケーションの種類: プライベートデスクトップ、共有デスクトップ、プライベートアプリケーション、または共有アプリケーション。**注:** プライベートデスク

割り当て名	ポリシーの適用基準
	トップと共有デスクトップのフィルターオプションは、Citrix Virtual Apps and Desktops 7.xでのみ利用可能です。詳細については、CTX219153を参照してください。
組織単位 (OU)	組織単位。
タグ	タグ。**注:** このポリシーをすべてのタグ付きマシンに適用します。アプリケーションタグは含まれません。
ユーザーまたはグループ	ユーザーまたはグループ名。

ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが特定されます。これらのポリシーは優先順位順に並べ替えられ、設定の複数のインスタンスが比較されます。各設定は、ポリシーの優先順位に従って適用されます。無効になっているポリシー設定は、有効になっている下位ランクの設定よりも優先されます。構成されていないポリシー設定は無視されます。

重要:

Group Policy Management Console を使用して Active Directory ポリシーと Citrix ポリシーの両方を構成する場合、割り当てと設定が期待どおりに適用されないことがあります。詳細については、CTX127461を参照してください。

「Unfiltered」という名前のポリシーがデフォルトで提供されます。

- Web Studioを使用してCitrixポリシーを管理する場合、「Unfiltered」ポリシーに追加した設定は、サイト内のすべてのサーバー、デスクトップ、および接続に適用されます。
- ローカルグループポリシーエディターを使用してCitrixポリシーを管理する場合、Unfilteredポリシーに追加した設定はすべてのサイトと接続に適用されます。サイトと接続は、ポリシーを含むグループポリシーオブジェクト (GPO) のスコープ内にある必要があります。たとえば、Sales OUには、米国の営業チームのすべてのメンバーを含むSales-USというGPOが含まれています。Sales-US GPOは、いくつかのユーザーポリシー設定を含むUnfilteredポリシーで構成されています。米国の営業マネージャーがサイトにログオンすると、Unfilteredポリシーの設定がセッションに自動的に適用されます。この構成は、ユーザーがSales-US GPOのメンバーであるためです。

割り当てのモードは、ポリシーがすべての割り当て条件に一致する接続にのみ適用されるかどうかを決定します。モードがAllow (デフォルト) に設定されている場合、ポリシーは割り当て条件に一致する接続にのみ適用されます。モードがDenyに設定されている場合、接続が割り当て条件に一致しない場合にポリシーが適用されます。以下の例は、複数の割り当てが存在する場合に割り当てモードがCitrixポリシーにどのように影響するかを示しています。

- **例: モードが異なる同種の割り当て** - 同じ種類の2つの割り当てがあり、一方がAllowに設定され、もう一方がDenyに設定されているポリシーでは、接続が両方の割り当てを満たす場合、Denyに設定された割り当てが優先されます。例:

  ポリシー1には、次の割り当てが含まれています。

  - 割り当てAはSalesグループを指定します。モードはAllowに設定されています。
  - 割り当てBはSalesマネージャーのアカウントを指定します。モードはDenyに設定されています。

  割り当てBのモードがDenyに設定されているため、Salesマネージャーがサイトにログオンしても、ユーザーがSalesグループのメンバーであってもポリシーは適用されません。

- **例: モードが同じで異なる種類の割り当て** - 異なる種類の2つ以上の割り当てがあり、Allowに設定されているポリシーでは、ポリシーが適用されるためには、接続が各種類の割り当ての少なくとも1つを満たす必要があります。例:

  ポリシー2には、次の割り当てが含まれています。

  - 割り当てCは、Salesグループを指定するユーザー割り当てです。モードはAllowに設定されています。
  - 割り当てDは、10.8.169.* (企業ネットワーク) を指定するクライアントIPアドレス割り当てです。モードはAllowに設定されています。

  Salesマネージャーがオフィスからサイトにログオンすると、接続が両方の割り当てを満たすため、ポリシーが適用されます。

  ポリシー3には、次の割り当てが含まれています。

  - 割り当てEは、Salesグループを指定するユーザー割り当てです。モードはAllowに設定されています。
  - 割り当てFは、NetScaler Gateway接続条件を指定するアクセスコントロール割り当てです。モードはAllowに設定されています。

  営業マネージャーがオフィスからサイトにログオンしても、接続が割り当てFを満たさないため、ポリシーは適用されません。

Web Studioを使用して、テンプレートに基づいてポリシーを作成する

1. Web Studioにサインインし、左側のペインで**［ポリシー］**を選択します。
2. **［テンプレート］**タブを選択し、テンプレートを選択します。
3. アクションバーで**［テンプレートからポリシーを作成］**を選択します。
4. デフォルトでは、新しいポリシーはテンプレートのすべてのデフォルト設定を使用します。この場合、 が選択されています。設定を変更する場合は、 を選択し、設定を追加または削除します。
5. 次のいずれかを選択して、ポリシーを適用する方法を指定します。
   - 。選択したユーザーおよびマシンオブジェクトにポリシーを適用するには、 をクリックして、ポリシーを適用する必要があるユーザーおよびマシンオブジェクトを選択します。
   - 。サイト内のすべてのユーザーおよびマシンオブジェクトにポリシーを適用します。
6. ポリシーの名前を入力します。ポリシーが影響する対象 (例: 経理部、リモートユーザーなど) に応じてポリシーに名前を付けることを検討してください。必要に応じて、説明を追加します。

   ポリシーはデフォルトで無効になっています。有効にすることができます。ポリシーを有効にすると、ログオンするユーザーにすぐに適用されます。無効にすると、ポリシーは適用されません。ポリシーの優先順位を付けたり、後で設定を追加したりする必要がある場合は、適用する準備ができるまでポリシーを無効にしておくことを検討してください。

Web Studio を使用してポリシーを作成する

1. Web Studio にサインインし、左ペインで を選択します。
2. タブを選択します。
3. アクションバーで を選択します。
4. ポリシー設定を追加および構成します。
5. 次のいずれかを選択して、ポリシーを適用する方法を指定します。
   - 選択したユーザーおよびマシンオブジェクトに割り当て、ポリシーを適用する必要があるユーザーおよびマシンオブジェクトを選択します。
   - サイト内のすべてのオブジェクトに割り当てて、サイト内のすべてのユーザーおよびマシンオブジェクトにポリシーを適用します。

6. ポリシーの名前を入力するか、デフォルトを受け入れます。ポリシーが影響する対象（例: 経理部、リモートユーザーなど）に基づいてポリシーに名前を付けることを検討してください。必要に応じて、説明を追加します。

   ポリシーはデフォルトで有効になっていますが、無効にすることもできます。ポリシーを有効にすると、ログオンするユーザーにすぐに適用されます。無効にすると、ポリシーは適用されません。ポリシーの優先順位を付けたり、後で設定を追加したりする必要がある場合は、適用する準備ができるまでポリシーを無効にしておくことを検討してください。

グループポリシーエディターを使用してポリシーを作成および管理する

グループポリシーエディターで、**コンピューターの構成**または**ユーザーの構成**を展開します。**ポリシー**ノードを展開し、**Citrixポリシー**を選択します。適切なアクションを選択します。

タスク	手順
ポリシーを作成する	**ポリシー**タブで、**新規**をクリックします。
既存のポリシーを編集する	**ポリシー**タブで、ポリシーを選択し、**編集**をクリックします。
既存のポリシーの優先順位を変更する	「**ポリシー**」タブでポリシーを選択し、「**上位**」または「**下位**」をクリックします。
ポリシーの概要情報を表示	「**ポリシー**」タブでポリシーを選択し、「**概要**」タブをクリックします。
ポリシー設定の表示と変更	「**ポリシー**」タブでポリシーを選択し、「**設定**」タブをクリックします。
ポリシーフィルターの表示と変更	「**ポリシー**」タブでポリシーを選択し、「**フィルター**」タブをクリックします。ポリシーに複数のフィルターを追加する場合、ポリシーが適用されるには、すべてのフィルター条件を満たす必要があります。
ポリシーを有効または無効にする	「**ポリシー**」タブでポリシーを選択し、「**アクション > 有効にする**」または「**アクション > 無効にする**」を選択します。
既存のテンプレートからポリシーを作成	「**テンプレート**」タブでテンプレートを選択し、「**新規ポリシー**」をクリックします。

ポリシーセット

ポリシーセットは、Citrix Virtual Apps and Desktops™ のオブジェクトであり、ポリシーを集約して、簡素化されたロールベースのアクセスと容易な管理を可能にします。管理者チームや会社の論理的な区分を反映するようにポリシーセットを作成できます。たとえば、地理的な地域、事業部門、または特定のユースケースごとにポリシーセットを作成できます。作成後、スコープとデリバリーグループがポリシーセットに割り当てられ、承認された管理者のみが関連するユーザーとマシンに適用されるポリシーを管理できるようになります。

注

ポリシーセットを有効にする前に、Citrix® は以下の点に注意することを推奨します。

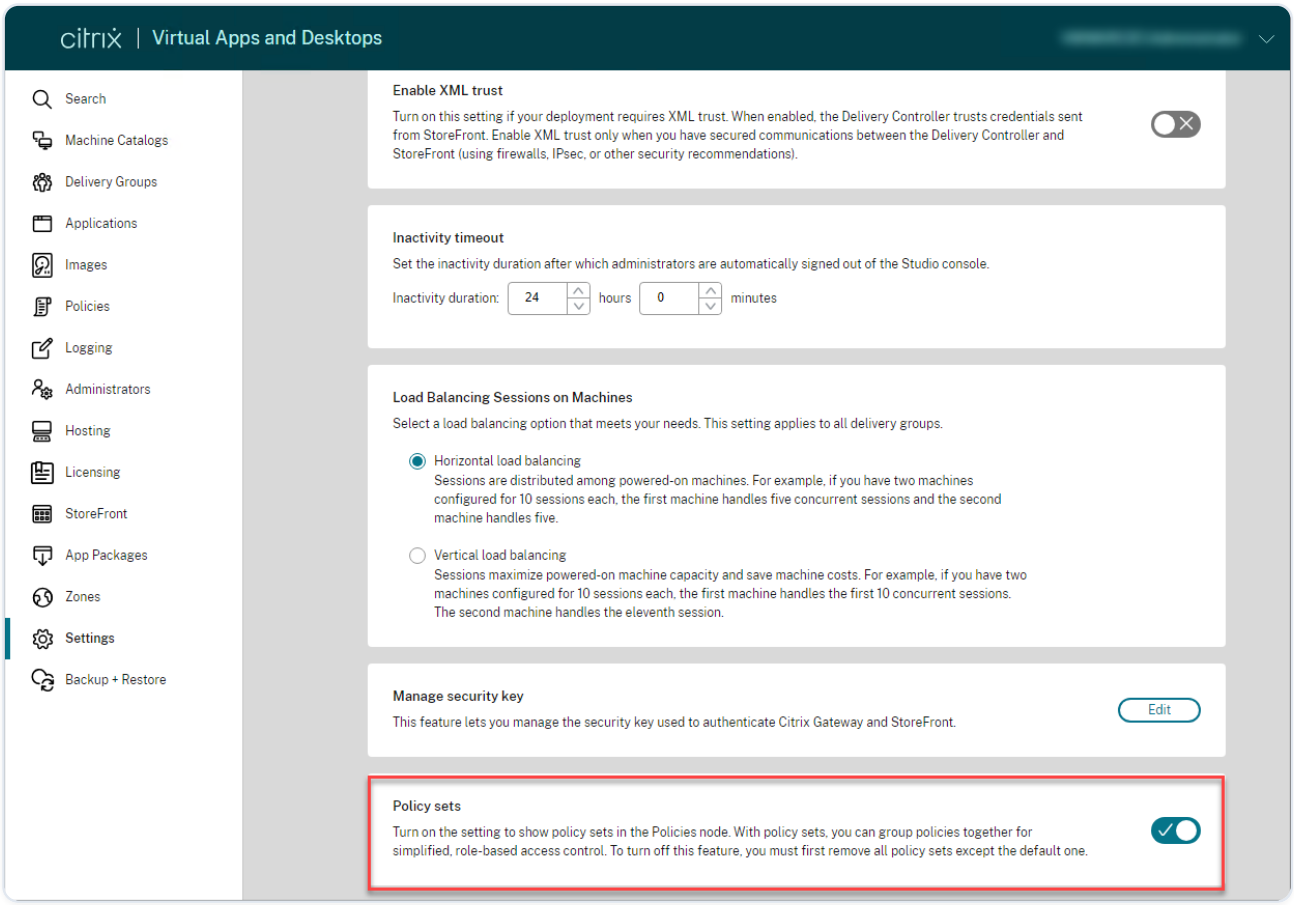
- 追加のポリシー検証が追加されます。その結果、無効なポリシー設定が存在する場合、インプレースアップグレードを行うとポリシーデータが失われる可能性があります。
- 無効なデータを検出するには、GPOスキャナーツール を使用し、アップグレードする前に必要な編集を行ってください。詳細については、CTX666304 を参照してください。
- 今後のすべてのアップグレードでは、Citrixは最新のSDKを使用することを推奨します。古いSDKを使用してポリシーを更新すると、無効なデータがポリシー設定に追加される可能性があり、ポリシーデータが失われるリスクにつながる可能性があります。

利点

- 分散管理者チーム向けのロールベースのアクセス制御
- 合併、買収、統合の簡素化
- 限定された障害ドメイン
- ポリシーのマルチテナントサポート

ポリシーセットを有効にする

Virtual Apps and Desktops の **管理** タブから、**設定** に移動し、**ポリシーセット** 設定をオンにします。



注:

ポリシーセットを作成する前に、ポリシーセットを有効にする必要があります。

機能の比較

ポリシーセットを適用する前	ポリシーセットを適用した後
サイト全体のポリシー、設定、フィルター、およびポリシーの優先順位は、Citrix Studio内で一箇所で構成されます。	ポリシー、設定、フィルター、およびポリシーの優先順位は、各ポリシーセットに対して個別に構成されます。
1つのポリシーを管理する場合、すべてのポリシーを管理する必要があります。	フル管理者は、特定のポリシーセットを個別に管理する機能を下位レベルの管理者に委任できます。
大規模で分散された環境のポリシーは、複雑になり管理が困難になります。	大規模で分散された環境のポリシーは、簡単に分割して管理できます。

ポリシーセットの仕組み?

概要

- ポリシーセットはデリバリーグループに割り当てられます
- ポリシーセットには1つまたは複数のスコープがあります
- ポリシーセットが割り当てられていないデリバリーグループは、デフォルトのポリシーセットを受け取ります
- デリバリーグループに割り当てられるポリシーセットは1つのみです
- 複数のデリバリーグループで同じポリシーセットを使用できます
- ポリシーセットがデリバリーグループに割り当てられていても、ポリシーはフィルターを維持します

詳細については、「フィルターはどのように適用されますか？」を参照してください。ポリシーセットのポリシー割り当てまたはポリシーフィルターの動作方法に変更はありません。つまり、ポリシーの場合と同じように機能します。

デフォルトのポリシーセット

- ポリシーセット設定がオンの場合、既存のすべてのポリシーはデフォルトのポリシーセット内にグループ化されます
- 管理チームがポリシーセットを作成してデリバリーグループに割り当てない限り、すべてのデリバリーグループはデフォルトのポリシーセットを受け取ります。
- デリバリーグループに別のポリシーセットが割り当てられると、デフォルトのポリシーセットからポリシーを受け取らなくなります

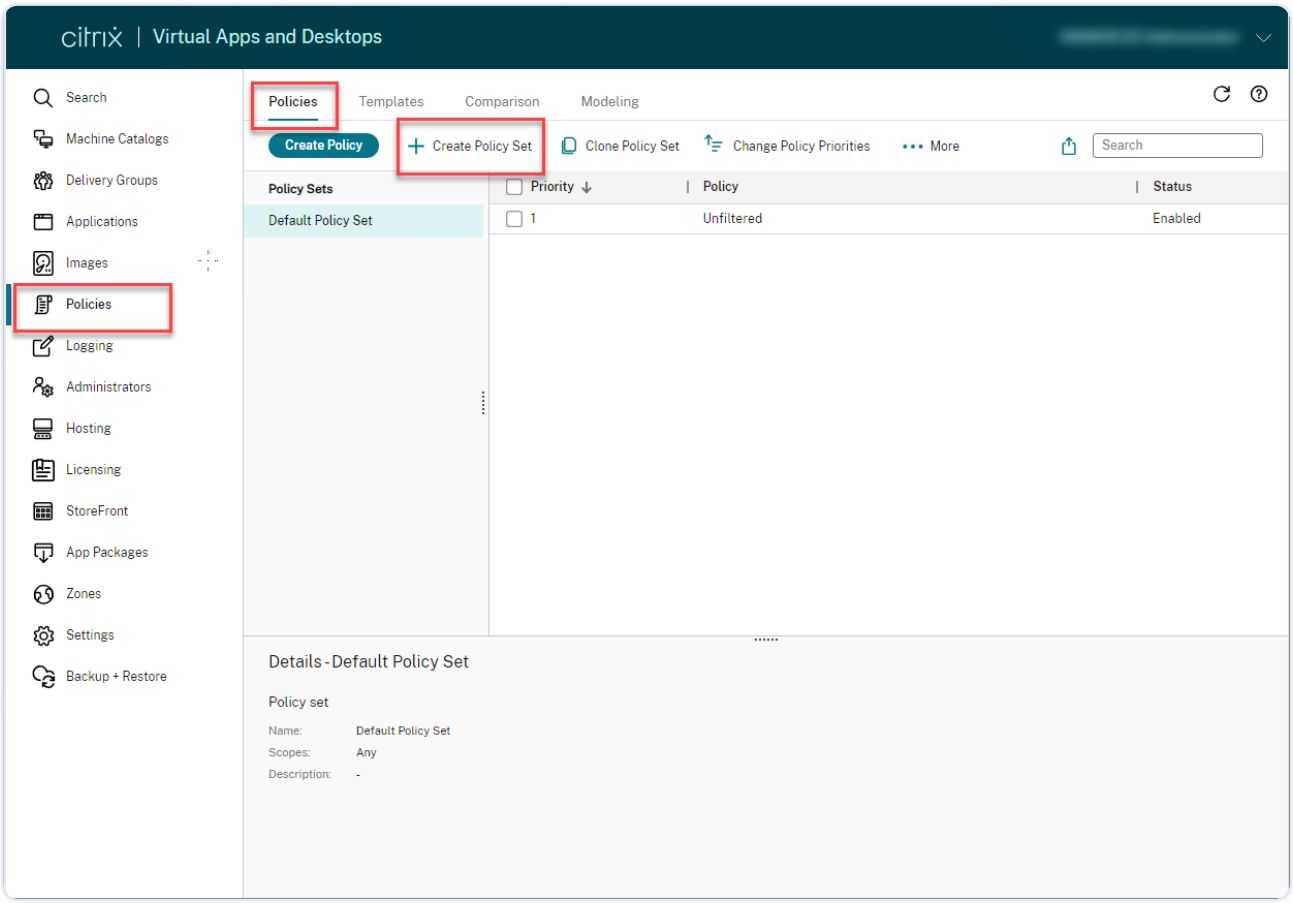
ポリシーセットの作成

ポリシーセットは次の2つの方法で作成できます。

- ポリシーセットの作成 - このアクションにより、空のポリシーセットが作成されます
- ポリシーセットの複製 - このアクションにより、既存のポリシーセットに基づいてポリシーセットが作成されます

ポリシーセットの作成

1. Web Studioにサインインし、左側のペインで **［ポリシー］** を選択します。



1. **ポリシーセットの作成**を選択します。**はじめに**タブが表示されます。
2. **次へ**をクリックするか、**名前と説明**タブをクリックします。
3. ポリシーセットの名前と説明を入力します。
4. **次へ**をクリックするか、**割り当て**タブをクリックします。
5. ポリシーセットを割り当てるデリバリーグループを1つ以上選択します。
6. **次へ**をクリックするか、**スコープ**タブをクリックします。
7. ポリシーセットのスコープを選択します。
8. **作成**をクリックします。定義された割り当てとスコープでポリシーセットが作成されます。

ポリシーセットの複製

1. Web Studioにサインインし、左側のペインで**ポリシー**を選択します。
2. **ポリシーセットの複製**を選択します。
3. ポリシーセットの名前を変更します。
4. ポリシーセットの割り当てを変更または作成し、**次へ**をクリックします。
5. 複製されたポリシーセットに含めるポリシーを選択または選択解除します。
6. ポリシーのスコープを変更します。

7. **作成**をクリックします。ポリシーセットが作成されます。

ポリシーセットの編集

1. Web Studioにサインインし、左側のペインで**ポリシー**を選択します。
2. **ポリシーセットの編集**を選択します。
3. ポリシーセットの名前を変更し、**次へ**をクリックします。
4. ポリシーセットの割り当てを変更または作成し、**次へ**をクリックします。
5. ポリシーのスコープを変更します。
6. **Create** をクリックします。

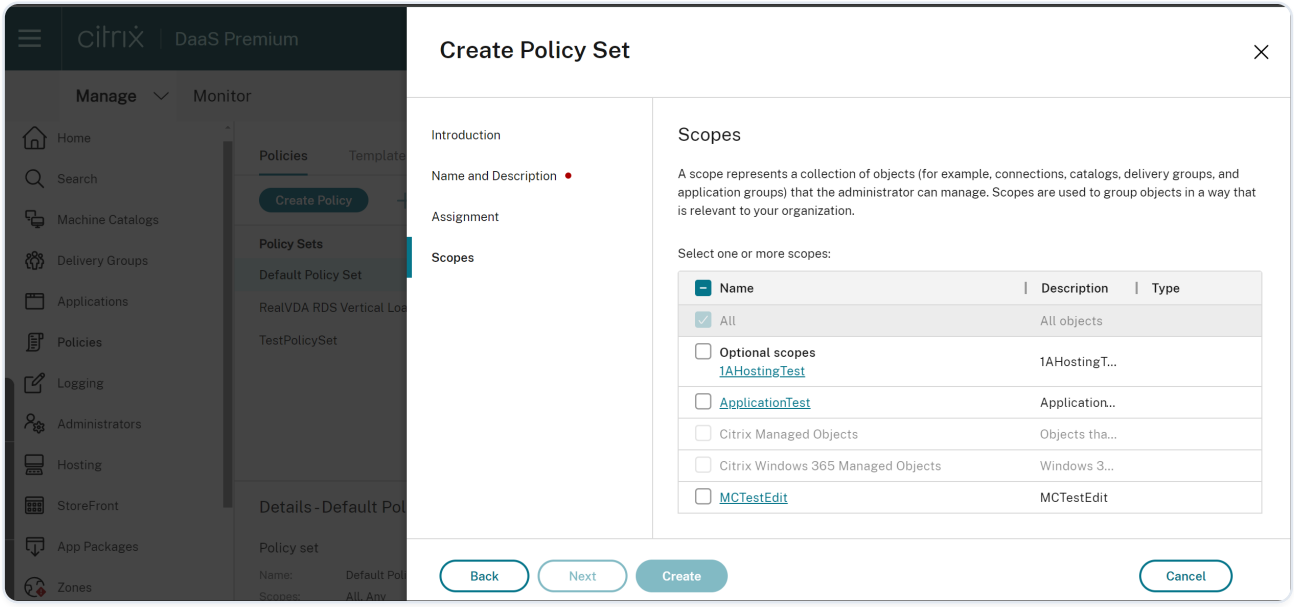
ポリシーセットの割り当て

ポリシーセットはデリバリーグループに割り当てられます。ポリシーセットの作成時または編集時に割り当てを構成できます。デリバリーグループの作成時または編集時にも割り当てを構成できます。

ポリシーセットのスコープ

管理者は、承認された管理者のみがポリシーセットを表示または編集できるように、ポリシーセットのスコープを定義できます。ポリシーセットの作成時または編集時にスコープを構成できます。

ポリシーセットの導入により、API を使用して Citrix ポリシーを作成および管理することもできます。詳細については、Citrix DaaS でポリシーセットを作成する方法を参照してください。



ポリシーの比較、優先順位付け、モデル化、トラブルシューティング

注:

Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

複数のポリシーを使用して、ユーザーの職務、地理的な場所、または接続の種類に基づいて、ユーザーのニーズを満たすように環境をカスタマイズできます。たとえば、セキュリティを強化するために、機密データを定期的に操作するユーザーグループに制限を設けることができます。

また、ユーザーが機密ファイルをローカルクライアントドライブに保存できないようにするポリシーを作成することもできます。ただし、ユーザーグループ内の一部のユーザーがローカルドライブへのアクセスを必要とする場合は、それらのユーザー専用の別のポリシーを作成できます。次に、どちらが優先されるかを制御するために、2つのポリシーをランク付けまたは優先順位付けします。複数のポリシーを使用する場合、次のことを決定する必要があります。

- ポリシーの優先順位付け方法
- 例外の作成方法
- ポリシーが競合する場合に有効なポリシーを表示する方法。

一般に、ポリシーは、サイト全体、特定のDelivery Controller、またはユーザーデバイス用に構成された同様の設定を上書きします。この原則の例外はセキュリティです。環境内で最も高い暗号化設定は、常に他の設定やポリシーを上書きします。最も高い暗号化設定には、オペレーティングシステムと最も制限の厳しいシャドウイング設定が含まれます。

Citrixポリシーは、オペレーティングシステムで設定したポリシーと相互作用します。Citrix環境では、Citrix設定は、Active Directoryポリシーまたはリモートデスクトップセッションホスト構成を使用して構成された同じ設定を上書きします。この設定には、一般的なリモートデスクトッププロトコル（RDP）クライアント接続設定に関連する設定が含まれます。一般的なRDP設定には、デスクトップの壁紙、メニューアニメーション、ドラッグ中のウィンドウコンテンツの表示などの設定が含まれます。

Secure ICA®などの一部のポリシー設定は、オペレーティングシステムの設定と一致している必要があります。より高い優先度の暗号化レベルが他の場所で設定されている場合、ポリシーで指定した、またはアプリケーションとデスクトップを配信するときに指定した**Secure ICAポリシー**設定は上書きされる可能性があります。

たとえば、デリバリーグループを作成するときに指定する暗号化設定は、環境全体で指定した暗号化設定と同じレベルである必要があります。

> **注:**
>
> ダブルホップシナリオの2番目のホップでは、シングルセッションOS VDAがマルチセッションOS VDAに接続することを考慮してください。この場合、Citrixポリシーは、シングルセッションOS VDAをユーザーデバイスであるかのように扱います。たとえば、ユーザーデバイスに画像をキャッシュするようにポリシーが設定されているとします。この例では、ダブルホップシナリオの2番目のホップ用にキャッシュされた画像は、シングルセッションOS VDAマシンにキャッシュされます。

ポリシーモデリングウィザードを使用する

ポリシーモデリングは、計画およびテスト目的で、フィルターが適用された有効なポリシーをシミュレートするのに役立ちます。フィルターが適用された有効なポリシーのみがモデル化されます。無効なポリシーは適用されず、フィルターが適用されていない有効なポリシーは常に適用されます。

ポリシーモデリングウィザードを開くには、次の手順を実行します。

1. 左側のナビゲーションから**ポリシー**を選択します。
2. **モデリング**タブを選択します。
3. アクションバーで**ポリシーモデリング**を選択します。
4. **はじめに**ページを読み、**次へ**をクリックします。
5. ユーザーまたはコンピューターを選択します。コンテナー、または特定のユーザーやコンピューターを参照できます。**次へ**をクリックします。
6. フィルターの証拠を選択します。オプションで、**デリバリーグループ**、**タグ**、**クライアントIPアドレス**などの追加の詳細を入力することで、シミュレーションをより詳細にすることができます。**次へ**をクリックします。
7. 選択内容の概要を確認し、**実行**をクリックします。

実行をクリックすると、ウィザードはモデリング結果のレポートを生成します。このレポートを表示している間、次のことができます。

- ドロップダウンメニューで、**すべての設定**、**コンピューター設定**、または**ユーザー設定**のいずれを表示するかを選択します。
- 検索バーを使用して、特定の設定を検索します。
- 特定の設定をクリックして、その設定の詳細を表示します。たとえば、特定のポリシーに対してすべてのユーザー設定が適用されなかった場合、**詳細**ペインには設定が適用されなかった理由が表示されます。
- **エクスポート**をクリックして、モデリング結果をJSON形式、HTML形式、またはその両方でエクスポートします。

ポリシーモデリングを実行すると、さらに多くのオプションが利用可能になります。次のことができます。

- 「**モデリングレポートの表示**」：これにより、上記のモデリングレポートが開き、再度表示したりエクスポートしたりできます。
- 「**ポリシーモデリングの再実行**」：これにより、以前に選択したのと同じ基準セットでポリシーモデリングを再実行し、新しいモデリング結果を生成できます。これは、一部のポリシーが変更され、それらの変更が現在のモデルにどのように影響するかを確認したい場合に役立ちます。
- 「**モデリングレポートの削除**」：現在のモデリングレポートを削除します。

ポリシーとテンプレートの比較

ポリシーまたはテンプレートの設定を、他のポリシーまたはテンプレートの設定と比較できます。たとえば、ベストプラクティスへの準拠を維持するために、設定値を確認する必要がある場合があります。また、ポリシーまたはテンプレートの設定を、Citrixが提供するデフォルト設定と比較したい場合もあります。

1. Web Studioにサインインし、左側のペインで「**ポリシー**」を選択します。
2. 「**比較**」タブをクリックし、「**選択**」をクリックします。
3. 比較するポリシーまたはテンプレートを選択します。比較にデフォルト値を含めるには、「**デフォルト設定と比較**」チェックボックスをオンにします。
4. 「**比較**」をクリックすると、構成された設定が列に表示されます。
5. すべての設定を表示するには、「**すべての設定を表示**」を選択します。デフォルトビューに戻るには、「**共通設定を表示**」を選択します。

ポリシーの優先順位付け

ポリシーの優先順位付けにより、競合する設定が含まれる場合にポリシーの優先順位を定義できます。ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが特定されます。これらのポリシーは優先順位順に並べ替えられ、任意の設定の複数のインスタンスが比較されます。各設定は、ポリシーの優先順位に従って適用されます。

ポリシーには異なる優先順位番号を付けて優先順位を付けます。デフォルトでは、新しいポリシーには最も低い優先順位が与えられます。ポリシー設定が競合する場合、優先順位が高いポリシー（優先順位番号1が最も高い）は、優先順位が低いポリシーを上書きします。設定は、優先順位と設定の条件（たとえば、設定が無効か有効か）に従ってマージされます。無効な設定は、有効な下位の設定を上書きします。構成されていないポリシー設定は無視され、下位の設定を上書きしません。

1. 左側のペインで「**ポリシー**」を選択します。「**ポリシー**」タブが選択されていることを確認してください。
2. 「**ポリシー**」タブで、アクションバーの「**ポリシーの優先順位の変更**」を選択します。「**ポリシーの優先順位の変更**」ページが表示されます。
3. 優先順位リストで、ポリシーの優先順位を変更するには、次のいずれかの方法を使用します。
   - ポリシーを目的の位置にドラッグします。
   - 1つ上または下に移動するには、それぞれ上矢印または下矢印アイコンをクリックします。
   - リストの先頭または末尾に移動するには、それぞれ先頭または末尾の矢印アイコンをクリックします。
   - 優先順位番号を変更するには、 アイコンをクリックし、必要に応じて番号を入力し、 をクリックします。
4. 「**保存**」をクリックします。

例外

ユーザー、ユーザーデバイス、またはマシンのグループに対してポリシーを作成する場合、グループの一部のメンバーが特定のポリシー設定の例外を必要とすることがあります。例外は、次の方法で作成できます。

- 例外を必要とするグループメンバーのみにポリシーを作成し、そのポリシーをグループ全体のポリシーよりも上位にランク付けする
- ポリシーに追加された割り当てに拒否モードを使用する

モードが拒否に設定された割り当ては、割り当て条件に一致しない接続にのみポリシーを適用します。たとえば、ポリシーには次の割り当てが含まれます。

- 割り当てAは、範囲208.77.88.*を指定するクライアントIPアドレス割り当てです。モードは許可に設定されています。
- 割り当てBは、特定のユーザーアカウントを指定するユーザー割り当てです。モードは拒否に設定されています。

ポリシーは、割り当てAで指定された範囲のIPアドレスを使用してサイトにログオンするすべてのユーザーに適用されます。ただし、割り当てBで指定されたユーザーアカウントを使用してサイトにログオンするユーザーには、ポリシーは適用されません。

接続に適用されるポリシーを決定する

複数のポリシーが適用されるため、接続が期待どおりに応答しない場合があります。優先度の高いポリシーが接続に適用される場合、元のポリシーで構成した設定が上書きされることがあります。ポリシーの結果セットを計算し、接続に対して最終的なポリシー設定がどのようにマージされるかを判断できます。

次のような方法でポリシーの結果セットを計算できます。

- **Citrix Group Policy Modeling** ウィザードを使用して接続シナリオをシミュレートし、Citrixポリシーがどのように適用されるかを判断します。接続シナリオの条件として、次のようなものを指定できます。
    - ドメインコントローラー
    - ユーザー
    - Citrixポリシー割り当ての証拠値
    - 低速ネットワーク接続などのシミュレートされた環境設定 ウィザードが生成するレポートには、シナリオで有効になるCitrixポリシーが一覧表示されます。ドメインユーザーとしてControllerにログオンするため、ウィザードはサイトポリシー設定とActive Directoryグループポリシーオブジェクト (GPO) の両方を使用して結果を計算します。
- **グループポリシーの結果**を使用して、特定のユーザーとコントローラーに適用されるCitrixポリシーを記述したレポートを作成します。グループポリシーの結果ツールは、環境内のGPOの現在の状態を評価するのに役立ち、レポートを生成します。生成されたレポートには、Citrixポリシーを含むこれらのオブジェクトが、特定のユーザーとコントローラーに現在どのように適用されているかが記述されています。

Web StudioでCitrix Group Policy Modelingウィザードを起動できます。または、Windowsのグループポリシー管理コンソールからグループポリシーの結果ツールを起動することもできます。

Web Studioを使用して作成されたサイトポリシー設定は、次の場合、ポリシーの結果セットに含まれません。

- グループポリシー管理コンソールからCitrixグループポリシーモデリングウィザードを実行する場合
- グループポリシー管理コンソールからグループポリシーの結果ツールを実行する場合

最も包括的なポリシーの結果セットが得られることを確認するには、グループポリシー管理コンソールのみを使用してポリシーを作成する場合を除き、Citrix Group Policy Modelingウィザードを Web Studioから起動することをお勧めします。

ポリシーのトラブルシューティング

ユーザー、IPアドレス、およびその他の割り当てられたオブジェクトには、同時に適用される複数のポリシーが存在する場合があります。このシナリオでは、ポリシーが期待どおりに動作しない競合が発生する可能性があります。Citrixグループポリシーモデリングウィザードまたはグループポリシー結果ツールを実行すると、ユーザー接続にポリシーが適用されていないことが判明する場合があります。このようなシナリオでは、ポリシー評価基準に一致する条件下でアプリケーションやデスクトップに接続するユーザーには、ポリシー設定が適用されません。この状況は、次の場合に発生します。

- ポリシー評価基準に一致する割り当てを持つポリシーがない場合。
- 割り当てに一致するポリシーに設定が構成されていない場合。
- 割り当てに一致するポリシーが無効になっている。

指定された基準を満たす接続にポリシー設定を適用したい場合は、以下を確認してください。

- それらの接続に適用したいポリシーが有効になっていること。
- 適用したいポリシーに適切な設定が構成されていること。

デフォルトのポリシー設定

以下の表に、ポリシー設定、そのデフォルト値、および適用されるVirtual Delivery Agent (VDA)のバージョンを示します。

ICA®

名前	デフォルト設定	VDA
アダプティブトランスポート	オフ。優先される場合に使用します	VDA 7.13～7.15、VDA 7.16以降
クライアントクリップボードリダイレクト	許可	すべてのVDAバージョン
クライアントクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6 以降
デスクトップの起動	禁止	マルチセッションOS用VDA 7以降
ICAリスナーポート番号	1494	すべてのVDAバージョン
クライアント接続中の非公開プログラムの起動	禁止	マルチセッションOS 7以降のVDA
クリップボードのクライアントからセッションへの転送サイズを制限	無効	VDA 2009
クリップボードのセッションからクライアントへの転送サイズを制限	無効	VDA 2009
損失許容モード	許可	VDA 2003。注：損失許容モードはまだ利用できません。このバージョンのVDAは、利用可能になった時点でそれをサポートします。
損失許容しきい値	損失許容モードが利用可能な場合：パケット損失：5%、遅延：300ミリ秒（RTT）	VDA 2003から現在まで
ランデブープロトコル	無効	Citrix Cloudを介して確立されたHDXセッションにのみ適用されます。

名前	デフォルト設定	VDA
クライアントクリップボードへの書き込みを制限	禁止	VDA 7.6から現在まで
セッションクリップボードへの書き込みを制限	禁止	VDA 7.6から現在まで
セッションクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6から現在まで
タブレットモードの切り替え	有効	VDA 7.16から現在まで。VDA 7.14および7.15 LTSRの場合は、レジストリを使用してこの設定を構成します。
仮想チャネル許可リスト	有効	VDA 2109から現在まで

ICA/Adobe Flash 配信/Flash リダイレクト

名前	デフォルト設定	VDA
Flashビデオのフォールバック防止	未構成	VDA 7.6 FP3 から現在まで
Flashビデオのフォールバック防止エラー *.swf	VDA 7.6 FP3 から現在まで	

ICA/オーディオ

名前	デフォルト設定	VDA
アダプティブオーディオ	有効	Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAの、シングルセッションOSおよびマルチセッションOSの両方のセッションに適用されます。
UDP経由のオーディオリアルタイムトランスポート	許可	すべてのVDAバージョン

名前	デフォルト設定	VDA
オーディオプラグアンドプレイ	許可	マルチセッションOS用VDA 7以降
オーディオ品質	高 - 高品位オーディオ	すべてのVDAバージョン
クライアントオーディオリダイレクト	許可	すべてのVDAバージョン
クライアントマイクのリダイレクト	許可	すべてのVDAバージョン

ICA/クライアント自動再接続

名前	デフォルト設定	VDA
クライアント自動再接続	許可	すべてのVDAバージョン
クライアント自動再接続認証	認証を要求しない	すべてのVDAバージョン
クライアント自動再接続ログ	自動再接続イベントをログに記録しない	すべてのVDAバージョン
クライアント自動再接続タイムアウト	120秒	VDA 7.13から現在まで
再接続UIの透過レベル	80%	VDA 7.13から現在まで

ICA/帯域幅

名前	デフォルト設定	VDA
オーディオリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
オーディオリダイレクト帯域幅制限率	0	すべてのVDAバージョン
クライアントUSBデバイスリダイレクト帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以

名前	デフォルト設定	VDA
		降、シングルセッションOS用VDA 7以降
クライアントUSBデバイスリダイレクト帯域幅制限率	0	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
クリップボードリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
クリップボードリダイレクト帯域幅制限の割合	0	すべてのVDAバージョン
COMポートリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
COMポートリダイレクト帯域幅制限の割合	0	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
ファイルリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
ファイルリダイレクト帯域幅制限 (%)	0	すべてのVDAバージョン
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、Multi-session OS用VDA 7およびSingle-session OS用VDA 7から現在のMulti-session OS用VDAおよびSingle-session OS用VDAまで
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限 (%)	0	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで

名前	デフォルト設定	VDA
LPTポートリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
LPTポートリダイレクト帯域幅制限 (%)	0	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
セッション全体の帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクトの帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクトの帯域幅制限の割合	0	すべてのVDAバージョン
TWAINデバイスリダイレクトの帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
TWAINデバイスリダイレクトの帯域幅制限の割合	0	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/双方向コンテンツリダイレクト

名前	デフォルト設定	VDA
双方向コンテンツリダイレクトを許可する	禁止	VDA 7.13 以降
クライアントにリダイレクトされる許可されたURL	空	VDA 7.13 以降
VDAにリダイレクトされる許可されたURL	空	VDA 7.13 以降

名前	デフォルト設定	VDA
クライアントからホスト (VDA) およびクライアントからクライアントへの双方向コンテンツリダイレクト	Citrix Workspace™アプリのグループポリシーオブジェクト管理用テンプレートを使用する	

ICA/ブラウザコンテンツリダイレクト

名前	デフォルト設定	VDA
ブラウザコンテンツリダイレクト	許可	VDA 7.16から現在まで
ブラウザコンテンツリダイレクトACL構成	`https://www.youtube.com/*`	VDA 7.16から現在まで
ブラウザコンテンツリダイレクト統合Windows認証サポート	禁止	VDA 2106から現在まで
ブラウザコンテンツリダイレクトプロキシ構成	空	VDA 7.16 以降
ブラウザコンテンツリダイレクトのサーバーフェッチWebプロキシ認証	禁止	VDA 2012 以降

ICA/クライアントセンサー

名前	デフォルト設定	VDA
アプリケーションによるクライアントデバイスの物理的な場所の使用を許可する	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで

ICA/デスクトップUI

名前	デフォルト設定	VDA
デスクトップコンポジションリダイレクト	無効 (7.6 FP3から現在まで); 有効 (5.6から7.6 FP2まで)	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップコンポジションリダイレクトのグラフィック品質	中	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップの壁紙	許可	すべてのVDAバージョン
メニューアニメーション	許可	すべてのVDAバージョン
ドラッグ中にウィンドウの内容を表示	許可	すべてのVDAバージョン

ICA/エンドユーザー監視

名前	デフォルト設定	VDA
ICAラウンドトリップ計算	有効	すべてのVDAバージョン
ICAラウンドトリップ計算間隔	15秒	すべてのVDAバージョン
アイドル接続のICAラウンドトリップ計算	無効	すべてのVDAバージョン

ICA/強化されたデスクトップエクスペリエンス

名前	デフォルト設定	VDA
強化されたデスクトップエクスペリエンス	許可	マルチセッションOS 7以降のVDA

ICA/ファイルリダイレクト

名前	デフォルト設定	VDA
クライアントドライブの自動接続	許可	すべてのVDAバージョン
クライアントドライブのリダイレクト	許可	すべてのVDAバージョン
クライアント固定ドライブ	許可	すべてのVDAバージョン
クライアントフロッピードライブ	許可	すべてのVDAバージョン
クライアントネットワークドライブ	許可	すべてのVDAバージョン
クライアント光学ドライブ	許可	すべてのVDAバージョン
クライアントリムーバブルドライブ	許可	すべてのVDAバージョン
ホストからクライアントへのリダイレクト	無効	マルチセッションOS向けVDA 7以降
クライアントドライブ文字を保持する	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS向けVDA 7以降
読み取り専用クライアントドライブアクセス	無効	VDA 5.5、5.6 FP1、マルチセッションOS向けVDA 7以降、シングルセッションOS向けVDA 7以降
特殊フォルダーのリダイレクト	許可	Web Interface展開のみ。マルチセッションOS向けVDA 7以降
非同期書き込みを使用する	無効	すべてのVDAバージョン

ICA/グラフィック

名前	デフォルト設定	VDA
視覚的にロスレスな圧縮を許可	無効	VDA 7.6から現在まで
表示メモリ制限	65,536 Kb	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7から現在まで
表示モードの劣化優先順位	まず色深度を劣化させる	すべてのVDAバージョン
動的ウィンドウプレビュー	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
グラフィックステータスインジケーター	無効	VDA 7.16以降
画像キャッシュ	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
レガシーグラフィックモード	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
最大許容色深度	32ビット/ピクセル	すべてのVDAバージョン
表示モードが低下したときにユーザーに通知	無効	マルチセッションOS用VDA 7以降
3Dグラフィックワークロード向けに最適化	無効	VDA 7.17以降
キューイングとトッシング	有効	すべてのVDAバージョン
画面共有	無効	VDA 2112
圧縮にビデオコーデックを使用	優先される場合にビデオコーデックを使用	VDA 7.6 FP3以降

名前	デフォルト設定	VDA
ビデオコーデックにハードウェアエンコードを使用	有効	VDA 7.11 から現在まで

ICA/グラフィック/キャッシュ

名前	デフォルト設定	VDA
永続キャッシュしきい値	300万 bps	マルチセッションOS用VDA 7 から現在まで

ICA/グラフィック/Framehawk

名前	デフォルト設定	VDA
Framehawk ディスプレイチャネル	無効	VDA 7.6 FP2 から現在まで
Framehawk ディスプレイチャネルポート範囲	3224,3324	VDA 7.6 FP2 から現在まで

ICA/キープアライブ

名前	デフォルト設定	VDA
ICAキープアライブタイムアウト	60秒	すべてのVDAバージョン
ICAキープアライブ	ICAキープアライブメッセージを送信しない	すべてのVDAバージョン

ICA/キーボードおよびIME

名前	デフォルト設定	VDA
クライアントキーボードレイアウト同期およびIMEの改善	無効	1912 LTSR CU2以降にのみ適用されます。
Unicode キーボードレイアウトマッピングを有効にする	禁止	1912 LTSR CU2以降にのみ適用されます。

名前	デフォルト設定	VDA
キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする	禁止	1912 LTSR CU2以降にのみ適用されます。

ICA/ローカルアプリアクセス

名前	デフォルト設定	VDA
ローカルアプリアクセスを許可	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクトブロックリスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクト許可リスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/モバイルエクスペリエンス

名前	デフォルト設定	VDA
キーボードの自動表示	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
タッチ最適化デスクトップの起動	許可	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降。この設定は、Windows 10およびWindows Server 2016マシンでは無効になっており、利用できません。
コンボボックスのリモート処理	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シ

名前	デフォルト設定	VDA
		ングルセッションOS用VDA 7以降

ICA/マルチメディア

名前	デフォルト設定	VDA
HTML5ビデオリダイレクト	禁止	VDA 7.12以降
ビデオ品質の制限	未構成	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Microsoft Teamsリダイレクト	許可	マルチセッションOS用VDA 1906以降、シングルセッションOS用VDA 1906以降。
マルチメディア会議	許可	すべてのVDAバージョン
WAN経由のWindows Media マルチメディアリダイレクトの最適化	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WAN経由のWindows Media マルチメディアリダイレクトの最適化にGPUを使用	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Windows Mediaフォールバック防止	未構成	VDA 7.6 FP3 から現在まで
Windows Media クライアント側コンテンツ取得	許可	マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで
Windows Media リダイレクト	許可	すべてのVDAバージョン
Windows Media リダイレクトバッファサイズ	5秒	VDA 5、5.5、5.6 FP1 から現在まで

名前	デフォルト設定	VDA
Windows Media リダイレクトバッファサイズの使用	無効	VDA 5、5.5、5.6 FP1 から現在まで

ICA/マルチストリーム接続

名前	デフォルト設定	VDA
UDP経由のオーディオ	許可	VDA for Multi-session OS 7から現在まで
オーディオUDPポート範囲	16500、16509	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチポートポリシー	プライマリポート (2598) は高優先度	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム コンピューター設定	無効	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム ユーザー設定	無効	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム仮想チャネルストリーム割り当て設定	デフォルトのストリーム割り当てについては、マルチストリーム仮想チャネル割り当て設定を参照してください。	VDA 2003

ICA/ポートリダイレクト

名前	デフォルト設定	VDA
クライアントCOMポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0～7.8の場合、この設定はレジストリを使用して構成します。
クライアントLPTポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0から7.8では、レジストリを使用してこの設定を構成します。
クライアントCOMポートリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0から7.8では、レジストリを使用してこの設定を構成します。
クライアントLPTポートリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0から7.8では、レジストリを使用してこの設定を構成します。

ICA/印刷

名前	デフォルト設定	VDA
クライアントプリンターリダイレクト	許可	すべてのVDAバージョン
デフォルトプリンター	クライアントのメインプリンターを既定のプリンターに設定する	すべてのVDAバージョン
プリンターの割り当て	ユーザーの現在のプリンターがセッションの既定のプリンターとして使用されます	すべてのVDAバージョン
プリンターの自動作成イベントログ設定	エラーと警告をログに記録する	すべてのVDAバージョン

名前	デフォルト設定	VDA
セッションプリンター	プリンターは指定されていません	すべてのVDAバージョン
プリンターが作成されるまで待機する（デスクトップ）	無効	すべてのVDAバージョン

ICA/印刷/クライアントプリンター

名前	デフォルト設定	VDA
クライアントプリンターを自動作成	すべてのクライアントプリンターを自動作成	すべてのVDAバージョン
汎用ユニバーサルプリンターを自動作成	無効	すべてのVDAバージョン
クライアントプリンター名	標準プリンター名	VDA 5.6
プリントサーバーへの直接接続	有効	すべてのVDAバージョン
プリンタードライバーのマッピングと互換性	ルールは指定されていません	すべてのVDAバージョン
プリンタープロパティの保持	クライアントに保存されていない場合にのみプロファイルに保持	すべてのVDAバージョン
保持および復元されたクライアントプリンター	許可	VDA 5、5,5、5.6 FP1

ICA/Printing/Drivers

名前	デフォルト設定	VDA
インボックスプリンタードライバーの自動インストール	有効	すべてのVDAバージョン
ユニバーサルドライバーの優先順位	EMF; XPS; PCL5c; PCL4; PS	すべてのVDAバージョン

名前	デフォルト設定	VDA
ユニバーサルプリントドライバーの使用	要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	すべてのVDAバージョン

ICA/印刷/ユニバーサルプリントサーバー

名前	デフォルト設定	VDA
ユニバーサルプリントサーバーを有効にする	無効	すべてのVDAバージョン
ユニバーサルプリントサーバー印刷データストリーム (CGP) ポート	7229	すべてのVDAバージョン
ユニバーサルプリントサーバー印刷ストリーム入力帯域幅制限 (kbps)	0	すべてのVDAバージョン
ユニバーサルプリントサーバーWebサービス (HTTP/SOAP) ポート	8080	すべてのVDAバージョン
負荷分散用のUniversal Print Server	VDA バージョン 7.9 から現在まで	
ユニバーサルプリントサーバーのサービス停止しきい値	180 (秒)	VDA バージョン 7.9 から現在まで

ICA/印刷/ユニバーサル印刷

名前	デフォルト設定	VDA
ユニバーサルプリントEMF処理モード	プリンターに直接スプールする	すべてのVDAバージョン
ユニバーサルプリント画像圧縮制限	最高品質 (ロスレス圧縮)	すべてのVDAバージョン

名前	デフォルト設定	VDA
ユニバーサルプリント最適化の既定値	画像圧縮: 希望する画質 = 標準品質, ヘビーウェイト圧縮を有効にする = False; 画像とフォントのキャッシュ: 埋め込み画像のキャッシュを許可する = True; 管理者以外のユーザーによるこれらの設定の変更を許可する = False;	すべてのVDAバージョン
ユニバーサルプリントプレビュー設定	自動作成されたプリンターまたは汎用ユニバーサルプリンターには印刷プレビューを使用しない	すべてのVDAバージョン
ユニバーサルプリント印刷品質制限	制限なし	すべてのVDAバージョン

ICA/セキュリティ

名前	デフォルト設定	VDA
SecureICAの最小暗号化レベル	基本	マルチセッションOS用VDA 7以降

ICA/サーバー制限

名前	デフォルト設定	VDA
サーバーアイドルタイマー間隔	0ミリ秒	マルチセッションOS用VDA 7以降

ICA/セッション制限

名前	デフォルト設定	VDA
切断されたセッションタイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7から現在まで

名前	デフォルト設定	VDA
リモートPCアクセス切断セッションタイマー	無効	シングルセッションOS用VDA 7から現在まで
切断されたセッションタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7から現在まで
セッション接続タイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー	有効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

ICA/セッションの信頼性

名前	デフォルト設定	VDA
セッションの信頼性接続	許可	すべてのVDAバージョン
セッションの信頼性ポート番号	2598	すべてのVDAバージョン
セッションの信頼性タイムアウト	180秒	すべてのVDAバージョン

ICA/タイムゾーン制御

名前	デフォルト設定	VDA
レガシークライアントの現地時間を推定	有効	マルチセッションOS用VDA 7以降の現在バージョン
セッション切断時またはログオフ時にシングルセッションOSのタイムゾーンを復元する	有効	現在のVDAバージョン
クライアントのローカル時刻を使用する	サーバーのタイムゾーンを使用する	すべてのVDAバージョン

ICA/TWAINデバイス

名前	デフォルト設定	VDA
クライアントTWAINデバイスリダイレクト	許可	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
TWAIN圧縮レベル	中	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/USBデバイス

名前	デフォルト設定	VDA
クライアントUSBデバイス最適化規則	有効 (VDA 7.6 FP3以降); 無効 (VDA 7.11以降); デフォルトでは、規則は指定されていません	VDA 7.6 FP3以降
クライアントUSBデバイスリダイレクト	禁止	すべてのVDAバージョン

名前	デフォルト設定	VDA
クライアントUSBデバイスリダイレクト規則	規則は指定されていません	すべてのVDAバージョン
クライアントUSBプラグアンドプレイデバイスリダイレクト	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/ビジュアルディスプレイ

名前	デフォルト設定	VDA
単純なグラフィックの優先色深度	24ビット/ピクセル	VDA 7.6 FP3 以降
ターゲットフレームレート	30 フレーム/秒	すべてのVDAバージョン
視覚品質	中	VDA for マルチセッションOS 7以降、VDA for シングルセッションOS 7以降

ICA/視覚表示/動画

名前	デフォルト設定	VDA
最低画質	通常	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、Single-session OS 用 VDA 7 以降
動画圧縮	有効	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、Single-session OS 用 VDA 7 以降
プログレッシブ圧縮レベル	なし	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
プログレッシブ圧縮しきい値	2,147,483,647 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
ターゲット最小フレームレート	10 フレーム/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

注:

「**目標最小フレームレート**」ポリシーは廃止されました。

ICA/視覚表示/静止画像

名前	デフォルト設定	VDA
追加の色圧縮	無効	すべてのVDAバージョン
追加の色圧縮のしきい値	8,192 キロビット/秒	すべてのVDAバージョン
高負荷圧縮	無効	すべてのVDAバージョン
非可逆圧縮レベル	中	すべてのVDAバージョン
非可逆圧縮しきい値	2,147,483,647 ケービーピーエス	すべてのVDAバージョン

ICA/WebSockets

名前	デフォルト設定	VDA
WebSockets接続	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
WebSocketsポート番号	8008	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WebSockets信頼済みオリジンサーバーリスト	ワイルドカード「*」は、すべてのReceiver for Web URLを信頼するために使用されます	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

負荷管理

名前	デフォルト設定	VDA
同時ログオン許容数	2	マルチセッションOS用VDA 7以降
CPU使用率	無効	マルチセッションOS用VDA 7以降
CPU使用率から除外するプロセスの優先度	通常以下または低	マルチセッションOS用VDA 7以降
ディスク使用率	無効	マルチセッションOS用VDA 7以降
最大セッション数	250	マルチセッションOS用VDA 7以降
メモリ使用率	無効	マルチセッションOS向けVDA 7以降
メモリ使用量のベース負荷	ゼロ負荷: 768 MB	マルチセッションOS向けVDA 7以降

プロファイル管理/詳細設定

名前	デフォルト設定	VDA
自動構成を無効にする	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
問題が発生した場合にユーザーをログオフする	無効	すべてのVDAバージョン
ロックされたファイルへのアクセス時の再試行回数	5	すべてのVDAバージョン
ログオフ時にインターネットCookieファイルを処理する	無効	すべてのVDAバージョン

プロファイル管理/基本設定

名前	デフォルト設定	VDA
アクティブな書き戻し	無効	すべてのVDAバージョン
プロファイル管理を有効にする	無効	すべてのVDAバージョン
除外グループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン
オフラインプロファイルのサポート	無効	すべてのVDAバージョン
ユーザーストアへのパス	ウィンドウズ	すべてのVDAバージョン
ローカル管理者によるログオンの処理	無効	すべてのVDAバージョン
処理されるグループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン

プロファイル管理/クロスプラットフォーム設定

名前	デフォルト設定	VDA
クロスプラットフォーム設定ユーザーグループ	無効。処理済みグループで指定されたすべてのユーザーグループが処理されます。	すべてのVDAバージョン
クロスプラットフォーム設定を有効にする	無効	すべてのVDAバージョン
クロスプラットフォーム定義へのパス	無効。パスは指定されていません。	すべてのVDAバージョン
クロスプラットフォーム設定ストアへのパス	無効。Windows\PM_CMが使用されます。	すべてのVDAバージョン
クロスプラットフォーム設定の作成元	無効	すべてのVDAバージョン

プロファイル管理/ファイルシステム/除外

名前	デフォルト設定	VDA
除外リスト - ディレクトリ	無効。ユーザープロファイル内のすべてのフォルダーが同期されます。	すべてのVDAバージョン
除外リスト - ファイル	無効。ユーザープロファイル内のすべてのファイルが同期されます。	すべてのVDAバージョン

プロファイル管理/ファイルシステム/同期

名前	デフォルト設定	VDA
同期するディレクトリ	無効。除外されていないフォルダーのみが同期されます。	すべてのVDAバージョン
同期するファイル	無効。除外されていないファイルのみが同期されます。	すべてのVDAバージョン

名前	デフォルト設定	VDA
ミラーリングするフォルダー	無効。フォルダーはミラーリングされません。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト

名前	デフォルト設定	VDA
管理者アクセスを許可する	無効	すべてのVDAバージョン
ドメイン名を含める	無効	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/AppData(Roaming)

名前	デフォルト設定	VDA
AppData(Roaming)パス	無効。場所は指定されていません。	すべてのVDAバージョン
AppData(Roaming)のリダイレクト設定	コンテンツは、AppData(Roaming) パス ポリシー設定で指定された UNC パスにリダイレクトされます。	すべての VDA バージョン

プロファイル管理/フォルダーリダイレクト/連絡先

名前	デフォルト設定	VDA
連絡先パス	無効。場所は指定されていません。	すべての VDA バージョン
連絡先のリダイレクト設定	コンテンツは、**連絡先パス ポリシー**設定で指定された UNC パスにリダイレクトされます。	すべての VDA バージョン

プロファイル管理/フォルダーリダイレクト/デスクトップ

名前	デフォルト設定	VDA
デスクトップパス	無効。場所は指定されていません。	すべてのVDAバージョン
デスクトップのリダイレクト設定	コンテンツは、**デスクトップパスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ドキュメント

名前	デフォルト設定	VDA
ドキュメントパス	無効。場所は指定されていません。	すべてのVDAバージョン
ドキュメントのリダイレクト設定	コンテンツは、**ドキュメントパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ダウンロード

名前	デフォルト設定	VDA
ダウンロードパス	無効。場所は指定されていません。	すべてのVDAバージョン
ダウンロードのリダイレクト設定	コンテンツは、**ダウンロードパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/お気に入り

名前	デフォルト設定	VDA
お気に入りパス	無効。場所は指定されていません。	すべてのVDAバージョン

名前	デフォルト設定	VDA
お気に入りのリダイレクト設定	コンテンツは、**お気に入りパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/リンク

名前	デフォルト設定	VDA
リンクパス	無効。場所は指定されていません。	すべてのVDAバージョン
リンクのリダイレクト設定	コンテンツは、**リンクパスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ミュージック

名前	デフォルト設定	VDA
ミュージックパス	無効。場所は指定されていません。	すべてのVDAバージョン
ミュージックのリダイレクト設定	コンテンツは、**ミュージックパスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ピクチャ

名前	デフォルト設定	VDA
画像パス	無効。場所は指定されていません。	すべてのVDAバージョン
画像のリダイレクト設定	コンテンツは、**画像パスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/保存されたゲーム

名前	デフォルト設定	VDA
保存されたゲームのパス	無効。場所は指定されていません。	すべてのVDAバージョン
保存されたゲームのリダイレクト設定	コンテンツは、「**保存されたゲームのパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/検索

名前	デフォルト設定	VDA
検索パス	無効。場所は指定されていません。	すべてのVDAバージョン
検索のリダイレクト設定	コンテンツは、「**検索パスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/スタートメニュー

名前	デフォルト設定	VDA
スタートメニューのパス	無効。場所は指定されていません。	すべてのVDAバージョン
スタートメニューのリダイレクト設定	コンテンツは、スタートメニューのパスのポリシー設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ビデオ

名前	デフォルト設定	VDA
ビデオのパス	無効。場所は指定されていません。	すべてのVDAバージョン

名前	デフォルト設定	VDA
ビデオのリダイレクト設定	コンテンツは、**ビデオパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/ログ設定

名前	デフォルト設定	VDA
Active Directoryアクション	無効	すべてのVDAバージョン
共通情報	無効	すべてのVDAバージョン
共通の警告	無効	すべてのVDAバージョン
ログを有効にする	無効	すべてのVDAバージョン
ファイルシステムアクション	無効	すべてのVDAバージョン
ファイルシステム通知	無効	すべてのVDAバージョン
ログオフ	無効	すべてのVDAバージョン
ログオン	無効	すべてのVDAバージョン
ログファイルの最大サイズ	1048576	すべてのVDAバージョン
ログファイルへのパス	無効。ログファイルはデフォルトの場所 (%SystemRoot%\System32\Logfiles\UserProfileManager) に保存されます。	すべてのVDAバージョン
パーソナライズされたユーザー情報	無効	すべてのVDAバージョン
ログオン時とログオフ時のポリシー値	無効	すべてのVDAバージョン
レジストリアクション	無効	すべてのVDAバージョン
ログオフ時のレジストリの差異	無効	すべてのVDAバージョン

プロファイル管理/プロファイルの処理

名前	デフォルト設定	VDA
キャッシュされたプロファイルを削除するまでの遅延	0	すべてのVDAバージョン
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	すべてのVDAバージョン
ローカルプロファイルの競合処理	ローカルプロファイルを使用する	すべてのVDAバージョン
既存プロファイルの移行	ローカルとローミング	すべてのVDAバージョン
テンプレートプロファイルへのパス	無効。新しいユーザープロファイルは、ユーザーが最初にログオンしたデバイスのデフォルトユーザープロファイルから作成されます。	すべてのVDAバージョン
テンプレートプロファイルがローカルプロファイルを上書きする	無効	すべてのVDAバージョン
テンプレートプロファイルが移動プロファイルを上書きする	無効	すべてのVDAバージョン
すべてのログオンでCitrix®必須プロファイルとして使用されるテンプレートプロファイル	無効	すべてのVDAバージョン

プロファイル管理/レジストリ

名前	デフォルト設定	VDA
除外リスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン

名前	デフォルト設定	VDA
包含リスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン

プロファイル管理/ストリーム配信ユーザープロファイル

名前	デフォルト設定	VDA
常にキャッシュ	無効	すべてのVDAバージョン
常にキャッシュサイズ	0 MB	すべてのVDAバージョン
プロファイルストリーミング	無効	すべてのVDAバージョン
ストリーミングされたユーザープロファイルグループ	無効。OU内のすべてのユーザープロファイルは通常どおり処理されます。	すべてのVDAバージョン
保留中のエリアロックファイルのタイムアウト (日数)	1日	すべてのVDAバージョン

レシーバー

名前	デフォルト設定	VDA
StoreFront™アカウントリスト	ストアは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ユーザーパーソナライゼーションレイヤー

名前	デフォルト設定	VDA
ユーザーレイヤーリポジトリパス	無効。パスは指定されていません。	VDA 19.12以降のバージョン
ユーザーレイヤーサイズ (GB)	10 GB。ユーザーレイヤーは、設定されたサイズまで拡張されるシンプロビジョニン	VDA 19.12以降のバージョン

名前	デフォルト設定	VDA
	グディスクです。ユーザーレイヤーのサイズが小さくなることはありません。	

バーチャル デリバリー エージェント

名前	デフォルト設定	VDA
コントローラー登録IPv6ネットマスク	ネットマスクは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
コントローラー登録ポート	80	すべてのVDAバージョン
コントローラーSID	SIDは指定されていません	すべてのVDAバージョン
コントローラー	コントローラーは指定されていません	すべてのVDAバージョン
コントローラーの自動更新を有効にする	有効	マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで
IPv6コントローラー登録のみを使用する	無効	マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで
サイトGUID	GUIDは指定されていません	すべてのVDAバージョン

バーチャル デリバリー エージェント/HDX 3D Pro

名前	デフォルト設定	VDA
ロスレスを有効にする	有効	VDA 5.5、5.6 FP1
HDX 3D Pro品質設定	VDA 5.5、5.6 FP1	

バーチャル デリバリー エージェント/監視

名前	デフォルト設定	VDA
プロセス監視を有効にする	無効	VDA 7.11以降
リソース監視を有効にする	有効	VDA 7.11以降

仮想IP

名前	デフォルト設定	VDA
仮想IPループバックサポート	無効	VDA 7.6 以降
仮想IP仮想ループバックプログラムリスト	なし	VDA 7.6 以降

ポリシー設定リファレンス

ポリシーには、ポリシーが適用されるときに適用される設定が含まれます。このセクションの説明では、機能を有効にするためにより多くの設定が必要かどうか、または設定に類似しているかどうかも示しています。

クイックリファレンス

以下の表は、ポリシー内で構成できる設定を一覧表示しています。左側の列で実行したいタスクを見つけ、右側の列で対応する設定を見つけてください。

すべてのポリシー設定の完全なリストは、.CHM (コンパイル済み HTML) 形式および .CSV 形式で利用できます。これらのファイルは、ブローカー (デリバリーコントローラー) がインストールされているサーバーの `\program files\citrix\grouppolicy` フォルダーにあります。こちら をクリックして、ポリシー設定の最新バージョンをダウンロードすることもできます。

オーディオ

タスク	ポリシー設定
複数のオーディオデバイスの使用を許可するかどうかを制御する	オーディオプラグアンドプレイ
ユーザーデバイスのマイクからのオーディオ入力を許可するかどうかを制御する	クライアントマイクのリダイレクト

タスク	ポリシー設定
ユーザーデバイスのオーディオ品質を制御する	オーディオ品質
ユーザーデバイスのスピーカーへのオーディオマッピングを制御する	クライアントオーディオのリダイレクト

ユーザーデバイスの帯域幅

使用される帯域幅を制限するには	このポリシー設定を使用
クライアントオーディオマッピング	オーディオリダイレクトの帯域幅制限またはオーディオリダイレクトの帯域幅制限率
ローカルクリップボードを使用した切り取りと貼り付け	クリップボードリダイレクトの帯域幅制限またはクリップボードリダイレクトの帯域幅制限率
セッション内でのローカルクライアントドライブへのアクセス	ファイルリダイレクトの帯域幅制限またはファイルリダイレクトの帯域幅制限率
HDX™ MediaStream マルチメディアアクセラレーション	HDX MediaStream マルチメディアアクセラレーションの帯域幅制限またはHDX MediaStream マルチメディアアクセラレーションの帯域幅制限率
クライアントセッション	セッション全体の帯域幅制限
印刷	プリンターリダイレクト帯域幅制限またはプリンターリダイレクト帯域幅制限率
TWAINデバイス（カメラやスキャナーなど）	TWAINデバイスリダイレクト帯域幅制限またはTWAINデバイスリダイレクト帯域幅制限率
USBデバイス	クライアントUSBデバイスリダイレクト帯域幅制限またはクライアントUSBデバイスリダイレクト帯域幅制限率

クライアントドライブとユーザーデバイスのリダイレクト

このタスクの場合	このポリシー設定を使用
ユーザーがサーバーにログオンしたときに、ユーザーデバイス上のドライブを接続するかどうかを制御します	クライアントドライブの自動接続
サーバーとローカルクリップボード間のカットアンドペーストデータ転送を制御します	クライアントクリップボードリダイレクト
ユーザーデバイスからドライブがどのようにマップされるかを制御します	クライアントドライブリダイレクト
ユーザーのローカルハードドライブがセッションで利用可能かどうかを制御します	クライアント固定ドライブおよびクライアントドライブリダイレクト
ユーザーのローカルフロッピードライブをセッションで利用可能にするかどうかを制御します	クライアントフロッピードライブおよびクライアントドライブリダイレクト
ユーザーのネットワークドライブをセッションで利用可能にするかどうかを制御します	クライアントネットワークドライブおよびクライアントドライブリダイレクト
ユーザーのローカルCD、DVD、またはBlu-rayドライブをセッションで利用可能にするかどうかを制御します	クライアント光学ドライブおよびクライアントドライブリダイレクト
ユーザーのローカルリムーバブルドライブをセッションで利用可能にするかどうかを制御します	クライアントリムーバブルドライブおよびクライアントドライブリダイレクト
ユーザーのスキャナーやカメラなどのTWAINデバイスをセッションで利用可能にするかどうかを制御し、画像データ転送の圧縮を制御します	クライアントTWAINデバイスリダイレクト；TWAIN圧縮リダイレクト
USBデバイスをセッションで利用可能にするかどうかを制御します	クライアントUSBデバイスリダイレクトおよびクライアントUSBデバイスリダイレクト規則
WAN経由でクライアントディスクへのファイルの書き込みとコピーの速度を向上させます	非同期書き込みを使用する

コンテンツリダイレクト

このタスクの場合	このポリシー設定を使用する
サーバーからユーザーデバイスへのコンテンツリダイレクトを使用するかどうかを制御します	ホストからクライアントへのリダイレクト

デスクトップUI

このタスクの場合	このポリシー設定を使用する
ユーザーセッションでデスクトップの壁紙を使用するかどうかを制御します	デスクトップの壁紙
ウィンドウのドラッグ中にウィンドウの内容を表示します	ドラッグ中のウィンドウの内容を表示

グラフィックとマルチメディア

重要:

Flashポリシーは、古いVDAを使用している顧客が新しいコントローラー（たとえば、バージョン1912コントローラー）を使用し、引き続きFlashを使用できるようにするためにのみ残されています。このVDAバージョンはFlashをサポートしていません。

このタスクの場合	このポリシー設定を使用します
仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を制御します	ターゲットフレームレート
ユーザーデバイスに表示される画像の視覚品質を制御します	視覚品質
セッションでアクセスされたときにWebサイトがFlashコンテンツを表示できるかどうかを制御します	Flashサーバー側コンテンツ取得URLリスト。Flash URL互換性リスト。Flashビデオフォールバック防止ポリシー設定。Flashビデオフォールバック防止エラー*.swf

このタスクの場合	このポリシー設定を使用します
サーバーレンダリングされたビデオの圧縮を制御します	圧縮にビデオコーデックを使用。ビデオコーデックにハードウェアエンコーディングを使用
HTML5マルチメディアWebコンテンツのユーザーへの配信を制御します	HTML5ビデオリダイレクト

マルチストリームネットワークトラフィックの優先順位付け

このタスクの場合	このポリシー設定を使用
複数の接続にわたるICA®トラフィックのポートを指定し、ネットワークの優先順位を確立する	マルチポートポリシー
サーバーとユーザーデバイス間のマルチストリーム接続のサポートを有効にする	マルチストリーム（コンピューターとユーザーの設定）

印刷

このタスクの場合	このポリシー設定を使用する
ユーザーデバイスでのクライアントプリンターの作成を制御する	クライアントプリンターの自動作成とクライアントプリンターのリダイレクト
プリンタープロパティの保存場所を制御する	プリンタープロパティの保持
クライアントまたはサーバーのどちらが印刷要求を処理するかを制御する	印刷サーバーへの直接接続
ユーザーが自分のユーザーデバイスに接続されているプリンターにアクセスできるかどうかを制御する	クライアントプリンターのリダイレクト
クライアントプリンターとネットワークプリンターを自動作成する際のネイティブWindowsドライバーのインストールを制御します	インボックスプリンタードライバーの自動インストール

このタスクの場合	このポリシー設定を使用する
ユニバーサルプリンタードライバーを使用するタイミングを制御します	ユニバーサルプリントドライバーの使用
ローミングユーザーセッション情報に基づいてプリンターを選択します	既定のプリンター
ユニバーサルプリントサーバーの負荷分散とフェールオーバーしきい値を設定します	負荷分散用のユニバーサルプリントサーバー。ユニバーサルプリントサーバーのサービス停止しきい値

注：

ポリシーを使用して、デスクトップセッションまたはアプリケーションセッションでスクリーンセーバーを有効にすることはできません。スクリーンセーバーを必要とするユーザーの場合、スクリーンセーバーはユーザーデバイスに実装できます。

ICA® ポリシー設定

注:

このページでは、ICA ポリシー設定の説明とサポートされている構成値を提供します。ポリシーの操作の詳細については、ポリシーの操作セクションを参照してください。

アダプティブトランスポート

この設定は、EDT をプライマリとして、TCP をフォールバックとしてデータ転送を許可または防止します。

デフォルトでは、アダプティブトランスポートは有効（**優先**）になっており、可能な場合はEDTが使用され、TCPにフォールバックします。必要に応じて設定を変更できます。

- **優先**。可能な場合はEDT経由のアダプティブトランスポートが使用され、TCPにフォールバックします。
- **診断モード**。EDTが強制的にオンになり、TCPへのフォールバックが無効になります。この設定はトラブルシューティングの場合にのみ推奨されます。

- **オフ**。TCPが強制的にオンになり、EDTが無効になります。

詳細については、アダプティブトランスポートを参照してください。

ドラッグアンドドロップ設定

この設定は、クライアントと仮想アプリケーションまたはデスクトップの間でのファイルのドラッグを許可または防止します。デフォルトでは、ドラッグアンドドロップポリシーは無効になっています。必要に応じてこのポリシーを有効にできます。

アプリケーション起動待機タイムアウト

この設定は、セッションが最初のアプリケーションの起動を待機するミリ秒単位の待機タイムアウト値を指定します。アプリケーションの起動がこの期間を超えると、セッションは終了します。

デフォルトの時間（10,000ミリ秒）を選択するか、ミリ秒単位の数値を指定できます。

クライアントクリップボードリダイレクト

この設定は、ユーザーデバイスのクリップボードがサーバー上のクリップボードにマップされることを許可または禁止します。

デフォルトでは、クリップボードのリダイレクトは許可されています。

セッションとローカルクリップボード間のコピー＆ペーストデータ転送を禁止するには、**禁止**を選択します。ユーザーは、セッション内で実行されているアプリケーション間では引き続きデータをコピー＆ペーストできます。

この設定を許可した後、クライアント接続でクリップボードが消費できる最大許容帯域幅を構成します。**クリップボードリダイレクト帯域幅制限**または**クリップボードリダイレクト帯域幅制限率**の設定を使用します。

クライアントクリップボード書き込み許可形式

クライアントクリップボード書き込みを制限設定が**有効**の場合、ホストクリップボードデータはクライアントエンドポイントと共有できません。この設定を使用して、特定のデータ形式をクライアントエンドポイントクリップボードと共有することを許可できます。この設定を使用するには、有効にして、許可する特定の形式を追加します。

次のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT

- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

以下のカスタム形式は、XenApp and XenDesktop および Citrix Virtual Apps and Desktops™ で事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML形式はデフォルトで無効になっています。この機能を有効にするには：

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **クライアントクリップボード書き込みの制限**が**有効**に設定されていることを確認します。

- **クライアントクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

カスタム形式をさらに追加できます。カスタム形式名は、システムに登録される形式と一致する必要があります。形式名は大文字と小文字を区別します。

この設定は、**クライアントクリップボードリダイレクト**ポリシーが**禁止**に設定されている場合、または**クライアントクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合には適用されません。

> **注:**
>
> HTML形式のクリップボードコピーサポート（CF_HTML）を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを進める前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

クリップボードクライアントからセッションへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中にクライアントエンドポイントから仮想セッションに転送できるクリップボードデータの最大サイズを指定します。

クリップボードの転送サイズを制限するには、**クリップボードのクライアントからセッションへの転送サイズを制限する**設定を有効にします。次に、**サイズ制限**フィールドにキロバイト単位の値を入力して、ローカルクリップボードとセッション間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、クライアントからセッションへの転送に制限はありません。

HDX™ ダイレクト

HDX Directを使用すると、直接通信が可能な場合にクライアントがセッションホストとの直接接続を自動的に確立できます。接続はネットワークレベルの暗号化を使用して安全に確立されます。

HDX Direct モード

HDX Directは、内部クライアントおよび外部クライアントのセッションホストとの直接接続を確立するために使用できます。この設定は、HDX Directが内部クライアントのみに利用可能か、内部クライアントと外部クライアントの両方に利用可能かを決定します。

内部のみに設定されている場合、HDX Direct は内部ネットワーク内のクライアントに対してのみ直接接続を確立しようとします。

内部および**外部**に設定されている場合、HDX Direct は内部クライアントと外部クライアントの両方に対して直接接続を確立しようとします。

既定では、HDX Direct は内部クライアントのみに設定されています。

HDX Direct ポート範囲

外部ユーザーからの接続にHDX Directが使用するポートの範囲です。 デフォルトでは、HDX Directはポート範囲55000～55250を使用します。

クリップボードのセッションからクライアントへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中に仮想セッションからクライアントエンドポイントに転送できるクリップボードデータの最大サイズを指定します。

クリップボードの転送サイズを制限するには、**クリップボードのセッションからクライアントへの転送サイズを制限する**設定を有効にします。次に、**サイズ制限**フィールドにキロバイト単位の値を入力して、セッションとローカルクリップボード間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、セッションからクライアントへの転送に制限はありません。

クライアントクリップボードへの書き込みを制限する

この設定が**有効**になっている場合、ホストのクリップボードデータはクライアントエンドポイントと共有できません。**クライアントクリップボードへの書き込み許可形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボードへの書き込みを制限する

この設定が**有効**になっている場合、クライアントのクリップボードデータはセッションアプリケーションと共有できません。**セッションクリップボードへの書き込み許可形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボード書き込み許可形式

セッションクリップボードへの書き込みを制限する設定が**有効**になっている場合、クライアントのクリップボードデータはセッションアプリケーションと共有できません。この設定を使用して、特定のデータ形式をセッションクリップボードと共有することを許可できます。

以下のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

XenApp and XenDesktopおよびCitrix Virtual Apps and Desktopsでは、以下のカスタム形式が事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML形式はデフォルトで無効になっています。この機能を有効にするには:

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **セッションクリップボード書き込みの制限**が**有効**に設定されていることを確認します。
- **セッションクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

さらにカスタム形式を追加できます。カスタム形式名は、システムに登録される形式と一致する必要があります。形式名は大文字と小文字を区別します。

この設定は、**クライアントクリップボードリダイレクト**ポリシーが**禁止**に設定されている場合、または**セッションクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合には適用されません。

> **注:**
>
> HTML形式のクリップボードコピーサポート (CF_HTML) を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを進める前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

デスクトップの起動

この設定は、VDA Direct Access Usersグループ内の非管理者ユーザーがICA接続を使用してそのVDA上のセッションに接続することを許可または禁止します。

デフォルトでは、非管理者ユーザーはこれらのセッションに接続できません。

この設定は、RDP接続を使用しているVDA Direct Access Usersグループ内の非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合でもVDAに接続できます。この設定は、VDA Direct Access Usersグループに属していない非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合でもVDAに接続できません。

FIDO2リダイレクト

この設定は、FIDO2リダイレクトを有効または無効にします。FIDO2リダイレクトにより、ユーザーは仮想マシン内のローカルエンドポイントFIDO2コンポーネントを利用できます。ユーザーは、TPM 2.0とWindows Helloを搭載したデバイスで、FIDO2セキュリティキーまたは統合生体認証を介して仮想セッションを認証できます。

この設定が**許可**されている場合、ユーザーはローカルエンドポイント機能を使用してFIDO2認証を行うことができます。デフォルトでは、この設定は**許可**されています。

ICAリスナー接続タイムアウト

この設定は、ICAプロトコルを使用した接続が完了するまでの最大待機時間を指定します。

デフォルトでは、最大待機時間は120,000ミリ秒、つまり2分です。

ICAリスナーポート番号

この設定は、サーバー上のICAプロトコルによって使用されるTCP/IPポート番号を指定します。

デフォルトでは、ポート番号は1494に設定されています。

有効なポート番号は0～65535の範囲でなければならず、他のよく知られたポート番号と競合してはなりません。ポート番号を変更した場合は、新しい値を有効にするためにサーバーを再起動してください。サーバーでポート番号を変更した場合は、そのサーバーに接続するすべてのCitrix Workspace™アプリまたはプラグインでも変更する必要があります。

キーボードと入力方式エディター (IME)

この設定は、次の項目を有効または無効にします。

- 動的キーボードレイアウト同期
- 入力方式エディター (IME)
- Unicode キーボードレイアウトマッピング
- キーボードレイアウト切り替え通知ダイアログメッセージを非表示または表示します

1. Web Studioで、**キーボードとIME**を選択します。
2. VDAでの動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME) 機能を制御するには、**クライアントキーボードレイアウトの同期とIMEの改善**を選択します。設定できる項目は次のとおりです。

   無効 - 動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME)。

   動的クライアントキーボードレイアウト同期のサポート - 動的キーボードレイアウト同期を有効にします。

   動的クライアントキーボードレイアウト同期とIMEの改善のサポート - 動的キーボードレイアウト同期と汎用クライアント入力方式エディター (IME) の両方を有効にします。

3. Unicodeキーボードマッピングを有効または無効にするには、**Unicodeキーボードレイアウトマッピングを有効にする**を選択します。
4. ユーザーがクライアントキーボードレイアウトを変更したときに、キーボードレイアウトが同期中であることを示すメッセージを表示するかどうかを制御するには、**キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする**を選択します。メッセージが表示されないように設定した場合、ユーザーは誤った文字入力にならないように、入力する前に数秒待つ必要があります。

デフォルト設定：

- **クライアントキーボードレイアウトの同期とIMEの改善**
  - Windows Server 2016およびWindows Server 2019では無効。
  - Windows Server 2012およびWindows 2010における動的クライアントキーボードレイアウト同期とIMEの改善をサポートします。
- **Unicodeキーボードレイアウトマッピングを無効にする**
- **キーボードレイアウト切り替えポップアップメッセージボックスを表示する**

このポリシーは、ポリシー設定の**説明**セクションに記載されているレジストリ設定を置き換えます。

ログオフチェッカーの起動遅延

この設定は、ログオフチェッカーの起動を遅延させる期間を指定します。このポリシーを使用して、クライアントセッションがセッションを切断するまでに待機する時間（秒単位）を設定します。

この設定は、ユーザーがサーバーからログオフするのにかかる時間も増加させます。

ロス許容モード

> **重要:**
>
> - この機能には、Windows版Citrix Workspaceアプリ2002以降が必要です。VDAのこのバージョンは、利用可能になった時点でこれをサポートします。
> - 損失許容モードは、Citrix GatewayまたはCitrix Gateway Serviceではサポートされていません。このモードは、直接接続でのみ利用可能です。

この設定は、ロストトレラントモードを有効または無効にします。

デフォルトでは、ロストトレラントモードは**許可**されています。

許可されている場合、パケット損失と遅延がしきい値を超えると、このモードに入ります。しきい値は、ロス許容しきい値ポリシーを使用して設定できます。

ロス許容しきい値

(/ja-jp/citrix-virtual-apps-desktops/2311/policies/reference/ica-policy-settings.html#loss-tolerant-mode)が利用可能な場合、この設定は、セッションが損失許容モードに切り替わるネットワークメトリックのしきい値を指定します。

デフォルトのしきい値は次のとおりです。

- パケット損失: 5%
- 遅延: 300 ms (RTT)

詳細については、「損失許容モード」を参照してください。

Rendezvousプロトコル

この設定は、Citrix Gateway Serviceを使用する際のHDXセッションのプロキシ方法を変更します。有効にすると、HDXトラフィックはCitrix Cloud Connectorを経由しなくなります。代わりに、VDAはCitrix Gateway Serviceに直接アウトバウンド接続を確立します（Cloud Connectorのスケーラビリティが向上します）。

重要:

Citrix Cloud™の機能トグルとHDXポリシー設定がこの機能を制御します。Citrix Cloudの機能トグルはデフォルトで有効になっており、HDX設定はデフォルトで無効になっています。HDX設定は、Citrix Gateway Serviceを介して確立されたHDXセッションにのみ影響します。この設定は、クライアントとVDA間で直接、またはオンプレミスのCitrix Gatewayを介して確立されたセッションには影響しません。

詳細については、「Rendezvousプロトコル」を参照してください。

Rendezvousプロキシ構成

この設定により、Rendezvousプロトコルで使用する明示的なプロキシを構成できます。透過型プロキシを使用している場合、この設定を有効にする必要はありません。

デフォルトでは、この設定は無効になっています。

無効にすると、VDAはGateway ServiceとのRendezvous接続を確立しようとするときに、非透過型プロキシを介してアウトバウンドトラフィックをルーティングしません。

有効にすると、VDAはこの設定で定義されたプロキシを介してGateway ServiceとのRendezvous接続を確立しようとします。

VDAは、Rendezvous接続にHTTPおよびSOCKS5プロキシの使用をサポートしています。Rendezvous接続にプロキシを使用するようにVDAを構成するには、この設定を有効にする必要があります。また、プロキシのアドレスまたはPACファイルへのパスを指定します。例：

- プロキシアドレス: `http://<URL or IP>:<port>` または `socks5://<URL or IP>:<port>`
- PACファイル: `http://<URL or IP>/<path>/<filename>.pac`

  VDAバージョン2103は、PACファイルを使用したプロキシ構成でサポートされる最小バージョンです。SOCKS5プロキシのPACファイルスキーマの詳細については、「プロキシ構成」を参照してください。

> **注:**
>
> SOCKS5プロキシのみがEDTを介したデータ転送をサポートしています。HTTPプロキシの場合は、ICAのトランスポートプロトコルとしてTCPを使用してください。

> 詳細については、「Rendezvousプロトコル」を参照してください。

クライアント接続中の非公開プログラムの起動

この設定は、サーバー上でRDPを介して初期アプリケーションの起動を許可するかどうかを指定します。

デフォルトでは、サーバー上でRDPを介して初期アプリケーションを起動することは許可されていません。

タブレットモード切り替えポリシー設定

タブレットモード切り替えは、VDA上のストアアプリ、Win32アプリ、およびWindowsシェルンの外観と動作を最適化します。これは、電話やタブレットなどの小型デバイス、またはタッチ対応デバイスから接続するときに、仮想デスクトップを自動的にタブレットモードに切り替えることによって行われます。

このポリシーが無効になっている場合、VDAはユーザーが設定したモードになり、クライアントの種類に関係なく、そのモードを維持します。

自動クライアント再接続ポリシー設定

「**自動クライアント再接続**」セクションには、セッションの自動再接続を制御するためのポリシー設定が含まれています。

自動クライアント再接続

この設定は、接続が中断された後に同じクライアントによる自動再接続を許可または禁止します。

Citrix Receiver for Windows 4.7以降およびCitrix Workspaceアプリ1808以降では、自動クライアント再接続はCitrix Studioからのポリシー設定のみを使用します。Studioでこれらのポリシーを更新すると、自動クライアント再接続がサーバーからクライアントに同期されます。以前のバージョンのCitrix Receiver for Windowsで自動クライアント再接続を構成するには、Studioポリシーを使用し、レジストリまたはdefault.icaファイルを変更します。

自動クライアント再接続を許可すると、接続が切断されたときに中断された場所からユーザーが作業を再開できます。自動再接続は、切断された接続を検出し、ユーザーをセッションに再接続します。

セッションIDと資格情報へのキーを含むCitrix Workspace™アプリのCookieが使用されない場合、自動再接続によって新しいセッションが開始される可能性があります。つまり、既存のセッションに再接続するのではなく、新しいセッションが開始されます。Cookieの有効期限が切れている場合、Cookieは使用されません。たとえば、再接続の遅延や、資格情報の再入力が必要な場合などに、Cookieの有効期限が切れることがあります。ユーザーが意図的に切断した場合、自動クライアント再接続はトリガーされません。

再接続が進行中の場合、セッションウィンドウはグレー表示されます。カウントダウンタイマーは、セッションが再接続されるまでの残り時間を表示します。セッションがタイムアウトすると、切断されます。

アプリケーションセッションの場合、自動再接続が許可されていると、通知領域にカウントダウンタイマーが表示されます。このタイマーは、セッションが再接続されるまでの残り時間を指定します。Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試みます。

ユーザーセッションの場合、自動再接続が許可されていると、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間セッションへの再接続を試みます。デフォルトでは、この期間は2分です。この期間を変更するには、ポリシーを編集します。

デフォルトでは、自動クライアント再接続は許可されています。ポリシーを**禁止**に設定することで無効にできます。

自動クライアント再接続認証

この設定は、自動クライアント再接続に認証が必要かどうかを指定します。

ユーザーが最初にログオンすると、資格情報は暗号化され、メモリに保存され、暗号化キーを含むCookieが作成されます。このCookieはCitrix Workspaceアプリに送信されます。この設定が構成されている場合、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続しようとすると、資格情報を要求するダイアログボックスがユーザーに表示されます。

デフォルトでは、認証は不要です。

自動クライアント再接続ログ

この設定は、イベントログへの自動クライアント再接続の記録を有効または無効にします。

ログが有効な場合、サーバーのシステムログは、成功および失敗した自動再接続イベントに関する情報をキャプチャします。サイトは、すべてのサーバーの再接続イベントの統合ログを提供しません。

デフォルトでは、ログは無効になっています。

自動クライアント再接続のタイムアウト

デフォルトでは、自動クライアント再接続タイムアウトは120秒に設定されており、自動クライアント再接続タイムアウトの最大設定可能値は300秒です。このポリシーを使用して、タイムアウト値を設定します。

再接続UIの透明度レベル

この設定により、セッションの信頼性再接続中にXenAppまたはXenDesktop®セッションウィンドウに適用される不透明度レベルを指定できます。

デフォルトでは、再接続UIの透明度は80%に設定されています。

オーディオポリシー設定

オーディオセクションには、パフォーマンスを低下させることなく、ユーザーデバイスがセッションでオーディオを送受信できるようにするポリシー設定が含まれています。

アダプティブオーディオ

この設定は、アダプティブオーディオを有効または無効にします。このポリシーを有効にすると、最高のユーザーエクスペリエンスを提供するために、オーディオ品質設定が動的に調整されます。

この設定は、Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAのシングルセッションOSおよびマルチセッションOSセッションの両方に適用されます。

この設定が禁止されている場合、オーディオ品質ポリシーが適用されます。詳細については、オーディオ品質を参照してください。

デフォルトでは、アダプティブオーディオポリシーは有効になっています。

UDPリアルタイムトランスポート経由のオーディオ

この設定は、User Datagram Protocol (UDP) を使用してRTP経由でVDAとユーザーデバイス間でオーディオを送受信することを許可または禁止します。この設定が無効になっている場合、オーディオはTCP経由で送受信されます。

デフォルトでは、UDP経由のオーディオは許可されています。

オーディオプラグアンドプレイ

この設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。

デフォルトでは、複数のオーディオデバイスの使用は許可されています。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

オーディオ品質

この設定は、ユーザーセッションで受信されるサウンドの品質レベルを指定します。

デフォルトでは、サウンド品質は「高 - 高精細オーディオ」に設定されています。

サウンド品質を制御するには、次のいずれかのオプションを選択します。

- 「低」を選択 - 低帯域幅接続の低速接続用。ユーザーデバイスに送信されるサウンドは最大16 Kbpsに圧縮されます。この圧縮により、音質が大幅に低下します。しかし、低帯域幅接続でも妥当なパフォーマンスを可能にします。
- 「中」を選択 - 音声に最適化されており、Voice over Internet Protocolアプリケーションを提供します。この設定は、512 Kbps未満の回線、または著しい輻輳やパケット損失があるような、困難なネットワーク接続でメディアアプリケーションを提供します。このコーデックはエンコード時間が速く、サーバー側のメディア処理が必要な場合にソフトフォンやユニファイドコミュニケーションアプリケーションでの使用に最適です。

  ユーザーデバイスに送信されるオーディオは最大64 Kbpsに圧縮されます。この圧縮により、ユーザーデバイスで再生されるオーディオの品質は中程度に低下しますが、低遅延で低帯域幅

を消費します。Voice over Internet Protocolの品質が不十分な場合は、「Audio over UDP Real-time Transport」ポリシー設定が「許可」に設定されていることを確認してください。

現在、UDPを介したリアルタイムトランスポート（RTP）は、このオーディオ品質が選択されている場合にのみサポートされます。低速（512 Kbps未満）回線のような困難なネットワーク接続でメディアアプリケーションを配信する場合でも、このオーディオ品質を使用してください。また、ネットワークに輻輳やパケット損失がある場合も同様です。

- 「高」を選択 - 帯域幅が豊富で音質が重要な接続には、高精細オーディオを使用します。クライアントはネイティブレートでサウンドを再生できます。サウンドはCD品質まで維持される高音質レベルで圧縮され、最大112 Kbpsの帯域幅を使用します。この量のデータを送信すると、CPU使用率の増加やネットワークの輻輳が発生する可能性があります。

帯域幅は、オーディオの録音または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。

最大帯域幅を指定するには、**オーディオリダイレクト帯域幅制限**または**オーディオリダイレクト帯域幅制限率**の設定を構成します。

クライアントオーディオリダイレクト

この設定は、サーバーでホストされているアプリケーションが、ユーザーデバイスにインストールされているサウンドデバイスを介してサウンドを再生できるかどうかを指定します。この設定は、ユーザーがオーディオ入力を録音できるかどうかも指定します。

デフォルトでは、オーディオリダイレクトは許可されています。

この設定を許可した後、オーディオの再生または録音によって消費される帯域幅を制限できます。オーディオによって消費される帯域幅の量を制限すると、アプリケーションのパフォーマンスが向上する可能性がありますが、オーディオ品質が低下する可能性もあります。帯域幅は、オーディオの録音または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。最大帯域幅を指定するには、**オーディオリダイレクト帯域幅制限**または**オーディオリダイレクト帯域幅制限率**の設定を構成します。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、**オーディオプラグアンドプレイ**設定が有効になっていることを確認してください。

重要：クライアントオーディオリダイレクトを禁止すると、すべてのHDX™オーディオ機能が無効になります。

クライアントマイクのリダイレクト

この設定は、クライアントマイクのリダイレクトを有効または無効にします。有効にすると、ユーザーはセッションでマイクを使用してオーディオ入力を録音できます。

デフォルトでは、マイクのリダイレクトは許可されています。

セキュリティのため、信頼されていないサーバーがデバイスを介してマイクにアクセスしようとすると、ユーザーに警告が表示されます。ユーザーはアクセスを許可するかどうかを選択できます。ユーザーはCitrix Workspace™アプリでこの警告を無効にできます。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、オーディオプラグアンドプレイ設定が有効になっていることを確認してください。

ユーザーデバイスで**クライアントオーディオリダイレクト**設定が無効になっている場合、このルールは無効になります。

帯域幅ポリシー設定

「**帯域幅**」セクションには、クライアントセッションの帯域幅使用に関連するパフォーマンスの問題を回避するためのポリシー設定が含まれています。

重要：これらのポリシー設定を**マルチストリームポリシー**設定と併用すると、予期しない結果が生じる可能性があります。ポリシーでマルチストリーム設定を使用する場合は、これらの帯域幅制限ポリシー設定が含まれていないことを確認してください。

オーディオリダイレクト帯域幅制限

この設定は、ユーザーセッションでオーディオを再生または録音するために許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

オーディオリダイレクト帯域幅制限の割合

この設定は、オーディオの再生または録音に許可される最大帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合は、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クライアントUSBデバイスリダイレクト帯域幅制限

この設定は、USBデバイスのクライアントとの間のリダイレクトに許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クライアントUSBデバイスリダイレクト帯域幅制限パーセント**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

クライアントUSBデバイスリダイレクト帯域幅制限パーセント

この設定は、クライアントとの間でUSBデバイスをリダイレクトするために許可される最大帯域幅を、総セッション帯域幅のパーセンテージとして指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クライアントUSBデバイスリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クリップボードリダイレクト帯域幅制限

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クリップボードリダイレクト帯域幅制限パーセント**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

クリップボードリダイレクトの帯域幅制限（パーセント）

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を、総セッション帯域幅のパーセンテージとして指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クリップボードリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

COMポートリダイレクトの帯域幅制限

注: Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。「レジストリを使用してCOMポートおよびLPTポートのリダイレクト設定を構成する」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするための最大許容帯域幅をキロビット/秒で指定します。この設定に値を入力し、**COMポートリダイレクト帯域幅制限の割合**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

COMポートリダイレクト帯域幅制限の割合

注: Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。「レジストリを使用してCOMポートおよびLPTポートのリダイレクト設定を構成する」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**COMポートリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

ファイルリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントドライブにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**ファイルリダイレクト帯域幅制限の割合**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

ファイルリダイレクト帯域幅制限の割合

この設定は、クライアントドライブにアクセスするために許可される最大帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

既定では、最大値 (ゼロ) は指定されていません。

この設定と**ファイルリダイレクト帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合は、クライアントセッションで利用可能な帯域幅の合計量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

HDX™ MediaStreamマルチメディアアクセラレーション帯域幅制限

この設定は、HDX MediaStreamマルチメディアアクセラレーションを使用してストリーミングオーディオおよびビデオを配信するための最大許容帯域幅制限を指定します。最大許容帯域幅はキロビット/秒で指定されます。

既定では、最大値 (ゼロ) は指定されていません。

この設定と**HDX MediaStreamマルチメディアアクセラレーション帯域幅制限の割合**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

HDX MediaStreamマルチメディアアクセラレーション帯域幅制限の割合

この設定は、HDX MediaStreamマルチメディアアクセラレーションを使用してストリーミングオーディオおよびビデオを配信するための最大許容帯域幅を、セッション全体の帯域幅に対する割合として指定します。

既定では、最大値 (ゼロ) は指定されていません。

この設定と**HDX MediaStreamマルチメディアアクセラレーション帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合は、クライアントセッションで利用可能な帯域幅の合計量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

LPTポートリダイレクト帯域幅制限

注：Virtual Delivery Agent 7.0〜7.8の場合、この設定はレジストリを使用して構成します。「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一ユーザーセッションでLPTポートを使用する印刷ジョブに許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**LPTポートリダイレクト帯域幅制限パーセント**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

LPTポートリダイレクトの帯域幅制限（パーセント）

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一クライアントセッションでLPTポートを使用する印刷ジョブの帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**LPTポートリダイレクト帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

セッション全体の帯域幅制限

この設定は、ユーザーセッションで利用可能な帯域幅の総量をキロビット/秒で指定します。

強制可能な帯域幅の上限は20 Mbps（20,000 Kbps）です。デフォルトでは、最大値（ゼロ）は指定されていません。

クライアント接続によって消費される帯域幅の量を制限すると、クライアント接続外の他のアプリケーションが限られた帯域幅を競合している場合にパフォーマンスが向上する可能性があります。

プリンターリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントプリンターにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅はキロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**プリンターリダイレクト帯域幅制限率**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

プリンターリダイレクトの帯域幅制限（パーセント）

この設定は、クライアントプリンターにアクセスするために許可される最大帯域幅を、総セッション帯域幅の割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**プリンターリダイレクト帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

TWAINデバイスリダイレクト帯域幅制限

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**TWAINデバイスリダイレクト帯域幅制限率**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

TWAINデバイスリダイレクト帯域幅制限の割合

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**TWAINデバイスリダイレクト帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

双方向コンテンツリダイレクトポリシー設定

「**双方向コンテンツリダイレクト**」セクションには、クライアントからVDAへ、およびVDAからクライアントへのURLリダイレクトを有効または無効にするポリシー設定があります。

サーバーポリシーはStudioで設定されます。Citrix Workspace™アプリバージョン2311以降、この設定はStudioの以下の3つの非推奨のレガシー設定に代わるものです。

- 双方向コンテンツリダイレクトを許可する
- VDAにリダイレクトされる許可されたURL
- クライアントにリダイレクトを許可するURL

また、Windowsクライアントの以下の3つのローカルGPO設定も置き換えます。

- 双方向コンテンツリダイレクト
- 双方向コンテンツリダイレクトのオーバーライド
- OAuthリダイレクト

この設定が有効になっている場合、公開されたアプリまたはデスクトップに接続すると、双方向コンテンツリダイレクトを構成するためのクライアントからVDAへの設定がクライアントに送信されます。

この設定が構成されている場合、Studioおよびクライアント上のレガシー設定よりも優先されます。

VDAとDDCがバージョン2311以降を実行している場合、クライアントポリシーを設定してはなりません。そうでない場合、クライアントポリシーはCitrix Workspaceアプリのグループポリシーオブジェクト管理テンプレートから設定されます。

Citrix®は、ホストからクライアントへのリダイレクトと、クライアントからURLへのリダイレクトのためのローカルアプリアクセスを提供します。ただし、Citrixは、ドメイン参加済みWindowsクライアントには双方向コンテンツリダイレクトを使用することを推奨します。

Citrixは、Desktop Studioではなく、Web Studioの新しいUIを使用してこの機能を構成することを推奨しています。

ワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトするURLを定義する際にワイルドカードの使用をサポートします。双方向コンテンツリダイレクトの詳細と構成については、構成の手順を参照してください。 Web Studioで、`hostToClientUrls`配列または`clientToHostUrls`配列の`url`キーの値としてJSON文字列を編集して、ワイルドカードURLを設定します。

> **注:**
>
> - 無限ループを避けるため、`hostToClientUrls`と`clientToHostUrls`に同じURLを設定しないでください。
> - トップレベルドメインはサポートされていません。たとえば、`<https://www.citrix.*>`や`<http://www.citrix.co*>`はリダイレクトされません。

双方向コンテンツリダイレクトの構成

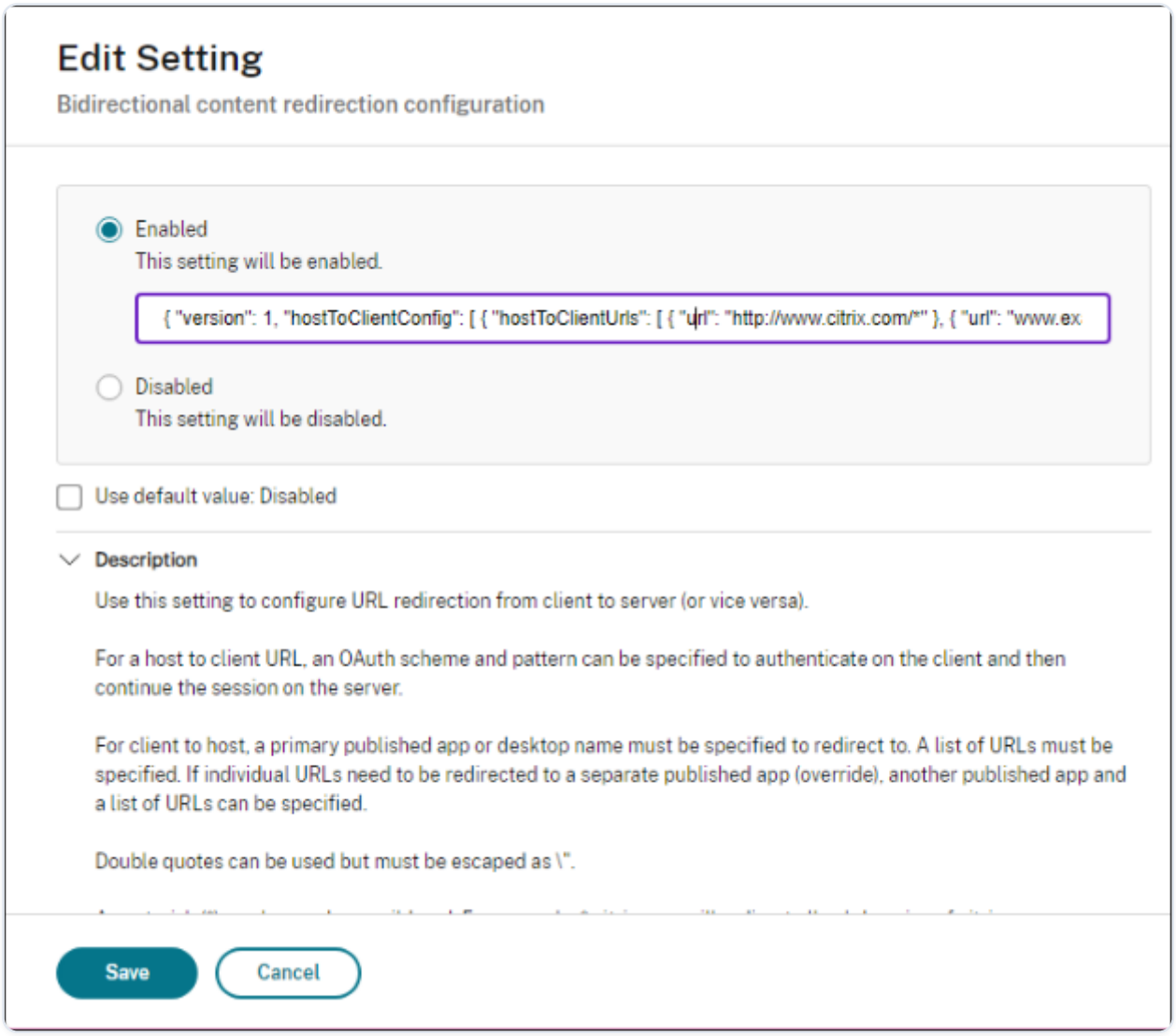
双方向コンテンツリダイレクトを構成するには、次の形式でJSON文字列を作成します。

```
{

  "version": 1,
```

```
  "hostToClientConfig": [
    {
      "hostToClientUrls": [
        {
          "url": "http://www.citrix.com/*"
        },
        {
          "url": "www.example.com"
        },
        {
          "url": "https://login.example.org/*",
          "oAuthRedirectionPattern": "https://login.example.org/
oauth2?.*",
          "oAuthScheme": "idm.desktop-authentication"
        }
      ]
    }
  ],
  "clientToHostConfig": [
    {
      "publishedAppOrDesktopNameType": "Desktop",
      "publishedAppOrDesktopName": "Win11Desktop",
```

```
      "clientToHostUrls": [
        "https://www.example.net",
        "https://*.citrix.example"
      ]
    },
    {
      "publishedAppOrDesktopNameType": "Application",
      "publishedAppOrDesktopName": "Chrome",
      "clientToHostUrls": [
        "https://tibco.example"
      ]
    }
  ]
}
```



次のパラメーターを設定する必要があります。

- version: (必須) 1に設定します。
- VDAからクライアントへのURLリダイレクトの場合、単一の `hostToClientConfig` を作成します。
- `hostToClientUrls`: (必須) ホスト (VDA) からクライアントにリダイレクトされるURLのリスト。ワイルドカードが許可されます。`*` が指定されている場合、`clientToHostConfig` は `publishedAppOrDesktopNameType`、空の `publishedAppOrDesktopName`、および空の `clientToHostUrls` とともに指定する必要があります。

OAuthリダイレクト

OAuthリダイレクトを使用すると、クライアントエンドポイントブラウザを使用して認証し、トークンをVDAに送り返すことができます。

利点:

- これらの資格情報をホストされた環境に保存することを回避できます。

- エンドポイントで利用可能で、VDAでは利用できない生体認証機能を使用できます。

URLのOAuthリダイレクトを構成するには、次のパラメーターを指定します。

- `oAuthRedirectionPattern`: (オプション) VDAからクライアントへのURLリダイレクトを介してクライアントにリダイレクトされると、OAuth認証フローが開始されたかのように追跡され、フローが完了したとき（結果のスキームまたはリダイレクトURLパターンが開かれたことによって検出される）、その結果のURLがそのフローを開始したホストVDAにリダイレクトされるURL正規表現。
- `oAuthScheme`: (オプション) スキームが指定されている場合、終了URLは`<scheme>`://`<something>`の形式であると想定されます。スキームが指定されていない（空である）場合、元の結果URLパターンは正規表現キャプチャグループ（パターンで指定する必要がある）を介してパターンから抽出され、元のURLは`citrix-oauth-redir://`リダイレクトURLを使用するように書き換えられます。フローが完了すると、元のリダイレクトURLはホスト（VDA）にリダイレクトされます。この場合、OAuth認証サーバーは`citrix-oauth-redir://byIndex/1 (2, 3, ... N)`リダイレクトURLを許可するように構成する必要があります。

クライアントからVDAへのリダイレクトの場合、リダイレクトする各リソースに対して`clientToHostConfig`を作成します。 各リソースには、次のパラメーターを含めます。

- `publishedAppOrDesktopNameType`: (必須) Studioで構成された公開デスクトップ（「Desktop」）または公開アプリケーション（「Application」）のいずれか。リソースが無効な場合、リダイレクトは正しく機能しません。
- `publishedAppOrDesktopName`: (必須) Studioで構成されたリソース名。
- `clientToHostUrls`: (必須) クライアントからホスト (VDA) にリダイレクトされるURLのリスト。ワイルドカードが許可されます。

ブラウザコンテンツリダイレクトポリシー設定

ブラウザコンテンツリダイレクトのセクションには、この機能を構成するためのポリシー設定が含まれています。

ブラウザコンテンツリダイレクトは、Citrix Virtual Apps and Desktops™ がユーザーにウェブブラウザコンテンツ（例：HTML5）を配信する方法を制御し、最適化します。コンテンツが表示されるブラウザの可視領域のみがリダイレクトされます。

HTML5ビデオのリダイレクトとブラウザコンテンツのリダイレクトは独立した機能です。この機能が動作するためにHTML5ビデオのリダイレクトポリシーは必要ありません。ただし、Citrix

HDX HTML5ビデオリダイレクトサービスはブラウザコンテンツのリダイレクトに使用されます。詳細については、「ブラウザコンテンツリダイレクト」を参照してください。

> **注:**
>
> Web Studioで利用可能なポリシー設定は、VDA上のレジストリキーで上書きできますが、レジストリキーはオプションです。

TLSとブラウザコンテンツリダイレクト

ブラウザコンテンツリダイレクトを使用してHTTPS Webサイトをリダイレクトできます。これらのWebサイトに挿入されるJavaScriptは、VDA上で実行されているCitrix HDX HTML5ビデオリダイレクトサービス（WebSocketService.exe）へのTLS接続を確立する必要があります。このリダイレクトを実現し、WebページのTLS整合性を維持するために、Citrix HDX HTML5ビデオリダイレクトサービスはVDA上の証明書ストアに2つのカスタム証明書を生成します。

HdxVideo.jsは、VDA上で実行されているWebSocketService.exeと通信するためにセキュアWebソケットを使用します。このプロセスはローカルシステムで実行され、SSL終端とユーザーセッションマッピングを実行します。

WebSocketService.exeは127.0.0.1ポート9001でリッスンしています。

ブラウザコンテンツリダイレクト

デフォルトでは、Citrix Workspace™アプリはクライアントフェッチとクライアントレンダリングを試行します。クライアントフェッチとクライアントレンダリングが失敗した場合、サーバーサイドレンダリングが試行されます。ブラウザコンテンツリダイレクトプロキシ構成ポリシーも有効にすると、Citrix Workspaceアプリはサーバーフェッチとクライアントレンダリングのみを試行します。

デフォルトでは、この設定は「許可」です。

ブラウザコンテンツリダイレクトの統合Windows認証サポート設定

ブラウザコンテンツリダイレクトは、認証にNegotiateスキームを使用するオーバーレイを有効にします。この機能強化により、VDAと同じドメイン内で統合Windows認証 (IWA) が構成されたWebサーバーへのシングルサインオンが提供されます。

許可に設定すると、ブラウザコンテンツリダイレクトオーバーレイは、ユーザーのVDA資格情報を使用してNegotiateチケットを取得します。その後、ユーザーはシングルサインオンでWebサーバーに認証します。

禁止に設定すると、ブラウザコンテンツリダイレクトオーバーレイは、VDAからNegotiateチケットを要求しません。ユーザーは基本認証方法を使用してWebサーバーに認証します。この認証方法では、ユーザーはWebサーバーにアクセスするたびにVDA資格情報を入力する必要があります。

デフォルトでは、この設定は禁止されています。

ブラウザコンテンツリダイレクトサーバーフェッチWebプロキシ認証設定

この設定は、オーバーレイで発生するHTTPトラフィックをダウンストリームWebプロキシ経由でルーティングします。ダウンストリームWebプロキシは、VDAユーザーのドメイン資格情報を使用して、Negotiate認証スキームを介してHTTPトラフィックを承認および認証します。

PACファイルで、ブラウザコンテンツリダイレクトプロキシ構成ポリシーを使用して、サーバーフェッチモードのブラウザコンテンツリダイレクトを構成する必要があります。PACスクリプトで、オーバーレイトラフィックをダウンストリームWebプロキシ経由でルーティングする手順を指定します。次に、ダウンストリームWebプロキシを構成して、Negotiate認証スキームを介してVDAユーザーを認証します。

許可に設定すると、Webプロキシは、**Proxy-Authenticate: Negotiate**ヘッダーを含む407 Negotiateチャレンジで応答します。その後、ブラウザコンテンツリダイレクトは、VDAユーザーのドメイン資格情報を使用してKerberosサービスチケットを取得します。また、その後のWebプロキシへの要求にはサービスチケットを含めます。

禁止に設定すると、ブラウザコンテンツリダイレクトは、オーバーレイとWebプロキシ間のすべてのTCPトラフィックを干渉することなくプロキシします。オーバーレイは、基本認証資格情報またはその他の利用可能な資格情報を使用してWebプロキシに認証します。

デフォルトでは、この設定は禁止されています。

ブラウザコンテンツリダイレクトアクセス制御リスト (ACL) ポリシー設定

この設定を使用して、ブラウザコンテンツリダイレクトを使用できる、またはブラウザコンテンツリダイレクトへのアクセスを拒否されるURLのアクセス制御リスト (ACL) を構成します。

承認されたURLは、コンテンツがクライアントにリダイレクトされる許可リスト内のURLです。

ワイルドカード `*` は許可されていますが、URLのプロトコルまたはドメインアドレス部分内では許可されていません。ただし、Citrix Virtual Apps and Desktops 7 2206以降では、ワイルドカード `*` はURLのサブドメインアドレス部分内で許可されています。

許可: `http://www.xyz.com/index.html`、`https://www.xyz.com/*`、`http://www.xyz.com/*videos*`、`http://*.xyz.com/`

不許可: `http://*.*.com/`

URLでパスを指定することで、よりきめ細かな設定が可能です。たとえば、`https://www.xyz.com/sports/index.html`を指定した場合、index.htmlページのみがリダイレクトされます。

デフォルトでは、この設定は `https://www.youtube.com/*` に設定されています。

詳しくは、Knowledge Centerの記事CTX238236を参照してください。

ブラウザーコンテンツリダイレクト認証サイト

この設定を使用して、URLのリストを構成します。ブラウザーコンテンツリダイレクトを使用してリダイレクトされたサイトは、このリストを使用してユーザーを認証します。この設定は、許可リスト内のURLから移動した場合に、ブラウザーコンテンツリダイレクトがアクティブ（リダイレクトされた状態）のままになるURLを指定します。

典型的なシナリオは、認証にIDプロバイダー（IdP）に依存するWebサイトです。たとえば、Webサイト`www.xyz.com`はエンドポイントにリダイレクトされる必要がありますが、Okta（`www.xyz.okta.com`）のようなサードパーティのIdPが認証部分を処理します。管理者は、ブラウザーコンテンツリダイレクトACL構成ポリシーを使用して`www.xyz.com`を許可リストに追加します。次に、ブラウザーコンテンツリダイレクト認証サイトを使用して`www.xyz.okta.com`を許可リストに追加します。

詳しくは、Knowledge Centerの記事CTX238236を参照してください。

ブラウザーコンテンツリダイレクトブロックリスト設定

この設定は、ブラウザーコンテンツリダイレクトACL構成設定と連携して機能します。ブラウザーコンテンツリダイレクトACL構成設定とブロックリスト構成設定の両方にURLが存在する場合、ブロックリスト構成が優先され、URLのブラウザーコンテンツはリダイレクトされません。

承認されていないURL: ブロックリスト内のURLのうち、ブラウザーコンテンツがクライアントにリダイレクトされず、サーバーでレンダリングされるURLを指定します。

ワイルドカード「*」は許可されていますが、プロトコルまたはURLのドメインアドレス部分内では許可されていません。

許可されるもの: `http://www.xyz.com/index.html`、`https://www.xyz.com/*`、`http://www.xyz.com/*videos*`

不許可: `http://*.xyz.com/`

URLでパスを指定することで、よりきめ細かな設定が可能です。たとえば、`https://www.xyz.com/sports/index.html`を指定した場合、index.htmlのみがブロックリストに含まれます。

ブラウザーコンテンツリダイレクトプロキシ設定

この設定は、ブラウザーコンテンツリダイレクト用のVDA上のプロキシ設定の構成オプションを提供します。有効なプロキシアドレスとポート番号、PAC/WPAD URL、または直接/透過設定で有効になっている場合、Citrix Workspaceアプリはサーバーフェッチとクライアントレンダリングのみを試行します。

無効になっているか、構成されておらず、デフォルト値を使用している場合、Citrix Workspaceアプリはクライアントフェッチとクライアントレンダリングを試行します。

デフォルトでは、この設定は禁止されています。

明示的なプロキシの許可パターン:

`http://<hostname/ip address\>:\<port\>`

例:

`http://proxy.example.citrix.com:80` `http://10.10.10.10:8080`

PAC/WPADファイルの許可パターン:

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

例: `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

例: `http://10.10.10.10/configuration/pac/wpad.dat`

直接または透過プロキシの許可パターン:

ポリシーテキストボックスに**DIRECT**と入力します。

ブラウザコンテンツリダイレクトのレジストリキーのオーバーライド

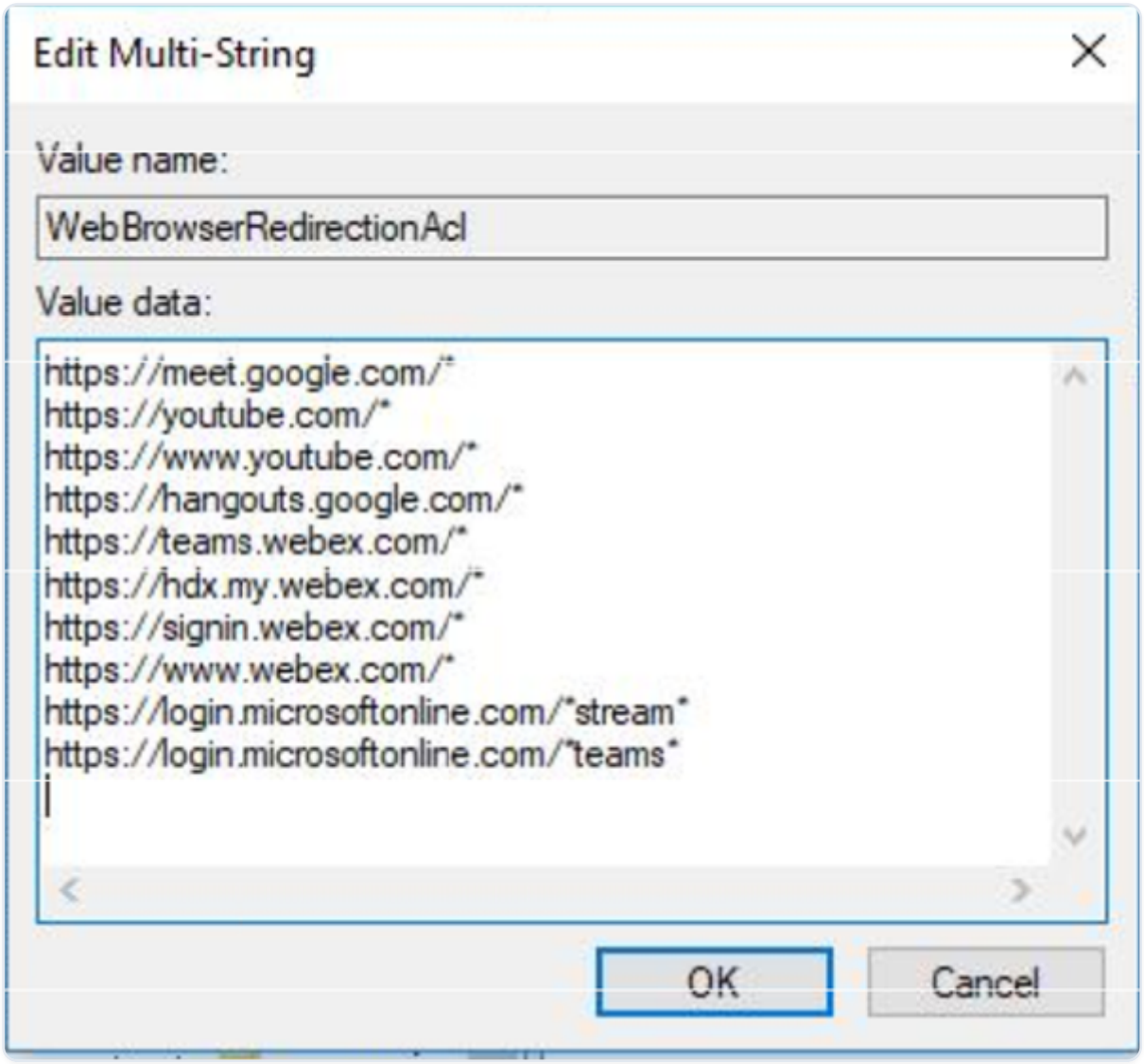
> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った

> 使用によって生じる問題が解決できることを保証できません。レジストリエディターの使用は自己責任で行ってください。編集する前に必ずレジストリをバックアップしてください。

> ポリシー設定のレジストリによるオプションのオーバーライド：

`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

名前	タイプ	値
WebBrowserRedirection	DWORD	1=許可、0=禁止
WebBrowserRedirectionAcl	REG_MULTI_SZ	
WebBrowserRedirectionAuthenticationSites	REG_MULTI_SZ	
WebBrowserRedirectionProxyAddress	REG_SZ	`http://myproxy.citrix.com:8080` または `http://10.10.10.10:8888`
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	



ブラウザコンテンツリダイレクトのためのHDXVideo.jsの挿入

ブラウザコンテンツリダイレクトの画像(/en-us/citrix-virtual-apps-desktops/2311/media/browsercontentredirectionflowchart-blacklist.png)

HdxVideo.js は、ブラウザコンテンツリダイレクトChrome拡張機能またはInternet Explorer Browser Helper Object (BHO) を使用して、ウェブページに挿入されます。BHO は Internet Explorer 用のプラグインモデルです。これはブラウザAPIのフックを提供し、プラグインがページのDocument Object Model (DOM) にアクセスしてナビゲーションを制御できるようにします。

BHO は、特定のページに HdxVideo.js を挿入するかどうかを決定します。この決定は、前のフローチャートに示されている管理ポリシーに基づいています。

JavaScript を挿入し、ブラウザコンテンツをクライアントにリダイレクトすることを決定した後、VDA 上の Internet Explorer ブラウザではウェブページが空白になります。**document.body.innerHTML** を空に設定すると、VDA 上のウェブページの本文全体が削除されま

す。ページは、クライアント上のオーバーレイブラウザ (Hdxbrowser.exe) に表示するために、クライアントに送信される準備ができています。

クライアントセンサーポリシー設定

クライアントセンサーセクションには、ユーザーセッションでモバイルデバイスのセンサー情報がどのように処理されるかを制御するためのポリシー設定が含まれています。

アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する

この設定は、モバイルデバイス上のセッションで実行されているアプリケーションが、ユーザーデバイスの物理的な位置情報を使用できるかどうかを決定します。

デフォルトでは、位置情報の使用は禁止されています。

この設定が禁止されている場合、アプリケーションが位置情報を取得しようとすると、「アクセス拒否」の値が返されます。

この設定が許可されている場合でも、ユーザーはCitrix Workspace™アプリの位置情報へのアクセス要求を拒否することで、位置情報の使用を禁止できます。AndroidおよびiOSデバイスでは、各セッションで位置情報が最初に要求されたときにプロンプトが表示されます。

「アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する」設定を使用するホスト型アプリケーションを開発する際は、以下を考慮してください。

- 位置情報対応アプリケーションが、位置情報が利用可能であることに依存しないようにしてください。その理由は次のとおりです。
  - ユーザーが位置情報へのアクセスを許可しない場合があります。
  - アプリケーションの実行中に位置情報が利用できない、または変更される場合があります。
  - ユーザーが、位置情報をサポートしていない別のデバイスからアプリケーションセッションに接続する場合があります。
- 位置情報対応アプリケーションは、次の要件を満たす必要があります。
  - デフォルトで位置情報機能をオフにする。
  - アプリケーションの実行中に、ユーザーがその機能を許可または禁止するオプションを提供する。
  - アプリケーションがキャッシュする位置情報データを消去するオプションをユーザーに提供します。（Citrix Workspaceアプリは位置情報データをキャッシュしません。）

- 位置情報対応アプリケーションは、位置情報の粒度を管理する必要があります。この管理により、取得されたデータがアプリケーションの目的に適切であることが保証されます。また、すべての関連法域の規制に準拠します。
- 位置情報サービスを使用する場合は、セキュアな接続（たとえば、TLSまたはVPNを使用）を強制します。Citrix Workspaceアプリを信頼できるサーバーに接続します。
- 位置情報サービスの使用に関して法的助言を得ることを検討してください。

デスクトップUIポリシー設定

デスクトップUIセクションには、デスクトップの壁紙、メニューアニメーション、ドラッグイメージなどの視覚効果を制御するポリシー設定が含まれています。これらのポリシー設定は、クライアント接続で使用される帯域幅の管理に役立ちます。帯域幅の使用量を制限することで、WANでのアプリケーションパフォーマンスを向上させることができます。

> **重要:**
>
> このリリースでは、レガシーグラフィックモードおよびデスクトップコンポジションリダイレクト（DCR）はサポートされていません。このポリシーは、以下を使用する場合の旧バージョンとの互換性のためのみに含まれています。
>
> - XenApp 7.15 LTSR
> - XenDesktop 7.15 LTSR
> - Windows 7およびWindows 2008 R2を使用する以前のVDAリリース。

デスクトップコンポジションリダイレクト

この設定は、ユーザーによりスムーズなWindowsデスクトップエクスペリエンスを提供するために、ローカルのDirectXグラフィックレンダリングで以下の処理能力を使用するかどうかを指定します。

- ユーザーデバイス上のグラフィック処理ユニット（GPU）
- または、,
- ユーザーデバイス上の統合グラフィックプロセッサ（IGP）

有効にすると、**デスクトップコンポジションリダイレクト**は、サーバー上での高いスケーラビリティを維持しながら、応答性の高いWindowsエクスペリエンスを提供します。

デフォルトでは、**デスクトップコンポジションリダイレクト**は無効になっています。

デスクトップコンポジションリダイレクトの選択を解除し、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加する際に、**無効**を選択します。

デスクトップコンポジションリダイレクトのグラフィック品質

この設定は、デスクトップコンポジションリダイレクトに使用されるグラフィックの品質を指定します。

デフォルトは「高」です。

「高」、「中」、「低」、または「ロスレス」品質から選択します。

デスクトップの壁紙

この設定は、ユーザーセッションでの壁紙の表示を許可または禁止します。

デフォルトでは、ユーザーセッションで壁紙を表示できます。

デスクトップの壁紙を選択解除し、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加する際に**禁止**を選択します。

メニューアニメーション

この設定は、ユーザーセッションでのメニューアニメーションを許可または禁止します。

デフォルトでは、メニューアニメーションは許可されています。

メニューアニメーションは、アクセシビリティのためのMicrosoftの個人設定です。有効にすると、短い遅延の後、スクロールまたはフェードインによってメニューが表示されます。メニューの下部には矢印アイコンが表示されます。その矢印をポイントするとメニューが表示されます。

このポリシー設定が**許可**に設定されており、メニューアニメーションのMicrosoft個人設定が有効になっている場合、デスクトップでメニューアニメーションが有効になります。

> **注:**
>
> メニューアニメーションのMicrosoft個人設定への変更は、デスクトップに影響を与えます。セッション終了時にデスクトップが変更を破棄するように設定されている場合を考慮してください。この場合、メニューアニメーションを有効にしているユーザーは、その後のセッションでメニューアニメーションを利用できない可能性があります。メニューアニメーションを必要とするユーザーのために、デスクトップのメインイメージでMicrosoft設定を有効にするか、デスクトップがユーザーの変更を保持するようにしてください。

ドラッグ中のウィンドウコンテンツの表示

この設定は、画面上でウィンドウをドラッグする際に、ウィンドウの内容の表示を許可または禁止します。

デフォルトでは、ウィンドウコンテンツの表示は許可されています。

許可に設定すると、ウィンドウ全体がドラッグ時に移動するように見えます。**禁止**に設定すると、ドロップするまで、ウィンドウの輪郭のみが移動するように見えます。

エンドユーザー監視ポリシー設定

「**エンドユーザー監視**」セクションには、セッションのトラフィックを測定するためのポリシー設定が含まれています。

ICA®ラウンドトリップ計算

この設定は、アクティブな接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アクティブな接続の計算は有効になっています。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザーインタラクションを示すトラフィックが発生するまで続きます。この遅延は無期限に続く可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

ICAラウンドトリップ計算間隔

この設定は、ICAラウンドトリップ計算が実行される頻度を秒単位で指定します。

デフォルトでは、ICAラウンドトリップは15秒ごとに計算されます。

アイドル接続のICAラウンドトリップ計算

この設定は、アイドル接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アイドル接続に対して計算は実行されません。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザーインタラクションを示すトラフィックが発生するまで続きます。この遅延は無期限に続く可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

ファイルリダイレクトポリシー設定

「**ファイルリダイレクト**」セクションには、クライアントドライブマッピングとクライアントドライブ最適化に関連するポリシー設定が含まれています。

クライアントドライブの自動接続

この設定は、ユーザーがログオンしたときのクライアントドライブの自動接続を許可または禁止します。

デフォルトでは、自動接続は許可されています。

この設定をポリシーに追加するときは、自動接続するドライブの種類の設定を有効にしてください。たとえば、ユーザーのCD-ROMドライブの自動接続を許可するには、この設定と「**クライアント光学ドライブ**」設定を構成します。

関連するポリシー設定は次のとおりです。

- **クライアントドライブリダイレクト**
- **クライアントフロッピーディスクドライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアントドライブリダイレクト

この設定は、ユーザーデバイス上のドライブとの間でファイルリダイレクトを有効または無効にします。

デフォルトでは、ファイルリダイレクトは有効になっています。

> **注:**
>
> クライアントドライブリダイレクトポリシー設定は、汎用USBリダイレクトを使用してセッションにマップされたドライブには適用されません。

> 有効にすると、ユーザーはすべてのクライアントドライブにファイルを保存できます。無効にすると、すべてのファイルリダイレクトが防止されます。この構成は、個々のファイルリ

> ダイレクト設定の状態に関係なく適用されます。個々のファイルリダイレクト設定には、クライアントフロッピードライブとクライアントネットワークドライブが含まれます。

関連するポリシー設定は次のとおりです。

- **クライアントフロッピードライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアント固定ドライブ

この設定により、ユーザーデバイス上の固定ドライブへのファイルのアクセスまたは保存を許可または禁止します。

デフォルトでは、クライアント固定ドライブへのアクセスは許可されています。

この設定をポリシーに追加する際は、**Client drive redirection**設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアント固定ドライブはマップされず、**Client fixed drives**設定の状態に関係なく、ユーザーはこれらのドライブに手動でアクセスできません。

ユーザーがログオンしたときに固定ドライブが自動的に接続されるように、**Auto connect client drives**設定を構成します。

クライアントフロッピードライブ

この設定により、ユーザーはユーザーデバイス上のフロッピードライブにアクセスしたりファイルを保存したりできるようになります。

デフォルトでは、クライアントフロッピードライブへのアクセスは許可されています。

この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、**クライアントフロッピーディスクドライブ**設定の状態に関わらず、クライアントフロッピーディスクドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。

ユーザーがログオンしたときにフロッピーディスクドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアントネットワークドライブ

この設定は、ユーザーがユーザーデバイスを介してネットワーク（リモート）ドライブにファイルにアクセスしたり保存したりすることを許可または禁止します。

デフォルトでは、クライアントネットワークドライブへのアクセスは許可されています。

この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントネットワークドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアントネットワークドライブ**設定の状態に関わらず適用されます。

ユーザーがログオンしたときにネットワークドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアント光学ドライブ

この設定は、ユーザーが以下の場所にアクセスしたり、ファイルを保存したりすることを許可または禁止します。

- ユーザーデバイス上のCD-ROM
- ユーザーデバイス上のDVD-ROM
- ユーザーデバイス上のBD-ROMドライブ。

デフォルトでは、クライアント光学ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、**許可**に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントの光学ドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアント光学ドライブ**設定の状態に関係なく適用されます。

ユーザーがログオンしたときに光学ドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアントリムーバブルドライブ

この設定により、ユーザーはユーザーデバイス上のUSBドライブへのファイルアクセスまたは保存を許可または禁止されます。

デフォルトでは、クライアントリムーバブルドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、クライアン

トのリムーバブルドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアントリムーバブルドライブ**設定の状態に関係なく適用されます。

ユーザーがログオンしたときにリムーバブルドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

ホストからクライアントへのリダイレクト

この設定により、URLおよび一部のメディアコンテンツのファイルタイプ関連付けを有効または無効にして、ユーザーデバイスで開くことができます。無効にすると、コンテンツはサーバーで開かれます。

デフォルトでは、ファイルタイプ関連付けは無効になっています。

この設定を有効にすると、以下のURLタイプがローカルで開かれます。

- HTTP
- HTTPS
- リアルプレイヤーおよびQuickTime (RTSP)
- Real Player および QuickTime (RTSPU)
- レガシー Real Player (PNM)
- マイクロソフト メディア サーバー (MMS)

クライアントドライブ文字の保持

この設定により、クライアントドライブをセッション内で同じドライブ文字にマップすることを有効または無効にします。

デフォルトでは、クライアントドライブ文字は保持されません。

この設定をポリシーに追加する場合は、**クライアントドライブリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。

クライアントドライブへの読み取り専用アクセス

この設定は、ユーザーとアプリケーションが以下を行うことを許可または防止します。

- マップされたクライアントドライブ上にファイルを作成する
- マップされたクライアントドライブ上のファイルを変更する
- マップされたクライアントドライブ上のフォルダーを変更する

デフォルトでは、マップされたクライアントドライブ上のファイルとフォルダーは変更できます。

「有効」に設定されている場合、ファイルとフォルダーは読み取り専用権限でアクセス可能です。

この設定をポリシーに追加する場合は、**クライアントドライブリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。

特殊フォルダーのリダイレクト

この設定により、Citrix Workspace™アプリおよびWeb Interfaceのユーザーがセッションからローカルのドキュメントおよびデスクトップの特殊フォルダーを閲覧することが許可または禁止されます。

デフォルトでは、特殊フォルダーのリダイレクトは許可されています。

この設定は、他の場所に存在する設定に関係なく、ポリシーによってフィルター処理されたオブジェクトが特殊フォルダーのリダイレクトを持つことを防止します。この設定が禁止されている場合、StoreFront™、Web Interface、またはCitrix Workspaceアプリに指定された関連設定はすべて無視されます。

どのユーザーが特殊フォルダーのリダイレクトを使用できるかを定義するには、**許可**を選択し、この機能を適用したいユーザーでフィルター処理されたポリシーにこの設定を含めます。この設定は、他のすべての特殊フォルダーのリダイレクト設定を上書きします。

ユーザーがローカルハードドライブにファイルにアクセスしたり保存したりするのを防ぐポリシー設定は、特殊フォルダーのリダイレクトが機能するのを妨げます。この状況は、特殊フォルダーのリダイレクトがユーザーデバイスと対話する必要があるために発生します。

この設定をポリシーに追加する際は、**クライアント固定ドライブ**設定が存在し、「許可」に設定されていることを確認してください。

ファイル転送ポリシー

デフォルトでは、ファイル転送は有効になっています。これらのポリシーは、**ユーザー設定 - ICA\ファイルリダイレクト**の下にあります。Web Studioを使用して変更してください。ファイル転送ポリシーを使用する際は、以下を考慮してください。

- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイル転送** - ユーザーがCitrix Virtual Apps and Desktopsセッションとデバイス間でファイルを転送することを許可または禁止します。
- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイルアップロード** - ユーザーがデバイスからCitrix Virtual Apps and Desktopsセッションにファイルをアップロードすることを許可または禁止します。

- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイルダウンロード** - ユーザーがCitrix Virtual Apps and Desktopsセッションからデバイスにファイルをダウンロードすることを許可または禁止します。

> **注:**
>
> ファイル転送ポリシーは、HTML5向けCitrix WorkspaceアプリおよびChrome OS向けCitrix Workspaceアプリにのみ適用されます。

非同期書き込みの使用

この設定は、非同期ディスク書き込みを有効または無効にします。

デフォルトでは、非同期書き込みは無効になっています。

非同期ディスク書き込みは、WAN を介したファイル転送とクライアントディスクへの書き込みの速度を向上させることができます。WAN は通常、比較的高帯域幅で高遅延が特徴です。ただし、接続またはディスクに障害が発生した場合、書き込み中のクライアントファイルは未定義の状態になる可能性があります。この未定義の状態が発生した場合、ポップアップウィンドウで影響を受けるファイルがユーザーに通知されます。ユーザーは、再接続時またはディスク障害が修正されたときに中断されたファイル転送を再開するなどの修復措置を講じることができます。

Citrix® は、リモート接続が必要で、良好なファイルアクセス速度を持つユーザーにのみ、非同期ディスク書き込みを有効にすることを推奨します。また、接続またはディスク障害が発生した場合に、失われたファイルやデータを簡単に回復できるユーザーにのみ推奨します。

この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。この設定が無効になっている場合、非同期書き込みは実行されません。

グラフィックポリシー設定

グラフィックセクションには、ユーザーセッションで画像がどのように処理されるかを制御するためのポリシー設定が含まれています。

視覚的にロスレスな圧縮を許可する

この設定により、グラフィックに対して真のロスレス圧縮の代わりに視覚的にロスレスな圧縮を使用できます。視覚的にロスレスな圧縮は、真のロスレス圧縮よりもパフォーマンスが向上しますが、目視では気づかない程度のわずかな損失があります。この設定は、視覚品質設定の値の使用方法を変更します。

デフォルトでは、この設定は無効になっています。

グラフィックステータスインジケーター

この設定は、グラフィックステータスインジケーターをユーザーセッションで実行するように構成します。このツールを使用すると、ユーザーはアクティブなグラフィックモードに関する情報を確認できます。この情報には、ビデオコーデック、ハードウェアエンコード、画質、およびセッションで使用されているモニターに関する詳細が含まれます。グラフィックステータスインジケーターを使用すると、ユーザーはピクセルパーフェクトモードを有効または無効にすることもできます。

Citrix Virtual Apps and Desktops™ 2103以降のリリースには、画質とインタラクティブ性の適切なバランスをユーザーが見つけるのに役立つ画質スライダーが含まれています。

Citrix Virtual Apps and Desktops 2109以降のリリースには、グラフィックステータスインジケーターを使用して起動されるユーザーインターフェイスを介して仮想ディスプレイレイアウトを構成する機能が含まれています。

グラフィックステータスインジケーターは、以前のバージョンのロスレスインジケーターツールを置き換えます。このポリシーは、Citrix Virtual Apps and Desktopsバージョン7.16から1809までロスレスインジケーターを有効にします。

画面共有

この設定により、ユーザーは画面コンテンツ、キーボード、マウスを含むセッションを他のユーザーと共有できます。

デフォルトでは、この設定は無効になっています。

VDAは、TCPポート範囲のポートを使用してデータを交換しようとします。これは、最も低いポートから始まり、後続の接続ごとにインクリメントされます。このポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

既定では、TCPポート範囲は52525～52625に設定されています。

画面共有に使用されるポートは、ファイアウォールの例外リストに追加する必要があります。このオプションは、VDAのインストール時にチェックボックスとして表示されます。既定では、このオプションはチェックされていません。

表示メモリ制限

この設定は、セッションの最大ビデオバッファサイズをキロバイト単位で指定します。

デフォルトでは、表示メモリ制限は65,536キロバイトです。

セッションの最大ビデオバッファサイズをキロバイト単位で指定します。128から4,194,303までのキロバイト単位の量を指定します。最大値4,194,303は表示メモリを制限しません。デフォルトでは、表示メモリは65,536キロバイトです。接続により多くの色深度と高解像度を使用するには、より多くのメモリが必要です。レガシーグラフィックモードでは、メモリ制限に達すると、「表示モードの劣化優先度」設定に従って表示が劣化します。

より多くの色深度と高解像度を必要とする接続の場合は、制限を増やしてください。次の式を使用して、必要な最大メモリを計算します。

メモリ深度（バイト）= (1ピクセルあたりの色深度（ビット） / 8) x (垂直解像度（ピクセル）) x (水平解像度（ピクセル）).

例えば、色深度32、垂直解像度600、水平解像度800のシナリオを考えます。この場合、必要な最大メモリは (32 / 8) x (600) x (800) = 1920000バイトであり、表示メモリ制限は1920 KBになります。

32ビット以外の色深度は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ利用できます。

HDX™ は、各セッションに必要な表示メモリの量のみを割り当てます。したがって、一部のユーザーのみがデフォルトよりも多くを必要とする場合でも、表示メモリ制限を増やすことによるスケーラビリティへの悪影響はありません。

表示モードの劣化優先度

> **注:**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

セッションの表示メモリ制限に達した場合、この設定は色深度と解像度のどちらが先に劣化するかを指定します。

デフォルトでは、色深度が先に劣化します。

セッションメモリの制限に達すると、表示される画像の品質を低下させることができます。カラー深度と解像度のどちらを先に低下させるかを選択することで、この品質を低下させることができます。カラー深度が最初に低下すると、表示される画像はより少ない色を使用します。解像度が最初に低下すると、表示される画像は1インチあたりのピクセル数が少なくなります。

カラー深度または解像度が低下したときにユーザーに通知するには、「表示モードが低下したときにユーザーに通知する」設定を構成します。

動的ウィンドウプレビュー

この設定は、シームレスウィンドウの表示を有効または無効にします。

- フリップ-
- フリップ 3D
- タスクバープレビュー
- Windows ピーク

WINDOWS AERO プレビューオプション	説明
タスクバープレビュー	ユーザーがウィンドウのタスクバーアイコンにマウスカーソルを合わせると、そのウィンドウの画像がタスクバーの上に表示されます。
Windows ピーク	ユーザーがタスクバーのプレビュー画像にマウスカーソルを合わせると、ウィンドウのフルサイズの画像が画面に表示されます。
フリップ	ユーザーが ALT+TAB を押すと、開いている各ウィンドウの小さなプレビューアイコンが表示されます。
フリップ 3D	ユーザーが TAB+Windows ロゴキーを押すと、開いているウィンドウの大きな画像が画面にカスケード表示されます。

デフォルトでは、この設定は有効になっています。

イメージキャッシュ

注:

Virtual Delivery Agent 7.x の場合、このポリシー設定は、レガシーグラフィックモードのポリシー設定が有効になっている場合にのみ適用されます。

この設定は、セッション内の画像のセクションのキャッシュと取得を有効または無効にします。画像をセクションにキャッシュし、必要に応じてこれらのセクションを取得すると、次のことが可能になります。

- ユーザーデバイスでのスクロールがよりスムーズになる
- ユーザーデバイスでのネットワーク経由で送信されるデータ量を削減する
- ユーザーデバイスで必要な処理を削減する

デフォルトでは、画像キャッシュ設定は有効になっています。

注:

イメージキャッシュ設定は、イメージがどのようにキャッシュされ、取得されるかを制御します。この設定は、イメージがキャッシュされるかどうかを制御するものではありません。レガシーグラフィックモード設定が有効になっている場合、イメージはキャッシュされます。

レガシーグラフィックモード - サポートされていません。下位互換性のためのみ

重要:

このリリースでは、レガシーグラフィックモードとデスクトップコンポジションリダイレクト (DCR) はサポートされていません。このポリシーは、XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、およびWindows 7とWindows 2008 R2を使用する以前のVDAリリースを使用する場合の下位互換性のためにのみ含まれています。

この設定は、リッチグラフィックエクスペリエンスを無効にします。この設定を使用して、レガシーグラフィックエクスペリエンスに戻し、WANまたはモバイル接続での帯域幅消費を削減します。XenAppおよびXenDesktop 7.13で導入された帯域幅の削減により、このモードは廃止されました。

デフォルトでは、この設定は無効になっており、ユーザーにはリッチグラフィックエクスペリエンスが提供されます。

レガシーグラフィックモードは以下でサポートされています。

- ウィンドウズ 7

- ウィンドウズ サーバー 2008 R2 VDA。

レガシーグラフィックモードは以下ではサポートされていません。

- Windows 8.xおよび10
- Windows Server 2012、2012 R2、および2016。

XenAppおよびXenDesktop 7.6 FP3以降でのグラフィックモードとポリシーの最適化に関する詳細については、CTX202687を参照してください。

最大許容色深度

> **注:**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、セッションで許可される最大色深度を指定します。

デフォルトでは、最大許容色深度は32ビット/ピクセルです。

この設定は、Thinwireドライバーと接続にのみ適用されます。プライマリディスプレイドライバーとしてThinWire以外のドライバーを使用するVDAには適用されません。これらのVDAは、プライマリディスプレイドライバーとしてWindows Display Driver Model (WDDM)ドライバーを使用するVDAです。Windows 8などのWDDMドライバーをプライマリディスプレイドライバーとして使用するシングルセッションOS VDAの場合、この設定は効果がありません。Windows Server 2012 R2などのWDDMドライバーを使用するWindowsマルチセッションOS VDAの場合、この設定によりユーザーがVDAに接続できなくなる可能性があります。

高い色深度を設定すると、より多くのメモリが必要になります。メモリ制限に達したときに色深度を低下させるには、**表示モードの低下設定**を構成します。色深度が低下すると、表示される画像はより少ない色を使用します。

表示モードが低下したときにユーザーに通知する

> **注:**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、色深度または解像度が低下したときに、ユーザーに簡単な説明を表示します。

デフォルトでは、ユーザーへの通知は無効になっています。

3Dグラフィックワークロード向けに最適化

この設定は、グラフィックを多用するワークロードに最適なデフォルト設定を構成します。グラフィックを多用するアプリケーションに重点を置くユーザーに対して、この設定を有効にします。このポリシーは、セッションでGPUが利用可能な場合にのみ適用してください。このポリシーによって設定されたデフォルト設定を明示的に上書きする他の設定は、優先されます。

デフォルトでは、3Dグラフィックワークロード向けに最適化は無効になっています。

キューイングとトッシング

注:

Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、別の画像に置き換えられたキュー内の画像を破棄します。

デフォルトでは、キューイングとトッシングは有効になっています。

この設定は、グラフィックがユーザーデバイスに送信される際の応答を改善します。この設定を構成すると、フレームがドロップされるため、アニメーションが途切れることがあります。

圧縮にビデオコーデックを使用する

エンドポイントでビデオデコードが利用可能な場合、グラフィックの圧縮にビデオコーデックの使用を許可します。**画面全体に適用**が選択されている場合、ビデオコーデックはすべてにデフォルトのコーデックとして適用されます。**アクティブに変更される領域に適用**が選択されている場合、ビデオコーデックは画面上で常に変化する領域に使用され、その他のデータには静止画圧縮とビットマップキャッシュが使用されます。エンドポイントでビデオデコードが利用できない場合、または**ビデオコーデックを使用しない**を指定した場合、静止画圧縮とビットマップキャッシュの組み合わせが使用されます。**推奨される場合にのみ使用**が選択されている場合、システムはさまざまな要因に基づいて選択します。選択方法が強化されるにつれて、バージョン間で結果が異なる場合があります。

推奨される場合にのみ使用を選択すると、システムは現在のシナリオに適切な設定を最大限に選択できるようになります。

画面全体に適用を選択すると、特にサーバーレンダリングされたビデオや3Dグラフィックを多用する場合に、ユーザーエクスペリエンスと帯域幅の向上に最適化されます。

アクティブに変更される領域に適用を選択すると、特に低帯域幅でビデオパフォーマンスが向上するように最適化され、静的およびゆっくりと変化するコンテンツのスケーラビリティを維持します。この設定はマルチモニター展開でサポートされています。

ビデオコーデックを使用しないを選択すると、サーバーのCPU負荷、および多数のサーバーレンダリングされたビデオやその他のグラフィックを多用するアプリケーションがない場合に最適化されます。

デフォルトは**推奨される場合にのみ使用**です。

ビデオにハードウェアエンコーディングを使用する

この設定により、利用可能な場合、グラフィックハードウェアを使用してビデオコーデックで画面要素を圧縮できます。そのようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。

このポリシー設定のデフォルトオプションは「**有効**」です。

複数のモニターがサポートされています。

ビデオデコードをサポートするCitrix Workspace™アプリは、ハードウェアエンコードで使用できます。

NVIDIA

NVIDIA GRID GPUの場合、Multi-session OSおよびSingle-session OS用VDAでハードウェアエンコーディングがサポートされています。

NVIDIA GPUはNVENCハードウェアエンコーディングをサポートしている必要があります。サポートされているGPUのリストについては、NVIDIAビデオコーデックSDKを参照してください。

NVIDIA GRIDにはドライバーバージョン3.1以降が必要です。NVIDIA Quadroにはドライバーバージョン362.56以降が必要です。CitrixはNVIDIA Release R361ブランチのドライバーを推奨しています。

ロスレステキストはNVENCハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがNVENCハードウェアエンコードよりも優先されます。

アクティブに変化する領域に対するH.264ハードウェアコーデックの選択的な使用がサポートされています。

視覚的にロスレス（YUV 4:4:4）圧縮がサポートされています。視覚的にロスレス（グラフィックポリシー設定、視覚的にロスレス圧縮を許可）には、Citrix Workspaceアプリ1808以降またはCitrix Receiver for Windows 4.5以降が必要です。

インテル

Intel Iris Proグラフィックプロセッサの場合、Single-session OSおよびMulti-session OS用VDAでハードウェアエンコーディングがサポートされています。

Intel Broadwellプロセッサファミリー以降のIntel Iris Proグラフィックプロセッサがサポートされています。Intel Remote Displays SDKバージョン1.0が必要であり、IntelのWebサイトからダウンロードできます: Remote Displays SDK。

ロスレステキストは、ビデオコーデックポリシーが画面全体に設定され、**3Dグラフィックワークロード向けに最適化**ポリシーが無効になっている場合にのみサポートされます。

視覚的にロスレス（YUV 4:4:4）はサポートされていません。

Intelエンコーダーは、最大8つのエンコードセッション（たとえば、1人のユーザーが8台のモニターを使用する場合、または8人のユーザーがそれぞれ1台のモニターを使用する場合）で良好なユーザーエクスペリエンスを提供します。8つ以上のエンコードセッションが必要な場合は、仮想マシンが接続するモニターの数を確認してください。管理者は、良好なユーザーエクスペリエンスを維持するために、このポリシー設定をユーザーごとまたはマシンごとに構成するかどうかを決定します。

AMD

AMDの場合、Single-session OS用VDAでハードウェアエンコーディングがサポートされています。

AMD GPUはRapidFire SDKをサポートする必要があります。例えば、AMD Radeon ProまたはFirePro GPUなどです。

エンコードを機能させるには、最新のAMDドライバーをインストールしてください。これらのドライバーは`<https://www.amd.com/en/support>`からダウンロードできます。

ロスレステキストはAMDハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがAMDハードウェアエンコードよりも優先されます。

活発に変化する領域に対してH.264ハードウェアコーデックを選択的に使用することがサポートされています。

キープアライブ ポリシー設定

「**キープアライブ**」セクションには、ICA® キープアライブメッセージを管理するためのポリシー設定が含まれています。

ICA キープアライブ タイムアウト

この設定は、連続するICAキープアライブメッセージ間の秒数を指定します。

デフォルトでは、キープアライブメッセージ間の間隔は60秒です。

ICAキープアライブメッセージを送信する1～3600秒の間隔を指定します。ネットワーク監視ソフトウェアが非アクティブな接続を閉じる役割を担っている場合は、この設定を構成しないでください。

ICA キープアライブメッセージ

この設定は、ICAキープアライブメッセージの定期的な送信を有効または無効にします。

デフォルトでは、キープアライブメッセージは送信されません。

この設定を有効にすると、切断された接続が切断状態のままになるのを防ぎます。サーバーがアクティビティを検出しない場合、この設定はリモートデスクトップサービス (RDS) がセッションを切断するのを防ぎます。サーバーは数秒ごとにキープアライブメッセージを送信して、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはそのセッションを切断済みとしてマークします。

セッションの信頼性を使用している場合、ICAキープアライブは機能しません。セッションの信頼性を使用していない接続に対してのみ、ICAキープアライブを構成してください。

関連するポリシー設定: セッションの信頼性接続。

ローカルアプリアクセス ポリシー設定

「**ローカルアプリアクセス**」セクションには、ユーザーのローカルにインストールされたアプリケーションをホストされたアプリケーションと連携させるポリシー設定が含まれています。これらのポリシー設定は、ホストされたデスクトップ環境での統合を管理します。

ローカルアプリアクセスを許可

この設定は、ユーザーのローカルにインストールされたアプリケーションとホストされたアプリケーションの統合を許可または禁止します。これらのポリシー設定は、ホストされたデスクトップ環境での統合を管理します。

ユーザーがローカルにインストールされたアプリケーションを起動すると、そのアプリケーションは実際にはローカルで実行されているにもかかわらず、仮想デスクトップ内で実行されているように見えます。

ローカルアプリアクセスを許可ポリシー設定を**有効**にすると、ブラウザコンテンツリダイレクトはサポートされず、デスクトップセッションにクライアント側の通知領域のバッテリーステータスは表示されません。

デフォルトでは、**ローカルアプリアクセスを許可**は禁止されています。

URLリダイレクトブロックリスト

この設定は、ローカルWebブラウザにリダイレクトされて起動されるWebサイトを指定します。これらのWebサイトには、次のものが含まれる場合があります。

- msn.comやnewsgoogle.comなど、ロケール情報を必要とするWebサイト
- ユーザーデバイスでより適切にレンダリングされるリッチメディアコンテンツを含むWebサイト。

デフォルトでは、サイトは指定されていません。

URLリダイレクト許可リスト

この設定は、起動された環境でレンダリングされるWebサイトを指定します。

デフォルトでは、サイトは指定されていません。

モバイルエクスペリエンスポリシー設定

「**モバイルエクスペリエンス**」セクションには、Citrix Mobility Packを処理するためのポリシー設定が含まれています。

キーボードの自動表示

この設定は、モバイルデバイス画面でのキーボードの自動表示を有効または無効にします。

デフォルトでは、キーボードの自動表示は無効になっています。

タッチ最適化デスクトップの起動

この設定は無効になっており、Windows 10またはWindows Server 2016マシンでは使用できません。

この設定は、Citrix Workspace™アプリの全体的なインターフェイス動作を決定します。この設定により、タブレットデバイス向けに最適化されたタッチフレンドリーなインターフェイスを許可または禁止します。

デフォルトでは、タッチフレンドリーなインターフェイスが使用されます。

Windowsインターフェイスのみを使用するには、このポリシー設定を「禁止」に設定します。

コンボボックスのリモート化

この設定は、モバイルデバイス上のセッションで表示できるコンボボックスの種類を決定します。このポリシー設定を「許可」に設定すると、デバイスネイティブのコンボボックスコントロールが表示されます。この設定が許可されている場合、ユーザーはCitrix Workspaceアプリfor iOSのセッション設定を変更して、Windowsコンボボックスを使用できます。

デフォルトでは、**コンボボックスのリモート化**機能は禁止されています。

マルチメディアポリシー設定

マルチメディアセクションには、ユーザーセッションでのストリーミングHTML5およびWindowsオーディオとビデオを管理するためのポリシー設定が含まれています。

> **警告**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

マルチメディアポリシー

デフォルトでは、Delivery Controller™で設定されたすべてのマルチメディアポリシーは、以下のレジストリに保存されます。

マシンポリシー:

`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies`

ユーザーポリシー:

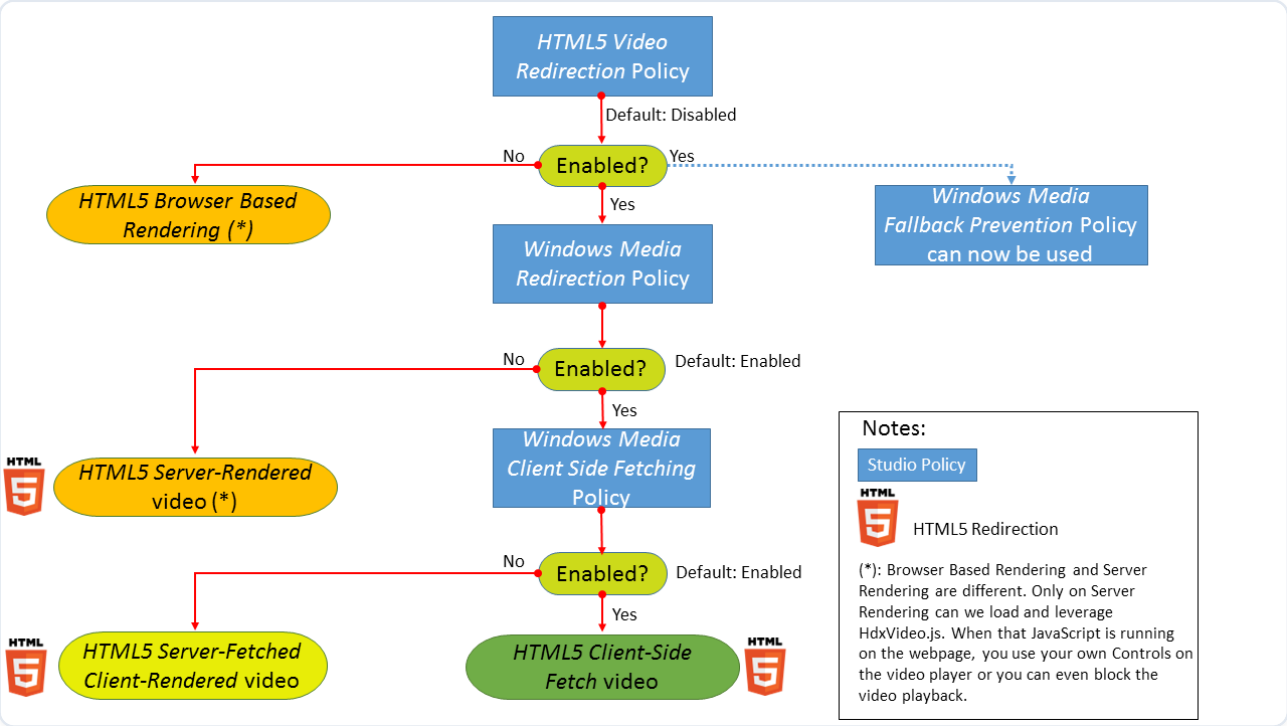
`HKEY_LOCAL_MACHINE\Software\Policies\Citrix{User Session ID}\User\MultimediaPolicies`

現在のユーザーセッションIDを見つけるには、Windowsコマンドラインで**qwinsta**コマンドを発行します。

HTML5ビデオリダイレクト

Citrix Virtual Apps and Desktops™サーバーがHTML5マルチメディアWebコンテンツをユーザーに配信する方法を制御し、最適化します。

デフォルトでは、この設定は無効になっています。



このリリースでは、この機能は制御されたWebページでのみ利用可能です。HTML5マルチメディアコンテンツが利用可能なWebページ（例: 社内トレーニングサイトのビデオ）にJavaScriptを追加する必要があります。

HTML5ビデオリダイレクトを構成するには:

1. VDAインストール上の%Program Files%/Citrix/ICA Service/HTML5 Video Redirectionからファイル**HdxVideo.js**を社内Webページの場所にコピーします。
2. この行をWebページに挿入します（Webページに他のスクリプトがある場合は、それらのスクリプトの前に**HdxVideo.js**を含めます）。 `<script src="HdxVideo.js" type="text/javascript"\></script>`

注: HdxVideo.jsがWebページと同じ場所にない場合は、**src**属性を使用してそのフルパスを指定します。

JavaScriptが制御されたWebページに追加されておらず、ユーザーがHTML5ビデオを再生する場合を考えてみましょう。この場合、Citrix Virtual Apps and Desktopsはサーバー側レンダリングにデフォルト設定されます。

HTML5ビデオのリダイレクトを機能させるには、***Windows Media Redirection***を許可します。このポリシーは、Server Fetch Client Renderには必須であり、Client Side Fetchingには必要です。Client Side Fetchingは、さらに*Windows Media client-side content fetching*が許可されていることも必要とします。

Microsoft Edgeはこの機能をサポートしていません。

HdxVideo.jsは、ブラウザのHTML5プレーヤーコントロールを独自のコントロールに置き換えます。特定のWebサイトでHTML5ビデオリダイレクトポリシーが有効になっていることを確認するには、プレーヤーコントロールを**HTML5ビデオリダイレクト**ポリシーが禁止されているシナリオと比較します。

（ポリシーが許可されている場合のCitrixカスタムコントロール）



（ポリシーが禁止されているか、構成されていない場合のネイティブWebページコントロール）



以下のビデオコントロールがサポートされています。

- 再生
- 一時停止
- シーク
- 繰り返し
- オーディオ
- 全画面表示

HTML5ビデオ リダイレクト テストページを表示できます。

TLS、HTML5ビデオ リダイレクト、およびブラウザコンテンツ リダイレクト

HTML5ビデオ リダイレクトを使用して、次のことができます。

- HTTPS Webサイトからのビデオをリダイレクトする
- または
- ブラウザコンテンツ リダイレクトを使用してWebサイト全体をリダイレクトする

これらのWebサイトに挿入されたJavaScriptは、VDAで実行されているCitrix HDX HTML5ビデオリダイレクトサービス (WebSocketService.exe) へのTLS接続を確立する必要があります。VDAの

証明書ストアにあるCitrix HDX HTML5ビデオ リダイレクトサービスは、次の目的で2つのカスタム証明書を生成します。

- ビデオ リダイレクトを実現する
- WebページのTLS整合性を維持する

HdxVideo.jsは、セキュアWebSocketを使用して、VDAで実行されているWebSocketService.exeと通信します。このプロセスはローカルシステムアカウントとして実行され、SSL終端とユーザーセッションマッピングを行います。

WebSocketService.exeは、127.0.0.1ポート9001でリッスンしています。

ビデオ品質の制限

この設定は、Windows Mediaにのみ適用され、HTML5には適用されません。**WAN経由のWindows Mediaマルチメディアリダイレクトの最適化**を有効にする必要があります。

この設定は、HDX™接続で許可される最大ビデオ品質レベルを指定します。設定すると、最大ビデオ品質は指定された値に制限され、環境内でマルチメディアのサービス品質 (QoS) が維持されます。

デフォルトでは、この設定は構成されていません。

許可される最大ビデオ品質レベルを制限するには、次のいずれかのオプションを選択します。

- 1080p/8.5Mbps
- 720p/4.0Mbps
- 480p/720Kbps
- 380p/400Kbps
- 240p/200Kbps

同じサーバーで複数のビデオを同時に再生すると、大量のリソースが消費され、サーバーのスケーラビリティに影響を与える可能性があります。

Microsoft Teamsのリダイレクト

この設定は、HDX テクノロジーに基づいた Microsoft Teams の最適化を有効にします。

このポリシーが有効で、サポートされているバージョンのCitrix Workspace™アプリを使用している場合、このレジストリキーはVDAで**1**に設定されます。Microsoft Teamsアプリケーションは、VDIモードでロードするためにこのキーを読み取ります。 レジストリキーを手動で設定する必要はありません。

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

名前: MSTeamsRedirSupport

値: DWORD (1 - オン, 0 - オフ)

> **注:**
>
> Web Studioでポリシーが利用できない古いバージョンのControllerと、バージョン1906.2以降のVDAを使用している場合を考慮してください。Controllerの古いバージョンの例として、バージョン7.15があります。この場合、VDAではHDX最適化がデフォルトで有効になっています。Workspaceアプリのバージョンが1907以降の場合、Microsoft Teamsは最適化モードで起動します。7.15 LTSR ControllerとCR VDAの混在に関する注意点については、Knowledge Centerの記事CTX205549を参照してください。

> この場合、特定のユーザーに対して機能を無効にするには、レジストリ設定を上書きできます。ユーザーの組織単位にログオンスクリプトを適用するグループポリシーを使用して、レジストリ設定を上書きします。

> デフォルトでは、Microsoft Teamsリダイレクトは有効になっています。

マルチメディア会議

この設定により、ビデオ会議アプリケーションによる最適化されたWebカメラリダイレクトテクノロジーの使用を許可または禁止します。

デフォルトでは、ビデオ会議のサポートは許可されています。

この設定をポリシーに追加する際は、**Windows Mediaリダイレクト**設定が存在し、**許可**（デフォルト）に設定されていることを確認してください。

マルチメディア会議を使用する場合は、次の条件が満たされていることを確認してください。

- マルチメディア会議に使用するWebカメラのメーカー提供ドライバーがクライアントにインストールされていること。
- ビデオ会議セッションを開始する前に、Webカメラをユーザーデバイスに接続します。サーバーは、一度に1つのインストールされたWebカメラのみを使用します。複数のWebカメラがユーザーデバイスにインストールされている場合、サーバーは各Webカメラを順番に試行します。この試行は、ビデオ会議セッションが正常に作成されるまで続行されます。

汎用USBリダイレクトを使用してWebカメラをリダイレクトする場合、このポリシーは必要ありません。その場合は、WebカメラドライバーをVDAにインストールしてください。

WAN経由でのWindows Mediaマルチメディアリダイレクトの最適化

この設定はWindows Mediaにのみ適用され、HTML5には適用されません。この設定により、以下が可能になります。

- リアルタイムマルチメディアトランスコーディング
- 劣化したネットワーク経由でのモバイルデバイスへのオーディオおよびビデオメディアストリーミングを可能にします
- WAN経由でのWindows Mediaコンテンツの配信方法を改善することで、ユーザーエクスペリエンスを向上させます。

デフォルトでは、WAN経由でのWindows Mediaコンテンツの配信は最適化されています。

この設定をポリシーに追加する場合、**Windows Mediaリダイレクト**設定が存在し、**許可**に設定されていることを確認してください。

この設定が有効になっている場合、メディアストリーミングを可能にするために、必要に応じてリアルタイムマルチメディアトランスコーディングが自動的に展開されます。また、極端なネットワーク条件下でもシームレスなユーザーエクスペリエンスを提供します。

WAN経由でのWindows Mediaマルチメディアリダイレクトの最適化にGPUを使用する

この設定はWindows Mediaにのみ適用され、Virtual Delivery Agent (VDA) 上のグラフィックス処理ユニット (GPU) でリアルタイムマルチメディアトランスコーディングを実行できるようにします。これにより、サーバーのスケーラビリティが向上します。GPUトランスコーディングは、VDAがハードウェアアクセラレーションに対応したGPUを搭載している場合にのみ利用可能です。そうでない場合、トランスコーディングはCPUにフォールバックします。

注: GPUトランスコーディングはNVIDIA GPUでのみサポートされています。

デフォルトでは、VDA上のGPUを使用してWAN経由でのWindows Mediaコンテンツの配信を最適化することは禁止されています。

この設定をポリシーに追加する場合、以下の設定が存在し、「許可」に設定されていることを確認してください。

- **Windows Mediaリダイレクト**
- **WAN経由でのWindows Mediaマルチメディアリダイレクトの最適化設定**

Windows Mediaフォールバック防止

この設定は、ブラウザコンテンツリダイレクト、HTML5、およびWindows Mediaに適用されます。HTML5をサポートするには、**HTML5 video redirection**ポリシーを**Allowed**に設定します。

管理者は、**Windows Media フォールバック防止**ポリシー設定を使用して、ストリーミングコンテンツをユーザーに配信するために試行される方法を指定できます。

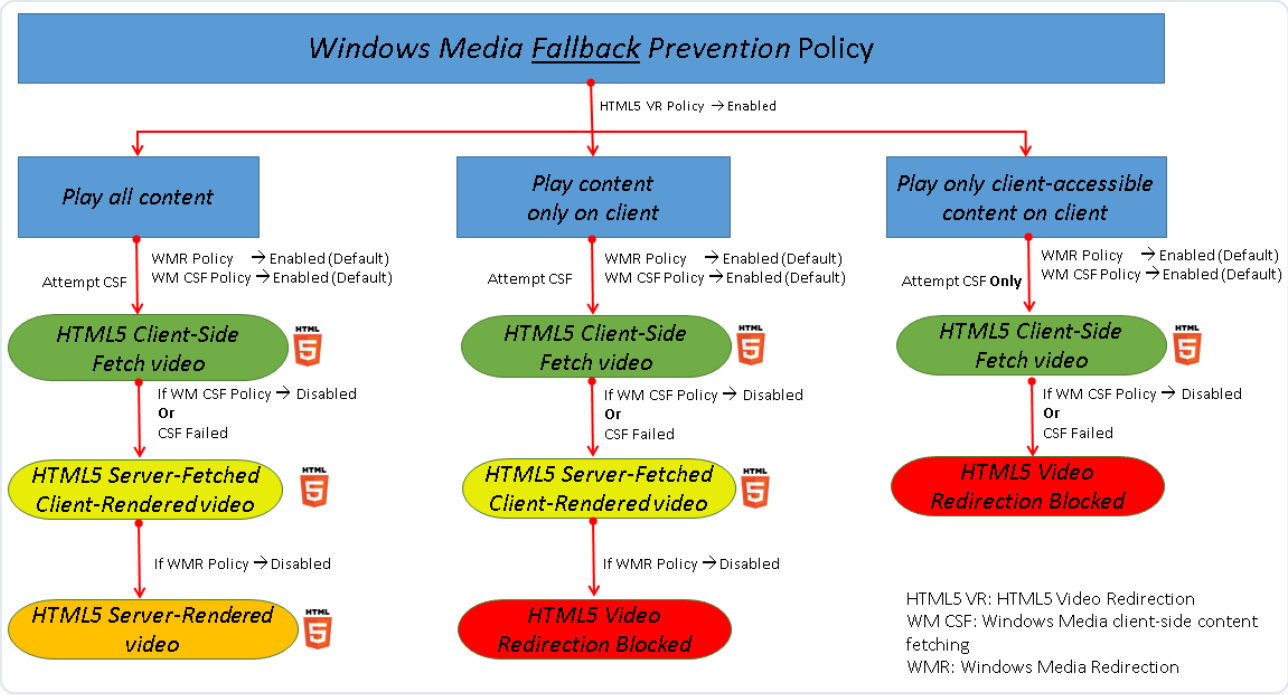
デフォルトでは、この設定は構成されていません。設定が「未構成」に設定されている場合、動作は**すべてのコンテンツを再生**と同じになります。

この設定を構成するには、次のいずれかのオプションを選択します。

- **すべてのコンテンツを再生**。クライアント側のコンテンツ取得を試行し、次にWindows Mediaリダイレクトを試行します。失敗した場合は、サーバーでコンテンツを再生します。
- **すべてのコンテンツをクライアントでのみ再生**。クライアント側の取得を試行し、次にWindows Mediaリダイレクトを試行します。失敗した場合は、コンテンツは再生されません。
- **クライアントでクライアントアクセス可能なコンテンツのみを再生**。クライアント側の取得のみを試行します。失敗した場合は、コンテンツは再生されません。

コンテンツが再生されない場合、プレーヤーウィンドウに次のエラーメッセージが表示されます（デフォルトの表示時間は5秒）。

```
"Company has blocked video because of lack of resources"
```



このエラーメッセージの表示時間は、VDA上の次のレジストリキーでカスタマイズできます。レジストリエントリが存在しない場合、表示時間はデフォルトで5秒になります。

レジストリパスは、VDAのアーキテクチャによって異なります。

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

または

\HKLM\SOFTWARE\Citrix\HdxMediastream

レジストリキー：

名前: VideoLoadManagementErrDuration

種類: DWORD

範囲: 1 - DWORDの制限まで (デフォルト = 5)

単位: 秒

Windows Mediaクライアント側コンテンツ取得

この設定はHTML5とWindows Mediaの両方に適用されます。この設定により、ユーザーデバイスは、XenAppまたはXenDesktop®ホストサーバーを介するのではなく、インターネットまたはイントラネット上のソースプロバイダーからマルチメディアファイルを直接ストリーミングできます。

デフォルトでは、この設定は**許可**されています。この設定を許可すると、ネットワーク使用率とサーバーのスケーラビリティが向上します。この改善は、メディアに関するあらゆる処理をホストサーバーからユーザーデバイスに移動することで実現されます。また、Microsoft DirectShowやMedia Foundationなどの高度なマルチメディアフレームワークをユーザーデバイスにインストールする必要がなくなります。ユーザーデバイスには、URLからファイルを再生する機能のみが必要です。

この設定をポリシーに追加するときは、**Windows Mediaリダイレクト**設定が存在し、**許可**に設定されていることを確認してください。**Windows Mediaリダイレクト**が無効になっている場合、ソースプロバイダーからユーザーデバイスへのマルチメディアファイルの直接ストリーミングも無効になります。

Windows Mediaリダイレクト

この設定はHTML5とWindows Mediaの両方に適用され、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御および最適化します。

デフォルトでは、この設定は**許可**されています。HTML5の場合、ポリシー**HTML5ビデオのリダイレクト**が**禁止**されている場合、この設定は有効になりません。

この設定が有効になっている場合、サーバーからレンダリングされるオーディオとビデオの品質は、ユーザーデバイスでローカルに再生されるオーディオとビデオに匹敵するレベルに向上します。サーバーはマルチメディアを元の圧縮形式でクライアントにストリーミングし、ユーザーデバイスがメディアを解凍してレンダリングできるようにします。

Windows Mediaリダイレクトは、Microsoft DirectShow、DirectX Media Objects (DMO)、およびMedia Foundationの標準に準拠するコーデックでエンコードされたマルチメディアファイルを最適化します。特定のマルチメディアファイルを再生するには、そのマルチメディアファイルのエンコード形式と互換性のあるコーデックがユーザーデバイスに存在する必要があります。

デフォルトでは、Citrix Workspaceアプリでオーディオは無効になっています。ユーザーがICA®セッションでマルチメディアアプリケーションを実行できるようにするには、オーディオをオンにするか、Citrix Workspaceアプリインターフェイスでオーディオをオンにする権限をユーザーに付与します。

Windows Mediaリダイレクトを使用してメディアを再生したときの表示が、基本的なICA圧縮と通常のオーディオを使用してレンダリングした場合よりも悪く見える場合にのみ、「**禁止**」を選択してください。この状況はまれですが、低帯域幅の条件下、たとえばキーフレームの頻度が低いメディアの場合などに発生する可能性があります。

Windows Mediaリダイレクトのバッファサイズ

この設定はレガシーであり、HTML5には適用されません。

この設定は、マルチメディアアクセラレーションのバッファサイズを1～10秒で指定します。

デフォルトでは、バッファサイズは5秒です。

Windows Mediaリダイレクトのバッファサイズの使用

この設定はレガシーであり、HTML5には適用されません。

この設定は、**Windows Media Redirection buffer size** 設定で指定されたバッファサイズの使用を有効または無効にします。

デフォルトでは、指定されたバッファサイズは使用されません。

この設定が無効になっている場合、または**Windows Media Redirection buffer size** 設定が構成されていない場合、サーバーはデフォルトのバッファサイズ値（5秒）を使用します。

マルチストリーム接続ポリシー設定

マルチストリーム接続セクションには、セッション内の複数のICA®接続に対するサービス品質の優先順位付けを管理するためのポリシー設定が含まれています。

> **注:**
>
> マルチストリーム接続ポリシーが有効になっている場合、MTU検出はサポートされていません。

UDP経由のオーディオ

この設定は、サーバー上でのUDP経由のオーディオを許可または禁止します。

デフォルトでは、サーバー上でのUDP経由のオーディオは許可されています。

有効にすると、この設定はサーバー上でUDPポートを開き、UDP経由のオーディオリアルタイムトランスポートを使用するように構成されたすべての接続をサポートします。

オーディオUDPポート範囲

この設定は、Virtual Delivery Agent (VDA) によって使用されるポート番号の範囲（最小ポート番号、最大ポート番号）を指定します。この指定は、ユーザーデバイスとの間でオーディオパケットデータを交換するのに役立ちます。VDAは、ユーザーデバイスとの間でデータを交換するために、各UDPポートペアを使用しようとします。これは、最小値から始まり、その後の各試行で2ずつ増加します。各ポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

デフォルトでは、この範囲は16500,16509に設定されています。

マルチポートポリシー

この設定は、ICAトラフィックに使用されるTCPポートを指定し、各ポートのネットワーク優先順位を確立します。

デフォルトでは、プライマリポート (2598) は高優先度です。

ポートを構成する際、次の優先順位を割り当てることができます。

- **非常に高い:** ウェブカメラ会議などのリアルタイムアクティビティ用
- **高:** 画面、キーボード、マウスなどの対話型要素用
- **中:** クライアントドライブマッピングなどのバルク処理用

- **低:** 印刷などのバックグラウンドアクティビティ用

各ポートには一意の優先順位が必要です。たとえば、CGPポート1とCGPポート3の両方に「非常に高」の優先順位を割り当てることはできません。

ポートを優先順位付けから削除するには、ポート番号を0に設定します。プライマリポートを削除したり、その優先度レベルを変更したりすることはできません。

この設定を構成するときは、サーバーを再起動してください。この設定は、**Multi-Stream computer**設定ポリシー設定が有効になっている場合にのみ有効になります。

マルチストリーム コンピューター設定

この設定は、サーバー上のMulti-Streamを有効または無効にします。

デフォルトでは、Multi-Streamは無効になっています。Citrix SD-WAN™またはサードパーティ製ルーターを使用して目的のQuality of Serviceを実現する場合は、Multi-Stream computerポリシー設定を構成してください。

Multi-Streamが有効になっている場合、Adaptive Transportの機能であるMTU Discoveryはサポートされません。

この設定を構成するときは、変更が適用されるようにサーバーを再起動してください。

> **重要:**
>
> このポリシー設定を、セッション全体の帯域幅制限などの帯域幅制限ポリシー設定と組み合わせて使用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定が含まれていないことを確認してください。

マルチストリーム ユーザー設定

この設定は、ユーザーデバイス上でMulti-Streamを有効または無効にします。

デフォルトでは、Multi-Streamはすべてのユーザーに対して無効になっています。Citrix SD-WANまたはサードパーティ製ルーターを使用して目的のQuality of Serviceを実現する場合は、Multi-Stream user設定を構成してください。

この設定は、**マルチストリームコンピューター**設定ポリシー設定が有効になっているホストでのみ有効になります。

> **重要:**

> このポリシー設定を、全体的なセッション帯域幅制限などの帯域幅制限ポリシー設定と併用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定を含めないようにしてください。

マルチストリーム仮想チャネル割り当て設定

この設定は、マルチストリームが使用されるときに仮想チャネルが割り当てられるICAストリームを指定します。

これらの設定を構成しない場合、仮想チャネルはデフォルトのストリームに保持されます。仮想チャネルをICAストリームに割り当てるには、仮想チャネル名の横にある**ストリーム番号**リストから、目的のストリーム番号（0、1、2、3）を選択します。

環境でカスタム仮想チャネルが使用されている場合は、**追加**をクリックし、**仮想チャネル**の下のテキストボックスに仮想チャネル名を指定し、その横にある**ストリーム番号**リストから目的のストリーム番号を選択します。指定する名前は、フレンドリ名ではなく、実際の仮想チャネル名である必要があります。たとえば、Citrix Browser AccelerationではなくCTXSBRなどです。

これらの設定は、マルチストリームコンピューター設定を有効にしている場合にのみ有効になります。

デフォルトでは、仮想チャネルとそのストリーム割り当ては次のとおりです。

- AppFlow®: 2
- オーディオ: 0
- ブラウザコンテンツリダイレクト: 2
- クライアントCOMポートマッピング: 3
- クライアントドライブマッピング: 2
- クライアントプリンターマッピング: 3
- クリップボード: 2
- CTXDND: 1 (**注:** これは、Citrixセッションとローカルエンドポイント間でファイルをドラッグアンドドロップする機能をサポートします。)
- DVCプラグイン (DVCプラグインのフレンドリ名から自動生成された静的VC名、または管理者によって割り当てられたもの): 2
- エンドユーザーエクスペリエンス監視: 1
- ファイル転送 (HTML5 Receiver): 2

- 汎用データ転送: 2
- ICAコントロール: 1
- 入力メソッドエディター: 1
- レガシー クライアント プリンター マッピング (COM1): 1, 3
- レガシー クライアント プリンター マッピング (COM2): 2, 3
- レガシー クライアント プリンター マッピング (LPT1): 1, 3
- レガシー クライアント プリンター マッピング (LPT2): 2, 3
- ライセンス管理: 1
- Microsoft Teams/WebRTC リダイレクト: 1
- モバイルレシーバー: 1
- マルチタッチ: 1
- ポートフォワーディング: 2
- リモートオーディオおよびビデオ拡張機能 (RAVE): 2
- シームレス (透過ウィンドウ統合): 1
- センサーと位置情報: 1
- スマートカード: 1
- シンワイヤーグラフィックス: 1
- 透過UI統合/ログオンステータス: 2
- TWAINリダイレクト: 2
- USB: 2
- ゼロレイテンシーフォントおよびキーボード: 2
- ゼロレイテンシーデータチャネル: 2

仮想チャネルの割り当てと優先順位の詳細については、Knowledge Centerの記事CTX131001を参照してください。

ポートリダイレクトポリシー設定

ポートリダイレクトセクションには、クライアントLPTおよびCOMポートマッピングのポリシー設定が含まれています。

Virtual Delivery Agentのバージョン**7.0より前**の場合、ポートリダイレクトを構成するには以下のポリシー設定を使用します。VDAバージョン**7.0から7.8**の場合、これらの設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイ

レクト設定の構成」を参照してください。VDAバージョン**7.9**の場合、以下のポリシー設定を使用します。

クライアントCOMポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のCOMポートの自動接続を有効または無効にします。

デフォルトでは、クライアントCOMポートは自動的に接続されません。

クライアントLPTポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のLPTポートの自動接続を有効または無効にします。

デフォルトでは、クライアントLPTポートは自動的に接続されません。

クライアントCOMポートリダイレクト

この設定は、ユーザーデバイス上のCOMポートへのアクセスを許可または禁止します。

デフォルトでは、COMポートリダイレクトは禁止されています。

関連するポリシー設定は次のとおりです。

- COMポートリダイレクトの帯域幅制限
- COMポートリダイレクトの帯域幅制限（パーセント）

クライアントLPTポートリダイレクト

この設定は、ユーザーデバイス上のLPTポートへのアクセスを許可または禁止します。

デフォルトでは、LPTポートリダイレクトは禁止されています。

LPTポートは、印刷ジョブをLPTポートに送信するレガシーアプリケーションでのみ使用されます。これらのポートは、印刷ジョブをユーザーデバイス上の印刷オブジェクトに送信するレガシーアプリケーションでは使用されません。今日のほとんどのアプリケーションは、印刷ジョブをプリンターオブジェクトに送信できます。このポリシー設定は、LPTポートに印刷するレガシーアプリケーションをホストするサーバーでのみ必要です。

クライアントCOMポートリダイレクトは双方向ですが、LPTポートリダイレクトは出力のみであり、ICAセッション内では\\client\LPT1および\\client\LPT2に制限されることに注意してください。

関連するポリシー設定は次のとおりです。

- LPTポートリダイレクト帯域幅制限

- LPTポートリダイレクト帯域幅制限の割合

印刷ポリシー設定

印刷セクションには、クライアント印刷を管理するためのポリシー設定が含まれています。

クライアントプリンターリダイレクト

この設定は、ユーザーがセッションにログオンしたときに、クライアントプリンターがサーバーにマップされるかどうかを制御します。

デフォルトでは、クライアントプリンターのマッピングは許可されています。この設定が無効になっている場合、セッション用のPDFプリンターは自動作成されません。

関連するポリシー設定: クライアントプリンターの自動作成

デフォルトプリンター

この設定は、ユーザーデバイス上のデフォルトプリンターがセッションでどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「ユーザーのデフォルトプリンターを調整しない」を選択します。このオプションを選択した場合、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントのプロパティに応じて変更されません。セッション内のデフォルトプリンターは、セッションで自動作成された最初のプリンターであり、次のいずれかです。

- **コントロールパネル > デバイス**と**プリンター**でWindowsサーバーにローカルに追加された最初のプリンター。
- サーバーにローカルに追加されたプリンターがない場合、最初に自動作成されたプリンター。

このオプションを使用すると、プロファイル設定を通じてユーザーに最も近いプリンターを提示できます（近接印刷として知られています）。

プリンターの割り当て

この設定は、デフォルトプリンターとセッションプリンターの設定の代替手段を提供します。個別のデフォルトプリンターとセッションプリンターの設定を使用して、サイト、大規模グループ、または組織単位の動作を構成します。**プリンターの割り当て**設定を使用して、多数のプリンターを複数のユーザーに割り当てます。

この設定は、リストされたユーザーデバイス上のデフォルトプリンターがセッションでどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

各ユーザーデバイスのセッションで自動作成されるネットワークプリンターも指定します。デフォルトでは、プリンターは指定されていません。

- デフォルトプリンターの値を設定する場合：

  ユーザーデバイスの現在のデフォルトプリンターを使用するには、「Do not adjust」を選択します。

  デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「Do no adjust」を選択します。このオプションを選択すると、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントのプロパティに応じて変更されません。セッション内のデフォルトプリンターは、セッションで最初に自動作成されたプリンターであり、次のいずれかです。

  - Windowsサーバーにローカルで追加された最初のプリンター（**コントロールパネル > デバイス**とプリンター）。
  - サーバーにローカルで追加されたプリンターがない場合、最初に自動作成されたプリンター。

- セッションプリンターの値を設定する場合：プリンターを追加するには、自動作成するプリンターのUNCパスを入力します。プリンターを追加した後、ログオンするたびに現在のセッションにカスタマイズされた設定を適用できます。

プリンター自動作成イベントログの優先設定

この設定は、プリンターの自動作成プロセス中にログに記録されるイベントを指定します。エラーや警告をログに記録しない、エラーのみをログに記録する、またはエラーと警告をログに記録する、のいずれかを選択できます。

デフォルトでは、エラーと警告がログに記録されます。

警告の例としては、プリンターのネイティブドライバーをインストールできず、代わりにUniversal print driverがインストールされるイベントがあります。このシナリオでUniversal print driverを使用するには、Universal print driverの使用設定を「Use universal printing only」または「Use universal printing only if the requested driver is unavailable」に構成します。

セッションプリンター

この設定は、セッションで自動作成されるネットワークプリンターを指定します。ICA/HDXセッション内では、Citrix Print Managerサービス（CpSvc.exe）が、**セッションプリンター**ポリシー設定で指定された各ネットワークプリンターに対して、セッションログオン中にネットワークプリンター接続を作成します。セッションログオフ中にプリンターを削除します。デフォルトでは、プリンターは指定されていません。

セッションプリンターポリシー設定では、ネットワークプリンターはWindows Print ServerまたはCitrix Universal™ Print Server上に存在できます。

- **Windows Print Server:** 1つ以上のネットワークプリンターを共有します。また、ネットワークプリンターを使用するために必要なネイティブプリンタードライバーも備えています。
- **Universal Print Server:** Citrix Universal Print Serverソフトウェアがインストールされている Windows Print Server。

Windows Print Server を使用する場合、Citrix Print Manager サービスはネイティブプリンタードライバーを使用してネットワークプリンター接続を作成します。Citrix Virtual Apps™ サーバーには、ネイティブプリンタードライバーがインストールされている必要があります。

Citrix Universal Print Server を使用する場合、Citrix Print Manager サービスは、ネイティブプリンタードライバー、Citrix Universal Printer Driver、または Citrix Universal XPS Printer Driver のいずれかを使用してネットワークプリンター接続を作成します。使用するドライバーは、Universal Print Driver の使用ポリシー設定によって制御されます。

現在、すべてのWindowsプリンタードライバーはv3またはv4ドライバーバージョンに分類されます。詳細については、「Microsoft V3およびV4プリンタードライバーアーキテクチャのサポート」を参照してください。

セッションプリンターを追加し、それらがセッションに表示されることを確認するには、次の手順を実行します。

1. Web Studio にサインインし、左ペインで を選択し、 タブをクリックします。
2. **セッションプリンター**ポリシーを有効にします。
3. ポリシーで、セッションプリンターを追加します。プリンターを追加するには、自動作成するプリンターのUNCパスを入力します。プリンターを追加した後、ログオンごとに現在のセッションにカスタマイズされた設定を適用できます。セッションプリンターがリストに表示される必要があります。

4. ポリシーが設定された後、公開されたアプリケーションにセッションプリンターが表示されない場合があります。この問題は、Citrix Virtual Apps サーバーにプリンタードライバーがないか、ポリシーが作成されたものの有効になっていないために発生する可能性があります。

   > **注:**
   >
   > セッションプリンターがネイティブプリンタードライバーを必要とし、そのネイティブプリンタードライバーがVDAにインストールされていない場合、セッションプリンターはセッションに作成されない可能性があります。

5. 公開されたデスクトップを起動し、 **>** でセッションプリンターを手動で追加します。
6. これが失敗した場合は、Citrix Virtual Apps サーバーとプリントサーバー間の通信を調査します。RDP を使用してテストを実行することを検討してください。

プリンターが作成されるのを待つ

Delivery Controller のポリシーを使用して、Citrix Virtual Desktops でこの機能を有効にします。

プリンターの作成を待機する (サーバーデスクトップ):

この設定により、セッションへの接続を遅延させ、クライアントリダイレクトされたプリンターを自動作成できるようになります。

デフォルトでは、接続遅延は発生しません。

プリンターの作成を待機する (Citrix Virtual Apps):

以下の PowerShell コマンドレットを実行すると、マルチセッションホストで実行されている仮想アプリへの接続を遅延させ、アプリケーションが開かれる前にクライアントリダイレクトされたプリンターを自動作成できるようになります。

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation $true
```

デフォルトでは、接続遅延は発生しません。

クライアントプリンターポリシー設定

「**クライアントプリンター**」セクションには、クライアントプリンターのポリシー設定が含まれています。これには、クライアントプリンターの自動作成、プリンタープロパティの保持、およびプリントサーバーへの接続に関する設定が含まれます。

クライアントプリンターの自動作成

この設定は、自動作成されるクライアントプリンターを指定します。この設定は、デフォルトのクライアントプリンター自動作成設定を上書きします。

デフォルトでは、すべてのクライアントプリンターが自動作成されます。

この設定は、**クライアントプリンターリダイレクト**設定が存在し、**許可**に設定されている場合にのみ有効になります。

この設定をポリシーに追加する際は、オプションを選択してください。

- **すべてのクライアントプリンターを自動作成**すると、ユーザーデバイス上のすべてのプリンターが自動的に作成されます。
- **クライアントのデフォルトプリンターのみを自動作成**すると、ユーザーデバイスでデフォルトプリンターとして選択されているプリンターのみが自動的に作成されます。
- **ローカル（非ネットワーク）クライアントプリンターのみを自動作成**すると、LPT、COM、USB、TCP/IP、またはその他のローカルポートを介してユーザーデバイスに直接接続されているプリンターのみが自動的に作成されます。
- **クライアントプリンターを自動作成しない**を選択すると、ユーザーがログオンしたときにすべてのクライアントプリンターの自動作成が無効になります。このオプションを選択すると、クライアントプリンターの自動作成に関するRemote Desktop Services (RDS) の設定が、優先度の低いポリシーのこの設定を上書きします。

汎用ユニバーサルプリンターの自動作成

この設定は、セッション用の汎用Citrix Universal™ Printerオブジェクトの自動作成を有効または無効にします。これらのセッションには、Universal Printingと互換性のあるユーザーデバイスが使用されているセッションのみが含まれます。

デフォルトでは、汎用Universal Printerオブジェクトは自動作成されません。

関連するポリシー設定は次のとおりです。

- ユニバーサルプリントドライバーの使用
- ユニバーサルドライバーの優先順位

PDFユニバーサルプリンターの自動作成

この設定は、以下のセッションでCitrix PDFプリンターの自動作成を有効または無効にします。

- Windows向けCitrix Workspaceアプリ（VDA 7.19以降）
- HTML5 用 Citrix Workspace™ アプリ

- Chrome向けCitrix Workspaceアプリ

デフォルトでは、Citrix PDFプリンターは自動作成されません。

クライアントプリンター名

この設定は、自動作成されたクライアントプリンターの名前付け規則を選択します。

デフォルトでは、標準のプリンター名が使用されます。

「**Standard printer names**」を選択すると、「HPLaserJet 4 from client name in session 3」のようなプリンター名が使用されます。

「**Legacy printer names**」を選択すると、旧式のクライアントプリンター名が使用され、製品のXenDesktopバージョンに存在するレガシープリンター名との下位互換性が維持されます。このオプションは、現在のCitrix Virtual Apps and Desktopsバージョンの製品でも使用できます。レガシープリンター名の例は「Client/clientname#/HPLaserJet 4」です。このオプションはセキュリティが低下します。

Citrix Workspace app for HTML5から起動されたセッションでCitrix PDFプリンターを使用する場合、「**Client printer names**」設定をデフォルトにするか、「**Standard printer names**」を選択してください。「**Legacy printer names**」を選択した場合、Citrix Workspace app for HTML5はCitrix PDFプリンターオプションをサポートしません。

プリントサーバーへの直接接続

この設定は、仮想デスクトップまたはサーバーホスティングアプリケーションからクライアントプリンター用の印刷サーバーへの直接接続を有効または無効にします。ここで、クライアントプリンターはアクセス可能なネットワーク共有でホストされます。

デフォルトでは、直接接続が有効になっています。

ネットワークプリントサーバーが仮想デスクトップまたはサーバーホスティングアプリケーションからWANを介していない場合は、直接接続を有効にします。ネットワークプリントサーバーと仮想デスクトップまたはサーバーホスティングアプリケーションが同じLAN上にある場合、直接通信により印刷が高速化されます。

ネットワークがWANを介している場合、または大幅な遅延や帯域幅の制限がある場合は、直接接続を無効にします。印刷ジョブはユーザーデバイスを介してルーティングされ、そこでネットワークプリントサーバーにリダイレクトされます。ユーザーデバイスに送信されるデータは圧縮されるため、WANを介してデータが転送される際の帯域幅の消費が少なくなります。

2つのネットワークプリンターが同じ名前を持つ場合、ユーザーデバイスと同じネットワーク上のプリンターが使用されます。

プリンタードライバーのマッピングと互換性

この設定は、自動作成されたクライアントプリンターのドライバー置換ルールを指定します。

この設定は、Microsoft OneNoteおよびXPS Document Writerを自動作成されたクライアントプリンターリストから除外するように構成されています。

ドライバー置換ルールを定義する際、指定されたドライバーでプリンターが作成されることを許可または防止できます。また、作成されたプリンターがユニバーサルプリントドライバーのみを使用することを許可できます。ドライバー置換は、ユーザーデバイスが提供するプリンタードライバー名を上書きまたはマッピングし、サーバー上の同等のドライバーに置き換えます。これらのルールにより、サーバーアプリケーションは、サーバーと同じドライバーを持つがドライバー名が異なるクライアントプリンターにアクセスできるようになります。

次のことができます。

- ドライバーマッピングを追加する
- 既存のマッピングを編集する
- マッピングのカスタム設定を上書きする
- マッピングを削除する
- リスト内のドライバーエントリの順序を変更する

マッピングを追加する際は、クライアントプリンタードライバー名を入力し、置き換えたいサーバードライバーを選択します。

プリンタープロパティの保持

この設定では、プリンタープロパティを保存するかどうか、および保存場所を指定します。

デフォルトでは、システムはプリンタープロパティをユーザーデバイスに保存するか（利用可能な場合）、またはユーザープロファイルに保存するかを決定します。

この設定をポリシーに追加するときは、オプションを選択してください。

- クライアントデバイスのみに保存は、保存されない必須プロファイルまたは移動プロファイルを持つユーザーデバイス用です。
- ユーザープロファイルのみに保持は、帯域幅（このオプションはネットワークトラフィックを削減します）とログオン速度によって制約されるユーザーデバイス、またはレガシープラグインを使用するユーザー用です。このオプションは、プリンタープロパティをサーバー上のユーザープロファイルに保存し、ユーザーデバイスとのプロパティ交換を防ぎます。このオプションは、Remote Desktop Services (RDS) の移動プロファイルが使用されている場合にのみ適用されます。

- クライアントに保存されていない場合のみプロファイルに保持すると、システムがプリンタープロパティの保存場所を決定できます。プリンタープロパティは、利用可能な場合はユーザーデバイスに、またはユーザープロファイルに保存されます。このオプションは最も柔軟ですが、ログオン時間を遅くしたり、システムチェックのために余分な帯域幅を使用したりする可能性があります。
- プリンタープロパティを保持しないは、プリンタープロパティの保存を防ぎます。

保持および復元されたクライアントプリンター

この設定は、ユーザーデバイス上のプリンターの保持と再作成を有効または無効にします。デフォルトでは、クライアントプリンターは自動的に保持および復元されます。

保持されたプリンターとは、次回のセッション開始時に再度作成される、または記憶されるユーザー作成のプリンターです。Citrix Virtual Apps™ が保持されたプリンターを再作成する場合、**クライアントプリンターの自動作成**設定を除くすべてのポリシー設定が考慮されます。

復元されたプリンターとは、管理者が完全にカスタマイズし、クライアントポートに永続的にアタッチされた保存状態を持つプリンターです。

CITRIX PDFユニバーサルプリンタードライバー

Citrix PDFユニバーサルプリンタードライバーを使用すると、ホストされたアプリケーションで開かれたドキュメントや、Citrix Virtual Apps and Desktops によって提供される仮想デスクトップで実行されているアプリケーションを印刷できます。ユーザーが**Citrix PDFプリンター**オプションを選択すると、ドライバーはファイルをPDFに変換し、PDFをローカルデバイスに転送します。その後、PDFはローカルに接続されたプリンターから表示および印刷するために開かれます。PDFは、Citrix Universal Printing でサポートされている形式の1つです（EMFおよびXPSに加えて）。PDFプリンターは、Citrixポリシーを使用して有効化、構成、およびデフォルトとして設定できます。**Citrix PDFプリンター**オプションは、Windows、Chrome、およびHTML5用のCitrix Workspaceアプリのユーザーが利用できます。

> **注：**
>
> WindowsエンドポイントにはPDFビューアーが必要です。クライアントには、PDFファイルを開くためにWindowsにファイルタイプ関連付けが登録されているアプリケーションが必要です。

ドライバーポリシー設定

「**ドライバー**」セクションには、プリンタードライバーに関連するポリシー設定が含まれています。

インボックスプリンタードライバーの自動インストール

> **注**
>
> このリリースでは、このポリシーはVDAをサポートしていません。

この設定は、以下のプリンタードライバーの自動インストールを有効または無効にします。

- Windowsインボックスドライバーセット
- `pnputil.exe /a`を使用してホストにステージングされたドライバーパッケージ

デフォルトでは、これらのドライバーは必要に応じてインストールされます。

ユニバーサルドライバーの優先順位

この設定は、リストの最初のエントリから始まる、ユニバーサルプリンタードライバーが使用される順序を指定します。

デフォルトでは、優先順位は次のとおりです。

- EMF
- XPS
- PCL5c (ピーシーエルファイブシー)
- PCL4
- PS

ドライバーの追加、編集、削除、およびリスト内のドライバーの順序変更が可能です。

ユニバーサルプリントドライバーの使用

この設定は、ユニバーサル印刷を使用するタイミングを指定します。

デフォルトでは、要求されたドライバーが利用できない場合にのみユニバーサル印刷が使用されます。

ユニバーサル印刷は、標準のモデル固有ドライバーの代わりに汎用プリンタードライバーを使用し、ホストコンピューターでのドライバー管理の負担を軽減する可能性があります。ユニバーサルプリントドライバーの可用性は、ユーザーデバイス、ホスト、およびプリントサーバーソフトウェアの機能に依存します。特定の構成では、ユニバーサル印刷が利用できない場合があります。

この設定をポリシーに追加する場合は、次の表からオプションを選択します。

オプション	説明
プリンターモデル固有のドライバーのみを使用する	クライアントプリンターが、サインイン時に自動作成される標準のモデル固有ドライバーのみを使用することを指定します。要求されたドライバーが利用できない場合、クライアントプリンターは自動作成できません。
ユニバーサル印刷のみを使用する	標準のモデル固有ドライバーは使用されないことを指定します。プリンターの作成にはユニバーサルプリントドライバーのみが使用されます。
要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	利用可能な場合、プリンター作成に標準のモデル固有ドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なユニバーサルドライバーで自動的に作成されます。
ユニバーサル印刷が利用できない場合にのみ、プリンターモデル固有のドライバーを使用する	利用可能な場合、ユニバーサルプリントドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なモデル固有のプリンタードライバーで自動的に作成されます。

ユニバーサルプリントサーバーポリシー設定

ユニバーサルプリントサーバーセクションには、ユニバーサルプリントサーバーを処理するためのポリシー設定が含まれています。

SSL暗号スイート

この設定は、暗号化された印刷データストリーム (CGP) 接続のためにユニバーサルプリントクライアントで使用されるSSL/TLS暗号スイートのセットを指定します。

暗号化された印刷Webサービス (HTTPS/SOAP) 接続のためにユニバーサルプリントクライアントで使用される暗号スイートパッケージを制御するには、を参照してください。

デフォルト値: ALL

この設定には次の値があります: ALL、COM、またはGOV。

各値に対応する暗号スイートは次のとおりです:

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL準拠モード

この設定は、Universal Print Clientが暗号化された印刷データストリーム (CGP) 接続に使用するNIST Special Publication 800-52への準拠レベルを指定します。

デフォルト値: なし。

この設定には次の値があります:

なし。

暗号化された印刷データストリーム (CGP) 接続は、デフォルトの準拠モードを使用します。

SP800-52。

暗号化された印刷データストリーム (CGP) 接続は、NIST Special Publication 800-52準拠モードを使用します。

SSL有効

この設定は、Universal Print Clientが次の目的でSSL/TLSを使用するかどうかを指定します:

- 印刷データストリーム (CGP) 接続
- Webサービス (HTTP/SOAP) 接続

Universal Print Serverを有効にするを**Windowsのネイティブリモート印刷へのフォールバックを有効にする**に設定すると、フォールバック接続はMicrosoft Windowsネットワーク印刷プロバイダーによって行われます。この設定は、これらのフォールバック接続には影響しません。

既定値: 無効

この設定には次の値があります。

有効。

Universal Print Clientは、SSL/TLSを使用してUniversal Print Serverに接続します。

無効。

Universal Print Clientは、SSL/TLSを使用してUniversal Print Serverに接続します。

SSL FIPSモード

この設定は、Universal Print Clientが印刷データストリーム（CGP）接続に使用するSSL/TLS暗号化モジュールがFIPSモードで実行されるかどうかを指定します。

既定値: 無効

この設定には次の値があります。

有効。

FIPSモードがオンになります。

無効。

FIPSモードがオフになります。

SSLプロトコルバージョン

この設定は、Universal Print Client が使用する SSL/TLS プロトコルバージョンを指定します。

デフォルト値: ALL

この設定には次の値があります。

ALL。

TLS バージョン 1.0、1.1、または 1.2 を使用します。

TLSv1. バージョン.

TLS バージョン 1.0 を使用します。

TLSv1.1。

TLS バージョン 1.1 を使用します。

TLSv1.2。

TLS バージョン 1.2 を使用します。

SSL UNIVERSAL PRINT SERVER 暗号化印刷データストリーム (CGP) ポート

この設定は、Universal Print Server 暗号化印刷データストリーム (CGP) ポートの TCP ポート番号を指定します。このポートは、印刷ジョブのデータを受信します。

デフォルト値: 443

SSL UNIVERSAL PRINT SERVER 暗号化 WEB サービス (HTTPS/SOAP) ポート

この設定は、Universal Print Serverの暗号化されたWebサービス（HTTPS/SOAP）ポートのTCPポート番号を指定します。このポートは、印刷コマンドのデータを受信します。

デフォルト値: 8443

UNIVERSAL PRINT SERVERの有効化

このポリシーは、Citrix Universal Print Server (UPS) の使用を有効または無効にします。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含む組織単位 (OU) に適用します。このポリシー設定には、Citrix UPSコンポーネントが要求されたプリントサーバーにインストールされていないか、利用できない場合に、ネイティブのWindowsリモート印刷サービスを使用してプリントサーバーへの接続を許可するフォールバックオプションが含まれています。このポリシーへの変更は、VDAが再起動された後にのみ適用されます。

デフォルトでは、Universal Print Serverは無効になっています。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- **Windows ネイティブのリモート印刷へのフォールバックを有効にする**: Universal Print Server は、可能であればネットワークプリンター接続を処理します。Universal Print Server が利用できない場合、Windows Print Provider が使用されます。Windows Print Provider は、以前に Windows Print Provider で作成されたすべてのプリンターを引き続き処理します。
- **Windows ネイティブのリモート印刷へのフォールバックなしで有効にする**: Universal Print Server は、ネットワークプリンター接続を排他的に処理します。Universal Print Server が利用できない場合、ネットワークプリンター接続は失敗します。この設定は、Windows Print Provider を介したネットワーク印刷を実質的に無効にします。この設定を含むポリシーがアクティブな間は、以前に Windows Print Provider で作成されたプリンターは作成されません。
- **無効**: Universal Print Server 機能は無効になります。UNC 名を持つネットワークプリンターに接続する際、Universal Print Server への接続は試行されません。リモートプリンターへの接続は、引き続き Windows ネイティブのリモート印刷機能を使用します。

UNIVERSAL PRINT SERVER印刷データストリーム (CGP) ポート

この設定は、Universal Print Server 印刷データストリームの Common Gateway Protocol (CGP) リスナーが使用する TCP ポート番号を指定します。このポリシー設定は、プリントサーバーを含む OU にのみ適用します。

デフォルトでは、ポート番号は7229に設定されています。

有効なポート番号は1～65535の範囲である必要があります。

UNIVERSAL PRINT SERVER印刷ストリーム入力帯域幅制限 (KBPS)

この設定は、印刷データの転送速度の上限（キロビット/秒）を指定します。転送速度は、各印刷ジョブからCGPを使用してUniversal Print Serverに配信される印刷データに対して計算されます。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含むOUに適用します。

デフォルトでは、値は0であり、上限がないことを指定します。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) ポート

この設定は、Universal Print ServerのWebサービス (HTTP/SOAP) リスナーが使用するTCPポート番号を指定します。Universal Print Serverは、ネットワーク印刷シナリオでCitrixユニバーサル印刷ドライバーの使用を可能にするオプションコンポーネントです。

Universal Print Serverが使用される場合、印刷コマンドはCitrix Virtual Apps and Desktopsホストから SOAP over HTTP経由でUniversal Print Serverに送信されます。この設定は、Universal Print Serverが受信HTTP/SOAPリクエストをリッスンするデフォルトのTCPポートを変更します。

ホストと印刷サーバーのHTTPポートは両方とも同じように構成する必要があります。ポートを同じように構成しない場合、ホストソフトウェアはUniversal Print Serverに接続しません。この設定は、Citrix Virtual Apps and Desktops上のVDAを変更します。さらに、Universal Print Serverのデフォルトポートも変更する必要があります。

デフォルトでは、ポート番号は8080に設定されています。

有効なポート番号は0～65535の範囲である必要があります。

負荷分散用のUNIVERSAL PRINT SERVER

この設定は、他のCitrix®印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用されるUniversal Print Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべての印刷サーバーが同じ共有プリンターのセットを持つことを推奨します。負荷分散のために追加できる印刷サーバーの数に上限はありません。

この設定は、印刷サーバーのフェイルオーバー検出とプリンター接続の回復も実装します。印刷サーバーは定期的に可用性がチェックされます。サーバー障害が検出された場合、そのサーバーは負荷分散スキームから削除されます。また、そのサーバー上のプリンター接続は、他の利用可能な印刷サーバーに再分散されます。障害が発生した印刷サーバーが回復すると、負荷分散スキームに戻されます。

Validate Serversをクリックして、各サーバーが印刷サーバーであること、サーバーリストに重複するサーバー名が含まれていないこと、およびすべてのサーバーに同一の共有プリンターセットがインストールされていることを確認します。この操作には時間がかかる場合があります。

UNIVERSAL PRINT SERVERサービス停止しきい値

この設定は、ロードバランサーが利用できない印刷サーバーが回復するのを待つ時間を指定します。この時間を過ぎると、サーバーは永続的にオフラインであると判断され、その負荷は他の利用可能な印刷サーバーに再分散されます。

デフォルトでは、しきい値は180（秒）に設定されています。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 接続タイムアウト

この設定は、Universal Print Client が Universal Print Server Web サービス connect() 操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1～60（両端を含む）の場合、Universal Print Client は操作が完了するまで指定された時間待機します。この操作は、TCPソケット接続操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Client はオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Client は、Universal Print Server と通信する Virtual Delivery Agent (VDA) のコンポーネントです。

> **注：**
>
> このポリシー設定は、VDAバージョン7.35以降に適用されます。

ユニバーサルプリントサーバー WEB サービス (HTTP/SOAP) 受信タイムアウト

この設定は、Universal Print Client が Universal Print Server Web サービス recv() 操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があり、これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1〜60（両端を含む）の場合、Universal Print Client は操作が完了するまで指定された時間待機します。この操作は、TCPソケット受信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Clientはオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Clientは、Universal Print Serverと通信するVirtual Delivery Agent (VDA) のコンポーネントです。

注:

このポリシー設定は、VDAバージョン7.35以降に適用されます。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 受信タイムアウト

この設定は、Universal Print ClientがUniversal Print Server Webサービスのsend()操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Clientは、操作が完了するまで指定された時間待機します。この操作は、TCPソケット受信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Clientはオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Clientは、Universal Print Serverと通信するVirtual Delivery Agent (VDA) のコンポーネントです。

> **注:**
>
> このポリシー設定は、VDAバージョン7.35以降で適用されます。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 送信タイムアウト

この設定は、Universal Print Client が Universal Print Server Webサービスの send() 操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Client は操作が完了するまで指定された時間待機します。この操作はTCPソケット送信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Client はオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Client は、Universal Print Server と通信するVDAのコンポーネントです。

> **注:**
>
> このポリシー設定は、VDAバージョン7.35以降で適用されます。

ユニバーサル印刷ポリシー設定

ユニバーサル印刷セクションには、ユニバーサル印刷を管理するためのポリシー設定が含まれています。

ユニバーサル印刷EMF処理モード

この設定は、Windowsユーザーデバイス上のEMFスプールファイルの処理方法を制御します。

デフォルトでは、EMFレコードはプリンターに直接スプールされます。

この設定をポリシーに追加するときは、オプションを選択します。

- プリンター用のEMFを再処理すると、EMFスプールファイルが強制的に再処理され、ユーザーデバイス上のGDIサブシステムを介して送信されます。この設定は、EMFの再処理を必要とするが、セッションで自動的に選択されない可能性のあるドライバーに使用できます。
- Citrix Universal™印刷ドライバーと併用すると、プリンターに直接スプールすることで、EMFレコードがスプールされ、処理のためにユーザーデバイスに配信されます。通常、これらのEMFスプールファイルはクライアントのスプールキューに直接挿入されます。EMF形式と互換性のあるプリンターおよびドライバーの場合、これが最速の印刷方法です。

ユニバーサル印刷画像圧縮制限

この設定は以下を指定します:

- Citrix Universal Print Driverで印刷される画像に利用可能な最大品質
- Citrix Universal Print Driverで印刷される画像に利用可能な最小圧縮レベル

デフォルトでは、画像圧縮制限は「最高品質（ロスレス圧縮）」に設定されています。

「圧縮なし」が選択されている場合、EMF印刷のみ圧縮が無効になります。

この設定をポリシーに追加するときは、オプションを選択します。

- 圧縮なし
- 最高品質 (ロスレス圧縮)
- 高音質
- 標準品質
- 低品質 (最大圧縮)

ユニバーサル印刷最適化のデフォルト設定を含むポリシーにこの設定を追加する場合は、次の点に注意してください。

- **ユニバーサル印刷画像圧縮制限**設定の圧縮レベルが、**ユニバーサル印刷最適化のデフォルト**設定で定義されているレベルよりも低いとします。この場合、画像はユニバーサル印刷画像圧縮制限設定で定義されているレベルで圧縮されます。

- 圧縮が無効になっている場合、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」および「ヘビーウェイト圧縮を有効にする」オプションは、ポリシーに影響しません。

ユニバーサル印刷最適化のデフォルト

この設定は、セッション用にユニバーサル印刷ドライバーが作成される際の印刷最適化のデフォルト値を指定します。

- 希望する画質は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、標準品質が有効になっており、ユーザーは標準または低品質の圧縮を使用してのみ画像を印刷できます。
- ヘビーウェイト圧縮を有効にするは、画質を損なうことなく、希望する画質で設定された圧縮レベルを超えて帯域幅を削減するかどうかを有効または無効にします。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
- 画像とフォントのキャッシュ設定は、印刷ストリームに複数回出現する画像とフォントをキャッシュするかどうかを指定します。この設定により、一意の画像またはフォントがプリンターに一度だけ送信されるようになります。デフォルトでは、埋め込み画像とフォントはキャッシュされます。これらの設定は、ユーザーデバイスがこの動作をサポートしている場合にのみ適用されます。
- 管理者以外のユーザーがこれらの設定を変更することを許可するは、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。

注：これらのオプションはすべてEMF印刷でサポートされています。XPS印刷では、「希望する画質」オプションのみがサポートされます。

この設定を**ユニバーサル印刷画像圧縮制限**設定を含むポリシーに追加する場合は、次の点に注意してください。

- **ユニバーサル印刷画像圧縮制限**設定の圧縮レベルが、**ユニバーサル印刷最適化のデフォルト**設定で定義されているレベルよりも低い場合を考慮してください。この場合、画像はユニバーサル印刷画像圧縮制限設定で定義されているレベルで圧縮されます。
- 圧縮が無効になっている場合、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」および「ヘビーウェイト圧縮を有効にする」オプションは、ポリシーに影響しません。

ユニバーサル印刷プレビューの優先設定

この設定は、自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビュー機能を使用するかどうかを指定します。

デフォルトでは、自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビューは使用されません。

この設定をポリシーに追加するときは、オプションを選択します。

- 自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビューを使用しない
- 自動作成されたプリンターに対してのみ印刷プレビューを使用する
- 汎用ユニバーサルプリンターに対してのみ印刷プレビューを使用する
- 自動作成されたプリンターと汎用ユニバーサルプリンターの両方に対して印刷プレビューを使用する

ユニバーサル印刷の印刷品質制限

この設定は、セッションで印刷出力を生成するために利用できる最大ドット/インチ (dpi) を指定します。

デフォルトでは、「制限なし」が有効になっており、ユーザーは接続先のプリンターで許可されている最高の印刷品質を選択できます。

この設定が構成されている場合、出力解像度の観点から、ユーザーが利用できる最大印刷品質が制限されます。印刷品質自体と、ユーザーが接続するプリンターの印刷品質機能の両方が、構成された設定に制限されます。

たとえば、中解像度 (600 DPI) に構成されている場合、ユーザーは最大 600 DPI の品質でしか出力を印刷できません。また、**ユニバーサルプリンター**ダイアログボックスの**詳細設定**タブにある**印刷品質**設定には、中品質 (600 DPI) までの解像度設定のみが表示されます。

この設定をポリシーに追加するときは、オプションを選択します。

- 下書き (150 DPI)
- 低解像度 (300 DPI)
- 中解像度 (600 DPI)
- 高解像度 (1200 DPI)
- 制限なし

セキュリティポリシー設定

セキュリティセクションには、セッション暗号化とログオンデータの暗号化を構成するためのポリシー設定が含まれています。

SecureICAの最小暗号化レベル

この設定は、サーバーとユーザーデバイス間で送信されるセッションデータを暗号化する最小レベルを指定します。

重要: Virtual Delivery Agent 7.xの場合、このポリシー設定は、RC5 128ビット暗号化によるログオンデータの暗号化を有効にするためにのみ使用できます。その他の設定は、Citrix Virtual Apps and Desktopsのレガシーバージョンとの下位互換性のためにのみ提供されています。

VDA 7.xの場合、セッションデータの暗号化はVDAのDelivery Groupの基本設定を使用して行われます。Delivery GroupでEnable Secure ICAが選択されている場合、セッションデータはRC5 (128ビット) 暗号化を使用して暗号化されます。Delivery GroupでEnable Secure ICAが選択されていない場合、セッションデータは基本暗号化で暗号化されます。

この設定をポリシーに追加するときは、オプションを選択してください。

- Basicは、非RC5アルゴリズムを使用してクライアント接続を暗号化します。これにより、データストリームが直接読み取られるのを防ぎますが、復号化は可能です。デフォルトでは、サーバーはクライアント-サーバー間のトラフィックにBasic暗号化を使用します。
- RC5 (128ビット) ログオンは、RC5 128ビット暗号化を使用してログオンデータのみを暗号化し、クライアント接続にはBasic暗号化を使用します。
- RC5 (40ビット) は、RC5 40ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (56ビット) は、RC5 56ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (128ビット) は、RC5 128ビット暗号化を使用してクライアント接続を暗号化します。

クライアント-サーバー暗号化に指定する設定は、環境内の他の暗号化設定やWindowsオペレーティングシステムと相互作用する可能性があります。サーバーまたはユーザーデバイスのいずれかで、より高い優先度の暗号化レベルが設定されている場合を考慮してください。この場合、公開リソースに指定した設定が上書きされる可能性があります。

特定のユーザーの通信とメッセージの整合性をさらに保護するために、暗号化レベルを上げることができます。ポリシーでより高い暗号化レベルが必要な場合、より低い暗号化レベルを使用しているCitrix Receiversは接続を拒否されます。

SecureICAは認証やデータ整合性のチェックを行いません。サイトにエンドツーエンドの暗号化を提供するには、SecureICAをTLS暗号化と組み合わせて使用してください。

SecureICA は FIPS 準拠のアルゴリズムを使用しません。この設定が問題となる場合、サーバーと Citrix Receiver を SecureICA を使用しないように構成してください。

SecureICAは、機密保持のためにRFC 2040で説明されているRC5ブロック暗号を使用します。ブロックサイズは64ビット（32ビットワード単位の倍数）です。キー長は128ビットです。ラウンド数は12です。

RC5 ブロック暗号のキーは、セッションが作成されるときにネゴシエートされます。ネゴシエーションは Diffie-Hellman アルゴリズムを使用して実行されます。このネゴシエーションでは、Diffie-Hellman の公開パラメーターが使用されます。これらのパラメーターは、Virtual Delivery Agent がインストールされるときに Windows レジストリに保存されます。公開パラメーターは秘密ではありません。Diffie-Hellman ネゴシエーションの結果は秘密鍵であり、そこから RC5 ブロック暗号のセッションキーが導出されます。ユーザーログオンとデータ転送には、個別のセッションキーが使用されます。また、Virtual Delivery Agent との間でのトラフィックにも個別のセッションキーが使用されます。したがって、各セッションには 4 つのセッションキーがあります。秘密鍵とセッションキーは保存されません。RC5 ブロック暗号の初期化ベクトルも秘密鍵から導出されます。

サーバー制限ポリシー設定

サーバー制限セクションには、アイドル接続を制御するためのポリシー設定が含まれています。

サーバーアイドルタイマー間隔

この設定は、ユーザーからの入力がない場合に、中断されないユーザーセッションがどのくらいの期間維持されるかを決定します。データはミリ秒で計算されます。

デフォルトでは、アイドル接続は切断されません（サーバーアイドルタイマー間隔 = 0）。Citrix® は、この値を最小 60000 ミリ秒（60 秒）に設定することを推奨します。

ポリシーを表示するには、「**複数のバージョン**」を選択し、シングルセッション OS バージョンの選択を解除してから、「**サーバー制限**」を選択します。

> **注**
>
> このポリシー設定が使用されている場合、セッションが指定された時間アイドル状態であったときに、「アイドルタイマーの期限が切れました」というダイアログボックスがユーザーに表示されることがあります。Citrix ポリシー設定は、この Microsoft ダイアログボックスメッセージを制御しません。詳細については、`<http://support.citrix.com/article/CTX118618>` を参照してください。

セッション制限ポリシー設定

セッション制限セクションには、セッションが強制的にログオフされるまでに接続状態を維持する期間を制御するポリシー設定が含まれています。

切断されたセッションタイマー

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされた状態を維持する期間を指定するタイマーを有効または無効にします。

このタイマーが有効になっている場合、タイマーの期限が切れると、切断されたセッションはログオフされます。

デフォルトでは、切断されたセッションはログオフされません。

Remote PC Accessの切断されたセッションタイマー

この設定は、タイマーの期限が切れた後に切断されたユーザーセッションをログオフするタイマーを有効または無効にします。この設定を有効にする場合は、**切断されたセッションタイマー間隔**設定を使用して、ユーザーセッションがログオフされるまでに切断されたデスクトップがロックされた状態を維持する分数を指定します。

デフォルトでは、この設定は無効になっています。

切断されたセッションタイマー間隔

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされた状態を維持する分数を指定します。

デフォルトでは、期間は1,440分（24時間）です。

切断されたセッションタイマー – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでに持続できる期間を決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっており、切断されたセッションはログオフされません。

切断されたセッションタイマー間隔 – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでにどのくらいの期間（分単位）持続できるかを決定します。デフォルトでは、期間は1440分（24時間）です。

セッション接続タイマー

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。このタイマーが有効になっている場合、タイマーの期限が切

れるとセッションは切断されるか、ログオフされます。Microsoft の「**時間制限に達したときにセッションを終了する**」設定が、セッションの次の状態を決定します。

デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大分数を示します。

デフォルトでは、最大継続時間は1,440分（24時間）です。

セッション接続タイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間の途切れない接続の最大分数を示します。デフォルトでは、最大継続時間は1440分（24時間）です。

セッションアイドルタイマー

ユーザーが何も入力しない場合、この設定は以下を有効または無効にするために使用されます。

- デスクトップへの途切れないユーザーデバイス接続がどのくらいの期間維持されるかを指定するタイマー。

このタイマーの期限が切れると、セッションは切断状態になり、「**切断されたセッションタイマー**」が適用されます。「**切断されたセッションタイマー**」が無効になっている場合、セッションはログオフされません。

デフォルトでは、このタイマーは有効になっています。

セッションアイドルタイマー間隔

ユーザーからの入力がない場合、この設定は以下を指定するために使用されます。

- デスクトップへのユーザーデバイスの途切れない接続が維持される分数。

デフォルトでは、アイドル状態の接続は1,440分（24時間）維持されます。

セッションアイドルタイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間のアイドル接続の最大期間を決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッションアイドルタイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間のアイドル接続が何分間維持されるかを指定します。デフォルトでは、最大期間は1440分（24時間）です。

> **注:**
>
> Citrix®ポリシーを使用して構成されたマルチセッションマシンのタイマー設定は、Microsoftグループポリシーを通じて構成されたタイマー設定を上書きすることが想定されています。予期しない動作を避けるため、いずれかの方法を使用してタイマー設定を構成することをお勧めします。

セッションの信頼性ポリシー設定

「**セッションの信頼性**」セクションには、セッションの信頼性接続を管理するためのポリシー設定が含まれています。

セッションの信頼性接続

この設定により、ネットワーク接続が失われたときにセッションを開いたままにすることができます。セッションの信頼性は、自動クライアント再接続とともに、ネットワーク障害から回復した後、ユーザーがCitrix Workspace™アプリセッションに自動的に再接続できるようにします。デフォルトでは、セッションの信頼性は許可されています。

Web Studioの設定は、以下のクライアントに適用されます。

- Citrix Workspaceアプリ1808以降
- シトリックス レシーバー Windows版 4.7 以降。

Web Studioポリシーは、クライアント上のCitrix Receiver™グループポリシーオブジェクトを上書きします。Web Studioでのこれらのポリシーの更新は、セッションの信頼性をサーバーからクライアントに同期します。

> **注:**
>
> - Citrix Receiver for Windows 4.7以降およびCitrix Workspaceアプリ for Windows - Web Studioでポリシーを設定します。

- Citrix Receivers for Windows 4.7より前のバージョン - Web Studioでポリシーを設定します。また、一貫した動作のために、クライアントでCitrix Receiverグループポリシーオブジェクトテンプレートを設定します。

セッションの信頼性により、ネットワーク接続が中断された場合でも、セッションはアクティブな状態を保ち、ユーザーの画面に表示されます。ユーザーは、ネットワーク接続が再開されるまで、使用しているアプリケーションを引き続き見ることができます。

セッションの信頼性を使用して、サーバー上でセッションをアクティブな状態に保ちます。接続が失われたことを示すために、ユーザーディスプレイは不透明になります。中断中にユーザーはフリーズしたセッションを見る可能性があります。ネットワーク接続が復元されると、ユーザーはアプリケーションとの対話を再開できます。セッションの信頼性により、再認証のプロンプトなしでユーザーが再接続されます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、2つの機能は順次動作します。セッションの信頼性は、セッションの信頼性タイムアウト設定で指定された時間の後にユーザーセッションを閉じ（または切断し）ます。その後、自動クライアント再接続設定が有効になり、切断されたセッションにユーザーを再接続しようとします。

デフォルトでは、セッションの信頼性は許可されています。

注:

Citrix ADCを使用している場合、ICA接続をプロキシするには、Citrix StoreFrontの「**Citrix Gatewayの管理**」/「**Secure Ticket Authority**」で「**セッションの信頼性を有効にする**」を選択する必要があります。

セッションの信頼性ポート番号

この設定は、受信セッションの信頼性接続に使用するTCPポート番号を指定します。

デフォルトでは、ポート番号は2598に設定されています。

セッションの信頼性タイムアウト

この設定は、秒単位の時間を指定します。この時間は、セッションの信頼性プロキシがユーザーの再接続を待機し、その後セッションが切断されるまでの時間です。

セッションが開いている時間を延長することはできますが、この機能は利便性のためであり、ユーザーに再認証を促すものではありません。セッションが開いている時間が長くなるほど、ユーザーがデバイスを放置し、不正なユーザーがアクセスする可能性が高まります。

デフォルトでは、タイムアウトは180秒、つまり3分に設定されています。

セッションウォーターマークポリシー設定

「**セッションウォーターマーク**」セクションには、この機能を構成するためのポリシー設定が含まれています。 この機能を有効にすると、VDAマシンのネットワーク帯域幅とCPU使用率が大幅に増加します。利用可能なハードウェアリソースに基づいて、選択したVDAマシンにセッションウォーターマークを設定することをお勧めします。

> **重要**
>
> 他のウォーターマークポリシー設定を有効にするには、セッションウォーターマークを有効にしてください。より良いユーザーエクスペリエンスを実現するために、2つを超えるウォーターマークテキスト項目を有効にしないでください。

セッションウォーターマークを有効にする

この設定を有効にすると、セッションディスプレイにはセッション固有の情報を表示する不透明なテキストウォーターマークが表示されます。他のウォーターマーク設定は、この設定が有効になっていることに依存します。

デフォルトでは、セッションウォーターマークは無効になっています。

クライアントIPアドレスを含める

この設定を有効にすると、セッションは現在のクライアントIPアドレスをウォーターマークとして表示します。

デフォルトでは、クライアントIPアドレスを含めるは無効になっています。

接続時間を含める

この設定を有効にすると、セッションウォーターマークに接続時間が表示されます。形式はyyyy/mm/dd hh:mmです。表示される時刻は、システムクロックとタイムゾーンに基づいています。

デフォルトでは、接続時間を含めるは無効になっています。

ログオンユーザー名を含める

この設定を有効にすると、セッションは現在のログオンユーザー名をウォーターマークとして表示します。表示形式はUSERNAME@DOMAINNAMEです。ユーザー名は最大20文字にすることをお勧めします。ユーザー名が20文字を超えると、文字フォントが過度に小さくなったり、切り捨てられたりして、ウォーターマークの効果が低下する可能性があります。

デフォルトでは、ログオンユーザー名を含めるが有効になっています。

VDAホスト名を含める

この設定を有効にすると、セッションは現在のICA®セッションのVDAホスト名をウォーターマークとして表示します。

デフォルトでは、VDAホスト名を含めるが有効になっています。

VDA IPアドレスを含める

この設定を有効にすると、セッションは現在のICAセッションのVDA IPアドレスをウォーターマークとして表示します。

デフォルトでは、VDA IPアドレスは無効になっています。

セッションウォーターマークのスタイル

この設定は、単一のウォーターマークテキストラベルを表示するか、複数のラベルを表示するかを制御します。**値**ドロップダウンメニューから**複数**または**単一**を選択します。

複数はセッションに5つのウォーターマークラベルを表示します。中央に1つ、四隅に4つです。

単一はセッションの中央に単一のウォーターマークラベルを表示します。

デフォルトでは、セッションウォーターマークスタイルは複数です。

ウォーターマークのカスタムテキスト

この設定を使用すると、セッションウォーターマークに表示するカスタムテキスト（例：会社名）を適用できます。空でない文字列を設定すると、ウォーターマークで有効になっている他の情報を追加して、テキストを新しい行に表示します。ウォーターマークカスタムテキストは25 Unicode文字に制限されています。より長い文字列を設定した場合、25文字に切り詰められます。

デフォルトのテキストはありません。

Citrix Virtual Apps and Desktops™ 7 2206以降、テキストにカスタムタグを使用してさらにカスタマイズを追加できます。その結果、カスタムテキストの最大文字数は1024に増加しました。

ウォーターマーク設定で利用可能なタグは、次の表に記載されています。

タグ	説明	例
`<font=value>`	ウォーターマークテキストのフォントを変更できます。値は、VDAで利用可能なフォントの名前です。	`<font=Courier New>`
`<fontzoom=value>`	フォントのズーム率を設定できます。ウォーターマークテキストの200%ズームの場合、値は200です。	`<fontzoom=200>`
`<position=value>`	ウォーターマークテキストの位置を変更できます。値は `center`、`topleft`、`topright`、`bottomleft`、および `bottomright` です。このタグはシングルスタイルでのみ適用可能です。	`<position=topright>`
`<rotation=value>`	ウォーターマークテキストを回転できます。値は度数で指定され、範囲は-360から360です。	`<rotation=45>`
`<style=value>`	表示スタイルを変更できます。このタグはセッションウォーターマークスタイルポリシーを上書きします。	`<style=single>`

利用可能なウォーターマークスタイルは次のとおりです。

- シングルスタイル - セッションの中央に単一のウォーターマークテキストラベルが表示されます。位置タグを使用して場所を変更できます。
- xスタイルまたは複数 - セッションに5つのウォーターマークラベルが表示されます。中央に1つ、各コーナーに1つずつです。
- タイル - セッションに複数のラベルが表示されます。ウォーターマークテキストは画面全体に均等に配置されます。

ウォーターマークテキストを変更するために利用可能なタグは、次の表に記載されています。

タグ	説明
`<clientip>`	エンドポイントのIPアドレス。
`<date>`	セッションが確立された日付。
`<domain>`	ログインしているユーザーアカウントのドメイン名。
`<hostname>`	VDA のマシン名。
`<newline>`	追加の行を作成します。
`<serverip>`	VDA の IP アドレス。
`<time>`	セッションが確立された時刻。
`<username>`	ユーザーの名前。

注:

- **ウォーターマークカスタムテキスト**ポリシーは、**セッションウォーターマークを有効にする**ポリシーが有効になっている場合にのみ適用されます。その既定値は*無効*です。
- ウォーターマークテキストを変更するためのタグを使用する場合、**セッションウォーターマークを有効にする**を除く、他のすべてのセッションウォーターマークポリシーは無視されます。ウォーターマークテキスト設定にタグを使用する場合、他のすべてのウォーターマークポリシーを使用できます。

透かしの透明度

ウォーターマークの不透明度を0から100まで指定できます。指定された値が大きいほど、ウォーターマークは不透明になります。

デフォルトでは、値は17です。

TWAINデバイスのポリシー設定

TWAINデバイスセクションには、次のポリシー設定が含まれています。

- デジタルカメラやスキャナーなどのクライアントTWAINデバイスのマッピング

- サーバーからクライアントへの画像転送の最適化

> **注:**
>
> TWAIN 2.0は、Citrix Receiver for Windows 4.5でサポートされています。

クライアントTWAINデバイスのリダイレクト

TWAINデバイスは、TWAINプロトコルを使用して、サーバーでホストされている画像処理アプリケーションと通信します。

この設定は、ユーザーがユーザーデバイス上のTWAINデバイスにアクセスすることを許可または禁止します。デフォルトでは、TWAINデバイスのリダイレクトは許可されています。

関連するポリシー設定は次のとおりです。

- TWAIN圧縮レベル
- TWAINデバイスのリダイレクト帯域幅制限
- TWAINデバイスリダイレクト帯域幅制限の割合

TWAIN圧縮レベル

この設定は、クライアントからサーバーへの画像転送の圧縮レベルを指定します。最良の画質には「低」、良好な画質には「中」、低い画質には「高」を使用します。デフォルトでは、中程度の圧縮が適用されます。

USBデバイスポリシー設定

USBデバイスセクションには、USBデバイスのファイルリダイレクトを管理するためのポリシー設定が含まれています。

クライアントUSBデバイス最適化ルール

クライアントUSBデバイス最適化ルールは、最適化を無効にするか、最適化モードを変更するためにデバイスに適用できます。

ユーザーがUSB入力デバイスを接続すると、ホストは**USBポリシー**設定がそのデバイスを許可するかどうかを確認します。デバイスが許可されている場合、ホストはデバイスの**クライアントUSBデバイス最適化ルール**を確認します。ルールが指定されていない場合、デバイスは最適化されません。キャプチャモード (04) は、署名デバイスに推奨されるモードです。高遅延によってパフォーマンスが低下する他のデバイスの場合、管理者はインタラクティブモード (02) を有効にできます。この記事の表で利用可能なモードの説明を参照してください。

知っておくとよいこと

- Wacomの署名パッドおよびタブレットを使用する場合は、スクリーンセーバーを無効にすることをお勧めします。スクリーンセーバーを無効にする手順は、このセクションの最後にあります。
- Wacom STU署名パッドおよびタブレットシリーズ製品の最適化のサポートは、Citrix Virtual Apps and Desktops™ポリシーのインストール時に事前設定されています。
- 署名デバイスはCitrix Virtual Apps and Desktops全体で機能し、署名デバイスとして使用するためにドライバーを必要としません。Wacomには、デバイスをさらにカスタマイズするためにインストールできる追加のソフトウェアがあります。`<http://www.wacom.com/>`を参照してください。
- 描画タブレット。特定の描画入力デバイスは、PCI/ACPIバス上でHIDデバイスとして表示される場合があり、サポートされていません。これらのデバイスは、Citrix Virtual Desktopsセッション内でリダイレクトされるように、クライアント上のUSBホストコントローラーに接続してください。

ポリシールールは、空白で区切られたtag=value式の形式を取ります。以下のタグがサポートされています。

タグ名	説明
モード	最適化モードは、class=**03**の入力デバイスでサポートされています。サポートされているモードは次のとおりです。最適化なし - 値**01**。インタラクティブモード - 値**02**。ペンタブレットや3D Proマウスなどのデバイスに推奨されます。キャプチャモード - 値**04**。署名パッドなどのデバイスに推奨されます。
VID	デバイス記述子からのベンダーID。4桁の16進数として。
PID	デバイス記述子からのプロダクトID。4桁の16進数として。
REV	デバイス記述子からのリビジョンID。4桁の16進数として。
クラス	デバイス記述子またはインターフェイス記述子のいずれかからのクラス。

タグ名	説明
サブクラス	デバイス記述子またはインターフェイス記述子のいずれかからのサブクラス。
プロトコル	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル。

例

Mode=00000004 VID=067B PID=1230 class=03 #キャプチャモードで動作する入力デバイス

Mode=00000002 VID=067B PID=1230 class=03 #対話モードで動作中の入力デバイス (既定)

Mode=00000001 VID=067B PID=1230 class=03 #最適化なしで動作する入力デバイス

Mode=00000100 VID=067B PID=1230 # デバイスセットアップの最適化が無効（デフォルト）

Mode=00000200 VID=067B PID=1230 #デバイスセットアップの最適化が有効

Wacom署名パッドデバイスのスクリーンセーバーを無効にする

Wacom署名パッドおよびタブレットを使用する場合、Citrix®は次のようにスクリーンセーバーを無効にすることを推奨します。

1. デバイスをリダイレクトした後、**Wacom-STU-Driver**をインストールします。
2. 署名パッドのコントロールパネルにアクセスするには、**Wacom-STU-Display MSI**をインストールします。
3. **コントロールパネル > Wacom STU Display > STU430**または**STU530**に移動し、お使いのモデルのタブを選択します。
4. **変更**を選択し、UACセキュリティウィンドウが表示されたら**はい**を選択します。
5. **スライドショーを無効にする**を選択し、**適用**をクリックします。

1つの署名パッドモデルに設定が適用されると、すべてのモデルに適用されます。

クライアントUSBデバイスのリダイレクト

この設定は、USBデバイスのユーザーデバイスとの間のリダイレクトを許可または禁止します。

デフォルトでは、USBデバイスはリダイレクトされません。

クライアントUSBデバイスリダイレクト規則

この設定は、USBデバイスのリダイレクトルールを指定します。

デフォルトでは、ルールは指定されていません。

ユーザーがUSBデバイスを接続すると、ホストデバイスは一致が見つかるまで各ポリシー規則と照合します。任意のデバイスに対する最初の一致が最終的なものと見なされます。最初の一致が許可ルールである場合、デバイスは仮想デスクトップにリモート接続されます。最初の一致が拒否ルールである場合、デバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合は、デフォルトのルールが使用されます。

ポリシー規則は、{Allow:|Deny:} の形式で、その後に空白で区切られた tag=value 式のセットが続きます。以下のタグがサポートされています。

タグ名	説明
VID	デバイス記述子からのベンダーID
PID	デバイス記述子からの製品ID
REL	デバイス記述子からのリリースID
クラス	デバイス記述子またはインターフェイス記述子のいずれかからのクラス
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス
プロトコル	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル

ポリシー規則を作成する際は、次の点に注意してください。

- ルールでは大文字と小文字は区別されません。
- ルールには、# で始まるオプションのコメントを末尾に含めることができます。
- 空行および純粋なコメント行は無視されます。
- タグは一致演算子 = を使用する必要があります（例：VID=067B_）。
- 各ルールは新しい行から開始するか、セミコロンで区切られたリストの一部である必要があります。
- USB Implementers Forum, Inc. のWebサイトで利用可能なUSBクラスコードを参照してください。

管理者定義の USB ポリシールールの例:

- 許可: VID=067B PID=0007 # 別の企業、別のフラッシュドライブ
- 拒否: Class=08 subclass=05 # マスストレージ
- すべての USB デバイスを拒否するルールを作成するには、他のタグなしで「DENY:」を使用します。

クライアント USB プラグアンドプレイデバイスのリダイレクト

この設定により、カメラやPOS (Point-of-Sale) デバイスなどのプラグアンドプレイデバイスをクライアントセッションで使用することが許可または禁止されます。

デフォルトでは、プラグアンドプレイデバイスのリダイレクトは許可されています。「許可」に設定すると、特定のユーザーまたはグループのすべてのプラグアンドプレイデバイスがリダイレクトされます。「禁止」に設定すると、デバイスはリダイレクトされません。

USB デバイスの自動リダイレクトを構成する

USB サポートが有効になっている場合、USB デバイスは自動的にリダイレクトされます。また、USB ユーザー設定は USB デバイスを自動的に接続するように設定されています。

> **注:**
>
> Receiver for Windows 4.2では、デスクトップアプライアンスモードで動作している場合も、USBデバイスは自動的にリダイレクトされます。また、接続バーは表示されません。以前のバージョンのCitrix Receiver for Windowsでは、USBデバイスは以下のモードで動作している場合も自動的にリダイレクトされます。
>
> - デスクトップアプライアンスモード
> - 仮想マシン (VM) ホスト型アプリケーション
>
> すべてのUSBデバイスをリダイレクトすることが常に最適とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントまたはDDCポリシーのいずれかでDeviceRulesを使用します。詳細については、管理者ガイドを参照してください。

> **注意:**

> レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤用によって生じた問題が解決されることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

USBデバイスの自動リダイレクトに関するユーザー設定

ポリシー:

1. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrix Components > Citrix Receiver™ > クライアントデバイスのリモート処理 > Generic USB Remoting**に移動します。
2. **新しいUSBデバイス**を開き、**有効**を選択して**OK**をクリックします。
3. 「**既存のUSBデバイス**」を開き、「**有効**」を選択して、「**OK**」をクリックします。

シトリックス レシーバー:

1. **Citrix Receiverの環境設定 > 接続**に移動します。
2. 以下のオプションが選択されていることを確認してください:
   - セッション開始時に、デバイスを自動的に接続する
   - セッション実行中に新しいデバイスが接続された場合、そのデバイスを自動的に接続する。
3. 「**OK**」をクリックします。

すべてのレジストリキーとポリシーの変更は、Windowsクライアントデバイスに適用されます。

通常のUSBプリンターのリダイレクト

通常のUSBプリンターに最適なソリューションは、専用のユニバーサルプリンタードライバーと仮想チャネルを使用して印刷を実行することです。デフォルトでは、通常のUSBプリンターは自動的にリダイレクトされません。

通常のプリンターはヒューリスティックを使用して検出されます。また、例えばスキャン機能を持つ高度なプリンターは、完全に機能させるにはUSBサポートを使用してリダイレクトする必要がある場合があります。

通常のプリンターが自動的にリダイレクトされるかどうかを構成するには、このレジストリを使用します:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

既定値は0（自動的にリダイレクトしない）です。値を0より大きい数値に変更すると、USBサポートが有効になり、通常のUSBプリンターがリダイレクトされます。

Active Directoryポリシーをこのレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

通常のオーディオデバイスのリダイレクト

通常のプリンターと同様に、通常のオーディオデバイスからオーディオデータを送信するには、ICA®の専用オーディオ仮想チャネルを使用することで最高のユーザーエクスペリエンスが実現されます。ただし、一部の特殊なデバイスはUSBサポートを使用してリダイレクトする必要がある場合があります。どのデバイスが通常のオーディオデバイスであるかを判断するためにヒューリスティックが使用されます。

通常のオーディオデバイスが自動的にリダイレクトされるかどうかを構成するには、クライアントエンドポイントでこのレジストリを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

既定値は0（自動的にリダイレクトしない）に設定されています。値を0以外に変更すると、USBサポートを使用して通常のUSBオーディオデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectVideo

種類: DWORD

データ: 00000000

プレーンストレージデバイス（マスストレージデバイス）のリダイレクト

プレーンストレージデバイスの場合、最適化も実行するクライアントドライブマッピングなどの専用仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。ファイルの単純な読み書きに加えて、CD/DVDの書き込みや暗号化されたファイルシステムデバイスへのアクセスなどの特定の特殊なタスクを実行するには、汎用USBサポートを使用してデバイスをリダイレクトする必要がある場合があります。

どのデバイスがプレーンストレージデバイスであるかを判断するためにヒューリスティックが使用されます。プレーンストレージデバイスを自動的にリダイレクトするかどうかを構成するには、このレジストリキーを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

デフォルトは0（自動的にリダイレクトしない）に設定されています。値を0以外に変更すると、汎用USBサポートを使用してプレーンUSBストレージデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値を以下のレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

> **注記:**
>
> 汎用USBサポートを使用している場合、通常のストレージデバイスへの読み取り専用アクセスは構成できませんが、CDMを使用している場合は構成可能です。

ハードウェア暗号化されたUSBフラッシュドライブのリダイレクト

ハードウェア暗号化されたUSBフラッシュドライブは通常、暗号化されたストレージパーティションと、暗号化されたパーティションのロックを解除するためのユーティリティが含まれる2番目のユーティリティパーティションで構成されています。USBフラッシュドライブデバイスの場合、最適化も実行する専用のクライアントドライブマッピング/動的サムドライブマッピングHDX仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。

汎用USBリダイレクトは、以下の場合に必要です。

- 非Windowsクライアント (例: Linuxクライアント)
- 顧客がクライアント上のローカル機能へのユーザーアクセスを制限している (ロックダウンしている) クライアント

汎用USBリダイレクトは、ハードウェア暗号化されていない任意のUSBストレージデバイスを、シングルセッションOSおよびマルチセッションOS VDAセッションの両方にリダイレクトできます。

Citrix Virtual Apps and Desktops 7 1808より前は、ハードウェア暗号化されたUSBフラッシュドライブは、シングルセッションOSまたはマルチセッションOS VDAセッションに有用な方法でリダイレクトできませんでした。Citrix Virtual Apps and Desktops 7 1808で導入された新機能強化により、ハードウェア暗号化されたUSBフラッシュドライブの汎用USBリダイレクトが、シングルセッションOSおよびマルチセッションOS VDAセッションでサポートされるようになりました。デバイスがリダイレクトされた後、そのドライブはローカルクライアントに表示されません。そのため、ドライブのロック解除が必要な場合は、セッション内で実行してください。この機能にはWindows Update KB4074590が必要です。

通常の静止画像デバイス (スキャナーおよびデジタルカメラ)

通常の静止画像デバイスの場合、最適化も実行する専用の仮想チャネル (TWAIN仮想チャネルなど) を使用することで、最高のユーザーエクスペリエンスを実現できます。これらのデバイスは業界標準に準拠している必要があります。デバイスが非準拠であるか、元の意図に従って使用されていないと見なされる場合、汎用USBリダイレクトがデバイスを使用する唯一の方法となる可能性があります。どのデバイスが通常の静止画像デバイスであるかを判断するためにヒューリスティックが使用されます。

このレジストリキーを使用して、通常の静止画像デバイスが自動的にリダイレクトされるかどうかを構成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています（自動的にリダイレクトされません）。値を0以外に変更すると、汎用USBのプレーンなUSB静止画デバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をこのレジストリキーに展開することもでき、両方が存在する場合は非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デバイス固有の設定

Citrix最適化可能デバイスを選択するために使用されるヒューリスティックは、必ずしもお客様の希望と一致するとは限りません。Citrix最適化可能デバイスの例としては、プリンター、オーディオ、ビデオ、ストレージ、静止画デバイスなどがあります。上記にリストされていないデバイスの自動リダイレクトを制御したい場合があります。デバイス固有の基準で自動リダイレクトを制御できます。

例として、DemoTech 2,000バーコードリーダーはUSBサポートを使用してリダイレクトする必要はありません。ベンダー識別子12AB、製品識別子5678を持っています。これらの16進数はデバイスマネージャーで確認できます。

これが自動的にリダイレクトされるのを防ぐには、このデバイス固有のレジストリキーを作成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

0の値は、デバイスが自動的にリダイレクトされるのを防ぎます。0以外の値は、デバイスが自動リダイレクトの対象となる必要があることを示します（ユーザー設定による）。ベンダーと製品の識別子の間には、単一のスペース文字があります。

このレジストリキーにActive Directoryポリシーを使用してこの値を展開することもできます。両方が存在する場合、非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

デバイス固有のAutoRedirect設定は、上記で説明したより一般的なAutoRedirectXXX値よりも優先されます。Citrix最適化デバイスのデフォルトのヒューリスティックは、デバイスを汎用として誤って解釈する可能性があります。したがって、デバイス固有のAutoRedirect値を1に設定して、自動的にリダイレクトします。

既存のUSBデバイスの自動接続を許可する

この設定は、セッション開始時にエンドポイントに接続されている既存のUSBデバイスをリモートセッションに自動接続することを許可または禁止します。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトします。

デフォルトでは、**利用可能なUSBデバイスをリダイレクトする前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**設定** > **デバイス**セクションで選択されたオプションが上書きされる場合があります。

> **注:**
>
> 現在、**既存のUSBデバイスの自動接続を許可する**ポリシーは、Windows版Citrix Workspace™アプリにのみ適用されます。

新しく接続されたUSBデバイスの自動接続を許可する

この設定は、セッション中にエンドポイントに挿入されたUSBデバイスのリモートセッションへの自動接続を許可または防止します。

この設定をポリシーに追加する際は、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトする。

デフォルトでは、**利用可能なUSBデバイスをリダイレクトする前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**設定** > **デバイス**セクションで選択されたオプションが上書きされる場合があります。

> **注：**
>
> 現在、**新しく接続されたUSBデバイスの自動接続を許可する**ポリシーは、Windows版Citrix Workspaceアプリにのみ適用されます。

新しく接続されたUSBデバイスの自動接続を許可する

この設定は、USBデバイスをフィルタリング、分割、およびリモートセッションに自動接続するための規則を指定します。

この設定が選択されている場合、ホストは*クライアントUSBデバイスリダイレクト規則*設定を、この設定で構成されたデバイス規則で上書きします。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトします。

デフォルトでは、**利用可能なUSBデバイスをリダイレクトする前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**基本設定** > **デバイス**セクションで選択されたオプションが上書きされる場合があります。

> **注:**

> 現在、**新しく接続されたUSBデバイスの自動接続を許可する**ポリシーは、Citrix Workspaceアプリ for Windowsにのみ適用されます。

クライアントUSBデバイスリダイレクト規則 (バージョン2)

この設定は、USBデバイスをリモートセッションにフィルタリング、分割、および自動接続するためのルールを指定します。

この設定が選択されている場合、ホストは*クライアントUSBデバイスリダイレクトルール*設定を、この設定で構成されたデバイスルールで上書きします。

詳しくは、「複合USBデバイスリダイレクトの構成」を参照してください。

仮想チャネル許可リストポリシー設定

仮想チャネル許可リストポリシー設定は、ICA®セッションで開くことが許可されている仮想チャネルを指定する許可リストの使用を有効にします。

無効にすると、すべての仮想チャネルが許可されます。

有効にすると、Citrix®仮想チャネルのみが許可されます。

カスタムまたはサードパーティの仮想チャネルを使用するには、仮想チャネルをリストに追加します。仮想チャネルをリストに追加するには：

1. 仮想チャネル名を入力し、その後にコンマを付けます。
2. 仮想チャネルにアクセスするプロセスへのパスを入力します。

複数の実行可能パスをリストでき、パスはコンマで区切られます。

例:

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

Citrix Virtual Apps and Desktops 7 2109以降、仮想チャネル許可リストはデフォルトで有効になっています。許可リストに仮想チャネルを追加する方法の詳細については、「許可リストへの仮想チャネルの追加」を参照してください。

Skype for Business向けHDX RealTime Optimization Packを使用している場合は、仮想チャネルを許可リストに追加します。詳細については、「HDX RealTime Optimization Packのドキュメント」を参照してください。

重要:

設定を有効にするには、VDAマシンを再起動する必要があります。

仮想チャネルの詳細については、ICA virtual channels を参照してください。

仮想チャネル許可リストのログ記録

このポリシー設定を使用して、仮想チャネル許可リストのログ記録レベルを構成できます。

次のオプションが利用可能です。

オプション	説明
無効	すべてのログイベントを無効にします。
警告のみをログに記録	許可リストに含まれていない、開こうとするカスタム仮想チャネルに対してのみイベントがログに記録されます。
すべてのイベントをログに記録	すべてのイベントがログに記録されます

仮想チャネル許可リストのログスロットリング

このポリシー設定を使用して、アクティブなセッションのイベントのログ記録頻度を構成できます。

各仮想チャネルのすべてのイベントは、最初に発生したときにログに記録されます。セッションがアクティブな間、スロットリング期間中は繰り返し発生するイベントは抑制されます。セッションが切断された場合、スロットリング期間はリセットされます。

視覚表示ポリシー設定

視覚表示セクションには、仮想デスクトップからユーザーデバイスに送信される画像の品質を制御するためのポリシー設定が含まれています。

シンプルなグラフィックの優先色深度

このポリシー設定は、VDAバージョン7.6 FP3以降で利用可能です。8ビットオプションは、VDAバージョン7.12以降で利用可能です。

この設定により、シンプルなグラフィックがネットワーク経由で送信される際の色深度を下げることができます。ピクセルあたり8ビットまたは16ビットに下げることで、低帯域幅接続での応答

性が向上する可能性があります。ただし、この操作は画質のわずかな劣化を招く可能性があります。(/ja-jp/citrix-virtual-apps-desktops/2311/policies/reference/ica-policy-settings/graphics-policy-settings.html)ポリシー設定が**画面全体**に設定されている場合、8ビットの色深度はサポートされません。

デフォルトの優先色深度はピクセルあたり24ビットです。

8ビット設定がVDAバージョン7.11以前に適用された場合、VDAは24ビット（デフォルト）の色深度にフォールバックします。

ターゲットフレームレート

この設定は、仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を指定します。

デフォルトでは、最大は1秒あたり30フレームです。

1秒あたりのフレーム数を高く設定する（例：30）と、ユーザーエクスペリエンスは向上しますが、より多くの帯域幅が必要になります。1秒あたりのフレーム数を減らす（例：10）と、ユーザーエクスペリエンスを犠牲にしてサーバーのスケーラビリティが最大化されます。CPUが遅いユーザーデバイスの場合、ユーザーエクスペリエンスを向上させるために低い値を指定してください。

1秒あたりの最大サポートフレームレートは60です。

視覚品質

この設定は、ユーザーデバイスに表示される画像の希望する視覚品質を指定します。

デフォルトでは、この設定は「中」です。

画像の品質を指定するには、次のいずれかのオプションを選択します。

- **低** - 帯域幅が制限されたネットワークで、インタラクティブ性のために視覚的な品質を犠牲にできる場合に推奨されます。
- **中** - ほとんどのユースケースで最高のパフォーマンスと帯域幅効率を提供します。
- **高** - 視覚的にロスレスな画質が必要な場合に推奨されます。
- **ロスレスにビルド** - ネットワークアクティビティが高い期間はロッシー画像をユーザーデバイスに送信し、ネットワークアクティビティが低下した後はロスレス画像を送信します。この設定により、帯域幅が制限されたネットワーク接続でのパフォーマンスが向上します。

- **常にロスレス** - 画像データの保持が不可欠な場合は、「**常にロスレス**」を選択して、ロッシーデータがユーザーデバイスに送信されないようにします。たとえば、画質の低下が許されないX線画像を表示する場合などです。

動画ポリシー設定

「**動画**」セクションには、動的画像の圧縮を削除または変更できる設定が含まれています。

最小画像品質

注: Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、アダプティブディスプレイの許容される最小画像品質を指定します。圧縮が少ないほど、表示される画像の品質は高くなります。圧縮レベルは、超高、非常に高、高、標準、低から選択します。

デフォルトでは、これは標準に設定されています。

動画圧縮

この設定は、アダプティブディスプレイが有効になっているかどうかを指定します。アダプティブディスプレイは、利用可能な帯域幅に基づいて、スライドショー内のビデオやトランジションスライドの画像品質を自動的に調整します。アダプティブディスプレイが有効になっている場合、ユーザーは品質の低下なしにスムーズなプレゼンテーションを見ることができます。

デフォルトでは、アダプティブディスプレイは有効になっています。

VDAバージョン7.0から7.6の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDAバージョン7.6 FP1以降の場合、この設定はレガシーグラフィックモードが有効になっている場合、またはレガシーグラフィックモードが無効でビデオコーデックがグラフィックの圧縮に使用されていない場合に適用されます。

レガシーグラフィックモードが有効になっている場合、ポリシー変更を有効にするにはセッションを再起動する必要があります。アダプティブディスプレイはプログレッシブディスプレイと相互排他的です。アダプティブディスプレイを有効にするとプログレッシブディスプレイは無効になり、その逆も同様です。ただし、プログレッシブディスプレイとアダプティブディスプレイの両方を同時に無効にすることができます。プログレッシブディスプレイはレガシー機能であるため、XenAppまたはXenDesktopでは推奨されません。プログレッシブしきい値レベルを設定すると、アダプティブディスプレイは無効になります。

プログレッシブ圧縮レベル

注: Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定により、画像の初期表示が詳細度は低いものの高速になります。

デフォルトでは、プログレッシブ圧縮は適用されません。

より詳細な画像は、通常の非可逆圧縮設定で定義され、利用可能になったときに表示されます。写真などの帯域幅を多く消費するグラフィックの表示を改善するには、非常に高い圧縮または超高圧縮を使用してください。

プログレッシブ圧縮が効果的であるためには、その圧縮レベルが非可逆圧縮レベル設定よりも高くなければなりません。

注：プログレッシブ圧縮に関連する圧縮レベルの増加は、クライアント接続を介した動的画像の対話性も向上させます。回転する3Dモデルのような動的画像の品質は、画像が動きを停止するまで一時的に低下し、その時点で通常の非可逆圧縮設定が適用されます。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値
- プログレッシブヘビーウェイト圧縮

プログレッシブ圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、プログレッシブ圧縮が適用される接続の最大帯域幅をキロビット/秒で表します。これは、この帯域幅以下のクライアント接続にのみ適用されます。

デフォルトでは、しきい値は2147483647キロビット/秒です。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値
- プログレッシブヘビーウェイト圧縮

目標最小フレームレート

この設定は、低帯域幅の条件下で、動的画像に対してシステムが維持しようとする1秒あたりの最小フレームレートを指定します。

デフォルトでは、これは10fpsに設定されています。

VDAバージョン7.0から7.6の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDAバージョン7.6 FP1以降の場合、この設定はレガシーグラフィックモードが無効または有効になっている場合に適用されます。

注:

目標最小フレームレートポリシーは非推奨となり、10 fpsに設定されています。これは、グラフィックステータスインジケーターの品質スライダーを使用してエンドユーザーが変更できます。

静止画像ポリシー設定

静止画像セクションには、静止画像の圧縮を削除または変更できる設定が含まれています。

追加の色圧縮

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に、追加の色圧縮を使用するかどうかを有効または無効にします。これにより、表示される画像の品質を低下させることで応答性が向上します。

デフォルトでは、追加の色圧縮は無効になっています。

有効にすると、追加の色圧縮は、クライアント接続の帯域幅が「追加の色圧縮しきい値」を下回る場合にのみ適用されます。クライアント接続の帯域幅がしきい値を超える場合、または「無効」が選択されている場合、追加の色圧縮は適用されません。

追加の色圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は「レガシーグラフィックモード」ポリシー設定が有効になっている場合にのみ適用されます。

この設定は、追加の色圧縮が適用される接続の最大帯域幅をキロビット/秒で表します。クライアント接続の帯域幅が設定値を下回ると、追加の色圧縮が有効になっている場合は適用されます。

デフォルトでは、しきい値は8192キロビット/秒です。

ヘビーウェイト圧縮

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は「レガシーグラフィックモード」ポリシー設定が有効になっている場合にのみ適用されます。

この設定は、より高度でCPU負荷の高いグラフィックアルゴリズムを使用することで、画質を損なうことなくプログレッシブ圧縮を超えて帯域幅を削減するかどうかを有効または無効にします。

デフォルトでは、ヘビーウェイト圧縮は無効になっています。

有効にすると、ヘビーウェイト圧縮はすべての非可逆圧縮設定に適用されます。Citrix Workspace™アプリではサポートされていますが、他のプラグインには影響しません。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮レベル
- プログレッシブ圧縮しきい値

非可逆圧縮レベル

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に使用される非可逆圧縮の度合いを制御します。このような場合、圧縮なしで画像を表示すると遅くなることがあります。

デフォルトでは、中程度の圧縮が選択されています。

帯域幅を多く消費する画像の応答性を向上させるには、高圧縮を使用します。画質の劣化が許容されないX線画像を表示する場合など、画像データの保持が不可欠な場合は、非可逆圧縮を使用しない方がよいでしょう。

関連ポリシー設定：非可逆圧縮しきい値

非可逆圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、非可逆圧縮が適用される接続の最大帯域幅を1秒あたりのキロビット数で表します。

デフォルトでは、しきい値は1秒あたり2147483647キロビットです。

ポリシーに非可逆圧縮レベル設定を追加し、しきい値を指定しないことで、LAN経由での写真などの高詳細ビットマップの表示速度を向上させることができます。

関連ポリシー設定：非可逆圧縮レベル

WebSocketsポリシー設定

WebSocketsセクションには、HTML5向けCitrix Workspace™アプリを使用して仮想デスクトップおよびホスト型アプリケーションにアクセスするためのポリシー設定が含まれています。WebSockets機能は、ブラウザベースのアプリケーションとサーバー間の双方向通信を行うことで、セキュリティを向上させ、オーバーヘッドを削減します。この機能は、複数のHTTP接続を開くことなくこれを実現します。

WebSockets接続

この設定では、WebSockets接続を許可または禁止します。

デフォルトでは、WebSocket接続は禁止されています。

WebSocketsポート番号

この設定では、受信WebSocket接続のポートを識別します。

デフォルトでは、値は8008です。

WebSockets信頼済みオリジンサーバーリスト

この設定は、通常はURLとして表現されるCitrix Workspace app for Webである、信頼済みオリジンサーバーのコンマ区切りリストを提供します。サーバーは、これらのアドレスのいずれかから発信されたWebSockets接続のみを受け入れます。

デフォルトでは、ワイルドカード * が使用され、すべてのCitrix Workspace app for Web URLが信頼されます。

リストにアドレスを入力する場合は、次の構文を使用します。

\<protocol>://\<ホストの完全修飾ドメイン名>:

プロトコルはHTTPまたはHTTPSである必要があります。ポートが指定されていない場合、HTTPにはポート80が、HTTPSにはポート443が使用されます。

ワイルドカード `*` は、IPアドレスの一部として使用する場合を除き（`10.105.*.*`）、URL内で使用できます。

レジストリを介して管理されるHDX™機能

> **注:**

> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターの使用は、お客様ご自身の責任において行ってください。編集する前に、必ずレジストリをバックアップしてください。

> レジストリエディターを開くには、サーバーで `regedit.exe` を実行します。その後、設定を追加または編集するためにレジストリキーに移動します。

デバイス

Bloombergキーボード

Citrix Virtual Apps and Desktops™ は、Bloombergモデル4およびモデル3のスターボードキーボードをサポートしています。既定では、拡張Bloombergキーボードのサポートは無効になっています。

Bloombergキーボードのサポートを有効にするには、接続を開始する前にクライアントマシンで以下のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB
- 値の名前: EnableBloombergHID
- 値の型: DWORD
- 値のデータ: 0 = 無効, 1 = 有効

詳細については、Bloombergキーボードを参照してください。

マップされたクライアントドライブ

セキュリティ上の予防措置として、ユーザーがCitrix Virtual Apps and Desktopsにログオンすると、既定では、サーバーはユーザーの実行権限なしでクライアントドライブをマップします。ユーザーがマップされたクライアントドライブにある実行可能ファイルを実行できるようにするには、サーバー上のレジストリを編集してこの既定値を上書きします。

アクセスを許可するには、次のレジストリ値を編集します (**CDMSettings**が存在しない場合は作成します)。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings
- 値の名前: ExecuteFromMappedDrive
- 値の型: DWORD
- 値のデータ: 1 = 許可, 0 = マップされたドライブでのアクセス許可を拒否

この変更は、レジストリを編集した後に接続されたセッションに適用されます。

Citrix Virtual Apps and Desktops 7 2006 は、このレジストリの場所を含む最初のバージョンです。以前のバージョンの Citrix Virtual Apps and Desktops では、異なるレジストリの場所が使用されていました。

詳しくは、「クライアントドライブマッピング」を参照してください。

Microsoft Surface Pro および Surface Book のペン

Citrix Virtual Apps and Desktops は、Windows Ink ベースのアプリケーションで標準のペン機能をサポートしています。デフォルトでは、この機能は有効になっています。

この機能を無効または有効にするには、次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi
- 値の名前: DisablePen
- 値の型: DWORD
- 値のデータ: 1 = 無効, 0 = 有効

詳細については、Microsoft Surface Pro および Surface Book ペン を参照してください。

Windows Image Acquisitionアプリケーションの許可リスト

この設定により、VDA 上のどのアプリケーションが Windows Image Acquisition スキャナーリダイレクトにアクセスできるかを制御できます。

デフォルトでは、どのアプリケーションも Windows Image Acquisition にアクセスできません。

VDA 上のアプリケーションに対して Windows Image Acquisition を調整するには、次のレジストリ設定を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix
- 値の名前: WIAAllowedProcesses

  WIAAllowedProcesses を選択して右クリックします。**新規 > 複数行文字列値** を選択し、新しい値を **AllowProcesses** に名前変更します。
- 値のデータ: Windows イメージ取得にアクセスできる各アプリケーションの完全なパスとプロセス名を入力します。各アプリケーションは新しい行に入力してください。

この設定への変更は、VDA でセッションを次回起動したときに有効になります。

一般

Rendezvousバージョンの構成

使用する Rendezvous のバージョンを構成するには、以下を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
- 値の型: DWORD
- 値の名前: GctRegistration

- 値のデータ:
  - 1 - V2を有効にする
  - 0 - V1を有効にする

VDAへの自動ログオンを構成する

この設定により、Windows 10シングルセッションOSおよびマルチセッションOS VDAで、Microsoftポリシー設定の**常にパスワードを要求する**を有効または無効にできます。

常にパスワードを要求するが有効になっている場合、ユーザーはリモートセッションを開始するときにVDAで資格情報を入力する必要があります。この設定が無効になっている場合、ユーザーはVDAで資格情報を提供することなく、自動的にリモートセッションに接続します。

デフォルトでは、Microsoftポリシー設定は無効になっています。**常にパスワードを要求する**設定を有効または無効にするには、VDAで次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica
- 値の名前: AutoLogon
- 値の型: DWORD
- 値のデータ:
  - 1 - Microsoftポリシー設定を無効にし、ユーザーがリモートセッションに自動的にサインインできるようにします。
  - 0 – Microsoftポリシー設定を有効にし、ユーザーがリモートセッションを起動するときに資格情報の入力を求めます。

タイムアウト警告を無効にする

デフォルトでは、非アクティブまたはアイドル状態のセッションを持つユーザーは、セッションが自動的に切断される2分前に警告メッセージを受け取ります。

この設定は、以下のアイドルセッションタイムアウト制限に達したユーザーに対する警告メッセージを無効にし、削除します。

- ウィンドウズ サーバー 2004
- Windows 10マルチセッション2004以降のマルチセッションOS

警告を削除するには、VDAで以下のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP

- 値の名前: fEnableTimeoutWarning
- 値の型: DWORD
- 値のデータ: 1 = 警告メッセージを無効にする、0 = 警告メッセージを有効にする

警告メッセージを表示するには、レジストリ値を削除するか、0に設定します。

EDT MTU検出

MTU検出により、EDTはセッション確立時に最大転送単位（MTU）を自動的に決定できます。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットの断片化を防ぎます。

この設定はデフォルトで有効になっています。EDT MTU検出を無効にするには、以下のレジストリ値を構成し、VDAを再起動します。

- キー: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
- 値の名前: MtuDiscovery
- 値の型: DWORD
- 値のデータ: 0

この設定はマシン全体に適用され、サポートされているクライアントから接続するすべてのセッションに影響します。

ロス耐性モードを有効にする

Citrix Workspace™ app for Windows、マルチユーザーVDA、およびデスクトップVDAの双方向オーディオサービスでは、ロス耐性モードを使用してアダプティブオーディオにアクセスできます。この設定はデフォルトで無効になっています。ロス耐性モードを有効にするには、使用しているマシンに応じて、次のレジストリ値を構成し、それぞれのマシンを再起動します。

Citrix Workspace app for Windowsクライアントの場合、,

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio
- 値の名前: EdtUnreliableAllowed
- 値の型: REG_SZ
- 値のデータ: 1

TS VDAの場合、,

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio
- 値の名前: EdtUnreliableAllowed
- 値の型: DWORD
- 値のデータ: 1

WS VDAの場合、,

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio
- 値の名前: EdtUnreliableAllowed
- 値の型: DWORD
- 値のデータ: 1

一般的なコンテンツリダイレクト

ホストからクライアントへのリダイレクトの URL タイプを追加する

デフォルトでは、HTTP、HTTPS、RTSP、RTSPU、PNM、MMS の URL タイプのリダイレクトをサポートしています。Windows クライアントで以下のレジストリキーと値を作成することで、URL タイプをリストに追加できます。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 値の名前: ExtraURLProtocols
- 値の型: REG_SZ
- 値のデータ: 必要な URL タイプをセミコロンで区切って指定します。URL のオーソリティ部分より前のすべてを含めます。例: `ftp://;mailto:;customtype1://;custometype2://`

URL タイプは Windows クライアントにのみ追加できます。このレジストリ設定がないクライアントは、Citrix セッションへのリダイレクトを拒否します。クライアントには、指定された URL タイプを処理するようにインストールおよび構成されたアプリケーションが必要です。

詳細については、「ホストからクライアントへのリダイレクト」を参照してください。

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセス可能になる方法を変更します。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成する場合を考えてみましょう。この場合、ユーザーによって指定されたローカルボリュームの一部がリダイレクトされます。

サーバーでクライアントフォルダーリダイレクトを有効にするには、次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection
- 値の名前: CFROnlyModeAvailable
- 値の型: DWORD
- 値のデータ: 1

詳細については、クライアントフォルダーリダイレクトを参照してください。

特定のWebサイトセットに対するホストからクライアントへのリダイレクト

特定のWebサイトセットに対してホストからクライアントへのリダイレクトを有効にするには、サーバーVDAで次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: ValidSites
- 値の型: REG_MULTI_SZ
- 値のデータ: 完全修飾ドメイン名 (FQDN) の任意の組み合わせを指定します。複数の FQDN を別々の行に入力します。プロトコル (`http://` または `https://`) を含めず、FQDN のみを含めます。FQDN には、最も左の位置にのみワイルドカード文字としてアスタリスク (`*`) を含めることができます。このワイルドカードは、RFC 6125 の規則と一致する単一レベルのドメインに一致します。例:

`www.example.com`

`*.example.com`

詳細については、ホストからクライアントへのリダイレクトを参照してください。

ログオフ時および切断時のローカルアプリケーションの動作

既定では、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、仮想デスクトップで利用可能な場合、ローカルアプリケーションは再統合されます。ログオフ時および切断時のローカルアプリケーションの動作を構成するには、ホストされているデスクトップで次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies
- 値の名前: セッション状態
- 値の型: DWORD

- 値のデータ:
  - 1 - ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、仮想デスクトップで利用可能な場合、ローカルアプリケーションは再統合されます。
  - 3 - ユーザーが仮想デスクトップからログオフまたは切断すると、ローカルアプリケーションは閉じます。

詳しくは、「Local App Access and URL redirection」を参照してください。

ホストからクライアントへのリダイレクトの既定のリストからURLタイプを削除する

既定のリダイレクトリストからURLタイプを削除するには、サーバーVDAで次のレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: DisableServerFTA
- 値の型: DWORD
- 値のデータ: 1
- 値の名前: NoRedirectClasses
- 値の型: REG_MULTI_SZ
- 値のデータ: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または`mms`の任意の組み合わせを指定します。複数の値を別々の行に入力します。例:

`http`

`https`

`rtsp`

詳細については、ホストからクライアントへのリダイレクトを参照してください。

サーバーVDAのデフォルトのブラウザー構成

サーバーVDA上のデフォルトのブラウザー構成を上書きするために、ホストからクライアントへのリダイレクトを有効にできます。Web URLがリダイレクトされない場合、Citrixランチャーは`command_backup`レジストリキーで構成されたブラウザーにURLを渡します。このキーはデフォルトでInternet Explorerを指していますが、別のブラウザーへのパスを含むように変更できます。

- Internet Explorer (デフォルト)
  - キー: HKEY_CLASSES_ROOT\http\shell\open\command_backup

    - 値の名前: Default
    - 値の型: REG_SZ
    - 値のデータ: `"c:\program files\internet explorer\iexplore.exe" "%1"`
    - Key: HKEY_CLASSES_ROOT\https\shell\open\command_backup`
    - 値の名前: Default
    - 値の型: REG_SZ
    - 値のデータ: `"c:\program files\internet explorer\iexplore.exe" "%1"`

- グーグル クローム
    - Key: HKEY_CLASSES_ROOT\http\shell\open\command_backup
    - 値の名前: Default
    - 値の型: REG_SZ
    - 値のデータ: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`
    - Key: HKEY_CLASSES_ROOT\https\shell\open\command_backup
    - 値の名前: Default
    - 値の型: REG_SZ
    - 値のデータ: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`

- マイクロソフト エッジ
    - Key: HKEY_CLASSES_ROOT\http\shell\open\command_backup
    - 値の名前: Default
    - 値の型: REG_SZ
    - 値のデータ: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`
    - キー: HKEY_CLASSES_ROOT\https\shell\open\command_backup
    - 値の名前: Default
    - 値の型: REG_SZ
    - 値のデータ: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`

公開アプリケーションのLocal App Access

Local App Accessは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。公開アプリケーションへのアクセスを提供するには、サーバーで次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio
- 値の名前: ClientHostedAppsEnabled
- 値の型: DWORD
- 値のデータ: 1 = 有効, 0 = 無効

詳細については、Local App AccessとURLリダイレクトを参照してください。

グラフィック

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDAアクセラレーションのPOC機能を使用するには、次のレジストリ設定を有効にします。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper
- 値の名前: CUDA
- 値の型: DWORD
- 値のデータ: 00000001

OpenCLアクセラレーションのPOC機能を使用するには、次のレジストリ設定を有効にします。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper
- 値の名前: OpenCL
- 値の型: DWORD
- 値のデータ: 00000001

詳細については、WindowsマルチセッションOSのGPUアクセラレーションを参照してください。

プログレッシブモード

プログレッシブモードはデフォルトで無効になっています。プログレッシブモードの状態は、以下のレジストリ値で変更できます。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 値の型: REG_DWORD
- 値の名前: ProgressiveDisplay
- 値のデータ:
  - 0 = 常にオフ (プログレッシブモードを無効にします。この値がデフォルトです。)
  - 1 = 自動 (ネットワークの状態に基づいて切り替えます。)
  - 2 = 常にオン

詳しくは、「プログレッシブモード」を参照してください。

> **注:**
>
> プログレッシブモードは非推奨になりました。Thinwire は、プログレッシブモードのほぼすべての利点を提供しながら、画像配信を最適化し、キャッシュ効率を維持する代替オプションです。

Windows Presentation Foundation (WPF) レンダリング

HDX 3D Pro を使用すると、Windows Multi-session OS セッションで実行されているグラフィックを多用するアプリケーションを、サーバーのグラフィック処理ユニット (GPU) でレンダリングできます。Windows Presentation Foundation (WPF) レンダリングをサーバーの GPU に移行することで、グラフィックレンダリングがサーバーの CPU を遅くすることはありません。

サーバーの GPU を使用して WPF アプリケーションのレンダリングを有効にするには、Windows Multi-session OS を実行しているサーバーのレジストリに次の設定を作成します。

1. VDA でレジストリエディターを開き、次のキーに移動します。

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`

2. 次のレジストリ値を作成または編集します。
   - AdapterHandle = 0x00000001
   - DevicePath = 0x00000001

- フラグ = 0x00000412
- WPF = 0x00000001

3. WPF アプリの実行可能ファイル名でサブキーを作成します。たとえば、アプリの名前が「mywpfapp.exe」の場合、次のキーを作成します。

```
HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe
```

4. 設定を有効にするには、サーバーを再起動します。

詳細については、WindowsマルチセッションOSのGPUアクセラレーションおよびWindowsマルチセッションOSでWPFアプリを最大限に活用するのブログを参照してください。

マルチメディア

マルチメディア会議中のエコーを回避する

Citrix Virtual Apps and Desktops には、エコーを最小限に抑えるエコーキャンセルオプションが用意されています。この機能はデフォルトで有効になっています。エコーキャンセルを無効にするには、次のいずれかのレジストリ設定を変更できます。

- キー:
  - 32ビット: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio
  - 64ビット: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio
- 値の名前: EchoCancellation
- 値の型: String/REG_SZ
- 値のデータ: False

詳細については、オーディオ機能を参照してください。

オーディオ制限

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にしてRDSセッションを開始した後、オーディオファイルが再生されない場合があります。回避策として、RDSマシンに以下のレジストリキーを追加し、マシンを再起動してください。

- キー: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig
- 値の名前: EnableSvchostMitigationPolicy
- 値の型: DWORD

- 値のデータ: 0

詳細については、オーディオ機能を参照してください。

ブラウザコンテンツリダイレクトとDPI

ユーザーのマシンでDPI（スケーリング）が100%を超えて設定されている状態でブラウザコンテンツリダイレクトを使用すると、リダイレクトされたブラウザコンテンツ画面が正しく表示されません。この問題を回避するには、ユーザーのマシンに次のレジストリ値を作成して、Chromeのブラウザコンテンツリダイレクト GPUアクセラレーションを無効にします。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- 値の名前: GPU
- 値の型: DWORD
- 値のデータ: 0

詳細については、ブラウザコンテンツリダイレクトとDPIを参照してください。

高解像度Webカメラの解像度

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度（640 x 480 ピクセル）にフォールバックします。クライアントのレジストリキーを使用して、デフォルトの解像度を構成できます。以下のレジストリキーを設定する前に、カメラが指定された解像度をサポートしていることを確認してください。

- キー: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- 幅
  - 値の名前: DefaultWidth
  - 値の型: DWORD
  - 値のデータ: 目的の幅 (10進数) (例: 1280)
- 高さ
  - 値の名前: DefaultHeight
  - 値の型: DWORD
  - 値のデータ: 目的の高さ (10進数) (例: 720)

Microsoft Teamsのフォールバックモード

最適化されたVDIモードでMicrosoft Teamsの読み込みに失敗した場合（Teams/バージョン情報/バージョンで「Citrix HDX Not Connected」と表示される場合）、VDAはWebカメラリダイレクト

やクライアントオーディオおよびマイクのリダイレクトなどのレガシーHDXテクノロジーにフォールバックします。Microsoft Teamsの最適化をサポートしないWorkspaceアプリのバージョン/プラットフォームOSを使用している場合、フォールバックレジストリキーは適用されません。

フォールバックメカニズムを制御するには、VDAで次のいずれかのレジストリ値を設定します。

- キー (いずれか1つのみ必要):
  - **コンピューター設定:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams
  - **ユーザー設定:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams
- 値の名前: DisableFallback
- 値の型: DWORD
- 値のデータ: 1 = フォールバックモードを無効にする, 2 = 音声のみを有効にする

値が存在しないか0に設定されている場合、フォールバックモードが有効になります。この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。詳しくは、「Microsoft Teamsの最適化」を参照してください。

Citrix App Layering™を使用したMicrosoft Teamsの最適化

Citrix App Layeringを使用してVDAとMicrosoft Teamsのインストールを異なるレイヤーで管理している場合は、コマンドラインから`ALLUSER=1`フラグを指定してMicrosoft Teamsをインストールする前に、Windows上に**PortICA**という名前の空のレジストリキーを作成します。既定の値の名前、型、データはそのままにします。

- レジストリエディターの32ビットバージョン用のキー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA
- レジストリエディターの64ビットバージョン用のキー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA

詳しくは、「Microsoft Teamsの最適化」を参照してください。

ブラウザーコンテンツリダイレクト用の統合Windows認証によるシングルサインオン

この設定は、VDA と同じドメイン内で統合 Windows 認証 (IWA) を使用して構成された Web サーバーへのシングルサインオンを提供します。シングルサインオンを有効にするには、以下のレジストリ値を 1 に設定します。

- キー:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream

または

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\HdxMediastream

- 値の名前: WebBrowserRedirectionIwaSupport
- 値の型: DWORD
- 値のデータ: 1

詳細については、「統合 Windows 認証によるシングルサインオン」を参照してください。

ユーザーエージェントリクエストヘッダー

ユーザーエージェントヘッダーは、ブラウザコンテンツリダイレクトから送信される HTTP 要求を識別するのに役立ちます。この設定は、プロキシとファイアウォールルールを構成する際に役立ちます。たとえば、サーバーがブラウザコンテンツリダイレクトから送信される要求をブロックする場合、ユーザーエージェントヘッダーを含むルールを作成して、特定の要件をバイパスできます。ユーザーエージェント要求ヘッダーは、Windows デバイスのみがサポートしています。

デフォルトでは、ユーザーエージェント要求ヘッダーストリングは無効になっています。クライアントでレンダリングされるコンテンツのユーザーエージェントヘッダーを有効にするには、レジストリエディターを使用します。

各 Citrix Workspace app for Windows クライアントで、以下のいずれかのレジストリ設定を行います。

- キー:
  - 32ビット: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStream
  - 64ビット: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- 値の名前: EnableCefUserAgentString
- 値の型: DWORD
- 値のデータ: 1

レジストリ値を追加すると、ユーザーエージェントヘッダーにはCitrixBCR/2102.1というテキストが含まれます。ここで、2102.1はWindows版Citrix Workspaceアプリのバージョンです。

Webカメラのソフトウェア圧縮

Webカメラがハードウェアエンコードをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコードを使用します。ハードウェアエンコードは、ソフトウェアエンコードよ

りも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントで次の値を追加します。

- キー: HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime
- 値の名前: DeepCompress_ForceSWEncode
- 値の型: DWORD
- 値のデータ: 1

詳しくは、「HDX webcam video compression」を参照してください。

Webカメラのビデオ圧縮

HDX Webカメラのビデオ圧縮は、仮想セッションで実行されているビデオ会議アプリケーションにH.264ビデオを直接送信します。VDAリソースを最適化するために、HDX Webカメラ圧縮はWebカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAで次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime
- 値の名前: OfferH264ToApp
- 値の型: DWORD
- 値のデータ: 0

詳細については、HDX webcam video compressionを参照してください。

Webカメラビデオ圧縮フレームレート

優先ビデオフレームレートを調整するには、クライアントで次のレジストリ値を編集します。

- キー: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- 値の名前: FramesPerSecond
- 値の型: DWORD
- 値のデータ: 15

ウェブカメラが指定されたフレームレートをサポートしていない場合、アプリケーションはデフォルトで15 FPSを使用します。

詳細については、HDXウェブカメラビデオ圧縮を参照してください。

ロード管理ポリシー設定

「**負荷管理**」セクションには、Windowsマルチセッション OSマシンを提供するサーバー間の負荷管理を有効化および構成するためのポリシー設定が含まれています。

ロード評価インデックスの計算については、CTX202150を参照してください。

同時ログオン許容数

この設定は、サーバーが受け入れることができる同時ログオンの最大数を指定します。

デフォルトでは、この値は2に設定されています。

この設定が有効な場合、負荷分散は、指定された数を超えるログオンが同時にServer VDAでアクティブにならないように試みます。ただし、この制限は厳密には適用されません。制限を適用し（指定された数を超える同時ログオンを失敗させる）、次のレジストリキーを作成します。

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit 種類: DWORD 値: 1

CPU使用率

この設定は、サーバーがフルロードを報告するCPU使用率のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%です。

デフォルトでは、この設定は無効になっており、CPU使用率は負荷計算から除外されます。

CPU使用率から除外されるプロセスの優先度

> **注：**

> Workspace Environment Managementがマシンを管理するシナリオでは、この設定をCPU Priority設定と併用すると、意図しない結果が生じる可能性があります。CPU Priority設定を使用することを選択した場合は、この設定を無効にすることをお勧めします。

> この設定は、プロセスのCPU使用率がCPU使用率負荷インデックスから除外される優先度レベルを指定します。

デフォルトでは、この値は**標準以下**または**低**に設定されています。

ディスク使用量

この設定は、サーバーが75%のフルロードを報告するディスクキューの長さを指定します。有効にすると、ディスクキューのデフォルト値は8です。

デフォルトでは、この設定は無効になっており、ディスク使用率は負荷計算から除外されます。

セッションの最大数

この設定は、サーバーがホストできるセッションの最大数を指定します。有効にすると、サーバーがホストできるセッションの最大数のデフォルト設定は250になります。

デフォルトでは、この設定は有効になっています。

メモリ使用量

この設定は、サーバーがフルロードを報告するメモリ使用量のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%です。

デフォルトでは、この設定は無効になっており、メモリ使用量は負荷計算から除外されます。

メモリ使用量のベースロード

この設定は、ベースオペレーティングシステムのメモリ使用量の近似値を指定します。また、サーバーがゼロロードと見なされるメモリ使用量（MB単位）を定義します。

デフォルトでは、この値は768 MBに設定されています。

プロファイル管理ポリシー設定

高度なポリシー設定

ロックされたファイルへのアクセス時の再試行回数

ロックされたファイルへのアクセス時の再試行回数を設定します。

このポリシーが無効になっている場合、デフォルト値である5回の再試行が使用されます。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、デフォルト値が使用されます。

ログオフ時にインターネットCookieファイルを処理する

一部の展開では、`Index.dat` が参照しない余分なインターネットCookieが残されます。継続的なブラウジングの後、ファイルシステムに残された余分なCookieは、プロファイルの肥大化につながる可能性があります。このポリシーを使用すると、Profile Managementを有効にして

Index.datの処理を強制し、余分なCookieを削除できます。このポリシーはログオフ時間を増加させるため、この問題が発生した後にのみ有効にしてください。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、Index.datの処理は行われません。

自動構成を無効にする

Profile Managementは、Citrix Virtual Desktops™環境（たとえば、パーソナルvDiskの有無）を検査し、それに応じてグループポリシーを構成します。未構成状態のProfile Managementポリシーのみが調整されるため、行ったカスタマイズはすべて保持されます。

このポリシーを使用すると、展開を高速化し、最適化を簡素化できます。このポリシーを構成する必要はありません。ただし、次のいずれかの操作を行うときに、自動構成を無効にできます。

- 以前のバージョンからの設定を保持するためにアップグレードする
- トラブルシューティング

自動構成は、実行時に環境に応じてデフォルトのポリシー設定を自動的に構成する動的構成チェッカーと見なすことができます。これにより、設定を手動で構成する必要がなくなります。実行時環境には以下が含まれます。

- ウィンドウズ OS
- Windows OSのバージョン
- シトリックス バーチャル デスクトップの存在
- 個人用 vDisk の存在

環境が変更された場合、自動構成によって以下のポリシーが変更される可能性があります。

- アクティブライトバック
- 常にキャッシュ
- ログオフ時にローカルにキャッシュされたプロファイルを削除
- キャッシュされたプロファイルを削除するまでの遅延
- プロファイルストリーミング

異なる OS でのポリシーのデフォルトの状態については、次の表を参照してください。

	マルチセッションOS	シングルセッションOS
アクティブライトバック	有効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は、有効。
常にキャッシュ	無効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は、有効。
ログオフ時にローカルにキャッシュされたプロファイルを削除	有効	次のいずれかの状況が発生した場合、*無効*になります: Personal vDiskが使用されている、Citrix Virtual Desktopsが割り当てられている、またはCitrix Virtual Desktopsがインストールされていない場合。それ以外の場合は有効です。
キャッシュされたプロファイルを削除するまでの遅延	0秒	ユーザーの変更が永続的でない場合は60秒。それ以外の場合は0秒。
プロファイルストリーミング	有効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は、有効。

ただし、自動構成が無効になっている場合、上記のすべてのポリシーはデフォルトで**無効**になります。

重要:

Personal vDiskは非推奨です。詳細については、PVD、AppDisk、およびサポートされていないホストの削除を参照してください。

Profile Management 1909以降、Windows 10 (バージョン1607以降) およびWindows Server 2016以降のスタートメニューで改善されたエクスペリエンスを得ることができます。この改善は、以下のポリシーの自動構成によって実現されます。

- `Appdata\Local\Microsoft\Windows\Caches`と`Appdata\Local\Packages`を**ミラーリングするフォルダー**に追加します。
- `Appdata\Local\Microsoft\Windows\UsrClass.Dat*`を**同期するファイル**に追加します。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、自動構成がオンになります。この場合、環境が変更されると、Profile Managementの設定が変更される可能性があります。

問題が発生した場合にユーザーをログオフする

問題が発生した場合に Profile Management がユーザーをログオフさせるかどうかを指定できます。

このポリシーが無効になっているか、構成されていない場合、問題が発生すると Profile Management はユーザーに一時プロファイルを提供します。たとえば、ユーザー ストアが利用できない場合などです。

有効になっている場合、エラーメッセージが表示され、ユーザーはログオフされます。この設定により、問題のトラブルシューティングが簡素化されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、一時プロファイルが提供されます。

カスタマー エクスペリエンス向上プログラム

デフォルトでは、Citrix®製品の品質とパフォーマンスを向上させるために、匿名統計と使用状況データを収集するカスタマーエクスペリエンス向上プログラムが有効になっています。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

Outlook の検索インデックス ローミングを有効にする

ユーザープロファイルとともに Outlook 検索データを自動的にローミングすることで、ユーザーベースの Outlook 検索エクスペリエンスを許可します。この機能には、Outlook の検索インデックスを保存するために、ユーザー ストアに追加のスペースが必要です。

このポリシーを有効にするには、ログオフしてから再度ログオンしてください。

Outlook 検索インデックス データベース – バックアップと復元

「Outlookの検索インデックスローミングを有効にする」ポリシーが有効になっている場合に、ログオン中にProfile Managementが何を行うかを指定できます。

このポリシーが有効になっている場合、Profile Managementは、ログオン時に検索インデックスデータベースが正常にマウントされるたびに、そのデータベースをバックアップします。Profile Managementは、このバックアップを検索インデックスデータベースの正常なコピーとして扱います。データベースの破損により検索インデックスデータベースのマウントが失敗した場合、Profile Managementは検索インデックスデータベースを最後に確認された正常なコピーに戻します。

> 注:
>
> 新しいバックアップが正常に保存されると、Profile Managementは以前に保存されたバックアップを削除します。バックアップは利用可能なVHDXストレージを消費します。

OUTLOOK検索データローミングの同時セッションサポートを有効にする

Profile Managementにより、同じユーザーの同時セッションでネイティブのOutlook検索エクスペリエンスが提供されます。このポリシーは、Outlookの検索インデックスローミングポリシーと併用してください。

このポリシーが有効な場合、各同時セッションは個別のOutlook OSTファイルを使用します。

デフォルトでは、Outlook OSTファイルを保存するために使用できるVHDXディスクは2つだけです（ディスクごとに1ファイル）。ユーザーがさらにセッションを開始した場合、そのOutlook OSTファイルはローカルユーザープロファイルに保存されます。Outlook OSTファイルを保存するためのVHDXディスクの最大数を指定できます。

ONEDRIVEコンテナを有効にする

OneDriveフォルダーをユーザーとともにローミングできるようにします。

OneDriveコンテナは、VHDXベースのフォルダーローミングソリューションです。Profile Managementは、ファイル共有上にユーザーごとにVHDXファイルを作成し、ユーザーのOneDriveフォルダーをVHDXファイルに保存します。VHDXファイルは、ユーザーがログオンするときにアタッチされ、ログオフするときにデタッチされます。

UWPアプリのローミング

UWP (Universal Windows Platform) アプリをユーザーとともにローミングできるようにします。これにより、ユーザーは異なるデバイスから同じUWPアプリにアクセスできます。

このポリシーが有効な場合、Profile ManagementはUWPアプリを個別のVHDXディスクに保存することで、ユーザーとともにローミングできるようにします。これらのディスクは、ユーザーのログオン中にアタッチされ、ログオフ中にデタッチされます。

構成の優先順位:

この設定がここで構成されていない場合、.iniファイルの値が使用されます。 この設定がここでも.iniファイルでも構成されていない場合、この機能は無効になります。

ログオン時のユーザーグループポリシーの非同期処理を有効にする

Windowsは、ユーザーグループポリシーに同期と非同期の2つの処理モードを提供します。Windowsは、次のユーザーログオンの処理モードを決定するためにレジストリ値を使用します。レジストリ値が存在しない場合、同期モードが適用されます。レジストリ値はマシンレベルの設定であり、ユーザーと共にローミングしません。したがって、ユーザーが次のいずれかの場合は、非同期モードが期待どおりに適用されません。

- 異なるマシンにログオンする。
- ログオフ時にローカルにキャッシュされたプロファイルを削除するポリシーが有効になっている同じマシンにログオンする。

このポリシーを有効にすると、レジストリ値はユーザーとともにローミングされます。その結果、ユーザーがログオンするたびに処理モードが適用されます。

VHDディスクの圧縮をトリガーする空き領域の比率

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮をトリガーする空き領域の比率を指定できます。ユーザーログオフ時に空き領域の比率が指定された値を超えると、ディスクの圧縮がトリガーされます。

空き領域の比率 = (現在のVHDファイルサイズ – 必要な最小VHDファイルサイズ*) ÷ 現在のVHDファイルサイズ

* Microsoft Windowsオペレーティングシステムの `MSFT_Partition` クラスのGetSupportedSizeメソッドを使用して取得されます。

VHDディスクの圧縮をトリガーするログオフ回数

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮をトリガーするユーザーログオフ回数を指定できます。

前回の圧縮以降のログオフ回数が指定された値に達すると、ディスクの圧縮が再度トリガーされます。

VHDディスク圧縮のデフラグを無効にする

(/ja-jp/citrix-virtual-apps-desktops/2311/policies/reference/profile-management/profile-container-policy-settings.html#enable-vhd-disk-compaction)が有効な場合に適用されます。VHDディスク圧縮のファイルデフラグを無効にするかどうかを指定できます。

VHDディスク圧縮が有効な場合、VHDディスクファイルはまずWindows組み込みの`defrag`ツールを使用して自動的にデフラグされ、その後圧縮されます。VHDディスクのデフラグはより良い圧縮結果をもたらしますが、無効にするとシステムリソースを節約できます。

プロファイルコンテナのマルチセッションライトバックを有効にする

マルチセッションシナリオでプロファイルコンテナへの書き戻しを有効にします。有効にすると、すべてのセッションでの変更がプロファイルコンテナに書き戻されます。そうでない場合、プロファイルコンテナでは最初のセッションのみが読み書きモードであるため、最初のセッションでの変更のみが保存されます。Citrix Profile Managementプロファイルコンテナは、Citrix Profile Management 2103以降でサポートされています。FSLogix Profile Containerは、Citrix Profile Management 2003以降でサポートされています。

FSLogix Profile Containerでこのポリシーを使用するには、以下の前提条件が満たされていることを確認してください。

- FSLogix Profile Container機能がインストールされ、有効になっていること。
- FSLogixで、プロファイルタイプが**読み書きプロファイルを試行し、読み取り専用にフォールバックする**に設定されていること。

ユーザーストアをレプリケートする

リモートユーザープロファイルストアを、ログオンおよびログオフごとに複数のパスにレプリケートできます。これにより、Profile Managementはユーザーログオンのプロファイル冗長性を提供できます。

このポリシーを有効にすると、システムI/Oが増加し、ログオフが長くなる可能性があります。

> **注:**
>
> - この機能は、ユーザーストアとフルプロファイルコンテナの両方で利用できます。
> - レプリケートされたプロファイルコンテナは、ユーザーログオンのプロファイル冗長性を提供しますが、セッション内フェールオーバーには対応していません。

ユーザーストアへの資格情報ベースのアクセスを有効にする

デフォルトでは、Citrix Profile Management は現在のユーザーを偽装してユーザー ストアにアクセスします。Profile Management がユーザー ストアへのアクセス時に現在のユーザーを偽装しない

ようにする場合は、この機能を有効にします。現在のユーザーがアクセス権を持たないストレージ リポジトリ (Azure Files など) にユーザー ストアを配置できます。

Profile Management がユーザー ストアにアクセスできるようにするには、プロファイル ストレージ サーバーの資格情報を Workspace Environment Management™ (WEM) または Windows 資格情報マネージャーに保存します。Profile Management が実行される各マシンで同じ資格情報を構成する必要をなくすために、Workspace Environment Management を使用することをお勧めします。Windows 資格情報マネージャーを使用する場合は、ローカル システム アカウントを使用して資格情報を安全に保存してください。

> **注:**
>
> このポリシーは、ファイルベースと VHDX ベースの両方のユーザー ストアで利用できます。Profile Management のバージョン 2212 より前では、このポリシーは VHDX ベースのユーザー ストアでのみ利用できます。

> ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。ここでも .ini ファイルでもこの設定が構成されていない場合、デフォルトで無効になります。

VHDX ファイルのストレージ パスをカスタマイズする

Profile Management は、次の VHDX ベースのポリシーを提供します: プロファイル コンテナ、Outlook の検索インデックス ローミング、およびフォルダ ミラーリングの高速化。デフォルトでは、VHDX ファイルはユーザー ストアに保存されます。このポリシーを使用すると、それらを保存するための別のパスを指定できます。

VHD コンテナのデフォルト容量

VHD コンテナのデフォルトのストレージ容量 (GB 単位) を指定できます。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。
2. ここでも .ini ファイルでもこのポリシーが構成されていない場合、デフォルトは 50 (GB) です。

セッションで VHDX ディスクを自動的に再アタッチする

このポリシーを有効にすると、Profile Management は VHDX ベースのポリシーの高い安定性を確保します。デフォルトでは、このポリシーは有効になっています。

このポリシーが有効になっている場合、Profile Management は VHDX ベースのポリシーで使用されている VHDX ディスクを監視します。いずれかのディスクがデタッチされた場合、Profile Management はそのディスクを自動的に再アタッチします。

プロファイルコンテナの自動拡張しきい値

プロファイルコンテナが自動拡張をトリガーするストレージ容量の使用率を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここまたは.iniファイルで構成されていない場合、デフォルトはストレージ容量の90%です。

プロファイルコンテナの自動拡張増分

自動拡張がトリガーされたときに、プロファイルコンテナが自動的に拡張するストレージ容量（GB単位）を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここまたは.iniファイルで構成されていない場合、デフォルトは10 GBです。

プロファイルコンテナの自動拡張制限

自動拡張がトリガーされたときに、プロファイルコンテナが自動的に拡張できる最大ストレージ容量（GB単位）を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここまたは.iniファイルで構成されていない場合、デフォルトは80 GBです。

ユーザーレベルのポリシー設定を有効にする

このポリシーを有効にすると、マシンレベルのポリシー設定がユーザーレベルで機能し、ユーザーレベルの設定がマシンレベルの設定を上書きします。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、無効になります。

ユーザーグループの優先順位を設定する

ユーザーグループの優先順位を指定できます。この順序は、ユーザーが異なるポリシー設定を持つ複数のグループに属している場合に、どのグループが優先されるかを決定します。

ユーザーが競合するポリシー設定を持つ複数のグループに属している場合、以下を考慮してください:

- ユーザーがこのポリシーで定義されている1つ以上のグループに属している場合、最も優先順位の高いグループが優先されます。
- ユーザーがこのポリシーで定義されているどのグループにも属していない場合、アルファベット順で最も早くリストされているSIDを持つグループが優先されます。

ユーザーストアの選択方法

複数のユーザーストアが利用可能な場合に、ユーザーストアの選択方法を指定できます。オプションは次のとおりです:

- **構成順序。** Profile Managementは、最初に構成されたストアを選択します。
- **アクセスパフォーマンス。** Profile Managementは、最高のアクセスパフォーマンスを持つストアを選択します。

構成の優先順位:

1. ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。
2. ここでも .ini ファイルでもこの設定が構成されていない場合、**構成順序**が使用されます。

基本的なポリシー設定

このセクションには、Profile Management の基本的な構成に関するポリシー設定が含まれています。

Profile Management を有効にする

デフォルトでは、展開を容易にするため、Profile Management はログオンまたはログオフを処理しません。Profile Management は、他のすべてのセットアップタスクを実行し、Citrix® ユーザープロファイルが環境でどのように動作するかをテストした後にのみ有効にしてください。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、Profile Management は Windows ユーザープロファイルを一切処理しません。

処理されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）の両方を使用できます。ドメイングループは、DOMAIN NAME\GROUP NAME の形式で指定する必要があります。

このポリシーがここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、Profile Management はすべてのユーザーを処理します。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、すべてのユーザーグループのメンバーが処理されます。

除外されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）を使用して、特定のユーザープロファイルが処理されないようにすることができます。ドメイングループは、DOMAIN NAME\ GROUP NAME の形式で指定します。

この設定がここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーを除外します。この設定が無効になっている場合、Profile Management はどのユーザーも除外しません。この設定がここで構成されていない場合、.ini ファイルの値が使用されます。この設定がここでも .ini ファイルでも構成されていない場合、どのグループのメンバーも除外されません。

ローカル管理者によるログオンの処理

BUILTIN\Administrators グループのメンバーのログオンが処理されるかどうかを指定します。Citrix Virtual Apps 環境などのマルチセッションオペレーティングシステムでは、このポリシーが無効になっているか、構成されていないと見なされます。この場合、Profile Management は、ドメインユーザーによるログオンは処理されるが、ローカル管理者によるログオンは処理されないと想定します。シングルセッションオペレーティングシステム（Citrix Virtual Desktops 環境など）では、ローカル管理者のログオンが処理されます。このポリシーにより、ローカル管理者権限を持つドメインユーザー（通常、割り当てられた仮想デスクトップを持つ Citrix Virtual Desktops ユーザー）は、次のことが可能になります。

- 処理をバイパスする
- ログオンする
- Profile Managementで問題が発生しているデスクトップのトラブルシューティング

注: ドメインユーザーのログオンは、通常、製品ライセンスへの準拠を確実にするために、グループメンバーシップによって課される制限の対象となる場合があります。 このポリシーが無効になっている場合、Profile Managementはローカル管理者によるログオンを処理しません。このポ

リシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、管理者は処理されません。

ユーザーストアへのパス

ユーザー設定（レジストリの変更と同期ファイル）が保存されるディレクトリ（ユーザーストア）へのパスを設定します。

パスは次のいずれかです。

- 相対パス。ホームディレクトリ（通常、Active Directoryのユーザーの#homeDirectory#属性として構成されます）に対する相対パスである必要があります。
- UNCパス。通常、サーバー共有またはDFS名前空間を指定します。
- 無効または未構成。この場合、#homeDirectory#\Windowsの値が想定されます。

このポリシーでは、次の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数（例: %ProfVer%）。システム環境変数は通常、追加の設定が必要です。
- ハッシュで囲まれたActive Directoryユーザーオブジェクトの属性（例: #sAMAccountName#）。
- Profile Management変数。詳細については、Profile Management変数の製品ドキュメントを参照してください。

`%username%`と`%userdomain%`を除き、ユーザー環境変数は使用できません。場所やユーザーなどを完全に定義するために、カスタム属性を作成することもできます。属性では大文字と小文字が区別されます。

例:

- \\server\share#sAMAccountName# は、ユーザー設定をUNCパス \\server\share\JohnSmith に保存します（現在のユーザーに対して#sAMAccountName# がJohnSmithに解決される場合）
- \\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS! は \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64 に展開される場合があります。

重要: どの属性または変数を使用する場合でも、このポリシーが NTUSER.DAT を含むフォルダーの1つ上のフォルダーに展開されることを確認してください。たとえば、このファイルが \\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile に含まれている場合、ユーザー ストア

へのパスは \\server\profiles$\JohnSmith.Finance\Win8x64 (\UPM_Profile サブフォルダーではない) に設定します。

ユーザー ストアへのパスを指定する際の変数の使用に関する詳細については、以下のトピックを参照してください。

- 複数のファイルサーバーでCitrixユーザープロファイルを共有する
- OU内およびOU間でプロファイルを管理する
- Profile Managementによる高可用性と災害復旧

ユーザー ストアへのパスが無効になっている場合、ユーザー設定はホーム ディレクトリのWindowsサブディレクトリに保存されます。

このポリシーが無効になっている場合、ユーザー設定はホーム ディレクトリのWindowsサブディレクトリに保存されます。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、ホーム ドライブのWindowsディレクトリが使用されます。

ユーザー ストアの移行

ユーザー設定（レジストリの変更と同期されたファイル）が以前に保存されていたフォルダーへのパス（以前使用していたユーザー ストアのパス）を指定します。

この設定が構成されている場合、以前のユーザー ストアに保存されているユーザー設定は、「ユーザー ストアへのパス」ポリシーで指定された現在のユーザー ストアに移行されます。

パスは絶対UNCパスまたはホーム ディレクトリに対する相対パスのいずれかです。

どちらの場合も、次の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数
- ハッシュ記号で囲まれたActive Directoryユーザー オブジェクトの属性

例:

- フォルダ `Windows\%ProfileVer%` は、ユーザー ストアの `Windows\W2K3` という名前のサブフォルダーにユーザー設定を保存します (%ProfileVer% が W2K3 に解決されるシステム環境変数である場合)。
- `\\server\share#SAMAccountName#` は、ユーザー設定を UNC パス `\\server\share\<JohnSmith>` に保存します (`#SAMAccountName#` が現在のユーザーに対して JohnSmith に解決される場合)。

パスでは、`%username%` と `%userdomain%` を除くユーザー環境変数を使用できます。

この設定が無効になっている場合、ユーザー設定は現在のユーザーストアに保存されます。

この設定がここで構成されていない場合、.ini ファイルの対応する設定が使用されます。

この設定がここで、または .ini ファイルで構成されていない場合、ユーザー設定は現在のユーザーストアに保存されます。

アクティブなライトバック

変更されたファイルとフォルダー (レジストリ エントリを除く) は、セッションの途中で、ログオフ前にユーザー ストアに同期できます。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここで、または .ini ファイルで構成されていない場合、有効になります。

オフラインプロファイルのサポート

このポリシーにより、プロファイルは可能な限り早い機会にユーザー ストアと同期できます。これは、ローミングするラップトップまたはモバイルデバイスのユーザーを対象としています。ネットワーク接続が切断されても、プロファイルは再起動または休止状態の後でもラップトップまたはデバイス上でそのまま維持されます。モバイルユーザーが作業すると、プロファイルはローカルで更新されます。また、ネットワーク接続が再確立されると、最終的にユーザー ストアと同期されます。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここで、または .ini ファイルで構成されていない場合、オフラインプロファイルは無効になります。

アクティブなライトバック レジストリ

このポリシーは「アクティブなライトバック」と併用してください。変更されたレジストリ エントリは、セッションの途中でユーザー ストアに同期できます。

ここでこの設定を構成しない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定を構成しない場合、アクティブライトバックレジストリは無効になります。

セッションロックおよび切断時のアクティブライトバック

このポリシーと**アクティブライトバック**ポリシーの両方が有効になっている場合、プロファイルファイルとフォルダーは、セッションがロックまたは切断されたときにのみ書き戻されます。

このポリシーと**アクティブライトバック**および**アクティブライトバックレジストリ**ポリシーの両方が有効になっている場合、レジストリエントリは、セッションがロックまたは切断されたときにのみ書き戻されます。

オフラインプロファイルのサポート

オフラインプロファイル機能を有効にします。この機能は、ネットワークから頻繁に切断されるコンピューター向けです。たとえば、サーバーやデスクトップではなく、ラップトップやモバイルデバイスなどです。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、オフラインプロファイルのサポートは無効になります。

クロスプラットフォームポリシー設定

このセクションには、**Profile Management cross-platform** 設定機能の構成に関連するポリシー設定が含まれています。

クロスプラットフォーム設定を有効にする

既定では、展開を容易にするために、クロスプラットフォーム設定は無効になっています。このポリシーを有効にすることで処理をオンにできますが、この機能の十分な計画とテストを行った後に限ります。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ユーザーグループ

1つ以上のWindowsユーザーグループを入力します。たとえば、このポリシーを使用して、テストユーザーグループのプロファイルのみを処理できます。このポリシーが構成されている場合、Profile Managementのクロスプラットフォーム設定機能は、これらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、この機能は「処理されたグループ」ポリシーで指定されたすべてのユーザーを処理します。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、すべてのユーザーグループが処理されます。

クロスプラットフォーム定義へのパス

ダウンロードパッケージからコピーした定義ファイルのネットワーク上の場所を識別します。このパスはUNCパスである必要があります。ユーザーはこの場所への読み取りアクセス権を持ち、管理者は書き込みアクセス権を持っている必要があります。この場所は、Server Message Block (SMB) またはCommon Internet File System (CIFS) ファイル共有である必要があります。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ストアへのパス

クロスプラットフォーム設定ストアへのパスを設定します。これは、ユーザーのクロスプラットフォーム設定が保存されるフォルダーです。ユーザーはこの領域への書き込みアクセス権を持っている必要があります。パスは絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。

この領域は、複数のプラットフォームで共有されるプロファイルデータが配置されるユーザー ストアの共通領域です。ユーザーは、この領域への書き込みアクセス権を持っている必要があります。パスは、絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。**ユーザー ストアへのパス** と同じ変数を使用できます。

このポリシーが無効になっている場合、パスWindows\PM_CPが使用されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、既定値が使用されます。

クロスプラットフォーム設定を作成するためのソース

このポリシーがそのプラットフォームのOUで有効になっている場合、プラットフォームをベースプラットフォームとして指定します。このポリシーは、ベースプラットフォームのプロファイルからクロスプラットフォーム設定ストアにデータを移行します。

各プラットフォーム独自のプロファイルセットは、別々のOUに保存されます。クロスプラットフォーム設定ストアをシードするために、どのプラットフォームのプロファイルデータを使用するかを決定する必要があります。これはベースプラットフォームと呼ばれます。クロスプラットフォーム設定ストアにデータのない定義ファイルが含まれている場合、または単一プラットフォームプロファイルのキャッシュデータがストア内の定義データよりも新しい場合を考慮してください。この場合、このポリシーを無効にしない限り、プロファイル管理は単一プラットフォームプロファイルからストアにデータを移行します。

> **重要:**

> このポリシーが複数のOU、または複数のユーザーオブジェクトやマシンオブジェクトで有効になっている場合、最初にユーザーがログオンするプラットフォームがベースプロファイルになります。 デフォルトでは、このポリシーは有効になっています。

ファイルシステム ポリシー設定

このセクションには、次の項目を設定するポリシーが含まれています:

- ユーザープロファイル内のどのファイルが、プロファイルがインストールされているシステムとユーザー ストア間で同期されるか
- ユーザープロファイル内のどのディレクトリが、プロファイルがインストールされているシステムとユーザー ストア間で同期されるか

除外ポリシー設定

このセクションでは、ユーザープロファイル内のどのファイルとディレクトリを同期プロセスから除外するかを設定するためのポリシー設定について説明します。

除外リスト - ファイル

同期中に無視されるファイルのリスト。ファイル名はユーザープロファイル (%USERPROFILE%) に対する相対パスである必要があります。ワイルドカードはファイル名とフォルダー名でサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。

例:

- `Desktop\Desktop.ini` は、`Desktop` フォルダー内のファイル `Desktop.ini` を無視します。
- `%USERPROFILE%*.tmp` は、プロファイル全体で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `AppData\Roaming\MyApp*.tmp` は、プロファイルの一部で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `Downloads*\a.txt` は、`Downloads` フォルダーの直下のサブフォルダーにある `a.txt` を無視します。

このポリシーが無効になっている場合、ファイルは除外されません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ファイルは除外されません。

デフォルトの除外リストを有効にする - ディレクトリ

同期中に無視されるディレクトリのデフォルトリスト。このポリシーを使用して、GPO 除外ディレクトリを手動で入力することなく指定できます。

このポリシーを無効にすると、Profile Management はデフォルトでどのディレクトリも除外しません。

このポリシーをここで構成しない場合、Profile Management は .ini ファイルの値を使用します。このポリシーをここでも .ini ファイルでも構成しない場合、Profile Management はデフォルトでどのディレクトリも除外しません。

除外リスト - ディレクトリ

同期中に無視されるフォルダーのリスト。フォルダー名はユーザープロファイル (%USERPROFILE%) に対する相対パスとして指定する必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

例:

- `Desktop` は、ユーザープロファイル内の `Desktop` フォルダーを無視します。

このポリシーが無効になっている場合、フォルダーは除外されません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、フォルダーは除外されません。

ログオン除外チェック

この設定は、ユーザーストア内のプロファイルに除外されたファイルまたはフォルダーが含まれている場合に、Profile Management が実行する動作を構成します。可能なポリシー設定とそれに対応するアクションを次の表に示します。

ポリシー設定	アクション
設定が無効になっているか、「ログオン時に除外されたファイルまたはフォルダーを同期する」の値がデフォルトに設定されている	ユーザーがログオンすると、Profile Management はユーザーストアからローカルプロファイルに除外されたファイルまたはフォルダーを同期します。
設定が「ログオン時に除外されたファイルまたはフォルダーを無視する」に設定されている	ユーザーがログオンすると、Profile Management はユーザーストア内の除外されたファイルまたはフォルダーを無視します。

ポリシー設定	アクション
設定が「ログオン時に除外されたファイルまたはフォルダーを削除する」に設定されている	ユーザーがログオンすると、Profile Management はユーザーストア内の除外されたファイルまたはフォルダーを削除します。
設定がWeb Studioで構成されていない	.ini ファイルの値が使用されます
Web Studio または .ini ファイルで設定が構成されていません	除外されたファイルまたはフォルダーは、ユーザーがログオンするときに、ユーザー ストアからローカル プロファイルに同期されます。

大容量ファイルの処理 - シンボリックリンクとして作成されるファイル

ログオンパフォーマンスを向上させ、サイズの大きいファイルを処理するために、Profile Management はこのリスト内のファイルをコピーする代わりにシンボリックリンクを作成します。

ファイルを参照するポリシーではワイルドカードを使用できます。例: `!ctx_localappdata!\Microsoft\Outlook*.OST`。

Microsoft Outlook のオフラインフォルダーファイル (`*.ost`) を処理するには、**Outlook** フォルダーが Profile Management の対象から除外されていないことを確認してください。

これらのファイルは、複数のセッションで同時にアクセスすることはできません。

同期ポリシー設定

「**同期**」セクションでは、ユーザープロファイル内のどのファイルとフォルダーが、プロファイルがインストールされているシステムとユーザーストアの間で同期されるかを指定するためのポリシー設定について説明します。

同期するディレクトリ

既定では、Profile Management は、ユーザープロファイルを、それがインストールされているシステムとユーザーストアの間で同期します。同期からフォルダーを除外した場合、このポリシーにより、除外されたフォルダーのサブフォルダーを同期に含めることができます。

このリストのパスは、ユーザープロファイルに対する相対パスである必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ユーザープロファイル内の除外されていないフォルダーのみが同期されます。

同期するファイル

既定では、Profile Management は、ユーザープロファイルを、それがインストールされているシステムとユーザーストアの間で同期します。同期からフォルダーを除外した場合、このポリシーにより、除外されたフォルダー内のファイルを同期に含めることができます。

このリストのパスは、ユーザープロファイルに対して相対的である必要があります。ファイル名とフォルダー名でワイルドカードがサポートされていますが、ファイル名でのワイルドカードのみが再帰的に適用されます。ワイルドカードをネストすることはできません。

例:

- `AppData\Local\Microsoft\Office\Access.qat` は、既定の構成で除外されているフォルダーの下にあるファイルを指定します
- `AppData\Local\MyApp*.cfg` は、プロファイルフォルダー `AppData\Local\MyApp` とそのサブフォルダー内の、拡張子 `.cfg` を持つすべてのファイルを指定します

このポリシーを無効にすると、有効にして空のリストを構成した場合と同じ効果があります。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ユーザープロファイル内の除外されていないファイルのみが同期されます。

ミラーリングするフォルダー

このポリシーを使用すると、トランザクションフォルダー（参照フォルダーとも呼ばれます）に関連する問題を解決できます。そのフォルダーには、相互に依存するファイルが含まれており、あるファイルが別のファイルを参照しています。

フォルダーをミラーリングすることで、Profile Managementはトランザクションフォルダーとその内容を単一のエンティティとして処理し、プロファイルの肥大化を防ぐことができます。たとえば、**Internet Explorer cookies**フォルダーをミラーリングして、Index.datがインデックスを作成するCookieと同期するようにできます。このような状況では、「最後の書き込みが優先されます」。そのため、複数のセッションで変更されたミラーリングされたフォルダー内のファイルは、最後の更新によって上書きされ、プロファイル変更が失われることになります。

たとえば、次の表は、ユーザーがインターネットを閲覧しているときにIndex.datがCookieをどのように参照するかを示しています。

シナリオ	INDEX.DAT が COOKIE を参照する方法	
ユーザーは、それぞれ異なるサーバーで2つのInternet Explorerセッションを持ち、各セッションで異なるサイトにアクセスします。	各サイトのCookieが適切なサーバーに追加されます。	各サイトのCookieが適切なサーバーに追加されます。
ユーザーが最初のセッションからログオフするか、セッションの途中でログオフします（アクティブなライトバック機能が構成されている場合）。	2番目のセッションのCookieは、最初のセッションのCookieを置き換える必要があります。	
最初のセッションと2番目のセッションがマージされ、Index.dat内のCookieへの参照が古くなります。	新しいセッションでのさらなる閲覧は、繰り返しのマージと肥大化したCookieフォルダーにつながります。	

Cookieフォルダーをミラーリングすることで、この問題は解決されます。この場合、ユーザーがログオフするたびに、Cookieは最後のセッションのCookieで上書きされます。そのため、Index.datは常に最新の状態に保たれます。

ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。ここで、または .ini ファイルでこのポリシーが構成されていない場合、フォルダーはミラーリングされません。

フォルダーのミラーリングを高速化する

このポリシーと**ミラーリングするフォルダー**ポリシーの両方を有効にすると、**Profile Management はミラーリングされた**フォルダーを VHDX ベースの仮想ディスクに保存します。ログオン時に仮想ディスクをアタッチし、ログオフ時にデタッチします。このポリシーを有効にすると、ユーザー ストアとローカル プロファイルの間でフォルダーをコピーする必要がなくなり、フォルダーのミラーリングが高速化されます。

フォルダーリダイレクトのポリシー設定

このセクションには、プロファイルによく表示されるフォルダーを共有ネットワークの場所にリダイレクトするかどうかを指定するポリシー設定が含まれています。

管理者アクセスの許可

この設定により、管理者はユーザーのリダイレクトされたフォルダーの内容にアクセスできるようになります。

> **注：**
>
> この設定は、ドメインへの完全かつ無制限のアクセス権を持つ管理者に対して権限を付与します。

> デフォルトでは、この設定は無効になっており、ユーザーにはリダイレクトされたフォルダーの内容への排他的アクセス権が付与されます。

ドメイン名を含める

この設定により、`%userdomain%` 環境変数をUNCパスの一部として含めることができます。このUNCパスは、リダイレクトされたフォルダーに対して指定されます。

デフォルトでは、この設定は無効になっています。また、`%userdomain%` 環境変数は、リダイレクトされたフォルダーに対して指定されたUNCパスの一部として含まれません。

デスクトップポリシー設定

このセクションには、`Desktop` フォルダーの内容を共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

デスクトップパス

この設定は、**デスクトップ**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

デスクトップのリダイレクト設定

この設定は、**デスクトップ**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、内容は UNC パスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ドキュメントポリシー設定

このセクションには、**ドキュメント**フォルダーの内容を共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ドキュメントパス

この設定は、**ドキュメント**フォルダー内のファイルがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ドキュメントパス設定は、**ドキュメント**フォルダーにファイルをリダイレクトするだけでなく、**ミュージック**、**ピクチャ**、**ビデオ**フォルダーにファイルをリダイレクトするためにも有効にする必要があります。

ドキュメントのリダイレクト設定

この設定は、**ドキュメント**フォルダーの内容をリダイレクトする方法を指定します。

デフォルトでは、内容は UNC パスにリダイレクトされます。

ドキュメントフォルダーの内容をリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次の UNC パスにリダイレクトします。コンテンツをドキュメントパスポリシー設定で指定された UNC パスにリダイレクトします。
- ユーザーのホームディレクトリにリダイレクトします。コンテンツをユーザーのホームディレクトリにリダイレクトします。これは通常、Active Directory のユーザーの #homeDirectory# 属性として構成されます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ダウンロード ポリシー設定

このセクションには、「**ダウンロード**」フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ダウンロード パス

この設定は、「**ダウンロード**」フォルダー内のファイルがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ダウンロードのリダイレクト設定

この設定は、「**ダウンロード**」フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

お気に入りポリシー設定

このセクションには、「**お気に入り**」フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

お気に入りパス

この設定は、「**お気に入り**」フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

お気に入りのリダイレクト設定

この設定は、「**お気に入り**」フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

リンクポリシー設定

このセクションには、**リンク**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

リンクパス

この設定は、**リンク**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

リンクのリダイレクト設定

この設定は、**リンク**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

音楽ポリシー設定

このセクションには、**Music**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

音楽パス

この設定は、**Music**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

音楽のリダイレクト設定

この設定は、**Music**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

Musicフォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次の UNC パスにリダイレクトします。Music パス ポリシー設定で指定された UNC パスにコンテンツをリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。ドキュメントフォルダーを基準としたフォルダーにコンテンツをリダイレクトします。

Documentsフォルダーを基準としたフォルダーにコンテンツをリダイレクトするには、**Documents path**設定を有効にする必要があります。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

Searchesポリシー設定

このセクションには、**Searches**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

SEARCHESのリダイレクト設定

この設定は、**Searches**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

SEARCHESパス

この設定は、**Searches**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ビデオポリシー設定

このセクションには、**ビデオ**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ビデオのリダイレクト設定

この設定は、**ビデオ**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ビデオフォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクトします。コンテンツを、ビデオパスポリシー設定で指定されたUNCパスにリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。コンテンツを、ドキュメントフォルダーを基準としたフォルダーにリダイレクトします。

コンテンツを**ドキュメント**フォルダーを基準としたフォルダーにリダイレクトするには、**ドキュメントパス**設定を有効にする必要があります。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ビデオパス

この設定は、**ビデオ**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ログポリシー設定

このセクションには、Profile Management のログを構成するポリシー設定が含まれています。

Active Directory のアクション

この設定は、Active Directory で実行されるアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログを有効にする**設定も有効になっていることを確認してください。

この設定が Web Studio で構成されていない場合、.ini ファイルの値が使用されます。

この設定が Web Studio または .ini ファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般情報

この設定は、一般情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログを有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般的な警告

この設定は、一般的な警告の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログの有効化

この設定は、デバッグ（詳細ログ）モードでのProfile Managementログを有効または無効にします。デバッグモードでは、"%SystemRoot%\System32\Logfiles\UserProfileManager" にあるログファイルに詳細なステータス情報が記録されます。

デフォルトでは、この設定は無効になっており、エラーのみがログに記録されます。

Citrix®は、Profile Managementのトラブルシューティングを行う場合にのみ、この設定を有効にすることをお勧めします。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここで、または.iniファイルで構成されていない場合、エラーのみがログに記録されます。

ファイルシステムのアクション

この設定は、ファイルシステムで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ファイルシステム通知

この設定は、ファイルシステム通知の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ

この設定は、ユーザーのログオフの詳細ログ記録を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオン

この設定は、ユーザーのログオンの詳細ログ記録を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログファイルの最大サイズ

この設定は、Profile Managementログファイルの最大許容サイズをバイト単位で指定します。

デフォルトでは、この値は1048576バイト（1 MB）に設定されています。

十分なディスク容量がある場合、Citrixはこのファイルのサイズを5 MB以上に増やすことを推奨します。ログファイルが最大サイズを超えて増加した場合：

- 既存のファイルのバックアップ（.bak）が削除されます
- ログファイルは.bakに名前が変更されます
- 新しいログファイルが作成されます

ログファイルは`%SystemRoot%\System32\Logfiles\UserProfileManager`に作成されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここで、または.iniファイルで構成されていない場合、デフォルト値が使用されます。

ログファイルへのパス

この設定は、Profile Managementログファイルを保存するための代替パスを指定します。

デフォルトでは、この設定は無効になっており、ログファイルはデフォルトの場所である%SystemRoot%\System32\Logfiles\UserProfileManagerに保存されます。

パスはローカルドライブまたはリモートのネットワークベースドライブ（UNCパス）を指すことができます。リモートパスは大規模な分散環境で役立つ場合がありますが、大量のネットワークトラフィックを発生させる可能性があり、ログファイルには不適切な場合があります。永続的なハードドライブを持つプロビジョニングされた仮想マシンでは、そのドライブへのローカルパスを設定します。この設定により、マシンの再起動時にログファイルが保持されます。永続的なハードドライブを持たない仮想マシンでは、UNCパスを設定することでログファイルを保持できます。ただし、マシンのシステムアカウントにはUNC共有への書き込みアクセス権が必要です。オフラインプロファイル機能によって管理されるラップトップには、ローカルパスを使用してください。

ログファイルにUNCパスを使用する場合、Citrixはログファイルフォルダーに適切なアクセス制御リストを適用することを推奨します。この設定により、承認されたユーザーまたはコンピューターアカウントのみが保存されたファイルにアクセスできるようになります。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、デフォルトの場所である%SystemRoot%\System32\Logfiles\UserProfileManagerが使用されます。

パーソナライズされたユーザー情報

この設定は、パーソナライズされたユーザー情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ時のレジストリの相違点

この設定は、ユーザーがログオンおよびログオフしたときのポリシー値の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

レジストリアクション

この設定は、レジストリで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ時のレジストリの差異

この設定は、ユーザーがログオフしたときにレジストリ内の差異を詳細にログ記録するかどうかを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

プロファイル処理ポリシー設定

このセクションには、プロファイル管理がユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

キャッシュされたプロファイルを削除するまでの遅延

この設定は、ログオフ時にプロファイル管理がローカルにキャッシュされたプロファイルを削除するまでの遅延を、分単位で任意に延長する時間を指定します。

値が0の場合、ログオフプロセスの終了時にプロファイルがすぐに削除されます。プロファイル管理は1分ごとにログオフをチェックします。その結果、値が60の場合、ユーザーがログオフしてから1〜2分以内にプロファイルが削除されることが保証されます。このアクションは、最後のチェックがいつ行われたかによって異なります。ログオフ中にプロセスがファイルまたはユーザー

レジストリハイブを開いたままにしていることがわかっている場合、遅延を延長すると便利です。大規模なプロファイルの場合、このプロセスはログオフを高速化することもできます。

デフォルトでは、この値は0に設定されており、プロファイル管理はローカルにキャッシュされたプロファイルをすぐに削除します。

この設定を有効にする場合は、「ログオフ時にローカルにキャッシュされたプロファイルを削除」も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここで、または.iniファイルでこの設定が構成されていない場合、プロファイルはすぐに削除されます。

ログオフ時にローカルにキャッシュされたプロファイルを削除

この設定は、ユーザーがログオフした後にローカルにキャッシュされたプロファイルを削除するかどうかを指定します。

この設定が有効になっている場合、ユーザーのローカルプロファイルキャッシュはログオフ後に削除されます。Citrix®は、ターミナルサーバーに対してこの設定を有効にすることをお勧めします。

デフォルトでは、この設定は無効になっており、ユーザーのローカルプロファイルキャッシュはログオフ後も保持されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここで、または.iniファイルでこの設定が構成されていない場合、キャッシュされたプロファイルは削除されません。

ローカルプロファイルの競合処理

この設定は、ユーザープロファイルが以下の両方に存在する場合のProfile Managementの動作を構成します。

- ユーザーストア
- ローカルWindowsユーザープロファイル（Citrixユーザープロファイルではない）

デフォルトでは、Profile Management はローカルの Windows プロファイルを使用しますが、それを一切変更しません。

Profile Managementの動作を制御するには、以下のいずれかのオプションを選択します。

- ローカルプロファイルを使用する。Profile Managementはローカルプロファイルを使用しますが、それを変更することはありません。
- ローカルプロファイルを削除する。Profile ManagementはローカルWindowsユーザープロファイルを削除し、その後ユーザーストアからCitrixユーザープロファイルをインポートします。
- ローカルプロファイルの名前を変更する。Profile ManagementはローカルWindowsユーザープロファイルの名前を変更し（バックアップ目的で）、その後ユーザーストアからCitrixユーザープロファイルをインポートします。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここで、または .ini ファイルで構成されていない場合、既存のローカルプロファイルが使用されます。

既存プロファイルの移行

この設定は、ユーザーがユーザーストアに現在のプロファイルを持っていない場合に、ログオン中にユーザーストアに移行されるプロファイルの種類を指定します。

ユーザーがユーザーストアにプロファイルを持っていない場合、Profile Managementはログオン中に既存のプロファイルを「その場で」移行できます。その後、ユーザーストアプロファイルはProfile Managementによって以下の両方で使用されます。

- 現在のセッション
- 同じユーザー ストアへのパスで構成された他のセッション

デフォルトでは、ローカルプロファイルと移動プロファイルの両方がログオン中にユーザー ストアに移行されます。

ログオン中にユーザー ストアに移行されるプロファイルの種類を指定するには、次のいずれかのオプションを選択します。

- ローカルプロファイルと移動プロファイル
- ローカル
- ローミング
- なし (無効)

なしを選択すると、システムは、Profile Managementがインストールされていない環境であるかのように、既存のWindowsメカニズムを使用してプロファイルを作成します。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここで、または.iniファイルでこの設定が構成されていない場合、既存のローカルプロファイルと移動プロファイルが移行されます。

既存のアプリケーションプロファイルの自動移行

この設定は、異なるオペレーティングシステム間で既存のアプリケーションプロファイルを自動的に移行するかどうかを有効または無効にします。アプリケーションプロファイルには、`AppData`フォルダー内のアプリケーションデータと、`HKEY_CURRENT_USER\SOFTWARE`の下のレジストリエントリの両方が含まれます。この設定は、異なるオペレーティングシステム間でアプリケーションプロファイルを移行したい場合に役立ちます。

たとえば、オペレーティングシステム (OS) をWindows 10バージョン1803からWindows 10バージョン1809にアップグレードするとします。この設定が有効になっている場合、各ユーザーが最初にログオンしたときに、Profile Managementは既存のアプリケーション設定をWindows 10バージョン1809に自動的に移行します。その結果、`AppData`フォルダー内のアプリケーションデータと、HKEY_CURRENT_USER\SOFTWAREの下のレジストリエントリが移行されます。

複数の既存のアプリケーションプロファイルがある場合、Profile Managementは次の優先順位で移行を実行します。

1. 同じOSタイプのプロファイル (シングルセッションOSからシングルセッションOSへ、マルチセッションOSからマルチセッションOSへ)。
2. 同じWindows OSファミリーのプロファイル (例: Windows 10からWindows 10、またはWindows Server 2016からWindows Server 2016)。
3. 以前のバージョンのOSのプロファイル (例: Windows 7からWindows 10、またはWindows Server 2012からWindows 2016)。
4. 最も近いOSのプロファイル。

注： ユーザーストアパスに変数「!CTX_OSNAME!」を含めることで、OSの短い名前を指定する必要があります。これにより、Profile Managementは既存のアプリケーションプロファイルを特定できます。

ここでこの設定が構成されていない場合、.iniファイルの設定が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、デフォルトで無効になります。

テンプレートプロファイルへのパス

この設定は、Profile Managementがユーザープロファイルを作成するためのテンプレートとして使用するプロファイルへのパスを指定します。

指定されたパスは、NTUSER.DATレジストリファイルと、テンプレートプロファイルに必要なその他のフォルダーおよびファイルを含むフォルダーへの完全なパスである必要があります。

注: パスにNTUSER.DATを含めないでください。たとえば、ファイル`\\myservername\myprofiles\template\ntuser.dat`の場合、場所を`\\myservername\myprofiles\template`として設定します。

絶対パスを使用します。これはUNCパスまたはローカルマシン上のパスのいずれかです。後者を使用すると、たとえば、Citrix Provisioning™ Servicesイメージ上にテンプレートプロファイルを永続的に指定できます。相対パスはサポートされていません。

注: この設定は、Active Directory属性、システム環境変数、または`%USERNAME%`および`%USERDOMAIN%`変数の展開をサポートしていません。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンするデバイスのデフォルトユーザープロファイルから作成されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルがローカルプロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルがローカルプロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、ローカルのWindowsユーザープロファイルを持っているとします。この場合、この値が有効になっていると、デフォルトでローカルプロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの作成時に使用されるローカルプロファイルをテンプレートプロファイルが上書きできるようになります。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルが移動プロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルが移動プロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、移動Windowsユーザープロファイルを持っているとします。この場合、この値が有効になっていると、デフォルトで移動プロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの

作成時に使用される移動プロファイルをテンプレートプロファイルが上書きできるようになります。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、テンプレートは使用されません。

すべてのログオンでCitrix必須プロファイルとして使用されるテンプレートプロファイル

この設定により、Profile Managementはテンプレートプロファイルをすべてのユーザープロファイルを作成するためのデフォルトプロファイルとして使用できるようになります。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンしたデバイスのデフォルトユーザープロファイルから作成されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、テンプレートは使用されません。

レジストリポリシー設定

このセクションには、Profile Management の処理に含めるレジストリキーと除外するレジストリキーを指定するポリシー設定が含まれています。

除外リスト

ログオフ時に無視されるHKCUハイブ内のレジストリキーのリスト。

例: Software\Policies

このポリシーが無効になっている場合、レジストリキーは除外されません。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、レジストリキーは除外されません。

含めるリスト

ログオフ時に処理されるHKCUハイブ内のレジストリキーのリスト。

例: Software\Adobe。

このポリシーが有効になっている場合、このリストにあるキーのみが処理されます。このポリシーが無効になっている場合、HKCUハイブ全体が処理されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、HKCUのすべてが処理されます。

デフォルトの除外リストを有効にする - Profile Management 5.5

ユーザープロファイルに同期されないHKCUハイブ内のレジストリキーのデフォルトリスト。このポリシーを使用して、GPO除外ファイルを手動で入力することなく指定できます。

このポリシーを無効にすると、Profile Management はデフォルトでレジストリキーを除外しません。ここでこのポリシーを構成しない場合、Profile Management は.iniファイルの値を使用します。ここで、または.iniファイルでこのポリシーを構成しない場合、Profile Management はデフォルトでレジストリキーを除外しません。

NTUSER.DATのバックアップ

NTUSER.DATの最後に正常だったコピーのバックアップと、破損時のロールバックを有効にします。

ここでこのポリシーを構成しない場合、Profile Management は .ini ファイルの値を使用します。ここで、または .ini ファイルでこのポリシーを構成しない場合、Profile Management は NTUSER.DAT をバックアップしません。

ストリーミングユーザープロファイルポリシー設定

このセクションには、Profile Management がストリーミングユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

常にキャッシュ

この設定は、ユーザーがログオンした直後に Profile Management がストリーミングファイルをキャッシュするかどうかを指定します。ユーザーがログオンした後にファイルをキャッシュすると、ネットワーク帯域幅が節約され、ユーザーエクスペリエンスが向上します。

この設定は、**プロファイルストリーミング**設定と組み合わせて使用します。

デフォルトでは、この設定は無効になっており、ユーザーがログオンした直後にストリーミングファイルはキャッシュされません。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

常にキャッシュするサイズ

この設定は、ストリーミングされるファイルのサイズの下限を MB 単位で指定します。Profile Management は、このサイズ以上のファイルを、ユーザーがログオンした直後にキャッシュします。

デフォルトでは、値は 0 (ゼロ) に設定されており、プロファイル全体をキャッシュする機能が使用されます。プロファイル全体をキャッシュする機能が有効になっている場合、Profile Management は、ユーザーがログオンした後、ユーザーストア内のすべてのプロファイルコンテンツをバックグラウンドタスクとしてフェッチします。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

プロファイルストリーミング

この設定は、Citrix® ストリーミングユーザープロファイル機能を有効または無効にします。有効にすると、プロファイルファイルとフォルダーは、ユーザーがログオン後にアクセスした場合にのみ、ユーザーストアからローカルコンピューターにフェッチされます。レジストリエントリと保留領域のファイルはすぐにフェッチされます。

デフォルトでは、プロファイルストリーミングは無効になっています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

ストリーム配信ユーザープロファイルグループ

この設定は、Windows ユーザーグループに基づいて、OU 内のどのユーザープロファイルをストリーム配信するかを指定します。

有効にすると、指定されたユーザーグループ内のユーザープロファイルのみがストリーミングされます。その他のすべてのユーザープロファイルは通常どおり処理されます。

デフォルトでは、この設定は無効になっており、OU内のすべてのユーザープロファイルは通常どおり処理されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、すべてのユーザープロファイルが処理されます。

プロファイルストリーミング除外を有効にする

プロファイルストリーミング除外が有効になっている場合：

- Profile Managementは除外リスト内のフォルダーをストリーミングしません
- ユーザーがログオンすると、すべてのフォルダーがユーザーストアからローカルコンピューターに即座にフェッチされます

詳細については、「ユーザープロファイルのストリーム」を参照してください。

ペンディングエリアロックファイルのタイムアウト

この設定は、ストレージサーバーが応答しなくなったときにユーザープロファイルストアがロックされたままの場合に、保留領域からユーザープロファイルストアにユーザーのファイルが書き戻されるまでの日数を指定します。この動作により、保留領域の肥大化を防ぎ、ユーザープロファイルストアに常に最新のファイルが含まれるようにします。

デフォルトでは、この設定は1日（1）に設定されています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、デフォルト値が使用されます。

ペンディングエリアのプロファイルストリーミングを有効にする

保留領域内のファイルとフォルダーに対してプロファイルストリーミング機能を有効にできます。

保留領域は、プロファイルストリーミングが有効になっている間のプロファイルの一貫性を確保するために使用されます。これは、同時セッションで変更されたプロファイルファイルとフォルダーを一時的に保存します。

デフォルトでは、このポリシーは無効になっており、保留領域内のすべてのファイルとフォルダーはログオン時にローカルプロファイルにフェッチされます。このポリシーを有効にすると、保留領域内のファイルは要求されたときにのみローカルプロファイルにフェッチされます。同時セッションのシナリオで最適なログオンエクスペリエンスを確保するには、このポリシーをプロファイルストリーミングポリシーと組み合わせて使用してください。

このポリシーは、フォルダーのプロファイルストリーミングを有効にするポリシーが有効になっている場合に、保留領域内のフォルダーに適用されます。

ユーザーパーソナライゼーションポリシー設定

Virtual Delivery Agent 内でのユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- 新しいユーザーレイヤーディスクがどのくらいのサイズまで拡張できるか。

これを行うには、利用可能なポリシーのリストに次の2つのポリシーが表示されます。

- ユーザーレイヤーリポジトリパス - 値フィールドに「\\サーバー名またはアドレス\フォルダー名」の形式でパスを入力します。
- ユーザーレイヤーサイズ (GB) - デフォルトのユーザーレイヤーサイズである10 GBは、Citrix® が推奨する最小値です。ユーザーレイヤーは、使用されるスペースに応じて設定されたサイズまで拡張するシンプロビジョニングディスクです。ユーザーレイヤーのサイズが小さくなることはありません。

> **注：**
>
> ユーザーレイヤーサイズを増やすと、新しいユーザーレイヤーに影響し、既存のレイヤーが拡張されます。レイヤーサイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

Virtual Delivery Agent のポリシー設定

Virtual Delivery Agent (VDA) セクションには、VDA とサイトのコントローラー間の通信を制御するポリシー設定が含まれています。

重要: 自動更新機能を使用しない場合、VDA は Delivery Controller™ に登録するために、これらの設定によって提供される情報を必要とします。この情報は登録に必要であるため、VDA のインストール中にこの情報を提供しない限り、グループポリシーエディターを使用して以下の設定を構成する必要があります。

- コントローラー登録 IPv6 ネットマスク
- コントローラー登録ポート
- コントローラー SID
- コントローラー
- IPv6 コントローラー登録のみを使用
- サイト GUID

コントローラー登録 IPv6 ネットマスク

このポリシー設定により、管理者は VDA を優先サブネットのみに制限できます（グローバル IP が登録されている場合でも）。この設定は、VDA が登録する IPv6 アドレスとネットワークを指定します。VDA は、指定されたネットマスクに一致する最初のアドレスにのみ登録します。この設

定は、「IPv6 コントローラー登録のみを使用」ポリシー設定が有効になっている場合にのみ有効です。

デフォルトでは、この設定は空白です。

コントローラー登録ポート

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する場合に、VDA がコントローラーに登録するために使用する TCP/IP ポート番号を指定します。

デフォルトでは、ポート番号は80に設定されています。

コントローラーSID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する際にVDAがコントローラーに登録するために使用する、スペース区切りのコントローラーセキュリティ識別子（SID）のリストを指定します。この設定はオプションであり、登録に使用されるコントローラーのリストを制限するために**コントローラー**設定と組み合わせて使用される場合があります。

デフォルトでは、この設定は空白です。

コントローラー

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する際にVDAがコントローラーに登録するために使用する、スペース区切りのコントローラー完全修飾ドメイン名（FQDN）のリストを指定します。この設定はオプションであり、**コントローラーSID**設定と組み合わせて使用される場合があります。

デフォルトでは、この設定は空白です。

コントローラーの自動更新を有効にする

この設定により、VDAはインストール後にコントローラーに自動的に登録できるようになります。

VDAが登録されると、登録先のコントローラーは現在のコントローラーFQDNとSIDのリストをVDAに送信します。VDAはこのリストを永続ストレージに書き込みます。各コントローラーは、90分ごとにサイトデータベースでコントローラー情報を確認します。以下のいずれかが発生した場合、コントローラーは登録済みのVDAに更新されたリストを送信します。

- 前回のチェック以降にコントローラーが追加または削除された場合
- ポリシーの変更が発生した場合

VDAは、受信した最新のリストにあるすべてのコントローラーからの接続を受け入れます。

デフォルトでは、この設定は有効になっています。

IPv6コントローラー登録のみを使用

この設定は、VDAがControllerに登録するために使用するアドレス形式を制御します。

- 有効にすると、VDAはマシンのIPv6アドレスを使用してControllerに登録します。VDAがControllerと通信する場合、次のアドレス順序を使用します: グローバルIPアドレス、ユニークローカルアドレス (ULA)、リンクローカルアドレス (他のIPv6アドレスが利用できない場合)。
- 無効にすると、VDAはマシンのIPv4アドレスを使用してControllerに登録し、通信します。

デフォルトでは、この設定は無効になっています。

サイトGUID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、Active Directoryベースの登録を使用する際に、VDAがControllerに登録するために使用するサイトのグローバル一意識別子 (GUID) を指定します。

デフォルトでは、この設定は空白です。

HDX™ 3D Pro ポリシー設定

HDX 3D Proセクションには、ユーザー向けの画質構成ツールを有効化および構成するためのポリシー設定が含まれています。このツールを使用すると、ユーザーは利用可能な帯域幅の使用を最適化できます。この最適化のために、画質と応答性のバランスがリアルタイムで調整されます。

ロスレスを有効にする

この設定は、ユーザーが画質構成ツールを使用してロスレス圧縮を有効または無効にできるかどうかを指定します。デフォルトでは、ユーザーにロスレス圧縮を有効にするオプションは提供されません。

ユーザーがロスレス圧縮を有効にしたとします。この場合、画質は画質構成ツールで利用可能な最大値に自動的に設定されます。デフォルトでは、ユーザーデバイスとホストコンピューターの機能に応じて、GPUまたはCPUベースの圧縮のいずれかを使用できます。

HDX 3D Pro 品質設定

この設定は、画質構成ツールでユーザーが利用できる最小値と最大値を指定します。これらの値を使用すると、画質構成ツールで画質調整の範囲を定義できます。

画質の値は0から100（両端を含む）の間で指定します。最大値は最小値以上である必要があります。

監視ポリシー設定

「**監視**」セクションには、プロセス、リソース監視、およびアプリケーション障害監視のポリシー設定が含まれています。

これらのポリシーのスコープは、以下に基づいて定義できます。

- サイト
- デリバリーグループ
- デリバリーグループの種類
- 組織単位
- タグ

プロセスおよびリソース監視のポリシー

CPU、メモリ、プロセスの各データポイントはVDAから収集され、監視データベースに保存されます。VDAからデータポイントを送信するとネットワーク帯域幅を消費し、それらを保存すると監視データベースの相当なスペースを消費します。特定のスコープ（たとえば、特定のデリバリーグループや組織単位）に対して、リソースデータ、プロセスデータ、またはその両方を監視したくない場合を考慮してください。この場合、ポリシーを無効にすることをお勧めします。

プロセス監視を有効にする

この設定を有効にすると、VDAがインストールされているマシンで実行されているプロセスの監視が可能になります。CPUやメモリ使用量などの統計情報は監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは無効です。

リソース監視を有効にする

この設定を有効にすると、VDAがインストールされているマシン上の重要なパフォーマンスカウンターの監視が可能になります。CPUやメモリ使用量、IOPS、ディスク遅延データなどの統計情報は監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは有効です。

スケーラビリティ

CPUおよびメモリデータは、各VDAから5分間隔でデータベースにプッシュされます。プロセスデータ（有効な場合）は10分間隔でデータベースにプッシュされます。IOPSおよびディスク待機時間データは1時間間隔でデータベースにプッシュされます。

CPUとメモリデータ

CPUとメモリデータは、デフォルトで**有効**です。データ保持期間の値は次のとおりです (Platinumライセンス):

データ粒度	日数
5分間隔のデータ	1日
10分間隔のデータ	7日
1時間間隔のデータ	30日
1日間隔のデータ	90日

IOPSおよびディスク遅延データ

IOPSおよびディスク遅延データは、デフォルトで**有効**です。データ保持値は次のとおりです（Platinumライセンス）：

データ粒度	日数
時間データ	3日間
日次データ	90日間

データ保持設定では、1つのVDAに対して1年間で以下のデータを保存するために、約276 KBのディスク容量が必要です。

- CPU

- メモリ
- IOPS
- ディスク遅延データ

マシンの数	必要なストレージの概算
1	276 KB
1K	270 MB
40K	10.6 GB

プロセスデータ

プロセスデータはデフォルトで**無効**です。必要に応じて、一部のマシンでプロセスデータを有効にすることをお勧めします。プロセスデータのデフォルトのデータ保持設定は次のとおりです。

データ粒度	日数
10分間データ	1日
時間データ	7日

プロセスデータがデフォルトの保持設定で有効になっている場合、プロセスデータは1年間でVDAあたり約1.5 MB、Terminal Services VDA (TS VDA)あたり3 MBを消費します。

マシン数	必要なストレージの目安 VDA	必要なストレージの目安 TS VDA
1	1.5 MB	3 MB
1K	1.5 GB	3 GB

注:

以前に提示された数値には、インデックス領域は含まれていません。また、すべての計算は概算であり、展開によって異なります。

オプションの構成

必要に応じて、デフォルトの保持設定を変更できます。ただし、この構成は追加のストレージを消費します。以下の設定を有効にすることで、プロセス使用率データの精度を高めることができます。有効にできる構成は次のとおりです。

ENABLEMINUTELEVELGRANULARITYPROCESSUTILIZATION

ENABLEDAYLEVELGRANULARITYPROCESSUTILIZATION

これらの構成は、監視PowerShellコマンドレットのSet-MonitorConfigurationから有効にできます。

アプリケーション障害監視のポリシー

デフォルトでは、**アプリケーション障害**タブには、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。アプリケーション障害監視の設定は、以下の監視ポリシーで変更できます。

アプリケーション障害の監視を有効にする

この設定を使用して、アプリケーション障害監視を構成し、アプリケーションエラーまたは障害（クラッシュおよび未処理の例外）、あるいはその両方を監視します。 **値**を**None**に設定すると、アプリケーション障害監視が無効になります。 この設定のデフォルトは「アプリケーション障害のみ」です。

シングルセッションOS VDAでのアプリケーション障害の監視を有効にする

デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションからの障害のみが監視されます。シングルセッションOS VDAを監視するには、ポリシーを**Allowed**に設定します。 この設定のデフォルトは**Prohibited**です。

障害監視から除外されるアプリケーションのリスト

障害監視の対象としないアプリケーションのリストを指定します。 デフォルトでは、このリストは空です。

Analytics 用データ収集のポリシー

ANALYTICS 用 VDA データ収集

このポリシーを使用して、パフォーマンスおよびセキュリティ分析のために、Monitorサービスが VDAのパフォーマンスおよびセキュリティ関連メトリックを収集するのを有効または無効にします。デフォルトでは、ポリシーは**Allowed**です。VDAからのデータ収集を停止するには、ポリシーを**Prohibited**に設定します。

セキュリティ監視のためのクリップボード場所メタデータ収集

このポリシーを使用して、セキュリティ監視、監査、およびコンプライアンスのために、Brokerサービスによるクリップボード場所メタデータ収集を有効または無効にします。デフォルトでは、このポリシーは**有効**です。VDA からのデータ収集を停止するには、ポリシーを**無効**に設定します。

パフォーマンス監視のための診断データ収集

このポリシーを使用して、監視サービスがセッション情報、UPM/EUEM サービスの状態、Microsoft Teams の最適化、接続プロトコルなどの診断データを収集できるようにします。デフォルトでは、このポリシーは**有効**です。VDA からのデータ収集を停止するには、ポリシーを**無効**に設定します。

ストレージ計画のヒント

グループポリシー。リソースデータまたはプロセスデータの監視に関心がない場合は、グループポリシーを使用してその両方または一方をオフにできます。詳細については、ポリシーの作成の「**グループポリシー**」セクションを参照してください。

データグルーミング。デフォルトのデータ保持設定を変更して、データを早期にグルーミングし、ストレージスペースを解放できます。グルーミング設定の詳細については、APIを使用したデータアクセスの「データの粒度と保持」を参照してください。

レジストリを使用してCOMポートおよびLPTポートリダイレクト設定を構成する

VDAバージョン7.0から7.8では、**COMポートおよびLPTポート**の設定は、レジストリを使用してのみ構成できます。VDAバージョン7.0より前、およびVDAバージョン7.9以降では、これらの設定はWeb Studioで構成できます。詳しくは、「ポートリダイレクトポリシー設定」および「帯域幅ポリシー設定」を参照してください。

COMポートおよびLPTポートリダイレクトのポリシー設定は、VDAイメージまたはマシン上のHKLM\Software\Citrix\GroupPolicy\Defaults\Deprecatedにあります。

COMポートおよびLPTポートリダイレクトを有効にするには、次のようにREG_DWORD型の新しいレジストリキーを追加します。

注意：レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

レジストリキー	説明	許可される値
AllowComPortRedirection	COMポートリダイレクトを許可または禁止する	1（許可）または0（禁止）
LimitComBw	COMポートリダイレクトチャネルの帯域幅制限	数値
LimitComBWPercent	COMポートリダイレクトチャネルの帯域幅制限（セッションの総帯域幅に対する割合）	0から100までの数値
AutoConnectClientComPorts	ユーザーデバイスからCOMポートを自動的に接続する	1 (許可) または 0 (禁止)
AllowLptPortRedirection	LPTポートリダイレクトを許可または禁止する	1 (許可) または 0 (禁止)
LimitLptBw	LPTポートリダイレクトチャネルの帯域幅制限	数値
LimitLptBwPercent	LPTポートリダイレクトチャネルの帯域幅制限（セッション全体の帯域幅に対する割合）	0から100までの数値
AutoConnectClientLptPorts	ユーザーデバイスからLPTポートを自動的に接続する	1 (許可) または 0 (禁止)

これらの設定を構成した後、新しいマスターイメージまたは更新された物理マシンを使用するようにマシンカタログを変更します。ユーザーが次回ログオフしたときに、デスクトップは新しい設定で更新されます。

Configuration Manager 2012用コネクタのポリシー設定

Configuration Manager 2012用コネクタのセクションには、Citrix Connector 7.5エージェントを構成するためのポリシー設定が含まれています。

> **重要:**

> 警告、ログオフ、および再起動メッセージのポリシーは、手動またはProvisioning Servicesによって管理されるマルチセッションOSマシンカタログへの展開にのみ適用されます。これらのマシンカタログの場合、コネクタサービスは、保留中のアプリケーションのインストールまたはソフトウェアの更新がある場合にユーザーに警告します。

> MCSによって管理されるカタログの場合、Web Studioを使用してユーザーに通知します。手動で管理されるシングルセッションOSカタログの場合、Configuration Managerを使用してユーザーに通知します。Provisioning Servicesによって管理されるシングルセッションOSカタログの場合、Provisioning Servicesを使用してユーザーに通知します。

警告頻度間隔

この設定は、ユーザーへの警告メッセージの表示間隔を定義します。

間隔は、ddd.hh:mm:ss の形式で設定されます。ここで、:

- ddd は日数で、オプションのパラメーターであり、範囲は 0〜999 です。
- hh は時間で、範囲は 0〜23 です。
- mm は分で、範囲は 0〜59 です。
- ss は秒で、範囲は 0〜59 です。

デフォルトでは、間隔設定は1時間（01:00:00）です。

警告メッセージボックスの本文

この設定には、今後のソフトウェア更新またはログオフを必要とするメンテナンスについてユーザーに通知するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは次のとおりです: {TIMESTAMP} 作業を保存してください。サーバーは{TIMELEFT}後にメンテナンスのためオフラインになります。

警告メッセージボックスのタイトル

この設定には、ユーザーへの警告メッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは次のとおりです: 今後のメンテナンス

警告期間

この設定は、メンテナンスのどれくらい前に警告メッセージが最初に表示されるかを定義します。

時刻は ddd.hh:mm:ss の形式で設定されます。ここで、:

- ddd は日数で、オプションのパラメーターであり、0〜999 の範囲です。
- hh は時間で、0〜23 の範囲です。
- mm は分で、0〜59 の範囲です。
- ss は秒で、0〜59 の範囲です。

デフォルトでは、設定は 16 時間 (16:00:00) であり、最初の警告メッセージがメンテナンスの約 16 時間前に表示されることを示します。

最終強制ログオフメッセージボックスの本文

この設定には、強制ログオフが開始されたことをユーザーに警告するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは次のとおりです: サーバーは現在、メンテナンスのためオフラインになります

最終強制ログオフメッセージボックスのタイトル

この設定には、最終強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「ITスタッフからの通知」です。

強制ログオフ猶予期間

この設定は、ユーザーにログオフを通知してから、保留中のメンテナンスを処理するための強制ログオフが実行されるまでの期間を定義します。

時間はddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメータであり、範囲は0〜999です。
- hhは時間で、範囲は0〜23です。
- mmは分で、範囲は0〜59です。
- ssは秒で、範囲は0〜59です。

デフォルトでは、設定は16時間 (16:00:00) であり、最初の警告メッセージがメンテナンスの約16時間前に表示されることを示します。

最終強制ログオフメッセージボックスの本文テキスト

この設定には、強制ログオフが開始されたことをユーザーに警告するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは「サーバーは現在メンテナンスのためオフラインになります」です。

最終強制ログオフメッセージボックスのタイトル

この設定には、最終的な強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「ITスタッフからの通知」です。

強制ログオフ猶予期間

この設定は、ユーザーにログオフを通知してから、保留中のメンテナンスを処理するための強制ログオフが実行されるまでの期間を定義します。

時間はddd.hh:mm:ssの形式で設定され、ここで:

- dddは日数で、オプションのパラメーターであり、範囲は0～999です。
- hhは時間で、範囲は0～23です。
- mmは分で、範囲は0～59です。
- ssは秒で、範囲は0～59です。

デフォルトでは、強制ログオフ猶予期間の設定は5分 (00:05:00) です。

強制ログオフメッセージボックスの本文

この設定には、強制ログオフが開始される前に、作業を保存してログオフするようユーザーに伝えるメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージには次の内容が含まれています: {TIMESTAMP} 作業を保存してログオフしてください。サーバーは{TIMELEFT}後にメンテナンスのためオフラインになります。

強制ログオフメッセージボックスのタイトル

この設定には、強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「ITスタッフからの通知」です。

イメージ管理モード

コネクタエージェントは、Provisioning ServicesまたはMCSによって管理されているマシンのクローン上で実行されているかどうかを自動的に検出します。エージェントは、イメージ管理されたクローンでのConfiguration Managerの更新をブロックし、カタログのマスターイメージに更新を自動的にインストールします。

マスターイメージが更新された後、Web Studioを使用してMCSカタログクローンの再起動を調整します。Connector Agentは、Configuration Managerのメンテナンスウィンドウ中にPVSカタログクローンの再起動を自動的に調整します。Configuration Managerによってカタログクローンにソフトウェアがインストールされるようにこの動作を上書きするには、「イメージ管理モード」を「無効」に変更します。

再起動メッセージボックスの本文

この設定には、サーバーが再起動されることをユーザーに通知するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは「サーバーは現在、メンテナンスのためにオフラインになります。」です。

エージェントタスクが実行される定期的な時間間隔

この設定は、Citrix Connector™エージェントタスクが実行される頻度を決定します。

時間はddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、範囲は0～999です。
- hhは時間で、範囲は0～23です。
- mmは分で、範囲は0～59です。
- ssは秒で、範囲は0～59です。

デフォルトでは、通常の時間間隔設定は5分（00:05:00）です。

管理

Citrix Virtual Apps and Desktops™ サイトの管理には、さまざまな項目とタスクが含まれます。

ライセンス

サイトを作成する際には、Citrix License Serverへの有効な接続が必要です。その後、Studioからライセンスの追加、ライセンスの種類やモデルの変更、ライセンス管理者の管理など、いくつかのライセンス関連タスクを実行できます。StudioからLicense Administration Consoleにアクセスすることもできます。

アプリケーション

Delivery GroupおよびオプションでApplication Group内のアプリケーションを管理します。

ゾーン

地理的に分散した展開では、ゾーンを使用してアプリケーションとデスクトップをエンドユーザーに近づけることで、パフォーマンスを向上させることができます。サイトをインストールして構成すると、すべてのController、マシンカタログ、およびホスト接続は1つのプライマリゾーンに配置されます。その後、Studioを使用して、これらの項目を含むサテライトゾーンを作成できます。サイトに複数のゾーンがある場合、新しく作成されたマシンカタログ、ホスト接続、または追加されたControllerがどのゾーンに配置されるかを示すことができます。ゾーン間で項目を移動することもできます。

接続とリソース

アプリケーションとデスクトップをユーザーに提供するマシンをホストするためにハイパーバイザーまたはその他のサービスを使用している場合、サイトを作成する際に、そのハイパーバイザーまたはその他のサービスへの最初の接続を作成します。その接続のストレージとネットワークの詳細がそのリソースを構成します。その後、その接続とそのリソースを変更したり、さらに多くの接続を作成したりできます。構成された接続を使用するマシンを管理することもできます。

ローカルホストキャッシュ

ローカルホストキャッシュにより、Delivery Controller™ とサイトデータベース間の接続が失敗した場合でも、サイトでの接続ブローカー操作を続行できます。

仮想IPと仮想ループバック

Microsoft の仮想IPアドレス機能は、公開アプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrix の仮想ループバック機能を使用すると、localhost との通信に依存するアプリケーションを、localhost 範囲内の一意の仮想ループバックアドレスを使用するように構成できます。

デリバリーコントローラー

この記事では、サイトへのControllerの追加と削除に関する考慮事項と手順について説明します。また、Controllerを別のゾーンまたはサイトに移動する方法、およびVDAを別のサイトに移動する方法についても説明します。

ControllerへのVDA登録

VDAがアプリケーションとデスクトップの配信を支援するには、Controllerに登録（通信を確立）する必要があります。Controllerのアドレスはいくつかの方法で指定でき、それについてはこの記事で説明します。サイトでControllerが追加、移動、削除される際に、VDAが最新の情報を持っていることが重要です。

セッション

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。いくつかの機能により、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減できます。

- セッションの信頼性
- 自動クライアント再接続
- ICA®キープアライブ
- ワークスペースコントロール
- セッションローミング

Studioでの検索の使用

Studioでマシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示したい場合は、柔軟な検索機能を使用します。

タグ

タグを使用して、マシン、アプリケーション、グループ、ポリシーなどのアイテムを識別します。その後、特定のタグを持つアイテムに適用されるように特定の操作を調整できます。

IPv4/IPv6

Citrix Virtual Apps and Desktops は、純粋な IPv4、純粋な IPv6、および IPv4 と IPv6 のネットワークが重複するデュアルスタック展開をサポートしています。この記事では、これらの展開について説明し、図解します。また、IPv4 または IPv6 の使用を制御する Citrix ポリシー設定についても説明します。

ユーザープロファイル

デフォルトでは、VDA をインストールすると Citrix Profile Management が自動的にインストールされます。このプロファイルソリューションを使用する場合は、この記事で一般的な情報を確認してください。詳細については、Profile Management のドキュメントを参照してください。

Citrix Diagnostic Facility (CDF) トレースの収集

CDFControl ユーティリティは、さまざまな Citrix トレースプロバイダーから表示される Citrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑な Citrix 関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集のために作成されています。

シトリックス インサイト サービス

Citrix Insight Services (CIS) は、計測、テレメトリ、およびビジネスインサイト生成のための Citrix プラットフォームです。

シトリックス スカウト

Citrix Scout は、診断情報を収集し、ヘルスチェックを実行します。結果は、Citrix Virtual Apps and Desktops 展開におけるプロアクティブなメンテナンスに利用できます。Citrix は、Citrix Insight Services を通じて、診断コレクションの包括的な自動分析を提供します。また、Scout を使用して、単独で、または Citrix サポートのガイダンスを受けて問題をトラブルシューティングすることもできます。

アプリケーション

> **注：**
>
> Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb

> Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

展開でデリバリーグループのみを使用している場合（アプリケーショングループを使用していない場合）、アプリケーションをデリバリーグループに追加します。アプリケーショングループも使用している場合は、通常、代わりにアプリケーションをアプリケーショングループに追加します。このガイダンスにより、管理が容易になります。アプリケーションは常に、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。

アプリケーションの追加ウィザードでは、1つ以上のデリバリーグループ、または1つ以上のアプリケーショングループを選択できますが、両方を同時に選択することはできません。後でアプリケーションのグループ関連付けを変更できますが（たとえば、アプリケーションをアプリケーショングループからデリバリーグループに移動するなど）、ベストプラクティスとしては、そのような複雑さを追加することは推奨されません。アプリケーションは1種類のグループに保持してください。

アプリケーションを複数のグループに関連付けると、それらのすべてのグループでアプリケーションを表示する十分な権限がない場合、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが関連付けられているすべてのグループを含むようにスコープを拡張してください。

同じ名前の2つのアプリケーション（異なるグループからのものかもしれません）を同じユーザーに公開する場合、Web Studioで`Application name (for user)`プロパティを変更します。そうしないと、ユーザーはCitrix Workspace™アプリで重複する名前を目にすることになります。

アプリケーションのプロパティ（設定）は、追加時または後で変更できます。アプリケーションが配置されているアプリケーションフォルダーも、アプリケーションの追加時または後で変更できます。

詳細については、以下を参照してください。

- デリバリーグループの作成
- アプリケーショングループの作成
- タグ

アプリケーションの追加

デリバリーグループまたはアプリケーショングループを作成する際に、アプリケーションを追加できます。これらの手順は、デリバリーグループの作成およびアプリケーショングループの作成で詳しく説明されています。次の手順では、グループ作成後にアプリケーションを追加する方法について説明します。

注意点:

- Remote PC Accessデリバリーグループにアプリケーションを追加することはできません。
- アプリケーションの追加ウィザードを使用して、デリバリーグループまたはアプリケーショングループからアプリケーションを削除することはできません。これは別の操作です。

1つ以上のアプリケーションを追加するには：

1. 左ペインで**アプリケーション**を選択し、アクションバーで**アプリケーションの追加**を選択します。
2. アプリケーションの追加ウィザードが**はじめに**ページとともに起動します。このページは、今後のウィザードの起動時に表示しないように設定できます。
3. ウィザードは、**グループ**、**アプリケーション**、**概要**の各ページを案内します。各ページの作業が完了したら、**概要**ページに到達するまで**次へ**をクリックします。

単一のデリバリーグループまたはアプリケーショングループにアプリケーションを追加する場合の、手順1の代替方法:

- **1つのデリバリーグループにのみアプリケーションを追加する場合:** 手順1で、Web Studioの左ペインで**デリバリーグループ**を選択し、中央ペインでデリバリーグループを選択してから、アクションバーで**アプリケーションの追加**を選択します。この場合、ウィザードには**グループ**ページが表示されません。
- **1つのアプリケーショングループにのみアプリケーションを追加する場合:** 手順1で、Web Studioの左ペインで**アプリケーション**を選択し、中央ペインでアプリケーショングループを選択してから、アクションバーのアプリケーショングループ名の下にある**アプリケーションの追加**エントリを選択します。この場合、ウィザードには**グループ**ページが表示されません。

グループページ

このページには、サイト内のすべてのデリバリーグループが一覧表示されます。アプリケーショングループも作成している場合は、アプリケーショングループとデリバリーグループが一覧表示されます。どちらかのグループを選択できますが、両方のグループを同時に選択することはできません。つまり、アプリケーショングループとデリバリーグループに同時にアプリケーションを追加す

ることはできません。通常、アプリケーショングループを使用している場合は、デリバリーグループではなくアプリケーショングループにアプリケーションを追加します。

アプリケーションを追加するときは、少なくとも1つのデリバリーグループ（または、利用可能な場合はアプリケーショングループ）の横にあるチェックボックスを選択します。すべてのアプリケーションは、常に少なくとも1つのグループに関連付けられている必要があります。

アプリケーションページ

アプリケーションソースを表示するには、**追加**をクリックします。

- **スタートメニューから：** 選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、**OK**をクリックします。

  このソースは、(1)関連付けられたデリバリーグループがないアプリケーショングループを選択した場合、(2)関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループを選択した場合、または(3)マシンが含まれていないデリバリーグループを選択した場合には選択できません。

- **手動:** デリバリーグループ内のVDAまたはネットワーク上の別の場所にあるアプリケーション。このソースを選択すると、次の方法で追加するアプリケーションを指定する新しいページが開きます。

  - 実行可能ファイルのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
  - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、**参照**をクリックし、VDAにアクセスするための資格情報を入力し、VDAへの接続を待ってから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティは、ページのフィールドに自動的に入力されます。

- **既存:** 以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。

  サイトにアプリケーションがない場合、このソースは選択できません。

- **アプリケーションパッケージ:** App-V、MSIX、MSIX app attach、またはFlexAppアプリケーションパッケージ内のアプリケーション。このソースを選択すると、**パッケージからアプリケーションを追加**ページが起動します。アプリケーションパッケージソースを選択し、表示さ

れた結果から追加したいアプリケーションを選択し、**OK**を選択します。詳細については、「アプリパッケージの展開と配信」を参照してください。

- **アプリケーショングループ**: アプリケーショングループ。このソースを選択すると、アプリケーショングループのリストを含む新しいページが起動します。(表示には各グループ内のアプリケーションもリストされますが、個々のアプリケーションではなくグループのみを選択できます。) 選択したグループ内の現在および将来のすべてのアプリケーションが追加されます。追加するアプリケーショングループのチェックボックスを選択し、**OK**をクリックします。

  このソースは、(1)アプリケーショングループがない場合、または(2)選択したデリバリーグループがアプリケーショングループをサポートしていない場合 (たとえば、静的に割り当てられたマシンを持つデリバリーグループ) には選択できません。

表に示されているように、**追加**リストの一部のソースは、そのタイプの有効なソースがない場合は選択できません。互換性のないソース (たとえば、アプリケーショングループにアプリケーショングループを追加することはできません) はリストに含まれません。選択したグループに既に追加されているアプリケーションは選択できません。

このページまたは後で、アプリケーションのプロパティ（設定）を変更できます。

デフォルトでは、追加されたアプリケーションは`Applications`という名前のアプリケーションフォルダーに配置されます。このページまたは後でアプリケーションを変更できます。アプリケーションを追加しようとして、同じ名前のアプリケーションが同じフォルダーに存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提示された新しい名前を受け入れるか、拒否してアプリケーションの名前を変更するか、別のフォルダーを選択できます。たとえば、**アプリケーション**フォルダーに`app`が既に存在し、そのフォルダーに`app`という名前の別のアプリケーションを追加しようとすると、新しい名前`app_1`が提示されます。

概要ページ

10個以下のアプリケーションを追加する場合、その名前は**追加するアプリケーション**にリストされます。10個を超えるアプリケーションを追加する場合、合計数が指定されます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーションのグループ関連付けを変更する

アプリケーションを追加した後、そのアプリケーションが関連付けられているデリバリーグループおよびアプリケーショングループを変更できます。

アプリケーションを別のグループにドラッグできます。これは、アクションバーのコマンドを使用する代替手段です。

アプリケーションが複数のデリバリーグループまたはアプリケーショングループに関連付けられている場合、グループの優先順位を使用して、複数のグループがアプリケーションを検索するためにチェックされる順序を指定できます。デフォルトでは、すべてのグループの優先順位は0（最高）です。同じ優先順位のグループは負荷分散されます。

アプリケーションは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。また、共有マシンを含むデリバリーグループがデスクトップのみを配信する場合でも、(1) デリバリーグループに共有マシンが含まれており、XenDesktop 7.xの7.9より前のバージョンで作成された場合、および (2) `Edit delivery group` 権限がある場合は、そのデリバリーグループを選択できます。プロパティダイアログがコミットされると、デリバリーグループの種類は自動的に `desktops and applications` に変換されます。

1. Web Studioにサインインし、左側のペインで**アプリケーション**を選択し、アプリケーションを選択します。
2. アクションバーで**プロパティ**を選択します。
3. **グループ**ページを選択します。
    - グループを追加するには、**追加**をクリックし、**アプリケーショングループ**または**デリバリーグループ**を選択します。（アプリケーショングループを作成していない場合、唯一の項目は**デリバリーグループ**です。）次に、利用可能なグループを1つ以上選択します。アプリケーションと互換性のないグループ、またはすでにアプリケーションに関連付けられているグループは選択できません。
    - グループを削除するには、1つ以上のグループを選択し、**削除**をクリックします。グループの関連付けを削除した結果、アプリケーションがどのグループにも関連付けられなくなる場合、アプリケーションが削除されることを警告されます。
    - グループの優先順位を変更するには、グループを選択し、**優先順位の編集**をクリックします。優先順位の値を選択し、**OK**をクリックします。
4. 完了したら、**適用**をクリックして変更を適用しウィンドウを開いたままにするか、**OK**をクリックして変更を適用しウィンドウを閉じます。

アプリケーションの複製、有効化または無効化、名前変更、または削除

次のアクションが利用可能です。

- **複製：** 異なるパラメーターやプロパティを持つ別のバージョンを作成するために、アプリケーションを複製したい場合があります。アプリケーションを複製すると、一意のサフィックスで自動的に名前が変更され、元のアプリケーションの隣に配置されます。アプリケーションを複

製してから、別のグループに追加したい場合もあります。（複製後、アプリケーションを移動する最も簡単な方法はドラッグすることです。）

- **有効化または無効化：** アプリケーションの有効化と無効化は、デリバリーグループまたはアプリケーショングループの有効化と無効化とは異なる操作です。
- **名前の変更：** 一度に1つのアプリケーションのみ名前を変更できます。アプリケーションの名前を変更しようとしたときに、同じ名前のアプリケーションが同じフォルダーまたはグループに存在する場合、別の名前を指定するように求められます。
- **削除：** アプリケーションを削除すると、関連付けられていたデリバリーグループおよびアプリケーショングループから削除されますが、元々アプリケーションを追加するために使用されたソースからは削除されません。アプリケーションの削除は、デリバリーグループまたはアプリケーショングループからアプリケーションを削除する操作とは異なります。

アプリケーションを複製、有効化、無効化、名前変更、または削除するには：

1. 左側のペインで を選択します。
2. 中央のペインで1つ以上のアプリケーションを選択し、アクションバーで適切なタスクを選択します。
3. プロンプトが表示されたら、操作を確定します。

デリバリーグループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている（属している）必要があります。アプリケーションをデリバリーグループから削除しようとしたときに、その操作によってアプリケーションとすべてのデリバリーグループまたはアプリケーショングループとの関連付けが解除される場合、続行するとアプリケーションが削除されることが通知されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左側のペインで を選択します。
2. デリバリーグループを選択します。中央下部のペインで、 タブの削除するアプリケーションを選択します。
3. アクションバーから を選択します。
4. 削除を確定します。

アプリケーショングループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。アプリケーションをアプリケーショングループから削除しようとしたと

きに、そのアプリケーションがどのグループにも属さなくなる場合、続行するとアプリケーションが削除されるという通知が表示されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左ペインで**アプリケーション**を選択します。
2. 中央ペインでアプリケーショングループを選択し、1つ以上のアプリケーションを選択します。
3. アクションバーで**アプリケーショングループから削除**を選択します。
4. 削除を確認します。

アプリケーションのプロパティを変更する

アプリケーションのプロパティは、一度に1つしか変更できません。

アプリケーションのプロパティを変更するには：

1. 左側のペインで を選択します。
2. アプリケーションを選択し、アクションバーで を選択します。
3. 変更するプロパティが含まれるページを選択します。
4. 完了したら、 をクリックして変更を適用し、ウィンドウを開いたままにするか、 をクリックして変更を適用してウィンドウを閉じます。

以下の一覧では、ページが括弧内に表示されています。

プロパティ	ページ
Citrix Workspaceアプリでアプリケーションが表示される分類または格納先	配信
コマンドライン引数。(#pass-parameters-to-published-applications)を参照してください。	場所
アプリケーションが利用可能なデリバリーグループおよびアプリケーショングループ	グループ
説明	識別
ファイル名拡張子とファイルの種類関連付け：アプリケーションが自動的に開く拡張子	ファイルの種類関連付け
アイコン	配信

プロパティ	ページ
StoreFront™ のキーワード	識別
制限。(#configure-application-limits)を参照してください。	配信
名前: ユーザーと管理者が参照する名前	識別
実行可能ファイルへのパス。「公開アプリケーションにパラメーターを渡す」(#pass-parameters-to-published-applications)を参照	場所
ユーザーのデスクトップ上のショートカット: 有効または無効	配信
可視性: Citrix Workspaceアプリでアプリケーションを表示できるユーザーを制限します。非表示のアプリケーションでも起動できます。利用不可かつ非表示にするには、別のグループに追加します。	可視性の制限
作業ディレクトリ	場所

アプリケーションの変更は、現在のアプリケーションユーザーがセッションからログオフするまで有効にならない場合があります。

アプリケーション制限を構成する

アプリケーションの使用状況を管理するために、アプリケーション制限を構成します。たとえば、アプリケーション制限を使用して、アプリケーションに同時にアクセスするユーザーの数を管理できます。同様に、アプリケーション制限は、リソースを大量に消費するアプリケーションの同時インスタンスの数を管理するためにも使用できます。この制限は、サーバーのパフォーマンスを維持し、サービスの劣化を防ぐのに役立ちます。

この機能は、Controller によって仲介されるアプリケーションの起動数（Citrix Workspace アプリや StoreFront からの起動など）を制限するものであり、他の方法で起動できる実行中のアプリケーションの数を制限するものではありません。これは、アプリケーション制限が同時使用を管理する際に管理者を支援するものの、すべてのシナリオで強制力を持つわけではないことを意味します。たとえば、Controller が停止モードの場合、アプリケーション制限は適用できません。

デフォルトでは、同時に実行できるアプリケーションインスタンスの数に制限はありません。アプリケーションの制限設定はいくつかあります。それらのいずれか、またはすべてを構成できます。

- デリバリーグループ内のすべてのユーザーによる、アプリケーションの同時実行インスタンスの最大数。
- デリバリーグループ内のユーザーごとのアプリケーションインスタンス数。
- マシンごとのアプリケーションの同時実行インスタンスの最大数（PowerShellのみ）。

制限が構成されている場合、ユーザーが構成された制限を超えるアプリケーションインスタンスを起動しようとすると、エラーメッセージが生成されます。複数の制限が構成されている場合、最初に制限に達したときにエラーが報告されます。

アプリケーション制限の使用例：

- **同時実行インスタンスの最大数制限:** デリバリーグループで、アプリケーション `Alpha` の同時実行インスタンスの最大数を15に構成します。その後、そのデリバリーグループのユーザーは、そのアプリケーションの15インスタンスを同時に実行しています。そのデリバリーグループのいずれかのユーザーが `Alpha` を起動しようとすると、エラーメッセージが生成されます。構成された同時アプリケーションインスタンス制限（15）を超えるため、`Alpha` は起動されません。
- **ユーザーごとのインスタンス数制限:** 別のデリバリーグループで、アプリケーション `Beta` のユーザーごとのインスタンス数オプションを有効にします。ユーザーのTonyはアプリケーション `Beta` を正常に起動します。その日の後半、そのアプリケーションがTonyのセッションでまだ実行されている間に、彼は `Beta` の別のインスタンスを起動しようとします。エラーメッセージが生成され、ユーザーごとのインスタンス数制限を超えるため、`Beta` は起動されません。
- **同時実行インスタンスの最大数とユーザーごとのインスタンス数制限:** 別のデリバリーグループで、同時実行インスタンスの最大数を10に構成し、アプリケーション `Delta` のユーザーごとのインスタンス数オプションを有効にします。その後、そのデリバリーグループの10人のユーザーがそれぞれ `Delta` のインスタンスを実行している場合、そのデリバリーグループの他のユーザーが `Delta` を起動しようとすると、エラーメッセージが表示されます。`Delta` は起動されません。現在の10人の `Delta` ユーザーのいずれかがそのアプリケーションの2番目のインスタンスを起動しようとすると、エラーメッセージが表示され、2番目のインスタンスは起動されません。
- **マシンごとの同時実行インスタンスの最大数とタグ制限の使用:** アプリケーション `Charlie` には、特定のサーバーで同時に実行できるインスタンスの数を規定するライセンスおよびパ

フォーマンス要件があります。これらの要件は、サイト内のすべてのサーバーで同時に実行できるインスタンスの数も規定します。

アプリケーションのインスタンス数/マシン制限は、サイト内の任意のサーバーに影響します（特定のデリバリーグループ内のマシンだけでなく）。サイトに3台のサーバーがあるとします。アプリケーション `Charlie` の場合、マシンごとのアプリインスタンス制限を2に構成します。したがって、サイト全体でアプリケーション `Charlie` のインスタンスは6つまでしか起動できません。（これは、3台のサーバーそれぞれでCharlieのインスタンスが2つという制限です。）

デリバリーグループ内の特定のコンピューターのみにアプリケーションの使用を制限するには（サイト全体のすべてのコンピューターでのインスタンス制限に加えて）：

- それらのマシンにタグ付け機能を使用します。
- そのアプリケーションのマシンごとのインスタンス数制限を構成します。

アプリケーションがControllerの仲介以外の方法（たとえば、Controllerが停止モードの場合など）で起動され、構成された制限を超過した場合、ユーザーは制限を超過しないように十分なインスタンスを閉じるまで、それ以上のインスタンスを起動できません。制限を超過したインスタンスは強制的にシャットダウンされません。ユーザーがそれらを閉じるまで、実行が許可されます。

セッションローミングを無効にする場合は、ユーザーごとのアプリケーションインスタンス数制限を無効にします。ユーザーごとのアプリケーションインスタンス数制限を有効にする場合は、新しいデバイスでの新しいセッションを許可する2つの値のいずれも構成しないでください。ローミングについて詳しくは、「セッション」を参照してください。

デリバリーグループごとの最大インスタンス数制限と、ユーザーごとのインスタンス数制限を構成するには：

1. 左側のペインで **［アプリケーション］** を選択し、アプリケーションを選択します。
2. アクションバーで **［アプリケーションプロパティの編集］** を選択します。
3. **［配信］** ページで、次のいずれかのオプションを選択します。

   - **［アプリケーションの無制限の使用を許可する］**。同時に実行できるインスタンスの数に制限はありません。これがデフォルトです。
   - **［アプリケーションの制限を設定する］**。制限の種類は2つあります。いずれか一方または両方を指定します。

     - マシンごとに同時に実行できるインスタンスの最大数を指定します
     - ユーザーごとにアプリケーションのインスタンスを1つに制限する

4. ［**OK**］ をクリックして変更を適用し、ダイアログボックスを閉じます。または、 ［**適用**］ をクリックして変更を適用し、ダイアログボックスを開いたままにします。

マシンごとの最大インスタンス数制限を構成するには（PowerShellのみ）：

- PowerShellで（Citrix Cloud™展開の場合はRemote PowerShell SDKを、オンプレミス展開の場合はPowerShell SDKを使用して）、適切な `BrokerApplication` コマンドレットを `MaxPerMachineInstances` パラメーターとともに実行します。
- ガイダンスについては、`Get-Help` コマンドレットを使用してください。例：

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

公開アプリケーションにパラメーターを渡す

アプリケーションのプロパティの**場所**ページを使用して、コマンドラインを入力し、公開アプリケーションにパラメーターを渡します。

公開アプリケーションをファイルの種類に関連付けると、`"%*"` (二重引用符で囲まれたパーセント記号とアスタリスク記号) がアプリケーションのコマンドラインの末尾に追加されます。これらの記号は、ユーザーデバイスに渡されるパラメーターのプレースホルダーとして機能します。

公開アプリケーションが期待どおりに起動しない場合は、そのコマンドラインに正しい記号が含まれていることを確認してください。デフォルトでは、`"%*"` 記号が追加されると、ユーザーデバイスから提供されるパラメーターが検証されます。ユーザーデバイスから提供されるカスタマイズされたパラメーターを使用する公開アプリケーションの場合、コマンドライン検証をバイパスするために、`"%**"` 記号がコマンドラインに追加されます。アプリケーションのコマンドラインにこれらの記号が表示されない場合は、手動で追加してください。

実行可能ファイルへのパスにスペースを含むディレクトリ名が含まれている場合 (`"C:\Program Files"` など)、スペースがコマンドラインの一部であることを示すために、アプリケーションのコマンドラインを二重引用符で囲みます。これを行うには、パスを二重引用符で囲み、`%*` 記号を別の二重引用符で囲みます。パスの閉じ引用符と `%*` 記号の開き引用符の間にスペースを含めるようにしてください。

たとえば、公開アプリケーションであるWindows Media Playerのコマンドラインは次のとおりです。

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **注:**

> 公開アプリケーションを起動するためのコマンドラインの最大文字数 (引数を含む) は203文字です。

アプリケーションフォルダーの管理

デフォルトでは、デリバリーグループに追加する新しいアプリケーションは、**Applications**という名前のフォルダーに配置されます。デリバリーグループの作成時、アプリケーションの追加時、または後で別のフォルダーを指定できます。

知っておくと良いこと:

- Applicationsフォルダーの名前を変更したり削除したりすることはできませんが、その中に含まれるすべてのアプリケーションを、作成した他のフォルダーに移動することはできます。
- フォルダー名には1～64文字を含めることができます。スペースも使用できます。
- フォルダーは最大5レベルまでネストできます。
- フォルダーにアプリケーションが含まれている必要はありません。空のフォルダーも許可されます。
- フォルダは、移動するか、作成時に別の場所を指定しない限り、Web Studioでアルファベット順に表示されます。
- 各フォルダに異なる親フォルダがある限り、同じ名前のフォルダを複数持つことができます。同様に、各アプリケーションが異なるフォルダにある限り、同じ名前のアプリケーションを複数持つことができます。
- フォルダ内のアプリケーションを表示するには`View Applications`権限が必要です。また、アプリケーションを含むフォルダを削除、名前変更、または削除するには、そのフォルダ内のすべてのアプリケーションに対して`Edit Application Properties`権限が必要です。
- 以下のほとんどの手順では、Web Studioのアクションバーを使用してアクションを要求します。または、右クリックメニューを使用するか、項目をドラッグすることもできます。たとえば、意図しない場所にフォルダを作成または移動した場合、ドラッグアンドドロップで正しい場所に移動できます。

アプリケーションフォルダーを管理するには、左ペインで**アプリケーション**を選択します。以下のリストを参考にしてください。

- **すべてのフォルダを表示するには（ネストされたフォルダを除く）：** フォルダリストの上にある**Show all**をクリックします。

- **最上位レベルにフォルダを作成するには（ネストしない）：** **Applications**フォルダを選択します。新しいフォルダを**Applications**以外の既存のフォルダの下に配置するには、そのフォルダを選択します。次に、アクションバーで**Create Folder**を選択します。名前を入力します。
- **フォルダを移動するには：** フォルダを選択し、アクションバーで**Move Folder**を選択します。ネストされたフォルダが含まれていない限り、一度に1つのフォルダしか移動できません。（フォルダを移動する最も簡単な方法は、ドラッグすることです。）
- **フォルダの名前を変更するには：** フォルダを選択し、アクションバーで**Rename Folder**を選択します。名前を入力します。
- **フォルダを削除するには：** フォルダを選択し、アクションバーで**Delete Folder**を選択します。アプリケーションや他のフォルダを含むフォルダを削除すると、それらのオブジェクトも削除されます。アプリケーションを削除すると、デリバリーグループからのアプリケーションの割り当てが削除されます。ただし、マシンからは削除されません。
- **アプリケーションをフォルダに移動するには：** 1つまたは複数のアプリケーションを選択します。次に、アクションバーで**Move Application**を選択します。フォルダを選択します。

デリバリーグループまたはアプリケーショングループを作成する際に、**Application**ページで追加するアプリケーションをフォルダに配置することもできます。デフォルトでは、追加されたアプリケーションは**Applications**フォルダに入ります。フォルダを選択または作成するには、**Change**をクリックします。

公開デスクトップでのアプリケーションのローカル起動を制御する

ユーザーが公開デスクトップ内から公開アプリケーションを起動するとき、そのアプリケーションがデスクトップセッション内で起動されるか、公開アプリケーションとして起動されるかを制御できます。Citrix Workspaceアプリは、VDA上のWindowsレジストリでアプリケーションのインストールパスを検索し、存在する場合はアプリケーションのローカルインスタンスを起動します。それ以外の場合は、ホストされたアプリケーションのインスタンスが起動されます。VDAにインストールされていないアプリケーションを起動すると、ホストされたアプリケーションが起動されます。詳細については、「vPrefer launch」を参照してください。

PowerShell（Citrix Cloud展開環境ではRemote PowerShell SDK、オンプレミス展開環境ではPowerShell SDKを使用）で、このアクションを変更できます。

「`New-Broker`アプリケーション」または「`Set-BrokerApplication`コマンドレット」で、`LocalLaunchDisabled`オプションを使用します。例：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

デフォルトでは、このオプションの値はfalse（`-LocalLaunchDisabled $false`）です。公開デスクトップ内から公開アプリケーションを起動すると、そのデスクトップセッション内でアプリケーションが起動されます。

オプションの値をtrue (`-LocalLaunchDisabled $true`) に設定すると、公開アプリケーションが起動されます。これにより、公開デスクトップから公開アプリケーションへの個別の追加セッションが作成されます（Windows向けCitrix Workspaceアプリを使用）。

要件と制限：

- アプリケーションの`ApplicationType`の値は`HostedOnDesktop`である必要があります。
- このオプションは、適切なPowerShell SDKを介してのみ利用可能です。現在、Web Studioのグラフィカルインターフェイスでは利用できません。
- このオプションには、StoreFront 3.14、Windows向けCitrix Receiver 4.11、およびDelivery Controller 7.17が最低限必要です。

アプリパッケージ

> **注:**
>
> Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

Microsoftは、ユーザーにアプリケーションを配信するための3つのパッケージングテクノロジーを提供しています：App-V、MSIX、およびMSIX app attachです。この記事では、**Web Studio > アプリケーションパッケージ**を使用してこれらのパッケージ化されたアプリケーションを展開および配信する方法について説明します。

- App-Vアプリケーションの展開と配信
- MSIXおよびMSIX app attachアプリケーションの展開と配信

App-Vアプリケーションの展開と配信

このセクションでは、以下の情報について説明します。

- 概要。App-Vパッケージを配信および管理するための管理方法について説明します。

- 手順。これらのパッケージを展開および配信するための手順を説明します。

概要

このセクションでは、App-Vパッケージを配信および管理するための管理方法について説明します。App-Vパッケージアプリケーションを配信する際に操作するコンポーネントと概念の詳細については、Microsoftのドキュメントを参照してください: `<https://docs.microsoft.com/ja-jp/windows/application-management/app-v/appv-for-windows>`。

App-Vパッケージを配信および管理するには、以下の方法を使用できます。

- **Dual Admin**。アプリケーションパッケージはApp-Vサーバーで構成および管理されます。Citrix Virtual Apps and DesktopsとApp-Vサーバーが連携してパッケージを配信および管理します。

  この方法では、Citrix Virtual Apps and DesktopsがApp-Vサーバーの状態のスナップショットビューを定期的に更新する必要があります。これには、ハードウェア、インフラストラクチャ、および管理のオーバーヘッドが発生します。Citrix Virtual Apps and DesktopsとApp-Vサーバーは、特にユーザー権限に関して同期を維持する必要があります。

  デュアル管理は、App-Vと環境が密接に連携している展開環境で最適に機能します。

  - **App-V管理サーバー**。App-Vパッケージと動的構成ファイルのライフサイクルを公開および管理します。
  - **Citrix Personalizationコンポーネント**。VDAマシンにインストールされます。アプリケーションの起動に必要な適切なApp-V公開サーバーの登録を管理します。

  この方法により、App-V公開サーバーが適切なタイミングでユーザーと同期されます。公開サーバーは、ログオン時の更新や接続グループなど、パッケージライフサイクルの他の側面を維持します。
- **シングル管理**。アプリケーションパッケージはネットワーク共有に保存されます。Citrix Virtual Apps and Desktopsは、パッケージを個別に配信および管理します。

  この方法では、展開環境でApp-Vサーバーとデータベースインフラストラクチャが不要になるため、オーバーヘッドが削減されます。

  この方法では、App-Vパッケージをネットワーク共有に保存し、その場所からメタデータを環境にアップロードします。VDAマシンにインストールされているCitrix Personalizationコンポーネントは、次のようにアプリケーションを管理および配信します。

  - アプリケーションが起動されたときに、展開構成ファイルとユーザー構成ファイルを処理します。

- ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。

両方の管理方法を同時に使用できます。つまり、デリバリーグループにアプリケーションを追加すると、アプリケーションはApp-Vサーバーまたはネットワーク共有に存在するApp-Vパッケージから取得できます。

> **注:**
>
> 両方の管理方法を同時に使用していて、App-Vパッケージが両方の場所に動的構成ファイルを持っている場合、App-Vサーバー上のファイル（デュアル管理）が使用されます。

手順

App-V アプリケーションの配信をサポートするには、VDA マシンに Citrix Personalization コンポーネントをインストールする必要があります。詳細については、「VDA マシンへの Citrix Personalization コンポーネントのインストール」を参照してください。

App-V パッケージ化されたアプリケーションをユーザーに配信するには、次の手順に従います。

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. アプリケーションをデリバリーグループに追加する。
4. 相互依存するApp-Vパッケージの自動配信を有効にするには、分離グループを作成します。

シングル管理者方式で Citrix Virtual Apps and Desktops が App-V 動的構成ファイルを認識して適用するようにするには、このCitrix ブログを参照してください。

MSIX および MSIX app attach アプリケーションの展開と配信

このセクションでは、次の情報について説明します。

- 概要(#overview-1)。MSIXおよびMSIX app attachパッケージがどのように配信および管理されるかについて説明します。
- 手順(#procedures-1)。これらのパッケージを展開および配信するための手順を説明します。

概要

Citrix Virtual Apps and Desktopsは、VDAマシンにインストールされているCitrix Personalizationコンポーネントを介して、MSIXおよびMSIX app attachアプリケーションをユーザーに配信します。

このコンポーネントは、ホストマシン上のパッケージのライフサイクルに関するすべての側面を管理します。

MSIXおよびMSIX app attachの詳細については、Microsoftのドキュメント（`<https://docs.microsoft.com/ja-jp/windows/msix/>`および`<https://docs.microsoft.com/ja-jp/azure/virtual-desktop/what-is-app-attach>`）をそれぞれ参照してください。

手順

MSIXおよびMSIX app attachパッケージの配信をサポートするには、VDAマシンにCitrix Personalizationコンポーネントをインストールする必要があります。詳細については、「VDAマシンにCitrix Personalizationコンポーネントをインストールする」を参照してください(#install-the-citrix-personalization-component-on-vda-machines)。

MSIXおよびMSIX app attachパッケージ化されたアプリケーションをユーザーに配信するには、次の手順に従います。

1. ネットワーク共有にアプリケーションパッケージを格納する(#store-application-packages-on-network-shares)。
2. アプリケーションパッケージを環境にアップロードする(#upload-application-packages-into-your-environment)。
3. アプリケーションをデリバリーグループに追加する(#add-applications-to-delivery-groups)。

VDAマシンにCitrix Personalizationコンポーネントをインストールする

Citrix Personalizationコンポーネントは、App-V、MSIX、およびMSIX app attach形式のアプリケーションパッケージの公開プロセスを管理します。このコンポーネントは、VDAをインストールする際にデフォルトではインストールされません。コンポーネントはVDAのインストール中またはインストール後にインストールできます。

VDAのインストール中にコンポーネントをインストールするには、次のいずれかの方法を使用します。

- インストールウィザードで、**Additional Components**ページに移動し、**Citrix Personalization for App-V - VDA**チェックボックスを選択します。
- コマンドラインインターフェイスで、**/includeadditional "Citrix Personalization for App-V – VDA"**オプションを使用します。

VDAのインストール後にコンポーネントをインストールするには、次の手順に従います。

1. VDAマシンで、**コントロールパネル > プログラム > プログラムと機能**に移動し、**Citrix Virtual Delivery Agent**を右クリックして、**変更**を選択します。

2. 表示されるウィザードで、**Additional Components**ページに進み、**Citrix Personalization for App-V - VDA**チェックボックスを有効にします。

> **注:**
>
> Microsoft App-V Desktop Clientは、ユーザーデバイス上でApp-Vパッケージから仮想アプリケーションを実行するコンポーネントです。Windows 10 (1607以降)、Windows Server 2016、およびWindows Server 2019には、このApp-Vクライアントソフトウェアがすでに含まれています。VDAマシンでこれを有効にするだけで済みます。詳細については、次のMicrosoftドキュメント記事を参照してください: `<https://docs.microsoft.com/ja-jp/windows/application-management/app-v/appv-enable-the-app-v-desktop-client>`。

ネットワーク共有にアプリケーションパッケージを格納する

インフラストラクチャをセットアップした後、アプリケーションパッケージを生成し、UNCまたはSMBネットワーク共有、あるいはAzureファイル共有などのネットワークロケーションに格納します。

詳細な手順は次のとおりです。

1. アプリケーションパッケージを生成します。詳細については、Microsoftのドキュメントを参照してください。
2. アプリケーションパッケージをネットワークロケーションに保存します。
   - **App-V Single Admin**の場合：パッケージと対応する動的構成ファイル（App-V）をUNCまたはSMBネットワーク共有、またはAzureファイル共有に保存します。
   - **App-V Dual Admin**の場合：UNCパスからApp-V管理サーバーにパッケージを公開します。（HTTP URLからの公開はサポートされていません。）
   - **MSIXまたはMSIX app attach**の場合：パッケージをUNCまたはSMBネットワーク共有、またはAzureファイル共有に保存します。
3. VDAがパッケージ保存パスに対する読み取り権限を持っていることを確認してください。
   - ADドメイン内のUNCまたはSMBネットワーク共有にパッケージを保存する場合は、VDAマシンにストレージパスへの読み取り権限を付与します。これを行うには、マシンのADアカウントに共有への読み取り権限を明示的に付与するか、その権限を持つADグループにアカウントを含めます。

- Azureファイル共有にパッケージを保存する場合、まずAzureのストレージパスに対する読み取り権限をユーザーアカウントに付与します。次に、VDAマシンで実行されている `ctxAppVService` を、そのユーザーアカウントを使用してパッケージストレージパスにアクセスするように構成します。詳細な手順については、次のセクションを参照してください。

ユーザーログオンアカウントの変更

VDAは `ctxAppVService` を呼び出してパッケージストレージパスにアクセスします。デフォルトでは、 `ctxAppVService` はマシンの**ローカルシステムアカウント**を使用してパッケージストレージパスにアクセスします。このタイプのマシン認証はADドメインで機能します。ただし、ユーザーアカウントベースの認証が必要なADとAzure ADの統合シナリオでは機能しません。

Azureファイル共有にパッケージを保存する場合、 `ctxAppVService` のログオンアカウントを、パッケージストレージパスに対する読み取り権限を持つユーザーアカウントに変更します。詳細な手順は次のとおりです。

1. **サービス**を開始し、**ctxAppVService**を右クリックし、**プロパティ**を選択します。
2. **［ログオン］タブで、［このアカウント］**を選択し、パッケージストレージパスへの読み取り権限を持つユーザーアカウントを入力し、ユーザーのパスワードを2回入力します。
3. **OK**をクリックします。

アプリケーションパッケージを環境にアップロードする

必要に応じてアプリケーションパッケージをネットワークの場所に保存した後、配信のために環境にアップロードします。必要に応じて、次のいずれかの方法を使用します。

- 一括アップロード
- 個別にアップロード

準備

Citrix Virtual Apps and Desktopsは、パッケージ検出のためにネットワークの場所への接続を設定するためにVDAマシンを使用します。したがって、事前にデリバリーグループを作成し、グループ内の少なくとも1つのVDAが次の要件を満たしていることを確認してください。

- VDAバージョン:
  - App-Vパッケージを検出する場合: 2203以降
  - MSIXおよびMSIX app attachパッケージを検出する場合: 2209以降
- Citrix Personalization for App-Vコンポーネント: インストール済み

- パッケージの場所に対する権限: 読み取り (詳細については、手順2: ネットワーク共有にアプリケーションパッケージを保存するを参照してください。)
- 電源: オン
- 状態: 登録済み

アプリケーションパッケージを一括でアップロードする

ネットワークの場所にあるパッケージを環境にアップロードします。アップロードする前に、次の項目を準備してください。

- (#preparations) の要件を満たすデリバリーグループ
- ネットワークの場所のパス

パッケージを一括でアップロードするには、次の手順に従います。

1. 左側のペインで、**App Packages** を選択します。
2. **ソース**タブで、**ソースの追加**ボタンをクリックします。**ソースの追加**ページが表示されます。
3. **名前**フィールドに、パッケージソースのわかりやすい名前を入力します。
4. **デリバリーグループ**フィールドで、**デリバリーグループの選択**をクリックします。次に、準備に記載されている要件を満たすデリバリーグループを選択し、**OK**をクリックします。
5. **場所の種類**フィールドで、パッケージの保存場所に応じて、**Microsoft App-Vサーバー**または**ネットワーク共有**を選択し、次に、対応する設定を完了します。
    - **Microsoft App-Vサーバー**を選択した場合は、次の情報を入力します。
        - 管理サーバーのURL。例：`http://appv-server.example.com`
        - 管理サーバー管理者のログイン資格情報。
        - 公開サーバーのURLとポート番号。例：`http://appv-server.example.com:3330`
    - **ネットワーク共有**を選択した場合は、次の情報を指定します。
        - ネットワーク共有のUNCパスを入力します。例：`\\Package-Server\apps\`
        - アップロードするパッケージの種類を選択します。オプションには、App-V、MSIX、およびMSIX app attachが含まれます。
        - パッケージのサブフォルダーを検索するかどうかを指定します。
6. **ソースの追加**をクリックします。

ソースの追加ページが閉じ、新しく追加されたソースがソースリストに表示されます。Citrix Virtual Apps and Desktops は、デリバリーグループ内の VDA を使用してパッケージを環境にアップロードします。アップロードが完了すると、ステータスフィールドに「*インポート成功*」と表示されます。対応するパッケージは、**パッケージ**タブに表示されます。

> **注:**
>
> ソースの場所でパッケージの更新を確認し、環境にインポートするには、ソースリストで場所を選択し、**パッケージの更新を確認**をクリックします。

アプリケーションパッケージを個別にアップロードする

ネットワーク共有から環境にアプリケーションパッケージをアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- (#preparations) で述べられている要件を満たすデリバリーグループ
- ネットワークの場所のパス。

パッケージを環境にアップロードするには、次の手順に従います。

1. 左側のペインで、**アプリパッケージ**を選択します。
2. **パッケージ**タブで、**パッケージの追加**ボタンをクリックします。**パッケージの追加**ページが表示されます。
3. **デリバリーグループ**フィールドで、**デリバリーグループの選択**をクリックします。次に、準備に記載されている要件を満たすデリバリーグループを選択し、**OK**をクリックします。
4. **パッケージの完全パス**フィールドに、必要に応じてパスを入力します。
   - 複数のパッケージを一度にアップロードするには、セミコロン (`;`) で区切って完全パスを入力します。例：`\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - ネットワーク共有に存在するすべてのパッケージをアップロードするには、ストレージパスを入力します。例: \\package-Server\apps\
5. **パッケージの追加**をクリックします。

   アプリケーションパッケージが**パッケージ**タブに表示されます。

アプリケーションをデリバリーグループに追加する

アプリケーションパッケージが完全にアップロードされたら、必要に応じてそのアプリケーションを1つ以上のデリバリーグループに追加します。その結果、それらのデリバリーグループに関連付けられたユーザーはアプリケーションにアクセスできるようになります。

パッケージ内の1つ以上のアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左ペインで、**アプリパッケージ**を選択します。
2. **パッケージ**タブで、必要に応じてパッケージを選択します。
3. アクションバーで、**デリバリーグループの追加**をクリックします。「デリバリーグループの追加」ページが表示されます。
4. 必要に応じてパッケージ内の1つ以上のアプリケーションを選択し、**次へ**をクリックします。*アプリケーション*配信タイプのデリバリーグループが表示されます。
5. デリバリーグループのリストで、アプリケーションを割り当てるグループを選択し、**次へ**をクリックします。 **注：**MSIXまたはMSIXアプリ添付パッケージを選択した場合、機能レベルが2106以降のデリバリーグループのみがリストに表示されます。
6. **完了**をクリックします。

パッケージ化されたアプリケーションは、次の場合にもデリバリーグループに追加できます。

- デリバリーグループを作成するとき。詳しくは、デリバリーグループの作成を参照してください。
- 既存のデリバリーグループまたはアプリケーショングループを編集するとき。詳しくは、アプリケーションの追加を参照してください。

（オプション）App-Vパッケージの分離グループを作成する

相互依存するApp-Vパッケージを自動的に配信できるように、分離グループを作成できます。

> **注:**
>
> 分離グループは、App-Vシングル管理者方式でサポートされています。App-Vデュアル管理者方式を使用している場合は、Microsoft App-Vインフラストラクチャで*接続グループ*を作成することで、同じ目標を達成できます。詳細については、このMicrosoftドキュメント記事を参照してください: `<https://docs.microsoft.com/ja-jp/windows/application-management/app-v/appv-connection-group-file>`。

分離グループについて

分離グループは、仮想環境を作成するために同じWindowsサンドボックス内で実行する必要がある、相互依存するアプリケーションパッケージの集合です。Citrix App-V分離グループは、App-V接続グループと似ていますが、同一ではありません。分離グループには、次の2種類のパッケージが含まれます。

- **明示的**アプリケーションパッケージ。特定のライセンス要件を持つアプリケーション。これらのアプリケーションをデリバリーグループに追加することで、特定の範囲のユーザーに制限できます。
- **自動**アプリケーションパッケージ。デリバリーグループに追加されているかどうかに関係なく、常にすべてのユーザーが利用できるアプリケーション。

たとえば、アプリケーション`app-a`を実行するにはJRE 1.7が必要です。app-a（*明示的*としてマーク）とJRE 1.7（*自動*としてマーク）を含む分離グループを作成できます。次に、`app-a`のApp-Vパッケージを1つ以上のデリバリーグループに追加します。ユーザーがapp-aを起動すると、JRE 1.7が自動的に展開されます。

ユーザーが分離グループ内で*明示的*としてマークされたApp-Vアプリケーションを起動すると、Citrix Virtual Apps and Desktopsはデリバリーグループ内のアプリケーションに対するユーザーのアクセス許可を確認します。ユーザーがアプリケーションにアクセスする権限を持っている場合、同じ分離グループ内の*自動*アプリケーションパッケージがユーザーに利用可能になります。

*自動*パッケージをデリバリーグループに追加する必要はありません。分離グループに別の*明示的*アプリケーションパッケージがある場合、そのパッケージは同じデリバリーグループにある場合にのみユーザーが利用できます。

分離グループについて詳しくは、このCitrixブログを参照してください。

APP-V分離グループを作成する

分離グループを作成し、相互依存するアプリケーションパッケージを追加します。詳細な手順は次のとおりです。

1. **「分離グループ」**タブで、「分離グループの追加」**をクリックします。
2. 分離グループの名前と説明を入力します。環境内のすべてのアプリケーションパッケージが、**［利用可能なパッケージ］** の一覧に表示されます。
3. **「利用可能なパッケージ」**リストから、必要に応じてアプリケーションを選択し、右矢印をクリックします。選択したアプリケーションが**「分離グループ内のパッケージ」**リストに表示されます。
4. **「展開」**フィールドで、アプリケーションに対して**「明示的」**または**「自動」**を選択します。

5. さらにパッケージを追加するには、手順2～3を繰り返します。
6. リスト内のパッケージの順序を調整するには、上矢印または下矢印をクリックします。
7. 「**保存**」をクリックします。

> **注:**
>
> 隔離グループの構成により、VDA上にApp-V接続グループが作成されます。展開シナリオは複雑になる可能性があり、App-Vクライアントは一度に1つのアクティブな接続グループにのみ存在するパッケージをサポートします。同じパッケージを、同じデリバリーグループに追加される2つの異なる隔離グループに追加することは避けることをお勧めします。

パッケージ化されたアプリケーションをシングルセッションまたは共有デスクトップVDAに公開する

これで、App-V、MSIX、およびMSIXアプリのアタッチパッケージを、デリバリーグループを介してシングルセッションまたは共有デスクトップVDAセッションに直接配信できるようになりました。アプリケーションに設定されたアクセス許可に基づいて、サインイン時にデスクトップVDAでパッケージ化されたアプリケーションにアクセスできます。

利点

- サインイン時にVDAで利用可能であり、WorkspaceまたはStoreFrontを介してオンデマンドでステージングされないアプリケーション。
- パッケージ化されたアプリケーションにアクセスする際の起動時間の改善。
- パッケージ化されたアプリケーションのメンテナンスを、VDAのベースイメージとは別に、独立して容易にします。

考慮事項

- このオプションは、適切なPowerShell SDKを介してのみ、シングルセッションVDAで利用可能です。現在、Web Studioワークフローでは利用できません。共有デスクトップへの公開は、PowerShell SDKを使用するか、Web Studioワークフローを介した既存の方法で行うことができます。既存の手順の詳細については、「デリバリーグループへのアプリケーションの追加」を参照してください。
- アプリケーションはデリバリーグループの一部である必要があります。

始める前に

- パッケージ化されたアプリケーションが署名されており、ファイル共有またはUNCの場所に存在することを確認してください。詳細については、「ネットワーク共有へのアプリケーションパッケージの保存」を参照してください。
- VDAマシンにCitrix Personalizationコンポーネントをインストールします。

手順

パッケージ化されたアプリケーションをデスクトップVDAに配信するには、次の手順に従います。

1. Web Studioへのアプリケーションパッケージのインポート。
2. パッケージ化されたBrokerApplicationの公開。
3. Web Studioでのアプリケーションの可視性の制限。

Web Studioへのアプリケーションパッケージのインポート

1. Webブラウザを開きます。`https://<address of the server hosting Web Studio>/Citrix/Studio`を入力します。
2. デリバリーグループを作成します。詳細については、「デリバリーグループの作成」を参照してください。
3. アプリケーションパッケージをWeb Studioにインポートします。詳細については、「アプリケーションパッケージの一括アップロード」を参照してください。

BrokerApplicationでのパッケージ化されたアプリケーションの公開

マルチセッション（共有）VDAまたはシングルセッションアプリケーションVDAに公開する場合、公開手順は変更されません。詳細については、「デリバリーグループへのアプリケーションの追加」を参照してください。 シングルセッションデスクトップVDAに公開する場合は、次の手順を実行します。

Delivery Controller™上で、以下のPowerShellコマンドを実行します:

1. パッケージ内に存在するコマンドを取得するには：

   ```
   Import-Module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
   ```

   > **注:**

> この機能をサポートする`App-V package discovery module`のバージョンは、上記のパスにあるCitrix Virtual Apps and Desktops ISO（2311以降のバージョン）で見つけることができます。

2. 関連するデリバリーグループIDとパッケージ化されたアプリケーションIDを取得するには:

   `Get-BrokerDesktopGroup | Format-Table Uid, Name` `Get-AppLibAppVApplication | Format-Table Uid, Name`

3. パッケージを公開し、適切なBrokerMachineConfigurationを作成するには:

   `Publish-PackagedApplication -AppLibararyApplicationUid <AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>`

4. VDA上のBrokerエージェントに後で送信されるBroker構成を同期するには：

   `Update-DesktopGroupMachineConfigurations -DesktopGroupUid <DesktopGroup.Uid>`

> **注:**
>
> VDAからパッケージ化されたアプリケーションを公開または削除した後で、PowerShellコマンド`Update-DesktopGroupMachineConfigurations`を実行してください。

Web Studio でのアプリケーションの可視性を制限する

デフォルトでは、ユーザーはVDAを提供するデリバリーグループに割り当てられたすべてのパッケージ化されたアプリケーションをデスクトップセッションで利用できます。Web Studioで特定のユーザーまたはグループにアプリケーションの可視性を設定することにより、デスクトップVDA上のパッケージ化されたアプリケーションの可視性を制御できます。パッケージ化されたアプリケーションの可視性を管理するには、アプリケーションプロパティの変更を参照してください。

ユニバーサル Windows プラットフォームアプリ

ユニバーサル Windows プラットフォーム (UWP) アプリについては、以下の Microsoft ドキュメントを参照してください。

- ユニバーサル Windows プラットフォーム (UWP) アプリとは
- Windows パッケージマネージャー

要件と制限

Citrix Virtual Apps and Desktops™ は、以下の Windows マシン上の VDA で UWP アプリを使用することをサポートしています。

- Windows 10 以降のバージョン
- Windows Server 2016 以降のバージョン

VDA はバージョン 7.11 以降である必要があります。

UWP アプリを使用する場合、以下の Citrix Virtual Apps and Desktops の機能はサポートされていないか、制限されています。

- ファイルタイプの関連付けはサポートされていません。
- ローカルアプリアクセスはサポートされていません。
- 動的プレビュー: セッションで実行中のアプリが重なっている場合、プレビューにはデフォルトのアイコンが表示されます。動的プレビューに使用される Win32 API は、UWP アプリではサポートされていません。
- アクションセンターのリモート処理: UWP アプリは、セッション内のメッセージを表示するためにアクションセンターを使用できます。これらのメッセージは現在、ユーザーに表示するためにエンドポイントにリダイレクトされません。

同じサーバーから UWP アプリと非 UWP アプリを起動することはサポートされていません。代わりに、UWP アプリと非 UWP アプリを別々のデリバリーグループまたはアプリケーショングループに配置してください。

マシンにインストールされているすべてのUWPアプリが列挙されるため、Citrix®はWindowsストアへのユーザーアクセスを無効にすることを推奨します。これにより、あるユーザーがインストールしたUWPアプリが別のユーザーによってアクセスされるのを防ぎます。

サイドローディング中、UWPアプリはマシンにインストールされ、他のユーザーが使用できるようになります。別のユーザーがアプリを起動すると、そのアプリがインストールされ、OSはそのユーザーによって「インストール済み」であることを示すようにAppXデータベースを更新します。

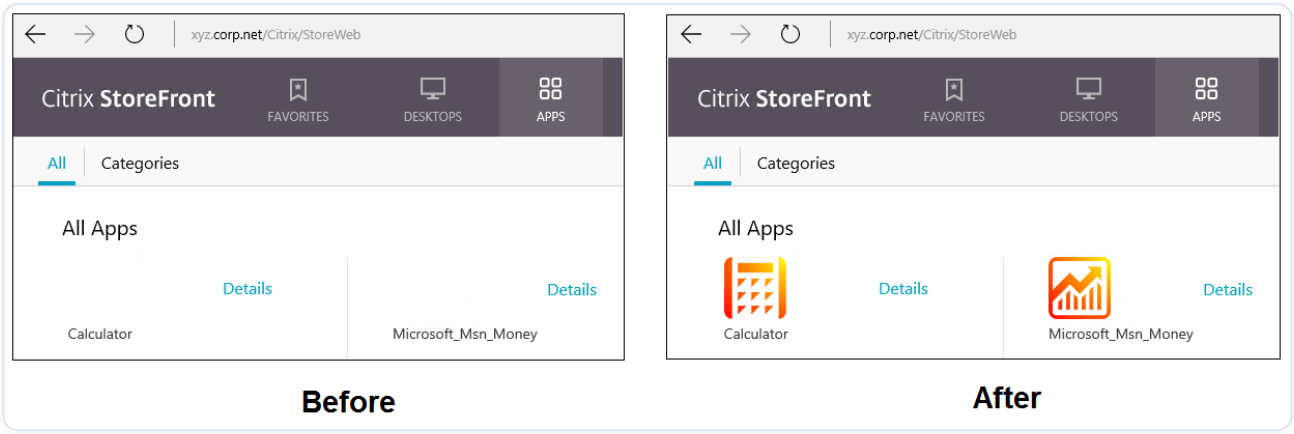
固定ウィンドウまたはシームレスウィンドウで起動された公開UWPアプリから開始された正常なログオフは、VDAセッションが閉じないようにし、ユーザーを強制的にログオフさせる可能性があります。この場合、VDAセッションに残っているいくつかのプロセスが、セッションが適切に閉じないようにします。これを解決するには、VDAセッションが閉じないようにしているプロセ

スを特定し、CTX891671のガイダンスに従って、「LogoffCheckSysModules」レジストリキー値に追加します。

UWPアプリのアプリケーション表示名と説明が正しくない場合があります。アプリケーションをデリバリーグループに追加する際に、これらのプロパティを編集して修正してください。

その他の問題については、(/ja-jp/citrix-virtual-apps-desktops/2311/whats-new/known-issues.html)を確認してください。

現在、いくつかのUWPアプリは透明度が有効な白いアイコンを持っており、StoreFrontの白い背景に対してアイコンが見えなくなることがあります。この問題を回避するには、背景を変更できます。たとえば、StoreFrontマシンでファイル`C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`を編集します。ファイルの最後に`.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`を追加します。次の図は、この例の変更前と変更後を示しています。



Windows Server 2016以降のバージョンでは、UWPアプリの起動時にサーバーマネージャーも起動する場合があります。これを防ぐには、`HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`レジストリキーを使用して、ログオン時のサーバーマネージャーの自動起動を無効にできます。詳細については、`<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`を参照してください。

UWPアプリのインストールと公開

UWPアプリのサポートはデフォルトで有効になっています。

VDA（またはマスターイメージ）に1つ以上のUWPアプリをインストールするには、次のいずれかの方法を使用します。

- Deployment Image Servicing and Management (DISM) などのツールを使用して、Windows Store for Business からオフラインインストールを完了し、アプリをデスクトップイメージに展開します。詳細については、Windows Package Managerを参照してください。
- アプリをサイドロードします。詳細については、Windows クライアント デバイスで業務基幹 (LOB) アプリをサイドロードするを参照してください。
- 各対象ユーザー向けに、Windows Store for Business から直接UWPアプリをインストールします。

Citrix Virtual AppsまたはCitrix Virtual Desktops™で1つ以上のUWPアプリを追加（公開）するには：

1. UWPアプリがマシンにインストールされた後、UWPアプリをデリバリーグループまたはアプリケーショングループに追加します。これは、グループの作成時または後で行うことができます。**アプリケーション**ページで、**追加**メニューから**スタートメニューから**を選択します。
2. アプリケーションリストが表示されたら、公開するUWPアプリを選択します。
3. ウィザードを続行するか、編集ダイアログを閉じます。

VDAでユニバーサルアプリの使用を無効にするには、レジストリ設定 **EnableUWASeamlessSupport**を `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` に追加し、**0**に設定します。

UWPアプリのアンインストール

`Remove-AppXPackage` のようなコマンドでUWPアプリをアンインストールすると、その項目は管理者に対してのみアンインストールされます。アプリを起動して使用した可能性のあるユーザーのマシンからアプリを削除するには、各マシンで削除コマンドを実行します。1つのコマンドですべてのユーザーのマシンからAppXパッケージをアンインストールすることはできません。

オートスケール™

Autoscaleは、マシンをプロアクティブに電源管理するための一貫性のある高性能なソリューションを提供する機能です。コストとユーザーエクスペリエンスのバランスを取ることを目的としています。

Autoscaleは、デリバリーグループ内の登録されているすべてのシングルセッションおよびマルチセッションOSマシンのプロアクティブな電源管理を可能にします。

Autoscaleの機能は次のとおりです。

- スケジュールベースおよび負荷ベースの設定(/ja-jp/citrix-virtual-apps-desktops/2311/manage-deployment/autoscale/schedule-based-and-load-based-settings.html)
- 動的セッションタイムアウト(/ja-jp/citrix-virtual-apps-desktops/2311/manage-deployment/autoscale/dynamic-session-timeout.html)
- Autoscaleタグ付きマシン（クラウドバースト）(/ja-jp/citrix-virtual-apps-desktops/2311/manage-deployment/autoscale/autoscale-tagged-machines.html)
- ユーザーログオフ通知(/ja-jp/citrix-virtual-apps-desktops/2311/manage-deployment/autoscale/force-user-logoff.html)

サポートされているVDAホスティングプラットフォーム

Autoscaleは、Citrix Virtual Apps and Desktopsがサポートするすべてのプラットフォームをサポートしています。これには、XenServer、Amazon Web Services、Google Cloud Platform、Microsoft Azure Resource Manager、VMware vSphereなど、さまざまなインフラストラクチャプラットフォームが含まれます。サポートされているプラットフォームの完全なリストについては、Citrix Virtual Apps and Desktopsのシステム要件を参照してください。

> **注:**
>
> パブリッククラウドホスト接続をデプロイに追加する場合、Hybrid Rights Licenseが必要です。Hybrid Rights Licenseの詳細については、Transition and Trade-Up (TTU) with Hybrid Rightsを参照してください。ライセンスの追加については、サイトの作成を参照してください。

サポートされているワークロード

Autoscaleは、マルチセッションOSとシングルセッションOSの両方のデリバリーグループをサポートしています。注意すべきユーザーインターフェイスは3つあります。

- マルチセッションOSデリバリーグループ（旧RDSデリバリーグループ）用のAutoscaleユーザーインターフェイス
- シングルセッションOSランダム（プール型）デリバリーグループ（旧プール型VDIデリバリーグループ）用Autoscaleユーザーインターフェイス
- シングルセッションOS静的デリバリーグループ（旧静的VDIデリバリーグループ）用Autoscaleユーザーインターフェイス

さまざまなデリバリーグループのユーザーインターフェイスの詳細については、「Autoscaleユーザーインターフェイス」を参照してください。

利点

Autoscale機能には、次の利点があります。

- デリバリーグループ内のマシンの電源管理を行うための、単一で一貫したメカニズムを提供します。
- 負荷ベースまたはスケジュールベースの電源管理、あるいはその両方の組み合わせによってマシンの電源を管理することで、可用性を確保し、コストを制御します。
- コスト削減やキャパシティ使用率などのメトリックを監視し、通知を有効にするには、Directorを使用します。

2分間のビデオを見る

次のビデオでは、Autoscaleの概要を簡単に説明します。

<iframe src="https://www.youtube.com/embed/5yxERrFZQ68" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Autoscale™ の概要

Autoscaleはデリバリーグループレベルで動作します。設定したスケジュールに基づいて、デリバリーグループ内のマシンをプロアクティブに電源管理します。

Autoscale は、すべての種類のデリバリーグループに適用されます。

- シングルセッション静的OS
- シングルセッションランダムOS
- マルチセッションランダムOS

この記事では、Autoscale に関連する基本的な概念について説明し、デリバリーグループで Autoscale を有効にして構成する方法に関するガイダンスを提供します。

基本的な概念

開始する前に、Autoscale の以下の基本的な概念について学習してください。

- スケジュール
- キャパシティバッファ
- ロードインデックス

スケジュール

オートスケールは、お客様が設定したスケジュールに基づいて、デリバリーグループ内のマシンの電源をオン/オフします。

スケジュールには、各タイムスロットのアクティブなマシンの数と、ピーク時およびオフピーク時が定義されています。

スケジュール設定はデリバリーグループの種類によって異なります。詳細については、以下を参照してください。

- マルチセッションOSデリバリーグループ
- シングルセッションOSランダムデリバリーグループ
- シングルセッションOS静的デリバリーグループ

容量バッファ

キャパシティバッファは、動的な負荷増加に対応するために、現在の需要に予備容量を追加するために使用されます。留意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、キャパシティバッファは、ロードインデックスの観点からデリバリーグループの総容量のパーセンテージとして定義されます。
- シングルセッションOSデリバリーグループの場合、キャパシティバッファは、デリバリーグループ内のマシンの総数のパーセンテージとして定義されます。

ロードインデックス

> **重要:**
>
> ロードインデックスは、マルチセッションデリバリーグループにのみ適用されます。

> ロードインデックスメトリックは、マシンがユーザーログオン要求を受信する可能性を決定します。これは、同時ログオン、セッション、CPU、ディスク、メモリの使用量に対して構成された**Citrix Load Management policy**設定を使用して計算されます。

ロードインデックスは0から10,000の範囲です。デフォルトでは、マシンが250セッションをホストしている場合、完全にロードされていると見なされます。

- 数字の「0」はアンロードされたマシンを示します。ロードインデックス値が0のマシンは、ベースライン負荷にあります。

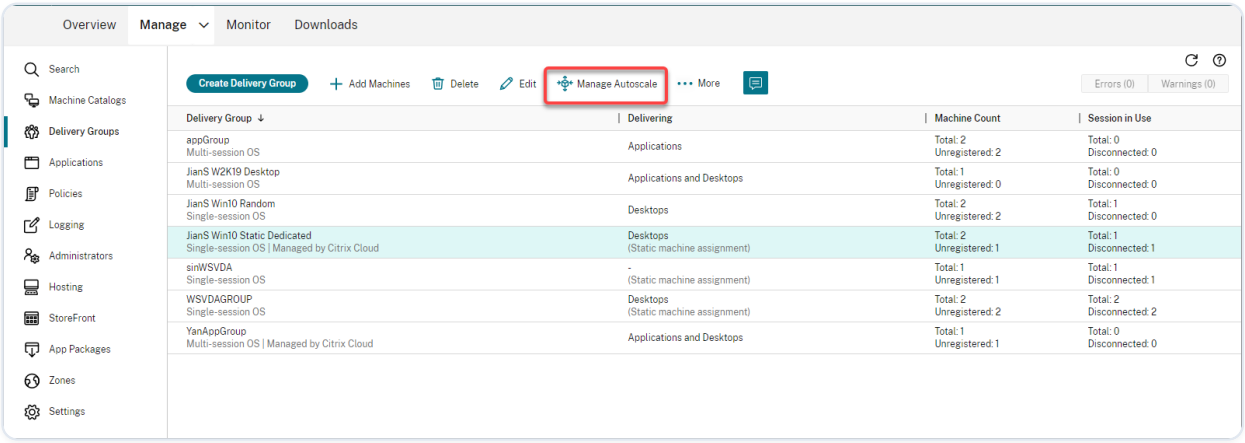
- 「10,000」は、これ以上セッションを実行できない完全にロードされたマシンを示します。

デリバリーグループのAutoscaleを有効にする

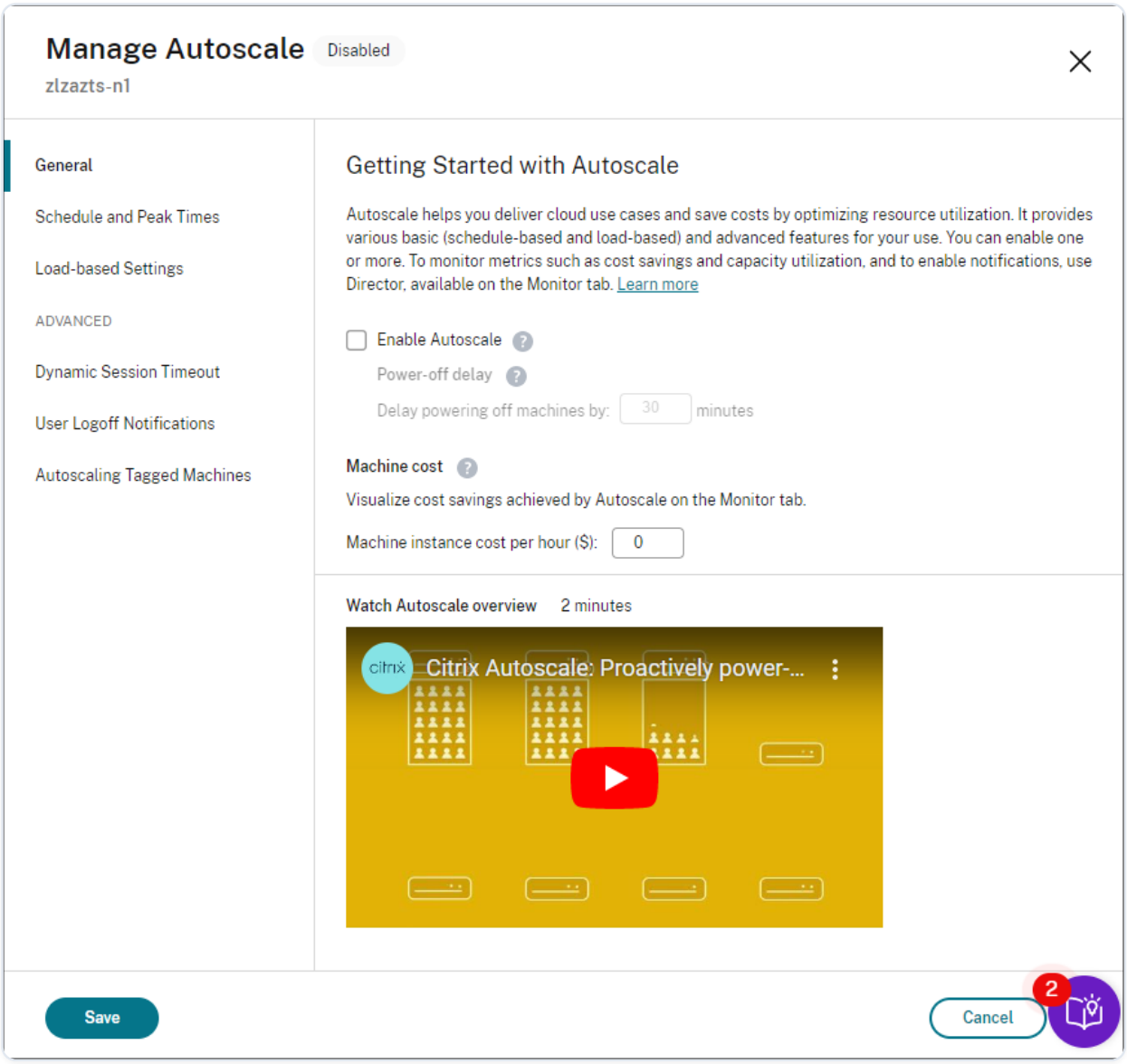
Autoscale は、デリバリーグループを作成するときにデフォルトで無効になっています。Web Studio を使用してデリバリーグループの Autoscale を有効にして構成するには、次の手順に従います。

PowerShell コマンドを使用して、デリバリーグループの Autoscale を有効にして構成することもできます。詳細については、Broker PowerShell SDK コマンド を参照してください。

1. 左側のペインで を選択します。
2. 管理するデリバリーグループを選択し、 をクリックします。



3. ページで、 チェックボックスをオンにして Autoscale を有効にします。Autoscale を有効にすると、ページ上のオプションが有効になります。



4. 組織のニーズに基づいてデフォルト設定を変更するには、次の設定を完了します。

   - スケジュールを設定する
   - 非アクティブなマシンをより効率的に電源オフにするには、動的セッションタイムアウト と ユーザーログオフ通知 を使用します。
   - デリバリーグループ内のマシンの一部を電源管理するには、タグ付きマシンのAutoscale を使用します。

Autoscale を無効にするには、 チェックボックスをオフにします。ページ上のオプションがグレー表示され、選択したデリバリーグループで Autoscale が無効になっていることを示します。

> **重要:**

- Autoscale を無効にすると、Autoscale によって管理されていたすべてのマシンは、無効化された時点の状態のままになります。
- Autoscale を無効にすると、ドレイン状態のマシンはドレイン状態から解除されます。ドレイン状態の詳細については、「ドレイン状態」を参照してください。

メトリックを監視する

デリバリーグループで Autoscale を有効にすると、Director から Autoscale で管理されているマシンの次のメトリックを監視できます。

- マシンの使用状況
- 推定節約額
- マシンとセッションのアラート通知
- マシンのステータス
- 負荷評価の傾向

注:

デリバリーグループで Autoscale を最初に有効にした場合、そのデリバリーグループの監視データが表示されるまでに数分かかることがあります。 Autoscale が有効になり、その後デリバリーグループで無効になった場合でも、監視データは引き続き利用できます。Autoscale は 5 分間隔で監視データを収集します。

メトリックの詳細については、「Autoscale で管理されているマシンを監視する」を参照してください。

知っておくと良いこと

Autoscale はデリバリーグループレベルで機能します。デリバリーグループごとに構成されます。選択したデリバリーグループ内のマシンのみを電源管理します。

容量とマシンの登録

Autoscale は、容量を決定する際に、サイトに登録されているマシンのみを含めます。登録されていない電源オンのマシンはセッション要求を受け入れることができません。その結果、それらはデリバリーグループの全体的な容量には含まれません。

複数のマシンカタログにわたるスケーリング

一部のサイトでは、複数のマシンカタログが単一のデリバリーグループに関連付けられている場合があります。Autoscaleは、スケジュールまたはセッションの需要要件を満たすために、各カタログからマシンをランダムに起動します。

たとえば、あるデリバリーグループに2つのマシンカタログがあるとします。カタログAには3台のマシンが起動しており、カタログBには1台のマシンが起動しています。Autoscaleが追加のマシンを起動する必要がある場合、カタログAまたはカタログBのいずれかのマシンを起動する可能性があります。

マシンのプロビジョニングとセッションの需要

デリバリーグループに関連付けられているマシンカタログには、需要の増減に応じて起動および停止するのに十分なマシンが必要です。セッションの需要がデリバリーグループ内の登録済みマシンの総数を超えた場合、Autoscaleはすべての登録済みマシンが起動していることを保証します。ただし、**Autoscaleは追加のマシンをプロビジョニングしません。**

インスタンスサイズの考慮事項

パブリッククラウドでインスタンスのサイズを適切に設定すると、コストを最適化できます。ワークロードのパフォーマンスと容量要件に合致する限り、より小さなインスタンスをプロビジョニングすることをお勧めします。

小さいインスタンスは、大きいインスタンスよりも少ないユーザーセッションをホストします。そのため、最後のユーザーセッションがログオフされるまでの時間が短いため、Autoscaleはマシンをより速くドレイン状態にします。結果として、Autoscaleは小さいインスタンスをより早くシャットダウンし、コストを削減します。

ドレイン状態

Autoscaleは、デリバリーグループ内の起動済みマシンの数を、構成されたプールサイズと容量バッファにまでスケールダウンしようとします。

この目標を達成するために、Autoscaleはセッション数が最も少ない余剰マシンを「ドレイン状態」にし、すべてのセッションがログオフされたときにそれらをシャットダウンします。この動作は、セッションの需要が減少し、スケジュールが起動しているマシンよりも少ないマシンを必要とする場合に発生します。

Autoscaleは余剰マシンを1台ずつ「ドレイン状態」にします。

- 2台以上のマシンが同じ数のアクティブセッションを持っている場合、Autoscaleは指定されたシャットダウン遅延時間起動していたマシンをドレインします。

そうすることで、最近起動されたマシンがドレイン状態になるのを避けることができます。なぜなら、それらのマシンはセッション数が最も少ない可能性が高いからです。

- 2台以上のマシンが指定されたシャットダウン遅延時間起動していた場合、Autoscaleはそれらのマシンをランダムに1台ずつドレインします。

ドレイン状態のマシンは新しいセッションの起動をホストしなくなり、既存のセッションがログオフされるのを待機しています。マシンは、すべてのセッションがログオフされた場合にのみシャットダウンの候補となります。ただし、セッション起動にすぐに利用できるマシンがない場合、Autoscaleは、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。

次のいずれかの条件が満たされた場合、マシンはドレイン状態から解除されます。

- マシンの電源がオフになる。
- マシンが属するデリバリーグループに対してAutoscaleが無効になっている。
- Autoscaleは、スケジュールまたは負荷需要の要件を満たすためにマシンを使用します。このケースは、スケジュール（スケジュールベースのスケーリング）または現在の需要（負荷ベースのスケーリング）が、現在電源がオンになっているマシンの数よりも多くのマシンを必要とする場合に発生します。

> **重要:**
>
> セッション起動にすぐに利用できるマシンがない場合、Autoscaleは、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。セッション起動をホストするドレイン状態のマシンは、ドレイン状態のままになります。

どのマシンがドレイン状態にあるかを確認するには、`Get-BrokerMachine` PowerShellコマンドを使用します。例: `Get-BrokerMachine -DrainingUntilShutdown $true`。または、管理コンソールを使用することもできます。「ドレイン状態のマシンを表示する」を参照してください。

ドレイン状態のマシンを表示する

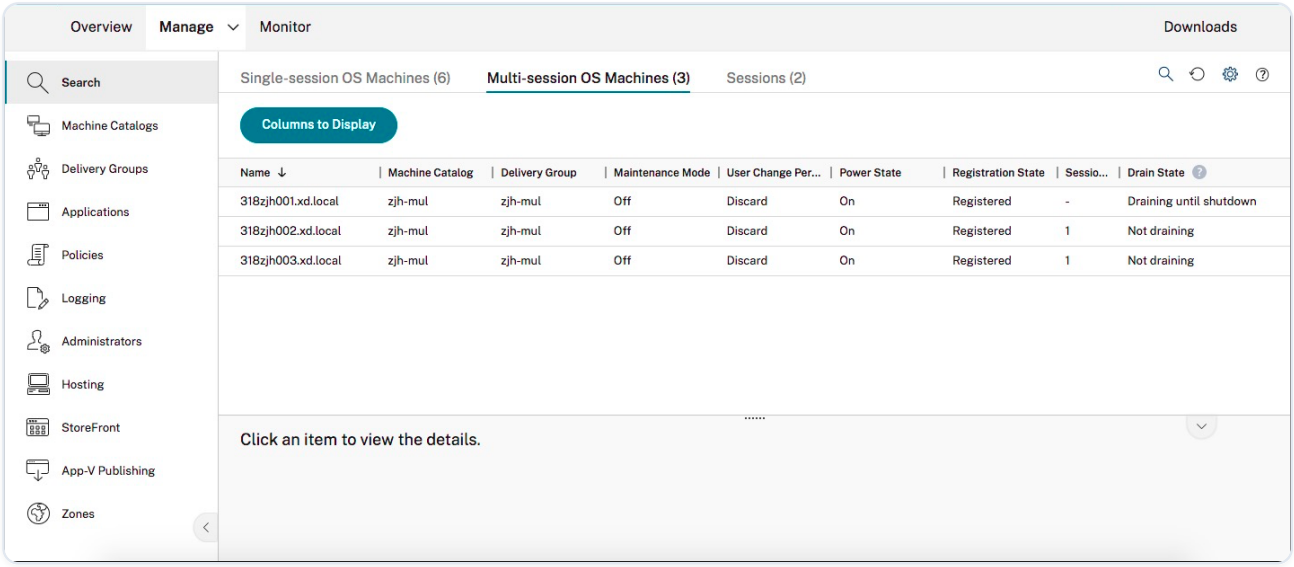
> **注:**
>
> この機能は、マルチセッションマシンにのみ適用されます。

> Web Studioでは、ドレイン状態のマシンを表示でき、どのマシンがシャットダウンしようとしているかを知ることができます。次の手順を実行します。

1. **検索**ノードに移動し、次に**表示する列**をクリックします。
2. **表示する列**ウィンドウで、**ドレイン状態**の横にあるチェックボックスをオンにします。
3. **保存**をクリックして、**表示する列**ウィンドウを終了します。

ドレイン状態列には、次の情報が表示されます。

- **シャットダウンまでドレイン中。** マシンがシャットダウンされるまでドレイン状態にある場合に表示されます。
- **ドレイン中ではありません。** マシンがまだドレイン状態ではない場合に表示されます。



詳細情報

Autoscale の詳細については、Tech Zone のCitrix Autoscale を参照してください。

スケジュールベースおよび負荷ベースの設定

Autoscale™ がマシンを電源管理する仕組み

Autoscale は、選択されたスケジュールに基づいてマシンの電源をオン/オフします。Autoscale を使用すると、特定の曜日を含む複数のスケジュールを設定し、それらの時間帯に利用可能なマシンの数を調整できます。特定の曜日の特定の時間に一連のユーザーがマシンリソースを消費すると予想される場合、Autoscale は最適化されたエクスペリエンスを提供するのに役立ちます。それらのマシンは、セッションが実行されているかどうかにかかわらず、スケジュール中に電源がオンになることに注意してください。

> **注:**
>
> Autoscale は、あらゆる電源管理されたマシンをサポートします。

> スケジュールは、デリバリーグループの**タイムゾーン**に基づいています。タイムゾーンを変更するには、デリバリーグループのユーザー設定を変更できます。詳細については、「デリバリーグループの管理」を参照してください。

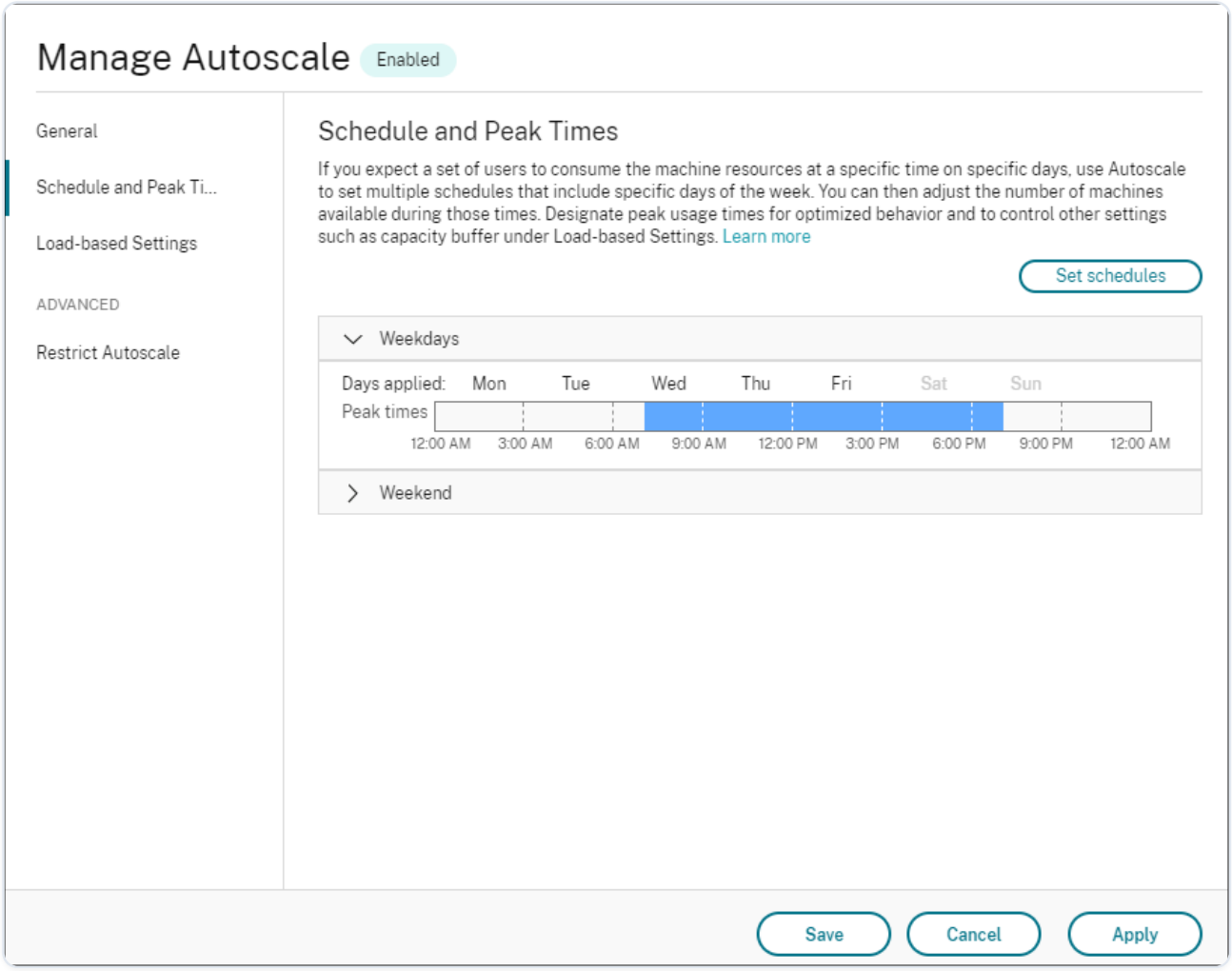
Autoscale には、2つのデフォルトスケジュールがあります。*平日*（月曜日から金曜日）と*週末*（土曜日と日曜日）です。デフォルトでは、**平日**スケジュールでは、ピーク時に午前7時から午後6時30分まで1台のマシンの電源がオンになり、オフピーク時には電源がオンになりません。デフォルトの容量バッファは、ピーク時とオフピーク時に10%に設定されています。デフォルトでは、**週末**スケジュールではマシンの電源はオンになりません。

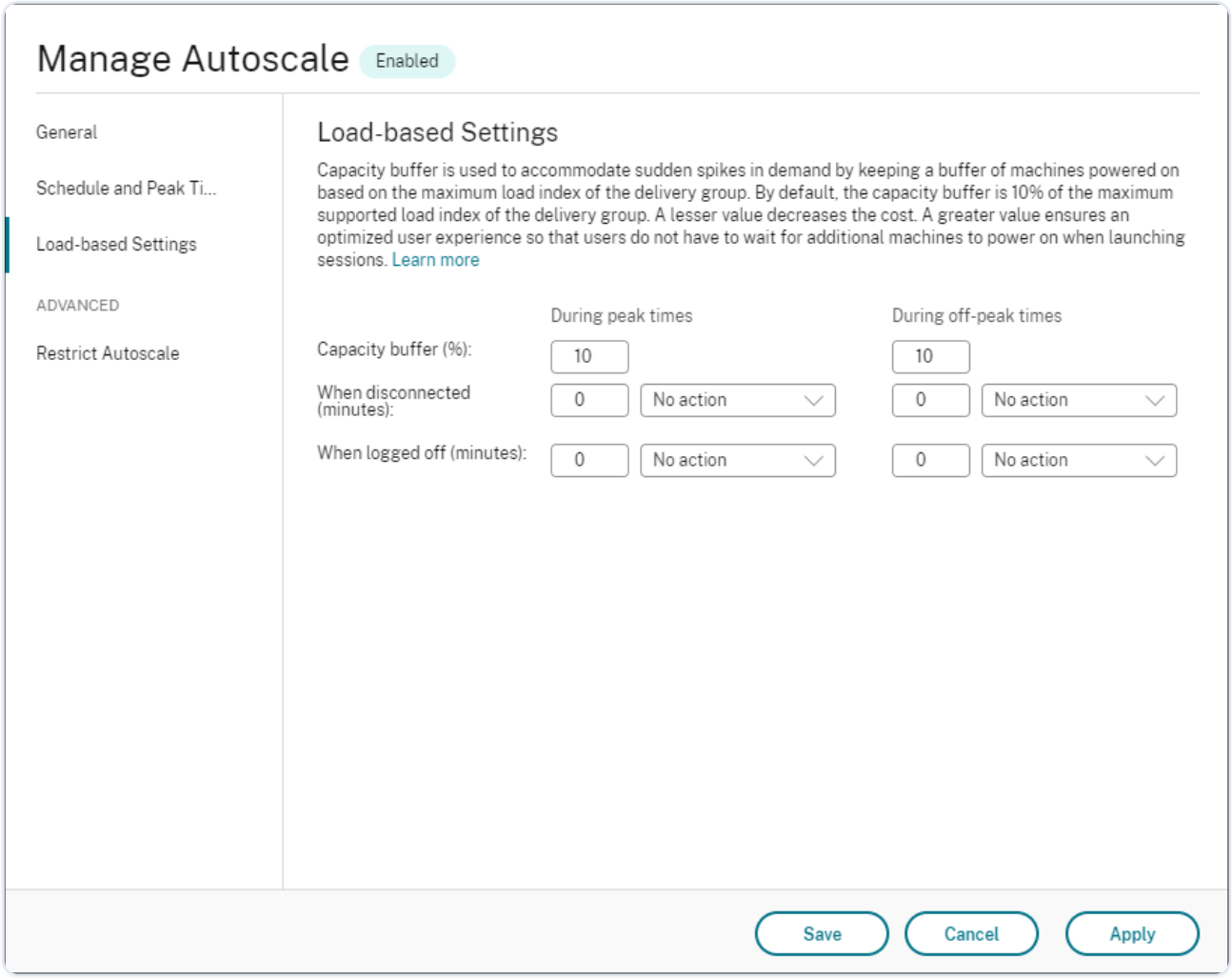
> **注:**
>
> Autoscale は、サイトに登録されているマシンのみを、計算における利用可能な容量の一部として扱います。「登録済み」とは、マシンが使用可能であるか、すでに使用中であることを意味します。これにより、ユーザーセッションを受け入れられるマシンのみがデリバリーグループの容量に含まれることが保証されます。

ユーザーインターフェイス

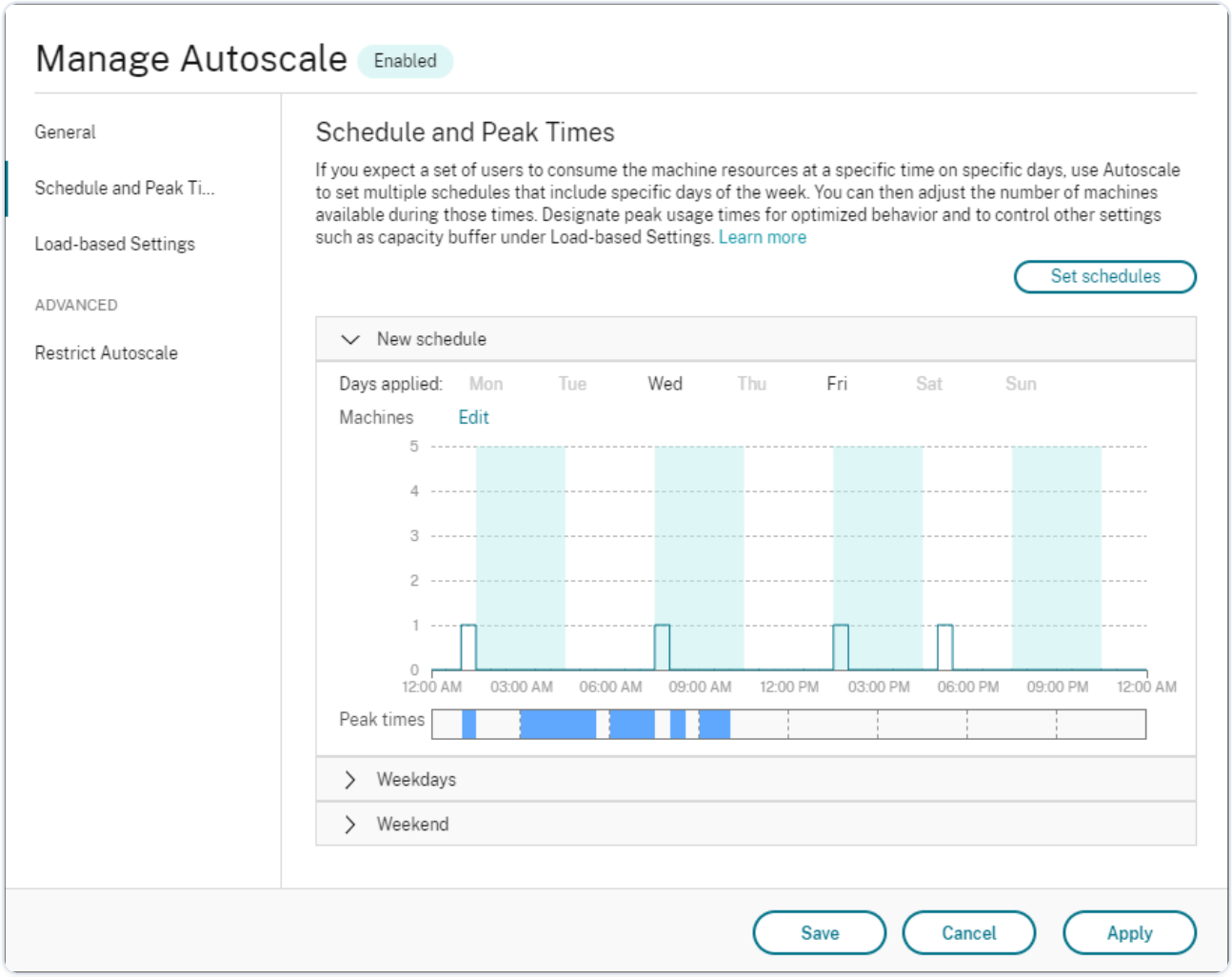
認識しておくべき3種類のユーザーインターフェイスがあります。

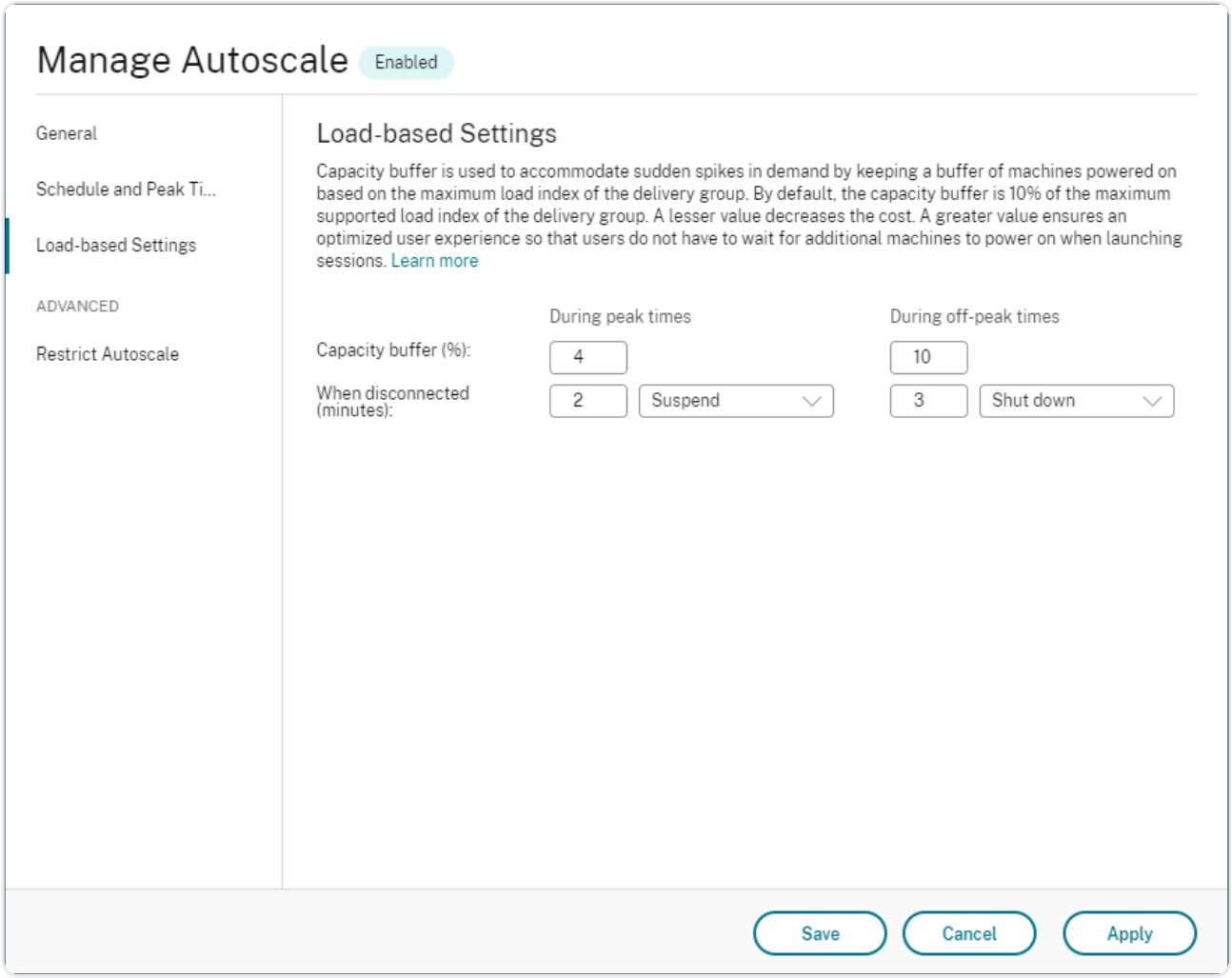
*シングルセッションOS静的デリバリーグループ*のユーザーインターフェイス：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
Weekdays
Days applied: Mon Tue Wed Thu Fri Sat Sun
Peak times
12:00 AM 3:00 AM 6:00 AM 9:00 AM 12:00 PM 3:00 PM 6:00 PM 9:00 PM 12:00 AM
Weekend
Save
Cancel
Apply

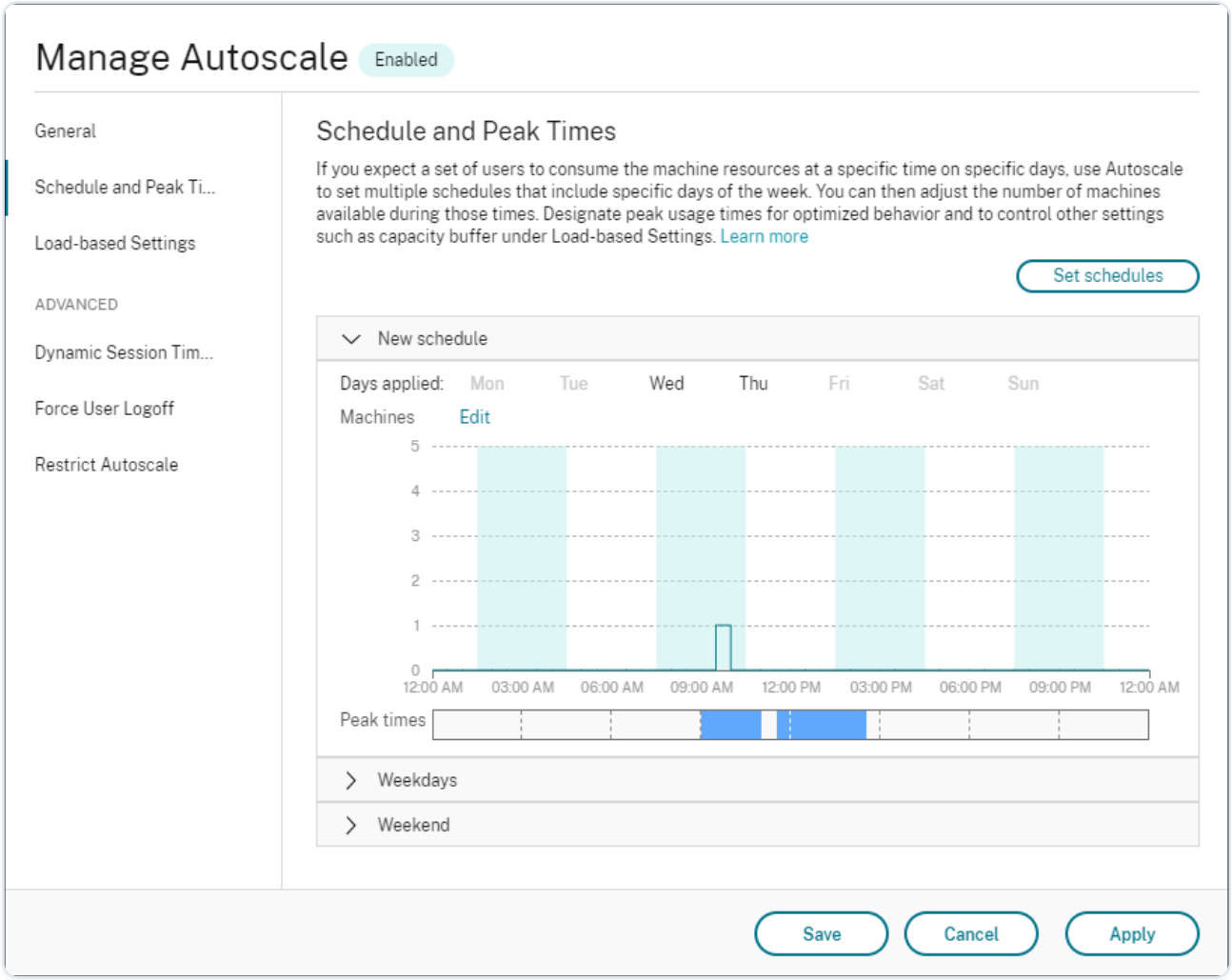


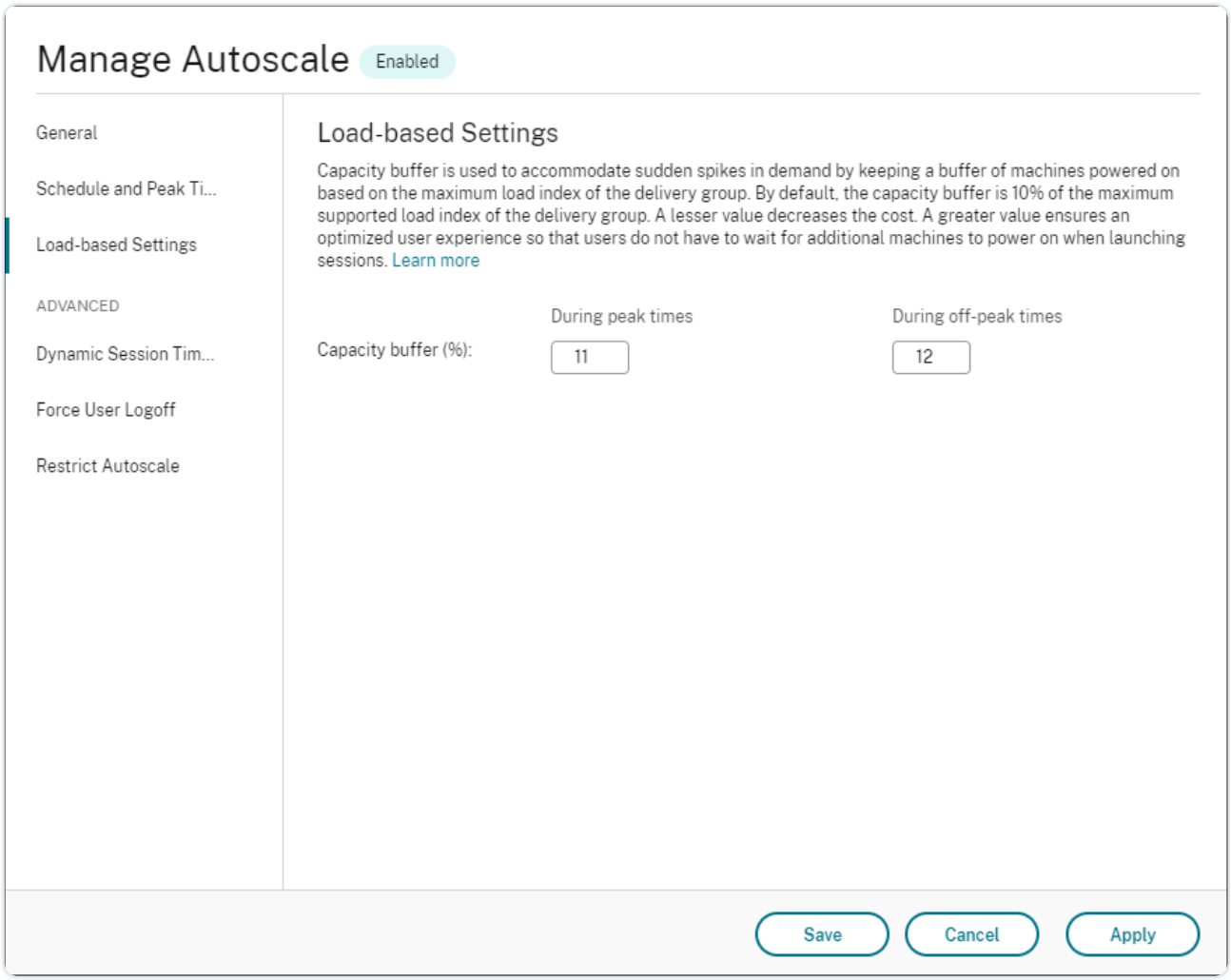
*シングルセッションOSランダムデリバリーグループの*Autoscale ユーザーインターフェイス：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



マルチセッションOSデリバリーグループのAutoscaleユーザーインターフェイス:


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Dynamic Session Tim...
Force User Logoff
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM
03:00 AM
06:00 AM
09:00 AM
12:00 PM
03:00 PM
06:00 PM
09:00 PM
12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



スケジュールベースの設定

Autoscaleスケジュール。スケジュールの追加、編集、選択、削除ができます。

適用された曜日。選択したスケジュールに適用した曜日が強調表示されます。残りの曜日はグレー表示されます。

編集。各時間または30分ごとにマシンを割り当てることができます。マシンは数値またはパーセンテージで割り当てることができます。

> **注:**
>
> - このオプションは、マルチセッションOSおよびシングルセッションOSランダムデリバリーグループのAutoscaleユーザーインターフェイスでのみ利用可能です。
> - **編集**の横にあるヒストグラムは、異なるタイムスロットで実行されているマシンの数または割合を示します。

- **ピーク時間**の上にある**編集**をクリックして、各タイムスロットに**マシンを割り当てる**ことができます。**起動するマシン**ウィンドウのメニューから選択したオプションに応じて、マシンを数値またはパーセンテージで割り当てることができます。
- マルチセッションOSデリバリーグループの場合、各日において30分単位で実行中のマシンの最小数を個別に設定できます。シングルセッションOSランダムデリバリーグループの場合、各日において60分単位で実行中のマシンの最小数を個別に設定できます。

独自のスケジュールを定義するには、次の手順に従います。

1. **Autoscaleの管理**ウィンドウの**スケジュールとピーク時間**ページで、**スケジュールを設定**をクリックします。
2. **Autoscaleスケジュールの編集**ウィンドウで、各スケジュールに適用する日を選択します。必要に応じてスケジュールを削除することもできます。
3. **完了**をクリックしてスケジュールを保存し、**スケジュールとピーク時間**ページに戻ります。
4. 該当するスケジュールを選択し、必要に応じて構成します。
5. **適用**をクリックして**Autoscaleの管理**ウィンドウを終了するか、他のページで設定を構成します。

重要：

- Autoscaleでは、異なるスケジュールで同じ日が重複することはできません。たとえば、スケジュール1で月曜日を選択した後、スケジュール2で月曜日を選択すると、スケジュール1の月曜日は自動的にクリアされます。
- スケジュール名は大文字と小文字を区別しません。
- スケジュール名は空白にしたり、スペースのみを含めたりすることはできません。
- Autoscaleでは、文字間に空白スペースを使用できます。
- スケジュール名には、次の文字を含めることはできません: \ / ; : # . * ? = < > \| ( ) { } " ' `。
- Autoscaleは重複するスケジュール名をサポートしていません。各スケジュールに異なる名前を入力してください。
- Autoscaleは空のスケジュールをサポートしていません。つまり、曜日が選択されていないスケジュールは保存されません。

注：

選択したスケジュールに含まれる日はハイライト表示され、含まれない日はグレー表示されます。

負荷ベースの設定

ピーク時間。選択したスケジュールに適用した日のピーク時間を定義できます。これを行うには、横棒グラフを右クリックします。ピーク時間を定義すると、残りの未定義の時間はデフォルトでオフピーク時間になります。**デフォルト**では、選択したスケジュールに含まれる日のピーク時間として、午前7時から午後7時までの時間帯が定義されています。

重要:

- マルチセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファに使用されます。
- シングルセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファに使用され、ログオフ後または切断後にトリガーされるアクションを制御します。
- マルチセッションOSおよびシングルセッションOSデリバリーグループの両方で、スケジュールに含まれる日のピーク時間を30分単位で細かく定義できます。または、代わりに`New-BrokerPowerTimeScheme PowerShell`コマンドを使用することもできます。詳細については、「Broker PowerShell SDKコマンド」を参照してください。

容量バッファ。電源がオンになっているマシンのバッファを維持できます。値が小さいほどコストが削減されます。値が大きいほど、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がないように、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、容量バッファはピーク時間とオフピーク時間で10%です。容量バッファを0（ゼロ）に設定すると、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がある場合があります。Autoscaleを使用すると、ピーク時間とオフピーク時間で容量バッファを個別に決定できます。

その他の設定

ヒント:

- Broker PowerShell SDKを使用してその他の設定を構成することを選択できます。詳細については、「Broker PowerShell SDKコマンド」を参照してください。
- 切断時とログオフ時の設定に関連するSDKコマンドを理解するには、`<https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy>`を参照してください。

切断時。セッション切断後、切断されロックされたマシンが、一時停止またはシャットダウンされるまでにどのくらいの時間電源オンのままにするかを指定できます。時間値を指定した場合、構成したアクションに応じて、指定された切断時間が経過するとマシンは一時停止またはシャットダウンされます。デフォルトでは、切断されたマシンにはアクションが割り当てられていません。ピーク時間とオフピーク時間でアクションを個別に定義できます。これを行うには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択した場合、セッション切断後のマシンは電源オンのままになります。Autoscaleはそれに対してアクションを実行しません。
- **一時停止**。選択した場合、指定された切断時間が経過すると、Autoscaleはマシンをシャットダウンせずに一時停止します。**一時停止**を選択すると、次のオプションが利用可能になります。
  - **再接続なしの場合（分）**。中断されたマシンは、切断されたユーザーが再接続する際には利用可能ですが、新しいユーザーには利用できません。すべてのワークロードを処理するためにマシンを再度利用可能にするには、シャットダウンします。Autoscaleがマシンをシャットダウンするまでのタイムアウトを分単位で指定します。
- **シャットダウン**。選択すると、指定された切断時間が経過したときに、Autoscaleはマシンをシャットダウンします。

注:

このオプションは、シングルセッションOSのランダムおよび静的デリバリーグループ用のAutoscaleユーザーインターフェイスでのみ利用可能です。

ログオフ時。セッションログオフ後にマシンがサスペンドまたはシャットダウンされるまで、どのくらいの時間電源がオンのままになるかを指定できます。時間値を指定した場合、設定したアクションに応じて、指定されたログオフ時間が経過するとマシンはサスペンドま

たはシャットダウンされます。デフォルトでは、ログオフされたマシンにはアクションが割り当てられていません。ピーク時とオフピーク時でアクションを個別に定義できます。そのためには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択すると、セッションログオフ後もマシンは電源がオンのままになります。Autoscaleはそれに対して何もアクションを実行しません。
- **サスペンド**。選択すると、指定されたログオフ時間が経過したときに、Autoscaleはマシンをシャットダウンせずに一時停止します。
- **シャットダウン**。選択すると、指定されたログオフ時間が経過したときに、Autoscaleはマシンをシャットダウンします。

注:

このオプションは、シングルセッションOSの静的デリバリーグループ用のAutoscaleユーザーインターフェイスでのみ利用可能です。

切断されたセッションを持つ、異なる時間帯に移行するシングルセッションOSマシンの電源管理

重要:

- この機能強化は、切断されたセッションを持つシングルセッションOSマシンにのみ適用されます。ログオフされたセッションを持つシングルセッションOSマシンには適用されません。
- この機能強化を有効にするには、該当するデリバリーグループでAutoscaleを有効にする必要があります。そうしないと、期間移行時に切断電源ポリシーアクションはトリガーされません。

以前のリリースでは、アクション（切断アクション = 「**サスペンド**」または「**シャットダウン**」）が必要な時間帯に移行するシングルセッションOSマシンは、電源がオンのままでした。このシナリオは、マシンがアクション（切断アクション = 「**何もしない**」）が不要な時間帯（ピーク時またはオフピーク時）に切断された場合に発生しました。

このリリース以降、Autoscaleは、指定された切断時間が経過したときに、移行先の時間帯に設定されている切断アクションに応じて、マシンをサスペンドまたは電源オフにします。

例えば、シングルセッションOSデリバリーグループに対して、以下の電源ポリシーを設定します。

- `PeakDisconnectAction` を「何もしない」に設定します
- `OffPeakDisconnectAction` を「シャットダウン」に設定します
- 'OffPeakDisconnectTimeout' を「10」に設定します

> **注：**
>
> 切断アクション電源ポリシーの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>` および `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>` を参照してください。

> 以前のリリースでは、ピーク時にセッションが切断されたシングルセッションOSマシンは、ピークからオフピークに移行しても電源が入ったままでした。このリリース以降、期間移行時に `OffPeakDisconnectAction` および `OffPeakDisconnectTimeout` ポリシーアクションがシングルセッションOSマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作（つまり、ピークからオフピークへ、またはオフピークからピークへ、切断されたセッションを持つマシンに対して何もしない）に戻したい場合は、以下のいずれかを実行してください。

- 「LegacyPeakTransitionDisconnectedBehaviour」レジストリ値を1（true; 以前の動作を有効にする）に設定します。デフォルトでは、値は0（false; 期間移行時に切断電源ポリシーアクションをトリガーする）です。
  - パス: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - 名前: LegacyPeakTransitionDisconnectedBehaviour
  - 種類: REG_DWORD
  - データ: 0x00000001 (1)
- `Set-BrokerServiceConfigurationData` PowerShellコマンドを使用して設定を構成します。例：

- `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

期間移行時に電源ポリシーアクションを適用する前に、マシンは次の基準を満たす必要があります。

- 切断されたセッションがあります。
- 保留中の電源操作がない。
- 異なる時間帯に移行するシングルセッションOSデリバリーグループに属している。
- 特定時間帯（ピーク時またはオフピーク時）にセッションが切断され、電源操作が割り当てられている期間に移行する。

容量バッファの仕組み

容量バッファは、動的な負荷増加に対応するために、現在の需要に予備容量を追加するために使用されます。注意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、容量バッファは、ロードインデックスの観点からデリバリーグループの総容量のパーセンテージとして定義されます。ロードインデックスの詳細については、ロードインデックスを参照してください。
- シングルセッションOSデリバリーグループの場合、容量バッファは、マシンの数の観点からデリバリーグループの総容量のパーセンテージとして定義されます。

> **注:**

> Autoscaleをタグ付きマシンに制限するシナリオでは、容量バッファは、ロードインデックスの観点から、デリバリーグループ内のタグ付きマシンの総容量のパーセンテージとして定義されます。

> Autoscaleでは、ピーク時とオフピーク時で容量バッファを個別に設定できます。容量バッファフィールドの値が小さいほど、Autoscaleが起動する予備容量が少なくなるため、コストが削減されます。値が大きいほど、ユーザーはセッション起動時により多くのマシンが起動するのを待つ必要がなくなり、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、容量バッファは10%です。

> **重要:**

容量バッファにより、総予備容量がデリバリーグループの総容量の「X」パーセントを下回るレベルに低下した場合にマシンが起動されます。これにより、必要な割合の予備容量が確保されます。

マルチセッションOSデリバリーグループ

マシンはいつ電源オンになるか?

重要:

スケジュールが選択されている場合、Autoscale はスケジュールで電源オンになるように構成されているすべてのマシンの電源をオンにします。Autoscale は、負荷に関係なく、スケジュール中に指定された数のマシンの電源をオンに保ちます。

デリバリーグループ内の電源オンになっているマシンの数が、負荷インデックスの観点からバッファ容量を尊重するために必要なバッファを満たせなくなった場合、Autoscale は追加のマシンの電源をオンにします。たとえば、デリバリーグループに 20 台のマシンがあり、スケジュールベースのスケーリングの一部として、容量バッファ 20% で 3 台のマシンの電源がオンになるようにスケジュールされているとします。最終的に、負荷がない場合でも 4 台のマシンの電源がオンになります。これは、バッファとして 4 x 10k の負荷インデックスが必要であるため、少なくとも 4 台のマシンの電源がオンになっている必要があるためです。このケースは、ピーク時、マシンへの負荷の増加、新しいセッションの起動、およびデリバリーグループに新しいマシンを追加するときに発生する可能性があります。Autoscale は、次の条件を満たすマシンのみの電源をオンにすることに注意してください。

- マシンがメンテナンスモードではない。
- マシンが実行されているハイパーバイザーがメンテナンスモードではない。
- マシンが現在電源オフになっている。
- マシンに保留中の電源操作はありません。

マシンはいつ電源オフになるか?

重要:

- スケジュールが選択されている場合、Autoscale はスケジュールに基づいてマシンの電源をオフにします。
- Autoscale は、スケジュール中に電源オンになるようにスケジュールで構成されたマシンの電源をオフにしません。

デリバリーグループのターゲットとなる電源オンのマシン数（バッファを含む）をサポートするのに十分なマシン数を超えている場合、Autoscale は余分なマシンの電源をオフにします。このケースは、オフピーク時、マシンへの負荷の減少、セッションログオフ、およびデリバリーグループからマシンを削除するときに発生する可能性があります。Autoscale は、次の条件を満たすマシンのみの電源をオフにします。

- マシンと、マシンが実行されているハイパーバイザーがメンテナンスモードではありません。
- マシンが現在電源オンになっている。
- マシンは利用可能として登録されているか、起動後に登録を待機しています。
- マシンにアクティブなセッションがありません。
- マシンに保留中の電源操作がありません。
- マシンは指定された電源オフ遅延を満たしています。これは、マシンが少なくとも「X」分間電源オンの状態であったことを意味します。「X」はデリバリーグループに指定された電源オフ遅延です。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscale で電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - 容量バッファは10%に設定されています。
  - 選択されたスケジュールにマシンは含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. さらにユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。

5. ユーザーセッションの負荷は、セッション負荷がオンプレミスリソースのみで処理されるまでさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかの詳細については、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - 1台のマシン（例：M1）が電源オンになります。このマシンは、構成された容量バッファのために電源オンになります。この場合、10（マシン数）x 10,000（負荷インデックス）x 10%（構成された容量バッファ）は10,000に等しくなります。したがって、1台のマシンが電源オンになります。
  - 電源オンになったマシン（M1）の負荷インデックス値は、ベースライン負荷（負荷インデックスは0）です。
- 最初のユーザーがログオンします
  - セッションはマシンM1でホストされるように指示されます。
  - 電源オンになったマシンM1の負荷インデックスが増加し、マシンM1はベースライン負荷ではなくなります。
  - Autoscaleは、構成された容量バッファのために需要を満たすために、追加のマシン（M2）の電源をオンにし始めます。
  - マシンM2の負荷インデックス値はベースライン負荷です。
- ユーザーが負荷を増加させます
  - セッションはマシンM1とM2の間で負荷分散されます。その結果、電源オンになったマシン（M1とM2）の負荷インデックスが増加します。
  - 総予備容量は、負荷インデックスの観点からまだ10,000を超えるレベルにあります。
  - マシンM2の負荷インデックス値はベースライン負荷ではなくなります。
- より多くのユーザーセッションが開始されます
  - セッションはマシン (M1 および M2) 間で負荷分散されます。その結果、電源がオンになっているマシン (M1 および M2) の負荷インデックスがさらに増加します。
  - 負荷インデックスの観点から、合計予備容量が10,000を下回るレベルに低下すると、Autoscaleは、構成された容量バッファにより、需要を満たすため追加のマシン (M3) の電源をオンにし始めます。
  - マシンM3の負荷インデックス値はベースライン負荷にあります。

- さらに多くのユーザーセッションが開始されます
  - セッションはマシン (M1～M3) 間で負荷分散されます。その結果、電源がオンになっているマシン (M1～M3) の負荷インデックスが増加します。
  - 負荷インデックスの観点から、合計予備容量は10,000を上回るレベルにあります。
  - マシンM3の負荷インデックス値は、もはやベースライン負荷ではありません。
- セッション終了によりユーザーセッション負荷が減少します
  - ユーザーがセッションからログオフするか、アイドルセッションがタイムアウトすると、マシンM1～M3で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
  - 負荷インデックスの観点から、合計予備容量が10,000を上回るレベルに増加すると、Autoscaleは、いずれかのマシン (たとえばM3) をドレイン状態にします。その結果、新しい変更が発生しない限り、他のユーザーが開始したセッションはそのマシンに転送されなくなります。たとえば、エンドユーザーの負荷が再び増加したり、他のマシンの負荷が最も低くなったりした場合です。
- ユーザーセッション負荷は減少し続けます
  - マシンM3上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、Autoscaleはマシン M3の電源をオフにします。
  - さらに多くのユーザーがセッションを終了すると、電源がオンになっているマシン (M1およびM2) で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
  - 負荷インデックスの観点から、合計予備容量が10,000を上回るレベルに増加すると、Autoscaleは、いずれかのマシン (たとえばM2) をドレイン状態にします。その結果、他のユーザーが開始したセッションはそのマシンに転送されなくなります。
- セッションがなくなるまでユーザーセッション負荷は減少し続けます
  - マシンM2上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、Autoscaleはマシン M2の電源をオフにします。
  - 電源がオンになっているマシン（M1）のロードインデックス値はベースラインロードにあります。構成されたキャパシティバッファのため、Autoscaleはマシン M1をドレイン状態にしません。

> **注：**

> マルチセッションOSデリバリーグループの場合、ユーザーがセッションからログオフすると、デスクトップへのすべての変更は失われます。ただし、構成されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSランダムデリバリーグループ

キャパシティバッファは、デリバリーグループ内のマシンの総数に基づいて、電源がオンになっているマシンのバッファを維持することで、急な需要の急増に対応するために使用されます。デフォルトでは、キャパシティバッファはデリバリーグループ内のマシンの総数の10%です。

マシンの数（キャパシティバッファを含む）が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加のマシンの電源がオンになります。マシンの数（キャパシティバッファを含む）が現在電源がオンになっているマシンの総数よりも少ない場合、超過したマシンは、構成したアクションに応じてシャットダウンまたは一時停止されます。

シナリオ例

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscaleで電源管理を行いたいデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - キャパシティバッファは10%に設定されています。
  - 選択されたスケジュールにはマシンは含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. より多くのユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。
5. セッション負荷がオンプレミスリソースのみで処理されるまで、ユーザーセッションの負荷はさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - 1台のマシン（例: M1）が電源オンになります。このマシンは、構成されたキャパシティバッファのために電源オンになります。この場合、10（マシン数）x 10,000（負荷イン

デックス）x 10%（構成されたキャパシティバッファ）は10,000に等しくなります。したがって、1台のマシンが電源オンになります。

- 電源オンになったマシン（M1）の負荷インデックス値は、ベースライン負荷（負荷インデックスは0）です。

- 最初のユーザーがログオンします
  - セッションはマシンM1でホストされるように指示されます。
  - 電源オンになったマシンM1の負荷インデックスが増加し、マシンM1はベースライン負荷ではなくなります。
  - 構成されたキャパシティバッファにより、Autoscale は需要を満たすために追加のマシン (M2) の電源をオンにし始めます。
  - マシン M2 の負荷インデックス値はベースライン負荷にあります。
- ユーザーが負荷を増加させます
  - セッションはマシン M1 と M2 の間で負荷分散されます。その結果、起動中のマシン (M1 と M2) の負荷インデックスが増加します。
  - 総予備容量は、負荷インデックスの観点から依然として 10,000 を超えるレベルにあります。
  - マシン M2 の負荷インデックス値はもはやベースライン負荷ではありません。
- より多くのユーザーセッションが開始されます
  - セッションはマシン (M1 と M2) の間で負荷分散されます。その結果、起動中のマシン (M1 と M2) の負荷インデックスがさらに増加します。
  - 負荷インデックスの観点から総予備容量が 10,000 を下回るレベルに低下すると、Autoscale は構成されたキャパシティバッファにより、需要を満たすために追加のマシン (M3) の電源をオンにし始めます。
  - マシン M3 の負荷インデックス値はベースライン負荷にあります。
- さらに多くのユーザーセッションが開始されます
  - セッションはマシン (M1 から M3) の間で負荷分散されます。その結果、起動中のマシン (M1 から M3) の負荷インデックスが増加します。
  - 総予備容量は、負荷インデックスの観点から 10,000 を超えるレベルにあります。
  - マシン M3 の負荷インデックス値はもはやベースライン負荷ではありません。
- セッション終了によりユーザーセッションの負荷が減少します

    - ユーザーがセッションからログオフするか、アイドルセッションがタイムアウトすると、M1からM3までのマシンで解放された容量が、他のユーザーが開始したセッションをホストするために再利用されます。
    - ロードインデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはマシンの1つ（たとえばM3）をドレイン状態にします。その結果、新しい変更が発生しない限り、他のユーザーが開始したセッションはそのマシンに転送されなくなります。たとえば、エンドユーザーの負荷が再び増加したり、他のマシンの負荷が最も低くなったりした場合です。

- ユーザーセッションの負荷は減少し続けます
    - マシンM3上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、AutoscaleはマシンM3の電源をオフにします。
    - さらに多くのユーザーがセッションを終了すると、電源がオンになっているマシン（M1とM2）で解放された容量が、他のユーザーが開始したセッションをホストするために再利用されます。
    - ロードインデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはマシンの1つ（たとえばM2）をドレイン状態にします。その結果、他のユーザーが開始したセッションはそのマシンに転送されなくなります。
- セッションがなくなるまでユーザーセッションの負荷は減少し続けます
    - マシンM2上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、AutoscaleはマシンM2の電源をオフにします。
    - 電源がオンになっているマシン（M1）のロードインデックス値はベースライン負荷です。構成された容量バッファーのため、AutoscaleはマシンM1をドレイン状態にしません。

> **注:**
>
> マルチセッションOSデリバリーグループの場合、ユーザーがセッションからログオフすると、デスクトップへのすべての変更は失われます。ただし、構成されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSランダムデリバリーグループ

容量バッファーは、デリバリーグループ内のマシンの総数に基づいて、電源がオンになっているマシンのバッファーを維持することで、需要の急増に対応するために使用されます。デフォルトでは、容量バッファーはデリバリーグループ内のマシンの総数の10%です。

マシンの数（容量バッファーを含む）が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加のマシンの電源がオンになります。マシンの数（容量バッファーを含む）が現在電源がオンになっているマシンの総数よりも少ない場合、余分なマシンは、構成したアクションに応じてシャットダウンまたは中断されます。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscaleで電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - 容量バッファは10%に設定されています。
  - 選択されたスケジュールにはマシンが含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. さらに多くのユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。
5. オンプレミスリソースのみでセッション負荷が処理されるまで、ユーザーセッションの負荷はさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - 1台のマシン（M1）が電源オンになります。このマシンは、構成された容量バッファのために電源オンになります。この場合、10（マシンの数）x 10%（構成された容量バッファ）は1に等しくなります。したがって、1台のマシンが電源オンになります。
- 最初のユーザーがログオンします
  - ユーザーがデスクトップを使用するために初めてログオンすると、電源オンになっているマシンでホストされているデスクトップのプールからデスクトップが割り当てられます。この場合、ユーザーにはマシンM1からデスクトップが割り当てられます。
  - 構成された容量バッファのために需要を満たすため、Autoscaleは追加のマシン（M2）の電源をオンにし始めます。

- 2番目のユーザーがログオンします
  - ユーザーにはマシンM2からデスクトップが割り当てられます。
  - 構成された容量バッファのために需要を満たすため、Autoscaleは追加のマシン（M3）の電源をオンにし始めます。
- 3番目のユーザーがログオンします
  - ユーザーにはマシンM3からデスクトップが割り当てられます。
  - Autoscale は、設定されたキャパシティバッファにより、需要を満たすため追加のマシン (M4) の電源をオンにし始めます。
- ユーザーがログオフします
  - ユーザーがログオフするか、ユーザーのデスクトップがタイムアウトすると、解放されたキャパシティ (M3 など) がバッファとして利用可能になります。その結果、キャパシティバッファが10%に設定されているため、Autoscale はマシン M4 の電源をオフにし始めます。
- ユーザーがいなくなるまで、さらに多くのユーザーがログオフします
  - さらに多くのユーザーがログオフした後、Autoscale はマシン (M2 または M3 など) の電源をオフにします。
  - ユーザーが残っていなくても、そのマシンは予備のキャパシティとして予約されているため、Autoscale は残りの1台のマシン (M1 など) の電源をオフにしません。

> **注：**
>
> シングルセッションOSのランダムデリバリーグループの場合、ユーザーがセッションをログオフすると、デスクトップへのすべての変更は失われます。ただし、設定されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSの静的デリバリーグループ

キャパシティバッファは、デリバリーグループ内の未割り当てマシンの総数に基づいて、未割り当てマシンのバッファの電源をオンに保つことで、急激な需要の急増に対応するために使用されます。デフォルトでは、キャパシティバッファはデリバリーグループ内の未割り当てマシンの総数の10%です。

> **重要：**
>
> デリバリーグループ内のすべてのマシンが割り当てられた後、キャパシティバッファはマシンの電源のオン/オフには関与しません。

> マシンの数 (キャパシティバッファを含む) が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加の未割り当てマシンの電源がオンになります。マシンの数 (キャパシティバッファを含む) が現在電源がオンになっているマシンの総数よりも少ない場合、設定したアクションに応じて、余分なマシンは電源がオフになるか、中断されます。

シングルセッションOS静的デリバリーグループの場合、Autoscaleは次のようになります。

- 適用されるシングルセッションOSデリバリーグループの `AutomaticPowerOnForAssigned` プロパティが true に設定されている場合にのみ、ピーク時には割り当てられたマシンの電源をオンにし、オフピーク時にはオフにします。
- ピーク時にマシンが電源オフになっている場合、そのマシンが属するデリバリーグループの `AutomaticPowerOnForAssignedDuringPeak` プロパティがtrueに設定されていれば、自動的に電源をオンにします。

割り当てられたマシンで容量バッファがどのように機能するかを理解するには、以下を考慮してください。

- 容量バッファは、デリバリーグループに1台以上の未割り当てのマシンがある場合にのみ機能します。
- デリバリーグループに未割り当てのマシンがない場合（デリバリーグループ内のすべてのマシンが割り当てられている場合）、容量バッファはマシンの電源オン/オフには関与しません。
- `AutomaticPowerOnForAssignedDuringPeak` プロパティは、ピーク時に割り当てられたマシンの電源がオンになるかどうかを決定します。trueに設定されている場合、Autoscaleはピーク時にマシンの電源をオンに保ちます。電源がオフになっている場合でも、Autoscaleはそれらの電源をオンにします。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscaleで電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**

- M1からM3までのマシンは割り当て済みで、M4からM10までのマシンは未割り当てです。
- ピーク時およびオフピーク時のキャパシティバッファは10%に設定されています。
- 選択されたスケジュールに従って、Autoscaleは午前9時から午後6時までマシンの電源を管理します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- スケジュールの開始 – 午前9時
  - AutoscaleはマシンM1～M3の電源をオンにします。
  - Autoscale は、設定された容量バッファのため、追加のマシン (例: M4) の電源をオンにします。マシン M4 は割り当てられていません。
- 最初のユーザーがログオンします
  - ユーザーがデスクトップを使用するために初めてログオンすると、割り当てられていない電源オン状態のマシンでホストされているデスクトップのプールからデスクトップが割り当てられます。この場合、ユーザーにはマシン M4 からデスクトップが割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられた同じデスクトップに接続します。
  - Autoscale は、設定された容量バッファのため、需要を満たすために追加のマシン (例: M5) の電源をオンにし始めます。
- 2番目のユーザーがログオンします
  - ユーザーには、割り当てられていない電源オン状態のマシンからデスクトップが割り当てられます。この場合、ユーザーにはマシン M5 からデスクトップが割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられた同じデスクトップに接続します。
  - Autoscale は、設定された容量バッファのため、需要を満たすために追加のマシン (例: M6) の電源をオンにし始めます。
- ユーザーがログオフします
  - ユーザーがデスクトップからログオフするか、デスクトップがタイムアウトすると、Autoscale は午前 9 時から午後 6 時までマシン M1 から M5 の電源をオンのままにします。それらのユーザーが次回ログオンするときは、初回使用時に割り当てられた同じデスクトップに接続します。
  - 割り当てられていないマシン M6 は、受信する割り当てられていないユーザーにデスクトップを提供するのを待機しています。

- スケジュールの終了 – 午後 6 時
  - 午後 6 時、Autoscale はマシン M1 から M5 の電源をオフにします。
  - Autoscale は、設定された容量バッファのため、割り当てられていないマシン M6 の電源をオンのままにします。そのマシンは、受信する割り当てられていないユーザーにデスクトップを提供するのを待機しています。
  - デリバリーグループでは、マシン M6 から M10 は割り当てられていないマシンです。

動的セッションタイムアウト

この機能を使用すると、ピーク時とオフピーク時の使用時間に合わせて、切断されたセッションとアイドルセッションのタイムアウトを設定でき、マシンのドレインを高速化し、コストを削減できます。この機能は以下に適用されます。

- シングルセッションおよびマルチセッションOSマシン。
- オートスケール用にタグ付けされているかどうかにかかわらず、デリバリーグループ内のすべてのマシン。

VDAは、10分以上アイドル状態であったセッションのアイドル時間を報告するため、動的セッションタイムアウトは、アイドル状態になってから10分以内にアイドルセッションを切断することはできません。より短い値を設定すると、残存するセッションがより早く削除され、コスト削減につながります。

Autoscaleマルチセッション OS - 動的セッションタイムアウト(/en-us/citrix-virtual-apps-desktops/2311/media/autoscale-session-timeout-ms.png)

注:

- この機能は、マルチセッションOSデリバリーグループで常に利用可能です。
- シングルセッションOSデリバリーグループの場合、この機能はバージョン2206 CR以降、または2203 LTSR CU3以降のVDAに適用されます。これらのVDAがCitrix Cloud™に少なくとも1回登録されていることを確認してください。利用できない場合、次のユーザーインターフェイスが表示されます。

動的セッションタイムアウトは利用できません(/en-us/citrix-virtual-apps-desktops/2311/media/autoscale-session-timeout-unavailable.png)

- Autoscale™の動的タイムアウトはコスト削減を目的としています。セキュリティ目的で使用する場合、設定されたタイムアウトがGPOまたはManage consoleポリシーと競合する可能性があります。競合が発生した場合、より短いタイムアウトが優先されます。

アイドルセッションタイムアウト。ユーザー入力がない場合に、中断されないユーザー接続が維持される時間を指定するタイマーを有効または無効にします。タイマーが期限切れになると、セッションは切断状態になり、**切断セッションタイムアウト**が適用されます。**切断セッションタイムアウト**が無効になっている場合、セッションはログオフされません。

重要:

- 10分（600秒）以下の値を指定した場合、Autoscaleは、関連するセッションが10分間アイドル状態になった後に切断します。これは、AutoscaleがVDAが報告するセッションのアイドル時間に依存しているためです。VDAは、10分以上アイドル状態であったセッションのアイドル時間のみを報告します。
- アイドルセッションタイムアウトに達するまでの最後の5分間にユーザーが操作した場合でも、アイドルセッションは切断状態になることがあります。

切断されたセッションのタイムアウト。切断されたデスクトップがセッションがログオフされるまでロックされたままになる時間を指定するタイマーを有効または無効にします。有効にすると、タイマーの期限が切れたときに切断されたセッションがログオフされます。

よくある質問

動的セッションタイムアウト機能は、オートスケール用にタグ付けされたマシンにのみ適用されますか?

動的セッションタイムアウト機能は、オートスケール用にタグ付けされているかどうかにかかわらず、デリバリーグループ内のすべてのマシンに適用されます。

動的セッションタイムアウトによりセッションがログオフされた場合、タグ付けされていないマシンも、タグ付けされたマシンのオートスケールターゲットに含まれますか?

動的セッションタイムアウト機能は、オートスケールのタグ付け機能とは関係ありません。動的セッションタイムアウトによってセッションが終了した場合、マシンがシャットダウンされるま

でドレイン状態になっている場合に限り、タグ付けされていないマシンもそのプロセス中にシャットダウンされる可能性があります。

タグ付けされたマシンの自動スケーリング（クラウドバースト）

> **注:**
>
> この機能は以前、Restrict Autoscaleという名称でした。

はじめに

Autoscaleは、デリバリーグループ内のマシンの一部のみを電源管理する柔軟性を提供します。これを実現するには、1つ以上のマシンにタグを適用し、Autoscaleがタグ付けされたマシンのみを電源管理するように構成します。

この機能は、クラウドバーストのユースケースで役立ちます。これは、クラウドベースのリソースが追加の需要（つまり、バーストワークロード）に対応する前に、オンプレミスリソース（または予約済みパブリッククラウドインスタンス）を使用してワークロードを処理する場合です。オンプレミスのマシン（または予約済みインスタンス）に最初にワークロードを処理させるには、タグ制限とゾーン優先度を組み合わせて使用する必要があります。

タグ制限は、Autoscaleによって電源管理されるマシンを指定します。ゾーン優先度は、ユーザー起動要求を処理するために優先ゾーン内のマシンを指定します。詳細については、タグおよびゾーン優先度を参照してください。

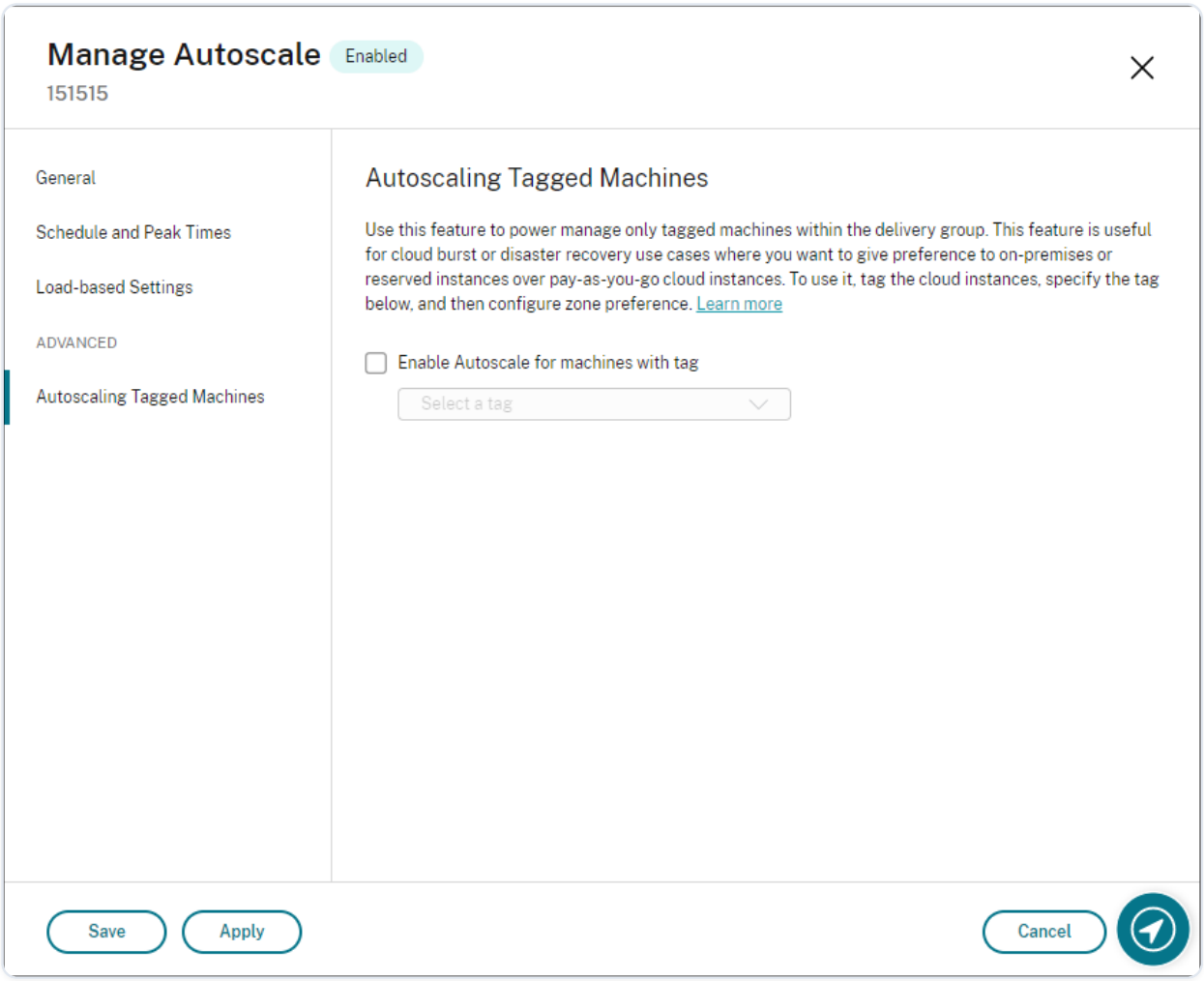
特定のタグ付けされたマシンを自動スケーリングするには、管理コンソールまたはPowerShellを使用できます。

管理コンソールを使用して特定のタグ付けされたマシンを自動スケーリングする

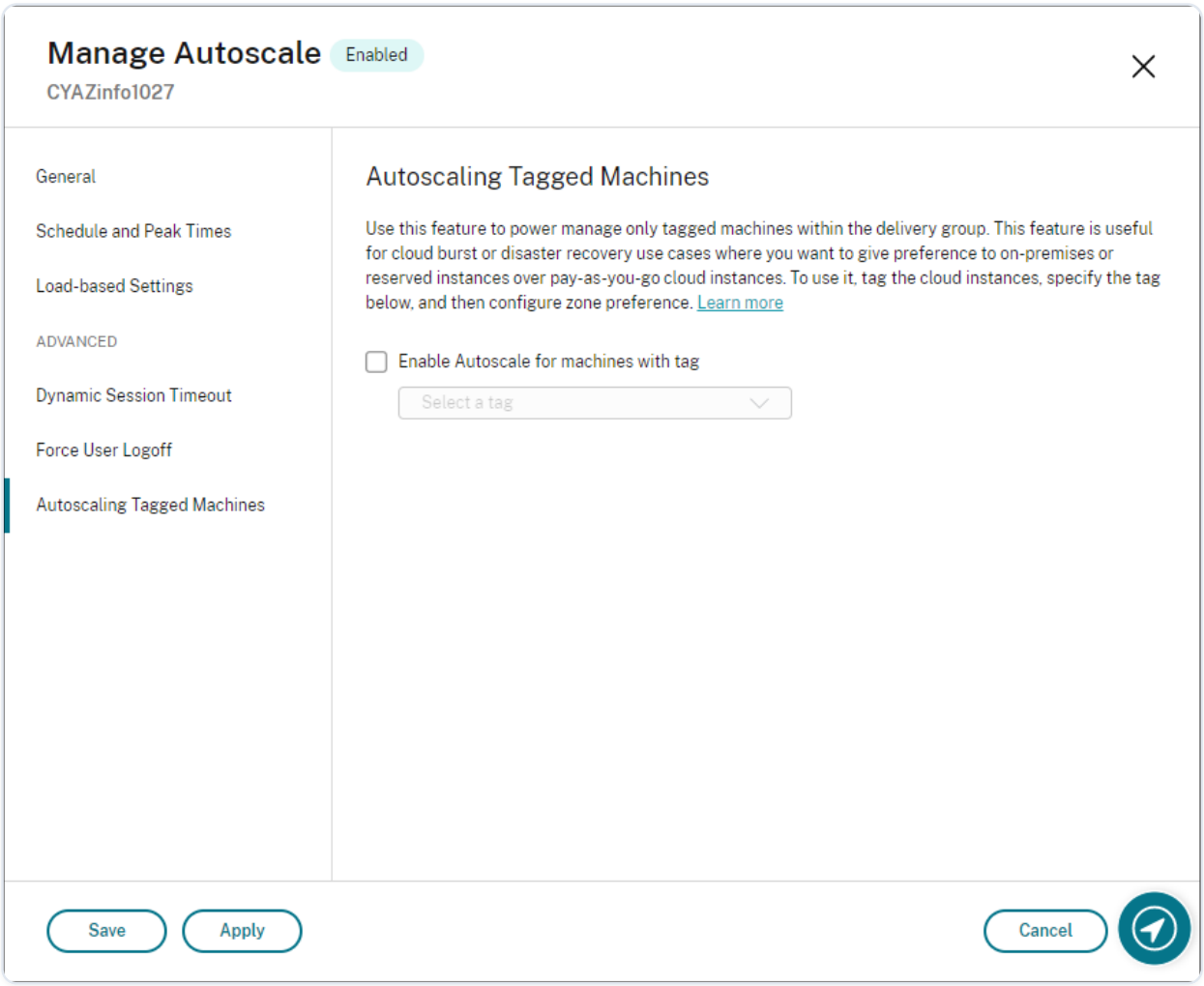
特定のタグ付けされたマシンを自動スケーリングするには、次の手順を実行します。

1. タグを作成し、そのタグをデリバリーグループ内の該当するマシンに適用します。詳細については、「タグとタグ制限の管理」を参照してください。
2. デリバリーグループを選択し、**Manage Autoscale** ウィザードを開きます。
3. **タグ付けされたマシンの自動スケーリング**ページで、**タグ付きマシンのAutoscaleを有効にする**を選択し、リストからタグを選択して、**適用**をクリックして変更を保存します。

   シングルセッションOSの*静的*および*ランダム*なデリバリーグループのユーザーインターフェイス:



マルチセッションOSデリバリーグループのユーザーインターフェイス:



警告:

- 特定のタグを持つマシンのAutoscaleを行うと、タグごとのマシン数を反映するようにヒストグラムが自動的に更新される可能性があります。**スケジュールとピーク時間**ページで、必要に応じて各時間帯にマシンを手動で割り当てることができます。
- タグ付きマシンで使用されているタグは削除できません。タグを削除するには、まずタグの制限を解除する必要があります。

タグの制限を適用した後、後でデリバリーグループから削除したい場合があります。そのためには、**Autoscaleの管理 > タグ付きマシンのAutoscale**ページに移動し、**タグ付きマシンのAutoscaleを有効にする**のチェックを外します。

警告:

- **タグ付きマシンのAutoscaleを有効にする**のチェックを外さずに、該当するマシンからタグを削除すると、**Autoscaleの管理**ウィザードを開いたときに警告が表示されることがあります。マシンからタグを削除すると、Autoscaleで指定したタグが無効になるため、Autoscaleが管理するマシンがなくなる可能性があります。警告を解決するには、**タグ付きマシンのAutoscale**ページに移動し、無効なタグを削除してから、**適用**をクリックして変更を保存します。

Autoscaleがリソースの電源をオンにするタイミングを制御する

タグなしマシンの使用状況に基づいて、Autoscaleがタグ付きマシンの電源をオンにし始めるタイミングを制御することもできます。これにより、タグ付きまたはパブリッククラウドのワークロードの消費をさらに最適化できます。

これを行うには、次の手順を完了します。

1. **タグ付きマシンのAutoscale**ページで、**Autoscaleがタグ付きマシンの電源をオンにし始めるタイミングを制御する**を選択します。
2. ピーク時とオフピーク時の両方で到達したいタグなしマシンの使用率を入力し、**適用**をクリックします。サポートされる値: 0〜100。

Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御する(/en-us/citrix-virtual-apps-desktops/2311/media/autoscale-powers-on-tagged-machines.png)

ヒント:

このパーセンテージは、Autoscaleがタグ付きマシンの電源をオンにし始めるタイミングを制御します。パーセンテージがしきい値（デフォルトは10%）を下回ると、Autoscaleはタグ付きマシンの電源をオンにし始めます。パーセンテージがしきい値を超えると、Autoscaleは電源オフモードに入ります。パーセンテージを入力する際は、次の2つのシナリオを考慮してください。

- シングルセッションOSデリバリーグループの場合: この値は、アイドル状態のタグなしマシンの総数のパーセンテージとして定義されます。例: タグなしのシングルセッションOSマシンが10台あります。セッションがないマシンが1台だけになった場合、Autoscaleはタグ付きマシンの電源をオンにし始めます。

- マルチセッションOSデリバリーグループの場合: この値は、利用可能なタグなしマシンの総容量（負荷インデックスの観点から）のパーセンテージとして定義されます。例: タグなしのマルチセッションOSマシンが10台あります。それらが90%ロードされた場合、Autoscaleはタグ付きマシンの電源をオンにし始めます。

PowerShellを使用して特定のタグ付きマシンを自動スケーリングする

PowerShell SDKを直接使用するには、次の手順を完了します。

1. **タグを作成します。** New-Brokertag PowerShellコマンドを使用してタグを作成します。
   - 例: `$managed = New-BrokerTag Managed`。この場合、タグは「Managed」という名前です。New-Brokertag PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/>`を参照してください。
2. **マシンにタグを適用します。** Get-Brokermachine PowerShellコマンドを使用して、Autoscaleが電源管理するカタログ内のマシンにタグを適用します。
   - 例: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`。この場合、カタログは「cloud」という名前です。
   - Get-Brokermachine PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/>`を参照してください。

   注:

   タグを適用した後で、新しいマシンをカタログに追加する場合があります。その場合、タグは新しいマシンに自動的に適用*されません*。

3. **Autoscaleが電源管理するデリバリーグループにタグ付きマシンを追加します。** Get-BrokerDesktopGroup PowerShellコマンドを使用して、マシンを含むデリバリーグループにタグ制限を追加します（つまり、「タグXを持つマシンへの起動を制限する」）。
   - 例: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`。この場合、デリバリーグループのUIDは1です。

- Get-BrokerDesktopGroup PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`を参照してください。

タグ制限を適用した後、後でデリバリーグループから削除したい場合があります。その場合は、Get-BrokerDesktopGroup PowerShellコマンドを使用します。

例: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscaleTagUid $null`。この場合、デリバリーグループのUIDは1です。

> **注:**
>
> タグ付けされていないマシンは、ユーザーが電源を切った後に自動的に再起動します。この動作により、ワークロードをより早く処理できるようになります。これは、`Set-BrokerDesktopGroup`の`AutomaticRestartForUntaggedMachines`プロパティを使用して、デスクトップグループごとに有効または無効にできます。詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

例のシナリオ

次のシナリオを想定します。

- **マシンカタログ構成**。2つのマシンカタログ（C1とC2）があります。
  - カタログC1には、オンプレミス展開にローカルな5台のマシン（M1～M5）が含まれています。
  - カタログC2には、クラウド展開にリモートな5台のマシン（M6～M10）が含まれています。
- **タグ制限**。「Cloud」という名前のタグが作成され、カタログC2内のマシンM6～M10に適用されます。
- **ゾーン構成**。2つのゾーン（Z1とZ2）が作成されます。
  - カタログC1を含むゾーンZ1は、オンプレミス展開に対応します。
  - カタログC2を含むゾーンZ2は、クラウド展開に対応します。
- **デリバリーグループ構成**

  - デリバリーグループには10台のマシン（M1～M10）が含まれており、そのうち5台はカタログC1（M1～M5）から、残りの5台はカタログC2（M6～M10）からのものです。
  - マシンM1からM5は手動で電源がオンにされ、スケジュール期間中ずっと電源がオンのままになります。

- **Autoscale構成**
  - 容量バッファは10%に設定されています。
  - Autoscaleは「Cloud」タグを持つマシンのみを電源管理します。この場合、Autoscaleはクラウドマシン M6からM10を電源管理します。

- **公開アプリケーションまたはデスクトップの構成**。公開デスクトップ（例）にはゾーン設定が構成されており、ユーザーの起動リクエストではゾーンZ2よりもゾーンZ1が優先されます。
  - ゾーンZ1は、公開デスクトップの優先ゾーン（ホームゾーン）として構成されています。

このシナリオは、次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. 利用可能なすべてのオンプレミス・マシンが消費されるまで、ユーザーセッションはさらに増加します。
4. さらに多くのユーザーセッションが開始されます。
5. セッション終了によりユーザーセッションが減少します。
6. セッション負荷がオンプレミス・マシンのみで処理されるまで、ユーザーセッションはさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - オンプレミス環境のマシンM1～M5はすべて電源がオンになっています。
  - クラウド内のマシン1台（例: M6）の電源がオンになっています。このマシンは、構成されたキャパシティバッファによって電源がオンになっています。この場合、10（マシン数）x 10,000（負荷インデックス）x 10%（構成されたキャパシティバッファ）は10,000に等しくなります。したがって、マシン1台の電源がオンになります。
  - 電源がオンになっているすべてのマシン（M1～M6）の負荷インデックス値は、ベースライン負荷（負荷インデックスは0）です。
- ユーザーがログオンします

    - セッションは、構成されたゾーン設定を通じてマシンM1～M5でホストされるように指示され、これらのオンプレミス環境のマシン間で負荷分散されます。
    - 電源がオンになっているマシン（M1～M5）の負荷インデックス値が増加します。
    - 電源がオンになっているマシンM6の負荷インデックス値は、ベースライン負荷です。
- ユーザーが負荷を増やし、すべてのオンプレミスリソースを消費します
    - セッションは、構成されたゾーン設定を通じてマシンM1～M5でホストされるように指示され、これらのオンプレミス環境のマシン間で負荷分散されます。
    - 電源がオンになっているすべてのマシン（M1～M5）の負荷インデックス値は10,000に達しました。
    - 電源がオンになっているマシンM6の負荷インデックス値は、ベースライン負荷のままです。
- もう1人のユーザーがログオンします
    - セッションはゾーン設定を超過し、クラウドマシンM6でホストされるように指示されます。
    - 電源がオンになっているすべてのマシン（M1～M5）の負荷インデックス値は10,000に達しました。
    - 電源がオンになっているマシンM6の負荷インデックス値が増加し、ベースライン負荷ではなくなります。総予備容量が負荷インデックスで10,000を下回ると、構成されたキャパシティバッファにより、Autoscaleは需要を満たすため追加のマシン（M7）の電源をオンにし始めます。マシンM7の電源がオンになるまでには時間がかかる場合があることに注意してください。そのため、マシンM7が準備できるまでに遅延が発生する可能性があります。
- さらに多くのユーザーがログオンします
    - セッションはマシンM6でホストされるように指示されます。
    - 起動中のすべてのマシン（M1～M5）のロードインデックス値が10,000に達しました。
    - 起動中のマシンM6のロードインデックス値はさらに増加しますが、総予備容量はロードインデックスに関して10,000を超えるレベルにあります。
    - 起動中のマシンM7のロードインデックス値はベースライン負荷のままです。
- さらに多くのユーザーがログオンします。
    - マシンM7の準備が整うと、セッションはマシンM6とM7でホストされるように指示され、これらのマシン間で負荷分散されます。

    - 起動中のすべてのマシン（M1～M5）のロードインデックス値が10,000に達しました。
    - マシンM7のロードインデックス値は、もはやベースライン負荷ではありません。
    - 起動中のマシン（M6とM7）のロードインデックス値が増加します。
    - 総予備容量は、ロードインデックスに関して依然として10,000を超えるレベルにあります。

- セッション終了によりユーザーセッション負荷が減少します。
    - ユーザーがセッションからログオフしたり、アイドルセッションがタイムアウトしたりすると、マシンM1～M7で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
    - ロードインデックスに関して総予備容量が10,000を超えるレベルに増加すると、Autoscaleはクラウドマシン（M6～M7）のいずれかをドレイン状態にします。その結果、新しい変更（たとえば、ユーザー負荷が再び増加したり、他のクラウドマシンの負荷が最も低くなったりする）が発生しない限り、他のユーザーが開始したセッションはそのマシン（たとえばM7）に転送されなくなります。
- 1つ以上のクラウドマシンが不要になるまで、ユーザーセッション負荷はさらに減少します。
    - M7マシン上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、AutoscaleはM7マシンを電源オフにします。
    - 電源オン状態のすべてのマシン（M1からM5）の負荷インデックス値は、10,000を下回るレベルまで低下する可能性があります。
    - 電源オン状態のマシン（M6）の負荷インデックス値は減少します。
- クラウドマシンが不要になるまで、ユーザーセッションはさらに減少します。
    - M6マシンにユーザーセッションがないにもかかわらず、Autoscaleは予備容量として予約されているため、それを電源オフにしません。
    - Autoscaleは、設定された容量バッファのため、残りのクラウドマシンM6を電源オンのままにします。そのマシンは、着信するユーザーにデスクトップを提供するのを待機しています。
    - オンプレミス環境のマシンに利用可能な容量がある限り、セッションはM6マシンでホストされるように指示されません。

ユーザーログオフ通知（旧称：強制ユーザーログオフ）

> **重要:**

> この機能は、マルチセッションアプリベースのデリバリーグループ向けのAutoscale™ユーザーインターフェイスでのみ利用可能です。

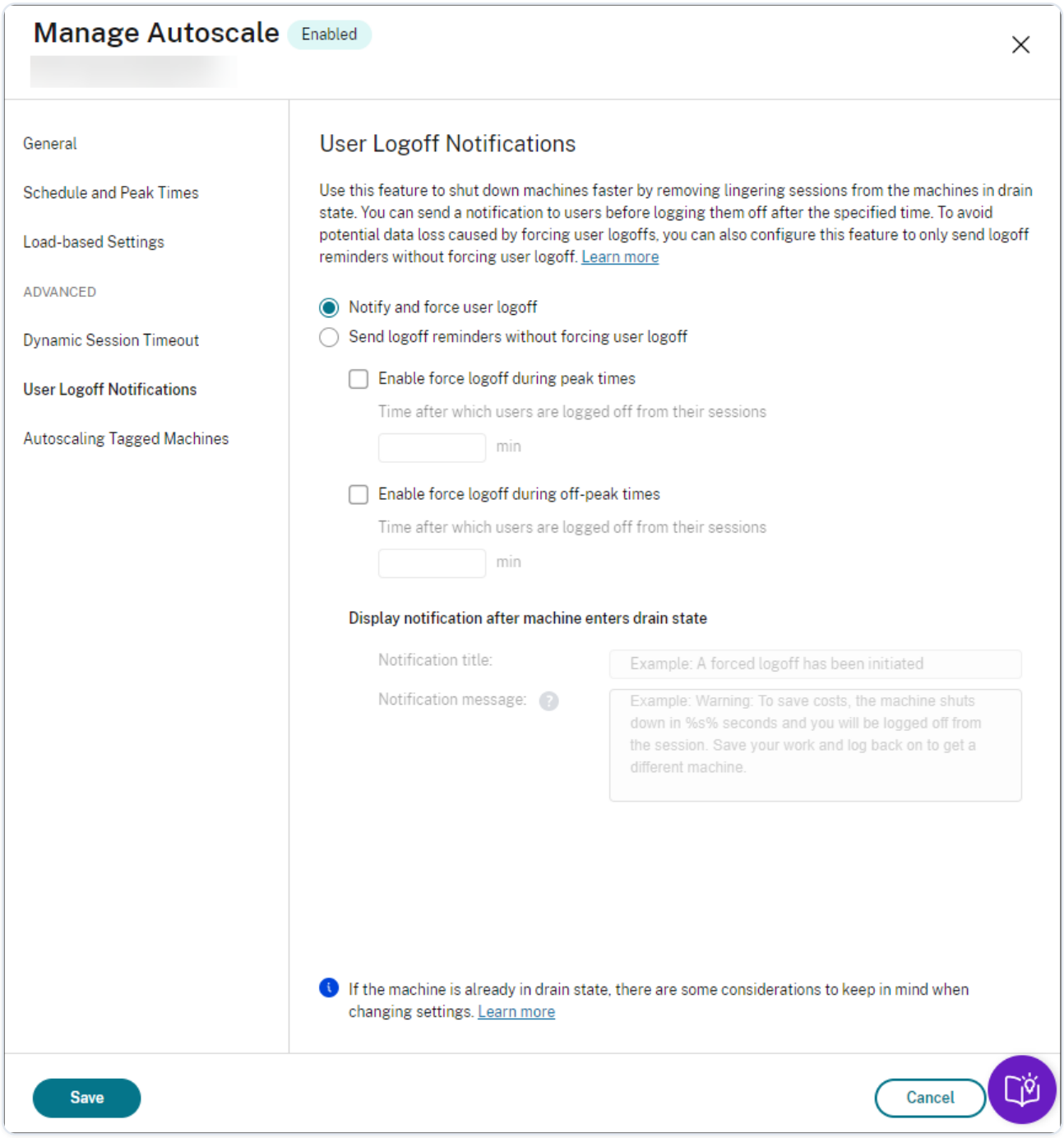
> コスト削減をより効果的に実現するため、Autoscaleでは残存セッションを強制的にログオフできます。これは、ユーザーにカスタム通知を送信し、その猶予期間が経過した後にセッションを強制的にログオフすることで行われます。これは、ドレイン状態のマシンに対してのみ行われ、すべての電源オンのマシンに対して行われるわけではありません。ユーザーの強制ログオフによって発生する可能性のあるデータ損失を避けるため、この機能をユーザーの強制ログオフなしでログオフリマインダーのみを送信するように構成することもできます。

以下の2つのオプションがあります。

- **ユーザーに通知して強制ログオフ**
- **ユーザーを強制ログオフせずにログオフリマインダーを送信**

ユーザーに通知して強制ログオフ

選択した場合、Autoscaleは以下の指定された時間が経過した後、ユーザーをセッションからログオフします。



ピーク時の強制ログオフを有効にする。選択した場合、指定された時間が経過すると、Autoscaleはピーク時にそれらのユーザーをセッションからログオフします。

オフピーク時の強制ログオフを有効にする。選択した場合、指定された時間が経過すると、Autoscaleはオフピーク時にそれらのユーザーをセッションからログオフします。

マシンがドレイン状態になった後に通知を表示。マシンがドレイン状態になった後、ユーザーに通知を送信できます。

- **通知のタイトル**。ユーザーに送信する通知のタイトルを指定できます。例: `A forced logoff has been initiated.`.

- **通知メッセージ**。ユーザーに送信する通知の内容を指定できます。メッセージ内で指定された時間を示す変数として、%s% または %m% を使用できます。時間を秒で表すには %s% を使用し、分で表すには %m% を使用します。例: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`.

ユーザーのログオフを強制せずにログオフリマインダーを送信する

このオプションを選択すると、マシンがドレイン状態になった後、ユーザーはマシンからログオフするようリマインダーを受け取ります。このリマインダーは、以下で指定された間隔で送信されるように構成できます。

AutoscaleマルチセッションOS - ログオフリマインダーを送信する(/en-us/citrix-virtual-apps-desktops/2311/media/autoscale-logoff-reminder-ms.png)

ピーク時にユーザーにリマインダーを送信する。このオプションを選択すると、ユーザーはピーク時にX分ごとにセッションからログオフするようリマインダーを受け取ります（Xは指定された時間を表します）。

オフピーク時にユーザーにリマインダーを送信する。このオプションを選択すると、ユーザーはオフピーク時にX分ごとにセッションからログオフするようリマインダーを受け取ります（Xは指定された時間を表します）。

ログオフリマインダー。マシンがドレイン状態になった後、ユーザーに送信されるリマインダーを構成できます。

- **リマインダーのタイトル**。ユーザーに送信されるリマインダーのタイトルを指定できます。例：`Please log off from your session`。
- **リマインダーメッセージ**。ユーザーに送信されるメッセージを指定できます。例：`Please log off from your session and log back on to save costs`。

考慮事項

マシンがすでにドレイン状態である場合、設定を変更する際には以下を考慮してください。

- 設定を**ユーザーのログオフを強制せずにログオフのリマインダーを送信する**から**通知してユーザーのログオフを強制する**に変更すると、新しい設定はすぐに有効になります。
- 設定を**通知してユーザーのログオフを強制する**から**ユーザーのログオフを強制せずにログオフのリマインダーを送信する**に変更しても、新しい設定はマシンが次にドレイン状態になるまで有効になりません。ユーザーは引き続きログオフを強制されます。

Broker PowerShell SDKコマンド

Broker PowerShell SDKを使用して、デリバリーグループのAutoscaleを構成できます。PowerShellコマンドを使用してAutoscaleを構成するには、PowerShell SDKバージョン7.21.0.12以降を使用する必要があります。PowerShell SDKの詳細については、「SDKとAPI」(/ja-jp/citrix-virtual-apps-desktops/2311/sdk-api.html)を参照してください。

Set-BrokerDesktopGroup

既存のBrokerDesktopGroupを無効または有効にするか、その設定を変更します。このcmdletの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

例

PowerShell cmdletの使用方法の詳細については、以下の例を参照してください。

Autoscale™を有効にする

- 「MyDesktop」という名前のデリバリーグループでAutoscaleを有効にしたいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -AutoscalingEnabled $true`

ピーク時とオフピーク時で容量バッファを個別に構成する

- 「MyDesktop」という名前のデリバリーグループで、容量バッファをピーク時に20%、オフピーク時に10%に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10`

when disconnected timeout設定を構成する

- 「MyDesktop」という名前のデリバリーグループで、**when disconnected timeout**値をピーク時に60分、オフピーク時に30分に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30`

ログオフ時のタイムアウト設定を構成する

- 「MyDesktop」という名前のデリバリーグループに対して、ピーク時には60分、オフピーク時には30分に**ログオフ時のタイムアウト**値を設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

電源オフ遅延設定を構成する

- 「MyDesktop」という名前のデリバリーグループに対して、電源オフ遅延を15分に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PowerOffDelay 15`

電源オフ遅延が適用されない期間を構成する

- 「MyDesktop」という名前のデリバリーグループに対して、電源オフ遅延が30分経過するまで適用されるようにしたいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -SettlementPeriodBeforeAutoShutdown 30`。

マシンインスタンスコスト設定を構成する

- 「MyDesktop」という名前のデリバリーグループに対して、1時間あたりのマシンインスタンスコストを0.2ドルに設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -MachineCost 0.2`

New-BrokerPowerTimeScheme

デリバリーグループのBrokerPowerTimeSchemeを作成します。詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/>`を参照してください。

例

UID値が3のデリバリーグループに対して、電力時間スキームを作成したいとします。新しいスキームは週末、月曜日、火曜日を対象とします。午前8時から午後6時30分までの時間帯は、スキームに含まれる日のピーク時間として定義されます。ピーク時間帯のプールサイズ（電源がオン

のまま維持されるマシンの数）は20です。オフピーク時間帯は5です。`Set-BrokerDesktopGroup` PowerShellコマンドを使用できます。例：

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

動的セッションタイムアウトのパラメーター

以下のBroker PowerShell SDKコマンドレットは、複数の新しいパラメーターをサポートすることで、動的セッションタイムアウト用に拡張されました。

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

これらのパラメーターには以下が含まれます。

- **DisconnectPeakIdleSessionAfterSeconds** – ピーク時間中にアイドルセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時間中の関連動作が無効になっていることを示します。0より大きい値は、ピーク時間中のみデリバリーグループの動作を有効にします。
- **DisconnectOffPeakIdleSessionAfterSeconds** - オフピーク時間中にアイドルセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク中の関連動作が無効になっていることを示します。0より大きい値は、オフピーク時間中のみデリバリーグループの関連動作を有効にします。
- **LogoffPeakDisconnectedSessionAfterSeconds** - ピーク時に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの関連動作を有効にします。
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - オフピーク時に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク時の関連動作が無効になっていることを示します。0より大きい値は、オフピーク時のみデリバリーグループの関連動作を有効にします。

例

「MyDesktop」という名前のデリバリーグループについて、ピーク時にアイドルセッションタイムアウトを3,600秒に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -DisconnectOffPeakIdleSessionAfterSeconds 3600`

これにより、「MyDesktop」という名前のデスクトップグループのオフピーク時に、1時間以上アイドル状態だったセッションが切断されます。

Citrix Insight Services (シトリックス インサイト サービス)

Citrix Insight Services (CIS) は、計測、テレメトリー、ビジネスインサイト生成のためのCitrixプラットフォームです。その計測およびテレメトリー機能により、技術ユーザー（顧客、パートナー、エンジニア）は問題を自己診断して修正し、環境を最適化できます。CISの機能の詳細と最新情報については、`<https://cis.citrix.com>`を参照してください（Citrixアカウントの資格情報が必要です）。

Citrixにアップロードされるすべての情報は、製品の品質、信頼性、パフォーマンスの向上、およびトラブルシューティングと診断の目的で使用されます。ただし、以下の条件に従います。

- `<https://cis.citrix.com/legal>`にあるCitrix Insight Servicesポリシー
- `<https://www.cloud.com/privacy-policy>`にあるCitrixプライバシーポリシー

このCitrix Virtual Apps and Desktops™リリースは、以下のテクノロジーをサポートしています。

- Citrix Virtual Apps and Desktopsのインストールおよびアップグレード分析
- Citrixカスタマーエクスペリエンス向上プログラム（CEIP）
- Citrix Call Home (シトリックス コール ホーム)
- Citrix Scout (シトリックス スカウト)

CISおよびCitrix Analyticsとは別に、Studioをインストール（またはアップグレード）すると、Google Analyticsが自動的に収集され（その後アップロードされます）。Studioのインストール後、レジストリキーHKLM\\Software\\Citrix\\DesktopStudio\\GAEnabledを使用してこの設定を変更できます。値が1の場合、収集とアップロードが有効になり、0の場合、収集とアップロードが無効になります。

インストールおよびアップグレード分析

フルプロダクトインストーラーを使用してCitrix Virtual Apps and Desktopsコンポーネントを展開またはアップグレードすると、インストールプロセスに関する匿名情報が収集され、コンポーネントをインストール/アップグレードしているマシンに保存されます。このデータは、Citrixが顧客のインストールエクスペリエンスを向上させるために使用されます。

情報は%ProgramData%\\Citrix\\CTQsの下にローカルに保存されます。

このデータの自動アップロードは、フルプロダクトインストーラーのグラフィカルインターフェイスとコマンドラインインターフェイスの両方で、デフォルトで有効になっています。

- レジストリ設定のデフォルト値を変更できます。インストール/アップグレード前にレジストリ設定を変更すると、フルプロダクトインストーラーを使用する際にその値が使用されます。
- コマンドラインインターフェイスでインストール/アップグレードする場合、コマンドでオプションを指定することで、デフォルト設定を上書きできます。

自動アップロードの制御:

- インストール/アップグレード分析の自動アップロードを制御するレジストリ設定（デフォルト = 1）：
  - 場所: `HKLM:\Software\Citrix\MetaInstall`
  - 名前: SendExperienceMetrics
  - 値: 0 = 無効、1 = 有効
- PowerShell を使用すると、次のコマンドレットでインストール/アップグレード分析の自動アップロードを無効にできます。

  ```
  New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
  SendExperienceMetrics -PropertyType DWORD -Value 0
  ```

- XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを無効にするには、`/disableexperiencemetrics` オプションを含めます。

  XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを有効にするには、`/sendexperiencemetrics` オプションを含めます。

Citrix カスタマーエクスペリエンス向上プログラム

Citrixカスタマーエクスペリエンス向上プログラム（CEIP）に参加すると、匿名の統計情報と使用状況情報がCitrixに送信され、Citrix製品の品質とパフォーマンスの向上に役立てられます。詳細については、https://more.citrix.com/XD-CEIPを参照してください。

サイト作成時またはアップグレード時の登録

サイトを作成すると（最初のDelivery Controller™をインストールした後）、CEIPに自動的に登録されます。データの初回アップロードは、サイト作成後約7日後に行われます。

サイト作成後、いつでも参加を停止できます。Web Studioの左ペインで**設定**ノードを選択し、**Citrixカスタマーエクスペリエンス向上プログラム**設定をオフにします。

Citrix Virtual Apps and Desktops 展開をアップグレードする場合:

- CEIPをサポートしていなかったバージョンからアップグレードする場合、参加を希望するかどうか尋ねられます。
- CEIPをサポートしていたバージョンからアップグレードし、参加が有効になっていた場合、アップグレードされたサイトでCEIPが有効になります。
- CEIPをサポートしていたバージョンからアップグレードし、参加が無効になっていた場合、アップグレードされたサイトでCEIPが無効になります。
- CEIPをサポートしていたバージョンからアップグレードし、参加状況が不明な場合、参加を希望するかどうか尋ねられます。

収集された情報は匿名であるため、Citrix Insight Servicesにアップロードされた後は閲覧できません。

VDAインストール時の登録

デフォルトでは、Windows VDAをインストールすると、CEIPに自動的に登録されます。このデフォルトはレジストリ設定で変更できます。VDAをインストールする前にレジストリ設定を変更すると、その値が使用されます。

CEIPへの自動登録を制御するレジストリ設定（デフォルト = 1）：

場所: HKLM: `\\Software\Citrix\Telemetry\CEIP` 名前: Enabled 値: 0 = 無効, 1 = 有効

デフォルトでは、`Enabled` プロパティはレジストリに隠されています。指定されていないままだと、自動アップロード機能が有効になります。

PowerShellを使用すると、次のコマンドレットでCEIPへの登録を無効にできます。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled
-PropertyType DWORD -Value 0
```

収集されたランタイムデータポイントは、定期的にファイルとして出力フォルダー（デフォルト%programdata%/Citrix/VdaCeip）に書き込まれます。

データの初回アップロードは、VDAのインストール後約7日で行われます。

その他の製品およびコンポーネントのインストール時の登録

関連するCitrix製品、コンポーネント、テクノロジー（Citrix Provisioning™、AppDNA、Citrix License Server、Windows用Citrix Workspace™アプリ、Universal Print Server、Session Recordingなど）をインストールする際にも、CEIPに参加できます。インストールと参加のデフォルト値の詳細については、各製品のドキュメントを参照してください。

Citrix コールホーム

Citrix Virtual Apps and Desktopsで特定のコンポーネントや機能をインストールすると、Citrix Call Homeへの参加を求められます。Call Homeは診断データを収集し、そのデータを含むテレメトリパッケージを分析とトラブルシューティングのためにCitrix Insight Servicesに直接（デフォルトポート443のHTTPS経由で）定期的にアップロードします。

Citrix Virtual Apps and Desktopsでは、Call HomeはCitrix Telemetry Serviceという名前のバックグラウンドサービスとして実行されます。詳細については、https://more.citrix.com/XD-CALLHOMEを参照してください。

Call Homeのスケジュール機能はCitrix Scoutでも利用できます。詳細については、Citrix Scoutを参照してください。

収集される情報

Citrix Diagnostic Facility (CDF) のトレースは、トラブルシューティングに役立つ情報をログに記録します。Call Homeは、VDA登録やアプリケーション/デスクトップの起動など、一般的な障害のトラブルシューティングに役立つCDFトレースのサブセットを収集します。このテクノロジーは、常時オンのトレース (AOT) として知られています。AOTログは、C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOTにディスクに保存されます。

Call Homeは、その他のEvent Tracing for Windows (ETW) 情報を収集せず、またそのように構成することもできません。

Call Homeは、次のようなその他の情報も収集します。

- Citrix Virtual Apps and Desktopsによって`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`に作成されたレジストリ。
- Citrix名前空間下のWindows Management Instrumentation (WMI) 情報。
- 実行中のプロセスリスト。
- %PROGRAM DATA%\\Citrix\\CDFに保存されているCitrixプロセスのクラッシュダンプ。
- インストールおよびアップグレード情報。これには、完全な製品メタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFront™ログ、ライセンス互換性チェックログ、および事前サイトアップグレードテストの結果が含まれる場合があります。

トレース情報は収集時に圧縮されます。Citrix Telemetry Serviceは、最大10 MBの圧縮された最新のトレース情報を、最大8日間の時間制限で保持します。

- データを圧縮することで、Call Home は VDA 上で小さなフットプリントを維持できます。
- プロビジョニングされたマシンでの IOP を回避するため、トレースはメモリに保持されます。
- トレースバッファは、メモリ内のトレースを保持するために循環メカニズムを使用します。

Call Home は、Call Home の主要データポイントに記載されている主要なデータポイントを収集します。

構成と管理の概要

フル製品のインストールウィザードを使用しているとき、または後で PowerShell コマンドレットを使用して、Call Home に登録できます。登録すると、デフォルトで、診断情報は毎週日曜日の現地時間午前 3 時頃に収集され、Citrix にアップロードされます。アップロードは、指定された時刻から 2 時間の範囲でランダム化されます。これは、デフォルトのスケジュールを使用するアップロードが午前 3 時から午前 5 時の間に行われることを意味します。

診断情報を定期的にアップロードしたくない場合（またはスケジュールを変更したい場合）は、PowerShell コマンドレットを使用して診断情報を手動で収集してアップロードするか、ローカルに保存することができます。

スケジュールされたCall Homeアップロードに登録する場合、および診断情報を手動でCitrixにアップロードする場合、CitrixアカウントまたはCitrix Cloud™の資格情報を提供します。Citrixは、資格情報を、顧客を識別してデータをアップロードするために使用されるアップロードトークンと交換します。資格情報は保存されません。

アップロードが行われると、Citrix アカウントに関連付けられているアドレスに通知メールが送信されます。

コンポーネントをインストールするときに Call Home を有効にした場合、後で無効にできます。

前提条件

- マシンは PowerShell 3.0 以降を実行している必要があります。
- マシン上で Citrix Telemetry Service が実行されている必要があります。
- システム変数 `PSModulePath` は、Telemetry のインストールパス（例: C:\\Program Files\\Citrix\\Telemetry Service\\.）に設定されている必要があります。

コンポーネントのインストール中に Call Home を有効にする

VDAのインストールまたはアップグレード中: フルプロダクトインストーラーのグラフィカルインターフェイスを使用してVirtual Delivery Agentをインストールまたはアップグレードする際、Call Homeに参加するかどうかを尋ねられます。2つのオプションがあります。

- Call Home に参加する。
- Call Home に参加しない。

VDAをアップグレードしていて、以前にCall Homeに登録していた場合、そのウィザードページは表示されません。

Controllerのインストールまたはアップグレード中: グラフィカルインターフェイスを使用してDelivery Controllerをインストールまたはアップグレードする際、Call Homeに参加するかどうかを尋ねられます。3つのオプションがあります。

Controllerをインストールする際、そのサーバーに「サービスとしてログオン」ポリシー設定が適用されたActive Directory GPOがある場合、インストールウィザードのCall Homeページで情報を構成することはできません。詳細については、CTX218094を参照してください。

Controllerをアップグレードしていて、以前にCall Homeに登録していた場合、参加について尋ねられることはありません。

PowerShellコマンドレット

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

アップロードにプロキシサーバーを使用するには、「プロキシサーバーの構成」を参照してください。

- **スケジュールされたアップロードを有効にする:** 診断コレクションはCitrixに自動的にアップロードされます。カスタムスケジュール用の追加のコマンドレットを入力しない場合、デフォルトのスケジュールが使用されます。

```
$cred = Get-Credential

Enable-CitrixCallHome -Credential $cred
```

スケジュールされたアップロードが有効になっていることを確認するには、`Get-CitrixCallHomeGet-CitrixCallHome`と入力します。有効になっている場合、戻り値は`IsEnabled=True`と`IsMasterImage=False`です。

- **マスターイメージから作成されたマシンに対するスケジュールされたアップロードを有効にする:** マスターイメージでスケジュールされたアップロードを有効にすると、マシンカタログで作成される各マシンを構成する必要がなくなります。

  `Enable-CitrixCallHome -Credential $cred -MasterImage`

  スケジュールされたアップロードが有効になっていることを確認するには、**Get-CitrixCallHome**と入力します。有効になっている場合、戻り値は`IsEnabled=True`と`IsMasterImage=True`です。

- **カスタムスケジュールを作成する:** 診断コレクションとアップロードの毎日または毎週のスケジュールを作成します。

  ```
  $timespan = New-TimeSpan –Hours hours -Minutes minutes

  Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
  -UploadFrequency {Daily|Weekly}
  ```

例:

次のコマンドレットは、毎日夜10時20分にデータをバンドルしてアップロードするスケジュールを作成します。Hoursパラメーターは24時間形式を使用します。`UploadFrequency`パラメーターの値がDailyの場合、`DayOfWeek`パラメーターは指定されていても無視されます。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。上記の例では、`StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`が返されます。

次のコマンドレットは、毎週水曜日の夜10時20分にデータをバンドルしてアップロードするスケジュールを作成します。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed
-UploadFrequency Weekly
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。上記の例では、`StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`が返されます。

Call Homeを無効にする

PowerShellコマンドレットを使用するか、Citrix Scoutを介してCall Homeを無効にできます。

Call Homeのスケジュールされたアップロードが無効になっている場合でも、AOTログは収集され、ディスクに保存されます。(スケジュールされたアップロードが無効になっている場合、AOTログはCitrixに自動的にアップロードされません。) AOTログの収集とローカルストレージを無効にできます。

PowerShellでCall Homeを無効にする

次のコマンドレットを実行すると、診断データはCitrixに自動的にアップロードされません。(Citrix ScoutまたはテレメトリPowerShellコマンドレットを使用して、診断データをアップロードすることは引き続き可能です。)

`Disable-CitrixCallHome`

Call Homeが無効になっていることを確認するには、`Get-CitrixCallHome`と入力します。無効になっている場合、戻り値は`IsEnabled=False`と`IsMasterImage=False`です。

Citrix Scoutを使用して収集スケジュールを無効にする

Citrix Scoutを使用して診断コレクションスケジュールを無効にするには、Schedule collectionsのガイダンスに従ってください。ステップ3で、**Off**をクリックして、選択したマシンのスケジュールをキャンセルします。

AOTログの収集を無効にする

次のコマンドレットを実行した後（`Enabled`フィールドを`false`に設定）、AOTログは収集されません。

`Enable-CitrixTrace -Listen'{"trace":{"enabled":false,"persistDirectory":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300}}'`

`Listen`パラメーターには、JSON形式の引数が含まれています。

Call Homeアップロード用のプロキシサーバーを構成する

Call Homeが有効になっているマシンで、次のタスクを完了します。以下の手順の例の図には、サーバーアドレスとポート10.158.139.37:3128が含まれています。お使いの情報は異なります。

1. ブラウザーにプロキシサーバー情報を追加します。Internet Explorerで、**［インターネットオプション \> 接続 \> LANの設定］の順に選択します。［LANにプロキシサーバーを使用する］**"を選択し、プロキシサーバーのアドレスとポート番号を入力します。
2. PowerShell で `netsh winhttp import proxy source=ie` を実行します。

```
PS C:\Users\administrator.JLGXH> netsh winhttp import proxy source=ie

Current WinHTTP proxy settings:

    Proxy Server(s) :  10.108.124.245:8080
    Bypass List     :  (none)
```

3. テキストエディターを使用して、C:\\Program Files\\Citrix\\Telemetry Serviceにある TelemetryService.exe構成ファイルを編集します。赤枠で示されている情報を追加します。



4. Telemetry Serviceを再起動します。

PowerShell で Call Home コマンドレットを実行します。

診断情報を手動で収集してアップロードする

CIS Webサイトを使用して、診断情報バンドルをCISにアップロードできます。PowerShell コマンドレットを使用して、診断情報を収集し、CISにアップロードすることもできます。

CIS Webサイトを使用してバンドルをアップロードするには:

1. Citrixアカウントの資格情報を使用してCitrix Insight Servicesにログオンします。
2. **My Workspace**を選択します。
3. **Healthcheck**を選択し、データの場所に移動します。

CISは、データアップロードを管理するいくつかのPowerShellコマンドレットをサポートしています。このドキュメントでは、2つの一般的なケースのコマンドレットについて説明します。

- `Start-CitrixCallHomeUpload` コマンドレットを使用して、診断情報バンドルを手動で収集し、CISにアップロードします。（バンドルはローカルに保存されません。）
- `Start-CitrixCallHomeUpload` コマンドレットを使用して、データを手動で収集し、診断情報バンドルをローカルに保存します。これにより、データをプレビューできます。その後、`Send-CitrixCallHomeBundle` コマンドレットを使用して、そのバンドルのコピーをCISに手動でアップロードします。(最初に保存したデータはローカルに残ります。)

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

データをCISにアップロードするコマンドレットを入力すると、アップロードの確認を求められます。アップロードが完了する前にコマンドレットがタイムアウトした場合は、システムイベントログでアップロードのステータスを確認してください。サービスがすでにアップロードを実行している場合、アップロード要求が拒否されることがあります。

データを収集してバンドルをCISにアップロードする:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath string]
[-Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploadHeader string] [-AppendHeaders string] [-Collect string]
[<CommonParameters>]
```

データを収集してローカルに保存する:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
strings] [<CommonParameters>]
```

次のパラメーターが有効です。

- **Credential:** CISへのアップロードを指示します。

- **InputPath:** バンドルに含めるzipファイルの場所。これはCitrixサポートが要求する追加ファイルである可能性があります。.zip拡張子を含めるようにしてください。
- **OutputPath:** 診断情報が保存される場所。このパラメーターは、Call Homeデータをローカルに保存する場合に必須です。
- **説明とインシデント時間:** アップロードに関する自由形式の情報。
- **SRNumber:** Citrix テクニカルサポートのインシデント番号。
- **名前:** バンドルを識別する名前。
- **UploadHeader:** CISにアップロードされたアップロードヘッダーを指定するJSON形式の文字列。
- **AppendHeaders:** CISにアップロードされた追加ヘッダーを指定するJSON形式の文字列。
- **収集:** 収集または省略するデータを指定するJSON形式の文字列。形式は {'collector': {'enabled':Boolean}} で、Boolean は true または false です。 有効なコレクター値は次のとおりです。

  - 'WMI'
  - 'プロセス'
  - 'レジストリ
  - 'クラッシュレポート'
  - 'トレース'
  - 'ファイル'
  - 'MSI'
  - 'ローカルデータ'
  - 'サイトデータ'
  - 'SFB'

  デフォルトでは、「sfb」を除くすべてのコレクターが有効になっています。

  'sfb'コレクターは、Skype for Businessの問題を診断するためにオンデマンドで使用されるように設計されています。「enabled」パラメーターに加えて、「sfb」コレクターはターゲットユーザーを指定するための「account」および「accounts」パラメーターをサポートしています。以下のいずれかの形式を使用してください。

  - "-収集 "`{'sfb':{'account':'domain\\user1'}}`"
  - "-収集 "{'sfb':{'accounts':}}"

- **共通パラメーター:** PowerShellのヘルプを参照してください。

以前にローカルに保存されたデータをアップロードする:

`Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<CommonParameters>]`

`Path` パラメーターは、以前に保存されたバンドルの場所を指定します。

例:

次のコマンドレットは、Call Homeデータ（WMIコレクターからのデータを除く）をCISにアップロードするよう要求します。このデータは、Citrix Provisioning VDAの登録失敗に関するもので、Citrixサポートケース123456について午後2時30分に記録されました。Call Homeデータに加えて、ファイル「c:\\Diagnostics\\ExtraData.zip」がアップロードされるバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:
\Diagnostics\ExtraData.zip" -Description "Registration failures with
Citrix Provisioning VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name
"RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}"
-UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

次のコマンドレットは、午前8時15分に記録されたCitrixサポートケース223344に関連するCall Homeデータを保存します。データはネットワーク共有上のファイルmydata.zipに保存されます。Call Homeデータに加えて、ファイル「c:\\Diagnostics\\ExtraData.zip」が保存されるバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \
\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip"
-Description "Diagnostics for incident number 223344" -IncidentTime "8:15"
-SRNumber 223344
```

以下のコマンドレットは、以前に保存したデータバンドルをアップロードします。

```
$cred=Get-Credential

C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \
\mynetwork\myshare\mydata.zip
```

シトリックス スカウト

はじめに

Citrix Scout は診断情報を収集し、ヘルスチェックを実行します。その結果を使用して、Citrix Virtual Apps and Desktops™ の展開を維持できます。Citrix は、Citrix Insight Services を通じて、診断情報収集の包括的で自動化された分析を提供します。また、Scout を使用して、単独で、または Citrix Support のガイダンスを受けて問題をトラブルシューティングすることもできます。

収集ファイルを Citrix にアップロードして、Citrix Support からの分析とガイダンスを受けることができます。または、収集したデータをローカルに保存して自分で確認し、後でその収集ファイルを Citrix にアップロードして分析することもできます。

Scout は次の手順を提供します。

- **収集:** サイトで選択したマシンに対して、1 回限りの診断情報収集を実行します。その後、ファイルを Citrix にアップロードするか、ローカルに保存できます。
- **トレースと再現:** 選択したマシンで手動トレースを開始します。その後、それらのマシンで問題を再現します。問題を再現した後、トレースは停止されます。その後、Scout は他の診断情報を収集し、ファイルを Citrix にアップロードするか、ローカルに保存します。
- **スケジュール:** 選択したマシンで、指定した時間に毎日または毎週診断情報収集が実行されるようにスケジュールします。ファイルは自動的に Citrix にアップロードされます。
- **ヘルスチェック:** サイトとそのコンポーネントの正常性と可用性を測定するチェックを実行します。Delivery Controller、Virtual Delivery Agent (VDA)、StoreFront™ サーバー、および Citrix License Server のヘルスチェックを実行できます。チェック中に問題が見つかった場合、Scout は詳細なレポートを提供します。Scout が起動するたびに、更新されたヘルスチェックスクリプトがチェックされます。新しいバージョンが利用可能な場合、Scout はそれらを自動的にダウンロードし、次回のヘルスチェック実行時に使用します。

> **注:**
>
> **トレースと再現**、**スケジュール**、および**ヘルスチェック**の手順は、現在 Linux VDA では利用できません。

> この記事で説明されているグラフィカルインターフェイスは、Scout を使用する主要な方法です。または、PowerShell を使用して、1 回限りの診断情報収集またはスケジュールされた

> 診断情報収集とアップロードを構成することもできます。「Call Home」を参照してください。

Scout を実行する場所:

- オンプレミス展開では、Delivery Controller™ から Scout を実行して、1 つ以上のVirtual Delivery Agent (VDA)、Delivery Controller、StoreFront サーバー、および License Server で診断情報を取得したり、チェックを実行したりできます。VDA から Scout を実行して、ローカル診断情報を収集することもできます。
- Citrix DaaS (旧称 Citrix Virtual Apps and Desktops service) を使用する Citrix Cloud 環境では、VDA から Scout を実行してローカル診断情報を収集します。

Scoutアプリケーションのログは`C:\ProgramData\Citrix\TelemetryService\ScoutUI.log`に保存されます。このファイルはトラブルシューティングに使用できます。

収集される情報

Scoutによって収集される診断情報には、Citrix Diagnostic Facility（CDF）トレースログファイルが含まれます。Always-on Tracing（AOT）と呼ばれるCDFトレースのサブセットも含まれます。AOT情報は、VDA登録やアプリケーション/デスクトップの起動などの一般的な問題のトラブルシューティングに役立ちます。その他のEvent Tracing for Windows（ETW）情報は収集されません。

収集される情報には以下が含まれます。

- Citrix Virtual Apps and Desktopsによって`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`の下に作成されたレジストリエントリ。
- **Citrix名前空間**の下のWindows Management Instrumentation（WMI）情報。
- 実行中のプロセス。
- `%PROGRAMDATA%\Citrix\CDF`に保存されているCitrixプロセスのクラッシュダンプ。
- Citrixポリシー情報（CSV形式）。
- インストールおよびアップグレード情報。収集される情報には、製品の完全なメタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFrontログ、ライセンス互換性チェックログ、および予備的なサイトアップグレードテストの結果が含まれる場合があります。

トレース情報について：

- トレース情報は収集時に圧縮されるため、マシン上のフットプリントは小さく保たれます。

- 各マシンでは、Citrix Telemetry Serviceが圧縮された最新のトレース情報を最大8日間保持します。
- Citrix Virtual Apps and Desktops 7 1808以降、AOTトレースはデフォルトでローカルディスクに保存されます。（以前のバージョンでは、トレースはメモリに保持されていました。）デフォルトパス = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`。
- Citrix Virtual Apps and Desktops 7 1811以降、ネットワーク共有に保存されたAOTトレースは、他の診断情報とともに収集されます。
- `Enable-CitrixTrace` cmdletまたは`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry` `DefaultListen`レジストリ文字列を使用して、最大サイズ（デフォルト = 10 MB）とスライス期間を変更できます。
- トレースは、ファイルが`MaxSize`の10%に達するまでファイルに追加されます。

Scoutが収集するデータポイントのリストについては、「Call Home key datapoints」を参照してください。

Scoutの構成

ScoutはLinux VDAで動作するように構成できます。Linux VDAとテレメトリの詳細については、「Integrate with the Citrix Telemetry Service」を参照してください。

Linux VDAは、`ctxtelemetry` ソケットポートまたはテレメトリサービスのポートを自動的に変更する場合があります。その場合、ポートを手動で構成する必要があります。

1. C:\Program Files\Citrix\Telemetry Service に移動します。
2. ScoutUI.exe.config ファイルを開きます。
3. LinuxVDATelemetryServicePort または LinuxVDATelemetryWakeupPort の値を、Linux VDAで構成された値に変更します。

- `<add key="LinuxVDATelemetryServicePort" value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort" value="7503"/>`

1. 変更を保存してファイルを閉じます。
2. 最新の構成がロードされていることを確認するために、Scoutを再度開きます。

ヘルスチェックについて

ヘルスチェックデータは、`C:\ProgramData\Citrix\TelemetryService\`の下のフォルダーに保存されます。

サイトのヘルスチェック

サイト健全性チェックは、FlexCast Management Architecture (FMA) サービスを包括的に評価する環境テストサービスに含まれています。サービスの可用性を確認するだけでなく、これらのチェックはデータベース接続などの他の健全性指標も確認します。

サイトのヘルスチェックはDelivery Controllerで実行されます。サイトの規模によっては、これらのチェックの完了に最大1時間かかる場合があります。

DELIVERY CONTROLLER の構成チェック

サイトの健全性チェックの一環として、Delivery Controller の構成チェックでは、Virtual Apps and Desktops サイトに関する Citrix の推奨事項に基づいて、以下の問題が存在するかどうかを確認します。

- 1 つ以上の Delivery Controller が失敗状態にある。
- サイトに Delivery Controller が 1 つしかない。
- Delivery Controller のバージョンが異なる。

健全性チェックの 権限と要件 を満たすことに加えて、Delivery Controller の構成チェックには以下が必要です。

- 少なくとも1つのControllerが電源オンになっていること。
- Controller上でBroker Serviceが実行されていること。
- ControllerからサイトデータベースへのActive接続。

VDA の健全性チェック

VDA の健全性チェックは、一般的な VDA 登録、セッション起動、およびタイムゾーンリダイレクトの問題の考えられる原因を特定します。

VDA での登録について、Scout は以下をチェックします。

- VDA ソフトウェアのインストール
- VDA マシンのドメインメンバーシップ
- VDA 通信ポートの可用性
- VDA サービスステータス
- Windows ファイアウォール構成
- Controller との通信
- Controller との時刻同期
- VDA 登録ステータス

VDA でのセッション起動について、Scout は以下をチェックします。

- セッション起動通信ポートの可用性
- セッション起動サービスのステータス
- セッション起動 Windows ファイアウォールの構成
- VDA リモートデスクトップサービス クライアントアクセスライセンス
- VDA アプリケーション起動パス
- セッション起動レジストリ設定

VDA でのタイムゾーンリダイレクトについて、Scout は以下をチェックします。

- Windows ホットフィックスのインストール
- Citrix ホットフィックスのインストール
- Microsoft グループポリシー設定
- Citrix グループポリシー設定

VDA 上の Profile Management について、Scout は以下をチェックします。

- ハイパーバイザーの検出
- プロビジョニングの検出
- シトリックス バーチャル アプリおよびデスクトップ
- Personal vDisk の構成
- ユーザー ストア
- Profile Management Service のステータス検出
- Winlogon.exe フックテスト

Profile Management のチェックを実行するには、VDA に Profile Management をインストールして有効にする必要があります。Profile Management の構成チェックの詳細については、Knowledge Center の記事 CTX132805 を参照してください。

StoreFront のヘルスチェック

StoreFront のチェックでは、以下を確認します。

- Citrix Default Domain サービスが実行中であること
- Citrix Credential Wallet サービスが実行中であること
- StoreFront サーバーから Active Directory ポート 88 への接続

- StoreFront サーバーから Active Directory ポート 389 への接続
- ベース URL に有効な FQDN があること
- ベース URL から正しい IP アドレスを取得できること
- IIS アプリケーションプールが .NET 4.0 を使用していること
- 証明書がホスト URL の SSL ポートにバインドされているかどうか
- 証明書チェーンが完全であるかどうか
- 証明書の有効期限が切れているかどうか
- 証明書の有効期限が間もなく切れるかどうか（30 日以内）

ライセンスサーバーのチェック

ライセンスサーバーのチェックでは、以下を確認します。

- Delivery Controllerからのライセンスサーバー接続
- ライセンスサーバーのファイアウォールリモートアクセスステータス
- Citrix Licensingサービスのステータス
- ライセンスサーバーのライセンスキャッシュモードの状態
- ライセンスサーバーのポート接続
- Citrixベンダーデーモン（CITRIX）が実行中であるかどうか
- システムクロックが同期されているかどうか
- Citrix Licensingサービスがローカルサービスアカウントで実行されているかどうか
- `CITRIX.opt`ファイルの存在
- Customer Success Servicesの資格取得日
- シトリックス ライセンス サーバー アップデート
- ライセンスサーバー証明書がDelivery Controllerの信頼されたルートストアにあるかどうか

ヘルスチェックの権限と要件を満たすことに加えて、ライセンスサーバーはドメインに参加している必要があります。そうでない場合、ライセンスサーバーは検出されません。

ヘルスチェックの実行

ヘルスチェックの手順は、マシンの選択、チェックの開始、および結果レポートの確認で構成されます。

1. Scoutを起動します。マシンの**スタート**メニューから、**Citrix > Citrix Scout**を選択します。開いたページで、**Health Check**をクリックします。

2. マシンを選択します。**マシンを検索**をクリックしてマシンを検出します。**マシンの選択**ページには、サイトで検出されたすべてのVDA、Delivery Controller、およびLicense Serverが一覧表示されます。マシン名で表示をフィルターできます。診断情報を収集する各マシンの横にあるチェックボックスをオンにしてから、**続行**をクリックします。

   他のコンポーネントタイプ（StoreFrontサーバーやVDAマシンなど）を追加するには、マシンを手動で追加するおよびVDAマシンをインポートするを参照してください。Citrix Provisioning™ ServerまたはLicense Serverを手動で追加することはできません。

   Scout は、選択された各マシンで検証テストを自動的に起動し、Verification tests に記載されている基準を満たしていることを確認します。検証に失敗した場合、 列にメッセージが表示され、そのマシンのチェックボックスがオフになります。次のいずれかを実行できます。

   - 問題を解決してから、そのマシンのチェックボックスを再度オンにします。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンではヘルスチェックは実行されません。

   検証テストが完了したら、**続行**をクリックします。

3. 選択したマシンでヘルスチェックを実行します。概要には、テストが実行されたマシン（検証テストに合格した選択済みのマシン）が一覧表示されます。**チェック開始**をクリックします。

   チェック中およびチェック後：

   - **ステータス**列は、マシンの現在のチェック状態を示します。
   - 進行中のすべてのチェックを停止するには、ページ右下隅の**チェック停止**をクリックします。（単一マシンのヘルスチェックをキャンセルすることはできず、選択されたすべてのマシンのみが対象です。チェックが完了したマシンからの情報は保持されます。
   - 選択されたすべてのマシンのチェックが完了すると、右下隅の**チェック停止**ボタンが**完了**に変わります。
   - チェックが失敗した場合、**アクション**列の**再試行**をクリックできます。
   - チェックが問題なく完了した場合、**アクション**列は空になります。
   - チェックで問題が検出された場合、**詳細表示**をクリックして結果を表示します。
   - 選択されたすべてのマシンのチェックが完了した後、**戻る**をクリックしないでください。（クリックすると、チェック結果が失われます。）

4. チェックが完了したら、「**完了**」をクリックしてScoutの開始ページに戻ります。

ヘルスチェックの結果

レポートを生成するCitrixチェックの場合、レポートには以下が含まれます。

- 結果レポートが生成された日時
- チェックされたマシン
- ターゲットマシンでチェックが探した条件

権限と要件

権限:

- 診断情報を収集するには:
  - 診断情報を収集する各マシンで、ローカル管理者およびドメインユーザーである必要があります。
  - 各マシンで LocalAppData ディレクトリへの書き込み権限が必要です。
- ヘルスチェックを実行するには:
  - ドメインユーザーグループのメンバーである必要があります。
  - フル管理者であるか、サイトに対して読み取り専用および「**環境テストの実行**」権限を持つカスタムロールを持っている必要があります。
  - スクリプトを実行できるように、スクリプト実行ポリシーを少なくとも`RemoteSigned`に設定します。例: `Set-ExecutionPolicy RemoteSigned`。**注:** 他のスクリプト実行権限でも機能する場合があります。
- Scoutを起動するときは、**管理者として実行**を使用します。

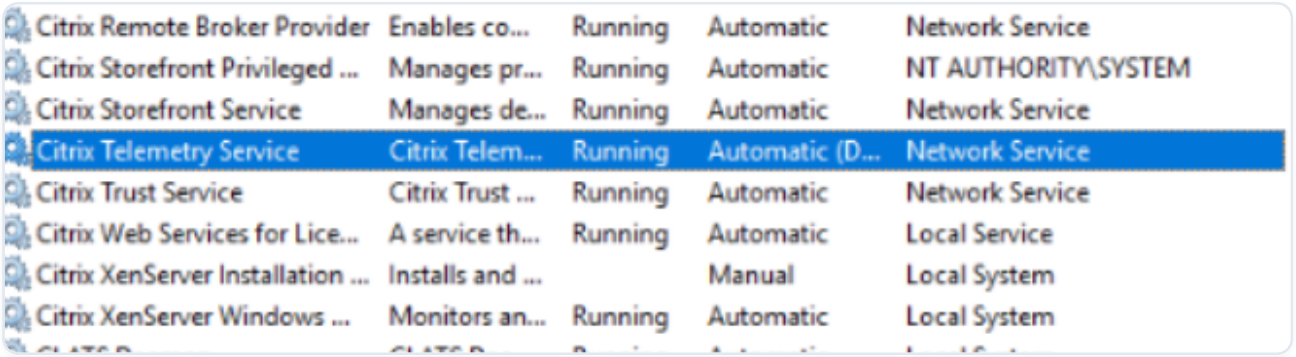
診断情報を収集したり、ヘルスチェックを実行したりする各マシンについて:

- Scoutはマシンと通信できる必要があります。
- ファイルとプリンターの共有が有効になっている必要があります。
- PSRemotingとWinRMが有効になっている必要があります。また、マシンではPowerShell 3.0以降が実行されている必要があります。
- Citrix Telemetry Serviceがマシンで実行されている必要があります。
- Windows Management Infrastructure (WMI)へのアクセスがマシンで有効になっている必要があります。
- 診断収集のスケジュールを設定するには、マシンで互換性のあるScoutバージョンが実行されている必要があります。

パス名で指定されたユーザー名にドル記号 ($) を使用しないでください。診断情報の収集が妨げられます。

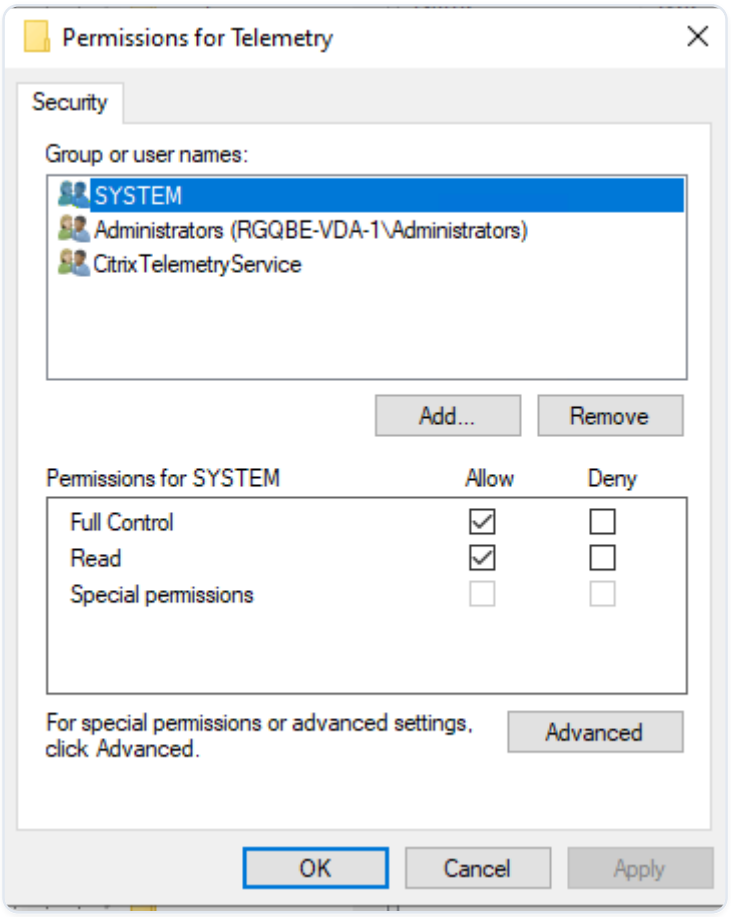
Scoutは、選択したマシンで検証テストを実行し、これらの要件が満たされていることを確認します。

Windows用Telemetry Serviceは、Network Serviceで実行されます。

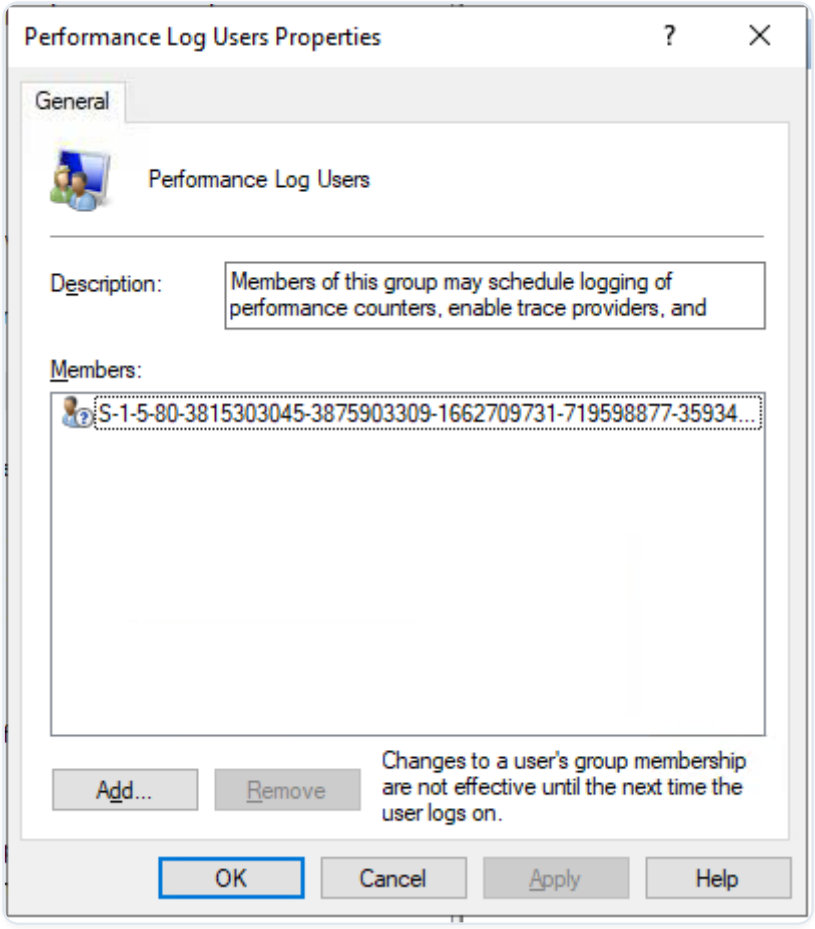


AOTトレースフォルダーは`C:\ProgramData\Citrix\TelemetryService\CitrixAOT`に保存されます。

Administratorグループ、System、およびTelemetry Service SIDのユーザーのみが、`HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry`レジストリにアクセスする権限を持っています。



Telemetry Serviceをアンインストールした後も、Telemetry Service SIDはPerformance Log Usersグループに残りますが、手動で削除できます。



検証テスト

診断コレクションまたはヘルスチェックが開始される前に、選択された各マシンに対して検証テストが自動的に実行されます。これらのテストは、要件が満たされていることを確認します。マシンのテストが失敗した場合、Scoutは推奨される修正措置とともにメッセージを表示します。

- **Scoutはこのマシンに到達できません** - 以下を確認してください。
  - マシンが電源オンになっていること。
  - ネットワーク接続が正常に機能していること。(これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。)
  - ファイルとプリンターの共有がオンになっていること。手順については、Microsoftのドキュメントを参照してください。
- **PSRemotingとWinRMを有効にする** - PowerShellリモート処理とWinRMを同時に有効にできます。**管理者として実行**を使用して、`Enable-PSRemoting`コマンドレットを実行します。詳細については、コマンドレットに関するMicrosoftのヘルプを参照してください。

- **ScoutにはPowerShell 3.0（最小）が必要です** - マシンにPowerShell 3.0（またはそれ以降）をインストールし、PowerShellリモート処理を有効にしてください。
- **このマシン上のLocalAppDataディレクトリにアクセスできません** - アカウントがマシン上のLocalAppDataディレクトリへの書き込み権限を持っていることを確認してください。
- **Citrix Telemetry Serviceが見つかりません** - Citrix Telemetry Serviceがマシンにインストールされ、開始されていることを確認してください。
- **スケジュールを取得できません** - マシンを(最小) XenApp and XenDesktop 7.14にアップグレードしてください。
- **WMIがマシンで実行されていません** - Windows Management Instrumentation (WMI) アクセスが有効になっていることを確認してください。
- **WMI接続がブロックされています** - WindowsファイアウォールサービスでWMIを有効にしてください。
- **Citrix Telemetry Serviceの新しいバージョンが必要です** - (バージョンは、収集とトレースおよび再現の場合にのみチェックされます。) マシン上のTelemetry Serviceのバージョンをアップグレードしてください (「インストールとアップグレード」を参照)。サービスをアップグレードしない場合、そのマシンは**収集**または**トレースおよび再現**アクションに含まれません。
- **Scoutはこのマシン上のsystemdソケットに接続できません** - 以下を確認してください。
  - ポート7503が開いていること。systemd ctxtelemetry.socketがマシン上のポート7503でリッスンしていることを確認してください。ctxtelemetry.socketポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、「Scoutの構成」を参照してください。
  - ネットワーク接続が正常に機能していること。(これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。)
- **このマシンでLinux VDAテレメトリーサービスが開始されていません** - 以下を確認してください。
  - ポート7502が開いていること。Linux VDA Telemetry Serviceがマシンにインストールされ、開始されていることを確認してください。テレメトリサービスポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、「Scoutの構成」を参照してください。
  - ネットワーク接続が正常に機能していること。(これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。)

バージョンの互換性

このバージョンのScout (3.x) は、Citrix Virtual Apps and Desktops (または最低でもXenApp and XenDesktop 7.14) のControllerおよびVDAで実行することを目的としています。

Scoutの以前のバージョンは、7.14より前のXenApp and XenDesktopバージョンで提供されています。以前のバージョンについては、「CTX130147」を参照してください。

7.14より前のControllerまたはVDAをバージョン7.14 (またはそれ以降のサポートされるバージョン) にアップグレードすると、以前のバージョンのScoutは現在のバージョンに置き換えられます。

| 機能 | スカウト 2.23 | スカウト 3.0 | --- | --- | ---| -- | Citrix Virtual Apps and Desktops (および XenApp and XenDesktop 7.14〜7.18) をサポート | はい | はい XenDesktop 5.x、7.1〜7.13をサポート | はい | いいえ XenApp 6.x、7.5〜7.13をサポート | はい | いいえ 製品に同梱 | 7.1〜7.13 | 7.14以降 CTX記事からダウンロード可能 | はい | いいえ CDFトレースをキャプチャ | はい | はい 常時稼働トレース (AOT) をキャプチャする | いいえ | はい 診断データの収集を許可する | 一度に最大10台のマシン (デフォルト) | 無制限 (リソースの可用性による) 診断データをCitrixに送信することを許可する | はい | はい 診断データをローカルに保存することを許可する | はい | はい Citrix Cloud™資格情報をサポートする | いいえ | はい Citrix資格情報をサポート | はい | はい アップロード用のプロキシサーバーをサポート | はい | はい スケジュールを調整 | 該当なし | はい スクリプトのサポート | コマンドライン（ローカルControllerのみ） | Call Homeコマンドレットを使用したPowerShell（Telemetry Serviceがインストールされているすべてのマシン） ヘルスチェック | いいえ | はい データマスキング | いいえ | 3.17以降

インストールとアップグレード

デフォルトでは、VDAまたはControllerをインストールまたはアップグレードする際に、Citrix Telemetry Serviceの一部としてScoutが自動的にインストールまたはアップグレードされます。

VDAのインストール時にCitrix Telemetry Serviceを省略した場合、または後でサービスを削除した場合は、Citrix Virtual Apps and Desktopsインストールメディアの`x64\Virtual Desktop Components`または`x86\Virtual Desktop Components`フォルダーから`TelemetryServiceInstaller_xx.msi`を実行します。

Collectまたは**Trace & Reproduce**アクションを選択すると、マシンが古いバージョンのCitrix Telemetry Serviceを実行している場合に通知されます。Citrixは、最新のサポートされているバージョンを使用することを推奨しています。そのマシンでTelemetry Serviceをアップグレードしない場合、**Collect**または**Trace & Reproduce**アクションには含まれません。Telemetry Serviceをアップグレードするには、インストールと同じ手順を使用します。

アップロードの承認

診断コレクションをCitrixにアップロードする予定がある場合は、CitrixまたはCitrix Cloudアカウントが必要です。（これらは、Citrixダウンロードにアクセスしたり、Citrix Cloud Control Centerにアクセスしたりするために使用する資格情報です。）アカウント資格情報が検証されると、トークンが発行されます。

CitrixアカウントまたはCitrix Cloudアカウントで認証する場合は、リンクをクリックして、デフォルトのブラウザーでHTTPSを使用してCitrix Cloudにアクセスします。Citrix Cloudの資格情報を入力すると、トークンが表示されます。トークンをコピーしてScoutに貼り付けます。その後、Scoutウィザードを続行できます。

トークンは、Scoutを実行しているマシンにローカルに保存されます。次回**Collect**または**Trace & Reproduce**を実行するときにそのトークンを使用できるようにするには、**Store token and skip this step in the future**チェックボックスを選択します。

Scoutの開始ページで**Schedule**を選択するたびに、再承認する必要があります。スケジュールを作成または変更する際には、保存されたトークンを使用できません。

アップロードにプロキシを使用する

Citrixにコレクションをアップロードするためにプロキシサーバーを使用したい場合、Scoutにブラウザのインターネットプロパティで設定されたプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を指定することもできます。

マシンを検索

Collect、**Trace & Reproduce**、および**Schedule**の手順では、Scoutは自動的に検出したControllerとVDAを一覧表示します。

Delivery ControllerからScout Health Checkを実行する場合、**マシンを検索**をクリックして、デリバリーコントローラー、VDA、ライセンスサーバー、StoreFrontサーバーなどのマシンを検出します。

Delivery Controllerではないドメイン参加済みマシンからScout Health Checkを実行する場合、Scoutはマシンを自動的に検出できません。マシンを手動で追加するか、VDAマシンをインポートする必要があります。

マシンを手動で追加

Scout が検出したコントローラーと VDA を一覧表示した後、StoreFront サーバー、ライセンスサーバー、Citrix Provisioning サーバーなど、展開内の他のマシンを手動で追加できます。

ヘルスチェック の実行時：

- ドメイン内の Citrix ライセンスサーバーは自動的に検出されます。ライセンスサーバーを手動で追加することはできません。
- ヘルスチェックは現在、Citrix Provisioning サーバーをサポートしていません。

検出されたマシンを一覧表示するScoutの任意のページで、**+ マシンを追加**をクリックします。追加したいマシンのFQDNを入力し、**続行**をクリックします。必要に応じて、他のマシンを追加するために繰り返します。（FQDNの代わりにDNSエイリアスを入力しても有効に見えることがありますが、ヘルスチェックが失敗する可能性があります。）

手動で追加されたマシンは、常に検出されたマシンよりも上の、マシンリストの先頭に表示されます。

手動で追加されたマシンを識別する簡単な方法は、行の右端にある赤い削除ボタンです。そのボタンがあるのは手動で追加されたマシンだけで、検出されたマシンにはありません。

手動で追加されたマシンを削除するには、行の右端にある赤いボタンをクリックします。削除を確認します。他の手動で追加されたマシンを削除するために繰り返します。

Scout は、手動で追加されたマシンを削除するまで記憶しています。Scout を閉じてから再度開くと、手動で追加されたマシンは引き続きリストの先頭に表示されます。

StoreFront サーバーで **Trace & Reproduce** を使用する場合、CDF トレースは収集されません。ただし、その他のすべてのトレース情報は収集されます。

VDA マシンをインポートする

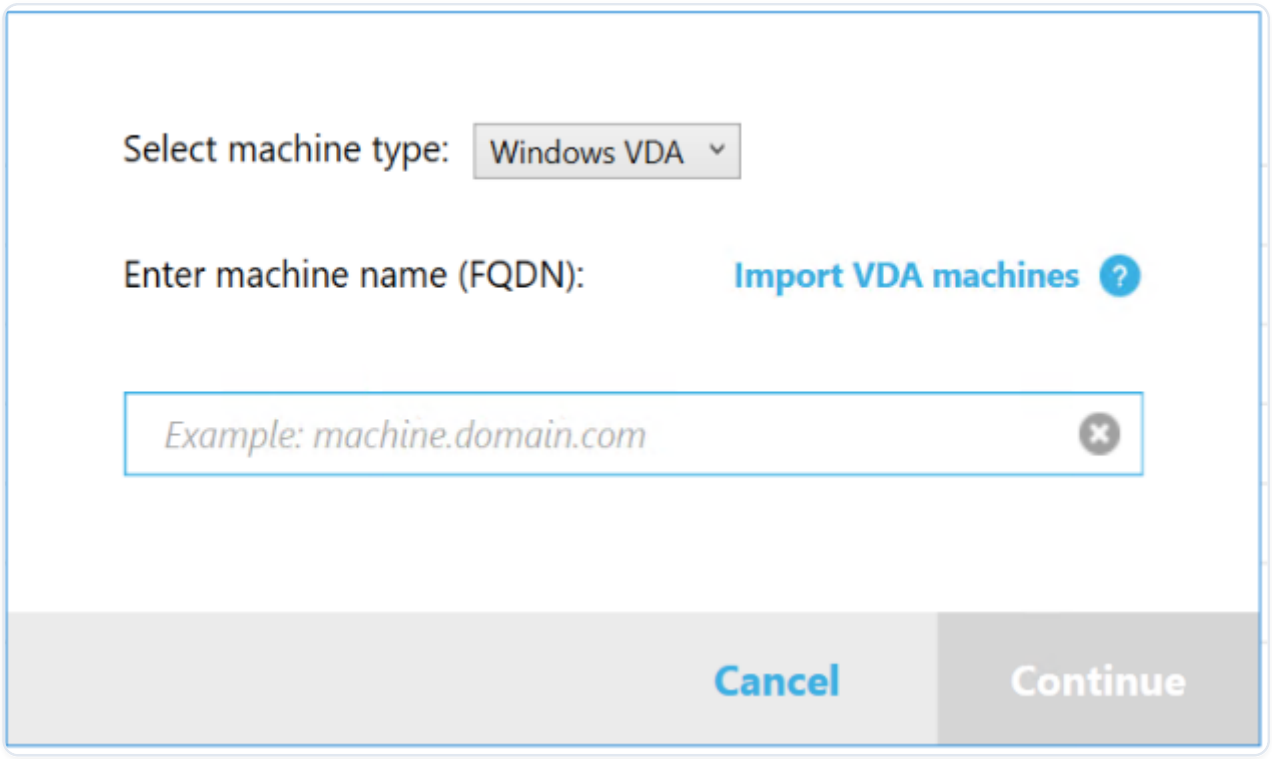
ヘルスチェックを実行する際に、展開環境にVDAマシンをインポートできます。

1. Delivery ControllerまたはConnectorで、PowerShellコマンドを使用してマシンリストファイルを生成します。Connectorでは、ポップアップダイアログでCitrix資格情報を入力し、顧客を選択する必要があります。

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
   ```

2. machineList.txt ファイルを、Scout Health Check を起動するドメイン参加済みマシンにコピーします。
3. Scout Health Check ページで、 をクリックします。
4. マシンタイプを選択します。
5. をクリックします。
6. machineList.txt ファイルを選択します。
7. をクリックします。

インポートされた VDA マシンが Scout Health Check ページに一覧表示されます。



診断情報の収集

収集手順には、マシンの選択、診断収集の開始、その後、収集を含むファイルをCitrixにアップロードするかローカルに保存する作業が含まれます。

1. Scout を起動します。マシンの メニューから、 **>** を選択します。開いたページで、 をクリックします。
2. マシンを選択します。

   - コントローラーでは、**Select machines**ページにサイト内のすべてのVDAとコントローラーが一覧表示されます。マシン名で表示をフィルタリングできます。他のマシン（StoreFrontやCitrix Provisioningサーバーなど）を手動で追加するには、「Add machines manually」を参照してください。
   - その他のコンポーネント（VDAサーバーなど）では、**Select machines**ページにはローカルマシンのみが表示されます。マシンの手動追加はサポートされていません。

   診断を収集する各マシンの横にあるチェックボックスを選択し、**Continue**をクリックします。

   Scoutは、選択された各マシンで検証テストを自動的に起動し、「Verification tests」に記載されている基準を満たしていることを確認します。検証に失敗した場合、**Status**列にメッセージが表示され、そのマシンのチェックボックスは選択解除されます。次のいずれかを実行できます。

- 問題を解決し、そのマシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。
- そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断は収集されません。

検証テストが完了したら、**続行**をクリックします。

3. 診断情報を収集します。概要には、診断情報が収集されるすべてのマシン（検証テストに合格した選択済みのマシン）が一覧表示されます。**収集開始**をクリックします。

   収集中:

   - **Status**列は、マシンの現在の収集状態を示します。
   - 単一マシンでの進行中の収集を停止するには、そのマシンの**Action**列にある**Cancel**をクリックします。
   - 進行中のすべての収集を停止するには、ページの右下隅にある**Stop Collection**をクリックします。収集が完了したマシンからの診断は保持されます。収集を再開するには、各マシンの**Action**列にある**Retry**をクリックします。
   - 選択されたすべてのマシンで収集が完了すると、右下隅にある**Stop Collection**ボタンが**Continue**に変わります。
   - 診断情報を再度収集するには、そのマシンの**アクション**列にある**Collect Again**をクリックします。新しい収集が以前のものを上書きします。
   - 収集が失敗した場合は、**アクション**列にある**Retry**をクリックできます。正常に収集されたもののみがアップロードまたは保存されます。
   - 選択したすべてのマシンで収集が完了したら、**Back**をクリックしないでください。（クリックすると、収集は失われます。）

   収集が完了したら、**続行**をクリックします。

4. コレクションを保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルマシンに保存するかを選択します。

   ファイルを今すぐアップロードする場合は、手順5に進みます。

   ファイルをローカルに保存することを選択した場合:

   - Windowsの**保存**ダイアログボックスが表示されます。目的の場所に移動します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。後でファイルをCitrixにアップロードできます。CTX136396を参照してください。

完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上ステップを完了する必要はありません。

5. アップロードの認証を行い、必要に応じてプロキシを指定します。詳細については、(#upload-authorization)を参照してください。

   - Scoutを介して認証していない場合は、この手順に進みます。
   - Scoutを介して認証済みの場合、保存されている認証トークンがデフォルトで使用されます。これを行う場合は、このオプションを選択して**Continue**をクリックします。この収集の資格情報は求められません。手順6に進みます。
   - 以前に認証済みだが、再認証して新しいトークンを取得したい場合は、**Change/Reauthorize**をクリックしてこの手順に進みます。

   アップロードを認証するためにCitrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで：

   - ファイルアップロードにプロキシサーバーを使用する場合は、 をクリックします。Scoutに、ブラウザのインターネットプロパティに設定されているプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合は、 をクリックします。デフォルトのブラウザがCitrix Cloudページを起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合は、資格情報を入力します。

   完了したら、 をクリックします。

6. アップロードに関する情報を入力します。

   - 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどのコレクションではこれで十分ですが、名前を変更することもできます。(デフォルト名を削除して名前フィールドを空のままにすると、デフォルト名が使用されます。)
   - 必要に応じて、8桁のCitrixサポートケース番号を指定します。
   - オプションの****フィールドに、問題について説明し、該当する場合は問題が発生した時期を示します。

   完了したら、 をクリックします。

アップロード中、ページの左下部分にアップロードの完了パーセンテージが概算で表示されます。進行中のアップロードをキャンセルするには、 をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所にアクセスし、アップロードの分析を表示したり、リンクをコピーしたりできます。

をクリックしてScoutの開始ページに戻ります。

トレースと再現

の手順には、マシンの選択、トレースの開始、問題の再現、診断コレクションの完了、そしてファイルをCitrixにアップロードするかローカルに保存することが含まれます。

この手順は、標準の**収集**手順に似ています。ただし、これによりマシン上でトレースを開始し、それらのマシンで問題を再現できます。すべての診断コレクションには、AOTトレース情報が含まれています。この手順は、トラブルシューティングに役立つCDFトレースを追加します。

1. Scoutを起動します。マシンの「**スタート**」メニューから「**Citrix > Citrix Scout**」を選択します。開始ページで、「**トレースと再現**」をクリックします。
2. マシンを選択します。**マシンの選択**ページには、サイト内のすべてのVDAとControllerが一覧表示されます。マシン名で表示をフィルターできます。トレースと診断を収集する各マシンの横にあるチェックボックスを選択します。次に、**続行**をクリックします。

   他のマシンを手動で追加するには（StoreFrontやCitrix Provisioningサーバーなど）、マシンの手動追加を参照してください。

   Scout は、選択された各マシンで検証テストを自動的に起動し、検証テスト に記載されている基準を満たしていることを確認します。マシンの検証が失敗した場合、**Status** 列にメッセージが投稿され、そのマシンのチェックボックスは選択解除されます。次のいずれかを実行できます。

   - 問題を解決し、そのマシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断情報とトレースは収集されません。

   検証テストが完了したら、**Continue** をクリックします。
3. トレースを開始します。概要には、トレースが収集されるすべてのマシンが一覧表示されます。**Start Tracing** をクリックします。

選択した1台以上のマシンで、発生した問題を再現します。その間、トレースの収集は続行されます。問題の再現が完了したら、Scoutで**続行**をクリックします。これによりトレースが停止します。

トレースを停止した後、トレース中に問題を再現したかどうかを示します。

4. マシンから診断情報を収集します。**Start Collecting** をクリックします。収集中に：

   - **ステータス**列には、マシンの現在の収集状態が表示されます。
   - 単一マシンでの進行中の収集を停止するには、そのマシンの**アクション**列にある**キャンセル**をクリックします。
   - 進行中のすべての収集を停止するには、ページの右下隅にある**収集の停止**をクリックします。収集が完了したマシンからの診断情報は保持されます。収集を再開するには、各マシンの**アクション**列にある**再試行**をクリックします。
   - 選択したすべてのマシンでコレクションが完了すると、右下隅の**コレクションの停止**ボタンが**続行**に変わります。
   - マシンから診断情報を再度収集するには、そのマシンの**アクション**列にある**再収集**をクリックします。新しいコレクションは以前のコレクションを上書きします。
   - コレクションが失敗した場合は、**アクション**列にある**再試行**をクリックできます。正常に完了したコレクションのみがアップロードまたは保存されます。
   - 選択したすべてのマシンでコレクションが完了したら、**戻る**をクリックしないでください。（クリックすると、コレクションは失われます。）

   収集が完了したら、**続行**をクリックします。

5. コレクションを保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルに保存するかを選択します。

   今すぐファイルをアップロードする場合は、手順6に進みます。

   ファイルをローカルに保存する場合：

   - Windowsの保存ダイアログボックスが表示されます。目的の場所を選択します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。注意：ファイルは後でCitrixからアップロードできます。Citrix Insight Servicesについては、CTX136396を参照してください。

   完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上完了する必要のある手順はありません。

6. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロードの承認を参照してください。

   - Scoutを通じて認証していない場合は、この手順に進みます。
   - Scoutを通じて認証済みの場合、保存されている認証トークンがデフォルトで使用されます。これを実行したい場合は、このオプションを選択して**続行**をクリックします。このコレクションの資格情報は求められません。手順7に進みます。
   - 以前に認証済みで、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこの手順に進みます。

   アップロードを認証するために、Citrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで:

   - ファイルアップロードにプロキシサーバーを使用する場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザーのインターネットプロパティで構成されているプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合、**トークンの生成**をクリックします。デフォルトのブラウザーがCitrix Cloudページを起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合は、資格情報を入力します。

   完了したら、**続行**をクリックします。

7. アップロードに関する情報を提供します。

   アップロードの詳細を入力します。

   - 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。名前の変更は可能ですが、ほとんどの収集ではこれで十分です。(デフォルト名を削除して名前フィールドを空のままにした場合でも、デフォルト名が使用されます。)
   - オプションで、8桁のCitrixサポートケース番号を指定します。
   - オプションの「説明」フィールドに、問題について記述し、該当する場合は問題が発生した時期を示します。

   完了したら、**アップロードの開始**をクリックします。

アップロード中、ページの左下部分にアップロードの完了率が概算で表示されます。進行中のアップロードをキャンセルするには、**アップロードの停止**をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所に移動し、アップロードの分析を表示したり、リンクをコピーしたりできます。

完了をクリックして、Scoutの開始ページに戻ります。

追加のログ収集を有効にする

追加ログ収集を有効にする機能を使用すると、perfmon、Netsh、DebugView、Wiresharkなどのツールでトレースおよび再現機能を使用できます。

> **注:**
>
> これはローカルマシンにのみ適用されます。

> 追加のログ収集を設定するには：

1. Citrix Scout を起動します。
2. **設定**ギアをクリックします。
3. **追加ツールによるログ収集を有効にする**をクリックします。
4. **保存**をクリックします。

追加のログを収集するには：

1. Scoutのホームページで、**トレースと再現**をクリックします。
2. **マシンの選択**ページで、ローカルマシンの右側にあるギアをクリックします。
3. **ログ記録に必要なツールを選択してください:** ページで、**ツールのダウンロード**をクリックします。
4. **ツールのダウンロード**ページで、使用したいツールを選択し、**ダウンロード**をクリックします。Wiresharkを除くツールがダウンロードされます。Wiresharkは手動でのみダウンロードおよびインストールできます。 注：他のツールを手動でダウンロードすることを選択した場合、ダウンロードした.zipファイルの内容を`C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\<toolname>`に抽出する必要があります。たとえば、DebugView.zipファイルをダウンロードした場合、ファイルの内容を`C:`

`\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\`に解凍します。

5. **ログ記録に必要なツールを選択してください:** ページで、**ステータスの更新**をクリックします。選択したすべてのツールが、ステータス列の下に**存在**として表示されます。
6. ログ記録用のツールを選択し、**次へ**をクリックします。
7. トレースと再現 の手順に従います。
8. 完了後、zip ファイル内のログを確認します。ログは *CDCLogs* フォルダーに圧縮されています。

> **注:**
>
> トレースに Procmon ツールが選択されている場合、Process Monitor のログはすぐに大きくなる可能性があります。必要なツールのみを選択するようにしてください。ログのサイズは *%temp%\Scout-CDC-Log* で監視することもできます。

コレクションのスケジュール

> **注:**
>
> 現在、コレクションはスケジュールできますが、ヘルスチェックはできません。

> スケジュール手順は、マシンを選択し、スケジュールを設定またはキャンセルすることで構成されます。スケジュールされたコレクションは、Citrixに自動的にアップロードされます。(PowerShellインターフェイスを使用して、スケジュールされたコレクションをローカルに保存できます。(/ja-jp/citrix-virtual-apps-desktops/2311/manage-deployment/cis.html#citrix-call-home)を参照してください。)

1. Scoutを起動します。マシンのスタートメニューから、**Citrix > Citrix Scout**を選択します。開いたページで、**Schedule**をクリックします。
2. マシンを選択します。サイト内のすべてのVDAとControllerが一覧表示されます。マシン名で表示をフィルタリングできます。

   グラフィカルインターフェイスを使用してVDAとコントローラーをインストールしたときに、Call Homeスケジュールを設定した場合 ((/ja-jp/citrix-virtual-apps-desktops/2311/manage-deployment/cis.html#citrix-call-home)を参照)、Scoutはデフォルトでそれらの設定を表示しま

す。このバージョンのScoutを使用して、スケジュールされたコレクションを初めて開始したり、以前に構成したスケジュールを変更したりできます。

コンポーネントのインストール中にマシンごとにCall Homeを有効/無効にした場合でも、Scoutで構成されたスケジュールは、選択したすべてのマシンに影響します。

診断情報を収集する各マシンの横にあるチェックボックスをオンにして、**Continue**をクリックします。

他のマシンを手動で追加するには（StoreFrontまたはCitrix Provisioningサーバーなど）、マシンの手動追加を参照してください。

Scoutは、選択された各マシンで検証テストを自動的に起動し、検証テストの基準を満たしていることを確認します。マシンの検証に失敗した場合、**ステータス**列にメッセージが表示され、そのマシンのチェックボックスがオフになります。次のいずれかを実行できます。

- 問題を解決し、そのマシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。
- そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断（またはトレース）は収集されません。

検証テストが完了したら、**Continue**をクリックします。

概要ページには、スケジュールが適用されているマシンが一覧表示されます。**続行**をクリックします。

3. スケジュールを設定します。診断を収集するタイミングを指定します。注意：スケジュールは、選択されたすべてのマシンに影響します。

   - 選択したマシンに週次スケジュールを設定するには、**週次**をクリックします。曜日を選択します。収集を開始する時刻（24時間形式）を入力します。
   - 選択したマシンに日次スケジュールを設定するには、**日次**をクリックします。収集を開始する時刻（24時間形式）を入力します。
   - 選択したマシンの既存のスケジュールをキャンセルするには（そして別のスケジュールに置き換えない場合）、**オフ**をクリックします。これにより、それらのマシンに対して以前に構成されたすべてのスケジュールがキャンセルされます。

   続行をクリックします。

4. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロード認証を参照してください。注意：Scoutスケジュールを使用している場合、保存されたトークンを使用して認証することはできません。

アップロードを認証するために、Citrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。

資格情報ページで：

- ファイルアップロードにプロキシサーバーを使用する場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザのインターネットプロパティ用に構成されたプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
- Citrix Cloudアカウントの場合、**トークンの生成**をクリックします。デフォルトのブラウザがCitrix Cloudページに起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
- Citrixアカウントの場合、資格情報を入力します。

完了したら、 をクリックします。

設定されたスケジュールを確認します。Scoutの開始ページに戻るには、**完了**をクリックします。

コレクション中、選択された各マシンの Windows アプリケーションログには、コレクションとアップロードに関するエントリが含まれます。

データマスキング

Citrix Scout を使用して収集された診断情報には、セキュリティ上機密性の高い情報が含まれる場合があります。Citrix Scout のデータマスキング機能を使用すると、診断ファイルを Citrix にアップロードする前に、機密データをマスクできます。

Scout のデータマスキングは、IP アドレス、マシン名、ドメイン名、ユーザー名、ハイパーバイザー名、デリバリーグループ名、カタログ名、アプリケーション名、および SID をマスクするように構成されています。

> **注:**
>
> CDF トレースは暗号化されており、マスクできません。
>
> Linux VDA ログは `.tar.gz2` 形式に圧縮されており、マスクできません。

新しい診断情報を収集し、データマスキングを実行する

Citrix Scoutのデータマスキング機能を使用するには、コマンドラインからScoutを起動します。

1. Windowsで、管理者としてコマンドプロンプトを開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. Scoutを起動します: `ScoutUI.exe datamasking`。
4. 「**Collect**」または「**Trace & Reproduce**」をクリックして診断情報を収集します。
5. 収集が完了したら、「**Enable data masking**」を選択します。このオプションはデフォルトで有効になっています。
6. データマスクを構成します。デフォルトのルールを使用することも、ルールをカスタマイズすることもできます。
7. 診断コレクションをアップロードするか保存するかを選択します。
   - 「**Upload the diagnostics collection to Citrix**」を選択すると、マスクされた診断ファイルがCitrixにアップロードされます。
   - 「**Save the diagnostics collection on your local machine**」を選択すると、元の診断情報とマスクされた診断情報の両方が指定された場所に保存されます。

既存の診断情報に対してデータマスキングを実行する

1. Windowsで、コマンドプロンプトを管理者として開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. データマスキングモードでScoutを直接起動します: `ScoutUI.exe datamasking filePath`。
4. 続行するには「Enable data masking」を選択します。このオプションはデフォルトで有効になっています。
5. データマスクを構成します。デフォルトのルールでデータマスキングを実行することも、ルールをカスタマイズすることもできます。
6. 診断コレクションをアップロードするか保存するかを選択します。
   - 「**Upload the diagnostics collection to Citrix**」を選択すると、マスクされた診断ファイルがCitrixにアップロードされます。
   - 「**Save the diagnostics collection on your local machine**」を選択すると、元の診断情報とマスクされた診断情報の両方が指定された場所に保存されます。

マスクされたデータファイルとマッピングファイルの場所

診断コレクションをアップロードまたは保存した後、リンクをクリックして元の診断とマスクされた診断を開き、マッピング情報ファイルを開きます。

使用状況データ収集

Scoutを使用すると、CitrixはGoogle Analyticsを使用して匿名の使用状況データを収集し、将来の製品機能や改善に役立てます。データ収集はデフォルトで有効になっています。

使用状況データの収集とアップロードを変更するには、Scout UIの**Settings**ギアをクリックします。その後、**Yes**または**No**を選択し、**Save**をクリックして情報を送信するかどうかを選択できます。

Scoutの使用状況データ収集(/en-us/citrix-virtual-apps-desktops/2311/media/scout-usage.png)

システム起動時にCitrix Diagnostic Facility (CDF) トレースを収集する

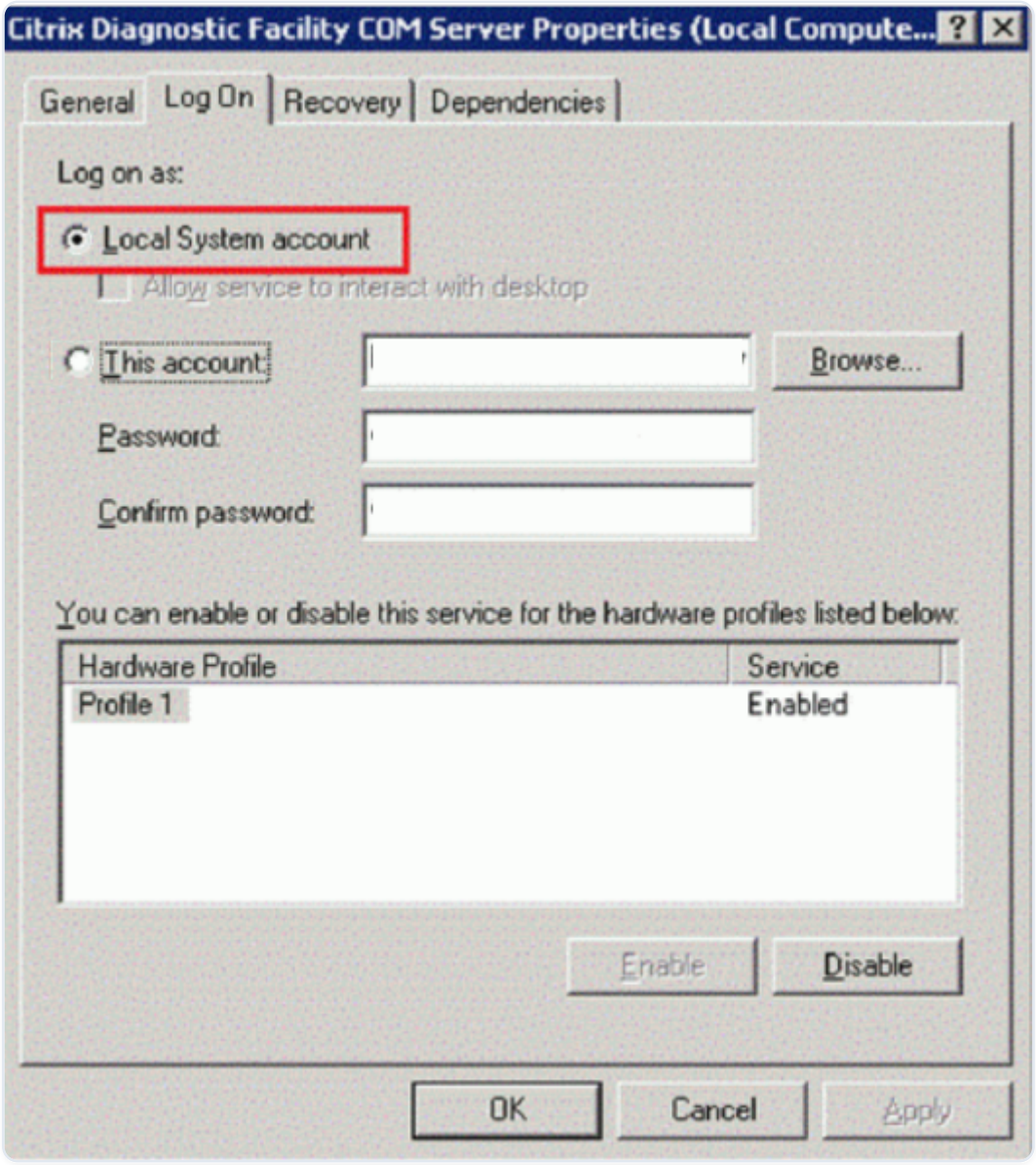
CDFControlユーティリティは、さまざまなCitrixトレースプロバイダーから表示されるCitrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑なCitrix関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集を目的としています。CDFControlユーティリティをダウンロードするには、CTX111961を参照してください。

ローカルシステムアカウントを使用する

CDF COMサーバーサービスにローカルシステムアカウントを使用するには、次の手順を実行します。

1. **スタート**メニューから**ファイル名を指定して実行**をクリックします。
2. ダイアログボックスに `services.msc` と入力し、**OK**をクリックします。
3. **Citrix Diagnostics Facility COM Server**サービスを選択し、**プロパティ**を選択します。

4. **ログオン**タブをクリックし、**ローカルシステム**アカウントを有効にします。次に**OK**をクリックします。



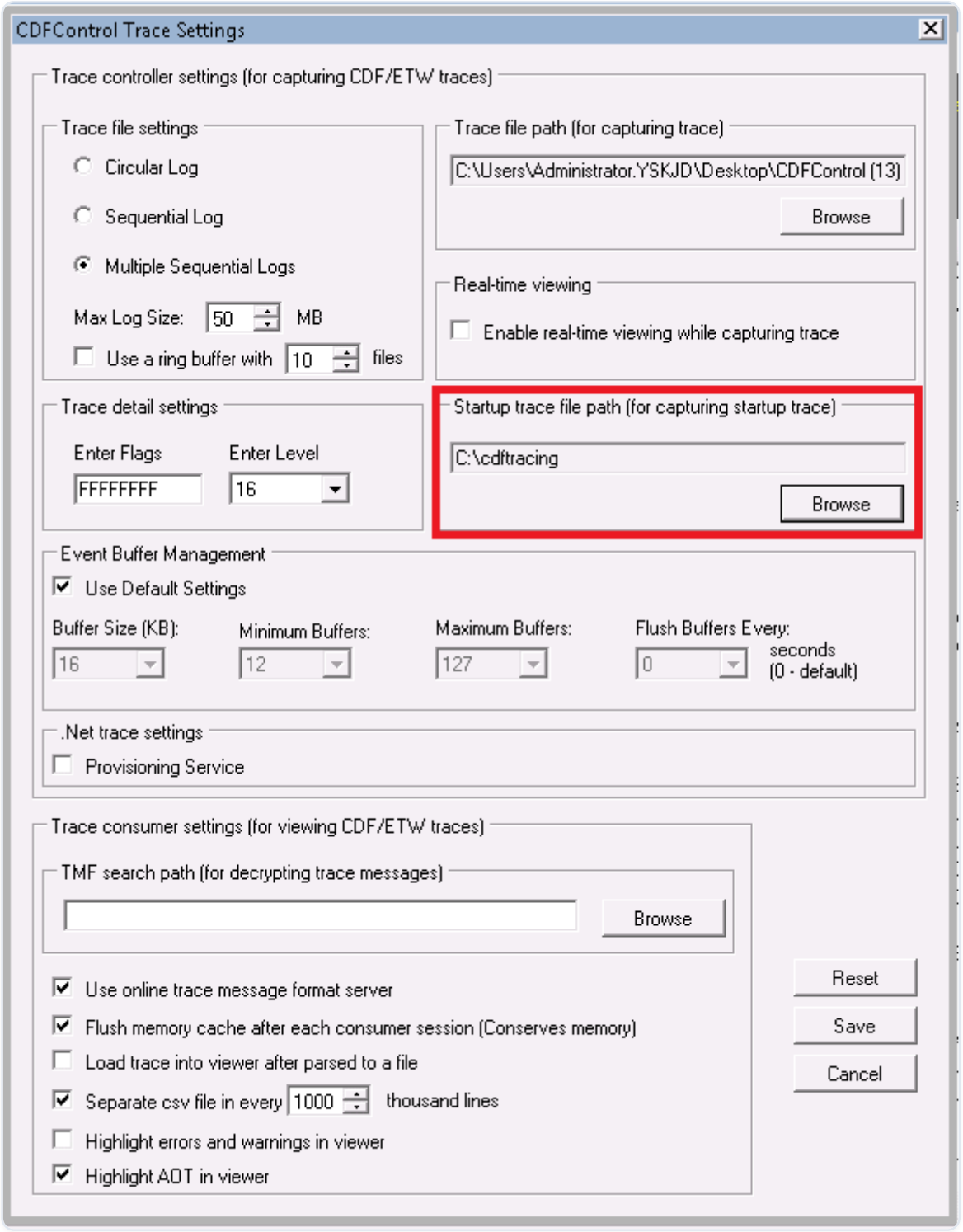
5. サービスを再起動します。

システム起動時にトレースを収集する

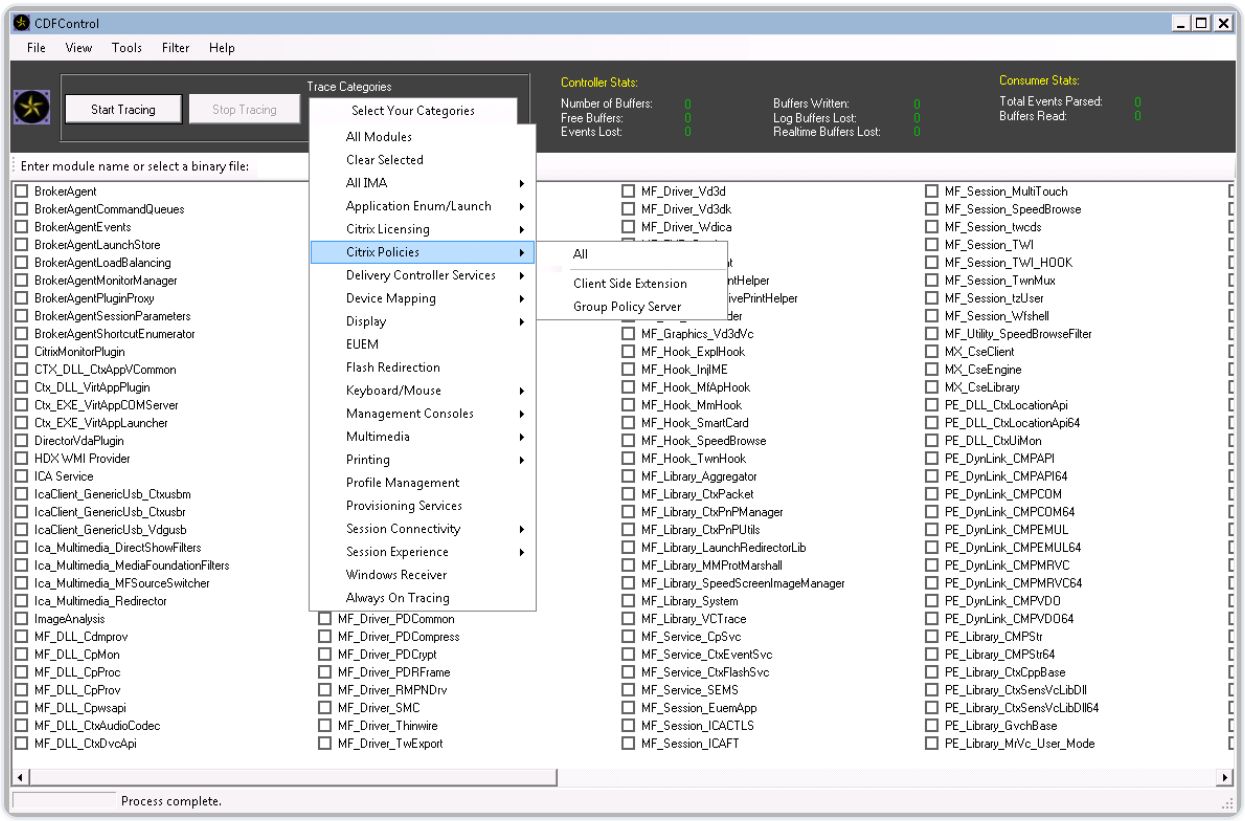
システム起動時にCDFトレースを収集するには、次の手順を使用します。管理者権限が必要です。

1. **CDFControl**を起動し、**ツール**メニューから**オプション**を選択します。

2. **起動トレースをキャプチャするための起動トレースファイルパス**セクションでトレースファイルパスを指定します。次に**保存**をクリックします。



3. Citrixサポートが推奨する**トレースカテゴリ**を選択します。（以下の例では、**Citrix Policies**が選択されています。この選択は単なる例です。トラブルシューティングしている特定の問題に対してプロバイダーを有効にすることをお勧めします。）



4. 「**スタートアップトレース**」を選択し、「**ツール**」メニューから「**有効にする**」を選択します。

   有効にするを選択すると、アニメーションバーがスクロールを開始します。このアクティビティは手順に影響しません。次のステップに進みます。

5. 「**スタートアップトレース**」が有効になったら、「**CDFControlユーティリティ**」を閉じ、システムを再起動します。
6. 「**CDFControl**」ユーティリティを起動します。システムが再起動し、エラーが表示されたら、「**ツール**」メニューから「**スタートアップトレース**」を選択し、「**無効にする**」をクリックして、スタートアップトレースを無効にします。
7. 「**Citrix Diagnostics Facility COM**」サーバーサービスを停止します。
8. ステップ2で指定されたトレースファイルのパスに移動し、分析のためにトレースログファイル（.etl）を収集します。
9. 「**Citrix Diagnostics Facility COM**」サーバーサービスを開始します。

委任管理

> **注:**

Citrix Virtual Apps and Desktops™の展開は、Web Studio (Webベース) とCitrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

委任管理モデルは、ロールベースおよびオブジェクトベースの制御を使用して、組織が管理アクティビティを委任したい方法に合わせた柔軟性を提供します。委任管理はあらゆる規模の展開に対応し、展開の複雑さが増すにつれて、より詳細な権限を設定できます。委任管理では、管理者、ロール、スコープの3つの概念を使用します。

- **管理者:** 管理者は、Active Directoryアカウントによって識別される個人またはグループを表します。各管理者は、1つ以上のロールとスコープのペアに関連付けられています。
- **ロール:** ロールは職務を表し、それに関連付けられた定義済みの権限を持ちます。たとえば、デリバリーグループ管理者ロールには、「デリバリーグループの作成」や「デリバリーグループからのデスクトップの削除」などの権限があります。管理者はサイトに対して複数のロールを持つことができるため、ある人物がデリバリーグループ管理者とマシンカタログ管理者を兼ねることができます。ロールは組み込みまたはカスタムにできます。

  組み込みロールは次のとおりです。

ロール	権限
フル管理者	すべてのタスクと操作を実行できます。フル管理者は常に「すべてのスコープ」と組み合わされます。
読み取り専用管理者	グローバル情報に加えて、指定されたスコープ内のすべてのオブジェクトを表示できますが、何も変更することはできません。たとえば、Scope=Londonの読み取り専用管理者は、すべてのグローバルオブジェクト（構成ログなど）とLondonスコープのオブジェクト（Londonデリバリーグループなど）を表示できます。ただし、その管理者はNew Yorkスコープのオブジェクトを表示できません（LondonとNew Yorkのスコープが重複しないと仮定した場合）。
ヘルプデスク管理者	デリバリーグループを表示し、それらのグループに関連付けられたセッションとマシン

ロール	権限
	を管理できます。監視対象のデリバリーグループのマシンカタログとホスト情報を表示できます。また、それらのデリバリーグループ内のマシンに対してセッション管理およびマシン電源管理操作を実行できます。
マシンカタログ管理者	マシンカタログを作成および管理し、それらのマシンをプロビジョニングできます。仮想化インフラストラクチャ、Provisioning Services、および物理マシンからマシンカタログを構築できます。この役割は、ベースイメージの管理とソフトウェアのインストールはできますが、アプリケーションやデスクトップをユーザーに割り当てることはできません。
デリバリーグループ管理者	アプリケーション、デスクトップ、およびマシンを配信できます。関連するセッションも管理できます。ポリシーや電源管理設定など、アプリケーションとデスクトップの構成も管理できます。
ホスト管理者	ホスト接続とそれに関連するリソース設定を管理できます。マシン、アプリケーション、またはデスクトップをユーザーに配信することはできません。

特定の製品エディションでは、組織の要件に合わせてカスタム役割を作成し、より詳細な権限を委任できます。カスタム役割を使用して、コンソール内のアクションまたはタスクの粒度で権限を割り当てることができます。

- **スコープ:** スコープはオブジェクトのコレクションを表します。スコープは、組織に関連する方法でオブジェクトをグループ化するために使用されます（たとえば、営業チームが使用するデリバリーグループのセット）。オブジェクトは複数のスコープに属することができます。オブジェクトに1つ以上のスコープがラベル付けされていると考えることができます。「すべて」という組み込みスコープが1つあり、すべてのオブジェクトが含まれています。フル管理者ロールは常に「すべて」スコープとペアになります。

例

XYZ社は、部門（経理、営業、倉庫）とデスクトップオペレーティングシステム（Windows 7またはWindows 8）に基づいてアプリケーションとデスクトップを管理することにしました。管理者は5つのスコープを作成し、各デリバリーグループに2つのスコープをラベル付けしました。1つは使用される部門用、もう1つは使用されるオペレーティングシステム用です。

次の管理者が作成されました。

管理者	ロール	スコープ
domain/fred	フル管理者	すべて (フル管理者ロールには常にすべてのスコープがあります)
domain/rob	読み取り専用管理者	すべて
domain/heidi	読み取り専用管理者、ヘルプデスク管理者	すべての営業
domain/warehouseadmin	ヘルプデスク管理者	倉庫
domain/peter	デリバリーグループ管理者、マシンカタログ管理者	Win7

- Fredはフル管理者であり、システム内のすべてのオブジェクトを表示、編集、削除できます。
- Rob はサイト内のすべてのオブジェクトを表示できますが、編集または削除はできません。
- ハイジはすべてのオブジェクトを表示でき、Sales スコープ内のデリバリーグループでヘルプデスクタスクを実行できます。これにより、彼女はそれらのグループに関連付けられているセッションとマシンを管理できますが、マシンの追加や削除など、デリバリーグループに変更を加えることはできません。
- warehouseadmin Active Directory セキュリティグループのメンバーであれば誰でも、Warehouse スコープ内のマシンを表示し、ヘルプデスクタスクを実行できます。
- ピーターは Windows 7 のスペシャリストであり、すべての Windows 7 マシンカタログを管理でき、どの部署スコープに属していても Windows 7 アプリケーション、デスクトップ、マシンを配信できます。管理者はピーターを Win7 スコープのフル管理者にする検討をしました。しかし、フル管理者は「サイト」や「管理者」など、スコープが設定されていないすべてのオブジェクトに対しても完全な権限を持つため、この案は却下されました。

委任管理の使用方法

一般に、管理者の数と権限の粒度は、展開の規模と複雑さによって異なります。

- 小規模な展開や概念実証の展開では、1人または数人の管理者がすべての作業を行います。委任はありません。この場合、各管理者を、All スコープを持つ組み込みのフル管理者ロールで作成します。
- マシン、アプリケーション、デスクトップが多い大規模な展開では、より多くの委任が必要です。複数の管理者が、より具体的な機能的責任（ロール）を持つ場合があります。たとえば、2人がフル管理者で、他の管理者がヘルプデスク管理者である場合があります。また、管理者はマシンカタログなど、特定のオブジェクトグループ（スコープ）のみを管理する場合があります。この場合、新しいスコープを作成し、組み込みロールのいずれかと適切なスコープを持つ管理者を作成します。
- さらに大規模な展開では、より多くの（またはより具体的な）スコープ、および型にはまらないロールを持つ異なる管理者が必要になる場合があります。この場合、スコープを編集または追加し、カスタムロールを作成し、組み込みロールまたはカスタムロール、および既存のスコープと新しいスコープを持つ各管理者を作成します。

柔軟性と構成の容易さのために、管理者を作成するときにスコープを作成できます。マシンカタログまたは接続を作成または編集するときに、スコープを指定することもできます。

管理者の作成と管理

ローカル管理者としてサイトを作成すると、ユーザーアカウントは自動的に、すべてのオブジェクトに対する完全な権限を持つフル管理者になります。サイトが作成された後、ローカル管理者には特別な権限はありません。

フル管理者ロールには常に All スコープがあります。これは変更できません。

デフォルトでは、管理者は有効になっています。管理者を今作成するが、その人が後で管理業務を開始する場合、管理者を無効にする必要があるかもしれません。既存の有効な管理者については、オブジェクト/スコープを再編成している間、それらのいくつかを無効にし、更新された構成で稼働準備ができたときに再度有効にしたい場合があります。有効なフル管理者がいなくなる場合、フル管理者を無効にすることはできません。有効/無効チェックボックスは、管理者を作成、コピー、または編集するときに利用できます。

管理者をコピー、編集、または削除する際にロール/スコープのペアを削除すると、その管理者に対するロールとスコープ間の関連付けのみが削除されます。ロールまたはスコープ自体は削除されません。また、そのロール/スコープのペアで構成されている他の管理者には影響しません。

管理者を作成および管理するには、次の手順に従います。

1. Web Studio にサインインし、左側のペインで をクリックし、 タブをクリックします。
2. 実行したいタスクの手順に従います。

   - **管理者を作成する:** アクションバーで をクリックします。ユーザーアカウント名を入力または参照し、スコープを選択または作成し、役割を選択します。新しい管理者はデフォルトで有効になっています。これは変更できます。
   - **管理者をコピーする:** 管理者を選択し、アクションバーで をクリックします。ユーザーアカウント名を入力または参照します。役割/スコープのペアを選択して編集または削除したり、新しいペアを追加したりできます。新しい管理者はデフォルトで有効になっています。これは変更できます。
   - **管理者を編集する:** 管理者を選択し、アクションバーで をクリックします。役割/スコープのペアを編集または削除したり、新しいペアを追加したりできます。
   - **管理者を削除する:** 管理者を選択し、アクションバーで をクリックします。有効なフル管理者がいなくなる場合は、フル管理者を削除できません。

上部のペインには、作成した管理者が表示されます。管理者を選択すると、下部のペインにその詳細が表示されます。 列は、管理者に関連付けられている役割とスコープのペアに、使用できない役割またはスコープが含まれているかどうかを示します。関連付けられている役割とスコープのペアに、使用できない役割またはスコープが含まれている場合、次の警告メッセージが表示されます。

- 関連付けられているロールまたはスコープが使用できません

> **重要:**

> 警告メッセージは、関連付けられているロールとスコープのペアに、使用できないロール、スコープ、またはその両方が含まれている場合にのみ表示されます。

> 管理者からロールとスコープのペアを削除するには、次のいずれかの手順を実行します。

- 役割とスコープのペアを削除します。

  a. アクションバーで をクリックします。

  b. ウィンドウで、役割とスコープのペアを選択し、 をクリックします。

  c. 「**保存**」をクリックして終了します。

- 管理者を削除します。

a. アクションバーで、「**管理者削除**」をクリックします。

b. 確認ウィンドウで、「**削除**」をクリックします。

ロールの作成と管理

管理者がロールを作成または編集する場合、自分自身が持っている権限のみを有効にできます。これにより、管理者が現在持っている権限よりも多くの権限を持つロールを作成し、それを自分自身に割り当てること（または既に割り当てられているロールを編集すること）を防ぎます。

ロール名には最大64個のUnicode文字を含めることができます。ただし、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左右の矢印、パイプ、左右の角かっこ、左右の丸かっこ、引用符、アポストロフィは含めることができません。説明には最大256個のUnicode文字を含めることができます。

組み込みロールを編集または削除することはできません。カスタムロールは、いずれかの管理者が使用している場合は削除できません。

> 「**注：**」：

> 特定の製品エディションのみがカスタムロールをサポートしています。カスタムロールをサポートするエディションのみが、アクションバーに関連エントリを持っています。

> ロールを作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで「**管理者**」をクリックし、次に「**ロール**」タブをクリックします。
2. 実行したいタスクの手順に従います。

   - **ロールの詳細を表示:** ロールを選択します。下部のペインに、そのロールのオブジェクトタイプと関連する権限が表示されます。下部のペインで「**管理者**」タブをクリックすると、現在このロールを持つ管理者の一覧が表示されます。
   - **カスタムロールを作成:** アクションペインで「**ロールの作成**」をクリックします。名前と説明を入力します。オブジェクトタイプと権限を選択します。
   - **ロールをコピーする:** ロールを選択し、アクションバーで**ロールをコピー**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。
   - **カスタムロールを編集する:** ロールを選択し、アクションバーで**ロールを編集**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。

- **カスタムロールを削除する:** ロールを選択し、アクションバーで**ロールを削除**をクリックします。プロンプトが表示されたら、削除を確認します。

スコープの作成と管理

サイトを作成するときに利用できるスコープは「すべて」スコープのみであり、これは削除できません。

以下の手順でスコープを作成できます。管理者を作成する際にもスコープを作成できます。各管理者は、少なくとも1つのロールとスコープのペアに関連付けられている必要があります。デスクトップ、マシンカタログ、アプリケーション、またはホストを作成または編集する際に、それらを既存のスコープに追加できます。スコープに追加しない場合、それらは「すべて」スコープの一部として残ります。

サイトの作成はスコープ化できません。また、委任管理オブジェクト（スコープとロール）もスコープ化できません。ただし、スコープ化できないオブジェクトは「すべて」スコープに含まれます。（フル管理者は常に「すべて」スコープを持ちます。）マシン、電源操作、デスクトップ、およびセッションは直接スコープ化されません。管理者は、関連付けられたマシンカタログまたはデリバリーグループを通じて、これらのオブジェクトに対する権限を割り当てることができます。

スコープの作成と管理に関するルール:

- スコープ名には、最大64個のUnicode文字を含めることができます。スコープ名には、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左矢印、右矢印、パイプ、左角かっこまたは右角かっこ、左丸かっこまたは右丸かっこ、引用符、アポストロフィを含めることはできません。
- スコープの説明には、最大256個のUnicode文字を含めることができます。
- スコープをコピーまたは編集する際は、スコープからオブジェクトを削除すると、それらのオブジェクトが管理者からアクセスできなくなる可能性があることに注意してください。編集されたスコープが1つ以上のロールとペアになっている場合、スコープの更新によってロール/スコープのペアが使用不能にならないようにしてください。

スコープを作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**管理者**をクリックしてから、**スコープ**タブをクリックします。
2. 完了したいタスクの手順に従います。

    - **スコープを作成する:** アクションバーで**新しいスコープを作成**をクリックします。名前と説明を入力します。特定の種類のすべてのオブジェクト（例: デリバリーグループ）を含める

には、オブジェクトの種類を選択します。特定のオブジェクトを含めるには、種類を展開し、個々のオブジェクト（例: 営業チームが使用するデリバリーグループ）を選択します。

- **スコープをコピー:** スコープを選択し、アクションバーの**スコープをコピー**をクリックします。必要に応じて、名前と説明を入力し、オブジェクトの種類とオブジェクトを変更します。
- **スコープを編集:** スコープを選択し、アクションバーの**スコープを編集**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、およびオブジェクトを変更します。
- **スコープを削除:** スコープを選択し、アクションバーの**スコープを削除**をクリックします。プロンプトが表示されたら、削除を確定します。

レポートの作成

委任管理レポートには、次の2種類を作成できます。

- 管理者に関連付けられている役割/スコープのペアと、各オブジェクトタイプ（例：デリバリーグループやマシンカタログ）の個々の権限を一覧表示するHTMLレポート。このレポートはWeb Studioから生成します。

  このレポートを作成するには、次の手順に従います。

  a. Web Studioにサインインし、左ペインで**管理者**をクリックします

  b. 管理者を選択し、アクションバーの**レポートの作成**をクリックします。

  管理者の作成、コピー、または編集時に、このレポートを要求することもできます。

- すべての組み込み役割とカスタム役割を権限にマッピングするHTMLまたはCSVレポート。このレポートは、OutputPermissionMapping.ps1という名前のPowerShellスクリプトを実行して生成します。

  このスクリプトを実行するには、フル管理者、読み取り専用管理者、またはロールの読み取り権限を持つカスタム管理者である必要があります。スクリプトは次の場所にあります: Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts。

  構文：

  `OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]`

パラメーター	説明
`-Help`	スクリプトのヘルプを表示します。

パラメーター	説明
`-Csv`	CSV 出力を指定します。デフォルト = HTML
`-Path string`	出力の書き込み先。デフォルト = stdout
`-AdminAddress string`	接続先のDelivery Controller™のIPアドレスまたはホスト名。デフォルト = localhost
`-Show`	(`-Path` パラメーターも指定されている場合にのみ有効) 出力をファイルに書き込むと、`-Show` によって、Webブラウザーなどの適切なプログラムで出力が開かれます。
共通パラメーター	`Verbose`、`Debug`、`ErrorAction`、`ErrorVariable`、`WarningAction`、`WarningVariable`、`OutBuffer`、および `OutVariable`。詳細については、Microsoft のドキュメントを参照してください。

次の例では、HTML テーブルを Roles.html という名前のファイルに書き込み、そのテーブルを Web ブラウザーで開きます。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

-Path Roles.html –Show
```

次の例では、CSVテーブルをRoles.csvという名前のファイルに書き込みます。テーブルは表示されません。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

–CSV -Path Roles.csv
```

Windowsのコマンドプロンプトから、上記の例のコマンドは次のとおりです。

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'

-CSV -Path Roles.csv"
```

デリバリーコントローラー

注:

Citrix Virtual Apps and Desktops™展開は、Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

デリバリーコントローラーは、ユーザーアクセス管理、接続の仲介と最適化を担当するサーバー側コンポーネントです。コントローラーは、デスクトップおよびサーバーイメージを作成するMachine Creation Services™も提供します。

サイトには少なくとも1つのコントローラーが必要です。最初のコントローラーをインストールした後、サイト作成時または後でコントローラーを追加できます。サイトに複数のコントローラーを配置することには、主に2つの利点があります。

- **冗長性:** ベストプラクティスとして、本番サイトでは、常に異なる物理サーバー上に少なくとも2つのコントローラーを配置してください。1つのコントローラーが故障した場合でも、他のコントローラーが接続を管理し、サイトを管理できます。
- **スケーラビリティ:** サイトのアクティビティが増加すると、コントローラーのCPU使用率とデータベースのアクティビティも増加します。追加のコントローラーにより、より多くのユーザー、アプリケーション、およびデスクトップ要求を処理できるようになり、全体的な応答性を向上させることができます。

各Controllerはサイトデータベースと直接通信します。複数のゾーンを持つサイトでは、すべてのゾーンのControllerがプライマリゾーンのサイトデータベースと通信します。

重要:

> サイトが構成された後で、Controllerのコンピューター名またはドメインメンバーシップを変更しないでください。

VDAがControllerに登録する方法

VDAを使用する前に、サイト内のDelivery Controllerに登録（通信を確立）する必要があります。VDA登録の詳細については、「ControllerへのVDA登録」を参照してください。

Controllerの追加、削除、または移動

Controllerを追加、削除、または移動するには、「データベース」の記事に記載されているサーバーロールおよびデータベースロールの権限が必要です。

SQLクラスタリングまたはSQLミラーリングインストール内のノードにControllerをインストールすることはサポートされていません。

Delivery Controller™ をサイトに追加する際は、高可用性のために使用するレプリカ SQL Server に、そのマシンのログオン資格情報を追加してください。

展開でデータベースミラーリングを使用している場合:

- Controller を追加、削除、または移動する前に、プライマリデータベースとミラーデータベースの両方が実行されていることを確認してください。さらに、SQL Server Management Studio でスクリプトを使用している場合は、スクリプトを実行する前に SQLCMD モードを有効にしてください。
- Controller を追加、削除、または移動した後にミラーリングを確認するには、PowerShell `Get-configdbconnection` コマンドレットを実行します。このコマンドレットは、接続文字列でミラーへのフェールオーバーパートナーが設定されていることを確認します。

Controller を追加、削除、または移動した後:

- 自動更新が有効になっている場合、VDA は 90 分以内に更新された Controller のリストを受け取ります。
- 自動更新が有効になっていない場合は、すべての VDA で Controller ポリシー設定または ListOfDDCs レジストリキーが更新されていることを確認してください。Controller を別のサイトに移動した後、両方のサイトでポリシー設定またはレジストリキーを更新してください。

Controller を追加する

Controller は、サイトの作成時および後から追加できます。このソフトウェアの以前のバージョンでインストールされた Controller を、このバージョンで作成されたサイトに追加することはできません。

1. サポートされているオペレーティングシステムを含むサーバーでインストーラーを実行します。Delivery Controller コンポーネントと、必要なその他のコアコンポーネントをインストールします。インストールウィザードを完了します。
2. まだサイトを作成していない場合は、この Controller で Citrix Site Manager を実行してサイトを作成します。この Controller の IP アドレスは、新しいサイトに自動的に追加されます。

   データベースを初期化するスクリプトを生成する予定がある場合は、スクリプトを生成する前に Controller を追加してください。
3. 既にサイトを作成している場合は、次の手順に従ってください。

   a. この Controller で Citrix Site Manager を実行し、 をクリックして、参加したいサイトの Controller のアドレスを入力します。

   b. Studio configuration tool を実行して、Controller を Web Studio に追加します。

Controller を削除する

サイトからControllerを削除しても、Citrixソフトウェアやその他のコンポーネントがアンインストールされることはありません。この操作により、Controllerがデータベースから削除され、接続の仲介やその他のタスクに使用できなくなります。Controllerを削除しても、後で同じサイトまたは別のサイトに再度追加できます。サイトには少なくとも1つのControllerが必要なため、Web Studioに表示されている最後のControllerを削除することはできません。

サイトからControllerを削除しても、Controllerのデータベースサーバーへのログオンは削除されません。これにより、同じマシン上の他の製品のサービスで使用されているログオンが誤って削除されるのを防ぎます。ログオンが不要になった場合は、手動で削除する必要があります。ログオンを削除するには、`securityadmin`サーバーロールのアクセス許可が必要です。

Controllerを削除した後：

- 自動更新を使用しているVDAは、他の利用可能なControllerに再登録されます。この再登録は、自動更新メカニズムが有効になっており、VDAが他のController（削除されたControllerと同じセカンダリゾーン、またはオンプレミス展開のプライマリゾーン）に到達できる場合にのみ発生します。
- Citrix StoreFrontでController情報を更新します。詳しくは、「Controllerの管理」を参照してください。

- Citrix StoreFrontで、Citrix Gatewayを介したリモートアクセス用のSecure Ticket Authority（STA）URLを更新します。詳しくは、「Secure Ticket Authorityの管理」を参照してください。
- Citrix Gatewayで、仮想サーバーのSTA URLを更新します。詳しくは、「Citrix Gateway」を参照してください。

重要：

サイトからControllerを削除するまで、Active DirectoryからControllerを削除しないでください。

1. Web Studioがロードされ、削除したいControllerが表示されるように、Controllerの電源がオンになっていることを確認してください。
2. Web StudioがControllerを完全にロードした後、Controller上のすべてのサービスが実行されており、Controllerの電源がオンのままであることを確認します。
3. Web Studioにサインインし、左ペインで**設定**を選択します。
4. **Delivery Controller**タイルを見つけて、**編集**をクリックします。
5. **Delivery Controllerの管理**ページで、削除するControllerを選択します。
6. **Remove Controller** を選択します。適切なデータベースロールと権限がない場合は、データベース管理者がコントローラーを削除できるようにするスクリプトを生成するオプションが提示されます。

   Web Studio は、コントローラーを削除する前に事前チェックを実行します。コントローラーが電源オフになっており、以下のサービスステータスにない場合は、安全に削除できます。

   - 不明
   - 障害保留中
   - 旧バージョン
   - 新バージョン
   - バージョン変更中
   - 必須機能が不足しています

   コントローラーの電源がオフになっておらず、上記のいずれかのサービスステータスにある場合、Web Studio はコントローラーの電源をオフにするよう促します。

7. データベースサーバーから Controller のマシンアカウントを削除する必要があります。削除する前に、別サービスがそのアカウントを使用していないことを確認してください。

Web Studio を使用してコントローラーを削除した後、現在のタスクが適切に完了するように、そのコントローラーへのトラフィックがしばらく残る場合があります。短時間でコントローラーの強制削除を希望する場合は、Citrix は、コントローラーがインストールされていたサーバーをシャットダウンするか、そのサーバーを Active Directory から削除することを推奨します。その後、サイト上の他のコントローラーを再起動して、削除されたコントローラーとの通信がこれ以上行われないようにします。

Controller を別のゾーンに移動する

サイトに複数のゾーンが含まれている場合、コントローラーを別のゾーンに移動できます。この移動が VDA 登録やその他の操作にどのように影響するかについては、ゾーン を参照してください。

1. 左ペインで を選択します。
2. 中央ペインでゾーンを選択し、Controller を選択します。
3. アクションバーで を選択します。
4. 表示される ページで、Controller を移動するゾーンを選択します。
5. 「**保存**」をクリックします。

VDAを別のサイトへ移動する

Citrix Provisioning™を使用してVDAがプロビジョニングされた場合、または既存のイメージである場合、アップグレード時、またはテストサイトで作成されたVDAイメージを本番サイトに移動する際に、VDAを別のサイト（サイト1からサイト2へ）に移動できます。Machine Creation Services (MCS) を使用してプロビジョニングされたVDAは、あるサイトから別のサイトへ移動できません。MCSは、VDAがControllerに登録するためにチェックするListOfDDCsの変更をサポートしていません。MCSを使用してプロビジョニングされたVDAは、常に作成されたサイトに関連付けられているListOfDDCsをチェックします。

VDA を別のサイトに移動する方法は、インストーラーを使用する方法と Citrix ポリシーを使用する方法の 2 つがあります。

インストーラー

インストーラーを実行し、サイト2のControllerのFQDN (DNSエントリ) を指定してControllerを追加します。

インストーラーでControllerを指定するのは、Controllerポリシー設定が使用されていない場合に限ります。

グループポリシーエディター

次の例では、複数のVDAをサイト間で移動します。

1. サイト1で以下の設定を含むポリシーを作成し、そのポリシーをデリバリーグループレベルにフィルターして、サイト間の段階的なVDA移行を開始します。
   - Controller: サイト2の1つ以上のControllerのFQDN（DNSエントリ）を含みます。
   - Controllerの自動更新を有効にする: 無効に設定します。
2. デリバリーグループ内の各VDAは、新しいポリシーが適用されてから90分以内に通知を受けます。VDAは受信したControllerのリストを無視し（自動更新が無効になっているため）、ポリシーで指定されたControllerのいずれかを選択します。これはサイト2のControllerをリストしています。
3. VDAがサイト2のControllerに正常に登録されると、サイト2のListOfDDCとポリシー情報を受け取ります。これらはデフォルトで自動更新が有効になっています。サイト1でVDAが登録されていたControllerは、サイト2のControllerから送信されたリストには含まれていません。そのため、VDAはサイト2のリストにあるControllerの中から選択して再登録します。それ以降、VDAはサイト2からの情報で自動的に更新されます。

グループポリシーエディターの使用方法については、Citrixポリシーのドキュメントを参照してください。

IPv4/IPv6 のサポート

このリリースでは、純粋なIPv4、純粋なIPv6、およびIPv4とIPv6のネットワークが重複するデュアルスタック展開をサポートしています。

以下のコンポーネントはIPv4のみをサポートします。その他すべてはIPv4とIPv6をサポートします。

- XenServer®
- **IPv6 Controller 登録のみを使用**ポリシー設定によって制御されていないVirtual Delivery Agent (VDA)

IPv6 通信は、VDA 接続に関連する2つの Citrix® ポリシー設定によって制御されます。

- **IPv6の使用を強制する主要な設定：** IPv6コントローラー登録のみを使用。

  このポリシー設定は、VDA が Delivery Controller に登録するために使用するアドレス形式を制御します。

有効にすると、VDAは次の優先順位で選択された単一のIPv6アドレスを使用して、Controllerに登録し、通信します：グローバルIPアドレス、ユニークローカルアドレス（ULA）、リンクローカルアドレス（他のIPv6アドレスが利用できない場合のみ）。

無効にすると、VDA はマシンの IPv4 アドレスを使用して Controller と登録および通信します。これがデフォルト値です。

チームが頻繁に IPv6 ネットワークを使用する場合は、**IPv6 Controller 登録のみを使用**ポリシー設定が有効になっているイメージまたは組織単位 (OU) に基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。

チームが頻繁に IPv4 ネットワークを使用する場合は、**IPv6 Controller 登録のみを使用**ポリシー設定が無効になっているイメージまたは OU に基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。

- **IPv6ネットマスクを定義する依存設定：** コントローラー登録IPv6ネットマスク。

  マシンは複数のIPv6アドレスを持つことができます。このポリシー設定により、管理者は、登録されている場合に、VDAをグローバルIPではなく、優先されるサブネットのみに制限できます。この設定は、VDAが登録するネットワークを指定します。VDAは、指定されたネットマスクに一致する最初のアドレスでのみ登録します。

  この設定は、**IPv6コントローラー登録のみを使用ポリシー**設定が有効になっている場合にのみ有効です。デフォルト = 空の文字列

展開に関する考慮事項

環境にIPv4とIPv6の両方のネットワークが含まれている場合は、IPv4のみのクライアントとIPv6ネットワークにアクセスできるクライアント用に、別々のデリバリーグループ構成を作成します。ユーザーを区別するために、命名規則、手動のActive Directoryグループ割り当て、またはSmartAccessフィルターの使用を検討してください。 接続がIPv6ネットワークで開始され、その後IPv4アクセスのみを持つクライアントから再接続しようとすると、セッションの再接続が失敗する可能性があります。

注記 - これらの考慮事項は、DNS解決が有効になっている場合は適用されません。

Web Studioを使用したCitrix Virtual Apps and Desktops™のライセンス

> **注：**

> Citrix Virtual Apps and Desktops展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> Web Studioから、ライセンスサーバーがWeb Studioと同じドメイン内にあるか、信頼されたドメイン内にある場合、ライセンスの管理と追跡ができます。ライセンス関連のタスクについては、ライセンスドキュメントおよび複数タイプのライセンスを参照してください。

次の表に、サポートされているエディションとライセンスモデルを示します。

製品	エディション	ライセンスモデル
シトリックス バーチャル アプリ	プレミアム、アドバンスト、スタンダード	同時使用
シトリックス バーチャル デスクトップ	プレミアム、アドバンスト、スタンダード	ユーザー/デバイスおよび同時使用

詳細については、同時使用ライセンスおよびユーザー/デバイスライセンスを参照してください。

サポートされている現在のリリース (CR) および長期サービスリリース (LTSR) のバージョン

Citrixでは、機能やセキュリティの改善を享受するために、常に(/ja-jp/licensing/current-release.html)を使用することを強くお勧めします。

> **注:**
>
> License Server VPXは非推奨となり、今後のメンテナンスやセキュリティ修正は提供されません。License Server VPXのバージョン11.16.6以前を使用しているお客様は、できるだけ早く(/ja-jp/licensing/current-release.html)に移行することをお勧めします。

> Citrix製品のライフサイクル日付の詳細については、Product Matrixを参照してください。

レガシー製品および製品バージョンについては、レガシー製品マトリックスを参照してください。

以下のタスクを完了するには、完全なライセンス管理者である必要があります。Web Studioでライセンス情報を表示するには、管理者は少なくとも「ライセンスの読み取り」の委任管理権限を持っている必要があります。組み込みの「完全管理者」および「読み取り専用管理者」の役割には、その権限があります。

Web Studioを使用してCitrixからライセンスをダウンロードしてインストールする

1. Web Studioにサインインし、左ペインで**［ライセンス］**を選択します。
2. アクションバーで**［ライセンスの割り当て］**を選択します。
3. ライセンスの購入または更新後にCitrixからメールで受け取ったライセンスアクセスコードを入力します。
4. 製品を選択し、**［ライセンスの割り当て］**を選択します。その製品で利用可能なライセンスが割り当てられ、ダウンロードされます。特定のライセンスアクセスコードのすべてのライセンスを割り当ててダウンロードすると、そのライセンスアクセスコードを再利用することはできません。同じコードで他のトランザクションを行うには、My Accountにログオンします。

ローカルコンピューターまたはネットワークに保存されているライセンスを追加する

1. Web Studioにサインインし、左ペインで**［ライセンス］**を選択します。
2. アクションバーで**［ライセンスの追加］**を選択します。
3. ライセンスファイルを参照し、ライセンスサーバーに追加します。

ライセンスサーバーを変更する

1. Web Studioにサインインし、左ペインで**Licensing**を選択します。
2. アクションバーで**Change License Server**を選択します。
3. ライセンスサーバーのアドレスを*name:port*の形式で入力します。ここで、nameはDNS、NetBIOS、またはIPアドレスです。ポート番号を指定しない場合、デフォルトポート（27000）が使用されます。

使用するライセンスの種類を選択する

- サイトを構成する際、ライセンスサーバーを指定した後、使用するライセンスの種類を選択するよう求められます。サーバーにライセンスがない場合、ライセンスなしで製品を30日間試用するオプションが自動的に選択されます。

- サーバーにライセンスがある場合、その詳細が表示され、そのうちの1つを選択できます。または、ライセンスファイルをサーバーに追加してから、そのファイルを選択することもできます。

製品エディションとライセンスモデルを変更する

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。
2. アクションバーで**［製品エディションの編集］**を選択します。
3. 適切なオプションを更新します。

License Administration Consoleにアクセスするには、アクションバーで**［License Administration Console］**を選択します。コンソールがすぐに表示されるか、ダッシュボードがパスワードで保護されている場合は、License Administration Consoleの資格情報の入力を求められます。コンソールの使用方法の詳細については、ライセンスドキュメントを参照してください。

> **注:**
>
> Web Studioでライセンスを切り替えると、その変更がCitrix Directorに反映されるまでに最大5分かかります。たとえば、AdvancedとPremiumを切り替える場合などです。

ライセンス管理者を追加する

1. Web Studio にサインインし、左側のペインで **Licensing** を選択します。
2. **Licensing Administrators** タブを選択します。
3. アクションバーで **Add licensing administrator** を選択します。
4. 管理者として追加するユーザーを参照し、権限を選択します。

ライセンス管理者のアクセス許可を変更またはライセンス管理者を削除する

1. Web Studio にサインインし、左側のペインで **Licensing** を選択します。
2. **Licensing Administrators** タブを選択し、管理者を選択します。
3. アクションバーで **Edit licensing administrator** または **Delete licensing administrator** のいずれかを選択します。

ライセンス管理者グループを追加する

1. Web Studio にサインインし、左側のペインで **Licensing** を選択します。

2. **Licensing Administrators** タブを選択します。
3. アクションバーで **Add licensing administrator group** を選択します。
4. ライセンス管理者として機能させるグループを参照し、権限を選択します。Active Directory グループを追加すると、そのグループ内のユーザーにライセンス管理者権限が付与されます。

ライセンス管理者グループの権限を変更または削除する

1. Web Studioにサインインし、左ペインで**Licensing**を選択します。
2. **Licensing Administrators**タブを選択し、管理者グループを選択します。
3. アクションバーで**ライセンス管理者グループの編集**または**ライセンス管理者グループの削除**のいずれかを選択します。

ライセンス情報を表示する

Web Studioにサインインし、左ペインで**ライセンス**を選択します。サイトのライセンス使用状況と設定の概要が、指定されたライセンスサーバーに現在インストールされているすべてのライセンスのリストとともに表示されます。

サイトのライセンス設定（製品タイプ、ライセンスエディション、ライセンスモデルを含む）が、構成済みのライセンスサーバーが使用するライセンスと一致していることを確認してください。一致しない場合は、サイトのライセンス設定に合わせて既存のライセンスをダウンロードまたは割り当てる必要がある場合があります。

ライセンス有効期限アラートを表示する

Web Studioは、Citrix License Serverからライセンスファイルの有効期限を照会します。ライセンスファイルの有効期限が近づいているか、すでに期限切れになっている場合、Web Studioは概要タブで管理者に警告します。

関連リンク

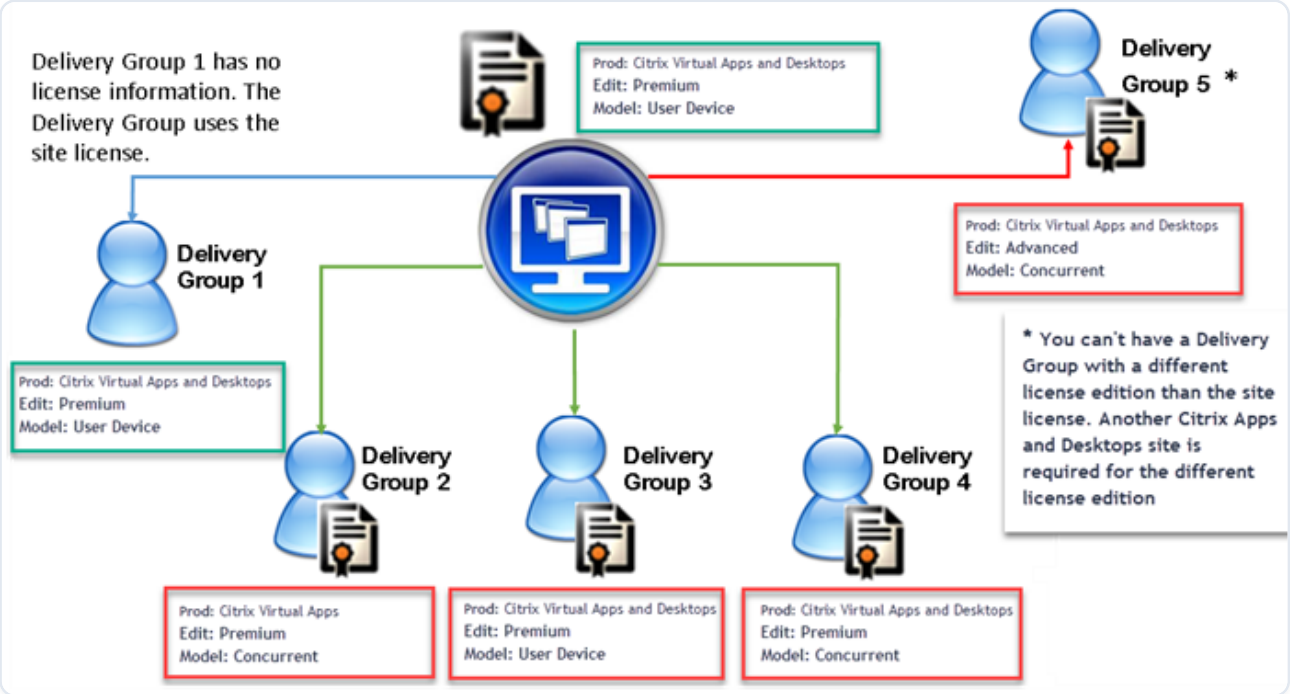
- 「年間および期間ベースの小売ライセンス向けCitrixオンプレミスサブスクリプション」を参照してください。
- 「Transition and Trade-Up (TTU) with Hybrid Rights」を参照してください。

マルチタイプライセンス

マルチタイプライセンスは、単一のCitrix Virtual Apps and Desktopsサイト上のデリバリーグループに対して、異なるライセンスタイプの消費をサポートします。**タイプ**は、製品ID（XDTまたはMPS）とモデル（UserDeviceまたはConcurrent）の単一の組み合わせです。デリバリーグループ

は、サイトレベルで構成されているものと同じ製品エディション（PLT/PremiumまたはENT/Advanced）を使用する必要があります。Citrix Virtual Apps and Desktops展開でマルチタイプライセンスを構成する際には、この記事の最後にある特別な考慮事項に注意してください。

マルチタイプライセンスが構成されていない場合、異なるライセンスタイプは、個別のサイト用に構成されている場合にのみ使用できます。デリバリーグループはサイトライセンスを使用します。マルチタイプライセンスが構成されている場合の重要な通知の制限については、特別な考慮事項 を参照してください。



異なる種類のライセンスを消費するデリバリーグループを特定するには、以下の Broker PowerShell コマンドレットを使用します。

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

ライセンスをインストールするには、以下を使用します。

- シトリックス スタジオ
- シトリックス ライセンシング マネージャー
- citrix.com

Customer Success Services の日付は、各ライセンスファイル、各製品、およびモデルに固有です。異なる設定のデリバリーグループは、互いに異なる Customer Success Services の日付を持つ場合があります。

特別な考慮事項

マルチタイプライセンスは、通常のCitrix Virtual Apps and Desktops™ライセンスとは異なる機能を持ちます。

DirectorまたはStudioからは、サイト構成とは異なるタイプを使用するように構成されたデリバリーグループに対するアラートや通知はありません。

- ライセンス制限に近づいている場合、またはライセンスバーストモードのトリガーや有効期限が切れた場合の情報はありません。
- 特定のグループに問題がある場合の通知はありません。

マルチタイプライセンス用に構成されたデリバリーグループは、そのライセンスタイプのみを消費し、完全に消費されてもサイト構成にフォールバックしません。

Citrix Virtual Apps StandardとCitrix Virtual Desktops™ Standardのライセンスエディション名はどちらもStandardであることを示していますが、これらは同じエディションではありません。マルチタイプライセンスは、Citrix Virtual Apps StandardおよびCitrix Virtual Desktop Standardライセンスでは利用できません。

ライセンス互換性マトリックス

この表は、古い製品名、新しい製品名、および関連する機能名を詳述しています。4つの互換性列は、マルチタイプライセンスで互換性のある製品とライセンスモデルの組み合わせを指定します。CCUとCCSは同時接続ライセンスを表し、UDはユーザー/デバイスライセンスです。

ライセンス互換性マトリックスと新旧の名称(/en-us/citrix-virtual-apps-desktops/2311/media/multi-type-compatibility-names.png)

ブローカー PowerShell SDK

DesktopGroupオブジェクトには、関連するNew-BrokerDesktopGroupおよびSet-BrokerDesktopGroupコマンドレットを使用して操作できるこれら2つのプロパティがあります。

名前	値	制限
LicenseModel	グループのライセンスモデルを指定するパラメーター(Concurrent または UserDevice)。指定されていない場合、サイト全体のライセンスモデルが使用されます。	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。

名前	値	制限
ProductCode	XDT (Citrix Virtual Desktops用) またはMPS (Citrix Virtual Apps™用) のテキスト文字列で、グループのライセンス製品IDを指定します。指定されていない場合、サイト全体の製品コードが使用されます。	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。

LicenseModelとProductCodeの詳細については、about_Broker_Licensingを参照してください。

New-BrokerDesktopGroup

デスクトップグループを作成し、デスクトップグループのブローカーを管理します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>`を参照してください。

Set-BrokerDesktopGroup

既存のブローカーデスクトップグループを無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

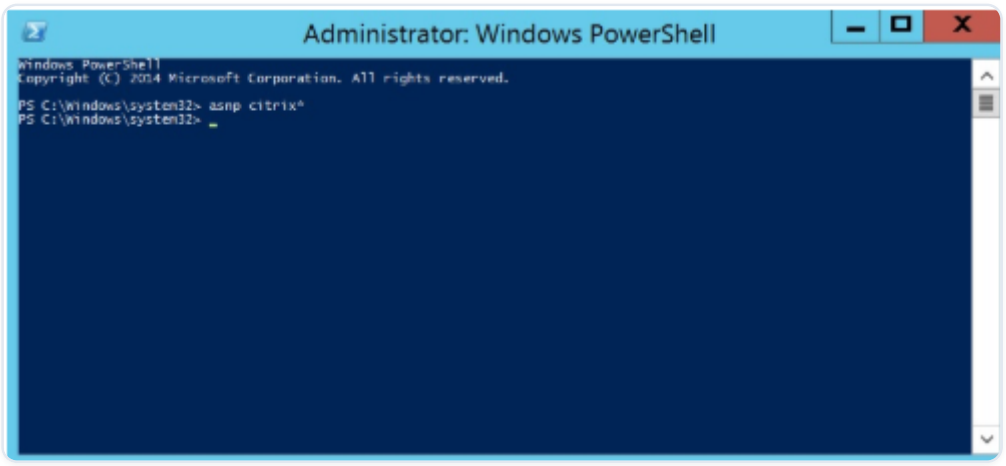
Get-BrokerDesktopGroup

指定された条件に一致するデスクトップグループを取得します。Get-BrokerDesktopGroupコマンドレットの出力には、グループの**ProductCode**および**LicenseModel**プロパティが含まれます。プロパティがNew-BrokerDesktopGroupまたはSet-BrokerDesktopGroupを使用して設定されていない場合、null値が返されます。nullの場合、サイト全体のライセンスモデルと製品コードが使用されます。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/>`を参照してください。

デリバリーグループごとに異なるライセンス製品とモデルを構成する

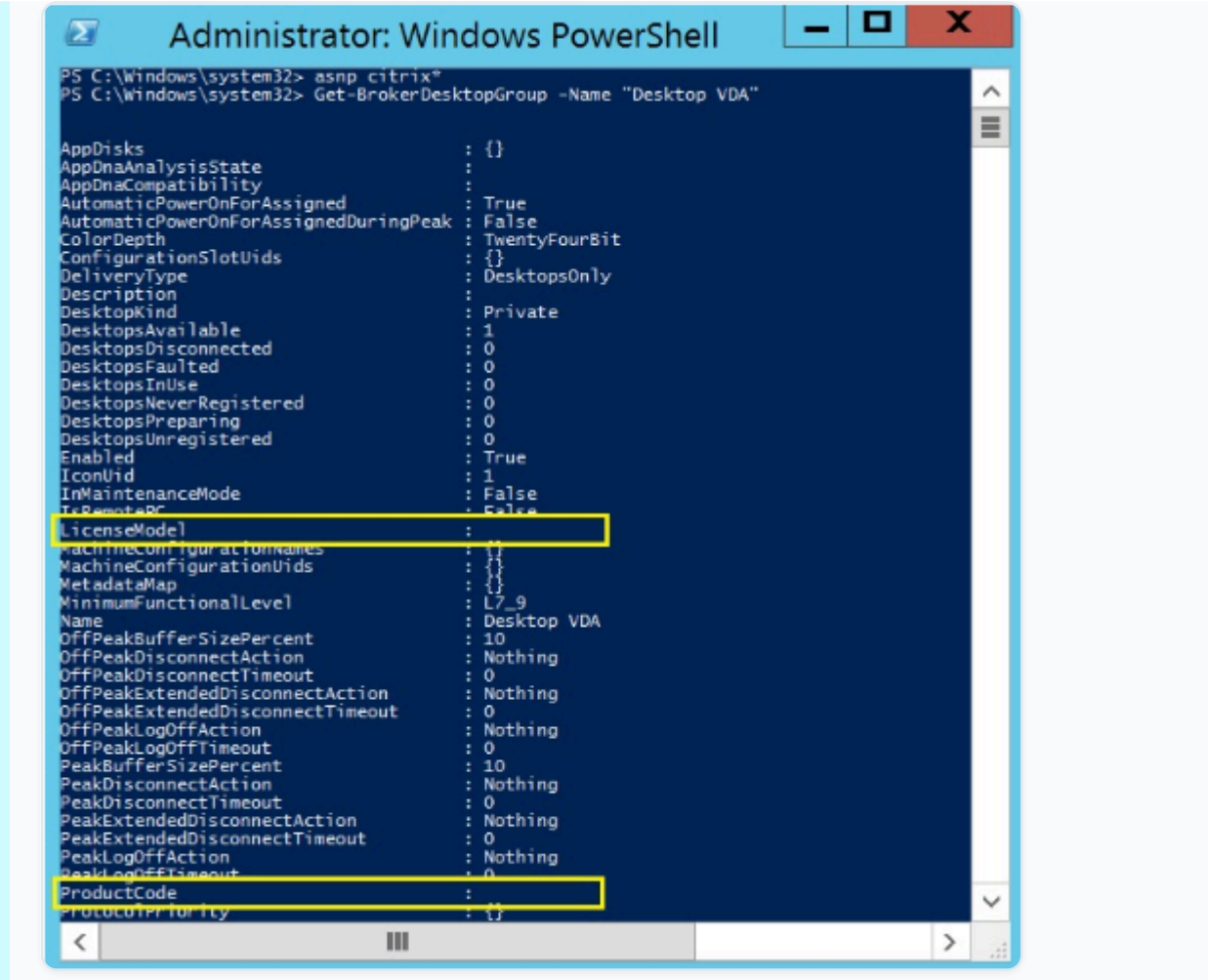
> **注：**
>
> 単一のデリバリーグループで、2つ以上の異なる種類の製品、エディション、またはライセンスモデルを構成することはできません。異なる種類の製品、エディション、またはライセンスモデルがある場合は、それらを個別のデリバリーグループで構成してください。

1. 管理者権限でPowerShellを開き、Citrixスナップインを追加します。

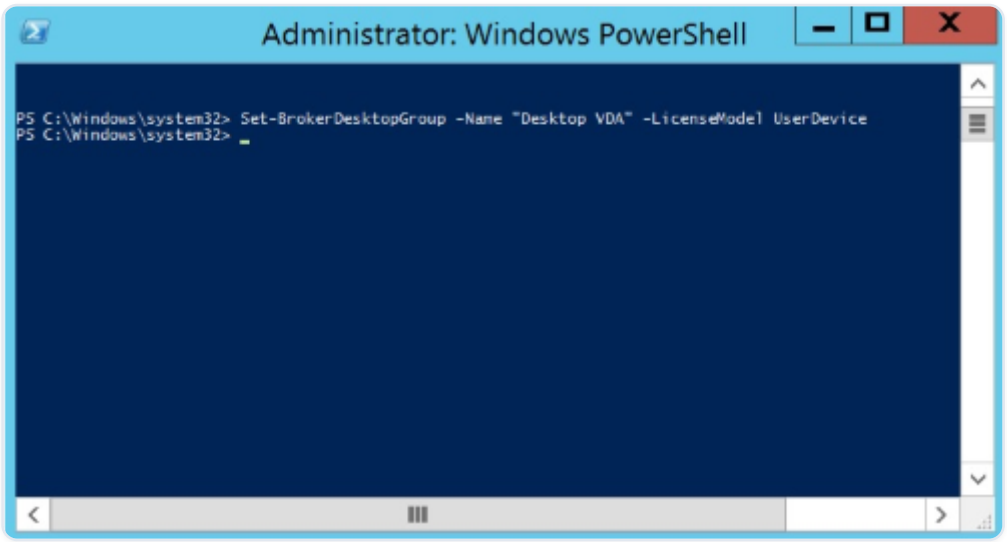


2. 現在のライセンス構成を表示するには、コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を実行します。パラメーター **LicenseModel** と **ProductCode** を見つけてください。これらのパラメーターを以前に構成していない場合、空白になっている可能性があります。

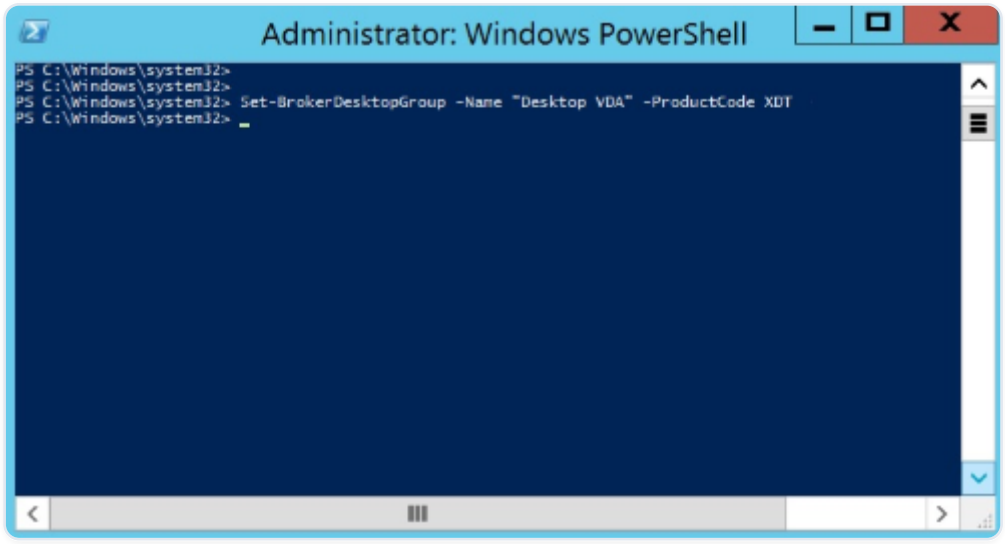
> **注:**
>
> デリバリーグループにライセンス情報が設定されていない場合、デフォルトで **サイトレベルのサイトライセンス** が適用されます。



3. コマンド **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel** を実行して、ライセンスモデルを変更します。

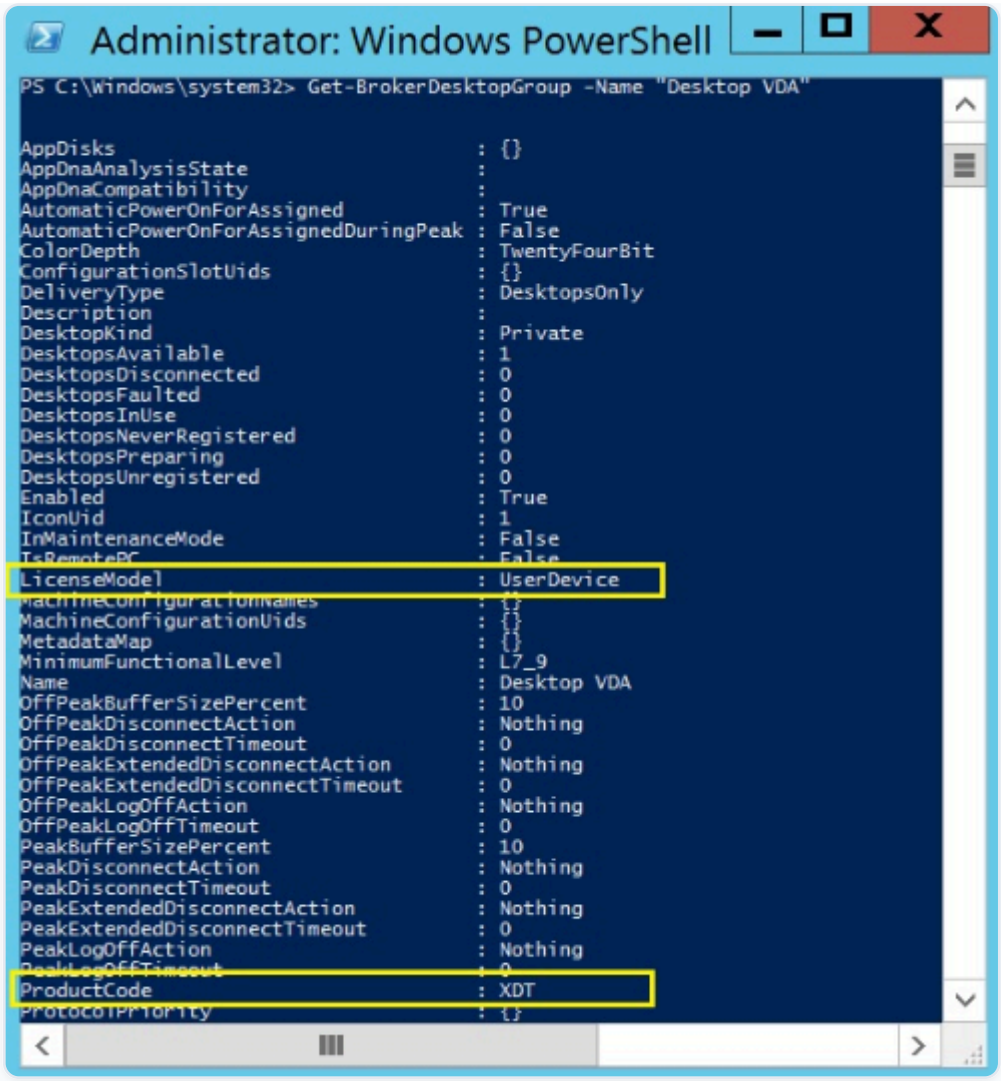


4. コマンド **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode** を実行して、ライセンス製品を変更します。



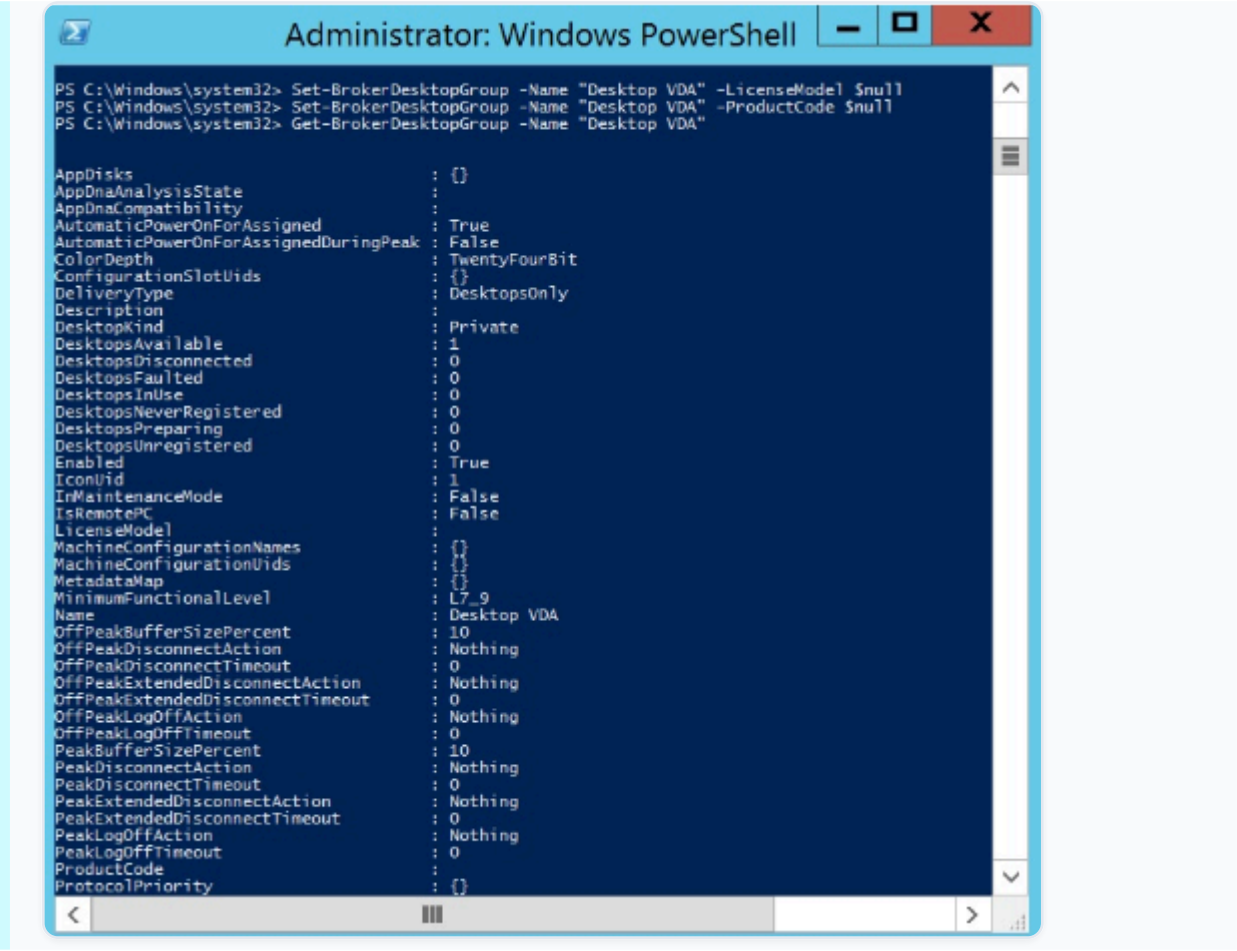
5. 変更を検証するには、コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を入力します。

> **注:**
>
> 同じサイト内でエディションを混在させることはできません。たとえば、Premium ライセンスと Advanced ライセンスなどです。異なるエディションのライセンスがある場合は、複数のサイトが必要です。



6. ライセンス構成を削除するには、前の手順で説明したのと同じ **Set-BrokerDesktopGroup** コマンドを実行し、値を **$null** に設定します。

> **注:**
>
> Studio では、各デリバリーグループのライセンス構成は表示されません。現在の構成を表示するには、PowerShell を使用します。



例

このPowerShellコマンドレットの例は、既存の2つのデリバリーグループに対するマルチタイプライセンスの設定と、3番目のデリバリーグループの作成および設定を示しています。

デリバリーグループに関連付けられているライセンス製品とライセンスモデルを確認するには、**Get-BrokerDesktopGroup** PowerShellコマンドレットを使用します。

1. 最初のデリバリーグループをXenApp®と同時使用に設定します。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル アプリ プレミアム同時接続 向けのデリバリーグループ" -ProductCode MPS -LicenseModel Concurrent

2. 2番目のデリバリーグループをXenDesktop®と同時使用に設定します。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル デスクトップ プレミアム同時接続 向けのデリバリーグループ" -ProductCode XDT -LicenseModel Concurrent

3. 3番目のデリバリーグループをXenDesktopとユーザー/デバイスに作成および設定します。

New-BrokerDesktopGroup -Name "Citrix Virtual Desktops Premium UserDevice 用デリバリーグループ" -PublishedName "マイデスクトップ" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

Citrix Virtual Apps and Desktops™ テレメトリデータ要素

ブローカー

セッション

ヘッダー

キー	説明	例
バージョン	テレメトリー使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Serviceがクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	SendBrokerTelemetryData
st	Brokerでイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
製品	使用イベントの発生元の製品と展開を識別します。	XenDesktop.Broker
prodVer	Citrix DaaS/Citrix Virtual Apps and Desktopsの製品バージョンを示します。	7.25.0.0

キー	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザーIDを識別します。	fullName: C648FE671A44B3F7 samName:C758LH671A44B3F7 ユーザープリンシパル名: C7948FE671A44B3F7 userLicenseId:C265FE671A44B3F7 userSid: C097FE671A44B3F7
テナント -> ID	Citrix Cloud™アカウントの顧客IDを示します。オンプレミス展開の場合、値は常に「CitrixOnPremises」です。	joj1mh0598tj
dvc を dvcId に	セッション起動が開始されたデバイスを一意に識別するためのデバイスIDを示します。	AE18C4D5
dvc から dvcName	デバイスのフレンドリ名を示します。	C758LH671A44B3F7

ペイロード

フィールド	説明	例
appProtectionKeyLoggingRequired	セッションがキーロギング保護を有効にして起動されたかどうかを示します。	いいえ
appProtectionScreenCaptureRequired	セッションが画面キャプチャ保護を有効にして起動されたかどうかを示します。	いいえ
cspTenantCustomerId	CSP テナントの Citrix Cloud アカウントの顧客 ID を示します。オンプレミス展開の場合、顧客 ID が利用できない場合、このフィールドは空のままになります。	6c2vtxgxyftt
isAnonymousUser	認証されていないセッションが起動されたかどうかを示します。	いいえ
licenseActivityTimeStamp	ペイロードが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
licenseActivityType	ライセンスイベントの種類を示します。このフィールドは、ライセンスイベントの種類が割り当てアクションか解放アクションかを示します。	接続
licenseModel	展開のライセンスモデルを示します。	UserDevice
productEdition	展開の製品エディションを示します。	Premium または Advanced
productId	展開内の製品の製品IDを示します。	CAVDS
プロトコル	セッションの起動に使用されたプロトコルを示します。	HDX™

フィールド	説明	例
sessionKey	セッションの一意の識別子を示します。	uq390c5fc3-86eb-4df3-bd9a-f4a8fed2c9e2
sessionSupport	セッションサポートの種類を示します。	SingleSession
sessionType	セッションの種類を示します。	アプリケーション
バージョン	ペイロードのバージョンを示します。	1.3
workerSid	セッションに使用されるVDAの一意の識別子を示します。**値はスクランブルされています。**	1E5LH671A44B3F7 **(常にスクランブルされています)**
isWindows365	セッションがWindows 365向けに起動されたかどうかを示します。	はい
entitlementType	顧客のライセンスエンタイトルメントの種類を示します。	本番
siteId	サイトの一意の識別子を示します。	a35647d0-901c-4477-87e0-dcd781d455f4
desktopGroupId	デスクトップまたはデリバリーグループの一意の識別子を示します。	e9d859dc-1bfc-4b3e-bad3-41806bb4e694
clientType	Citrix Workspace™ アプリの種類を示します。	ウィンドウズ
clientVersion	Citrix Workspace アプリのバージョンを示します。	23.5.1.83
workerCloudType	VDAプロビジョニングに使用されるパブリッククラウドの種類を示します。	アジュール

フィールド	説明	例
enabledFeatures	セッションで有効になっている機能を示します。たとえば、`AppProtectionScreenCaptureRequired` と `SessionRecording` が有効になっているセッションでは、このフィールドの値は 66 です。	66
isEvents	{{page.lic}}における重大な障害を示します。	STデータベースを作成できません。
heartBeatTime	CISまたはCitrix Analytic Serviceへのライセンスサーバーのハートビート時間を示します。	1689058813

ライセンス テレメトリ データを難読化する

ライセンス テレメトリで送信される情報の機密性を考慮し、Citrix はデータを難読化するオプションを提供します。

次の表に、難読化できるデータを示します。

フィールド	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザーIDを特定します。	• fullName: `C648FE671A44B3F7` • samName: `C758LH671A44B3F7` • upn： `C7948FE671A44B3F7`

フィールド	説明	例
		• userLicenseId: `C265FE671A44B3F7` • userSid: `C097FE671A44B3F7`
dvc を dvcName に	デバイスのフレンドリ名を示します。	`C758LH671A44B3F7`
workerSid	セッションに使用されるVDAの一意の識別子を示します。	`1E5LH671A44B3F7`
AdminLoginList	一意の管理者SamAccountNameのリストを示します	`{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}`

スクランブルを有効または無効にするには、Delivery Controllerで次のPowerShellコマンドを実行します。

> **注:**
>
> Citrix Service Provider™ (CSP)のお客様の場合、スクランブルは常に無効になっています。CSPのお客様は、PowerShellコマンドを使用してスクランブルを有効にすることはできません。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. コマンド `asnp citrix` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. スクランブルを有効または無効にするには、次のコマンドを実行します。

   既定では、値は `0` または `false` であり、ライセンステレメトリデータのスクランブルを無効にします。

   有効にするには:

```
Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
-SettingValue $true
```

スクランブルを有効にした後、次のコマンドを使用して無効にできます。

```
Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
-SettingValue $false
```

ライセンスに関するFAQ

注:

- COVID-19パンデミックに関連する事業継続リソースについては、CTX27055を参照してください。
- 事業継続の維持に関する一般情報については、Business continuity — on demandを参照してください。
- 現在のCitrix License Serverに関する詳細については、Licensingを参照してください。

Citrix®ライセンス

ライセンスファイルはどのように入手できますか?

ライセンスアクセスコードは電子メールで送信されます。ライセンスアクセスコードを使用してライセンスファイルを生成する方法は3つあります。

- `citrix.com` のMyAccountページにある**ライセンスの管理**。詳細については、citrix.comでライセンスを管理するを参照してください。
- Web Studioを使用して購入を割り当てると、ライセンスファイルがCitrixライセンスサーバーに自動的にインストールされます。
- Citrixライセンスサーバー内のCitrix Licensing Managerを使用して購入を割り当て、ライセンスファイルをインストールします。詳細については、ライセンスのインストールを参照してください。

MyAccountでライセンスを割り当てる方法?

ライセンスの割り当てを参照してください。

割り当てられたライセンスをライセンスサーバーに追加する方法?

ライセンスの変更を参照してください。

Citrixライセンスはどのポートを使用しますか?

- ライセンスサーバーのポート番号は27000です。
- ベンダーデーモンのポート番号は7279です。
- ライセンス用Webサービスのポートは8083です。

Citrixライセンスサーバーとは何ですか?

Citrixライセンスサーバーは、ライセンスをネットワーク全体で共有できるようにするシステムです。詳細については、「ライセンス操作の概要」を参照してください。

Citrixライセンスサーバーを仮想化またはクラスター化できますか?

はい、Citrixライセンスサーバーを仮想化またはクラスター化できます。詳細については、「クラスター化されたライセンスサーバー」を参照してください。

Citrixライセンスサーバーを仮想化すると、どのようなメリットがあります?

Citrixライセンスサーバーを仮想化すると、冗長性のあるソリューションが提供されます。このソリューションにより、ダウンタイムなしで複数の物理サーバー間を移動できます。

Citrixライセンスサーバーを仮想化する場合、考慮すべき制限はありますか?

いいえ。

Citrixライセンスサーバーは、Citrix Virtual Apps and Desktops™展開のすべてのライセンスを管理するか?

Citrixライセンスサーバーは、Citrix Virtual Apps™およびDesktop用に受け取るすべてのライセンスを管理します。ただし、Citrix Gatewayで使用されるPremium Editionのライセンスは除きます。これらのセキュリティ指向のネットワークデバイスに必要なネットワークアプライアンスに組み込まれたライセンスサーバーが、それらのライセンスを管理します。

Citrix Licensing Manager とは何ですか?

Citrix Licensing Managerは、Citrix Licensing Managerをインストールしたライセンスサーバーからライセンスファイルのダウンロードと割り当てを可能にします。Citrix Licensing Managerは、推奨されるライセンスサーバー管理方法であり、以下のことを可能にします。

- ライセンスサーバーのCitrix Cloud™へのショートコード登録と、登録の簡単な削除。
- ユーザーアカウントとグループアカウントを構成します。

- ダッシュボードを使用して、インストール済み、使用中、期限切れ、利用可能なライセンス、およびCustomer Success Servicesの期日を表示します。
- レポート作成に使用するため、ライセンス使用状況データをエクスポートします。
- 履歴使用状況データの保持期間を構成します。デフォルトのデータ保持期間は180日です。
- ライセンスアクセスコードまたはダウンロードしたファイルを使用して、ライセンスサーバーへのライセンスファイルのインストールを簡素化します。
- ライセンスバーストモードを有効または無効にします。
- カスタマーエクスペリエンス向上プログラム (CEIP) とコールホームを構成します。
- Customer Success Servicesの更新ライセンスを自動または手動で確認し、見つかった場合は通知するか、ライセンスをインストールします。
- ライセンスサーバーの状態（起動ライセンスの不足、時間に関する問題、アップローダーの障害）を通知します。
- これらのポートを変更します。
  - ライセンスサーバー（デフォルト27000）
  - ベンダーデーモン（デフォルト7279）
  - ライセンス用Webサービス（デフォルト8083）

詳細については、Citrix Licensing Managerを参照してください。

Citrix License Administration Consoleはどこにありますか?

License Administration Consoleはサポートされなくなり、License Serverバージョン11.16.6から削除されました。Citrix Licensing Managerの使用をお勧めします。

License ServerがStudioと同じドメイン内、または信頼されたドメイン内にある場合、Studioを使用してライセンスを管理および追跡できます。

詳細については、Citrix Licensing Managerを参照してください。

ライセンス割り当て期間とは何ですか?

ライセンス割り当て期間とは、Citrix Virtual Apps and Desktopsライセンスがユーザーまたはデバイスに割り当てられる期間のことです。デフォルトのライセンス割り当て期間は90日です。

組織が購入したライセンスの数を確認するにはどうすればよいですか?

購入したすべてのライセンスは、`<https://www.citrix.com>`の**My Account**ページにある安全な**Manage Licenses**ツールボックスから、いつでも（24時間365日）確認およびアクセスできます。

いつでも使用中のライセンス数を確認するにはどうすればよいですか?

Citrix Licensing ManagerとStudioは、リアルタイムのライセンス使用状況に関する詳細を提供します。

License Serverの災害復旧とメンテナンス

License Serverの災害復旧とメンテナンスについては、Citrix Licensingドキュメントの災害復旧とメンテナンスを参照してください。

Citrix Virtual Apps and Desktopsのライセンス

Citrix Virtual Apps and Desktopsはどのようにライセンスされますか?

Citrix Virtual Apps and Desktops のライセンスは、ユーザー/デバイスおよび同時接続ライセンスモデルを提供します。

ユーザー/デバイス:

柔軟なユーザー/デバイスモデルは、以下と連携します。

- 企業全体のデスクトップ利用。
- 基盤となるMicrosoftデスクトップ仮想化ライセンス。
- 仮想デスクトップとアプリへのアクセスが時々しか必要ないユーザー向けの同時接続ライセンス。

ユーザー/デバイスライセンスにより、ユーザーは無制限の数のデバイスから仮想デスクトップとアプリにアクセスできます。デバイスライセンスにより、無制限の数のユーザーが単一のデバイスから仮想デスクトップとアプリにアクセスできます。このアプローチにより、最大限の柔軟性が提供され、Microsoftデスクトップ仮想化ライセンスとの整合性が向上します。

> **重要:**

> ライセンスをユーザーまたはデバイスに手動で割り当てることはできません。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。ユーザー/デバイスライセンスでは、一度割り当てられたライセンスは、90日間非アクティブになるまで別のユーザーに割り当てることはできません。

> **同時使用:**

同時接続ライセンスは、任意のユーザーおよび任意のデバイスに対して、無制限の数の仮想アプリおよびデスクトップへの1つの接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了すると、ライセンスはプールに戻されます。

ユーザー/デバイスライセンスの詳細については、ユーザー/デバイスライセンス を参照してください。同時使用ライセンスについては、同時使用ライセンス を参照してください。

ライセンスを購入する前にCitrix Virtual Apps and Desktopsを試用することはできますか?

はい。Citrix Virtual Apps and Desktopsソフトウェアをダウンロードし、試用モードで実行できます。試用モードでは、ライセンスなしで、Citrix Virtual Apps and Desktopsをオンプレミスで30日間、10接続まで使用できます。詳細については、評価ライセンスを参照してください。

Citrix Cloud向けのCitrix DaaS™（旧Citrix Virtual Apps and Desktopsサービス）は、承認に基づいて試用サービスとして利用できます。詳細については、Citrix担当者にお問い合わせください。

Citrix Virtual Apps and Desktopsにおける同時接続の定義は何ですか?

Citrix Virtual Apps and Desktopsの同時接続モデルでは、任意のユーザーと任意のデバイスに対して、無制限の数の仮想アプリとデスクトップへの1つの接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了した場合、ライセンスは再発行のためにプールに戻されます。詳細については、「同時接続ライセンス」を参照してください。

共通のライセンスサーバーにCitrix Virtual Apps and Desktopsライセンスの複数のエディションを展開できますか?

はい。ライセンスサーバーは、Citrix Virtual AppsとDesktopsの両方のライセンスを同時に管理します。最新のライセンスサーバーバージョンをインストールすることをお勧めします。お使いのライセンスサーバーのバージョンが最新であるか不明な場合は、Citrixダウンロードサイトの番号と比較して確認してください。

単一のサイトでCitrix Virtual AppsとCitrix Virtual Apps and Desktopsの両方のライセンスを使用できますか?

バージョンによっては、単一のCitrix Virtual AppsまたはCitrix Virtual Apps and Desktopsサイトで、ユーザー/デバイスまたは同時接続の両方のライセンスモデルをサポートできます。単一のCitrix Virtual AppsまたはCitrix Virtual Apps and Desktopsサイトは、1つのエディションのみをサポートできます。詳細については、「複数タイプライセンス」を参照してください。

複数タイプライセンスをサポートする最小バージョンは、XenAppおよびXenDesktop 7.15 Long Term Service Release (LTSR) とCitrix Virtual Apps and Desktops 7 1808です。

ライセンスサーバーにCitrix Virtual Apps and Desktopsユーザー/デバイスまたはCitrix Virtual Apps and Desktops同時接続ライセンスがインストールされている場合、製品モデルとしてCitrix Virtual Apps同時接続を選択できますか?

Citrix Virtual AppsをCitrix Virtual Apps and Desktops AdvancedまたはPremium Editionの機能として使用する場合、Citrix Virtual Appsのライセンスモデルは、Citrix Virtual Apps and DesktopsのAdvancedまたはPremium Editionと同じになります。Citrix Virtual Apps and Desktopsを購入した場合、Citrix Virtual Apps機能のみを使用する予定であっても、ライセンスをCitrix Virtual Apps and Desktopsとして構成してください。Citrix Virtual Apps同時接続スタンドアロンライセンスがライセンスサーバーにインストールされている場合にのみ、製品モデルとしてCitrix Virtual Appsを選択してください。

各Citrix Virtual AppsおよびCitrix Virtual Apps and Desktopsエディションには、どのような製品コンポーネントが含まれています?

エディションごとの全機能マトリックスについては、「Citrix Virtual Apps and Desktopsの機能」を参照してください。

Citrix Virtual Apps and Desktops EULAに準拠したCitrix Virtual Desktops™環境のライセンス付与?

Citrix Virtual Apps and Desktops EULAに準拠して、ユーザー/デバイスまたは同時接続ライセンスモデルでCitrix Virtual Apps and Desktopsを展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。購入した製品に基づいて製品を構成することをお勧めします。たとえば、Citrix Virtual Apps and Desktops Premiumを購入したが、Citrix Virtual Apps機能のみを使用したい場合は、コンプライアンスを満たすために製品をCitrix Virtual Apps and Desktopsに構成してください。詳細については、「製品ライセンスコンプライアンスセンター」を参照してください。

Citrix Virtual Apps EULAに準拠して、Citrix Virtual Apps環境のライセンスを付与するにはどうすればよいですか?

Citrix Virtual Apps EULAに準拠して、同時接続ライセンスモデルでCitrix Virtual Appsを展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。

Citrix Virtual Apps and Desktopsのサービスオプション（Long Term Service Release (LTSR)またはCurrent Release (CR)）にライセンス要件はありますか?

Long-Term Service Release などの Citrix Virtual Apps and Desktops Servicing Options は、Customer Success Services プログラムの特典です。LTSR の特典を受けるには、アクティブな Customer Success Services が必要です。詳細については、「[Citrix Virtual Apps、Citrix Virtual Apps and Desktops、および XenServer Servicing Options」を参照してください。

Remote Browser Isolation (RBI) Service のプールされた時間はどのように機能しますか?

サービスを最低 25 ユーザー購入すると、すべてのユーザーでプールされた 5000 時間のサービス使用権が付与されます。その後のユーザー権限の購入では、プールされた時間のエンタイトルメントは増加しません。サービス時間のエンタイトルメントを増やすには、アドオンパックを購入してください。

CCU ライセンスで Remote PC Access を使用できますか?

はい。

Remote PC Access の詳細については、「Remote PC Access」を参照してください。

Citrix 環境のソフトウェアメンテナンスの有効期限が切れるとどうなりますか?

ソフトウェアメンテナンス (SWM) またはサブスクリプションの有効期限が切れると、ソフトウェアアップグレードとテクニカルサポートへのアクセスが一時停止されます。また、ライセンスの種類と製品バージョンによっては、エンドユーザーと管理者に、環境がサポート対象外であることを示す特定の警告通知が届きます。

これらの通知は、サーバー上のすべてのライセンスの有効期限が切れた場合にのみトリガーされます。

エンドユーザーエクスペリエンス

ユーザーはセッションの起動後に警告メッセージを受け取ります。メッセージには次のように表示されます。

```
Citrix Virtual Apps and Desktops warning: Your corporate Citrix
environment is currently unsupported. Please contact your IT department to
resolve.
```

管理者エクスペリエンス

管理者は、Citrix Studio コンソール内で、間近に迫った、またはアクティブな有効期限を警告するアラートを確認できます。

ライセンスの種類による有効期限の動作

これらのメッセージの表示タイミングは、ライセンスの種類とインストールされているCitrix Virtual Apps and Desktopsのバージョンによって異なります。

オンプレミスサブスクリプションライセンス

- エンドユーザー警告: サブスクリプションの有効期限が切れた後、猶予期間中に表示されます。

- 管理者警告: サブスクリプションの有効期限が切れる30日前にStudioに表示されます。
- サポートされているバージョン:
  - 現在のリリース: Citrix Virtual Apps and Desktops 2411以降。
  - LTSR: 2203 CU6、2402 CU1、およびそれ以降のLTSRリリース

ユーザー/デバイスライセンス

Citrixは、ユーザー/デバイスライセンスモデルでどのようにユーザーにライセンスを割り当てますか?

ユーザー/デバイスライセンスモデルでは、ライセンスサーバーがライセンスを一意のユーザーIDに割り当てます。これにより、その単一ユーザーは無制限のデバイスから無制限の接続を行うことができます。ユーザーがデスクトップまたはデバイスに接続する場合、仮想デスクトップまたはアプリケーションにアクセスするには、そのユーザーに割り当てられた1つのライセンスが必要です。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。これらのライセンスを手動で割り当てることはできません。ライセンスは共有デバイスではなく、ユーザーに割り当てられます。一度ライセンスが割り当てられると、90日間非アクティブになるまで、別のユーザーに割り当てることはできません。詳細については、「ユーザー/デバイスライセンス」を参照してください。

Citrixは、ユーザー/デバイスライセンスモデルにおいて、ライセンスされたデバイスをどのように定義しますか?

ライセンスされたデバイスには、一意のエンドポイントデバイスIDが必要です。ユーザー/デバイスモデルでは、デバイスとは、Citrix Virtual Apps and Desktopsのインスタンスにアクセスするために、個人が使用することを許可したあらゆる機器を指します。共有デバイスの場合、1つのCitrix Virtual Apps and Desktopsユーザー/デバイスライセンスで、そのデバイスを共有する複数のユーザーをサポートできます。たとえば、共有デバイスは教室のワークステーションや病院の臨床ワークステーションなどです。

Citrix Virtual Desktops Standard Edition の同時接続ライセンスをユーザー/デバイスモデルに変換できますか？

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをCitrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスに変換することはできません。同様に、Citrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスをCitrix Virtual Desktops Standard Editionの同時使用ライセンスに変換することもできません。

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをお持ちで、ユーザー/デバイスライセンスモデルをご希望の場合は、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードしてください。

元	STANDARD同時接続へ	STANDARDユーザー/デバイスへ	ADVANCEDユーザー/デバイスへ	PREMIUMユーザー/デバイスへ
Citrix Virtual Desktops Standard Edition同時接続ライセンス	N/A	同時接続からユーザー/デバイスへの変換は許可されていません	ライセンスモデルを変換することはできませんが、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードすることはできます。	ライセンスモデルを変換することはできませんが、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードすることはできます。
Citrix Virtual Desktops スタンダード エディション ユーザー/デバイス ライセンス	ユーザー/デバイスから同時接続への変換は許可されていません	N/A	N/A	N/A

同時使用ライセンスとユーザー/デバイスライセンスの違い?

同時接続ライセンスは、デバイスの同時接続に基づいています。同時接続ライセンスは、デバイスがアクティブな接続を確立している場合にのみ使用されます。接続が終了すると、同時接続ライセンスはすぐに使用可能なライセンスプールに戻されます。このライセンスモデルは、一時的な使用におすすめです。ユーザー/デバイスライセンスは一定期間リースされ、リース期間が終了するまで他のユーザーは利用できません。

ユーザー/デバイスモデルにおける、同じ企業内でのユーザーとデバイスへのライセンス割り当て?

はい。両方のタイプを同じ企業内で使用できます。ライセンスサーバーは、使用状況に基づいてユーザーまたはデバイスにライセンスを最適に割り当てます。これらのライセンスを手動で割り当てることはできません。

ライセンスを付与するユーザーまたはデバイスの数をどのように決定すればよいですか?

適切なライセンス数を決定するために、ユースケースの要件を評価してください。ユーザー/デバイスライセンスは、無制限のデバイスから無制限の仮想デスクトップと仮想アプリへの無制限のアクセスを可能にします。同時接続ライセンスは、無制限のユーザーが使用できる単一のデバイスから無制限の仮想デスクトップと仮想アプリへの無制限のアクセスを可能にします。次の式を考慮してください。

```
(Number of total users) – (number of users that only access exclusively

 with shared devices) + (number shared devices) = total number

 of licenses to buy.



For example, there are 1000 total users at the hospital. If 700 of them
access only

Citrix Virtual Desktops from 300 shared devices in the hospital, the
number of

licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

ユーザー/デバイスモデルでは、ライセンスユーザーが自分の環境に接続するために使用できるデバイスの最大数?

各ライセンスユーザーは、接続されているかオフラインであるかにかかわらず、無制限のデバイスを使用できます。

ユーザー/デバイスモデルでは、ライセンスされたデバイスにアクセスできるユーザーの最大数?

各ライセンスデバイスは、組織内で無制限のユーザーにサービスを提供できます。

ユーザー/デバイスモデルでは、ライセンスユーザーが一度に利用できる仮想デスクトップまたはRBI Webアプリケーションの最大数?

各ライセンスユーザーは、無制限の仮想デスクトップまたはWebアプリケーションに接続できます。

既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できますか?

はい。既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できます。

承認されたユーザー/デバイスライセンスを解放するにはどうすればよいですか?

承認済みユーザー/デバイスの割り当てを解除するには、EULAの条項に従って`udadmin`ユーティリティを使用します。その後、ライセンスサーバーは次の適切なユーザー/デバイスにライセンスを割り当てます。詳細については、「ユーザーまたはデバイスのライセンスの表示または解放」を参照してください。

購入したユーザー/デバイスライセンス数を超過した場合、どうなりますか?

ユーザー/デバイスライセンスには10%の超過分が含まれており、これはライセンス生成時に含まれます。この超過分は、インストール済みのライセンス数にも含まれます。使用量の急増が、超過分を含むインストール済みの数を超えた場合、それ以上のユーザーのアクセスは拒否されます。より多くのユーザーのアクセスを有効にするには、新しいライセンスを購入して展開してください。

ライセンスの超過分を含め、すべてのライセンスが使用中の場合、ライセンスバーストモードにより、製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーを中断することなく追加のライセンスを購入するための時間を提供します。この期間は、15日経過するか、追加の小売ライセンスをインストールするかのいずれか早い方まで続きます。詳細については、「ライセンスバーストモード」を参照してください。

Director はライセンスキャッシュモードの状態を表示します。詳細については、「Director ダッシュボードのパネル」(/ja-jp/citrix-virtual-apps-desktops/2311/director/site-analytics.html#panels-on-the-director-dashboard)を参照してください。

ライセンスユーザーが一度に利用できる仮想アプリケーションの最大数はいくつですか?

各ライセンスユーザーは、無制限の数の仮想アプリケーションに接続できます。

ライセンスユーザーが組織を離れた場合、どうなりますか?

既存のライセンスユーザーが組織を離れる場合、Citrixに通知することなく、そのユーザーのライセンスを解放できます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは90日間アクティビティがないライセンスを自動的に解放します。この情報はEULAに指定された条項に従います。

ライセンスユーザーが長期間不在の場合、どうなりますか?

既存のライセンスユーザーが長期間不在の場合、Citrixに通知することなくライセンスを解放し、再割り当て可能にすることができます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。

組織内のライセンスデバイスを交換した場合、どうなりますか?

既存のライセンスデバイスを交換する場合、Citrixに通知することなくライセンスを解放し、再割り当て可能にすることができます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。

ライセンスデバイスが長期間サービス停止した場合、どうなりますか?

既存のライセンスデバイスが長期間サービス停止になった場合、Citrixに通知することなくライセンスを解放し、再割り当て可能にすることができます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは90日間アク

ティビティがないライセンスを自動的に解放します。この情報はEULAに指定された条項に従います。

ユーザーライセンスをデバイスライセンスに、またはその逆に、ライセンスをデバイスまたはユーザーに割り当てた後に切り替えることはできますか?

はい、できます。この変更は自動的に行われます。ライセンスサーバーは、使用パターンに基づいて、ユーザーまたはデバイスのいずれかにライセンスを割り当てます。使用パターンが変更された場合、ライセンスサーバーは新しい使用状況に基づいて割り当てを切り替えることがあります。ライセンスサーバーは常に、お客様にとって最も経済的な方法でライセンスを割り当てます。また、ライセンスサーバーは、90日間の割り当て期間が経過した後に**未使用**のライセンスを特定するためにライセンスを監視します。90日間の割り当て期間後に未使用と識別されたライセンスは、他のユーザーまたはデバイスに再割り当てできます。

同時使用ライセンス

同時使用モデルでは、Citrix Virtual Apps and Desktopsのライセンスを持つユーザーが一度に消費できる仮想デスクトップの最大数はいくつですか?

エンドポイントは多数のユーザーにサービスを提供でき、無制限の接続を許可します。

Citrix Virtual Apps and Desktops の以前のバージョンの同時使用ライセンスと、新しいユーザー/デバイスライセンスまたは同時使用ライセンスを単一のライセンスサーバーに展開できますか？

はい、できます。ユーザー/デバイスライセンスまたは同時使用ライセンスの展開をサポートするために、同じライセンスサーバーを引き続き使用できます。

同時使用ライセンスとユーザー/デバイスライセンスまたは同時使用ライセンスを単一のライセンスサーバーに展開できますか?

はい、できます。同時使用ライセンスとユーザー/デバイスライセンスまたは同時使用ライセンスの展開をサポートするために、同じライセンスサーバーを引き続き使用できます。

Citrix Virtual Apps and Desktops AdvancedおよびPremiumエディションには、Citrix Virtual Appsの同時使用ライセンスが含まれていますか?

Citrix Virtual Apps and Desktops AdvancedおよびPremiumのユーザー/デバイスライセンスには、互換性のためのみにCitrix Virtual Appsの同時使用ライセンスが含まれています。これらの同時使用ライセンスは、ユーザー/デバイスライセンスと互換性のない以前の製品バージョンでのみ使用できます。ユーザー/デバイスライセンスに含まれる同時使用互換ライセンスの使用は、XenApp 6.5より前のバージョンおよびXenDesktop 5.0 Service Pack 1より前のバージョンでのみ許可されます。

購入した同時使用ライセンス数を超過した場合、どうなりますか?

すべてのライセンスが使用中の場合、ライセンスバーストモードにより、製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーを中断することなく追加のライセンスを購入するための時間を提供します。この期間は、15日が経過するか、追加の小売ライセンスをインストールするかのいずれか早い方まで続きます。詳細については、ライセンスバーストモードを参照してください。

Directorはライセンスキャッシュモードの状態を表示します。詳細については、Directorダッシュボードのパネルを参照してください。

超過ライセンス

超過ライセンスはどのように入手できますか?

ユーザー/デバイス、ユーザー、またはデバイスのライセンスモデルをサポートする製品（Citrix Cloudを除く）には、アクセス拒否を防ぐために限られた数の追加ライセンスを使用できるライセンス超過機能が含まれています。超過機能は、ライセンスの権利ではなく、便宜のために提供されます。同時接続ライセンスとサーバーライセンスには超過機能は含まれていません。使用された超過ライセンスは、初回使用から30日以内に購入する必要がありますが、使用期間は30日に限定されません。Citrixは、新しい製品リリースで超過機能を削除する権利を留保します。詳細については、「ライセンス超過」を参照してください。

ライセンス超過をどのように識別できますか?

Citrix Licensing Managerで、超過しているライセンス数を含む使用状況情報を表示できます。Studioにも超過使用状況情報が含まれています。

超過ライセンスが消費されるとどうなりますか?

Citrix Virtual Apps and Desktops環境へのアクセスを有効にするために、インストールされているライセンスからライセンスが割り当てられます。この超過ライセンスは、他のライセンスと同等のアクセスと機能を提供します。

超過ライセンスが消費されたときにアラートを受け取ることはできますか?

現在、オーバードラフトライセンスが消費されたときに提供される特定の警告はありません。

超過ライセンスはどのくらいの期間消費できます?

最初に使用してから30日以内に使用されたオーバードラフトライセンスを購入してください。

その他の製品固有のライセンス情報

- シトリックス ADC
- シトリックス クラウド

- シトリックス エンドポイント マネジメント
- シトリックス ゲートウェイ
- XenServer
- Citrix ライセンス

マシンの負荷分散

> **注:**
>
> この機能は、すべてのカタログ（シングルセッションOSまたはマルチセッションOSカタログ）に適用されます。垂直負荷分散はマルチセッションOSマシンにのみ適用されます。

負荷分散は、サイトレベルとデリバリーグループレベルで構成できます。垂直と水平の2つのオプションがあります。デフォルトでは、水平負荷分散が有効になっています。

サイトレベルでの負荷分散設定

- **垂直負荷分散**。受信ユーザーセッションを、まだ最大負荷に達していない最も負荷の高いマシンに割り当てます。これにより、新しいマシンに移行する前に既存のマシンが飽和状態になります。既存のマシンから切断するユーザーは、それらのマシンの容量を解放します。その後、受信負荷はそれらのマシンに割り当てられます。垂直負荷分散はユーザーエクスペリエンスを低下させますが、コストを削減します（セッションは電源オンのマシン容量を最大化します）。

  例：それぞれ10セッション用に構成された2台のマシンがあるとします。最初のマシンが最初の10の同時セッションを処理します。2番目のマシンが11番目のセッションを処理します。

  > **ヒント:**
  >
  > マシンがホストできるセッションの最大数を指定するには、最大セッション数 ポリシー設定を使用します。
  >
  > あるいは、PowerShellを使用して、サイト全体で垂直負荷分散を有効または無効にできます。`Set-BrokerSite`コマンドレットで`UseVerticalScalingForRdsLaunches`設定を使用します。`UseVerticalScalingForRdsLaunches`設定の値を表示するには、

> `Get-BrokerSite`を使用します。詳細については、コマンドレットのヘルプを参照してください。

- **水平負荷分散**。受信ユーザーセッションを、利用可能な最も負荷の低い電源オンのマシンに割り当てます。水平負荷分散はユーザーエクスペリエンスを向上させますが、コストが増加します（より多くのマシンが電源オンのままになるため）。デフォルトでは、水平負荷分散が有効になっています。

  例：それぞれ10セッション用に構成された2台のマシンがあるとします。最初のマシンが5つの同時セッションを処理します。2番目のマシンも5つを処理します。

この機能を構成するには、**管理 > 完全な構成**から、左ペインで**設定**を選択します。**マルチセッションカタログの負荷分散**の下のオプションを選択します。

デリバリーグループレベルでの負荷分散設定

デリバリーグループレベルで負荷分散を構成すると、サイトレベルから継承された負荷分散設定を上書きできます。デリバリーグループレベルで垂直負荷分散を選択すると、各マシンの最大利用率を達成できます。これにより、パブリッククラウドでのコスト削減に役立ちます。この構成は、新しいデリバリーグループの作成時または既存のデリバリーグループの編集時に行うことができます。

水平負荷分散。セッションは電源オンのマシン間で分散されます。たとえば、それぞれ10セッション用に構成された2台のマシンがある場合、最初のマシンが5つの同時セッションを処理し、2番目のマシンも5つ処理します。

垂直負荷分散。セッションは電源オンのマシン容量を最大化し、マシンコストを節約します。たとえば、それぞれ10セッション用に構成された2台のマシンがある場合、最初のマシンが最初の10の同時セッションを処理します。2番目のマシンが11番目のセッションを処理します。

ローカルホストキャッシュ

Citrix Virtual Apps and Desktopsサイトデータベースが常に利用可能であることを保証するため、CitrixはMicrosoftの可用性に関するベストプラクティスに従い、フォールトトレラントなSQL Server展開から始めることを推奨します。(サポートされているSQL Serverの高可用性機能については、データベースを参照してください。)しかし、ネットワークの問題や中断により、ユーザーがアプリケーションやデスクトップに接続できなくなる可能性があります。

「ローカルホストキャッシュ」機能により、障害発生時でもサイト内の接続仲介操作を継続できます。オンプレミスのCitrix®環境で、Delivery Controller™とサイトデータベース間の接続が失敗

すると、障害が発生します。サイトデータベースに90秒間アクセスできない場合、ローカルホストキャッシュが作動します。

XenAppおよびXenDesktop 7.16以降、接続リース機能（以前のリリースにおける先行の高可用性機能）は製品から削除され、利用できなくなりました。

データコンテンツ

ローカルホストキャッシュには、メインデータベースの情報の一部である以下の情報が含まれます。

- サイトから公開されたリソースへの権限が割り当てられているユーザーおよびグループのID。
- 現在使用している、または最近使用した、サイトから公開されたリソースのユーザーのID。
- サイトで構成されているVDAマシン（リモートPCアクセスを含む）のID。
- 公開されたリソースへの接続に積極的に使用されているクライアントCitrix Receiver™マシンのID（名前とIPアドレス）。

また、メインデータベースが利用できなかった間に確立された、現在アクティブな接続に関する情報も含まれます。

- Citrix Receiver によって実行されたクライアントマシンのエンドポイント分析の結果。
- サイトに関与するインフラストラクチャマシン（NetScaler Gateway や StoreFront™ サーバーなど）の ID。
- ユーザーによる最近のアクティビティの日付、時刻、および種類。

動作の仕組み

次の図は、通常の操作中のローカルホストキャッシュのコンポーネントと通信パスを示しています。

ローカルホストキャッシュの通常の操作中の通信パスの図(/en-us/citrix-virtual-apps-desktops/2311/media/lhc-normal1.png)

通常の操作中

- Controller上の *プリンシパルブローカー*（Citrix Broker Service）は、StoreFrontからの接続要求を受け入れます。ブローカーはサイトデータベースと通信し、Controllerに登録されているVDAにユーザーを接続します。
- Citrix Config Synchronizer Service (CSS) は、約5分ごとにブローカーに問い合わせて、変更があったかどうかを確認します。これらの変更は、管理者によって開始されたもの（デリバリー

グループのプロパティの変更など）である場合もあれば、システムアクション（マシンの割り当てなど）である場合もあります。

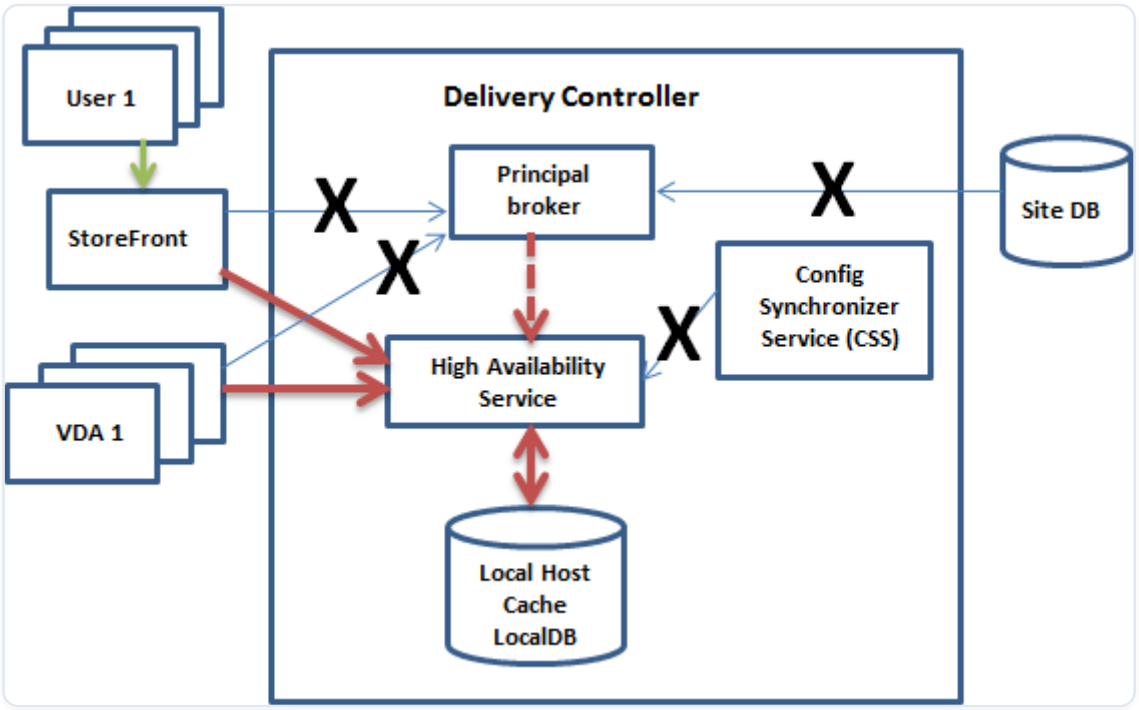
- 前回のチェック以降に構成変更があった場合、CSSは情報をController上のセカンダリブローカーに同期（コピー）します。（セカンダリブローカーは高可用性サービスとも呼ばれます。）

  前回のチェック以降に変更された項目だけでなく、すべての構成データがコピーされます。CSSは構成データをController上のMicrosoft SQL Server Express LocalDBデータベースにインポートします。このデータベースはローカルホストキャッシュデータベースと呼ばれます。CSSは、ローカルホストキャッシュデータベースの情報がサイトデータベースの情報と一致することを確認します。ローカルホストキャッシュデータベースは、同期が行われるたびに再作成されます。

  Microsoft SQL Server Express LocalDB (ローカルホストキャッシュデータベースで使用) は、Controller をインストールするときに自動的にインストールされます。(コマンドラインから Controller をインストールする際に、このインストールを禁止できます。) ローカルホストキャッシュデータベースは、複数の Controller 間で共有できません。ローカルホストキャッシュデータベースをバックアップする必要はありません。構成変更が検出されるたびに再作成されます。

- 前回のチェック以降に変更がない場合、データはコピーされません。

次の図は、プリンシパルブローカーがサイトデータベースとの接続を失った場合（停止が開始された場合）の通信パスの変化を示しています。



停止中

停止が開始されると、次のようになります。

- セカンダリブローカーは接続要求のリッスンと処理を開始します。
- 停止が開始された時点では、セカンダリブローカーは現在のVDA登録データを持っていませんが、VDAがセカンダリブローカーと通信すると、登録プロセスがトリガーされます。そのプロセス中に、セカンダリブローカーはそのVDAに関する現在のセッション情報も取得します。
- セカンダリブローカーが接続を処理している間、ブローカリングプリンシパルは接続の監視を続けます。接続が復元されると、ブローカリングプリンシパルはセカンダリブローカーに接続情報のリスニングを停止するよう指示し、ブローカリングプリンシパルはブローカリング操作を再開します。VDAが次にブローカリングプリンシパルと通信するときに、登録プロセスがトリガーされます。セカンダリブローカーは、以前の停止から残っているVDA登録をすべて削除します。CSSは、展開で構成変更が発生したことを認識すると、情報の同期を再開します。

同期中に停止が開始されるという万が一の事態が発生した場合、現在のインポートは破棄され、最後に認識された構成が使用されます。

イベントログには、同期と停止に関する情報が記載されています。

停止モードでの操作に時間制限はありません。

通常モードと停止モード間の移行は、既存のセッションには影響しません。新しいセッションの起動のみに影響します。

意図的に停止をトリガーすることもできます。その理由と方法の詳細については、「停止の強制」を参照してください。

複数のControllerがあるサイト

CSSは、他のタスクの中でも、ゾーン内のすべてのControllerに関する情報をセカンダリブローカーに定期的に提供します。（展開に複数のゾーンが含まれていない場合、このアクションはサイト内のすべてのControllerに影響します。）この情報を持つことで、各セカンダリブローカーは、ゾーン内の他のControllerで実行されているすべてのピアセカンダリブローカーについて認識します。

セカンダリブローカーは、別のチャネルで相互に通信します。これらのブローカーは、実行されているマシンのFQDN名のアルファベット順リストを使用して、停止が発生した場合にゾーンでブローカー操作を行うセカンダリブローカーを決定（選出）します。停止中、すべてのVDAは選出されたセカンダリブローカーに登録します。ゾーン内の選出されていないセカンダリブローカーは、受信接続およびVDA登録要求を積極的に拒否します。

停止中に選出されたセカンダリブローカーが失敗した場合、別のセカンダリブローカーが引き継ぐために選出され、VDAは新しく選出されたセカンダリブローカーに登録します。

停止中にControllerが再起動された場合：

- そのControllerが選出されたブローカーでない場合、再起動による影響はありません。
- そのControllerが選出されたブローカーである場合、別のControllerが選出され、VDAが登録されます。再起動されたControllerが起動すると、自動的にブローカリングを引き継ぎ、VDAが再度登録されます。このシナリオでは、登録中にパフォーマンスが影響を受ける可能性があります。

通常の操作中にControllerの電源を切り、停止中に電源を入れた場合、そのControllerがブローカーとして選出されると、ローカルホストキャッシュはそのControllerで使用できません。

イベントログには、選出に関する情報が記載されています。

停止中に利用できないもの、およびその他の違い

停止モードでの運用に時間制限はありません。ただし、Citrixは可能な限り迅速に接続を復元することを推奨しています。

停止中：

- Studioを使用できません。
- PowerShell SDKへのアクセスは制限されます。
    - まず、次の操作を行う必要があります。
        - 値が1のレジストリキー `EnableCssTestMode` を追加します: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
        - ポート89を使用します: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
    - これらのコマンドを実行した後、次のものにアクセスできます。
        - すべての `Get-Broker*` コマンドレット。
- ハイパーバイザーの資格情報はホストサービスから取得できません。すべてのマシンは不明な電源状態になり、電源操作を発行できません。ただし、ホスト上で電源がオンになっているVMは、接続要求に使用できます。

- 割り当てられたマシンは、通常の操作中に割り当てが行われた場合にのみ使用できます。停止中に新しい割り当てを行うことはできません。
- Remote PC Accessマシンの自動登録と構成はできません。ただし、通常の操作中に登録および構成されたマシンは使用可能です。
- サーバーでホストされているアプリケーションおよびデスクトップのユーザーは、リソースが異なるゾーンにある場合、構成されたセッション制限よりも多くのセッションを使用する可能性があります。
- ユーザーは、現在アクティブ/選出されているセカンダリブローカーを含むゾーン内の登録済みVDAからのみアプリケーションとデスクトップを起動できます。ゾーンをまたぐ起動（あるゾーンのセカンダリブローカーから別のゾーンのVDAへの起動）は、停止中はサポートされません。
- 配信グループ内のVDAのスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了したときに再起動が開始されます。これは意図しない結果を招く可能性があります。詳細については、「データベース停止により遅延するスケジュールされた再起動」を参照してください。
- ゾーン設定は構成できません。構成されている場合、セッション起動時に設定は考慮されません。
- タグがゾーンの指定に使用されるタグ制限は、セッション起動ではサポートされていません。このようなタグ制限が構成されており、StoreFrontストアの高度なヘルスチェックオプションが有効になっている場合、セッションが断続的に起動に失敗する可能性があります。

アプリケーションとデスクトップのサポート

ローカルホストキャッシュは、サーバーホスト型アプリケーションとデスクトップ、および静的（割り当て済み）デスクトップをサポートします。

ローカルホストキャッシュは、プールされたデリバリーグループ内のデスクトップVDAを次のようにサポートします。

- デフォルトでは、プールされた配信グループ（MCSまたはCitrix Provisioning™によって作成されたもの）内の電源管理されたデスクトップVDAで`ShutdownDesktopsAfterUse`プロパティが有効になっている場合、ローカルホストキャッシュイベント中に新しい接続には利用できません。このデフォルトを変更して、ローカルホストキャッシュ中にこれらのデスクトップを使用できるようにすることができます。

  ただし、停止中の電源管理に頼ることはできません。（電源管理は通常の操作が再開された後に再開されます。）また、これらのデスクトップは再起動されていないため、以前のユーザーのデータが含まれている可能性があります。

- デフォルトの動作を上書きするには、サイト全体で、および影響を受ける各デリバリーグループで有効にする必要があります。次のPowerShellコマンドレットを実行します。

  サイト全体：

  ```
  Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
  ```

  影響を受ける各デリバリーグループに対して、次のPowerShellコマンドを実行します。

  ```
  Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
  ```

デリバリーグループ設定をデフォルトで有効にするには、次のPowerShellコマンドを実行します。

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

この設定は、この設定を有効にした後に作成されるすべての新しいデリバリーグループに適用されます。

既存のデリバリーグループでこの設定を有効にするには、次のPowerShellコマンドを実行します。

```
Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
```

サイトおよびデリバリーグループでこの機能を有効にしても、通常の操作中に構成された `ShutdownDesktopsAfterUse` プロパティの動作に影響はありません。この機能が有効になっている場合、LHCイベントが完了してもVDAは自動的に再起動しません。プールされたデリバリーグループの電源管理されたデスクトップVDAは、VDAが再起動されるまで以前のセッションのデータを保持できます。これは、ユーザーが非LHC操作中にVDAからログオフした場合、または再起動が手動でトリガーされた場合に発生する可能性があります。

> **重要:**
>
> サイトレベルで ReuseMachinesWithoutShutdownInOutageAllowed を、デリバリーグループレベルで ReuseMachinesWithoutShutdownInOutage を有効にしないと、ローカルホストキャッシュイベント中に、プールされたデリバリーグループ内の電源管理されたデスクトップVDAへのすべてのセッション起動試行が失敗します。

RAM サイズに関する考慮事項

LocalDBサービスは、約1.2 GBのRAM（データベースキャッシュに最大1 GB、SQL Server Express LocalDBの実行に200 MB）を使用できます。セカンダリブローカーは、多数のログオンが発生する長時間の停止（たとえば、10,000ユーザーで12時間）の場合、最大1 GBのRAMを使用できます。これらのメモリ要件は、コントローラーの通常のRAM要件に追加されるため、RAM容量の合計を増やす必要がある場合があります。

サイトデータベースにSQL Server Expressインストールを使用している場合、サーバーには2つのsqlserver.exeプロセスがあります。

CPU コアとソケット構成に関する考慮事項

コントローラーのCPU構成、特にSQL Server Express LocalDBで利用可能なコア数は、メモリ割り当てよりもさらに、ローカルホストキャッシュのパフォーマンスに直接影響します。このCPUオーバーヘッドは、データベースにアクセスできず、セカンダリブローカーがアクティブな停止期間中にのみ観察されます。

LocalDBは複数のコア（最大4つ）を使用できますが、単一のソケットに制限されています。ソケットを追加してもパフォーマンスは向上しません（たとえば、各ソケットに1コアを持つ4つのソケット）。代わりに、Citrixは複数のソケットと複数のコアを使用することを推奨しています。Citrixのテストでは、2x3（2ソケット、3コア）構成が4x1および6x1構成よりも優れたパフォーマンスを提供しました。

ストレージに関する考慮事項

停止中にユーザーがリソースにアクセスすると、LocalDBは増大します。たとえば、1秒あたり10ログオンで実行されるログオン/ログオフテスト中に、データベースは2～3分ごとに1 MB増加しました。通常の操作が再開されると、ローカルデータベースが再作成され、スペースが返されます。ただし、停止中のデータベースの増大を許容するために、LocalDBがインストールされているドライブには十分な空き容量が必要です。ローカルホストキャッシュは、停止中により多くのI/Oも発生させます。具体的には、1秒あたり約3 MBの書き込みと、数十万回の読み取りが発生します。

パフォーマンスに関する考慮事項

障害発生時には、1つのセカンダリブローカーがすべての接続を処理するため、通常の操作中に複数のコントローラー間で負荷分散を行うサイト（またはゾーン）では、選出されたセカンダリブローカーが障害発生時に通常よりもはるかに多くの要求を処理する必要がある場合があります。したがって、CPUの要求は高くなります。サイト（ゾーン）内のすべてのセカンダリブローカーは、ローカルホストキャッシュデータベースと影響を受けるすべてのVDAによって課される追加の

負荷を処理できる必要があります。これは、障害発生時に選出されるセカンダリブローカーが変更される可能性があるためです。

VDIの制限:

- シングルゾーンVDI展開では、障害発生時に最大10,000台のVDAを効果的に処理できます。
- マルチゾーンVDI展開では、停止中に各ゾーンで最大10,000のVDA、サイト全体で最大40,000のVDAを効果的に処理できます。例えば、以下の各サイトは停止中に効果的に処理できます。
  - 4つのゾーンを持ち、各ゾーンに10,000のVDAを含むサイト。
  - 7つのゾーンを持ち、1つは10,000のVDAを含み、残りの6つはそれぞれ5,000のVDAを含むサイト。

停止中、サイト内の負荷管理が影響を受ける可能性があります。負荷評価器（特にセッション数ルール）が超過する可能性があります。

すべてのVDAがセカンダリブローカーに登録するのにかかる時間の間、そのサービスは現在のセッションに関する完全な情報を持っていない可能性があります。そのため、その期間中のユーザー接続要求は、既存のセッションへの再接続が可能であったとしても、新しいセッションが起動される結果となる可能性があります。この期間（「新しい」セカンダリブローカーが再登録中にすべてのVDAからセッション情報を取得する間）は避けられません。停止が開始されたときに接続されているセッションは移行期間中に影響を受けませんが、新しいセッションやセッションの再接続は影響を受ける可能性があります。

この期間は、VDAが登録する必要がある場合に発生します。

- 停止の開始: プリンシパルブローカーからセカンダリブローカーに移行するとき。
- 停止中のセカンダリブローカーの障害: 障害が発生したセカンダリブローカーから新しく選出されたセカンダリブローカーに移行するとき。
- 停止からの復旧: 通常の運用が再開され、プリンシパルブローカーが制御を再開するとき。

Citrix Broker Protocolの`HeartbeatPeriodMs`レジストリ値を下げることで、この間隔を短縮できます（デフォルト = 600000 ms、つまり10分）。このハートビート値は、VDAがpingに使用する間隔の2倍であるため、デフォルト値では5分ごとにpingが実行されます。

例えば、次のコマンドはハートビートを5分（300000ミリ秒）に変更し、2.5分ごとにpingが実行されるようにします。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

ハートビート値を変更する際は注意してください。頻度を増やすと、通常モードと障害モードの両方でControllerへの負荷が増大します。

VDAがどれだけ迅速に登録されても、この間隔を完全に排除することはできません。

セカンダリブローカー間の同期にかかる時間は、オブジェクト（VDA、アプリケーション、グループなど）の数が増えるにつれて長くなります。例えば、5000のVDAを同期するには10分以上かかる場合があります。

XenApp 6.xリリースとの違い

このローカルホストキャッシュの実装は、XenApp 6.xおよびそれ以前のXenAppリリースにおけるローカルホストキャッシュ機能と同じ名前を共有していますが、大幅な改善が加えられています。この実装はより堅牢で、破損の影響を受けにくいです。定期的な`dsmaint`コマンドの必要性を排除するなど、メンテナンス要件が最小限に抑えられています。このローカルホストキャッシュは、技術的には全く異なる実装です。

ローカルホストキャッシュの管理

ローカルホストキャッシュが正しく機能するには、各ControllerのPowerShell実行ポリシーをRemoteSigned、Unrestricted、またはBypassに設定する必要があります。

SQL Server エクスプレス ローカルDB

ローカルホストキャッシュが使用するMicrosoft SQL Server Express LocalDBソフトウェアは、Controllerをインストールするか、バージョン7.9より前のControllerをアップグレードすると自動的にインストールされます。このデータベースと通信するのはセカンダリブローカーのみです。PowerShellコマンドレットを使用してこのデータベースに関する何も変更することはできません。LocalDBはController間で共有できません。

SQL Server Express LocalDBデータベースソフトウェアは、ローカルホストキャッシュが有効になっているかどうかにかかわらずインストールされます。

そのインストールを防ぐには、`XenDesktopServerSetup.exe`コマンドを使用してControllerをインストールまたはアップグレードし、`/exclude "Local Host Cache Storage (LocalDB)"`オプションを含めます。ただし、ローカルホストキャッシュ機能はデータベースなしでは機能せず、セカンダリブローカーで別のデータベースを使用することはできないことに注意してください。

このLocalDBデータベースのインストールは、サイトデータベースとして使用するためにSQL Server Expressをインストールするかどうかには影響しません。

以前のSQL Server Express LocalDBバージョンを新しいバージョンに置き換える方法については、「Replace SQL Server Express LocalDB」を参照してください。

製品のインストールとアップグレード後のデフォルト設定

Citrix Virtual Apps and Desktopsの新規インストール時（最小バージョン7.16）には、ローカルホストキャッシュが有効になります。

アップグレード後（バージョン7.16以降）は、展開全体で10,000未満のVDAがある場合、ローカルホストキャッシュが有効になります。

ローカルホストキャッシュの有効化と無効化

- ローカルホストキャッシュを有効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  ローカルホストキャッシュが有効になっているかどうかを確認するには、`Get-BrokerSite`と入力します。`LocalHostCacheEnabled`プロパティが`True`であることを確認してください。
- ローカルホストキャッシュを無効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

注意：XenAppおよびXenDesktop 7.16以降、接続リース（バージョン7.6以降のローカルホストキャッシュに先行する機能）は製品から削除され、利用できなくなりました。

ローカルホストキャッシュが機能していることを確認する

ローカルホストキャッシュが正しく設定され、機能していることを確認するには：

- 同期インポートが正常に完了していることを確認します。イベントログを確認してください。
- 各Delivery ControllerにSQL Server Express LocalDBデータベースが作成されていることを確認します。これにより、必要に応じてセカンダリブローカーが引き継ぐことができることが確認されます。
  - Delivery Controllerサーバーで、`C:\Windows\ServiceProfiles\NetworkService`に移動します。
  - `HaDatabaseName.mdf`と`HaDatabaseName_log.ldf`が作成されていることを確認します。
- Delivery Controllerで障害を強制的に発生させます。ローカルホストキャッシュが機能することを確認したら、すべてのControllerを通常モードに戻すことを忘れないでください。これには約15分かかる場合があります。

イベントログ

イベントログは、同期と停止が発生した時期を示します。イベントビューアーログでは、停止モードは*HA モード.** と呼ばれます。

構成同期サービス:

通常の操作中に、CSSがローカルホストキャッシュブローカーを使用して構成データをローカルホストキャッシュデータベースにインポートすると、次のイベントが発生する可能性があります。

- 503: Citrix Config Sync Serviceが更新された構成を受信しました。このイベントは、同期プロセスの開始を示します。
- 504: Citrix Config Sync Serviceが更新された構成をインポートしました。構成のインポートが正常に完了しました。
- 505: Citrix Config Sync Serviceがインポートに失敗しました。構成のインポートは正常に完了しませんでした。以前に正常な構成が利用可能な場合、障害発生時にそれが使用されます。ただし、それは現在の構成から古くなっています。以前の構成が利用できない場合、サービスは障害発生時にセッションブローカーに参加できません。この場合、トラブルシューティングセクションを参照し、Citrixサポートに連絡してください。
- 507: システムが障害モードであり、ローカルホストキャッシュブローカーがブローカー処理に使用されているため、Citrix Config Sync Serviceがインポートを中止しました。サービスは新しい構成を受信しましたが、障害が発生したためインポートは中止されました。これは予期される動作です。
- 510: プライマリ構成サービスから構成サービス構成データが受信されませんでした。
- 517: プライマリブローカーとの通信に問題がありました。
- 518: セカンダリブローカー（高可用性サービス）が実行されていないため、構成同期スクリプトが中止されました。

高可用性サービス:

このサービスは、ローカルホストキャッシュブローカーとも呼ばれます。

- 3502: 停止が発生し、ローカルホストキャッシュブローカーがブローカー操作を実行しています。
- 3503: 停止が解決され、通常の操作が再開されました。
- 3504: どのLocal Host Cacheブローカーが選出されたか、および選出に関与した他のLocal Host Cacheブローカーを示します。

- 3507: 選出されたブローカーでLocal Host Cacheモードがアクティブであることを示す、Local Host Cacheのステータス更新を2分ごとに提供します。停止期間、VDA登録、セッション情報を含む停止の概要が含まれます。
- 3508: 選出されたブローカーでLocal Host Cacheがアクティブでなくなり、通常の操作が復元されたことを通知します。停止期間、Local Host Cacheイベント中に登録されたマシンの数、LHCイベント中の起動成功数を含む停止の概要が含まれます。
- 3509: 非選出ブローカーでLocal Host Cacheがアクティブであることを通知します。2分ごとの停止期間が含まれ、選出されたブローカーを示します。
- 3510: 非選出ブローカーでLocal Host Cacheがアクティブでなくなったことを通知します。停止期間が含まれ、選出されたブローカーを示します。

停止を強制する

意図的に停止を強制したい場合があります。

- ネットワークが繰り返し停止したり復旧したりする場合。ネットワークの問題が解決するまで停止を強制することで、通常モードと停止モード間の継続的な移行（およびそれに伴う頻繁なVDA登録ストーム）を防ぎます。
- ディザスタリカバリ計画をテストするため。
- Local Host Cacheが正しく機能していることを確認するため。
- サイトデータベースサーバーの交換または保守中。

停止を強制するには、Delivery Controllerを含む各サーバーのレジストリを編集します。`HKLM\Software\Citrix\DesktopServer\LHC`で、`OutageModeForced`を`REG_DWORD`として`1`に作成して設定します。この設定により、データベースの状態に関係なく、Local Host Cacheブローカーは停止モードに入ります。値を`0`に設定すると、Local Host Cacheブローカーは停止モードを終了します。

イベントを確認するには、`C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`にある`Current_HighAvailabilityService`ログファイルを監視します。

トラブルシューティング

Local Host Cacheデータベースへの同期インポートが失敗し、505イベントが投稿された場合、いくつかのトラブルシューティングツールが利用可能です。

CDFトレース: `ConfigSyncServer`と`BrokerLHC`モジュールのオプションが含まれています。これらのオプションは、他のブローカーモジュールとともに、問題の特定に役立つでしょう。

レポート: 同期インポートが失敗した場合、レポートを生成できます。このレポートは、エラーの原因となっているオブジェクトで停止します。このレポート機能は同期速度に影響するため、Citrixは使用しないときは無効にすることを推奨します。

CSSトレースレポートを有効にして生成するには、次のコマンドを入力します。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTMLレポートは`C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htm`に投稿されます。

レポートが生成されたら、レポート機能を無効にするには次のコマンドを入力します。

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

ブローカー構成のエクスポート: デバッグ目的で正確な構成を提供します。

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

例: `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`。

ローカルホストキャッシュのPowerShellコマンド

PowerShellコマンドを使用して、Delivery Controllerでローカルホストキャッシュ (LHC) を管理できます。

PowerShellモジュールは、Delivery Controllerの次の場所にあります。

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **重要:**
>
> このモジュールはDelivery Controllerでのみ実行してください。

PowerShell モジュールのインポート

モジュールをインポートするには、Delivery Controllerで次を実行します。

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

LHC を管理するための PowerShell コマンド

以下のコマンドは、Delivery Controller で LHC モードをアクティブ化および管理するのに役立ちます。

コマンドレット	機能
`Enable-LhcForcedOutageMode`	ブローカーをLHCモードにします。`Enable-LhcForcedOutageMode`が適切に機能するためには、ConfigSyncサービスによってLHCデータベースファイルが正常に作成されている必要があります。このコマンドレットは、実行されたDelivery ControllerでのみLHCを強制します。LHCをアクティブにするには、このコマンドをゾーン内のすべてのDelivery Controllerで実行する必要があります。
`Disable-LhcForcedOutageMode`	ブローカーをLHCモードから解除します。このコマンドレットは、実行されたDelivery ControllerでのみLHCモードを無効にします。`Disable-LhcForcedOutageMode`は、ゾーン内のすべてのDelivery Controllerで実行する必要があります。
`Set-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を設定します。時間間隔は60秒（1分）から3600秒（1時間）まで設定できます。この設定は、実行されたDelivery Controllerにのみ適用されます。Delivery Controller間で一貫性を持たせるには、このコマンドレットを各Delivery Controllerで実行することを検討してください。例: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を、デフォルト値の 300 秒 (5 分) に設定します。この設定は、実行された Delivery Controller にのみ適用されます。Delivery Controller 間の一貫性を保つために、この cmdlet を各 Delivery

コマンドレット	機能
	Controller で実行することを検討してください。
`Enable-LhcHighAvailabilitySDK`	実行された Delivery Controller 内のすべての `Get-Broker*` コマンドレットへのアクセスを有効にします。
`Disable-LhcHighAvailabilitySDK`	実行された Delivery Controller 内の Broker コマンドレットへのアクセスを無効にします。

注:

- Delivery Controller で `Get-Broker*` コマンドレットを実行するときは、ポート 89 を使用します。例:
  - `Get-BrokerMachine -AdminAddress localhost:89`
- LHC モードでない場合、Delivery Controller 上の LHC Broker は構成情報のみを保持します。
- LHC モード中、選出された Delivery Controller 上の LHC Broker は以下の情報を保持します。
  - リソースの状態
  - セッションの詳細
  - VDA の登録
  - 構成情報

セキュリティキーの管理

重要:

- この機能は、StoreFront™ 1912 LTSR CU2以降と組み合わせて使用する必要があります。

- Secure XML機能は、Citrix ADCおよびCitrix Gatewayリリース12.1以降でのみサポートされています。

注:

Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

この機能を使用すると、承認されたStoreFrontおよびCitrix Gatewayマシンのみがデリバリーコントローラーと通信できるようになります。この機能を有効にすると、キーを含まないすべての要求はブロックされます。この機能を使用して、内部ネットワークから発生する攻撃から保護するための追加のセキュリティ層を追加します。

この機能を使用するための一般的なワークフローは次のとおりです。

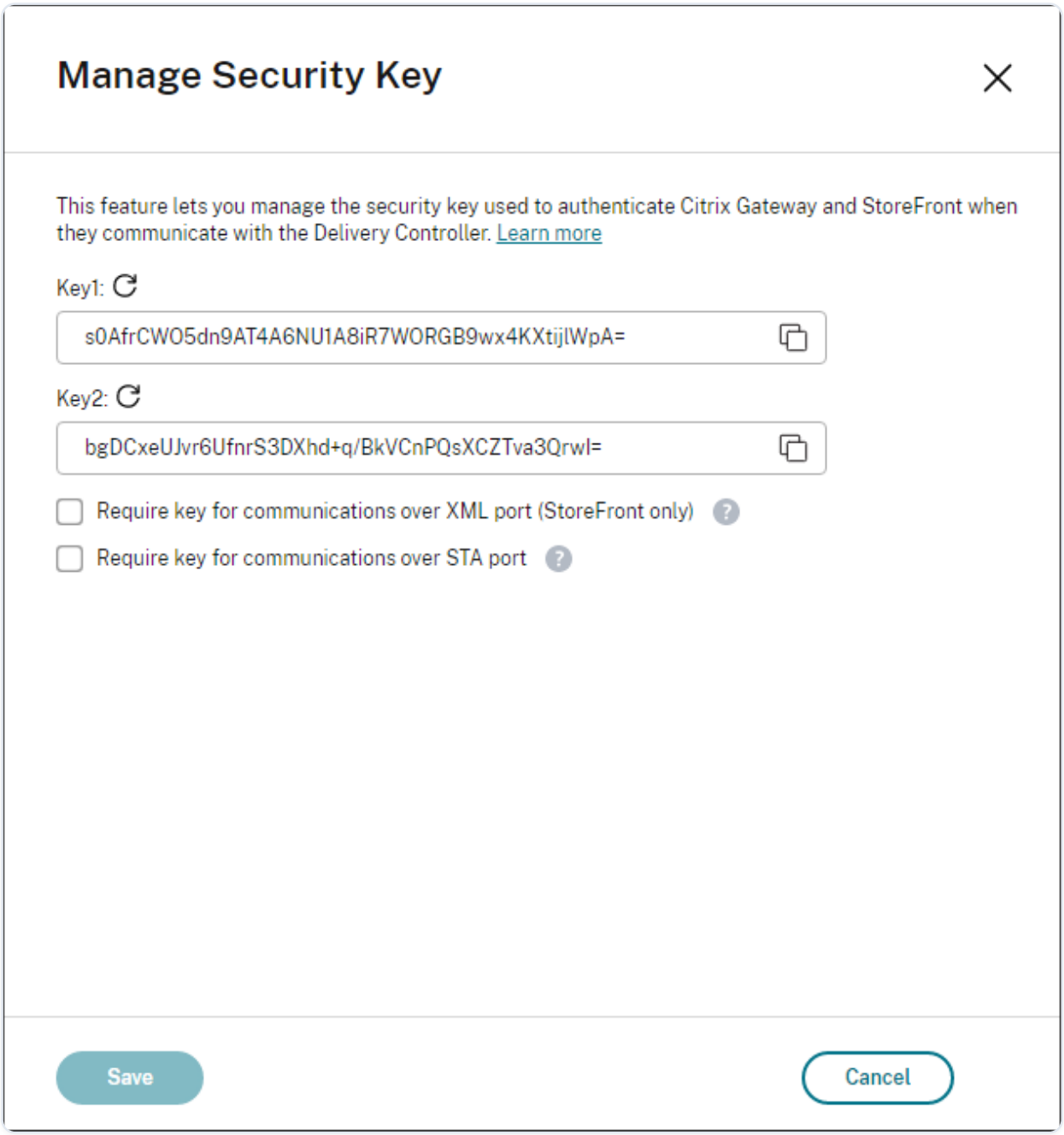
1. Web Studioで機能設定を表示できるようにします。
2. サイトの設定を構成します。
3. StoreFrontの設定を構成します。
4. Citrix ADCの設定を構成します。

サイトの設定を構成する

Web StudioまたはPowerShellを使用して、サイトのセキュリティキー設定を構成できます。

Web Studioを使用する

1. Web Studio にサインインし、左側のペインで**設定**を選択します。
2. **セキュリティキーの管理**タイルを見つけて、**編集**をクリックします。**セキュリティキーの管理**ページが表示されます。



3. 更新アイコンをクリックしてキーを生成します。

重要:

- 使用可能なキーは2つあります。XMLポートおよびSTAポートを介した通信には、同じキーまたは異なるキーを使用できます。一度に1つのキーのみを使用することをお勧めします。未使用のキーは、キーのローテーションにのみ使用されます。
- すでに使用中のキーを更新するために更新アイコンをクリックしないでください。クリックすると、サービスが中断されます。

4. 通信にキーが必要な場所を選択します。

   - **XMLポートを介した通信にキーを要求する（StoreFrontのみ）**。選択した場合、XMLポートを介した通信を認証するためにキーを要求します。StoreFrontはこのポートを介してCitrix Cloudと通信します。XMLポートの変更については、Knowledge Centerの記事CTX127945を参照してください。
   - **STAポートを介した通信にキーを要求する**。選択した場合、STAポートを介した通信を認証するためにキーを要求します。Citrix GatewayとStoreFrontはこのポートを介してCitrix Cloudと通信します。STAポートの変更については、Knowledge Centerの記事CTX101988を参照してください。

5. **「保存」**をクリックして変更を適用し、ウィンドウを閉じます。

PowerShell を使用する

以下は、Web Studioの操作に相当するPowerShellの手順です。

1. Citrix Virtual Apps and Desktops Remote PowerShell SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します。

   - `Add-PSSnapIn Citrix*`

3. 次のコマンドを実行して、キーを生成し、Key1 をセットアップします。

   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`

4. 次のコマンドを実行して、キーを生成し、Key2 をセットアップします。

   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`

5. 次のコマンドのいずれかまたは両方を実行して、通信の認証でキーの使用を有効にします。

   - XML ポート経由で通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - STAポート経由の通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

StoreFrontの設定を構成する

サイトの構成が完了したら、PowerShellを使用してStoreFrontの関連設定を構成する必要があります。

StoreFront サーバーで、以下の PowerShell コマンドを実行します。

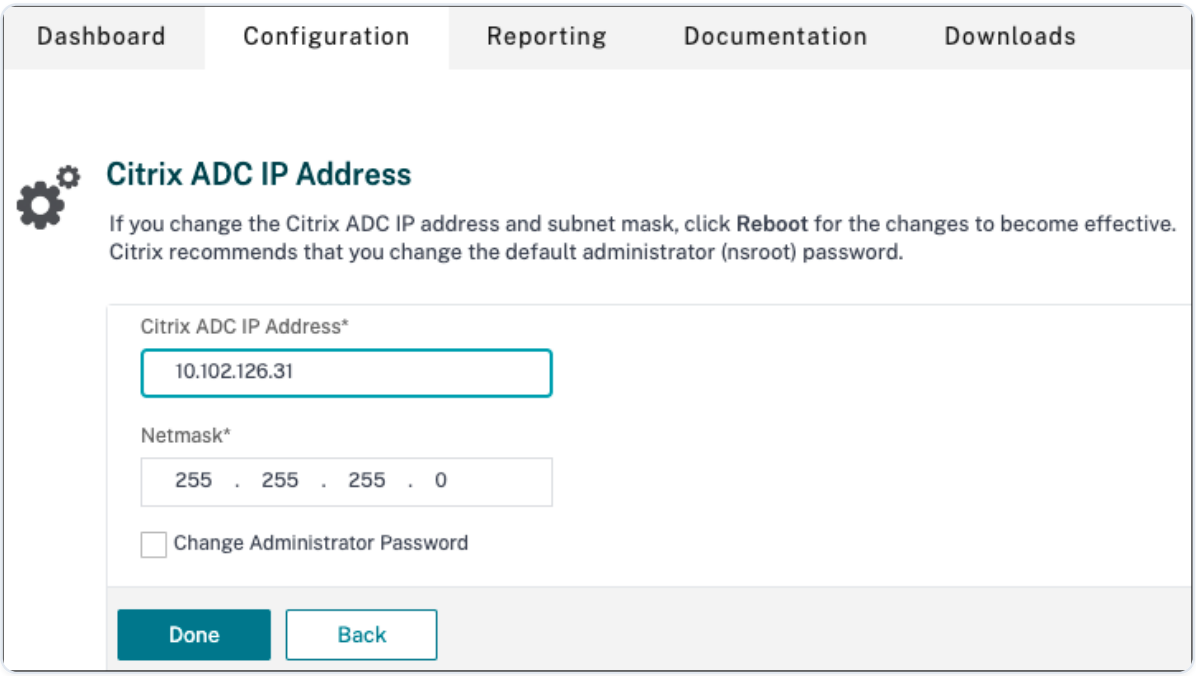
- XMLポートを介した通信用のキーを構成するには、`Get-STFStoreServie`コマンドと`Set-STFStoreService`コマンドを使用します。例：
  - `PS C:\> Set-STFStoreFarm $farm -Farmtype XenDesktop -Port 80 -TransportType HTTP -Servers <domain name1, domain name2> -XMLValidationEnabled $true -XMLValidationSecret <the key you generated in Web Studio>`
- STAポートを介した通信用のキーを構成するには、`New-STFSecureTicketAuthority`コマンドを使用します。例：
  - `PS C:\> $sta = New-STFSecureTicketAuthority –StaUrl <STA URL> -StaValidationEnabled $true -StavalidationSecret <the key you generated in Web Studio>`

ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

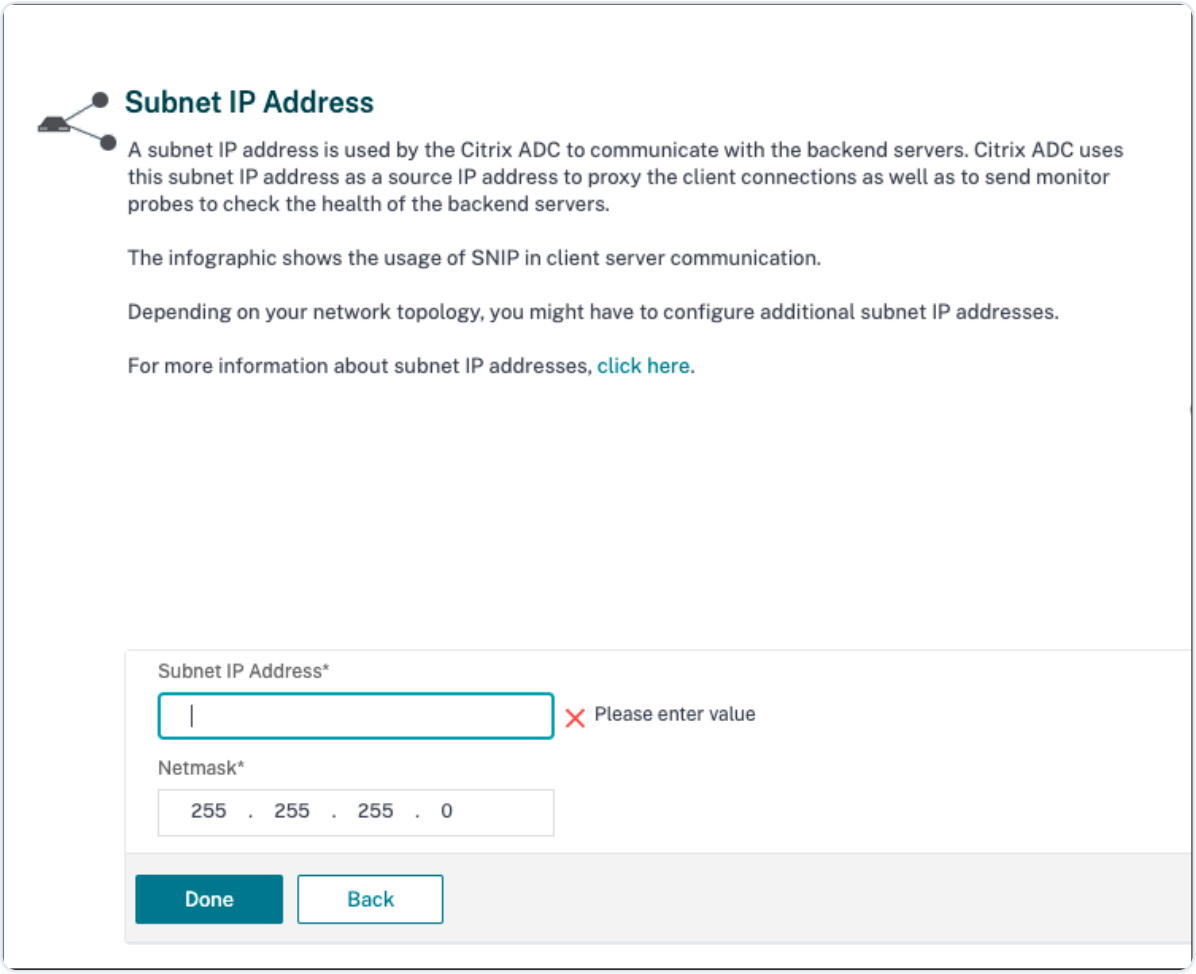
Citrix ADCの設定を構成する

> **注:**
>
> Citrix ADCをゲートウェイとして使用しない限り、Citrix ADCのこの機能の構成は不要です。Citrix ADCを使用する場合は、次の手順に従います。

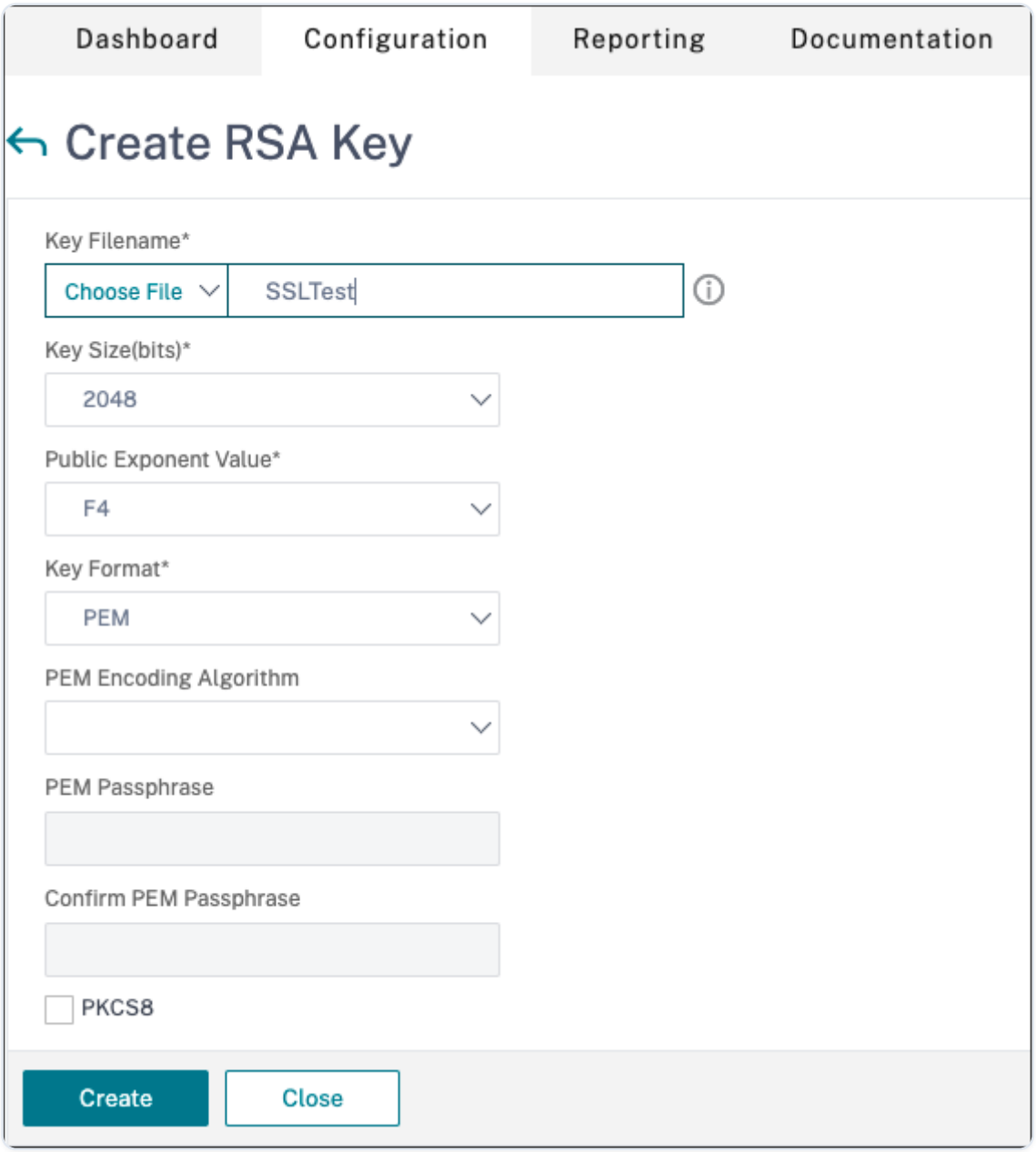
1. 次の前提条件となる構成がすでに設定されていることを確認してください。
   - 次のCitrix ADC関連のIPアドレスが構成されています。
     - Citrix ADCコンソールにアクセスするためのCitrix ADC管理IP (NSIP) アドレス。詳細については、「NSIPアドレスの構成」を参照してください。



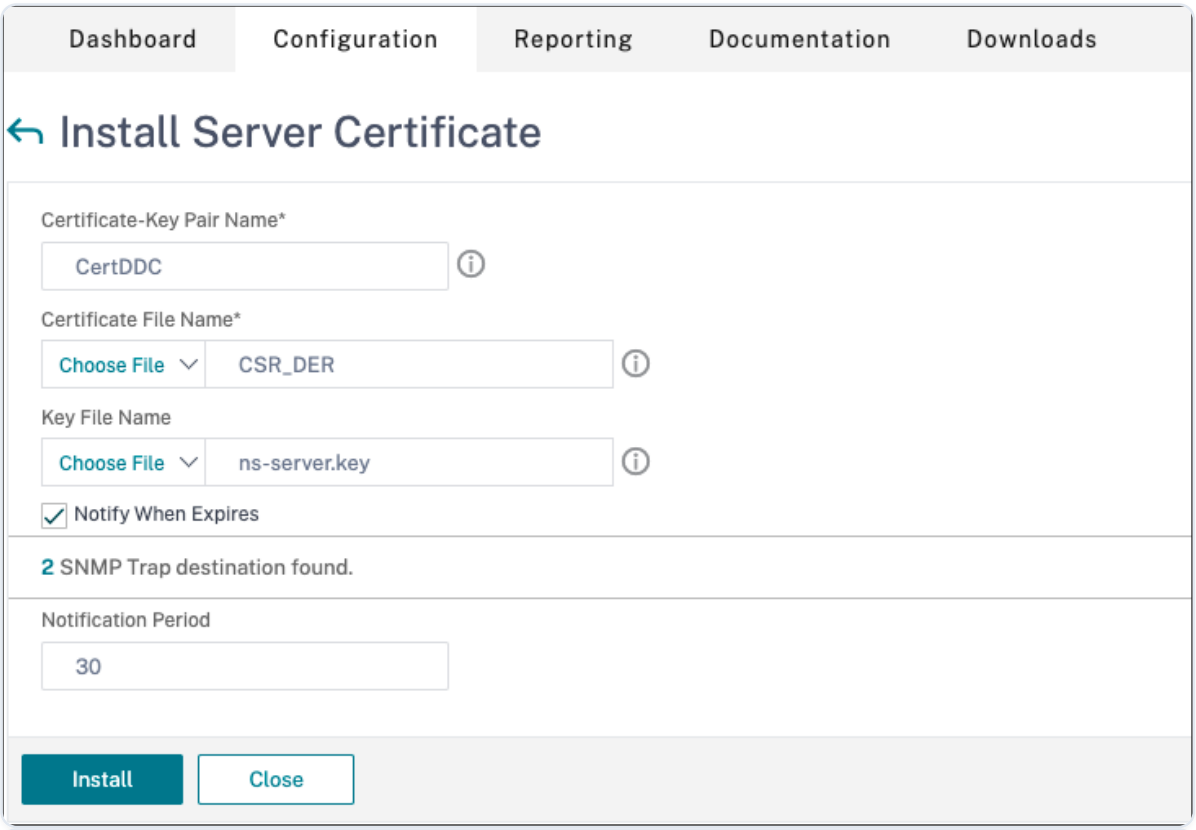
- Citrix ADCアプライアンスとバックエンドサーバー間の通信を有効にするためのサブネットIP（SNIP）アドレス。詳細については、「サブネットIPアドレスの構成」を参照してください。
- セッション起動のためにADCアプライアンスにログインするためのCitrix Gateway仮想IPアドレスとロードバランサー仮想IPアドレス。詳細については、「仮想サーバーの作成」を参照してください。

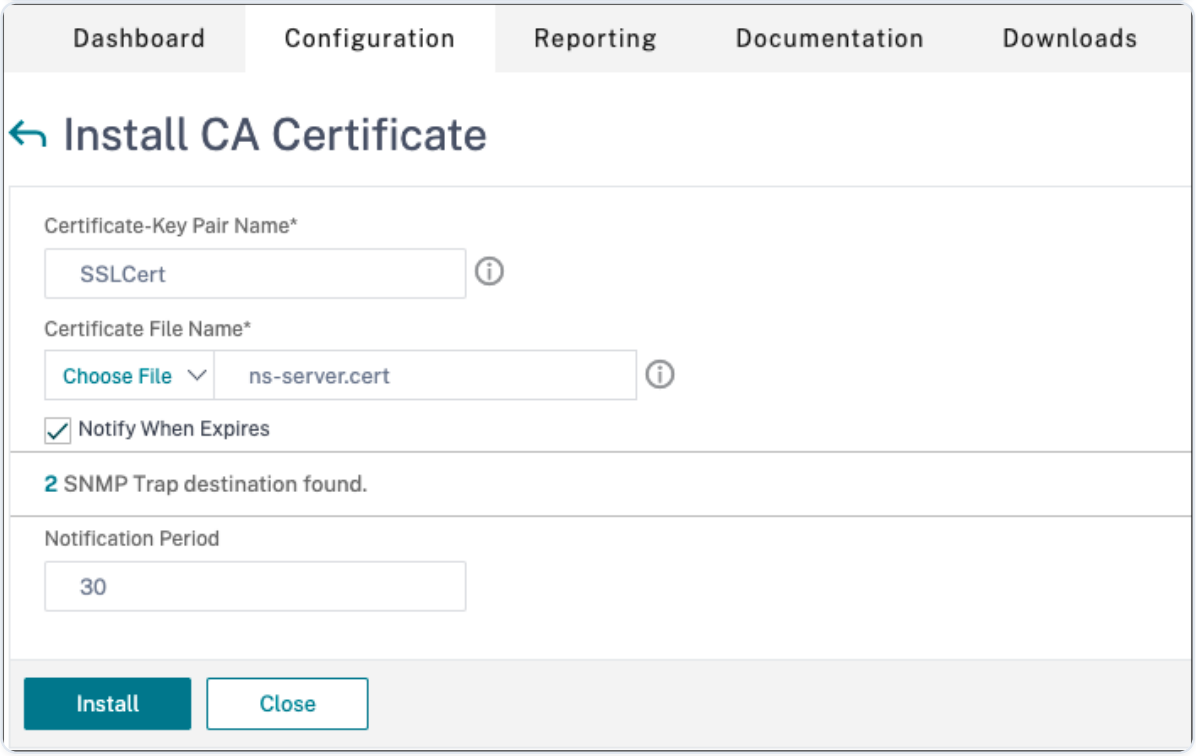


- Citrix ADCアプライアンスで必要なモードと機能が有効になっています。
  - モードを有効にするには、Citrix ADC GUIで**System > Settings > Configure Mode**に移動します。
  - 機能を有効にするには、Citrix ADC GUIで**System > Settings > Configure Basic Features**に移動します。
- 証明書関連の構成が完了しました。
  - 証明書署名要求 (CSR) が作成されます。詳細については、「証明書の作成」を参照してください。

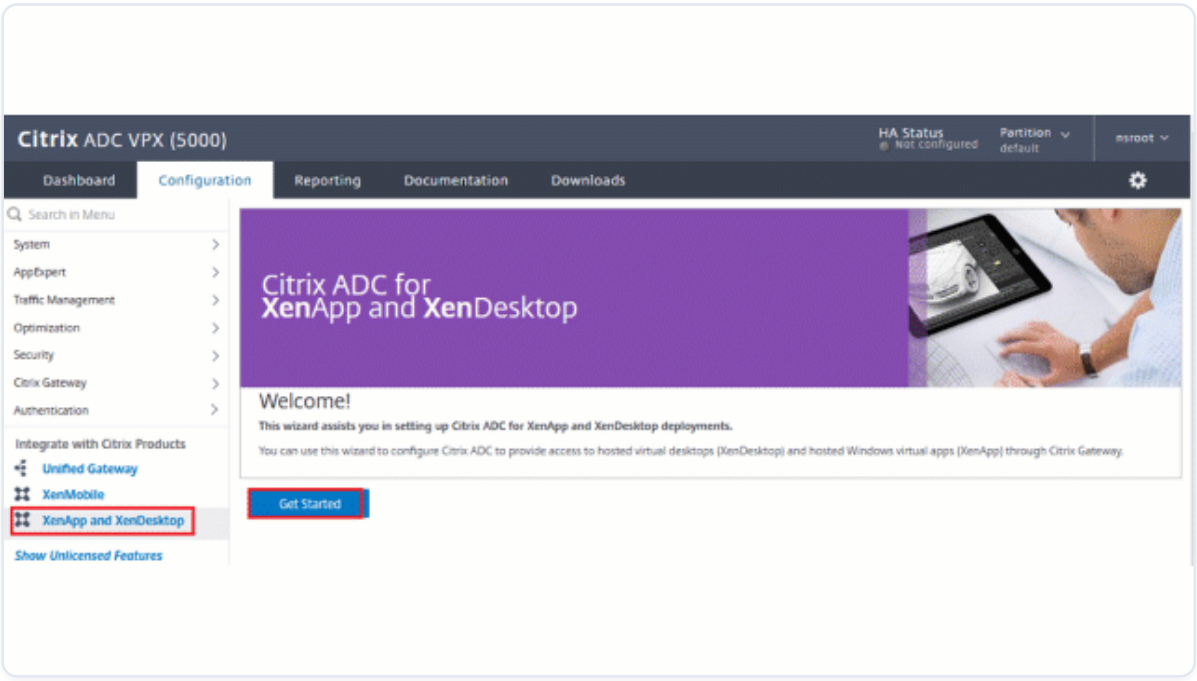


- サーバー証明書、CA証明書、およびルート証明書がインストールされます。詳細については、「インストール、リンク、および更新」を参照してください。





- Citrix Virtual Desktops 用のCitrix Gatewayが作成されました。**Test STA Connectivity** ボタンをクリックして接続をテストし、仮想サーバーがオンラインであることを確認します。詳細については、「Citrix Virtual Apps and Desktops 用のCitrix ADCのセットアップ」を参照してください。



2. リライトアクションを追加します。詳細については、「リライトアクションの構成」を参照してください。

   a. **AppExpert > Rewrite > Actions**に移動します。

   b. 新しい書き換えアクションを追加するには、**追加**をクリックします。アクションの名前は「set Type to INSERT_HTTP_HEADER」にすることができます。

   書き換えアクションの追加(/en-us/citrix-virtual-apps-desktops/2311/media/adc-appexpert-rewrite-action.png)

   a. **タイプ**で、**INSERT_HTTP_HEADER**を選択します。

   b. **ヘッダー名**に「X-Citrix-XmlServiceKey」と入力します。

   c. **式**に、引用符付きで`<XmlServiceKey1 value>`を追加します。XmlServiceKey1 の値は、Desktop Delivery Controller™ の構成からコピーできます。

   XMLサービスキーの値(/en-us/citrix-virtual-apps-desktops/2311/media/xml-service-key-values.png)

3. 書き換えポリシーを追加します。詳細については、「書き換えポリシーの構成」を参照してください。

   a. **AppExpert > Rewrite > Policies**に移動します。

   b. **Add**をクリックして、新しいポリシーを追加します。

   書き換えポリシーの追加(/en-us/citrix-virtual-apps-desktops/2311/media/adc-appexpert-rewrite-policy.png)

a. **アクション**で、前の手順で作成したアクションを選択します。

b. **式**に「HTTP.REQ.IS_VALID」を追加します。

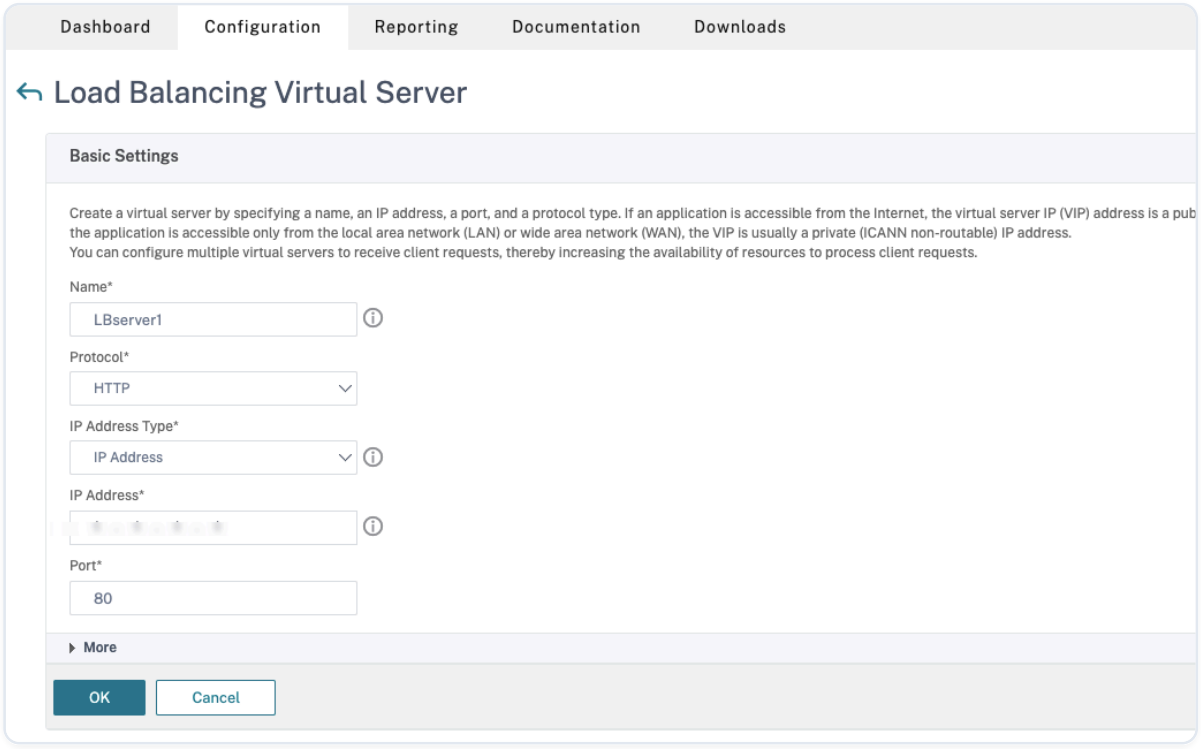
c. **OK**をクリックします。

4. 負荷分散を設定します。STAサーバーごとに1つの負荷分散仮想サーバーを構成する必要があります。構成しない場合、セッションの起動に失敗します。

   詳しくは、「基本的な負荷分散の設定」を参照してください。

   a. 負荷分散仮想サーバーを作成します。

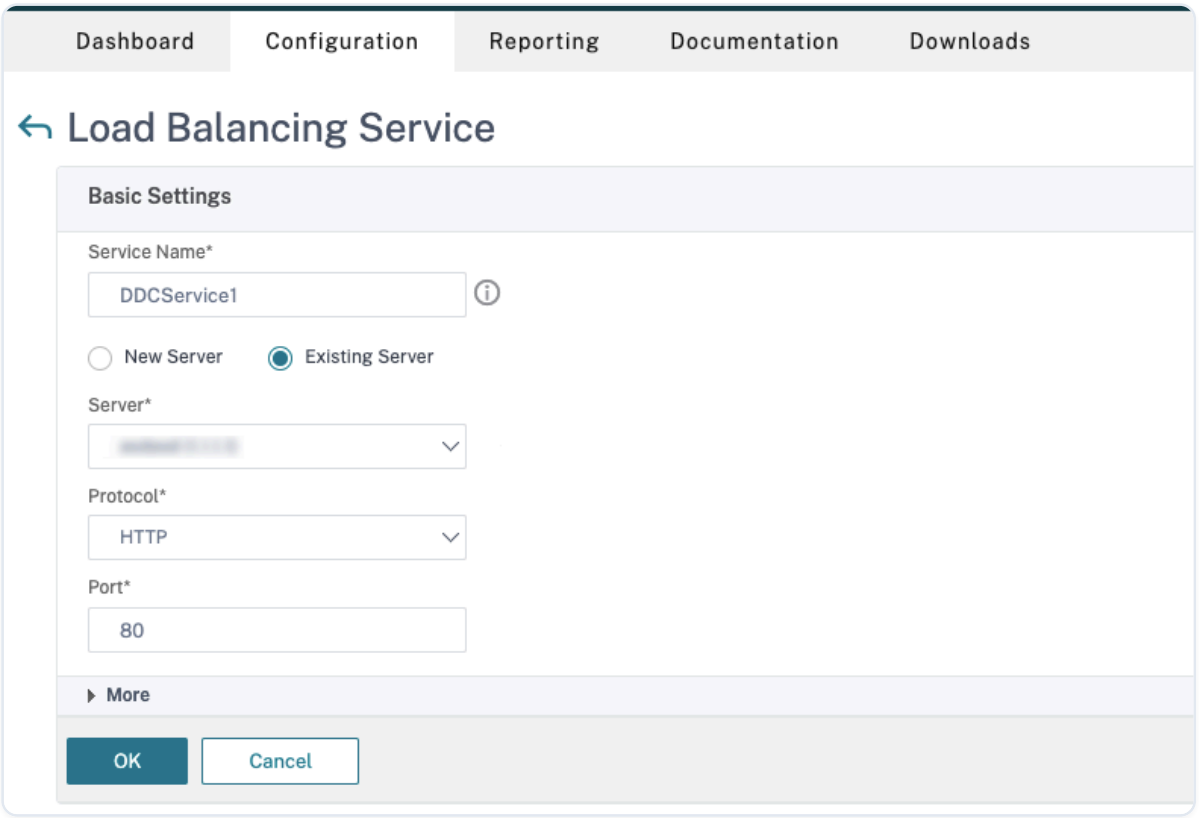
      - 「**トラフィック管理 > 負荷分散 > サーバー**」に移動します。
      - 「**Virtual Servers**」ページで、「**Add**」をクリックします。



      - 「**Protocol**」で、「**HTTP**」を選択します。
      - ロードバランシング仮想IPアドレスを追加し、「**Port**」で「**80**」を選択します。
      - 「**OK**」をクリックします。

   b. ロードバランシングサービスを作成します。

      - 「**トラフィック管理 > 負荷分散 > サービス**」に移動します。



- **Existing Server**で、前のステップで作成した仮想サーバーを選択します。
- **Protocol**で**HTTP**を選択し、**Port**で**80**を選択します。
- **OK**をクリックし、その後**Done**をクリックします。

c. サービスを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、「**Edit**」をクリックします。
- 「**サービスとサービスグループ**」で、「**ロードバランシング仮想サーバーサービスバインディングなし**」をクリックします。

仮想サーバーにサービスをバインドする(/en-us/citrix-virtual-apps-desktops/2311/media/adc-bind-service-to-lbvserver.png)

- で、以前に作成したサービスを選択します。
- をクリックします。

d. 以前に作成した書き換えポリシーを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、 をクリックします。
- で をクリックし、 セクションで をクリックします。

書き換えポリシーをバインドする(/en-us/citrix-virtual-apps-desktops/2311/media/adc-bind-rewrite-policy.png)

- で を選択し、 で を選択します。
- をクリックします。
- で、以前に作成した書き換えポリシーを選択します。
- をクリックします。
- をクリックします。

e. 必要に応じて、仮想サーバーの永続性を設定します。

- 以前に作成した仮想サーバーを選択し、 をクリックします。
- で をクリックします。

永続性の設定(/en-us/citrix-virtual-apps-desktops/2311/media/adc-lb-vserver-persistence.png)

- 永続性タイプを**Others**として選択します。
- 仮想サーバーによって選択されたサービス (宛先 IP アドレス) の IP アドレスに基づいて永続性セッションを作成するには、**DESTIP** を選択します。
- **IPv4 Netmask** で、DDC と同じネットワークマスクを追加します。
- **OK** をクリックします。

f. 他の仮想サーバーについても、これらの手順を繰り返します。

Citrix ADCアプライアンスがCitrix Virtual Desktops™で既に構成されている場合の構成の変更点

Citrix ADCアプライアンスをCitrix Virtual Desktopsで既に構成している場合、Secure XML機能を使用するには、以下の構成変更を行う必要があります。

- セッション起動前に、ゲートウェイの**Security Ticket Authority URL**を、負荷分散仮想サーバーのFQDNを使用するように変更します。
- `TrustRequestsSentToTheXmlServicePort` パラメーターが False に設定されていることを確認します。デフォルトでは、`TrustRequestsSentToTheXmlServicePort` パラメーターは False に設定されています。ただし、顧客がCitrix Virtual Desktops用にCitrix ADCを既に構成している場合、`TrustRequestsSentToTheXmlServicePort` は True に設定されます。

1. Citrix ADC GUIで、**Configuration > Integrate with Citrix Products** に移動し、**XenApp and XenDesktop®** をクリックします。
2. ゲートウェイインスタンスを選択し、編集アイコンをクリックします。

既存のゲートウェイ構成を編集(/en-us/citrix-virtual-apps-desktops/2311/media/edit-gateway-instance.png)

3. StoreFrontペインで、編集アイコンをクリックします。

   StoreFrontの詳細を編集(/en-us/citrix-virtual-apps-desktops/2311/media/edit-storefront-details.png)

4. **セキュアチケットオーソリティURL**を追加します。

   - Secure XML機能が有効になっている場合、STA URLはロードバランシングサービスのURLである必要があります。
   - Secure XML機能が無効になっている場合、STA URLはSTAのURL（DDCのアドレス）である必要があり、DDC上のTrustRequestsSentToTheXmlServicePortパラメーターをTrueに設定する必要があります。

   STA URLを追加(/en-us/citrix-virtual-apps-desktops/2311/media/add-sta-urls.png)

セッション

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。信頼性の低いネットワーク、変動の大きいネットワーク遅延、ワイヤレスデバイスの範囲制限による接続の喪失は、ユーザーの不満につながる可能性があります。デバイス間を素早く移動し、ログオンするたびに同じアプリケーションにアクセスすることは、医療従事者などの多くのモバイルワーカーにとって優先事項です。

この記事で説明する機能は、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減します。これらの機能を使用することで、モバイルユーザーはデバイス間を迅速かつ簡単にローミングできます。

セッションからユーザーをログオフさせたり、セッションを切断したり、セッションの事前起動と残存を構成したりすることもできます。詳細については、「デリバリーグループの管理」を参照してください。

セッションの信頼性

セッションの信頼性は、ネットワーク接続が中断されたときにセッションをアクティブに保ち、ユーザーの画面に表示し続けます。ユーザーは、ネットワーク接続が再開されるまで、使用しているアプリケーションを引き続き見ることができます。

この機能は、ワイヤレス接続を使用するモバイルユーザーにとって特に便利です。たとえば、ワイヤレス接続を使用しているユーザーが鉄道トンネルに入り、一時的に接続が失われたとします。通

常、セッションは切断されてユーザーの画面から消え、ユーザーは切断されたセッションに再接続する必要があります。セッションの信頼性を使用すると、セッションはマシン上でアクティブなままになります。接続が失われたことを示すために、ユーザーのディスプレイはフリーズし、カーソルは回転する砂時計に変わり、トンネルの反対側で接続が再開されるまで続きます。ユーザーは中断中もディスプレイにアクセスし続け、ネットワーク接続が復元されるとアプリケーションとの対話を再開できます。セッションの信頼性は、再認証のプロンプトなしでユーザーを再接続します。

Citrix Workspace™アプリのユーザーは、Controllerの設定を上書きできません。

セッションの信頼性は、Transport Layer Security (TLS) とともに使用できます。TLSは、ユーザーデバイスとCitrix Gatewayの間で送信されるデータのみを暗号化します。

次のポリシー設定を使用して、セッションの信頼性を有効にして構成します。

- 「セッションの信頼性接続」ポリシー設定は、セッションの信頼性を許可または禁止します。
- 「セッションの信頼性タイムアウト」ポリシー設定のデフォルトは180秒、つまり3分です。セッションの信頼性がセッションを開いたままにする時間を延長することはできますが、この機能はユーザーの利便性のために設計されています。そのため、ユーザーに再認証を促すことはありません。セッションを開いたままにする時間を延長すると、ユーザーが注意散漫になり、ユーザーデバイスから離れてしまう可能性が高まります。これらの行動は、セッションを不正なユーザーがアクセスできる状態にする可能性があります。
- 受信セッションの信頼性接続は、ポート番号を「セッションの信頼性ポート番号」ポリシー設定で変更しない限り、ポート2598を使用します。
- ユーザーが再認証なしで中断されたセッションに再接続するのを防ぐには、自動クライアント再接続機能を使用します。中断されたセッションに再接続する際にユーザーに再認証を促すように、「自動クライアント再接続認証」ポリシー設定を構成できます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順次動作します。セッションの信頼性は、「セッションの信頼性タイムアウト」ポリシー設定で指定した時間の経過後、ユーザーセッションを閉じるか、切断します。その後、自動クライアント再接続ポリシー設定が有効になり、切断されたセッションにユーザーを再接続しようとします。

クライアントの自動再接続

自動クライアント再接続機能を使用すると、Citrix WorkspaceアプリはICA®セッションの意図しない切断を検出し、影響を受けるセッションにユーザーを自動的に再接続できます。この機能がサーバーで有効になっている場合、ユーザーは作業を続行するために手動で再接続する必要はありません。

アプリケーションセッションの場合、Citrix Workspaceアプリは、正常に再接続されるか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試行します。

デスクトップセッションの場合、Citrix Workspaceアプリは、正常に再接続されるか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間、セッションへの再接続を試行します。デフォルトでは、この期間は5分です。この期間を変更するには、ユーザーデバイスで次のレジストリ設定を編集します（`seconds` は、セッションの再接続がそれ以上試行されなくなるまでの秒数です）。

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

次のポリシー設定で自動クライアント再接続を有効にして構成します。

- **自動クライアント再接続:** 接続が中断された後、Citrix Workspaceアプリによる自動再接続を有効または無効にします。
- **自動クライアント再接続認証:** 自動再接続後のユーザー認証の要件を有効または無効にします。
- **自動クライアント再接続ログ記録:** イベントログでの再接続イベントのログ記録を有効または無効にします。ログ記録はデフォルトで無効になっています。有効にすると、サーバーのシステムログは、成功および失敗した自動再接続イベントに関する情報をキャプチャします。各サーバーは、再接続イベントに関する情報を独自のシステムログに保存します。サイトは、すべてのサーバーの再接続イベントの結合されたログを提供しません。

注:

再認証なしの自動クライアント再接続は、パスワード認証のみでサポートされます。フェデレーション認証サービスまたはスマートカード認証を使用する場合、再認証なしの自動クライアント再接続はサポートされません。そのような場合、ユーザーはログイン画面にリダイレクトされます。

Auto Client Reconnectは、暗号化されたユーザー資格情報に基づく認証メカニズムを組み込んでいます。ユーザーが最初にログオンすると、サーバーはユーザー資格情報を暗号化してメモリに保存します。サーバーはまた、暗号化キーを含むCookieを作成し、Citrix Workspaceアプリに送信します。Citrix Workspaceアプリは、再接続のためにキーをサーバーに送信します。サーバーは資格情報を復号化し、認証のためにWindowsログオンに送信

> します。Cookieの有効期限が切れると、ユーザーはセッションに再接続するために再認証する必要があります。

自動クライアント再接続認証設定を有効にすると、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続を試行すると、資格情報を要求するダイアログボックスがユーザーに表示されます。

ユーザー資格情報とセッションを最大限に保護するために、クライアントとサイト間のすべての通信に暗号化を使用してください。

icaclient.admファイルを使用して、Windows版Citrix WorkspaceアプリでAuto Client Reconnectを無効にします。詳細については、お使いのWindows版Citrix Workspaceアプリのバージョンのドキュメントを参照してください。

接続の設定も、自動クライアント再接続に影響します。

- 既定では、前述のとおり、自動クライアント再接続はサイトレベルのポリシー設定によって有効になっています。ユーザーの再認証は不要です。ただし、サーバーのICA TCP接続が、切断された通信リンクでセッションをリセットするように構成されている場合、自動再接続は行われません。自動クライアント再接続は、切断された接続またはタイムアウトした接続がある場合にサーバーがセッションを切断する場合にのみ機能します。このコンテキストでは、ICA TCP接続とは、TCP/IPネットワーク上のセッションに使用されるサーバーの仮想ポート（実際のネットワーク接続ではなく）を指します。
- 既定では、サーバー上のICA TCP接続は、切断された接続またはタイムアウトした接続を持つセッションを切断するように設定されています。切断されたセッションはシステムメモリにそのまま残り、Citrix Workspaceアプリによる再接続が可能です。
- 接続は、切断された接続またはタイムアウトした接続を持つセッションをリセットまたはログオフするように構成できます。セッションがリセットされると、再接続を試みると新しいセッションが開始されます。使用中のアプリケーションでユーザーを同じ場所に戻すのではなく、アプリケーションが再起動されます。
- サーバーがセッションをリセットするように構成されている場合、自動クライアント再接続は新しいセッションを作成します。このプロセスでは、ユーザーがサーバーにログオンするために資格情報を入力する必要があります。
- Citrix Workspaceアプリまたはプラグインが誤った認証情報を送信した場合（攻撃中に発生する可能性や、サーバーが切断された接続を検出してから時間が経ちすぎたと判断した場合など）、自動再接続は失敗する可能性があります。

ICA キープアライブ

ICA Keep-Alive機能を有効にすると、切断された接続が切断されるのを防ぎます。有効にすると、サーバーがアクティビティを検出しない場合、この機能はリモートデスクトップサービスがそのセッションを切断するのを防ぎます。アクティビティがない例としては、クロックの変更がない、マウスの動きがない、画面の更新がないなどが挙げられます。サーバーは数秒ごとにキープアライブパケットを送信して、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはそのセッションを切断済みとしてマークします。

> **重要:**
>
> ICA Keep-Aliveは、セッションの信頼性を使用していない場合にのみ機能します。セッションの信頼性には、切断された接続が切断されるのを防ぐ独自のメカニズムがあります。ICA Keep-Aliveは、セッションの信頼性を使用しない接続に対してのみ構成してください。

> ICA Keep-Alive設定は、Windowsグループポリシーで構成されているキープアライブ設定を上書きします。

次のポリシー設定を使用して、ICA Keep-Aliveを有効にして構成します。

- **ICAキープアライブタイムアウト:** ICAキープアライブメッセージの送信に使用される間隔（1～3600秒）を指定します。切断された接続が非常にまれで、ユーザーがセッションに再接続できることが問題にならない環境で、ネットワーク監視ソフトウェアが非アクティブな接続を閉じるようにしたい場合は、このオプションを構成しないでください。

  既定の間隔は60秒です。ICA Keep-Aliveパケットは60秒ごとにユーザーデバイスに送信されます。ユーザーデバイスが60秒以内に応答しない場合、ICAセッションのステータスは切断済みに変わります。

- **ICAキープアライブ:** ICAキープアライブメッセージの送信を許可または禁止します。

ワークスペースコントロール

ワークスペースコントロールにより、デスクトップとアプリケーションはユーザーを追ってデバイス間を移動できます。このローミング機能により、ユーザーはログオンするだけで、すべてのデスクトップまたは開いているアプリケーションにどこからでもアクセスでき、各デバイスでデスクトップやアプリケーションを再起動する必要がありません。たとえば、ワークスペースコントロールは、病院で異なるワークステーション間を迅速に移動し、ログオンするたびに同じアプリケーションセットにアクセスする必要がある医療従事者を支援できます。ワークスペースコントロールオプションを許可するように構成すると、これらの医療従事者は、1つのクライアントデバイスで

複数のアプリケーションから切断し、別のクライアントデバイスで同じアプリケーションに再接続できます。

ワークスペースコントロールは、次のアクティビティに影響します。

- **ログオン:** デフォルトでは、ワークスペースコントロールにより、ユーザーはログオン時に実行中のすべてのデスクトップとアプリケーションに自動的に再接続でき、手動で再開する必要がありません。ワークスペースコントロールを通じて、ユーザーは切断されたデスクトップまたはアプリケーション、および別のクライアントデバイスでアクティブなものを開くことができます。デスクトップまたはアプリケーションから切断しても、それはサーバー上で実行されたままになります。一部のデスクトップまたはアプリケーションを1つのクライアントデバイスで実行したまま、別のクライアントデバイスでデスクトップまたはアプリケーションのサブセットに再接続する必要があるローミングユーザーがいる場合、ログオン再接続動作を、以前にユーザーが切断したデスクトップまたはアプリケーションのみを開くように構成できます。
- **再接続:** サーバーにログオンした後、ユーザーはいつでも をクリックして、すべてのデスクトップまたはアプリケーションに再接続できます。デフォルトでは、 は切断されたデスクトップまたはアプリケーション、および現在別のクライアントデバイスで実行されているものを開きます。 を、以前にユーザーが切断したデスクトップまたはアプリケーションのみを開くように構成できます。
- **ログオフ:** StoreFront™ を介してデスクトップまたはアプリケーションを開くユーザーの場合、**ログオフ** コマンドを構成して、ユーザーをStoreFrontとすべてのアクティブなセッションからログオフさせるか、StoreFrontのみからログオフさせることができます。
- **切断:** ユーザーは、実行中のすべてのデスクトップとアプリケーションから一度に切断でき、個別に切断する必要はありません。

ワークスペースコントロールは、Citrix StoreFront接続を介してデスクトップおよびアプリケーションにアクセスするCitrix Workspaceアプリユーザーのみが利用できます。デフォルトでは、仮想デスクトップセッションではワークスペースコントロールは無効になっていますが、ホスト型アプリケーションでは有効になっています。公開されたデスクトップと、それらのデスクトップ内で実行されている公開されたアプリケーションの間では、デフォルトではセッション共有は行われません。

ユーザーが新しいクライアントデバイスに移動すると、ユーザーポリシー、クライアントドライブマッピング、およびプリンター構成が適切に変更されます。ポリシーとマッピングは、ユーザーがセッションにログオンしているクライアントデバイスに従って適用されます。たとえば、医療従事者が救急治療室のデバイスからログオフし、X線検査室のワークステーションにログオンします。X線検査室でのセッションに適したポリシー、プリンターマッピング、およびクライアントドライブマッピングは、セッション開始時に有効になります。

ユーザーが場所を変更したときに表示されるプリンターをカスタマイズできます。また、ユーザーがローカルプリンターに印刷できるかどうか、ユーザーがリモートで接続したときに消費される帯域幅の量、および印刷エクスペリエンスのその他の側面を制御することもできます。

ユーザー向けのワークスペースコントロールの有効化と構成については、StoreFrontのドキュメントを参照してください。

セッションローミング

> **注:**
>
> 以下の情報は、PowerShellを使用してセッションローミングを構成するためのガイドです。代わりにWeb Studioを使用することもできます。詳細については、「デリバリーグループの管理」を参照してください。

> デフォルトでは、セッションはユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、アプリケーションは両方のデバイスで利用可能になります。アプリケーションは、デバイスや現在のセッションの有無にかかわらず追従します。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追従します。

このデフォルトの動作には多くの利点がありますが、すべての場合に理想的とは限りません。PowerShell SDKを使用してセッションローミングを防止できます。

例1：医療従事者が2つのデバイスを使用しています。デスクトップPCで保険フォームを完成させ、タブレットで患者情報を確認しています。

- セッションローミングが有効になっている場合、両方のアプリケーションが両方のデバイスに表示されます（1つのデバイスで起動されたアプリケーションは、使用中のすべてのデバイスで表示されます）。これはセキュリティ要件を満たさない可能性があります。
- セッションローミングが無効になっている場合、患者記録はデスクトップPCに表示されず、保険フォームもタブレットに表示されません。

例2：生産マネージャーがオフィスにあるPCでアプリケーションを起動します。デバイス名と場所によって、そのセッションで利用可能なプリンターやその他のリソースが決まります。その日の後半、彼はプリンターの使用が必要な会議のため、隣の建物のオフィスに行きます。

- セッションローミングが有効になっている場合、生産マネージャーは会議室近くのプリンターにアクセスできない可能性があります。なぜなら、彼がオフィスで以前に起動したアプリケーションによって、その場所に近いプリンターやその他のリソースが割り当てられたためです。
- セッションローミングが無効になっている場合、彼が別のマシンに（同じ資格情報を使用して）ログオンすると、新しいセッションが開始され、近くのプリンターやリソースが利用可能になります。

セッションローミングの構成

セッションローミングを構成するには、「SessionReconnection」プロパティを持つ以下のエンタイトルメントポリシー規則コマンドレットを使用します。オプションで、「LeasingBehavior」プロパティも指定できます。

デスクトップセッションの場合：

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

アプリケーションセッションの場合：

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

`value` には、次のいずれかを指定できます。

- **Always:** クライアントデバイスやセッションが接続されているか切断されているかに関わらず、セッションは常にローミングします。これがデフォルト値です。
- **切断済みのみ:** 既に切断されているセッションにのみ再接続します。そうでない場合は、新しいセッションを起動します。(セッションは、まず切断するか、Workspace Control を使用して明示的にローミングすることで、クライアントデバイス間をローミングできます。) 別のクライアントデバイスからのアクティブな接続済みセッションは使用されません。代わりに、新しいセッションが起動されます。
- **同じエンドポイントのみ:** ユーザーは、使用するクライアントデバイスごとに一意のセッションを取得します。これにより、ローミングが完全に無効になります。ユーザーは、以前セッションで使用したのと同じデバイスにのみ再接続できます。

「LeasingBehavior」プロパティについては、以下で説明します。

その他の設定による影響：

セッションローミングを無効にすると、デリバリーグループのアプリケーションのプロパティにあるアプリケーション制限「**ユーザーごとにアプリケーションのインスタンスを1つのみ許可**」の影響を受けます。

- セッションローミングを無効にする場合は、「インスタンスを1つのみ許可...」アプリケーション制限を無効にしてください。
- 「インスタンスを1つのみ許可...」アプリケーション制限を有効にする場合は、新しいデバイスで新しいセッションを許可する2つの値のいずれも構成しないでください。

ログオン間隔

デスクトップVDAを含む仮想マシンがログオンプロセス完了前に閉じられた場合、そのプロセスにより多くの時間を割り当てることができます。バージョン7.6以降のデフォルトは180秒です（バージョン7.0〜7.5のデフォルトは90秒です）。

マシン（またはマシンカタログで使用されるマスターイメージ）で、次のレジストリキーを設定します。

キー: `HKLM\SOFTWARE\Citrix\PortICA`

- 値: `AutoLogonTimeout`
- 種類: `DWORD`
- 0〜3600の範囲で、10進数で時間を秒単位で指定します。

マスターイメージを変更した場合は、カタログを更新します。

この設定は、デスクトップVDAを持つVMにのみ適用されます。Microsoftは、サーバーVDAを持つマシンでのログオンタイムアウトを制御します。

タグ

> **注:**

> Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

タグは、マシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ、ポリシーなどの項目を識別する文字列です。タグを作成して項目に追加すると、特定の操作を、指定されたタグを持つ項目にのみ適用するように調整できます。

- Web Studioでの検索表示を調整します。

  たとえば、テスター向けに最適化されたアプリケーションのみを表示するには、「test」という名前のタグを作成し、それらのアプリケーションに追加（適用）します。これで、Web Studioの検索を「test」タグでフィルタリングできます。

- 選択したデリバリーグループ内のマシンの一部のみを考慮して、アプリケーショングループからアプリケーションを公開したり、デリバリーグループから特定のデスクトップを公開したりできます。これは*タグ制限*と呼ばれます。

  タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、より多くのマシンを展開および管理するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。その機能は、XenApp 7.x以前のリリースにおけるワーカーグループと似ていますが、同一ではありません。

  タグ制限付きのアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンの一部を分離してトラブルシューティングする際に役立ちます。

- デリバリーグループ内のマシンの一部に対して定期的な再起動をスケジュールします。

  マシンにタグ制限を使用すると、新しいPowerShellコマンドレットを使用して、デリバリーグループ内のマシンの一部に対して複数の再起動スケジュールを構成できます。例と詳細については、「デリバリーグループの管理」を参照してください。

- Citrixポリシーの適用（割り当て）を、指定されたタグを持つ（または持たない）デリバリーグループ、デリバリーグループの種類、またはOU内のマシンの一部に調整する。

  たとえば、より強力なワークステーションにのみCitrixポリシーを適用したい場合は、それらのマシンに「high power」という名前のタグを追加します。次に、ポリシー作成ウィザードの**ポリシーの割り当て**ページで、そのタグと**有効にする**チェックボックスを選択します。デリバリーグループにタグを追加し、そのグループにCitrixポリシーを適用することもできます。詳細については、「ポリシーの作成」を参照してください。

タグは以下に適用できます。

- マシン
- アプリケーション

- マシンカタログ（PowerShellのみ。詳細については、「マシンカタログのタグ」を参照してください）
- デリバリーグループ
- アプリケーショングループ

Web Studioで以下を作成または編集する際に、タグ制限を構成できます。

- 共有デリバリーグループ内のデスクトップ
- アプリケーショングループ

> **重要:**
>
> タグは、明示的にマシンに適用することも、マシンカタログまたはデリバリーグループレベルで明示的に適用することもできます。タグがマシンカタログまたはデリバリーグループレベルで適用されると、そのカタログまたはデリバリーグループ内のすべてのマシンが暗黙的にそのタグを継承します。これらの継承されたタグは、マシンレベルで削除することはできません。タグの効果を削除するには、マシンカタログまたはデリバリーグループレベルからタグを削除する必要があります。

デスクトップまたはアプリケーショングループのタグ制限

タグ制限にはいくつかの手順があります。

- タグを作成し、マシンに追加（適用）します。
- タグ制限付きのグループを作成または編集します（つまり、「タグxを持つマシンへの起動を制限する」）。

タグ制限は、ブローカーのマシン選択プロセスを拡張します。ブローカーは、関連付けられたデリバリーグループから、アクセスポリシー、構成されたユーザーリスト、ゾーン設定、起動準備、およびタグ制限（存在する場合）に従ってマシンを選択します。アプリケーションの場合、ブローカーは優先順位に従って他のデリバリーグループにフォールバックし、検討される各デリバリーグループに同じマシン選択ルールを適用します。

例1：シンプルなレイアウト

この例では、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限するシンプルなレイアウトを紹介します。このサイトには、1つの共有デリバ

リーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。

シンプルなレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/2311/media/tags-example.png)

- 3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。
- 共有デリバリーグループ内のデスクトップは、「Red」というタグ制限で作成されました。デスクトップは、そのデリバリーグループ内で「Red」タグを持つマシン（VDA 101および102）でのみ起動できます。
- アプリケーショングループは「Orange」タグ制限で作成されたため、その各アプリケーション（CalculatorとNotepad）は、そのデリバリーグループ内で「Orange」タグを持つマシン（VDA 102および103）でのみ起動できます。

マシンVDA 102は両方のタグ（RedとOrange）を持っているため、アプリケーションとデスクトップの起動に考慮されます。

例2：より複雑なレイアウト

この例には、タグ制限付きで作成された複数のアプリケーショングループが含まれています。これにより、デリバリーグループのみを使用した場合に必要となるよりも少ないマシンで、より多くのアプリケーションを配信できるようになります。

例2の構成方法は、この例でタグを作成および適用し、タグ制限を構成する手順を示しています。

複雑なレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/2311/media/tags-example2.png)

この例では、10台のマシン（VDA 101～110）、1つのデリバリーグループ（D01）、および3つのアプリケーショングループ（A100、A200、A300）を使用します。各マシンにタグを適用し、各アプリケーショングループの作成時にタグ制限を指定することで、次のようになります。

- グループ内の経理ユーザーは、5台のマシン（VDA 101～105）で必要なアプリにアクセスできます
- グループ内のCAD設計者は、5台のマシン（VDA 106-110）で必要なアプリにアクセスできます
- グループ内でOfficeアプリケーションを必要とするユーザーは、10台のマシン（VDA 101～110）でOfficeアプリにアクセスできます

10台のマシンのみが使用され、デリバリーグループは1つだけです。デリバリーグループのみを使用する場合（アプリケーショングループなし）、マシンは1つのデリバリーグループにしか属せないため、2倍のマシンが必要になります。

タグとタグ制限の管理

タグは、Web Studioの**タグの管理**アクションを通じて、選択したアイテムから作成、追加（適用）、編集、および削除されます。

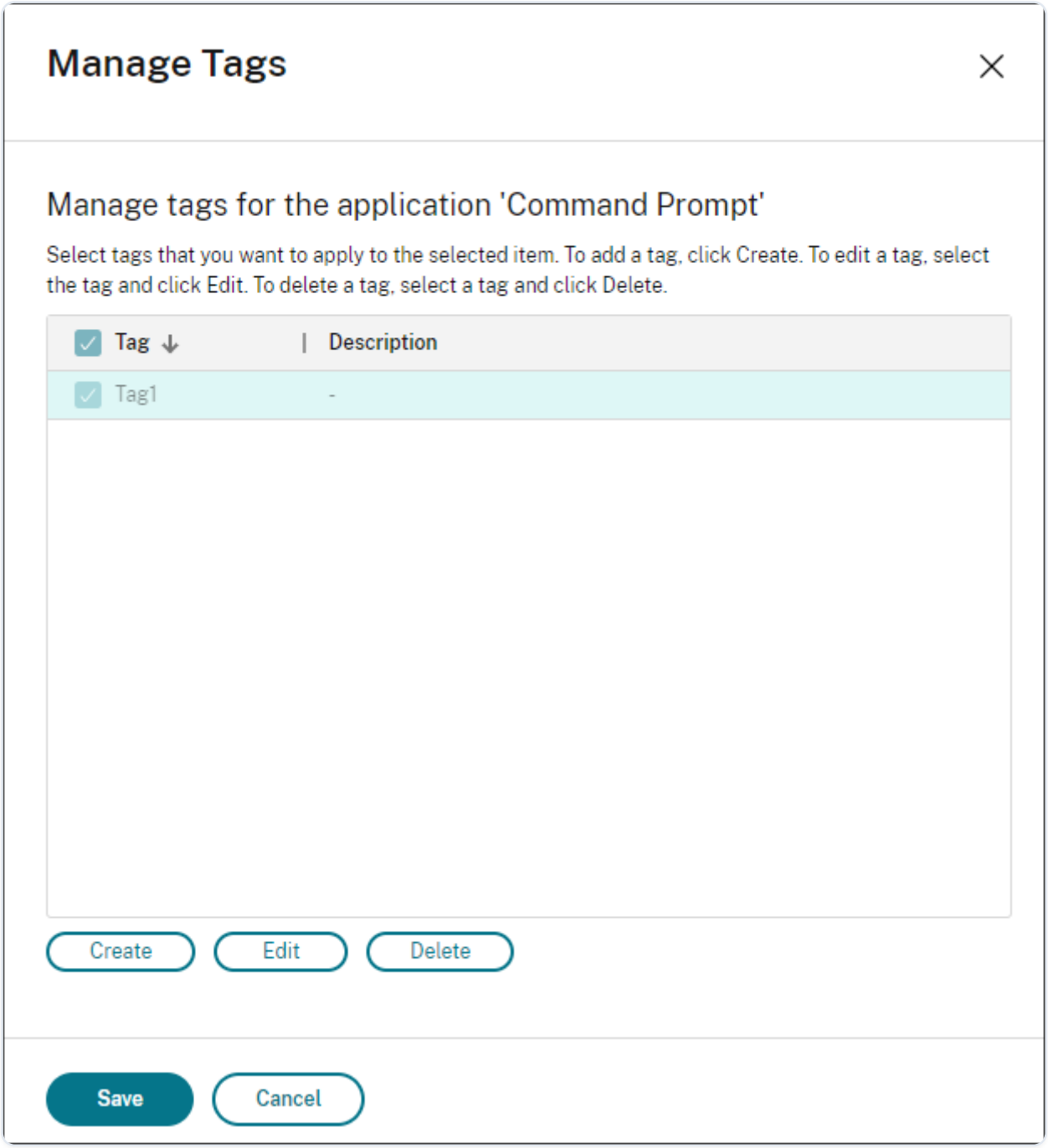
（例外：ポリシー割り当てに使用されるタグは、Web Studioの**［タグの管理］**アクションを通じて作成、編集、削除されます。ただし、タグはポリシーの作成時に適用（割り当て）されます。詳細については、「ポリシーの作成」を参照してください。）

タグ制限は、デリバリーグループでデスクトップを作成または編集するとき、およびアプリケーショングループを作成および編集するときに構成されます。

Web Studioで［タグの管理］ダイアログを使用する

Web Studioで、タグを適用するアイテム（1つ以上のマシン、アプリケーション、デスクトップ、デリバリーグループ、またはアプリケーショングループ）を選択し、アクションバーで**タグの管理**を選択します。ダイアログボックスには、選択したアイテムだけでなく、サイトで作成されたすべてのタグが一覧表示されます。

- チェックマークが付いたチェックボックスは、そのタグが選択したアイテムに既に追加されていることを示します。（以下のスクリーンショットでは、選択したマシンに「Tag1」という名前のタグが適用されています。）
- 複数のアイテムを選択した場合、ハイフンを含むチェックボックスは、選択したアイテムの一部にのみそのタグが追加されていることを示します。



タグの管理ダイアログボックスから、次のアクションを実行できます。タグを使用する際の注意点を必ず確認してください。

- **タグを作成するには:**

  作成をクリックします。名前と説明を入力します。タグ名は一意である必要があり、大文字と小文字は区別されません。次に、**OK**をクリックします。（タグを作成しても、選択したアイテムに自動的に適用されるわけではありません。チェックボックスを使用してタグを適用します。）

- **1つ以上のタグを追加（適用）するには:**

タグ名の横にあるチェックボックスを有効にします。複数のアイテムを選択し、タグの横にあるチェックボックスにハイフンが含まれている場合（選択したアイテムの一部にのみタグが既に適用されていることを示す）、それをチェックマークに変更すると、選択したすべてのマシンに影響します。

1つ以上のマシンにタグを追加しようとしたときに、そのタグがアプリケーショングループで制限として使用されている場合、その操作によってそれらのマシンが起動可能になる可能性があるという警告が表示されます。それが意図した操作であれば、続行してください。

- **1つ以上のタグを削除するには:**

  タグ名の横にあるチェックボックスをオフにします。複数の項目を選択していて、タグの横にあるチェックボックスにハイフンが含まれている場合（選択した項目の一部にのみタグが適用されていることを示す）、チェックボックスをオフにすると、選択したすべてのマシンからタグが削除されます。

  タグを制限として使用しているマシンからタグを削除しようとすると、その操作によって起動対象となるマシンに影響が出る可能性があるという警告が表示されます。それが意図した操作であれば、続行してください。

- **タグを編集するには:**

  タグを選択し、**編集**をクリックします。新しい名前、説明、またはその両方を入力します。一度に編集できるタグは1つだけです。

- **1つ以上のタグを削除するには:**

  タグを選択し、**削除**をクリックします。「タグの削除」ダイアログボックスには、現在選択されているタグを使用している項目の数が表示されます（例：「2台のマシン」）。項目をクリックすると、詳細情報が表示されます。たとえば、「2台のマシン」項目をクリックすると、そのタグが適用されている2台のマシンの名前が表示されます。タグを削除するかどうかを確認します。

  Web Studioを使用して、制限として使用されているタグを削除することはできません。まず、アプリケーショングループを編集し、タグの制限を削除するか、別のタグを選択してください。

タグの管理ダイアログボックスでの作業が完了したら、**保存**をクリックします。

マシンにタグが適用されているかどうかを確認するには、左ペインで**デリバリーグループ**を選択します。中央ペインでデリバリーグループを選択し、アクションバーで**マシンの表示**を選択します。中央ペインでマシンを選択し、**詳細**ペインで**タグ**タブを選択します。

タグ制限の管理

タグ制限の構成は、複数のステップからなるプロセスです。まずタグを作成し、それをマシンに追加/適用します。次に、アプリケーショングループまたはデスクトップに制限を追加します。

- **タグの作成と適用：**

  タグを作成し、前述の**タグの管理**アクションを使用して、タグ制限の影響を受けるマシンにタグを追加（適用）します。

- **アプリケーショングループにタグ制限を追加するには：**

  アプリケーショングループを作成または編集します。**デリバリーグループ**ページで、**タグを持つマシンへの起動を制限**を選択し、リストからタグを選択します。

- **アプリケーショングループのタグ制限を変更または削除するには：**

  グループを編集します。**デリバリーグループ**ページで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限**のチェックを外してタグ制限を完全に削除します。

- **デスクトップにタグ制限を追加するには：**

  デリバリーグループを作成または編集します。**デスクトップ**ページで、**追加**または**編集**をクリックします。「デスクトップの追加」ダイアログボックスで、**タグを持つマシンへの起動を制限**を選択し、メニューからタグを選択します。

- **デリバリーグループのタグ制限を変更または削除するには：**

  グループを編集します。デスクトップページで、**編集**をクリックします。ダイアログボックスで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限**のチェックを外してタグ制限を完全に削除します。

タグを使用する際の注意点

アイテムに適用されたタグはさまざまな目的で使用できるため、タグの追加、削除、および消去が意図しない影響を与える可能性があることに留意してください。タグを使用して、Web Studioの検索フィールドでマシン表示を並べ替えることができます。同じタグを、アプリケーショングループまたはデスクトップを構成する際の制限として使用できます。このタグは、指定されたデリバリーグループ内でそのタグを持つマシンのみに起動の考慮事項を制限します。

デスクトップまたはアプリケーショングループのタグ制限として構成されたタグをマシンに追加しようとすると、警告が表示されます。そのタグを追加すると、マシンが追加のアプリケーションまたはデスクトップの起動に利用可能になる可能性があります。それが意図したものであれば、続行してください。そうでない場合は、操作をキャンセルできます。

たとえば、「Red」タグ制限を持つアプリケーショングループを作成したとします。その後、そのアプリケーショングループで使用されている同じデリバリーグループに他のマシンをいくつか追加します。そのマシンに「Red」タグを追加しようとすると、Web Studioは次のようなメッセージを表示します。「タグ「Red」は以下のアプリケーショングループの制限として使用されています。このタグを追加すると、選択したマシンがこのアプリケーショングループ内のアプリケーションを起動できるようになる可能性があります。」その後、その追加のマシンにタグを追加することを確認またはキャンセルできます。

同様に、アプリケーショングループが起動を制限するためにタグを使用している場合、Web Studioは、制限として削除するためにグループを編集するまでタグを削除できないことを警告します。（アプリケーショングループで制限として使用されているタグを削除することが許可された場合、その結果、アプリケーショングループに関連付けられたデリバリーグループ内のすべてのマシンでアプリケーションが起動できるようになる可能性があります。）タグがデスクトップ起動の制限として使用されている場合も、タグの削除に対する同じ禁止が適用されます。そのタグ制限を削除するために、デリバリーグループ内のアプリケーショングループまたはデスクトップを編集した後、タグを削除できます。

すべてのマシンが同じアプリケーションセットを持っているとは限りません。ユーザーは複数のアプリケーショングループに属することができ、それぞれ異なるタグ制限と、デリバリーグループからの異なるまたは重複するマシンセットを持っています。以下の表は、マシンの考慮事項がどのように決定されるかを示しています。

アプリケーションが追加された場合	選択されたデリバリーグループ内のこれらのマシンが起動対象と見なされます
タグ制限のないアプリケーショングループが1つ	任意のマシン。
タグ制限Aのあるアプリケーショングループが1つ	タグAが適用されているマシン。
タグ制限Aのあるアプリケーショングループが1つと、タグ制限Bのあるアプリケーショングループが1つ（合計2つ）	タグAとタグBの両方を持つマシン。利用可能なマシンがない場合は、タグAまたはタグBのいずれかを持つマシン。
タグ制限Aのあるアプリケーショングループが1つと、タグ制限のないアプリケーショングループが1つ（合計2つ）	タグAを持つマシン。利用可能なマシンがない場合は、任意のマシン。

マシン再起動スケジュールでタグ制限を使用した場合、タグの適用または制限に影響を与える変更は、次のマシン再起動サイクルに影響します。変更が行われている間に進行中の再起動サイクルには影響しません。

例2の構成方法

以下の手順では、タグを作成して適用し、2番目の例で示されているアプリケーショングループのタグ制限を構成する手順を示します。

VDAとアプリケーションはすでにマシンにインストールされており、デリバリーグループも作成済みです。

マシンにタグを作成して適用します。

1. Web Studioで、デリバリーグループD01を選択し、アクションバーで「**マシンの表示**」を選択します。
2. マシン VDA 101～105 を選択し、アクションバーで**タグの管理**を選択します。
3. タグの管理ダイアログボックスで、**作成**をクリックし、`CADApps`という名前のタグを作成します。**OK**をクリックします。
4. もう一度**作成**をクリックし、OfficeAppsという名前のタグを作成します。**OK**をクリックします。
5. **タグの管理**ダイアログボックスを開いたまま、各タグの名前（`CADApps`と`OfficeApps`）の横にあるチェックボックスをオンにして、新しく作成したタグを選択したマシンに追加（適用）します。完了したら、ダイアログボックスを閉じます。
6. デリバリーグループD01を選択し、アクションバーで**マシンの表示**を選択します。
7. マシン VDA 106～110 を選択し、アクションバーで**タグの管理**を選択します。
8. **タグの管理**ダイアログボックスで、**作成**をクリックします。`AcctgApps`という名前のタグを作成します。**OK**をクリックします。
9. 新しく作成した`AcctgApps`タグと`OfficeApps`タグを、各タグ名の横にあるチェックボックスをクリックして、選択したマシンに適用し、ダイアログボックスを閉じます。

タグ制限付きのアプリケーショングループを作成します。

1. Web Studioで、左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択し、アクションバーで**アプリケーショングループの作成**を選択します。アプリケーショングループの作成ウィザードが起動します。
2. ウィザードの**デリバリーグループ**ページで、デリバリーグループD01を選択します。**タグ付きマシンへの起動を制限**を選択し、リストから`AcctgApps`タグを選択します。

3. 経理ユーザーと経理アプリケーションを指定して、ウィザードを完了します。（アプリケーションを追加するときは、`AcctgApps`タグを持つマシンでアプリケーションを検索する**スタートメニューから**ソースを選択します。）**概要**ページで、グループに`A100`という名前を付けます。
4. 前述の手順を繰り返してアプリケーショングループ`A200`を作成し、`CADApps`タグを持つマシン、および適切なユーザーとアプリケーションを指定します。
5. 手順を繰り返してアプリケーショングループ`A300`を作成し、`OfficeApps`タグを持つマシン、および適切なユーザーとアプリケーションを指定します。

マシンカタログのタグ

マシンカタログでタグを使用できます。タグを作成してカタログに適用する全体的な手順は、前述のとおりです。ただし、カタログへのタグの適用はPowerShellインターフェイスを介してのみサポートされています。Web Studioを使用してカタログにタグを適用したり、カタログからタグを削除したりすることはできません。Web Studioのカタログ表示では、タグが適用されているかどうかは示されません。

概要: Web StudioまたはPowerShellを使用して、カタログで使用するタグを作成または削除できます。PowerShellを使用して、タグをカタログに適用します。

カタログでタグを使用する例をいくつか示します。

- デリバリーグループには複数のカタログのマシンが含まれていますが、特定のカタログ内のマシンのみに操作（再起動スケジュールなど）を適用したい場合があります。そのカタログにタグを適用することで、これが実現します。
- アプリケーショングループでは、アプリケーションセッションを特定のカタログ内のマシンに制限したい場合があります。そのカタログにタグを適用することで、これが実現します。

影響を受けるPowerShellコマンドレット:

- `Add-BrokerTag`や`Remove-BrokerTag`などのコマンドレットにカタログオブジェクトを渡すことができます。
- `Get-BrokerTagUsage`は、タグを含むカタログの数を示します。
- `Get-BrokerCatalog`には、`Tags`という名前のプロパティがあります。

たとえば、次のコマンドレットは、`acctg`という名前のカタログに`fy2018`という名前のタグを追加します。`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`。(このタグは、以前にWeb StudioまたはPowerShellを使用して作成されています。)

詳細なガイダンスと構文については、PowerShellコマンドレットのヘルプを参照してください。

自動タグ (プレビュー)

自動タグ付けにより、管理者はカスタムルールに基づいて、さまざまなCitrix Virtual Apps and Desktopsオブジェクトにタグを自動的に設定および削除できます。この機能強化により、環境最適化のために定期的に実行されるさまざまなスクリプトを維持する必要がなくなります。

ユースケース

自動タグ付けを使用すると、コスト削減、インフラストラクチャの最適化、消費の促進など、ビジネスドライバーに関連するルールを実装できます。以下にいくつかのユースケースを示します。

- **未使用のVDIを再利用する** - 事前に設定された日数以上使用されていない専用ワークロードを、利用可能なプールに解放するため。
- **アプリの煩雑さを解消する** - 事前に設定された日数以上使用されていないアプリケーションを特定することで、アプリケーションの煩雑さを軽減するため。
- **X機能レベル未満のDG** - 特定の機能レベル未満のデリバリーグループを見つけるため。
- **非アクティブユーザー** - 事前に設定された日数以上ログオンしていないユーザーのリソースを再利用するため。

PowerShellコマンド

PowerShellコマンドを使用してオートタグを作成できます。オートタグルールが作成されると、600秒の頻度で評価されます。詳細については、New-BrokerAutoTagRuleを参照してください。

例

`New-BrokerAutoTagRule`は、`Get-BrokerMachine`コマンドレットと同じオブジェクトタイプとフィルターパラメーターを使用します。詳細については、GetBrokerMachineを参照してください。

1. 30日以上使用されていない専用VDIにID 123でタグを付けます:
    a. 未使用のVDIにタグ付けするためのタグを定義します。例えば、**unused-VDI**です。
        - タグ名 : unused-VDI
        - タグID : 123
    b. 未使用のマシンにタグを付ける自動タグ付けルールを作成します。ルールパラメーターを定義します:
        - 名前 : ルールの一般的な名前。
        - オブジェクトタイプ : マシン。

- ルールテキスト : 静的で、最終接続時間が30日以上前であるか、値がない割り当て済みマシン。
- タグUid : 関連付けたいタグID、123。

```
New-BrokerAutoTagRule -Name ‘UnusedVdi’ -ObjectType ‘Machine’ -RuleText “-AllocationType Static -IsAssigned $true -Filter { SummaryState -ne `”InUse`” -and ( LastConnectionTime -lt ‘-30’ -or LastConnectionTime -eq `$null ) }” -TagUid 123
```

c. タグ**unused-VDI**でマークされたマシンを確認し、それらを解放します。

2. X未満の機能レベルを持つデリバリーグループにタグを付けるには（**L7_20**を閾値機能レベルとして使用）：

```
New-BrokerAutoTagRule -Name 'LowFL' -ObjectType 'DesktopGroup' -RuleText " -Filter { MinimumFunctionalLevel -lt 'L7_20' } " -TagUid 123
```

1. フォルダーなしで公開された、ユーザーに表示されるアプリにタグを付けるには:

```
New-BrokerAutoTagRule -Name 'NoFolder' -ObjectType 'Application' -RuleText "-Enabled $true -Filter { ClientFolder -eq $null )} " -TagUid 123
```

詳細情報

ブログ投稿: 特定のサーバーにデスクトップを割り当てる方法。

Studio で検索機能を使用する

> **注:**
>
> Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前の対応する記事を参照してください。

特定の仮想マシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示するには、検索機能を使用します。Web Studioで**検索**を選択すると、いくつかのオプションが表示されます。

- タブを使用して、マシンを種類（シングルセッションまたはマルチセッションOS）別に一覧表示するか、すべてのセッションを一覧表示します。
- 検索ボックスに名前を入力します。入力すると、クイック検索用のフィルターが提供されます。
- フィルターを使用して検索を絞り込みます。
    - デフォルトでは、次のフィルターがビューにピン留めされています: 、、。フィルターを選択して式を作成します。フィルターをカスタマイズするには、省略記号をクリックします。表示されるウィンドウで、次のことができます。
        - フィルターをピン留めまたはピン留め解除します。ピン留め解除されたフィルターは一度限りの使用であり、保存されません。
        - フィルターをクリックしてビューに追加します。
        - フィルターをクリアして、現在のフィルター済み検索をクリアし、ピン留め解除されたフィルターを削除します。
    - オペレーターをクリックして、**すべて一致**（**AND**演算子）または**いずれか一致**（**OR**演算子）を切り替えます。**すべて一致**に設定すると、検索はすべてのフィルター条件に一致する結果を返します。いずれか一致に設定すると、検索はいずれかのフィルター条件に一致する結果を返します。
    - 星の記号をクリックして、使用中のフィルターを保存します。保存された項目はフィルターセットとして知られています。保存された項目は「保存されたフィルターセット」リストに表示されます。（リストにアクセスするには、検索ボックスを選択します。）保存されたフィルターセットをクリックすると、検索にフィルターを適用できます。保存されたフィルターセットを管理するには、検索ボックスを選択し、**管理**を選択します。

フィルターセットを管理する(/en-us/citrix-virtual-apps-desktops/2311/media/manage-filter-sets.png)

フィルターなしで検索

検索ボックスに入力すると、プロンプト付きのメニューが表示され、検索をすばやく絞り込むのに役立つさまざまな検索オプションが提供されます。入力したコンテンツが *VM01* であるとします。次のプロンプトのいずれかを選択します。

- VM01 名前。名前で検索します。
- VM01 マシンカタログ。名前で検索します。
- VM01 Delivery Group。デリバリーグループ名で検索します。

一般的な検索を実行すると、Citrix Virtual Apps and Desktops は以下の条件に一致するものを検索し、関連する結果を提供します。

- **名前**。マシン名またはDNS名で検索します。
- **マシンカタログ**。マシンカタログ名で検索します。
- **デリバリーグループ**。デリバリーグループ名で検索します。
- **ユーザー**。セッションユーザー名で検索します。
- **クライアント**。セッションクライアント名で検索します。
- **VM**。ホストされているマシン名で検索します。これは、ハイパーバイザーによって使用されるホストされたマシンのフレンドリ名です。
- **ホスティングサーバー名**。ホスティングサーバー名で検索します。

ユーザー、デスクトップグループ、カタログ、マシンなどの特定のアイテムを検索する場合、一般的な検索は必要な情報を見つける便利な方法を提供します。

マシンカタログまたはデリバリーグループの検索

マシンカタログノードとデリバリーグループノード内でリソースを検索および特定できます。これらのノードの検索機能は、検索ノードと同じインターフェイスを提供し、Citrix Virtual Apps and Desktops 全体でシームレスな検索エクスペリエンスを提供します。

一般検索とフィルターベースの検索を実行できます。マシンカタログでは、次のフィルターが利用可能です。

- **カタログ名**。マシンカタログの名前で検索します。
- **割り当ての種類**。静的（専用）またはランダム（プール）割り当て、あるいはその両方でフィルターします。
- **プロビジョニングの種類**。手動またはMCSプロビジョニング方法、あるいはその両方でフィルターします。
- **セッションサポート**。シングルセッションまたはマルチセッションマシン、あるいはその両方でフィルターします。
- **割り当て済み数**。割り当て済みのマシンの数でフィルターします。
- **永続性**。非永続的（破棄）または永続的（ローカルディスク上）なマシンの変更、あるいはその両方でフィルターします。
- **マシンの種類**。物理または仮想マシンの種類、あるいはその両方でフィルターします。

デリバリーグループでは、次のフィルターが利用可能です。

- **グループ名**。デリバリーグループの名前で検索します。
- **説明**。デリバリーグループ作成時に指定されたデリバリーグループの説明でフィルターします。
- **セッションサポート**。シングルセッションまたはマルチセッションマシン、あるいはその両方でフィルターします。
- **マシンID**。マシンのIDでフィルターします。
- **Remote PC Access**。Remote PC Accessマシンでフィルターします。
- **メンテナンスモード**。メンテナンスモードのマシン（オン、オフ、またはその両方）でフィルターします。
- **グループの状態**。グループの状態によってフィルタリングします。(デリバリーグループの編集 > ユーザー設定にある オプションは、アプリケーションとデスクトップの配信を停止するかどうかを制御します。)
- **割り当ての種類**。静的 (専用) またはランダム (プール) の種類、あるいはその両方でフィルタリングします。

一般検索を実行すると、Citrix Virtual Apps and Desktops は、以下の条件で項目を検索し、関連する結果を提供します。

- マシンカタログ:
  - 名前: フォルダーパスを含む名前でマシンカタログを検索します。
  - マシンカタログ: 名前でマシンカタログを検索します。
  - 説明。カタログ作成時に指定されたマシンカタログの説明で検索します。
- デリバリーグループ:
  - デリバリーグループ名: 名前でデリバリーグループを検索します。
  - 説明: デリバリーグループ作成時に指定されたデリバリーグループの説明で検索します。

アプリケーショングループの検索

アプリケーショングループに対して、一般検索とフィルターベースの検索を実行できます。アプリケーショングループでは、次のフィルターが利用可能です。

- **名前**。アプリケーショングループの名前でフィルタリングします。
- **タグ**。アプリケーショングループのタグでフィルタリングします。
- **説明**。アプリケーショングループ作成時に指定されたアプリケーショングループの説明でフィルタリングします。

- **デリバリーグループ**。アプリケーショングループのデリバリーグループでフィルタリングします。
- **状態**。アプリケーショングループの状態によってフィルタリングします。

表示する列をカスタマイズする

列をカスタマイズする際、「**パフォーマンスを低下させる**」というラベルが付いた列が表示されます。これらの列を選択すると、コンソールのパフォーマンスが低下する可能性があります。カスタマイズが完了すると、選択した列を表示するためにテーブルが更新されます。これらの列が存在すると、テーブルを更新する際に遅延が発生する可能性があります。

カスタマイズにパフォーマンスを低下させる列が含まれている場合、それらを保持するかどうかを決定するよう求められます。このプロンプトは、ブラウザウィンドウを更新するか、コンソールからサインアウトして再度サインインした後に表示されます。列を保持することを決定した場合、以下の考慮事項に注意してください。

- コンソールのパフォーマンスを確保するため、1分間に複数回テーブルを更新することはできません。この制限は、**シングルセッションOSマシン**、**マルチセッションOSマシン**、および**セッション**のすべてのタブに適用されます。より頻繁な更新が必要な場合は、パフォーマンスを低下させるすべての列を削除してください。

検索結果をCSVファイルにエクスポートする

検索結果（最大10,000項目）をCSVファイルにエクスポートできます。ファイルはブラウザのデフォルトのダウンロード場所に保存されます。

この機能は、マシンとセッションの両方で利用できます。検索結果をエクスポートするには、右上隅のエクスポートアイコンをクリックします。エクスポートには最大1分かかる場合があります。

検索ノードの各タブで、エクスポートが進行中の間は、別のエクスポートを実行できません。

検索を強化するためのヒント

検索機能を使用する際は、以下のヒントを考慮してください。

- **検索**ノードで、項目を並べ替えるには、任意の列を選択します。
- 検索および並べ替えが可能な表示に含める特性をさらに表示するには、**表示する列**を選択するか、任意の列をクリックして**表示する列**を選択します。**表示する列**ウィンドウで、表示したい項目の横にあるチェックボックスを選択し、**保存**を選択して終了します。

> **注：**
>
> パフォーマンスを低下させる項目には、**パフォーマンスを低下させる**ラベルが付けられます。

- マシンに接続されているユーザーデバイスを見つけるには、**クライアント (IP)** と **Is** を使用し、デバイスのIPアドレスを入力します。
- アクティブなセッションを見つけるには、**セッションの状態**、**Is**、および **接続済み** を使用します。
- デリバリーグループ内のすべてのマシンを一覧表示するには、左ペインで**デリバリーグループ**を選択します。グループを選択し、アクションバーまたはコンテキストメニューから**マシンの表示**を選択します。

並べ替え操作を実行する際は、以下の考慮事項に留意してください。

- 項目の数が5,000を超えない限り、任意の列をクリックして項目を並べ替えることができます。数が5,000を超えると、名前または現在のユーザー（現在表示しているタブによる）でのみ並べ替えることができます。並べ替えを有効にするには、フィルターを使用して項目の数を5,000以下に減らしてください。
- アイテム数が500より多く、5,000以下の場合:
  - 並べ替えのパフォーマンスを向上させるため、すべてのデータをローカルにキャッシュします。**シングルセッションOSマシン**タブと**マルチセッションOSマシン**タブでは、列（**名前**列を除く任意の列）を初めてクリックして並べ替えるときにデータをキャッシュします。**セッション**タブでは、列（**現在のユーザー**列を除く任意の列）を初めてクリックして並べ替えるときにデータをキャッシュします。その結果、並べ替えの完了に時間がかかります。パフォーマンスを向上させるには、名前または現在のユーザーで並べ替えるか、フィルターを使用して項目数を減らしてください。
  - テーブルの下に「最終更新日時: `<the time when you refreshed the table>`」というメッセージが表示されている場合、データがキャッシュされていることを示します。この場合、並べ替え操作は以前に読み込まれた項目に基づいています。これらの項目は最新ではない可能性があります。最新の状態にするには、更新アイコンをクリックしてください。

設定

注:

Citrix Virtual Apps and Desktops™展開は、Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の対応する記事を参照してください。

Web Studioを使用して、以下の設定を管理できます。

- 認証の管理
- Citrixカスタマーエクスペリエンス向上プログラム
- デリバリーコントローラーを削除
- ログデータベースの変更
- 日付と時刻の設定
- サイト管理の一元化
- リモートPCアクセスでの複数ユーザーの自動割り当てを有効にする
- DNS解決の有効化
- XML信頼の有効化
- セキュリティキーの管理
- Studioコンソールの非アクティブタイムアウトの設定

認証の管理

デフォルトでは、ユーザーはドメイン資格情報（ユーザー名とパスワード）を使用してWeb Studioに認証します。統合Windows認証を有効にすると、ユーザーはKerberosまたはNTLMを使用してWindows資格情報でStudioにアクセスできます。ドメイン資格情報によるサインインの無効化はサポートされていません。

重要

Web Studio が Delivery Controller のプロキシとして構成されている場合、統合 Windows 認証は機能しません。

> **統合Windows認証**オプションを有効にすると、次回ユーザーがログオンしたときに、自動的にサインインされます。ユーザーとして自動的にサインインできない場合は、以下の手順に従ってWebブラウザーを構成し、統合Windows認証を許可してください。

Google Chromeの場合:

1. コントロールパネルから、インターネットオプションを選択します。
2. **詳細設定**タブを選択します。
3. **統合Windows認証を有効にする**を選択します。
4. **セキュリティ**タブを選択します。
5. **ローカルイントラネット > サイト > 詳細設定**を選択します。
6. **このWebサイトをゾーンに追加する**ボックスで:
   - Web StudioとDelivery Controller™が同じサーバー上にある場合、Web Studioを実行しているホストのURLを入力します。
   - そうでない場合は、ワイルドカードドメインを入力します。例: Delivery Controllerが `ddc.domain.com` にある場合、`*.domain.com` と入力します。
7. **追加 > 閉じる**をクリックします。

Mozilla Firefoxの場合：

1. ブラウザから、URLボックスに `about:config` と入力します。
2. **検索**ボックスに `network negotiate` と入力します。
3. **network.negotiate-auth.trusted-uris**を右クリックし、**変更**を選択します。
4. **文字列値を入力**ボックスで:
   - Web Studio と Delivery Controller が同じサーバー上にある場合は、Web Studio をホストしているサーバー名を参照する URL および/またはエイリアスのコンマ区切りリストを追加します。
   - そうでない場合は、次のように URL を追加します。例: Delivery Controller が `ddc.domain.com` にある場合、「`*.domain.com`」と入力します。

ブラウザーを設定したら、サインインページで「**Windows 統合サインイン**」をクリックして再試行できます。

Web Studio と Delivery Controller が異なるマシンにインストールされている場合、統合 Windows 認証を機能させるには、「**クロスオリジンアクセスを許可**」を有効にする必要があります。

「**クロスオリジンアクセスを許可**」を有効にするには、次の手順に従います。

1. **クロスオリジンアクセスを許可**チェックボックスをオンにします。
2. Web StudioサーバーのURLを許可リストに追加します。
3. **URLを入力**フィールドにURLを入力します。必要に応じて、**追加**をクリックしてさらに追加します。

> **注**
>
> - URL は正しい形式 `<scheme>://<hostname>` に従う必要があります。パスや末尾のスラッシュを含まないようにしてください。
> - IP アドレスと FQDN がサポートされています。URL を追加するときは、Web Studio へのアクセス方法と一致していることを確認してください。たとえば、IP アドレスを使用して Web Studio にアクセスする場合は、IP アドレスベースの URL をリストに追加します。
> - デフォルト以外のポートを使用する場合は、ポート番号を含めるようにしてください。

4. 必要に応じて、「**追加**」をクリックしてさらに追加します。
5. 完了したら、「**完了**」をクリックして保存し、終了します。

タイムゾーンを設定する

日付と時刻の形式を好みに合わせてカスタマイズするには、次の手順に従います。

1. Web Studio にサインインし、左ペインで「**設定**」を選択します。
2. 「**日付と時刻**」タイルを見つけて「**編集**」をクリックし、次のオプションを設定します。
   - **時刻形式:**
     - 時刻を12時間形式（例：午後09:00）または24時間形式（例：21:00）で表示するように選択します。
   - **日付形式:**
     - yyyy/MM/dd のように、好みに合わせて日付形式を設定します。
   - **タイムゾーン:**

- **UTC:** ユーザーインターフェイス全体で日付と時刻をUTCで表示します。日付と時刻にマウスを合わせると、その情報がローカルタイムゾーンで表示されます。
- **ローカルタイムゾーン:** ユーザーインターフェイス全体で日付と時刻をローカルタイムゾーンで表示します。日付と時刻にマウスを合わせると、その情報がUTCで表示されます。

DNS解決を有効にする

ICA®ファイルでIPアドレスの代わりにDNS名を表示するには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで**設定**を選択します。
2. **DNS解決を有効にする**設定をオンにします。

Studioコンソールの非アクティビティタイムアウトを設定する

管理者がStudioコンソールから自動的にサインアウトされるまでの非アクティビティ期間を設定できます。

1. Web Studioにサインインし、左側のペインで**設定**を選択します。
2. 10分から24時間の範囲で期間を入力します。
3. この設定を適用するには、ページを更新するか、サインアウトしてから再度サインインします。

サイト管理の一元化

この機能を使用すると、1つのWeb Studioコンソールで複数のCitrix Virtual Apps and Desktopsサイトを管理できます。詳細については、複数のサイト管理を有効にするを参照してください。

ユーザープロファイル

デフォルトでは、Virtual Delivery Agentのインストール時にCitrix Profile Managementがマスターイメージにサイレントインストールされますが、プロファイルソリューションとしてProfile Managementを使用する必要はありません。

ユーザーのさまざまなニーズに合わせて、Citrix Virtual Apps and Desktops™ポリシーを使用して、各デリバリーグループ内のマシンに異なるプロファイル動作を適用できます。たとえば、あるデリバリーグループでは、テンプレートが1つのネットワークの場所に保存されているCitrix強制プロファイルが必要な場合があります。一方、別のデリバリーグループでは、複数のリダイレクトされたフォルダーを持つ別の場所に保存されているCitrixローミングプロファイルが必要な場合があります。

- 組織内の他の管理者がCitrix Virtual Apps and Desktopsポリシーを担当している場合は、それらの管理者と協力して、デリバリーグループ全体でプロファイル関連のポリシーが設定されていることを確認してください。
- Profile Managementポリシーは、グループポリシー、Profile Management .iniファイル、および個々の仮想マシン上でローカルに設定することもできます。プロファイル動作を定義するこれらの複数の方法は、次の順序で読み取られます。

  a. グループポリシー（.admまたは.admxファイル）

  b. ポリシーノードのCitrix Virtual Apps and Desktopsポリシー

  c. ユーザーが接続する仮想マシン上のローカルポリシー

  d. Profile Management .iniファイル

  たとえば、グループポリシーとポリシーノードの両方で同じポリシーを構成した場合、システムはグループポリシーのポリシー設定を読み取り、Citrix Virtual Apps and Desktopsポリシー設定は無視します。

どのプロファイルソリューションを選択しても、Director 管理者は診断情報にアクセスし、ユーザープロファイルのトラブルシューティングを行うことができます。詳しくは、Directorドキュメントを参照してください。

自動構成

デスクトップの種類は、Virtual Delivery Agentのインストールに基づいて自動的に検出され、Studioで行う構成の選択に加えて、それに応じてProfile Managementのデフォルトを設定します。

Profile Managementが調整するポリシーを次の表に示します。デフォルト以外のポリシー設定は保持され、この機能によって上書きされることはありません。各ポリシーの詳細については、Profile Managementのドキュメントを参照してください。プロファイルを作成するマシンの種類は、調整されるポリシーに影響します。主な要因は、マシンが永続的かプロビジョニング済みか、および複数のユーザーで共有されるか、1人のユーザー専用であるかです。

永続システムには何らかの種類のローカルストレージがあり、システムがシャットダウンしてもその内容が保持されることが期待されます。永続システムでは、SANなどのストレージテクノロジーを使用して、ローカルディスクを模倣する場合があります。対照的に、プロビジョニングされたシステムは、ベースディスクと何らかの種類のIDディスクから「オンザフライ」で作成されます。ローカルストレージは通常、RAMディスクまたはネットワークディスクによって模倣され、後者は高速リンクを備えたSANによって提供されることがよくあります。プロビジョニングテクノロジーは通常、Citrix ProvisioningまたはMachine Creation Services™（あるいはサードパーティ

の同等品）です。プロビジョニングされたシステムが永続的なローカルストレージを持つ場合もあります。これらは永続システムとして分類されます。

これら2つの要素を組み合わせることで、以下のマシンタイプが定義されます。

- **永続的かつ専用**。例としては、Machine Creation Servicesで作成された静的割り当てと永続的なローカルストレージを持つシングルセッションOSマシン、物理ワークステーション、およびラップトップがあります。
- **永続的かつ共有**。例としては、Machine Creation Servicesで作成されたマルチセッションOSマシン、およびCitrix Virtual Appsサーバーがあります。
- **プロビジョニング済みかつ専用**。例としては、Citrix Provisioning Service (Citrix Virtual Desktops™内) で作成された、静的割り当てを持つが永続ストレージを持たないシングルセッションOSマシンがあります。
- **プロビジョニング済みかつ共有**。例としては、Citrix Provisioning™ Service (Citrix Virtual Desktops内) で作成されたランダム割り当てを持つシングルセッションOSマシン、およびCitrix Virtual Appsサーバーがあります。

以下のProfile Managementポリシー設定は、異なるマシンタイプに対する推奨ガイドラインです。これらはほとんどの場合にうまく機能しますが、展開の要件に応じて変更することもできます。

> **重要:**
>
> **ログオフ時にローカルにキャッシュされたプロファイルを削除**、**プロファイルストリーミング**、および**常にキャッシュ**は、自動構成機能によって適用されます。その他のポリシーは手動で調整してください。

永続マシン

ポリシー	永続的かつ専用	永続的かつ共有
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	有効
プロファイルストリーミング	無効	有効
常にキャッシュ	有効 (注1)	無効 (注2)

ポリシー	永続的かつ専用	永続的かつ共有
アクティブライトバック	無効	無効 (注3)
ローカル管理者によるログオンの処理	有効	無効 (注4)

プロビジョニング済みマシン

ポリシー	プロビジョニング済みと専用の両方	プロビジョニング済みと共有の両方
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効 (注5)	有効
プロファイルストリーミング	有効	有効
常にキャッシュ	無効 (注6)	無効
アクティブライトバック	有効	有効
ローカル管理者によるログオンを処理する	有効	有効 (注 7)

1. このマシンタイプでは**プロファイルストリーミング**が無効になっているため、**常にキャッシュ**設定は常に無視されます。
2. **常にキャッシュ**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルに読み込まれるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。
3. Citrix Virtual Appsサーバー間をローミングするユーザーのプロファイルに変更を保存する場合を除き、**アクティブライトバック**を無効にします。この場合は、このポリシーを有効にします。
4. ホスト型共有デスクトップの場合を除き、**ローカル管理者ログオンの処理**を無効にします。この場合は、このポリシーを有効にします。
5. **ログオフ時にローカルにキャッシュされたプロファイルを削除**を無効にします。この設定により、ローカルにキャッシュされたプロファイルが保持されます。マシンはログオフ時にリセッ

トされますが、個々のユーザーに割り当てられるため、プロファイルがキャッシュされている場合はログオンが高速になります。

6. **常にキャッシュ**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルに読み込まれるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。
7. Citrix Virtual Apps and Desktopsサーバー間をローミングするユーザーのプロファイルの場合を除き、**ローカル管理者ログオンの処理**を有効にします。この場合は、このポリシーを無効にします。

フォルダーリダイレクト

フォルダーリダイレクトを使用すると、プロファイルが保存されている場所とは異なるネットワーク共有にユーザーデータを保存できます。フォルダーリダイレクトはプロファイルのサイズと読み込み時間を短縮しますが、ネットワーク帯域幅に影響を与える可能性があります。フォルダーリダイレクトは、Citrixユーザープロファイルが使用されていることを必要としません。ユーザープロファイルを独自に管理し、フォルダーをリダイレクトすることもできます。

StudioのCitrixポリシーを使用してフォルダーリダイレクトを構成します。

- リダイレクトされたフォルダーのコンテンツを保存するために使用されるネットワークの場所が利用可能であり、適切な権限を持っていることを確認してください。場所のプロパティは検証されます。
- リダイレクトされたフォルダーはネットワーク上に設定され、そのコンテンツはログオン時にユーザーの仮想デスクトップから入力されます。

フォルダーリダイレクトは、CitrixポリシーまたはActive Directoryグループポリシーオブジェクトのいずれか一方のみを使用して構成し、両方は使用しないでください。両方のポリシーエンジンを使用してフォルダーリダイレクトを構成すると、予期しない動作が発生する可能性があります。

高度なフォルダーリダイレクト

複数のオペレーティングシステム (OS) を使用する展開では、ユーザープロファイルの一部を各OSで共有したい場合があります。プロファイルの残りの部分は共有されず、1つのOSでのみ使用されます。OS間で一貫したユーザーエクスペリエンスを確保するには、各OSで異なる構成、つまり高度なフォルダーリダイレクトが必要です。たとえば、2つのOSで実行されているアプリケーションの異なるバージョンが共有ファイルを読み書きする必要がある場合、両方のバージョンがアクセスできる単一のネットワーク場所にリダイレクトすることを決定します。あるいは、2つのOSで**スタートメニュー**フォルダーの内容が異なる構造になっているため、両方ではなく片方の

フォルダーのみをリダイレクトすることを決定します。このアプローチにより、各OSで**スタートメニュー**フォルダーとその内容が分離され、ユーザーに一貫したエクスペリエンスが保証されます。

展開で高度なフォルダーリダイレクトが必要な場合は、ユーザーのプロファイルデータの構造を理解し、そのどの部分をOS間で共有できるかを判断する必要があります。フォルダーリダイレクトが正しく使用されないと、予期しない動作が発生する可能性があります。

高度な展開でフォルダーをリダイレクトするには：

- 各OSに個別のデリバリーグループを使用します。
- 仮想デスクトップ上のものを含む仮想アプリケーションがユーザーデータと設定をどこに保存するか、およびデータがどのように構造化されているかを理解します。
- 安全にローミングできる共有プロファイルデータ（各OSで同じ構造になっているため）については、各デリバリーグループで、そのデータを含むフォルダーをリダイレクトします。
- ローミングできない非共有プロファイルデータについては、デスクトップグループのいずれか1つでのみ、そのデータを含むフォルダーをリダイレクトします。通常、最も使用頻度の高いOS、またはデータが最も関連性の高いOSのグループです。あるいは、OS間でローミングできない非共有データの場合、両方のシステムで、そのデータを含むフォルダーを個別のネットワーク場所にリダイレクトします。

高度な展開の例

この展開には、Windows 10デスクトップで実行されるMicrosoft OutlookおよびInternet Explorerのバージョンを含むアプリケーションと、Windows Server 2019によって提供される、OutlookおよびInternet Explorerの他のバージョンを含むアプリケーションがあります。2つのOS用に2つのデリバリーグループをすでに設定しています。ユーザーは、2つのアプリケーションのどちらのバージョンでも、同じ**連絡先**と**お気に入り**のセットにアクセスしたいと考えています。

重要: 以下の決定とアドバイスは、説明されているOSと展開に有効です。組織では、リダイレクトするフォルダーとそれらを共有するかどうかの決定は、特定の展開に固有のさまざまな要因に依存します。

- デリバリーグループに適用されるポリシーを使用して、以下のフォルダーをリダイレクトするように選択します。

フォルダ	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
マイ ドキュメント	はい	はい

フォルダ	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
アプリケーションデータ	いいえ	いいえ
連絡先	はい	はい
デスクトップ	はい	いいえ
ダウンロード	いいえ	いいえ
お気に入り	はい	はい
リンク	はい	いいえ
マイミュージック	はい	はい
マイピクチャ	はい	はい
マイビデオ	はい	はい
検索	はい	いいえ
保存されたゲーム	いいえ	いいえ
スタートメニュー	はい	いいえ

- 共有され、リダイレクトされるフォルダーの場合：
  - OutlookとInternet Explorerの異なるバージョンによって保存されたデータの構造を分析した結果、**連絡先**フォルダーと**お気に入り**フォルダーを共有しても安全であると判断しました。
  - **マイ ドキュメント**、**マイ ミュージック**、**マイ ピクチャ**、および**マイ ビデオ**フォルダーの構造はOS間で標準的であることがわかっています。そのため、これらのフォルダーを各デリバリーグループで同じネットワーク場所に保存しても安全です。
- 共有されない、リダイレクトされたフォルダーの場合:
  - Windows Serverデリバリーグループでは、デスクトップ、リンク、検索、または**スタートメニュー**フォルダーをリダイレクトしません。これらのフォルダー内のデータは2つのOSで異なる方法で整理されているためです。したがって、共有することはできません。

    - この非共有データの予測可能な動作を保証するために、Windows 10デリバリーグループでのみリダイレクトします。Windows 10は、ユーザーが日常業務でより頻繁に使用します。ユーザーは、Windows Serverによって提供されるアプリケーションにたまにしかアクセスしません。また、この場合、非共有データはアプリケーション環境よりもデスクトップ環境により関連性が高くなります。たとえば、デスクトップショートカットは**デスクトップ**フォルダーに保存され、Windows 10マシンから作成されたものであれば役立つ可能性がありますが、Windows Serverマシンから作成されたものでは役立ちません。

- リダイレクトされないフォルダーの場合:

    - ユーザーのダウンロードファイルでサーバーを散らかしたくないため、ダウンロードフォルダーをリダイレクトしないことを選択します
    - 個々のアプリケーションからのデータは互換性やパフォーマンスの問題を引き起こす可能性があるため、アプリケーションデータフォルダーをリダイレクトしないことを決定します

フォルダーリダイレクトの詳細については、「フォルダーリダイレクト、オフラインファイル、およびローミングユーザープロファイルの概要」を参照してください。

フォルダーリダイレクトと除外

Citrix Profile Management（Studioではない）では、パフォーマンス強化により、除外を使用してフォルダーが処理されるのを防ぐことができます。この機能を使用する場合、リダイレクトされたフォルダーを除外しないでください。フォルダーリダイレクト機能と除外機能は連携して動作します。リダイレクトされたフォルダーが除外されないようにすることで、後でリダイレクトしないと決定した場合でも、Profile Managementがそれらをプロファイルフォルダー構造に戻し、データ整合性を維持できます。除外の詳細については、「アイテムの含める/除外」を参照してください。

VDA登録

はじめに

> **注:**
>
> オンプレミス環境では、VDAはDelivery Controllerに登録します。Citrix Cloudサービス環境では、VDAはCloud Connectorに登録します。ハイブリッド環境では、一部のVDAはDelivery Controllerに登録し、他のVDAはCloud Connectorに登録します。

> VDAを使用する前に、サイト上の1つ以上のControllerまたはCloud Connectorに登録（通信を確立）する必要があります。VDAは、`ListofDDCs`と呼ばれるリストを確認することで、ControllerまたはConnectorを見つけます。VDA上の`ListOfDDCs`には、そのVDAをサイト上のControllerまたはCloud ConnectorにポイントするDNSエントリが含まれています。負荷分散のため、VDAはリスト内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。

VDA登録がそれほど重要であるのはなぜですか？

- セキュリティの観点から見ると、登録は機密性の高い操作です。ControllerまたはCloud ConnectorとVDA間の接続を確立しています。このような機密性の高い操作では、すべてが完璧な状態でない場合、接続を拒否するのが期待される動作です。VDAからControllerまたはCloud Connectorへ、およびControllerまたはCloud ConnectorからVDAへの2つの別々の通信チャネルを効果的に確立しています。接続にはKerberosが使用されるため、時刻同期やドメインメンバーシップの問題は許容されません。Kerberosはサービスプリンシパル名（SPN）を使用するため、負荷分散されたIP\\ホスト名を使用することはできません。
- Controller（またはCloud Connector）を追加および削除する際に、VDAが正確で最新のControllerまたはCloud Connector情報を持っていない場合、VDAはリストにないControllerまたはCloud Connectorによって仲介されたセッション起動を拒否する可能性があります。無効なエントリは、仮想デスクトップシステムソフトウェアの起動を遅らせる可能性があります。VDAは、不明で信頼されていないControllerまたはCloud Connectorからの接続を受け入れません。

`ListofDDCs`に加えて、`ListOfSIDs`（セキュリティID）は、`ListofDDCs`内のどのマシンが信頼されているかを示します。`ListofSIDs`は、Active Directoryへの負荷を軽減したり、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避したりするために使用できます。詳細については、ListOfSIDsを参照してください。

`ListofDDCs`が複数のControllerまたはCloud Connectorを指定している場合、VDAはランダムな順序でそれらに接続しようとします。オンプレミス展開では、`ListofDDCs`にはControllerグループも含まれる場合があります。VDAは、`ListofDDCs`内の他のエントリに移動する前に、グループ内の各Controllerに接続しようとします。

Citrix Virtual Apps and Desktops™は、VDAのインストール中に構成されたControllerまたはCloud Connectorへの接続を自動的にテストします。ControllerまたはCloud Connectorに到達できない場合、エラーが表示されます。ControllerまたはCloud Connectorに接続できないという警告を無視した場合（またはVDAのインストール中にControllerまたはCloud Connectorのアドレスを指定しなかった場合）、メッセージが表示されて通知されます。

ControllerまたはCloud Connectorアドレスを構成する方法

管理者は、VDAが初めて登録するとき（初回登録時）に使用する構成方法を選択します。初回登録時に、VDA上に永続的なキャッシュが作成されます。その後の登録では、構成の変更が検出されない限り、VDAはこのローカルキャッシュからControllerまたはCloud Connectorのリストを取得します。

その後の登録でそのリストを取得する最も簡単な方法は、自動更新機能を使用することです。自動更新はデフォルトで有効になっています。詳細については、「自動更新」を参照してください。

VDA上でControllerまたはCloud Connectorアドレスを構成する方法はいくつかあります。

- ポリシーベース (LGPOまたはGPO)
- レジストリベース (手動、グループポリシー設定 (GPP)、VDAインストール時に指定)
- Active Directory OUベース (レガシーOU検出)
- MCSベース (personality.ini)

VDAをインストールする際に、初期登録方法を指定します。(自動更新を無効にすると、VDAインストール時に選択した方法が以降の登録に使用されます。)

次のグラフィックは、VDAインストールウィザードの**Delivery Controller**ページを示しています。

VDAインストールウィザードのDelivery Controllerページ(/en-us/citrix-virtual-apps-desktops/2311/media/vda-install-controllers-all.png)

ポリシーベース (LGPO\\GPO)

Citrix®は、初期VDA登録にGPOを使用することを推奨しています。これは最も高い優先順位を持ちます。(自動更新が最も高い優先順位としてリストされていますが、自動更新は初期登録後にのみ使用されます。)ポリシーベースの登録は、構成にグループポリシーを使用することによる一元化の利点を提供します。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**後で実行 (詳細)** を選択します。VDAインストール中にコントローラーアドレスを指定しない場合でも、ウィザードはコントローラーアドレスを指定するよう何度か通知します。(VDA登録はそれほど重要です。)
- Citrixポリシーを使用して、`Virtual Delivery Agent Settings > Controllers`設定でポリシーベースのVDA登録を有効または無効にします。(セキュリティが最優先事項である場合は、`Virtual Delivery Agent Settings > Controller SIDs`設定を使用します。)

この設定は、`HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`に保存されます。

レジストリベース

この方法を指定するには、以下のいずれかの手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**手動で実行** を選択します。次に、インストールされているControllerのFQDNを入力し、**追加** をクリックします。複数のControllerをインストールしている場合は、それらのアドレスを追加します。
- コマンドラインVDAインストールの場合、/controllersオプションを使用し、インストールされているControllerまたはCloud ConnectorのFQDNを指定します。

この情報は、レジストリキー`HKLM\Software\Citrix\VirtualDesktopAgent`または`HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`の下のレジストリ値`ListOfDDCs`に保存されます。

このレジストリキーを手動で構成することも、グループポリシー設定 (GPP) を使用することもできます。この方法は、ポリシーベースの方法よりも好ましい場合があります (たとえば、異なるControllerまたはCloud Connectorの条件付き処理が必要な場合。例: XDW-001-で始まるコンピューター名にはXDC-001を使用する)。

サイト内のすべてのControllerまたはCloud ConnectorのFQDNを一覧表示する`ListOfDDCs`レジストリキーを更新します。（このキーは、Active Directoryサイト OUに相当します。）

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`レジストリの場所に`ListOfDDCs`と`FarmGUID`の両方のキーが含まれている場合、ControllerまたはCloud Connectorの検出には`ListOfDDCs`が使用されます。VDAインストール中にサイトOUが指定された場合、`FarmGUID`が存在します。（これはレガシー展開で使用される可能性があります。）

オプションで、`ListOfSIDs`レジストリキーを更新します (詳細については、「ListOfSIDs」を参照してください)。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)`

注意: Citrixポリシーを介してポリシーベースのVDA登録も有効にすると、それはVDAインストール中に指定した設定を上書きします。これは、より優先度の高い方法であるためです。

Active Directory OUベース (レガシー)

この方法は主に下位互換性のためにサポートされており、推奨されません。まだこの方法を使用している場合は、別の方法に変更することをお勧めします。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**Active Directoryから場所を選択**を選択します。
- （すべてのControllerで利用可能な）`Set-ADControllerDiscovery.ps1`スクリプトを使用します。また、各VDAで`FarmGuid`レジストリエントリを構成して、適切なOUを指すようにします。この設定はグループポリシーを使用して構成できます。

MCSベース

MCSを使用してVMをプロビジョニングする場合、MCSはControllerまたはCloud Connectorのリストを設定します。この機能は自動更新と連携します。カタログの作成時、MCSは初期プロビジョニング中にControllerまたはCloud Connectorのリストを `Personality.ini` ファイルに挿入します。自動更新により、リストは最新の状態に保たれます。

この方法を指定するには、VDAインストールウィザードの **Delivery Controller** ページで、**Machine Creation Services™に任せる** を選択します。

レビューと推奨事項

ベストプラクティスとして:

- 初期登録にはグループポリシー登録方法を使用します。
- Controllerのリストを最新の状態に保つには、自動更新（デフォルトで有効）を使用します。
- マルチゾーン展開では、初期構成にグループポリシーを使用します（少なくとも2つのControllerまたはCloud Connectorを使用）。VDAを、そのゾーン内のローカルなControllerまたはCloud Connectorにポイントします。自動更新を使用して、それらを最新の状態に保ちます。自動更新は、サテライトゾーンのVDAに対して`ListofDDCs`を自動的に最適化します。
- Controllerが利用できない場合の登録問題を回避するため、`ListOfDDCs`レジストリキーに複数のControllerをスペースまたはコンマで区切ってリストします。例：

```
DDC7x.xd.local DDC7xHA.xd.local



32-bit: HKEY_LOCAL_MACHINE
```

```
\Software\Citrix\VirtualDesktopAgent\ListOfDDCs



HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs
(REG_SZ)
```

- `ListofDDCs`の下にリストされているすべての値が有効な完全修飾ドメイン名にマッピングされていることを確認し、起動時の登録遅延を防ぎます。

自動更新

自動更新（XenAppおよびXenDesktop 7.6で導入）はデフォルトで有効になっています。これは、VDA登録を最新の状態に保つための最も効率的な方法です。初期登録には使用されませんが、初期登録時に自動更新ソフトウェアが`ListofDDCs`をダウンロードし、VDA上の永続キャッシュに保存します。このプロセスは各VDAに対して実行されます。キャッシュにはマシンポリシー情報も保持され、ポリシー設定が再起動後も保持されることを保証します。

MCSまたはCitrix Provisioning™を使用してマシンをプロビジョニングする場合、自動更新がサポートされますが、Citrix Provisioningのサーバー側キャッシュは例外です。サーバー側キャッシュは、自動更新キャッシュ用の永続ストレージがないため、一般的なシナリオではありません。

この方法を指定するには:

- 設定`Virtual Delivery Agent Settings > Enable auto update of Controllers`を含む Citrix ポリシーを通じて、自動更新を有効または無効にします。この設定はデフォルトで有効になっています。

仕組み:

- VDAが再登録するたび（たとえば、マシンの再起動後）、キャッシュが更新されます。各ControllerまたはCloud Connectorも、90分ごとにサイトデータベースをチェックします。前回のチェック以降にControllerまたはCloud Connectorが追加または削除された場合、あるいはVDA登録に影響するポリシー変更が発生した場合、ControllerまたはCloud Connectorは登録済みのVDAに更新されたリストを送信し、キャッシュが更新されます。VDAは、最新のキャッシュリストにあるすべてのControllerまたはCloud Connectorからの接続を受け入れます。
- VDAが、登録されているControllerまたはCloud Connectorが含まれていないリスト（つまり、そのControllerまたはCloud Connectorがサイトから削除された）を受信した場合、VDAは`ListofDDCs`内のControllerまたはCloud Connectorの中から選択して再登録します。

例:

- 展開には3つのController（A、B、C）があります。VDAはController Bに登録します（これはVDAのインストール時に指定されました）。
- その後、2つのController（DとE）がサイトに追加されます。90分以内に、VDAは更新されたリストを受信し、Controller A、B、C、D、Eからの接続を受け入れます。（VDAが再起動されるまで、負荷はすべてのControllerに均等に分散されません。）
- さらにその後、Controller Bが別のサイトに移動されます。90分以内に、元のサイトのVDAは、前回のチェック以降にControllerの変更があったため、更新されたリストを受信します。元々Controller Bに登録されていたVDA（リストにはもうありません）は、現在のリスト（A、C、D、E）のControllerの中から選択して再登録します。

マルチゾーン展開では、サテライトゾーンの自動更新は、まずすべてのローカルControllerを自動的にキャッシュします。プライマリゾーンのすべてのControllerはバックアップグループにキャッシュされます。サテライトゾーンにローカルControllerが利用できない場合、プライマリゾーンのControllerで登録が試行されます。

次の例に示すように、キャッシュファイルにはホスト名とセキュリティID (`ListofSIDs`) のリストが含まれています。VDAはSIDを照会しないため、Active Directoryの負荷が軽減されます。

VDAの登録キャッシュファイルの例(/en-us/citrix-virtual-apps-desktops/2311/media/vda-registration-cache-file.png)

キャッシュファイルはWMI呼び出しで取得できます。ただし、SYSTEMアカウントのみが読み取り可能な場所に保存されています。

> **重要:**
>
> この情報は情報提供のみを目的としています。このファイルを変更しないでください。このファイルまたはフォルダーへの変更は、サポートされていない構成になります。

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

セキュリティ上の理由（Active Directoryの負荷軽減とは異なる）で `ListofSIDs` を手動で構成する必要がある場合、自動更新機能は使用できません。詳細については、「ListOfSIDs」を参照してください。

自動更新の優先順位の例外

自動更新は通常、すべてのVDA登録方法の中で最も高い優先順位を持ち、他の方法の設定を上書きしますが、例外があります。キャッシュ内の`NonAutoListOfDDCs`要素は、初期VDA構成方法を指定します。自動更新はこの情報を監視します。初期登録方法が変更された場合、登録プロセスは自動更新をスキップし、次に高い優先順位で構成された方法を使用します。このプロセスは、VDAを別のサイトに移動する場合（たとえば、災害復旧中）に役立ちます。

構成に関する考慮事項

一般的なVDA登録構成を表示します。

<iframe src="https://www.youtube.com/embed/MgGMZp4SnZgEq9ieibQc9j" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録手順を表示します。

<iframe src="https://www.youtube.com/embed/iwsbajSVY5QvoUTh6m7AjG" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録に影響を与える可能性のある項目を構成する際には、以下を考慮してください。

ControllerまたはCloud Connectorのアドレス

ControllerまたはCloud Connectorを指定するためにどの方法を使用するかにかかわらず、CitrixはFQDNアドレスを使用することを推奨します。IPアドレスは信頼できる構成とは見なされません。なぜなら、DNSレコードよりもIPを侵害する方が簡単だからです。`ListofSIDs`を手動で入力する場合、`ListofDDCs`でIPを使用できます。ただし、FQDNが引き続き推奨されます。

負荷分散

前述のとおり、VDAは`ListofDDCs`内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。フェールオーバーと負荷分散機能は、Citrix Brokering Protocol (CBP) に組み込まれています。構成で複数のControllerまたはCloud Connectorを指定した場合、必要に応じて登録はそれらの間で自動的にフェールオーバーします。自動更新では、すべてのVDAで自動フェールオーバーが自動的に発生します。

セキュリティ上の理由から、Citrix ADCなどのネットワークロードバランサーを使用することはできません。VDA登録ではKerberos相互認証が使用され、クライアント（VDA）はサービス（Controller）に対して自身のIDを証明する必要があります。しかし、ControllerまたはCloud ConnectorもVDAに対して自身のIDを証明する必要があります。これは、VDAとControllerまたはCloud Connectorが同時にサーバーとクライアントとして機能することを意味します。この記事の

冒頭で述べたように、VDAからController/Cloud Connectorへ、およびController/Cloud ConnectorからVDAへの2つの通信チャネルがあります。

このプロセスにおけるコンポーネントの1つは、サービスプリンシパル名（SPN）と呼ばれ、Active Directoryコンピューターオブジェクトのプロパティとして保存されます。VDAがControllerまたはCloud Connectorに接続するとき、通信したい相手を指定する必要があります。このアドレスがSPNです。負荷分散されたIPを使用すると、Kerberos相互認証は、そのIPが予期されるControllerまたはCloud Connectorに属していないことを正しく認識します。

詳細については、以下を参照してください。

- Kerberosの概要
- Kerberosを使用した相互認証

自動更新によるCNAMEの置き換え

自動更新機能は、XenAppおよびXenDesktop 7.xより前のバージョンにおけるCNAME (DNSエイリアス) 機能を置き換えます。CNAME機能は、XenAppおよびXenDesktop 7以降では無効になっています。CNAMEの代わりに自動更新を使用してください。(CNAMEを使用する必要がある場合は、CTX137960を参照してください。DNSエイリアスを常に機能させるには、自動更新とCNAMEを同時に使用しないでください。)

Controller/Cloud Connectorグループ

特定のシナリオでは、ControllerまたはCloud Connectorをグループで処理し、一方のグループを優先し、すべてのController/Cloud Connectorが失敗した場合に他方のグループをフェールオーバーに使用したい場合があります。ControllerまたはCloud Connectorはリストからランダムに選択されるため、グループ化することで優先的な使用を強制するのに役立ちます。

これらのグループは、単一のサイト内での使用を目的としています（複数のサイトではありません）。

Controller/Cloud Connectorのグループを指定するには、かっこを使用します。たとえば、4つのController（プライマリ2つとバックアップ2つ）がある場合、グループ化は次のようになります。

```
(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)
```

この例では、最初のグループのController（001と002）が最初に処理されます。両方が失敗した場合、2番目のグループのController（003と004）が処理されます。

XenDesktop 7.0以降の場合、**登録グループ**機能を使用するには、追加の手順を実行する必要があります。Studioから**Controllerの自動更新を有効にする**ポリシーを**禁止**する必要があります。

ListOfSIDs

VDA が登録のために連絡できる Controller のリストは `ListofDDCs` です。VDA はどの Controller を信頼すべきかも知っている必要があります。VDA は `ListofDDCs` 内の Controller を自動的に信頼しません。`ListofSIDs` (セキュリティ ID) は、信頼された Controller を識別します。VDA は信頼された Controller にのみ登録を試みます。

ほとんどの環境では、`ListofSIDs` は `ListofDDCs` から自動的に生成されます。CDFトレースを使用して `ListofSIDs` を読み取ることができます。

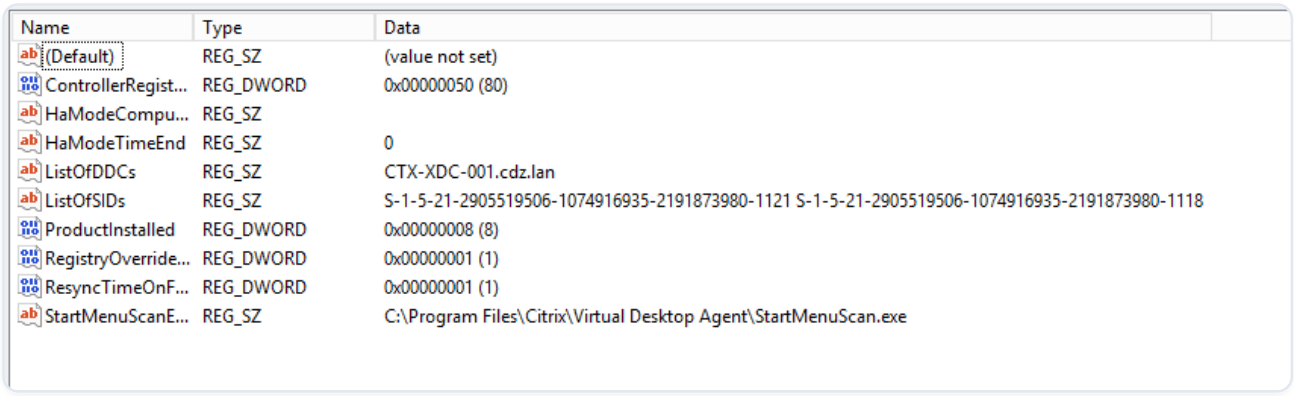
一般的に、`ListofSIDs` を手動で変更する必要はありません。いくつかの例外があります。最初の2つの例外は、新しいテクノロジーが利用可能になったため、もはや有効ではありません。

- **Controller の役割の分離:** XenApp および XenDesktop 7.7 でゾーンが導入される前は、Controller の一部のみが登録に使用される場合に、`ListofSIDs` が手動で構成されていました。たとえば、XDC-001 と XDC-002 を XML ブローカーとして使用し、XDC-003 と XDC-004 を VDA 登録に使用する場合、すべての Controller を `ListofSIDs` に、XDC-003 と XDC-004 を `ListofDDCs` に指定していました。これは一般的または推奨される構成ではありません。新しい環境では使用しないでください。代わりにゾーンを使用してください。
- **Active Directory の負荷軽減:** XenApp および XenDesktop 7.6 で自動更新機能が導入される前は、`ListofSIDs` を使用してドメインコントローラーの負荷を軽減していました。`ListofSIDs` を事前に入力することで、DNS 名から SID への解決をスキップできます。ただし、この永続キャッシュには SID が含まれているため、自動更新機能によりこの作業は不要になります。Citrix は自動更新機能を有効にしておくことを推奨します。
- **セキュリティ:** 一部の高度に保護された環境では、侵害された DNS サーバーからの潜在的なセキュリティ脅威を回避するために、信頼された Controller の SID が手動で構成されていました。ただし、これを行う場合は、自動更新機能も無効にする必要があります。そうしないと、永続キャッシュからの構成が使用されます。

したがって、特別な理由がない限り、`ListofSIDs` を変更しないでください。

`ListofSIDs` を変更する必要がある場合は、`HKLM\Software\Citrix\VirtualDesktopAgent` の下に `ListOfSIDs (REG_SZ)` という名前のレジストリキーを作成します。値は信頼された SID のリストで、複数ある場合はスペースで区切ります。

次の例では、1 つの Controller が VDA 登録に使用され (`ListofDDCs`)、2 つの Controller がブローカリングに使用されます (List OfSIDs)。



Name	Type	Data
(Default)	REG_SZ	(value not set)
ControllerRegist...	REG_DWORD	0x00000050 (80)
HaModeCompu...	REG_SZ	
HaModeTimeEnd	REG_SZ	0
ListOfDDCs	REG_SZ	CTX-XDC-001.cdz.lan
ListOfSIDs	REG_SZ	S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118
ProductInstalled	REG_DWORD	0x00000008 (8)
RegistryOverride...	REG_DWORD	0x00000001 (1)
ResyncTimeOnF...	REG_DWORD	0x00000001 (1)
StartMenuScanE...	REG_SZ	C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe

VDA 登録中の Controller 検索

VDA が登録を試行すると、Broker Agent はまずローカルドメインで DNS ルックアップを実行し、指定された Controller に到達できることを確認します。

最初のルックアップで Controller が見つからない場合、Broker Agent は AD でフォールバックのトップダウンクエリを開始できます。このクエリはすべてのドメインを検索し、頻繁に繰り返されます。Controller アドレスが無効な場合（たとえば、管理者が VDA のインストール時に誤った FQDN を入力した場合）、そのクエリのアクティビティがドメインコントローラーで分散型サービス拒否（DDoS）状態を引き起こす可能性があります。

次のレジストリキーは、Broker Agent が最初の検索中に Controller を見つけられない場合に、フォールバックのトップダウンクエリを使用するかどうかを制御します。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- 名前: `DisableDdcWildcardNameLookup`
- 種類: `DWORD`
- 値: `0` (デフォルト) または任意のゼロ以外の値

`0` に設定すると、フォールバック検索が有効になります。Controller の最初の検索が失敗した場合、フォールバックのトップダウン検索が開始されます。これはデフォルトの動作です。ただし、ゼロ以外の値に設定すると、フォールバック検索は無効になります。Controller の最初の検索が失敗した場合、Broker Agent は検索を停止します。

読み取り専用ドメインコントローラーを使用した VDA 登録中の LDAP バインディングシーケンス

VDAが読み取り専用ドメインコントローラー (RODC) に登録されると、ブローカーエージェントは無視するLight Directory Access Protocol (LDAP) バインディングを選択する必要があります。この選択を行うには、ブローカーエージェントに適切なレジストリキーが必要です。

レジストリキーが指定されていない場合、またはレジストリキーフィールドが空の場合、RODCへのVDA登録は、元のLDAPバインディングシーケンスを経由する必要があるため、時間がかかります。

LDAPバインディングシーケンスを変更するために、レジストリキー`ListofIgnoredBindings`が`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`に追加されました。`ListofIgnoredBindings`を使用すると、必要に応じてLDAPバインディングシーケンスを変更でき、RODCへのVDA登録を高速化できます。

- 名前: `ListofIgnoredBindings`
- 種類: `REG_SZ`
- 値: `DefaultPath`、`DomainPath`、`PDCPath`

値は、コンマで区切られたバインディングパスオプションのリストです。レジストリキーは、有効と認識しない値をすべて無視します。

VDA登録の問題のトラブルシューティング

前述のとおり、VDAは、仲介されたセッションを起動する際に考慮されるために、Delivery ControllerまたはCloud Connectorに登録されている必要があります。未登録のVDAは、利用可能なリソースの活用不足につながる可能性があります。VDAが登録されない理由はさまざまであり、その多くは管理者がトラブルシューティングできます。Studioは、カタログ作成ウィザードおよびデリバリーグループ作成後にトラブルシューティング情報を提供します。

- **マシンカタログ作成中の問題の特定:** カタログ作成ウィザードで、既存のマシンを追加した後、コンピューターアカウント名のリストは、各マシンがカタログに追加するのに適しているかどうかを示します。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

  メッセージで問題のあるマシンが特定された場合、そのマシンを削除する（**削除**ボタンを使用）か、マシンを追加することができます。たとえば、マシンに関する情報が取得されなかった（おそらく登録されたことがないため）ことを示すメッセージが表示された場合でも、そのマシンを追加することを選択できます。

  カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要になる場合があります。機能レベルを設定すると、そのバージョンで導入されたすべての機能（および機能レベルが変更されない場合はそれ以降の機能）がカタログ内のマシンで利用可能になります。ただし、そのカタログ内の以前のVDAバージョンのマシンは登録できません。

- **デリバリーグループ作成後の問題の特定:** デリバリーグループを作成した後、Studioはそのグループに関連付けられたマシンの詳細を表示します。

  デリバリーグループの詳細ペインには、登録されるべきだが登録されていないマシンの数が表示されます。つまり、1つ以上のマシンが電源オンでメンテナンスモードではないにもかかわらず、現在コントローラーに登録されていない可能性があります。「登録されていないが、登録されるべき」マシンを表示している場合、詳細ペインの**トラブルシューティング**タブで、考えられる原因と推奨される是正措置を確認してください。

VDA登録のトラブルシューティングに関する詳細情報

- 機能レベルの詳細については、VDAのバージョンと機能レベルを参照してください。
- VDA登録のトラブルシューティングの詳細については、CTX136668を参照してください。
- Citrix Scoutのヘルスチェックを使用して、VDA登録とセッション起動のトラブルシューティングを行うこともできます。詳細については、ヘルスチェックについてを参照してください。

仮想IPおよび仮想ループバック

> **重要:**
>
> - Windows 10 Enterprise multi-session はリモートデスクトップIP仮想化 (仮想IP) をサポートしておらず、Windows 10 Enterprise multi-session ではリモートデスクトップIP仮想化または仮想ループバックをサポートしていません。
> - リモートデスクトップIP仮想化 (仮想IP) は、クラウドホスト型マシンではサポートされていません。 詳細については、Microsoft ドキュメントを参照してください。

> リモートデスクトップIP仮想化および仮想ループバック機能は、Windows Server 2016、Windows Server 2019、および Windows Server 2022 マシンでサポートされています。これらの機能は、Windows デスクトップOSマシンには適用されません。

Microsoft リモートデスクトップIP仮想化アドレス機能は、公開されたアプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrix 仮想ループバック機能を使用すると、localhost (デフォルトでは 127.0.0.1) との通信に依存するアプリケーションを、localhost 範囲 (127.*) 内の一意の仮想ループバックアドレスを使用するように構成できます。

CRM やコンピュータテレフォニー統合 (CTI) などの特定のアプリケーションは、アドレス指定、ライセンス、識別、または一意のIPアドレスやループバックアドレスを必要とするその他の目的のためにIPアドレスを使用します。他のアプリケーションは静的ポートにバインドする可能性があり、その場合、マルチユーザー環境でアプリケーションの追加インスタンスを起動しようとすると、ポートが使用中であるため失敗します。このようなアプリケーションが Citrix Virtual Apps™ 環境で正しく機能するには、デバイスごとに一意のIPアドレスが必要です。

Remote Desktop IP Virtualization と仮想ループバックは、互いに独立した機能です。どちらか一方、または両方を使用できます。

管理者アクションの概要:

- Microsoft リモートデスクトップIP仮想化を使用するには、Windows サーバーで有効にして構成します。(Citrix® ポリシー設定は不要です。)
- Citrix 仮想ループバックを使用するには、Citrix ポリシーで2つの設定を構成します。

リモートデスクトップIP仮想化 (仮想IP)

リモートデスクトップIP仮想化が Windows サーバーで有効化および構成されている場合、セッションで実行されている構成済みの各アプリケーションは、一意のアドレスを持っているように見えます。ユーザーは、他の公開アプリケーションにアクセスするのと同じ方法で、Citrix Virtual Apps サーバー上のこれらのアプリケーションにアクセスします。プロセスがリモートデスクトップIP仮想化を必要とするのは、次のいずれかのケースです。

- プロセスがハードコードされたTCPポート番号を使用している場合
- プロセスが Windows ソケットを使用し、一意のIPアドレスまたは指定されたTCPポート番号を必要とする場合

アプリケーションが Remote Desktop IP Virtualization アドレスを使用する必要があるかどうかを判断するには：

1. Microsoft から **TCPView** ツールを入手します。このツールは、特定の IP アドレスとポートをバインドするすべてのアプリケーションを一覧表示します。TCPView の詳細については、Microsoft ドキュメント を参照してください。
2. **IP アドレスの解決**機能を無効にして、ホスト名ではなくアドレスが表示されるようにします。
3. アプリケーションを起動し、**TCPView** を使用して、アプリケーションが開いている IP アドレスとポート、およびこれらのポートを開いているプロセス名を確認します。
4. サーバーのIPアドレス、0.0.0.0、または127.0.0.1を開くプロセスを構成します。

5. アプリケーションが異なるポートで同じ IP アドレスを開かないようにするには、アプリケーションの別のインスタンスを起動します。

Microsoft Remote Desktop (RD) IP仮想化の仕組み

- 仮想IPアドレス指定は、Microsoftサーバーで有効にする必要があります。

  たとえば、Windows Server 2016 環境では、サーバーマネージャーから **Remote Desktop Services > RD Session Host Connections** を展開して、RD IP Virtualization 機能を有効にし、セッションごとまたはプログラムごとに動的ホスト構成プロトコル (DHCP) サーバーを使用して IP アドレスを動的に割り当てる設定を構成します。Remote Desktop IP Virtualization の構成の詳細については、Microsoft ドキュメント を参照してください。

- 機能を有効にすると、セッションの起動時に、サーバーはDHCPサーバーから動的に割り当てられたIPアドレスを要求します。
- The **RD IP Virtualization**機能は、リモートデスクトップ接続にセッションごとまたはプログラムごとにIPアドレスを割り当てます。複数のプログラムにIPアドレスを割り当てる場合、それらはセッションごとのIPアドレスを共有します。
- アドレスがセッションに割り当てられた後、次の呼び出しが行われるたびに、セッションはシステムのプライマリIPアドレスではなく仮想アドレスを使用します:
  `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`。

リモートデスクトップセッションホスティング構成内でMicrosoft IP仮想化機能を使用する場合、アプリケーションとWinsock関数呼び出しの間に「フィルター」コンポーネントを挿入することで、アプリケーションは特定のIPアドレスにバインドされます。これにより、アプリケーションは使用すべき正しいIPアドレスのみを認識します。アプリケーションがTCPまたはUDP通信をリッスンしようとすると、自動的に割り当てられた仮想IPアドレス（またはループバックアドレス）にバインドされます。アプリケーションによって開かれた発信接続はすべて、アプリケーションにバインドされたIPアドレスから発信されます。

アドレスを返す関数（Windowsポリシーが制御する`GetAddrInfo()`など）で、ローカルホストIPアドレスが要求された場合、リモートデスクトップIP仮想化は返されたIPアドレスを調べ、それをセッションのリモートデスクトップIP仮想化アドレスに変更します。このような名前関数を介してローカルサーバーのIPアドレスを取得しようとするアプリケーションは、そのセッションに割り当てられた一意のリモートデスクトップIP仮想化アドレスのみを認識します。このIPアドレスは、bindやconnectなどの後続のソケット呼び出しでよく使用されます。Windowsポリシーの詳細については、RDS IP Virtualization in Windows Serverを参照してください。

多くの場合、アプリケーションはアドレス0.0.0.0でリッスンするためにポートへのバインドを要求します。アプリケーションがこれを行い、静的ポートを使用する場合、アプリケーションの複数のインスタンスを起動することはできません。リモートデスクトップIP仮想化アドレス機能は、これらの呼び出しタイプで0.0.0.0も検索します。これにより、呼び出しが特定のリモートデスクトップIP仮想化アドレスでリッスンするように変更され、複数のアプリケーションが同じコンピューター上の同じポートでリッスンできるようになります。これは、それらすべてが異なるアドレスでリッスンしているためです。呼び出しは、ICAセッション内であり、リモートデスクトップIP仮想化アドレス機能が有効になっている場合にのみ変更されます。たとえば、異なるセッションで実行されているアプリケーションの2つのインスタンスが、両方ともすべてのインターフェイス（0.0.0.0）と特定のポート（9000など）にバインドしようとすると、VIPAddress1:9000とVIPAddress2:9000にバインドされ、競合は発生しません。

仮想ループバック

Citrix Remote Desktop IP Virtualization loopback policy設定を有効にすると、各セッションが通信用に独自のループバックアドレスを持つことができます。アプリケーションがWinsock呼び出しでlocalhostアドレス（デフォルト = 127.0.0.1）を使用する場合、仮想ループバック機能は127.0.0.1を127.X.X.Xに置き換えます。ここで、X.X.Xはセッション ID + 1を表します。たとえば、セッションIDが7の場合、アドレスは127.0.0.8になります。セッションIDが4番目のオクテット（255を超える）を超えるというまれなケースでは、アドレスは次のオクテット（127.0.1.0）にロールオーバーし、最大127.255.255.255までとなります。

プロセスが仮想ループバックを必要とするのは、次のいずれかのケースです。

- プロセスがWindowsソケットループバック（localhost）アドレス（127.0.0.1）を使用している場合
- プロセスがハードコードされたTCPポート番号を使用している場合

プロセス間通信にループバックアドレスを使用するアプリケーションには、仮想ループバックポリシー設定を使用します。追加の構成は不要です。仮想ループバックは仮想IPに依存しないため、Microsoftサーバーを構成する必要はありません。

- 仮想IPループバックサポート。有効にすると、このポリシー設定により、各セッションが独自の仮想ループバックアドレスを持つことができます。この設定はデフォルトで無効になっています。この機能は、仮想IP仮想ループバックプログラムリストポリシー設定で指定されたアプリケーションにのみ適用されます。
- 仮想IP仮想ループバックプログラムリスト。このポリシー設定は、仮想IPループバック機能を使用するアプリケーションを指定します。この設定は、仮想IPループバックサポートポリシー設定が有効になっている場合にのみ適用されます。

関連機能

仮想IPよりも仮想ループバックが優先されるように、以下のレジストリ設定を使用できます。この機能は「優先ループバック」と呼ばれます。ただし、注意して進めてください。

- 優先ループバックは、仮想IPと仮想ループバックの両方が有効になっている場合にのみ使用してください。そうしないと、意図しない結果が生じる可能性があります。
- レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

アプリケーションが常駐するサーバーでregeditを実行します。

- HKEY_LOCAL_MACHINE\\SOFTWARE\\Wow6432Node\\Citrix\\VIP
- 名前: PreferLoopback, 種類: REG_DWORD, データ: 1
- 名前: PreferLoopbackProcesses, 種類: REG_MULTI_SZ, データ: \<list of processes\>

ゾーン

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> WANで接続された広範囲に分散した場所にまたがる展開では、ネットワークの遅延と信頼性の問題に直面する可能性があります。これらの課題を軽減する2つのオプションがあります。

- 複数のサイトを展開し、それぞれに独自のSQL Serverサイトデータベースを持たせる。

  このオプションは、大規模なエンタープライズ展開に推奨されます。複数のサイトは個別に管理され、それぞれに独自のSQL Serverサイトデータベースが必要です。各サイトは独立したCitrix Virtual Apps™展開です。
- 単一サイト内に複数のゾーンを構成する。

ゾーンを構成することで、遠隔地のユーザーがWANの大部分を通過するように接続を強制することなく、リソースに接続できるようになります。ゾーンを使用すると、単一のWeb Studioコンソール、Citrix Director、およびサイトデータベースから効果的なサイト管理が可能になります。これにより、遠隔地に個別のデータベースを含むより多くのサイトを展開、人員配置、ライセンス供与、および運用するコストを節約できます。

ゾーンは、あらゆる規模の展開で役立ちます。ゾーンを使用すると、アプリケーションとデスクトップをエンドユーザーに近づけることができ、パフォーマンスが向上します。ゾーンには、冗長性と回復性のために1つ以上のControllerをローカルにインストールできますが、必須ではありません。

サイトに構成されているControllerの数は、サイト自体に新しいControllerを追加するなどの一部の操作のパフォーマンスに影響を与える可能性があります。これを避けるため、Citrix Virtual AppsまたはCitrix Virtual Desktops™サイトのゾーン数を50以下に制限することをお勧めします。

ゾーンのネットワーク遅延が250ミリ秒RTTを超える場合は、ゾーンではなく複数のサイトを展開することをお勧めします。

この記事全体を通して、「ローカル」という用語は、議論されているゾーンを指します。たとえば、「VDAがローカルControllerに登録する」とは、VDAがVDAが配置されているゾーン内のControllerに登録することを意味します。

このリリースでのゾーンは、XenAppバージョン6.5以前のゾーンと似ていますが、同一ではありません。たとえば、このゾーンの実装では、データコレクターはありません。サイト内のすべてのControllerは、プライマリゾーンの1つのサイトデータベースと通信します。また、このリリースではフェイルオーバーゾーンと優先ゾーンの動作が異なります。

ゾーンの種類

サイトには常に1つのプライマリゾーンがあります。オプションで1つ以上のサテライトゾーンを持つこともできます。サテライトゾーンは、災害復旧、地理的に離れたデータセンター、支店、クラウド、またはクラウド内のアベイラビリティゾーンに使用できます。

プライマリゾーン:

プライマリゾーンのデフォルト名は「Primary」です。このゾーンには、SQL Serverサイトデータベース（および使用されている場合は高可用性SQLサーバー）、Web Studio、Director、Citrix StoreFront™、Citrix License Server、Citrix Gatewayが含まれます。サイトデータベースは常にプライマリゾーンに保持してください。

プライマリゾーンには、冗長性のために少なくとも2つのControllerが必要です。プライマリゾーンには、データベースおよびインフラストラクチャと密接に連携するアプリケーションを持つVDAを含めることができます。

サテライトゾーン:

サテライトゾーンには、1つ以上のVDA、Controller、StoreFrontサーバー、およびCitrix Gatewayサーバーが含まれます。通常の運用では、サテライトゾーンのControllerはプライマリゾーンのデータベースと直接通信します。

サテライトゾーン、特に大規模なゾーンには、そのゾーンのマシンをプロビジョニングおよび保存するために使用されるハイパーバイザーが含まれる場合もあります。サテライトゾーンを構成する際、ハイパーバイザーまたはその他のサービス接続を関連付けることができます。（その接続を使用するカタログがすべて同じゾーンにあることを確認してください。）

サイトには、独自のニーズと環境に基づいて、さまざまな構成のサテライトゾーンを含めることができます。次の図は、プライマリゾーンとサテライトゾーンの例を示しています。

プライマリゾーンとサテライトゾーンの図(/en-us/citrix-virtual-apps-desktops/2311/media/zones1.png)

図では次のようになっています。

- **プライマリゾーン:** 2つのController、Web Studio、Director、StoreFront、License Server、およびサイトデータベース（高可用性SQL Server展開を含む）が含まれます。プライマリゾーンには、複数のVDAとCitrix Gatewayも含まれます。
- **サテライトゾーン1: Controllerを持つVDA:** サテライトゾーン1には、Controller、VDA、およびStoreFrontサーバーが含まれます。このサテライトゾーンのVDAは、ローカルのControllerに登録されます。ローカルのControllerは、プライマリゾーンのサイトデータベースおよびライセンスサーバーと通信します。

  WANに障害が発生した場合、ローカルホストキャッシュ機能により、サテライトゾーンのControllerは、そのゾーンのVDAへの接続の仲介を継続できます。このような展開は、従業員がローカルのStoreFrontサイトとローカルのControllerを使用してローカルリソースにアクセスするオフィスで効果的です。
- **サテライトゾーン2: 冗長Controllerを持つVDA:** サテライトゾーン2には、2つのController、VDA、およびStoreFrontサーバーが含まれます。これは最も回復力の高いゾーンタイプであり、WANとローカルControllerのいずれか一方の同時障害に対する保護を提供します。

VDAの登録場所とControllerのフェイルオーバー場所

プライマリゾーンとサテライトゾーンを含むサイトで、VDAが最小バージョン7.7の場合：

- Primary zoneのVDAは、Primary zoneのControllerに登録します。Primary zoneのVDAは、Satellite zoneのControllerに登録しようとすることはありません。
- Satellite zoneのVDAは、可能であればローカルのControllerに登録します。(これは優先Controllerと見なされます。) ローカルのControllerが利用できない場合 (たとえば、これ以上VDA登録を受け入れられない、または障害が発生した場合など)、VDAはPrimary zoneのControllerに登録しようとします。この場合、Satellite zoneのControllerが再び利用可能になったとしても、VDAはPrimary zoneに登録されたままになります。Satellite zoneのVDAは、別のSatellite zoneのControllerに登録しようとすることはありません。
- ControllerのVDA検出で自動更新が有効になっており、VDAのインストール中にControllerアドレスのリストを指定した場合、最初の登録のためにそのリストからControllerがランダムに選択されます (Controllerがどのゾーンにあるかに関係なく)。そのVDAがインストールされているマシンが再起動されると、VDAはローカルゾーンのControllerへの登録を優先するようになります。
- Satellite zoneのControllerで障害が発生した場合、可能であれば別のローカルControllerにフェールオーバーします。ローカルControllerが利用できない場合は、Primary zoneのControllerにフェールオーバーします。
- Controllerをゾーンの内外に移動し、自動更新が有効になっている場合、両方のゾーンのVDAは、どのControllerがローカルで、どのControllerがPrimary zoneにあるかを示す更新されたリストを受け取ります。これにより、VDAはどのControllerに登録し、どのControllerから接続を受け入れることができるかを知ることができます。
- カタログを別のゾーンに移動すると、そのカタログ内のVDAは、カタログを移動したゾーンのControllerに再登録します。(カタログを別のゾーンに移動するときは、このゾーンと関連するホスト接続があるゾーンが適切に接続されていることを確認してください。帯域幅が制限されている場合や、待ち時間が長い場合は、ホスト接続を関連するマシンカタログを含む同じゾーンに移動してください。)

Primary zoneのすべてのControllerで障害が発生した場合：

- Web Studioはサイトに接続できません。
- Primary zoneのVDAへの接続はできません。
- Primary zoneのControllerが利用可能になるまで、サイトのパフォーマンスが低下します。

VDAバージョン7.7より前のバージョンを含むサイトの場合：

- Satellite zoneのVDAは、ローカルゾーンおよびPrimary zoneのControllerからの要求を受け入れます。(最小バージョン7.7のVDAは、他のSatellite zoneのControllerからの要求を受け入れることができます。)
- Satellite zoneのVDAは、Primary zoneまたはローカルゾーンのControllerにランダムに登録します。(最小バージョン7.7のVDAはローカルゾーンを優先します。)

ゾーンの優先順位

ゾーンの優先順位機能を使用するには、StoreFront 3.7およびCitrix Gateway 11.0-65.x以降を使用している必要があります。

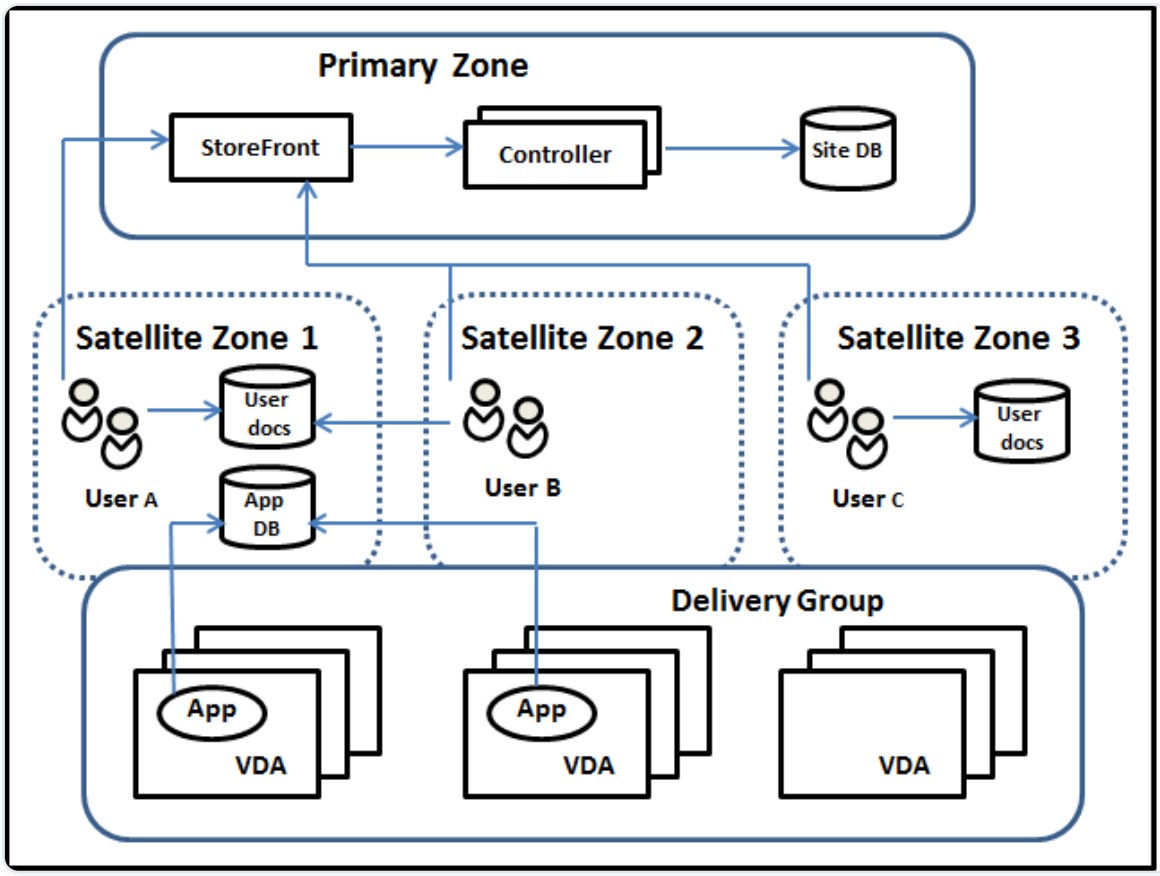
マルチゾーンサイトでは、ゾーン優先機能により、管理者はアプリケーションまたはデスクトップの起動に使用するVDAをより柔軟に制御できます。

ゾーンの優先順位の仕組み

ゾーン優先には3つの形式があります。特定のゾーンのVDAを使用することを好む場合があります。その判断基準は次のとおりです。

- アプリケーションのデータが保存されている場所。これはアプリケーションホームと呼ばれます。
- ユーザーのホームデータ（プロファイルやホーム共有など）の場所。これはユーザーホームと呼ばれます。
- ユーザーの現在の場所（Citrix Workspace™アプリが実行されている場所）。これはユーザーロケーションと呼ばれます。

次の図は、マルチゾーン構成の例を示しています。



この例では、VDAは3つのサテライトゾーンに分散されていますが、すべて同じデリバリーグループに属しています。したがって、ブローカーはユーザーの起動要求に対してどのVDAを使用するかを選択する可能性があります。この例は、ユーザーがCitrix Workspaceアプリのエンドポイントを実行できる場所がいくつかあることを示しています。

- ユーザーAは、サテライトゾーン1でCitrix Workspaceアプリがインストールされたデバイスを使用しています。
- ユーザーBは、サテライトゾーン2でデバイスを使用しています。
- ユーザーのドキュメントはさまざまな場所に保存できます。
  - ユーザーAとBは、サテライトゾーン1にある共有を使用します。
  - ユーザーCは、サテライトゾーンCの共有を使用します。
  - 公開されているアプリケーションの1つは、サテライトゾーン1にあるデータベースを使用します。

ユーザーまたはアプリケーションのホームゾーンを構成することで、ユーザーまたはアプリケーションをゾーンに関連付けます。その後、Delivery Controller™内のブローカーは、これらの関連付けを使用して、リソースが利用可能な場合にセッションが起動されるゾーンの選択を支援します。次のことができます。

- ユーザーをゾーンに追加して、ユーザーのホームゾーンを構成する。

- アプリケーションのプロパティを編集して、アプリケーションのホームゾーンを構成する。

ユーザーまたはアプリケーションは、一度に1つのホームゾーンしか持つことができません。（ユーザーグループのメンバーシップにより複数のゾーンメンバーシップが発生する場合、ユーザーに例外が発生することがあります。「その他の考慮事項」セクションを参照してください。ただし、この場合でも、ブローカーは1つのホームゾーンのみを使用します。）

ユーザーおよびアプリケーションのゾーン設定を構成できますが、ブローカーは起動に対して1つの優先ゾーンのみを選択します。優先ゾーンを選択するためのデフォルトの優先順位は、アプリケーションホーム \> ユーザーホーム \> ユーザーロケーションです。この順序を制限できます。詳細については、「ゾーン設定の調整」を参照してください。ユーザーがアプリケーションを起動すると、次のようになります。

- そのアプリケーションに構成済みのゾーン関連付け（アプリケーションホーム）がある場合、優先ゾーンはそのアプリケーションのホームゾーンになります。
- アプリケーションに構成済みのゾーン関連付けがないが、ユーザーに構成済みのゾーン関連付け（ユーザーホーム）がある場合、優先ゾーンはそのユーザーのホームゾーンになります。
- アプリケーションにもユーザーにも構成済みのゾーン関連付けがない場合、優先ゾーンはユーザーがCitrix Workspaceアプリインスタンスを実行しているゾーン（ユーザーロケーション）になります。そのゾーンが定義されていない場合、ランダムなVDAとゾーンの選択が使用されます。優先ゾーン内のすべてのVDAに負荷分散が適用されます。優先ゾーンがない場合、Delivery Group内のすべてのVDAに負荷分散が適用されます。

ゾーンの優先順位の調整

ユーザーまたはアプリケーションのホームゾーンを構成（または削除）する際に、ゾーン設定の使用方法をさらに制限することもできます。

- **ユーザーホームゾーンの強制使用:** Delivery Groupでは、ユーザーのホームゾーンに利用可能なリソースがない場合でも、セッションがユーザーのホームゾーン（構成されている場合）で起動され、他のゾーンへのフェイルオーバーが行われないように指定できます。この制限は、ゾーン間で大きなプロファイルやデータファイルをコピーするリスクを回避する必要がある場合に役立ちます。つまり、異なるゾーンでセッションを起動するよりも、セッションの起動を拒否する方が望ましいということです。
- **アプリケーションホームゾーンの強制使用:** 同様に、アプリケーションのホームゾーンを構成する際に、アプリケーションがそのゾーンでのみ起動され、アプリケーションのホームゾーンにリソースがない場合に他のゾーンへのフェイルオーバーが行われないように指定できます。
- **アプリケーションホームゾーンなし、および構成済みユーザーホームゾーンを無視:** アプリケーションのホームゾーンを指定しない場合、そのアプリケーションを起動する際に、構成済

みのユーザーゾーンを考慮しないように指定することもできます。たとえば、一部のユーザーが異なるホームゾーンを持っている場合でも、ユーザーロケーションゾーン設定を使用して、ユーザーがデバイスの近くのVDAでアプリケーションを実行することを好む場合があります。

優先ゾーンがセッションの使用に与える影響

ユーザーがアプリケーションまたはデスクトップを起動すると、ブローカーは既存のセッションを使用するよりも優先ゾーンを使用することを優先します。

アプリケーションまたはデスクトップを起動するユーザーが、起動されるリソースに適したセッションをすでに持っている場合（たとえば、アプリケーションのセッション共有を使用できるセッション、または起動されるリソースがすでに実行されているセッション）、そのセッションがユーザー/アプリケーションの優先ゾーン以外のゾーンにあるVDAで実行されている場合、システムは新しいセッションを作成する可能性があります。これにより、そのユーザーのセッション要件にとって優先度の低いゾーンのセッションに再接続するよりも、正しいゾーンでの起動（利用可能な容量がある場合）が満たされます。

到達できなくなった孤立セッションを防ぐため、既存の切断されたセッションへの再接続は、たとえそれが非優先ゾーンにある場合でも許可されます。

起動を満たすためのセッションの望ましさの順序は次のとおりです。

1. 優先ゾーン内の既存のセッションに再接続します。
2. 優先ゾーン以外のゾーンにある既存の切断されたセッションに再接続します。
3. 優先ゾーンで新しいセッションを開始します。
4. 優先ゾーン以外のゾーンにある接続済みの既存セッションに再接続します。
5. 優先ゾーン以外のゾーンで新しいセッションを開始します。

その他のゾーン優先度に関する考慮事項

- ユーザーグループ（セキュリティグループなど）にホームゾーンを構成すると、そのグループのユーザー（直接的または間接的なメンバーシップを通じて）は指定されたゾーンに関連付けられます。ただし、ユーザーは複数のセキュリティグループのメンバーになることができ、そのため、他のグループメンバーシップを通じて異なるホームゾーンが構成されている場合があります。このような場合、そのユーザーのホームゾーンの決定は曖昧になる可能性があります。

ユーザーがグループメンバーシップを通じて取得されていない構成済みのホームゾーンを持っている場合、そのゾーンがゾーン優先度に使用されます。グループメンバーシップを通じて取得されたゾーン関連付けはすべて無視されます。

ユーザーがグループメンバーシップのみを通じて取得した複数の異なるゾーン関連付けを持っている場合、ブローカーはゾーンの中からランダムに選択します。ブローカーがこの選択を行うと、そのゾーンは、ユーザーのグループメンバーシップが変更されるまで、以降のセッション起動に使用されます。

- ユーザーロケーションゾーンの優先度では、エンドポイントデバイス上のCitrix Workspaceアプリが、そのデバイスが接続しているCitrix Gatewayによって検出される必要があります。Citrix Gatewayは、IPアドレスの範囲を特定のゾーンに関連付けるように構成する必要があり、検出されたゾーンIDはStoreFrontを介してControllerに渡される必要があります。

ゾーン優先度について詳しくは、「ゾーン優先度の内部」を参照してください。

考慮事項、要件、およびベストプラクティス

- ゾーンには、次の項目を配置できます。コントローラー、マシンカタログ、ホスト接続、ユーザー、およびアプリケーション。カタログがホスト接続を使用する場合、カタログと接続が同じゾーンにあることを確認してください。（ただし、低遅延で高帯域幅の接続が利用可能な場合は、異なるゾーンに配置できます。）
- サテライトゾーンにアイテムを配置すると、サイトがそれらやそれらに関連する他のオブジェクトとどのようにやり取りするかに影響します。
    - コントローラーがサテライトゾーンに配置されると、それらのマシンは同じゾーン内のハイパーバイザーおよびVDAと良好な（ローカル）接続性を持つと想定されます。そのサテライトゾーン内のコントローラーは、それらのハイパーバイザーおよびVDAマシンの処理において、プライマリゾーン内のコントローラーよりも優先的に使用されます。
    - ハイパーバイザー接続がサテライトゾーンに配置されると、そのハイパーバイザー接続を介して管理されるすべてのハイパーバイザーもそのサテライトゾーンに存在すると想定されます。そのサテライトゾーン内のコントローラーは、そのハイパーバイザー接続との通信において、プライマリゾーン内のコントローラーよりも優先的に使用されます。
    - マシンカタログがサテライトゾーンに配置されると、そのカタログ内のすべてのVDAマシンがサテライトゾーンにあると想定されます。各VDAの初回登録後にコントローラーリストの自動更新メカニズムがアクティブになった後、サイトへの登録を試みる際には、プライマリゾーン内のコントローラーよりもローカルコントローラーが優先的に使用されます。
    - Citrix Gateway インスタンスもゾーンに関連付けることができます。これは、ここで説明されている他の要素のようにサイト構成の一部としてではなく、StoreFront Optimal HDX™ Routing 構成の一部として行われます。Citrix Gateway がゾーンに関連付けられて

いる場合、そのゾーン内のVDAマシンへのHDX接続が使用される際に、優先的に使用されます。

- 本番サイトを作成し、最初のカタログとデリバリーグループを作成すると、すべての項目はプライマリゾーンに配置されます。この初期設定が完了するまでサテライトゾーンを作成することはできません。（空のサイトを作成した場合、プライマリゾーンには最初はコントローラーのみが含まれます。カタログとデリバリーグループを作成する前または後にサテライトゾーンを作成できます。）
- 1つ以上の項目を含む最初のサテライトゾーンを作成すると、サイト内の他のすべての項目はプライマリゾーンに残ります。
- プライマリゾーンはデフォルトで「Primary」という名前ですが、その名前は変更できます。Web Studio はどのゾーンがプライマリゾーンであるかを示しますが、プライマリゾーンには識別しやすい名前を使用することがベストプラクティスです。プライマリゾーンを再割り当て（つまり、別のゾーンをプライマリゾーンにする）できますが、常にサイトデータベースと高可用性サーバーが含まれている必要があります。
- サイトデータベースは常にプライマリゾーンに保持してください。
- ゾーンを作成した後、後で項目をあるゾーンから別のゾーンに移動できます。この柔軟性により、近接して動作するのが最適な項目を分離できる可能性があります。たとえば、カタログ内のマシンを作成する接続（ホスト）とは異なるゾーンにカタログを移動すると、パフォーマンスに影響を与える可能性があります。項目をゾーン間で移動する前に、予期せぬ影響を考慮してください。カタログとそれが使用するホスト接続は同じゾーンに、または良好に接続されたゾーン（たとえば、低遅延で高帯域幅のネットワークを介して）に保持してください。
- For optimal performance, install Web Studio and Director only in the primary zone. You can access Web Studio and Director from a satellite zone (for example, a satellite zone containing Controllers to use as failover if the primary zone becomes inaccessible) because they are web application.
- Ideally, Citrix Gateway in a satellite zone is used for user connections coming into that zone from other zones or external locations, although you can use it for connections within the zone.
- 注意：ゾーン優先機能を使用するには、最低でもStoreFront 3.7およびCitrix Gateway 11.0-65.xを使用している必要があります。

接続品質の制限

サテライトゾーンのコントローラーは、サイトデータベースと直接SQL対話を行います。これにより、サテライトゾーンとサイトデータベースを含むプライマリゾーン間のリンクの品質にいくつかの制限が課されます。具体的な制限は、サテライトゾーンに展開されているVDAの数と、それらのVDA上のユーザーセッションの数に比例します。したがって、VDAとセッションの数が少ないサ

テライトゾーンは、VDAとセッションの数が多いサテライトゾーンよりも、データベースへの接続品質が低い場合でも機能できます。

詳しくは、「待機時間とSQLブロッキングクエリの改善」を参照してください。

ブローカリングパフォーマンスに対する遅延の影響

ゾーンによってユーザーは遅延の大きいリンクを使用できますが、ローカルブローカーがある場合でも、追加の遅延はエンドユーザーエクスペリエンスに必然的に影響を与えます。ユーザーが行うほとんどの作業において、サテライトゾーンのコントローラーとサイトデータベース間のラウンドトリップによって引き起こされる遅延を経験します。

アプリケーションの起動では、セッションブローカリングプロセスがセッション起動要求を送信するのに適したVDAを特定する際に、余分な遅延が発生します。

ゾーンの作成と管理

フル管理者は、すべてのゾーン作成および管理タスクを実行できます。ただし、ゾーンの作成、編集、削除を許可するカスタムロールを作成することもできます。ゾーン間でアイテムを移動する場合、ゾーン関連の権限（ゾーン読み取り権限を除く）は必要ありませんが、移動するアイテムに対する編集権限が必要です。たとえば、カタログをあるゾーンから別のゾーンに移動するには、そのカタログに対する編集権限が必要です。詳しくは、「委任管理」を参照してください。

Citrix Provisioning™を使用する場合： Citrix Provisioningコンソールはゾーンを認識しないため、Web Studioを使用してサテライトゾーン用のカタログを作成することをお勧めします。Web Studioでカタログを作成し、正しいサテライトゾーンを指定します。その後、Citrix Provisioningコンソールを使用して、そのカタログ内のマシンをプロビジョニングします。（Citrix Provisioningウィザードを使用してカタログを作成した場合、カタログはプライマリゾーンに配置されます。後でWeb Studioを使用してサテライトゾーンに移動する必要があります。）

ゾーンを作成する

1. Web Studioにサインインします。
2. 左ペインで を選択します。
3. アクションバーで を選択します。
4. ゾーンの名前と説明（オプション）を入力します。名前はサイト内で一意である必要があります。
5. 新しいゾーンに配置するアイテムを選択します。選択可能なアイテムのリストをフィルター処理したり、検索したりできます。空のゾーンを作成することもできます。その場合は、どのアイテムも選択しないでください。

6. 「**保存**」をクリックします。

この方法の代わりに、Web Studioで1つ以上の項目を選択し、アクションバーで**ゾーンの作成**を選択できます。

ゾーン名または説明の変更

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択します。
3. 中央ペインでゾーンを選択し、アクションバーで**ゾーンの編集**を選択します。
4. ゾーン名、説明、またはその両方を変更します。プライマリゾーンの名前を変更する場合は、そのゾーンがプライマリゾーンとして簡単に識別できることを確認してください。
5. **保存**または**適用**をクリックします。

項目をあるゾーンから別のゾーンに移動する

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択します。
3. 中央ペインでゾーンを選択し、1つ以上の項目を選択します。
4. 項目を移動先のゾーンにドラッグするか、アクションバーで**項目の移動**を選択し、移動先のゾーンを指定します。

確認メッセージには、選択した項目が一覧表示され、それらすべてを移動してもよろしいか尋ねられます。

注意: カタログがハイパーバイザーまたはその他のサービスへのホスト接続を使用する場合、カタログと接続の両方を同じゾーンに配置してください。そうしないと、パフォーマンスに影響が出る可能性があります。一方を移動する場合は、もう一方も移動してください。

ゾーンを削除する

ゾーンは、削除する前に空である必要があります。プライマリゾーンは削除できません。

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択します。
3. 中央ペインでゾーンを選択します。
4. アクションバーから**ゾーンの削除**を選択します。ゾーンが空でない場合（項目が含まれている場合）、それらの項目を移動するゾーンを選択するよう求められます。
5. 削除を確認します。

ユーザーのホームゾーンを追加する

ユーザーのホームゾーンを構成することは、*ユーザーをゾーンに追加する*とも呼ばれます。

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択し、中央ペインでゾーンを選択します。
3. アクションバーで**ゾーンへのユーザーの追加**を選択します。
4. **ゾーンへのユーザーの追加**ダイアログボックスで、**追加**をクリックし、ゾーンに追加するユーザーとユーザーグループを選択します。すでにホームゾーンを持つユーザーを指定した場合、メッセージが表示され、2つの選択肢が提示されます。**はい** = ホームゾーンを持たない指定したユーザーのみを追加します。**いいえ** = ユーザー選択ダイアログに戻ります。
5. **OK**をクリックします。

ホームゾーンが構成されているユーザーの場合、セッションをそのホームゾーンからのみ起動するように要求できます。

1. デリバリーグループを作成または編集します。
2. 「**ユーザー**」ページで、「**セッションは、構成されている場合、ユーザーのホームゾーンで起動する必要があります**」チェックボックスをオンにします。

そのデリバリーグループのユーザーが起動するすべてのセッションは、そのユーザーのホームゾーン内のマシンから起動する必要があります。デリバリーグループ内のユーザーに構成済みのホームゾーンがない場合、この設定は無効です。

ユーザーのホームゾーンを削除する

この手順は、ゾーンからユーザーを削除することとも呼ばれます。

1. Web Studioにサインインします。
2. 左側のペインで「**ゾーン**」を選択し、中央のペインでゾーンを選択します。
3. アクションバーで「**ゾーンからユーザーを削除**」を選択します。
4. 「**ゾーンにユーザーを追加**」ダイアログボックスで、「**削除**」をクリックし、ゾーンから削除するユーザーとグループを選択します。この操作では、ユーザーはゾーンからのみ削除されます。それらのユーザーは、所属するデリバリーグループおよびアプリケーショングループに残ります。
5. プロンプトが表示されたら、削除を確認します。

アプリケーションのホームゾーンを管理する

アプリケーションのホームゾーンを構成することは、アプリケーションをゾーンに追加することとも呼ばれます。デフォルトでは、マルチゾーン環境では、アプリケーションにホームゾーンはありません。

アプリケーションのホームゾーンは、アプリケーションのプロパティで指定されます。アプリケーションをグループに追加するとき、または後でアプリケーションのプロパティを構成できます。

- デリバリーグループを作成する、アプリケーショングループを作成する、または既存のグループにアプリケーションを追加するときに、ウィザードの「**アプリケーション**」ページで「**プロパティ**」を選択します。
- アプリケーションの追加後にアプリケーションのプロパティを変更するには、左側のペインで「**アプリケーション**」を選択します。アプリケーションを選択し、アクションバーで「**アプリケーションプロパティの編集**」を選択します。

アプリケーションのプロパティ/設定の ページで、次の操作を行います。

- アプリケーションにホームゾーンを設定する場合：
  - **選択したゾーンを使用して決定する**ラジオボタンを選択し、ゾーンを選択します。
  - アプリケーションを、選択したゾーンからのみ（他のゾーンからは起動しないように）起動する場合は、ゾーン選択の下にあるチェックボックスをオンにします。
- アプリケーションにホームゾーンを設定しない場合：
  - **ホームゾーンを構成しない**ラジオボタンを選択します。
  - このアプリケーションを起動する際に、ブローカーが構成済みのユーザーゾーンを考慮しないようにする場合は、ラジオボタンの下にあるチェックボックスをオンにします。この場合、アプリケーションのホームゾーンもユーザーのホームゾーンも、このアプリケーションをどこで起動するかを決定するために使用されません。

ゾーンの指定を含むその他のアクション

少なくとも1つのサテライトゾーンを作成した後、ホスト接続を追加するか、カタログを作成する際にゾーンを指定できます。

通常、プライマリゾーンがデフォルトです。Machine Creation Services™を使用してカタログを作成する場合、ホスト接続用に構成されたゾーンが自動的に選択されます。

サイトにサテライトゾーンが含まれていない場合、プライマリゾーンが想定され、ゾーン選択ボックスは表示されません。

モニター

管理者およびヘルプデスク担当者は、さまざまな機能とツールを使用してCitrix Virtual Apps and Desktops™サイトを監視できます。これらのツールを使用すると、以下を監視できます:

- ユーザーセッションおよびセッションの使用状況
- ログオンパフォーマンス
- 接続とマシン（障害を含む）
- 負荷評価
- 履歴トレンド
- インフラストラクチャ

Citrix Director (シトリックス ディレクター)

Directorは、監視、トラブルシューティング、およびエンドユーザーのサポートタスクの実行に使用できるリアルタイムのWebツールです。

詳細については、Director の記事を参照してください。

構成ログ

構成ログを使用すると、管理者はサイトに対する管理上の変更を追跡できます。構成ログは、構成変更が行われた後の問題の診断とトラブルシューティング、変更管理と構成の追跡を支援し、管理アクティビティを報告するのに役立ちます。

Studioからログに記録された情報のレポートを表示および生成できます。また、Directorでトレンドビューを使用して、構成変更の通知を提供するログ項目を表示することもできます。この機能は、Studioにアクセスできない管理者にとって役立ちます。

トレンドビューは、一定期間にわたる構成変更の履歴データを提供するため、管理者は、サイトに対してどのような変更がいつ誰によって行われたかを評価し、問題の原因を特定できます。このビューは、構成情報を次の3つのカテゴリに分類します:

- 接続障害
- 失敗したシングルセッションマシン

- 失敗したマルチセッションマシン

構成ログの有効化と構成方法の詳細については、構成ログを参照してください。Directorの記事では、そのツールからログに記録された情報を表示する方法について説明しています。

イベントログ

Citrix Virtual Apps and Desktops内のサービスは、発生したイベントをログに記録します。イベントログは、操作の監視とトラブルシューティングに使用されます。

詳細については、イベントログを参照してください。個々の機能に関する記事にもイベント情報が含まれている場合があります。

構成ログ

構成ログは、サイト構成の変更と管理アクティビティをデータベースに記録する機能です。この機能はデフォルトで有効になっています。記録されたコンテンツを使用して、次のことができます。

- 構成変更が行われた後の問題を診断し、トラブルシューティングします。ログは追跡記録を提供します。
- 変更管理を支援し、構成を追跡します。
- 管理アクティビティを報告します。

Citrix Studioから、構成ログ設定の指定、構成ログの表示、HTMLおよびCSVレポートの生成を行います。構成ログの表示は、日付範囲と全文検索結果でフィルターできます。必須ログが有効になっている場合、ログに記録できない構成変更は行われません。適切な権限があれば、構成ログからエントリを削除できます。構成ログ機能を使用してログコンテンツを編集することはできません。

構成ログは、PowerShell SDKと構成ログサービスを使用します。構成ログサービスは、サイト内のすべてのControllerで実行されます。いずれかのControllerが失敗した場合、別のController上のサービスがログ要求を自動的に処理します。

デフォルトでは、構成ログ機能は有効になっており、サイトの作成時に作成されるデータベース（サイト構成データベース）を使用します。データベースの別の場所を指定できます。構成ログデータベースは、サイト構成データベースと同じ高可用性機能をサポートしています。

構成ログへのアクセスは、委任管理を通じて、「ログ設定の編集」および「構成ログの表示」の権限で制御されます。

構成ログは、作成時にローカライズされます。たとえば、英語で作成されたログは、閲覧者のロケールに関係なく、英語で読み取られます。

ログに記録される内容

Studio、Director、およびPowerShellスクリプトから開始された構成変更と管理アクティビティがログに記録されます。ログに記録される構成変更の例には、次のものとの連携（作成、編集、削除、割り当て）が含まれます。

- マシンカタログ
- デリバリーグループ（電源管理設定の変更を含む）
- 管理者ロールとスコープ
- ホストリソースと接続
- Studio を介した Citrix ポリシー

ログに記録される管理変更の例には、以下が含まれます。

- 仮想マシンまたはユーザーデスクトップの電源管理
- Studio または Director がユーザーにメッセージを送信する

次の操作はログに記録されません。

- プール管理による仮想マシンの電源投入などの自律的な操作。
- グループポリシー管理コンソール (GPMC) を介して実装されたポリシーアクション。これらのアクションのログを表示するには、Microsoft ツールを使用します。
- レジストリ、データベースへの直接アクセス、または Studio、Director、PowerShell 以外のソースを介して行われた変更。
- 展開が初期化されると、最初の構成ログサービスインスタンスが構成サービスに登録されたときに構成ログが利用可能になります。したがって、構成の初期段階はログに記録されません（たとえば、データベーススキーマが取得および適用されたとき、ハイパーバイザーが初期化されたときなど）。

構成ログの管理

デフォルトでは、構成ログはサイトを作成するときに作成されるデータベース（サイト構成データベースとも呼ばれます）を使用します。Citrix は、次の理由により、構成ログデータベース（および監視データベース）に別の場所を使用することをお勧めします。

- 構成ログデータベースのバックアップ戦略は、サイト構成データベースのバックアップ戦略とは異なる可能性があります。
- 構成ログ（および監視サービス）のために収集されるデータ量が多いと、サイト構成データベースで利用可能な領域に悪影響を及ぼす可能性があります。
- これにより、3つのデータベースの単一障害点が分割されます。

構成ログをサポートしない製品エディションには、Studioにログノードがありません。

構成ログと強制ログの有効化と無効化

デフォルトでは、構成ログは有効になっており、強制ログは無効になっています。

1. Web Studioにサインインし、左ペインで**ログ**を選択します。
2. アクションバーで**設定**を選択します。構成ログダイアログボックスには、データベース情報が含まれており、構成ログと強制ログが有効になっているか無効になっているかを示します。
3. 目的のアクションを選択します。

   構成ログを有効にするには、**有効にする**を選択します。これはデフォルト設定です。データベースに書き込みできない場合、ログ情報は破棄されますが、操作は続行されます。

   構成ログを無効にするには、**無効にする**を選択します。以前にログが有効になっていた場合、既存のログはPowerShell SDKで読み取り可能です。

   強制ログを有効にするには、**データベースが利用できない場合にサイト構成への変更を防止する**を選択します。通常ログに記録される構成変更または管理アクティビティは、構成ログデータベースに書き込みできない限り許可されません。強制ログは、構成ログが有効になっている場合（**有効にする**が選択されている場合）にのみ有効にできます。構成ログサービスが失敗し、高可用性が使用されていない場合、強制ログが想定されます。このような場合、通常ログに記録される操作は実行されません。

   強制ログを無効にするには、**データベースが利用できない場合にサイト構成への変更を許可する**を選択します。構成ログデータベースにアクセスできない場合でも、構成変更と管理アクティビティは許可されます。これはデフォルト設定です。

構成ログデータベースの場所を変更する

強制ログが有効になっている場合、データベースの場所を変更することはできません。場所の変更には、ログに記録できない短い切断間隔が含まれるためです。

1. サポートされているSQL Serverバージョンを使用して、データベースサーバーを作成します。
2. Web Studioにサインインし、左ペインで**ログ**を選択します。

3. アクションバーで**設定**を選択します。
4. 「ログ設定」ダイアログボックスで、「**ログデータベースの変更**」を選択します。
5. 「ログデータベースの変更」ダイアログボックスで、新しいデータベースサーバーを含むサーバーの場所を指定します。有効な形式については、「データベースアドレス形式」を参照してください。
6. Studioでデータベースを作成するには、「**OK**」をクリックします。プロンプトが表示されたら「**OK**」をクリックすると、データベースが自動的に作成されます。Studioは、現在のStudioユーザーの資格情報を使用してデータベースへのアクセスを試行します。失敗した場合は、データベースユーザーの資格情報の入力を求められます。その後、Studioはデータベーススキーマをデータベースにアップロードします。（資格情報はデータベース作成中のみ保持されます。）
7. データベースを手動で作成するには、「**データベーススクリプトの生成**」をクリックします。生成されたスクリプトには、データベースを手動で作成するための手順が含まれています。スキーマをアップロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

以前のデータベースの構成ログデータは、新しいデータベースにはインポートされません。ログを取得する際に、両方のデータベースからログを集約することはできません。新しい構成ログデータベースの最初のログエントリは、データベースの変更が発生したことを示しますが、以前のデータベースを特定するものではありません。

構成ログコンテンツの表示

構成変更や管理アクティビティを開始すると、StudioとDirectorによって作成された高レベル操作がStudioの上部中央ペインに一覧表示されます。高レベル操作は、1つ以上のサービスおよびSDK呼び出し（低レベル操作）をもたらします。上部ペインで高レベル操作を選択すると、下部ペインに低レベル操作が表示されます。

操作が完了する前に失敗した場合、ログ操作がデータベースで完了しない可能性があります。たとえば、開始レコードに対応する停止レコードがない場合があります。このような場合、ログには情報が欠落していることが示されます。時間範囲に基づいてログを表示すると、ログ内のデータが基準に一致する場合、不完全なログが表示されます。たとえば、過去5日間のすべてのログが要求され、過去5日間に開始時刻があるが終了時刻がないログが存在する場合、それは含まれます。

PowerShellコマンドレットを呼び出すスクリプトを使用する場合、親の高レベル操作を指定せずに低レベル操作を作成すると、構成ログはサロゲート高レベル操作を作成します。

構成ログコンテンツを表示するには、Studioナビゲーションペインで「**ログ**」を選択します。デフォルトでは、中央ペインにログコンテンツが日付ごとに区切られ、時系列順（最新のエントリが最初）に表示されます。次のことができます。

- 列ヘッダーで表示を並べ替えます。
- 日付間隔を指定するか、「**検索**」ボックスにテキストを入力して表示をフィルターします。検索を使用した後に標準表示に戻るには、「**検索**」ボックスのテキストをクリアします。

レポートを生成する

構成ログデータを含むCSVおよびHTMLレポートを生成できます。

- CSVレポートには、指定された時間間隔のすべてのログデータが含まれます。データベース内の階層データは、単一のCSVテーブルにフラット化されます。データのどの側面もファイル内で優先されません。書式設定は使用されず、人間が読み取れることは想定されていません。ファイル（MyReportという名前）には、普遍的に利用可能な形式でデータが含まれています。CSVファイルは、データのアーカイブや、Microsoft Excelなどのレポート作成ツールまたはデータ操作ツールのデータソースとしてよく使用されます。
- HTMLレポートは、指定された時間間隔のログデータを人間が判読できる形式で提供します。変更を確認するための構造化されたナビゲート可能なビューを提供します。HTMLレポートは、SummaryとDetailsという名前の2つのファイルで構成されます。Summaryには、各操作がいつ、誰によって行われたか、およびその結果といった高レベルの操作が一覧表示されます。各操作の横にある**詳細**リンクをクリックすると、Detailsファイル内の低レベルの操作に移動し、追加情報が提供されます。

構成ログレポートを生成するには、Studioナビゲーションペインで**Logging**を選択し、アクションバーで**Create custom report**を選択します。

- レポートの日付範囲を選択します。
- レポート形式（CSV、HTML、またはその両方）を選択します。
- レポートを保存する場所を参照します。

構成ログコンテンツを削除する

構成ログを削除するには、特定の委任管理権限とSQL Serverデータベース権限が必要です。

- **委任管理:** 展開構成の読み取りを許可する委任管理の役割が必要です。フル管理者役割にはこの権限があります。カスタム役割では、その他の権限カテゴリで「読み取り専用」または「管理」が選択されている必要があります。

構成ログデータを削除する前にバックアップを作成するには、カスタム役割でログ権限カテゴリの「読み取り専用」または「管理」も選択されている必要があります。

- **SQL Serverデータベース:** データベースからレコードを削除する権限を持つSQL Serverログインが必要です。これには2つの方法があります。
  - sysadminサーバー役割を持つSQL Serverデータベースログインを使用します。これにより、データベースサーバー上で任意の活動を実行できます。あるいは、`serveradmin` または `setupadmin` サーバー役割を使用すると、削除操作を実行できます。
  - 展開でより高いセキュリティが必要な場合は、データベースからレコードを削除する権限を持つデータベースユーザーにマッピングされた非sysadminデータベースログインを使用します。
    a. SQL Server Management Studioで、「sysadmin」以外のサーバー役割を持つSQL Serverログインを作成します。
    b. ログインをデータベース内のユーザーにマッピングします。SQL Serverは、ログインと同じ名前のユーザーをデータベース内に自動的に作成します。
    c. データベース役割のメンバーシップで、データベースユーザーの役割メンバーの少なくとも1つ（`ConfigurationLoggingSchema_ROLE` または `dbowner`）を指定します。

    詳細については、SQL Server Management Studioのドキュメントを参照してください。

構成ログを削除するには:

1. Web Studio にサインインし、左側のペインで を選択します。
2. アクションバーで を選択します。
3. ログを削除する前にバックアップを作成するかどうかを尋ねられます。バックアップを作成することを選択した場合は、バックアップアーカイブが保存される場所を参照します。バックアップはCSVファイルとして作成されます。

構成ログがクリアされた後、ログの削除は空のログに投稿される最初のアクティビティです。そのエントリには、誰がいつログを削除したかに関する詳細が記載されています。

API および PowerShell ログを表示する

現在のセッション中に作成されたAPIリクエストを監視するには、**API**タブをクリックします。APIログは、Web Studioからサインアウトするとクリアされます。

その日に行ったUIアクションに対応するPowerShellコマンドを表示するには、**PowerShell**タブをクリックします。

構成ログにメタデータを関連付ける

ログレコードに`MetadataMap`と呼ばれる`name-value`ペアを関連付けることで、構成ログにメタデータを添付できます。

> **注:**
>
> - メタデータは、高レベルの操作オブジェクトにのみ添付できます。
> - メタデータは、実行時に既存のレコードに関連付けられます。

メタデータを設定する

PowerShellコマンド`Set-LogHighLevelOperationMetadata`を実行して、ログレコードを`MetadataMap`に関連付けます。`Set-LogHighLevelOperationMetadata`は以下のパラメーターを受け取ります。

- **Id**: 高レベル操作のID。
- **InputObject**: メタデータを追加する高レベル操作。これは、高レベル操作オブジェクトまたはオブジェクトのリストがPowerShellコマンドに渡される`Id`パラメーターの代替です。
- **Name**: 追加するメタデータのプロパティ名。プロパティは、指定された高レベル操作に対して一意である必要があります。プロパティには、次の文字 ()\/;:#.*?=<>|'" を含めることはできません。
- **Value**: プロパティの値。
- **Map**: プロパティの(名前、値)ペアの辞書。これは、`-Name`および`-Value`パラメーターを使用してメタデータを設定する代替手段です。

例えば、Id 40 のすべての高レベルログレコードにメタデータを添付するには、次のPowerShellコマンドを実行します。

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata -Name A -Value B
```

ユーザー`abc@example.com`を持つ高レベルレコードにメタデータを添付するには、次のPowerShellコマンドを実行します。

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperationMetadata -Name C -Value D
```

メタデータを使用して取得する

関連付けられたメタデータを使用してログレコードを取得するには、次のPowerShellコマンドを実行します。

- キーと値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- 任意のキーの値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- キーと任意の値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

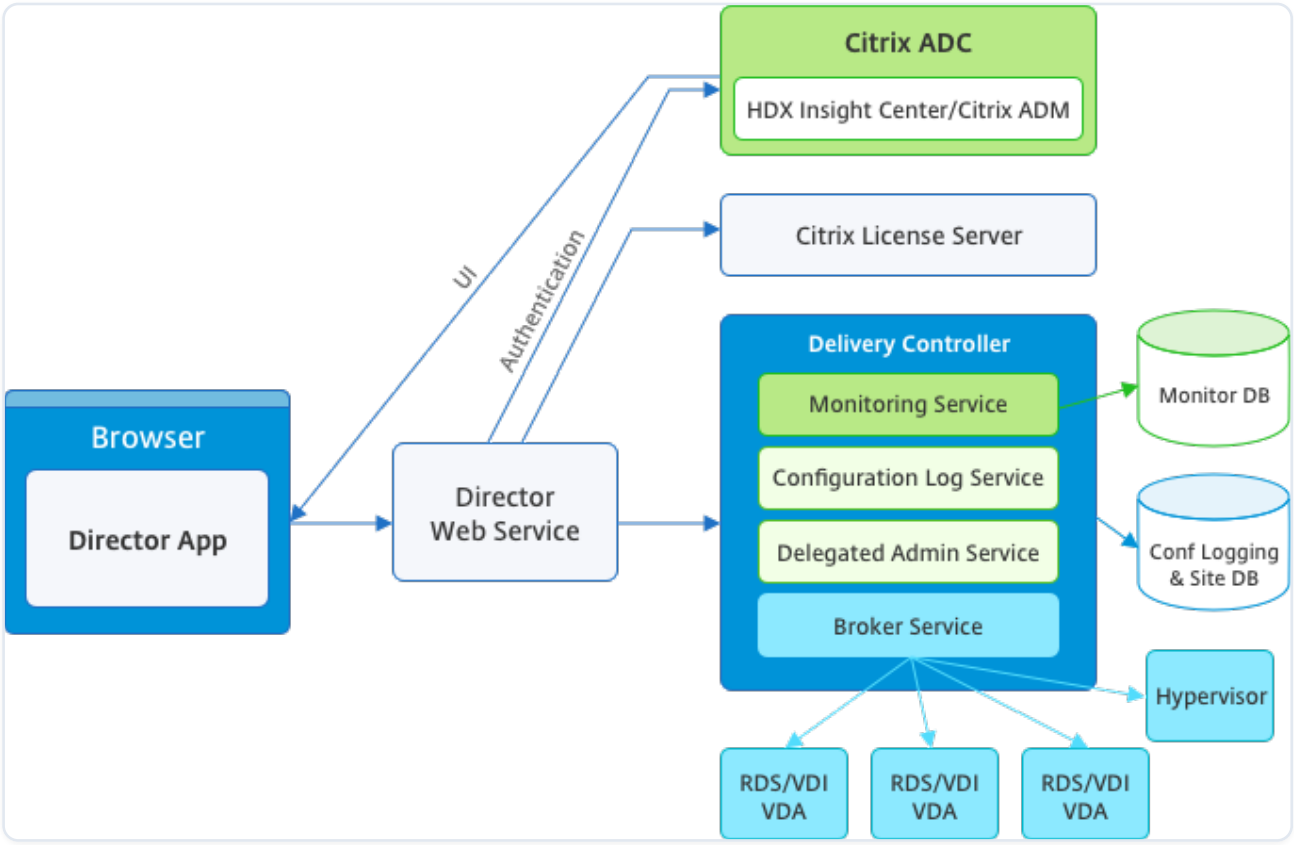
メタデータを削除する

関連付けられたメタデータを削除するには、PowerShellコマンド `Remove-LogHighLevelOperationMetadata` を実行します。 `Remove-LogHighLevelOperationMetadata` は次のパラメーターを受け取ります。

- **Id**: 高レベル操作のID。
- **InputObject**: メタデータを追加する高レベル操作。これは、高レベル操作オブジェクトまたはオブジェクトのリストがPowerShellコマンドに渡される `Id`` パラメーターの代替です。
- **Name**: 削除するメタデータのプロパティ名。指定されたオブジェクトのすべてのメタデータを削除するには、$nullに設定します。
- **Map**: プロパティの (名前、値) ペアの辞書。これは、ハッシュテーブル (@{"name1" = "val1"; "name2" = "val2"} で作成) または文字列辞書 (new-object "System.Collections.Generic.Dictionary" で作成) のいずれかです。マップ内のキーと名前が一致するプロパティは削除されます。

ディレクター

ディレクターは、Citrix Virtual Apps and Desktops 用の監視およびトラブルシューティングコンソールです。



Director は以下にアクセスできます。

- Analytics、Performance Manager、および Network Inspector と統合された統合コンソールを使用して、Broker Agent からのリアルタイムデータ。Citrix ADM は、Citrix Virtual Apps™ または Desktops 環境におけるネットワークに起因するボトルネックを特定するために、以下の分析機能を提供します。
  - 健全性と容量保証のためのパフォーマンス管理
  - 履歴傾向とネットワーク分析
- Configuration Logging データベースにアクセスするために、Monitor データベースに保存されている履歴データ。
- Citrix ADM を使用した Citrix Gateway からの ICA® データ。

- Citrix Virtual Apps または Desktops の仮想アプリケーション、デスクトップ、およびユーザーのエンドユーザーエクスペリエンスを可視化します。
- ネットワークデータをアプリケーションデータおよびリアルタイムメトリックと関連付け、効果的なトラブルシューティングを行います。
- Citrix Virtual Desktop 7 Director 監視ツールと統合します。

Director は、Citrix Virtual Apps または Desktops Site のリアルタイムおよび履歴の健全性監視を提供するトラブルシューティングダッシュボードを使用します。この機能により、障害をリアルタイムで確認でき、エンドユーザーがどのような状況にあるかをよりよく把握できます。

Director の機能と Delivery Controller (DC)、VDA、およびその他の依存コンポーネントとの互換性に関する詳細については、機能互換性マトリックスを参照してください。

注:

MeltdownおよびSpectreの投機的実行サイドチャネル脆弱性が開示されたことを受け、Citrixは関連する緩和パッチをインストールすることを推奨します。これらのパッチは、SQL Serverのパフォーマンスに影響を与える可能性があります。詳細については、Microsoftサポート記事「Protect SQL Server from attacks on Spectre and Meltdown side-channel vulnerabilities」を参照してください。Citrixは、実稼働環境にパッチを展開する前に、規模をテストし、ワークロードを計画することを推奨します。

Directorは、Delivery Controller上にWebサイトとしてデフォルトでインストールされます。前提条件およびその他の詳細については、このリリースのシステム要件ドキュメントを参照してください。Directorのインストールと構成に関する具体的な情報については、「Directorのインストールと構成」を参照してください。

Directorへのログオン

DirectorのWebサイトはhttpsまたは`http://<Server FQDN>/Director`です。

マルチサイト展開でいずれかのサイトがダウンしている場合、ダウンしているサイトへの接続を試みるため、ログオンに少し時間がかかります。

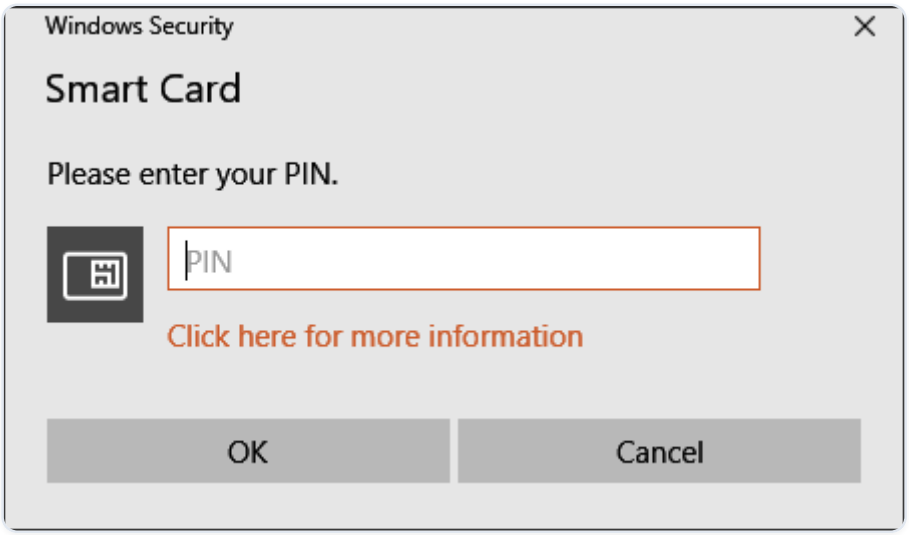
PIVスマートカード認証でDirectorを使用する

Directorは、個人識別検証（PIV）ベースのスマートカード認証によるログオンをサポートするようになりました。この機能は、アクセス制御にスマートカードベースの認証を使用する組織や政府機関にとって役立ちます。 スマートカード認証には、DirectorサーバーおよびActive Directoryでの特定の構成が必要です。構成手順は、「PIVスマートカード認証の構成」に詳しく記載されています。

> **注：**
>
> スマートカード認証は、同じActive Directoryドメインのユーザーのみがサポートされます。

必要な構成を実行した後、スマートカードを使用してDirectorにログオンできます。

1. スマートカードをスマートカードリーダーに挿入します。
2. ブラウザーを開き、DirectorのURLにアクセスします。`https://<directorfqdn>/Director`.
3. 表示されたリストから有効なユーザー証明書を選択します。
4. スマートカードトークンを入力します。



5. 認証後、Directorログオンページで追加の資格情報を入力することなくDirectorにアクセスできます。

統合 Windows 認証での Director の使用

統合Windows認証 (IWA) を使用すると、ドメインに参加しているユーザーは、Directorログオンページで資格情報を再入力することなく、Directorに直接アクセスできます。統合Windows認証とDirectorを使用するための前提条件は次のとおりです。

- DirectorをホストするIIS Webサイトで統合Windows認証を有効にします。Directorをインストールすると、匿名認証とフォーム認証が有効になります。統合Windows認証とDirectorをサポートするには、匿名認証を無効にし、Windows認証を有効にします。ドメイン外のユーザーの認証のために、フォーム認証は有効のままにしておく必要があります。

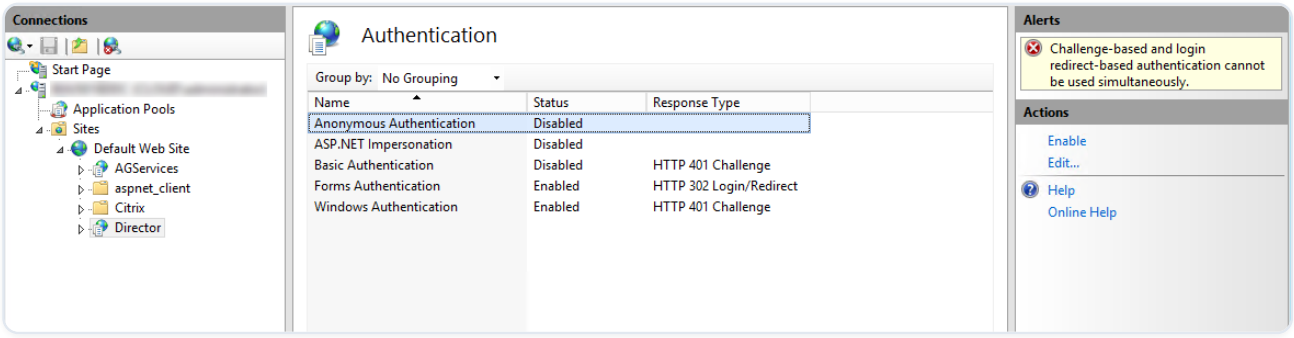
  a. IISマネージャーを起動します。

  b. **サイト** > **既定のWebサイト** > **Director** に移動します。

  c. **認証** を選択します。

  d. **匿名認証** を右クリックし、**無効** を選択します。

  e. **Windows認証** を右クリックし、**有効** を選択します。



- Directorマシンに対してActive Directoryの委任権限を構成します。構成が必要となるのは、DirectorとDelivery Controller™が別々のマシンにインストールされている場合のみです。

  a. Active Directoryマシンで、Active Directory管理コンソールを開きます。

  b. Active Directory管理コンソールで、**ドメイン名** \> **コンピューター**に移動します。Directorマシンを選択します。

  c. 右クリックして**プロパティ**を選択します。

  d. プロパティで、**委任**タブを選択します。

  e. **このコンピューターを、任意のサービスへの委任のために信頼する（Kerberosのみ）** オプションを選択します。

- Director へのアクセスに使用するブラウザーは、統合 Windows 認証をサポートしている必要があります。Firefox および Chrome では、追加の構成手順が必要になる場合があります。詳しくは、ブラウザーのドキュメントを参照してください。

- Monitoring Service は、Microsoft .NET Framework 4.5.1 以降、または Director のシステム要件に記載されているサポート対象バージョンを実行している必要があります。詳しくは、「システム要件」を参照してください。

ユーザーがDirectorからログオフするか、セッションがタイムアウトすると、ログオンページが表示されます。ログオンページから、ユーザーは認証の種類を**自動ログオン**または**ユーザー資格情報**に設定できます。

インターフェイスビュー

Directorは、特定の管理者向けに調整されたさまざまなインターフェイスビューを提供します。製品の権限によって、表示される内容と利用可能なコマンドが決まります。

たとえば、ヘルプデスク管理者は、ヘルプデスクタスクに合わせたインターフェイスを表示します。Director を使用すると、ヘルプデスク管理者は、問題を報告しているユーザーを検索し、そのユーザーに関連付けられているアクティビティを表示できます。たとえば、ユーザーのアプリケーションとプロセスのステータスなどです。応答しないアプリケーションやプロセスを終了する、ユーザーのマシンでシャドウ操作を実行する、マシンを再起動する、ユーザープロファイルをリセットするなどの操作を実行することで、問題を迅速に解決できます。

対照的に、完全な管理者はサイト全体を表示および管理し、複数のユーザーおよびマシンに対してコマンドを実行できます。ダッシュボードは、セッションのステータス、ユーザーログオン、サイトインフラストラクチャなど、展開の主要な側面を概観できます。情報は毎分更新されます。問題が発生した場合、発生した障害の数と種類に関する詳細が自動的に表示されます。

Director のさまざまな役割とその権限について詳しくは、「委任管理と Director」を参照してください。

Pendoによる使用状況データの収集

Directorのインストール後、DirectorサービスはPendoを使用して使用状況データの収集を開始します。トレンドページの利用状況に関する統計とOData API呼び出しの分析が収集されます。分析の収集は、Citrixプライバシーポリシーに準拠しています。Directorをインストールすると、データ収集はデフォルトで有効になります。

Pendo のデータ収集をオプトアウトするには、Director がインストールされているマシンのレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Director インスタンスを更新してください。

注意: レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix は、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。Citrix は、Windows レジストリを変更する前にバックアップすることをお勧めします。

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前：DisableGoogleAnalytics

> **注:**
>
> 以前、Director Service は Google Analytics を使用してデータを収集していました。現在、同じレジストリキーが Pendo に使用されています。

> 値：0 = 有効（デフォルト）、1 = 無効

Pendo によるデータ収集を無効にするには、以下の PowerShell コマンドレットを使用できます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

新機能ガイド

Director には、現在のバージョンの Director でリリースされた新機能に関する洞察を提供する Pendo を使用した製品内ガイドがあります。適切な製品内メッセージと組み合わせた簡単な概要により、製品の新機能を理解するのに役立ちます。

この機能をオプトアウトするには、Director がインストールされているマシンで、以下に説明するようにレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Director インスタンスを更新してください。

> **注意:**

> レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix は、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。Citrix は、変更する前に Windows レジストリをバックアップすることをお勧めします。

> 場所: HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前: DisableGuidedHelp

値: 0 = 有効（デフォルト）、1 = 無効

製品内ガイドを無効にするには、以下の PowerShell コマンドレットを使用できます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
-PropertyType DWORD -Value 1
```

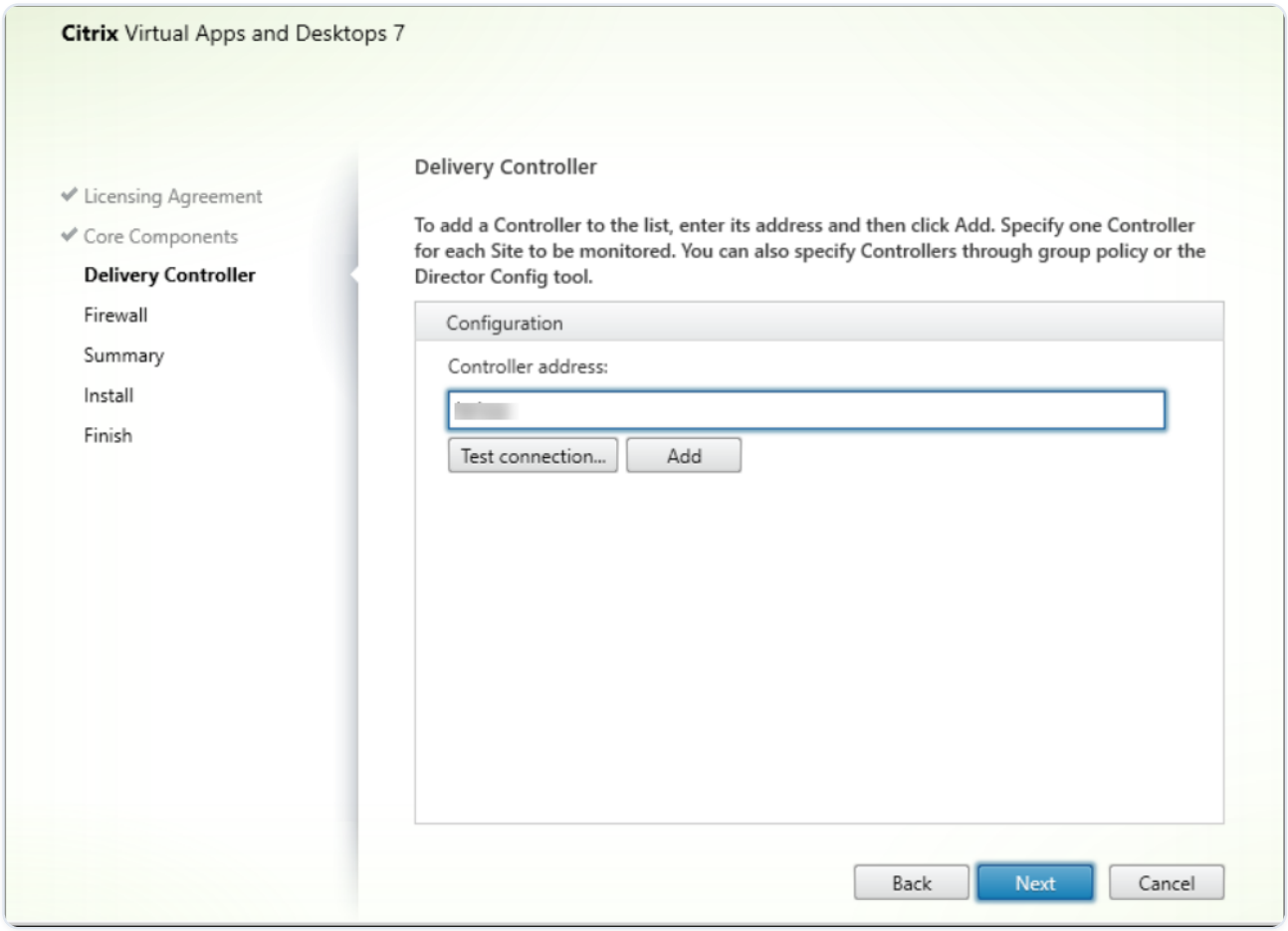
インストールと構成

Directorのインストール

Citrix Virtual Apps and Desktopsのフル製品ISOインストーラーを使用してDirectorをインストールします。これにより、前提条件の確認、不足しているコンポーネントのインストール、Director Webサイトのセットアップ、および基本的な構成が実行されます。前提条件およびその他の詳細については、このリリースのシステム要件ドキュメントを参照してください。このリリースのDirectorは、Virtual Apps 6.5以前の展開またはVirtual Desktops 7以前の展開とは互換性がありません。 ISOインストーラーによって提供されるデフォルト構成は、一般的な展開に対応します。インストール時にDirectorが含まれていなかった場合は、ISOインストーラーを使用してDirectorを追加します。追加のコンポーネントを追加するには、ISOインストーラーを再実行し、インストールするコンポーネントを選択します。ISOインストーラーの使用方法については、インストールドキュメントのコアコンポーネントのインストールを参照してください。Citrixでは、.MSIファイルではなく、フル製品ISOインストーラーのみを使用してインストールすることをお勧めします。

DirectorがControllerにインストールされている場合、サーバーアドレスとしてlocalhostが自動的に構成され、Directorはデフォルトでローカルのcontrollerと通信します。Controllerから離れた専用

サーバーにDirectorをインストールするには、ControllerのFQDNまたはIPアドレスを入力するよう求められます。



注:

「**追加**」をクリックして、監視するControllerを追加します。

Directorは、デフォルトで指定されたControllerと通信します。監視するサイトごとにControllerアドレスを1つだけ指定します。Directorは、同じサイト内の他のすべてのControllerを自動的に検出し、指定したControllerが失敗した場合、それらの他のControllerにフォールバックします。

注:

DirectorはController間で負荷分散を行いません。

> ブラウザーとWebサーバー間の通信を保護するために、Citrix®はDirectorをホストするIIS WebサイトでTLSを実装することを推奨します。手順については、Microsoft IISのドキュメントを参照してください。TLSを有効にするためにDirectorの構成は必要ありません。

Directorの展開と構成

Directorが複数のサイトを含む環境で使用される場合、Controller、Director、およびその他のコアコンポーネントがインストールされているすべてのサーバーでシステムクロックを同期してください。そうしないと、Directorでサイトが正しく表示されない可能性があります。

> **重要:**
>
> ネットワーク経由でプレーンテキストで送信されるユーザー名とパスワードのセキュリティを保護するため、Director接続はHTTPではなくHTTPSのみを使用するようにしてください。特定のツールは、HTTP（暗号化されていない）ネットワークパケット内のプレーンテキストのユーザー名とパスワードを読み取ることができ、ユーザーにとって潜在的なセキュリティリスクを生み出す可能性があります。

権限の構成

Directorにログオンするには、Directorの権限を持つ管理者はActive Directoryドメインユーザーであり、以下の権限を持っている必要があります。

- 検索対象となるすべてのActive Directoryフォレストにおける読み取り権限 ((/ja-jp/citrix-virtual-apps-desktops/2311/director/install-and-configure/advanced-configuration.html)を参照)。
- 構成された委任管理者ロール ((/ja-jp/citrix-virtual-apps-desktops/2311/director/install-and-configure/permissions.html)を参照)。
- ユーザーをシャドウするには、管理者はWindowsリモートアシスタンス用のMicrosoftグループポリシーを使用して構成されている必要があります。さらに:
  - VDAをインストールする際は、すべてのユーザーデバイスでWindowsリモートアシスタンス機能が有効になっていることを確認してください (デフォルトで選択されています)。
  - サーバーにDirectorをインストールする場合、Windowsリモートアシスタンスがインストールされていることを確認してください (デフォルトで選択されています)。ただし、サーバーではデフォルトで無効になっています。Directorがエンドユーザーにアシスタンスを提供するために、この機能を有効にする必要はありません。Citrixは、サーバーのセキュリティを向上させるために、この機能を無効のままにしておくことを推奨します。

- 管理者がWindowsリモートアシスタンスを開始できるようにするには、リモートアシスタンス用の適切なMicrosoftグループポリシー設定を使用して、必要な権限を付与します。詳細については、CTX127388: How to Enable Remote Assistance for Desktop Directorを参照してください。

高度な構成

Director は、ユーザー、Delivery Controller (DC)、VDA、および Director が異なるフォレストに配置されているフォレスト構成にまたがるマルチフォレスト環境をサポートできます。これには、フォレスト間の信頼関係と構成設定の適切なセットアップが必要です。

マルチフォレスト環境での推奨構成

推奨される構成では、ドメイン全体の認証を伴うフォレスト間で、送信および受信フォレスト信頼関係を作成する必要があります。

マルチフォレストサイト構成(/en-us/citrix-virtual-apps-desktops/2311/media/multiforest-config.png)

Director からの信頼関係により、異なるフォレストに存在するユーザーセッション、VDA、および Delivery Controller の問題をトラブルシューティングできます。

Director が複数のフォレストをサポートするために必要な高度な構成は、Internet Information Services (IIS) マネージャーで定義された設定によって制御されます。

> **重要:**

> IIS で設定を変更すると、Director サービスは自動的に再起動し、ユーザーはログオフされます。

> IIS を使用して高度な設定を構成するには:

1. Internet Information Services (IIS) マネージャーコンソールを開きます。
2. デフォルトの Web サイトの下にある Director Web サイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. 設定をダブルクリックして編集します。
5. をクリックして新しい設定を追加します。

Director は Active Directory を使用してユーザーを検索し、追加のユーザーおよびマシン情報を参照します。デフォルトでは、Director は次のドメインまたはフォレストを検索します。

- 管理者アカウントがメンバーである。
- Director Web サーバーがメンバーである（異なる場合）。

Directorは、Active Directoryグローバルカタログを使用してフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

別のActive Directoryドメインまたはフォレストからデータを検索または参照するには、検索するドメインまたはフォレストを明示的に設定する必要があります。IISマネージャーで、Director Web サイトに次のアプリケーション設定を構成します。

```
Connector.ActiveDirectory.Domains = (user),(server)
```

値属性の user と server は、それぞれ Director ユーザー（管理者）と Director サーバーのドメインを表します。

追加のドメインまたはフォレストからの検索を有効にするには、この例に示すように、ドメイン名をリストに追加します。

```
Connector.ActiveDirectory.Domains = (user),(server),\&lt;domain1\>,
\&lt;domain2\>
```

リスト内の各ドメインについて、Directorはフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

ドメインローカルグループの構成

ほとんどの Citrix Service Provider (CSP) は、インフラストラクチャフォレストに VDA、DC、および Director が含まれる同様の環境設定を持っています。ユーザーまたはユーザーグループのレコードは顧客フォレストに属します。インフラストラクチャフォレストから顧客フォレストへの一方向の送信信頼が存在します。

CSP管理者は通常、インフラストラクチャフォレストにドメインローカルグループを作成し、カスタマーフォレストのユーザーまたはユーザーグループをこのドメインローカルグループに追加します。

推奨されるマルチフォレストサイト構成(/en-us/citrix-virtual-apps-desktops/2311/media/domainlocalgroup-config.png)

Directorはこのようなマルチフォレスト設定をサポートし、ドメインローカルグループを使用して構成されたユーザーのセッションを監視できます。

1. IISマネージャーで、Director Webサイトに次のアプリケーション設定を追加します。

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true



   DomainLocalGroupSearchDomains= \&lt;domain1\>,\&lt;domain2\>
   ```

   \<domain1\>\<domain2\> は、ドメインローカルグループが存在するフォレストの名前です。

2. Web Studioでドメインローカルグループをデリバリーグループに割り当てます。
3. IISを再起動し、変更を有効にするためにDirectorに再度ログオンします。これで、Directorはこれらのユーザーのセッションを監視し、表示できるようになります。

Directorにサイトを追加する

Directorがすでにインストールされている場合は、複数のサイトで動作するように構成します。構成するには、各DirectorサーバーのIISマネージャーコンソールを使用して、アプリケーション設定のサーバーアドレスのリストを更新します。

各サイトのControllerのアドレスを次の設定に追加します。

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAControllerとSiteBControllerは、2つの異なるサイトのDelivery Controllerのアドレスです。

アクティビティマネージャーで実行中のアプリケーションの表示を無効にする

デフォルトでは、DirectorのActivity Managerは、ユーザーセッションのすべての実行中のアプリケーションのリストを表示します。この情報は、DirectorのActivity Manager機能にアクセスできるすべての管理者が表示できます。委任された管理者ロールの場合、これにはフル管理者、デリバリーグループ管理者、およびヘルプデスク管理者が含まれます。

ユーザーのプライバシーと実行中のアプリケーションを保護するために、**アプリケーション**タブを無効にして、実行中のアプリケーションを一覧表示しないようにすることができます。

> **警告:**

> レジストリを誤って編集すると、オペレーティングシステムを再インストールする必要があるような深刻な問題が発生する可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証しません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

1. VDAで、HKEY_LOCAL_MACHINE\\Software\\Citrix\\Director\\TaskManagerDataDisplayed のレジストリキーを変更します。デフォルトでは、このキーは1に設定されています。値を0に変更すると、VDAから情報が収集されなくなり、Activity Managerに表示されなくなります。
2. Directorがインストールされているサーバーで、実行中のアプリケーションの表示を制御する設定を変更します。デフォルトでは、値は「true」であり、アプリケーションタブで実行中のアプリケーションの表示が許可されます。値を「false」に変更すると、表示が無効になります。このオプションは、VDAではなく、DirectorのActivity Managerのみに影響します。 次の設定の値を変更します。 UI.TaskManager.EnableApplications = false

> **重要:**
>
> 実行中のアプリケーションの表示を無効にするには、Activity Managerにデータが表示されないように両方の変更を行います。

PIVスマートカード認証を構成する

この記事では、スマートカード認証機能を有効にするためにDirectorサーバーとActive Directoryで必要な構成を一覧表示します。

> **注：**
>
> スマートカード認証は、同じActive Directoryドメインのユーザーのみがサポートされます。

Directorサーバーの構成

Directorサーバーで以下の構成手順を実行します。

1. クライアント証明書マッピング認証をインストールして有効にします。Microsoftドキュメントのクライアント証明書マッピング認証にある**Active Directoryを使用したクライアント証明書マッピング認証**の手順に従います。
2. Directorサイトでフォーム認証を無効にします。

IISマネージャーを起動します。

サイト \> **既定のWebサイト** \> **Director** に移動します。

認証 を選択します。

フォーム認証 を右クリックして、**無効** を選択します。

フォーム認証を無効にする(/en-us/citrix-virtual-apps-desktops/2311/media/dir-smartcard-config1.png)

3. クライアント証明書認証のために、Director URLをより安全なHTTPSプロトコル（HTTPの代わりに）に構成します。

   a. IISマネージャーを起動します。
   b. **サイト** \> **既定のWebサイト** \> **Director** に移動します。
   c. 「**SSL Settings**」を選択します。
   d. 「**SSLを必須にする**」と「**クライアント証明書**」\>「**必須**」を選択します。

   SSL設定(/en-us/citrix-virtual-apps-desktops/2311/media/dir-smartcard-config2.png)

4. web.configを更新します。web.configファイル（c:\\inetpub\\wwwroot\\Directorにあります）をテキストエディターで開きます。

`<system.webServer>` 親要素の下に、次のスニペットを最初の子要素として追加します。

```
&lt;defaultDocument>

   &lt;files>

       &lt;add value="LogOn.aspx"/>

   &lt;/files>

&lt;/defaultDocument>
```

Active Directory の構成

デフォルトでは、Directorアプリケーションは**Application Pool**のIDプロパティで実行されます。スマートカード認証には委任が必要であり、そのためにはDirectorアプリケーションのIDがサービスホスト上でTrusted Computing Base (TCB)権限を持っている必要があります。

Citrixでは、Application Pool ID用に個別のサービスアカウントを作成することをお勧めします。Microsoft MSDNの記事「Protocol Transition with Constrained Delegation Technical Supplement」の指示に従って、サービスアカウントを作成し、TCB権限を割り当ててください。

新しく作成したサービスアカウントを Director アプリケーションプールに割り当てます。次の図は、サンプルサービスアカウント「Domain Pool」のプロパティダイアログを示しています。

サンプルサービスアカウント(/en-us/citrix-virtual-apps-desktops/2311/media/dir-smartcard-config3.png)

このアカウントに対して、次のサービスを構成します。

- Delivery Controller™：ホスト、エイチティーティーピー
- Director：ホスト、HTTP
- Active Directory：ジーシー、エルダップ

構成するには、,

1. 「ユーザーアカウントのプロパティ」ダイアログで、「**追加**」をクリックします。
2. **サービスの追加**ダイアログで、をクリックします。
3. Delivery Controllerのホスト名を選択します。
4. 「**利用可能なサービス**」リストから、HOSTとHTTPの「**サービスの種類**」を選択します。

サービスを設定する(/en-us/citrix-virtual-apps-desktops/2311/media/dir-smartcard-config4.png)

同様に、**Director**および**Active Directory**ホストのサービスの種類を追加します。

サービスプリンシパル名レコードを作成する

各Directorサーバーおよびディレクターサーバーのプールへのアクセスに使用される負荷分散された仮想IP（VIP）ごとにサービスアカウントを作成する必要があります。新しく作成されたサービスアカウントへの委任を設定するには、サービスプリンシパル名（SPN）レコードを作成する必要があります。

- DirectorサーバーのSPNレコードを作成するには、次のコマンドを使用します。

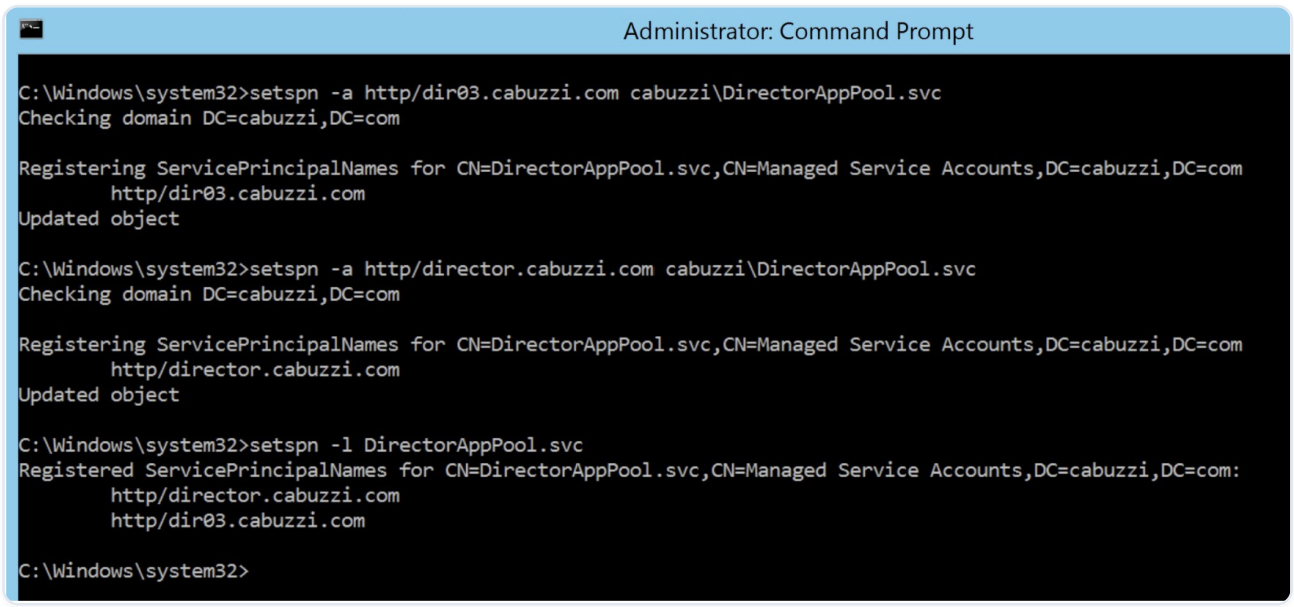
```
  setspn -a http/<directorServer>.<domain_fqdn>
<domain>\<DirectorAppPoolServiceAcct>
```

- 負荷分散されたVIPのSPNレコードを作成するには、次のコマンドを使用します。

```
setspn -S http/<DirectorFQDN> <domain>\<DirectorAppPoolServiceAcct>
```

- 作成されたSPNを表示またはテストするには、次のコマンドを使用します。

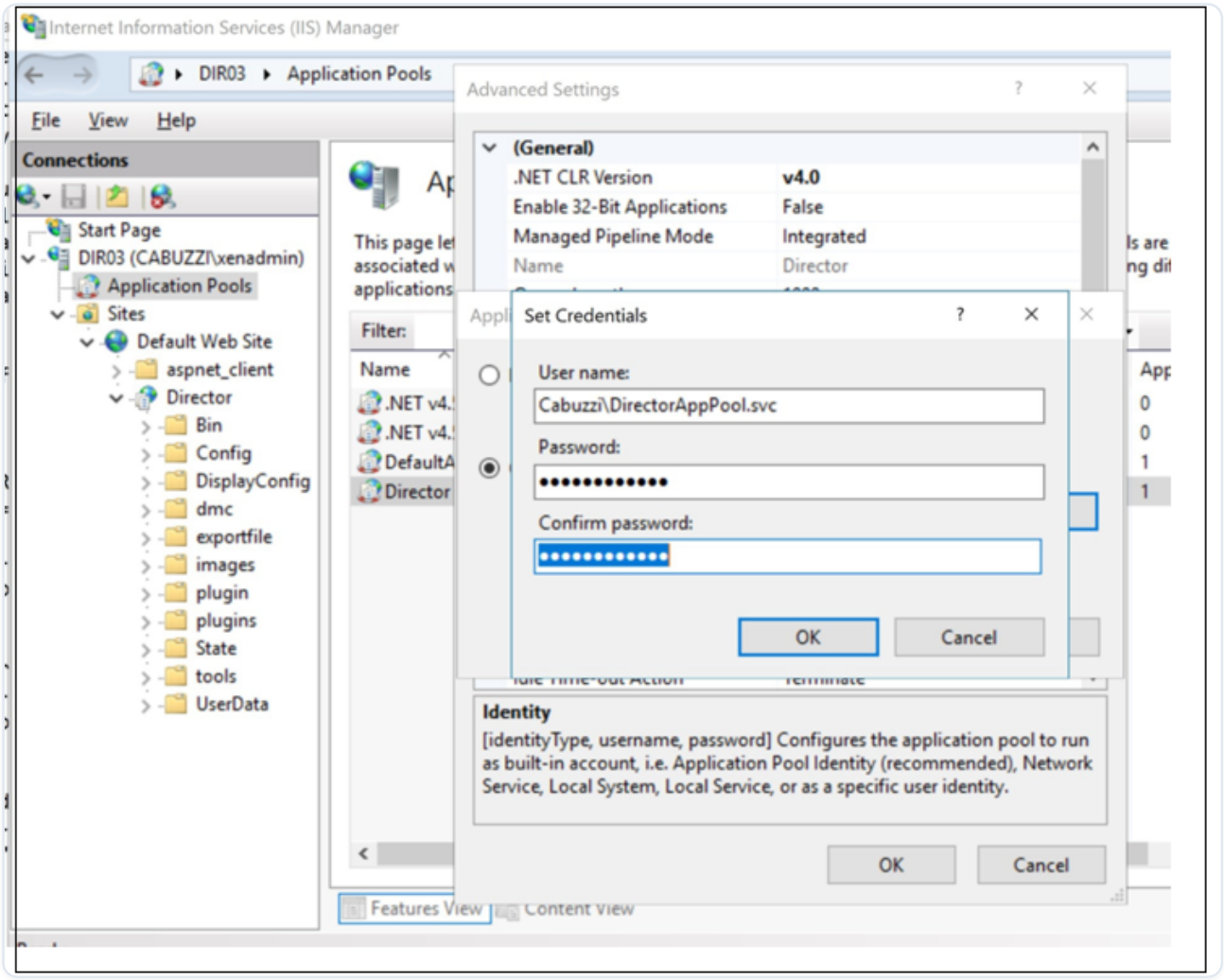
```
setspn –l <DirectorAppPoolServiceAcct>
```



- 左ペインでDirector仮想ディレクトリを選択し、 をダブルクリックします。 ウィンドウで をクリックし、**AllowKerberosConstrainedDelegation** が1に設定されていることを確認します。

ケルベロス(/en-us/citrix-virtual-apps-desktops/2311/media/dir-smart-card-auth-3.png)

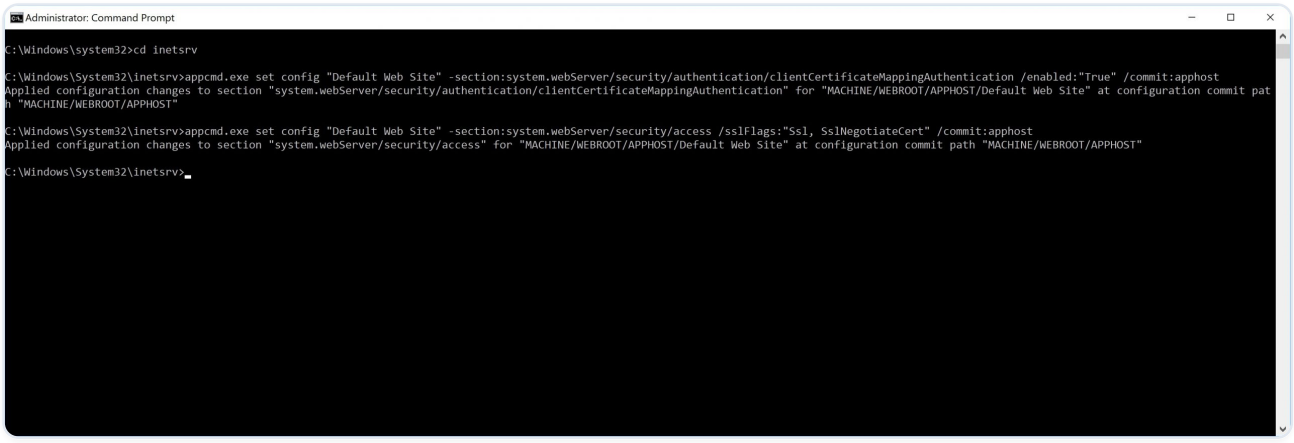
- 左側のペインで を選択し、Directorアプリケーションプールを右クリックして を選択します。
- 「**ID**」を選択し、省略記号（「…」）をクリックしてサービスアカウントのドメイン\ログオンとパスワードの資格情報を入力します。IISコンソールを閉じます。



- 管理者として実行したコマンドプロンプトから、ディレクトリを C:\Windows\System32\inetsrv に変更し、次のコマンドを入力します。

```
   appcmd.exe set config “Default Web Site” -section:system.webServer/
security/authentication/clientCertificateMappingAuthentication /
enabled:”True” /commit:apphost
```

```
    appcmd.exe set config “Default Web Site” -section:system.webServer/
security/access /sslFlags:”Ssl, SslNegotiateCert” /commit:apphost
```



Firefoxブラウザーの構成

Firefoxブラウザーを使用するには、OpenSC 0.17.0で入手可能なPIVドライバーをインストールします。インストールと構成の手順については、「Installing OpenSC PKCS#11 Module in Firefox, Step by Step」を参照してください。 Directorでのスマートカード認証機能の使用方法については、Directorの記事の「Use Director with PIV based smart card authentication」セクションを参照してください。

ネットワーク分析の構成

> **注：** この機能の利用可否は、組織のライセンスと管理者権限によって異なります。

> DirectorはCitrix ADMと統合し、ネットワーク分析とパフォーマンス管理を提供します。

- ネットワーク分析は、Citrix ADMのHDX™ Insightレポートを使用して、ネットワークのアプリケーションおよびデスクトップのコンテキストビューを提供します。この機能により、Directorは展開におけるICAトラフィックの高度な分析を提供します。
- パフォーマンス管理は、履歴保持と傾向レポートを提供します。リアルタイム評価と比較してデータの履歴を保持することで、容量や健全性の傾向を含むトレンドレポートを作成できます。

Directorでこの機能を有効にすると、HDX InsightレポートはDirectorに追加情報を提供します。

- ［傾向］ページの［ネットワーク］タブには、展開環境全体におけるアプリケーション、デスクトップ、およびユーザーの遅延と帯域幅の影響が表示されます。
- ［ユーザー詳細］ページには、特定のユーザーセッションに固有の遅延と帯域幅の情報が表示されます。

制限事項:

- トレンドビューでは、バージョン7より前のVDAのHDX接続ログオンデータは収集されません。それより前のVDAの場合、グラフデータは0として表示されます。

ネットワーク分析を有効にするには、DirectorにCitrix ADMをインストールして構成する必要があります。Directorには、Citrix ADMバージョン11.1ビルド49.16以降が必要です。MASはXenServer上で動作する仮想アプライアンスです。ネットワーク分析を使用することで、Directorは展開に関連する情報を通信し、収集します。

詳しくは、Citrix ADMドキュメントを参照してください。

注:

Citrix NetScaler Insight Centerは、15 May 2018をもってメンテナンス終了日を迎えました。Citrix製品マトリックス を参照してください。ネットワーク分析のためにDirectorをCitrix ADMと統合してください。NetScaler Insight CenterをCitrix ADMに移行するには、「NetScaler Insight CenterからCitrix ADMへの移行」を参照してください。

1. Directorがインストールされているサーバーで、C:\\inetpub\\wwwroot\\Director\\toolsにあるDirectorConfigコマンドラインツールを見つけ、コマンドプロンプトからパラメーター/confignetscalerを指定して実行します。
2. プロンプトが表示されたら、Citrix ADMマシン名（FQDNまたはIPアドレス）、ユーザー名、パスワード、HTTPS接続タイプ（HTTPよりも推奨）、およびCitrix ADM統合を選択します。
3. 変更を確認するには、ログオフして再度ログオンします。

注:

セキュリティ上の理由から、DirectorとのADM統合のために、HDX Insightへのアクセスに十分な権限を持つカスタムロールを作成することをお勧めします。

詳細については、アクセスポリシーの構成を参照してください。

委任管理とDirector

委任管理では、管理者、役割、スコープという3つの概念を使用します。権限は、管理者の役割とこの役割のスコープに基づいています。たとえば、管理者は、1つのサイトのエンドユーザーに対する責任を伴うスコープを持つヘルプデスク管理者役割を割り当てられる場合があります。

委任管理者の作成については、メインの委任管理の記事を参照してください。

管理権限は、管理者に表示されるDirectorインターフェイスと、管理者が実行できるタスクを決定します。権限によって以下が決定されます。

- 管理者がアクセスできるビュー（総称してビューと呼ばれる）。
- 管理者が表示および操作できるデスクトップ、マシン、およびセッション。
- 管理者が実行できるコマンド（ユーザーセッションのシャドウイングやメンテナンスモードの有効化など）。

組み込みの役割と権限は、管理者がDirectorを使用する方法も決定します。

管理者役割	DIRECTORでの権限
フル管理者	すべてのビューへのフルアクセス権を持ち、ユーザーセッションのシャドウイング、メンテナンスモードの有効化、トレンドデータのエクスポートを含むすべてのコマンドを実行できます。
デリバリーグループ管理者	すべてのビューへのフルアクセス権を持ち、ユーザーセッションのシャドウイング、電源管理とセッション管理、メンテナンスモードの有効化、トレンドデータのエクスポートを含むすべてのコマンドを実行できます。
読み取り専用管理者	すべてのビューにアクセスし、指定されたスコープ内のすべてのオブジェクトとグローバル情報を表示できます。HDX™チャネルからレポートをダウンロードし、トレンドビューの[エクスポート]オプションを使用してトレンドデータをエクスポートできます。その他のコマンドを実行したり、ビュー内の何かを変更したりすることはできません。
ヘルプデスク管理者	ヘルプデスクビューとユーザー詳細ビューのみにアクセスでき、管理者が管理を委任されて

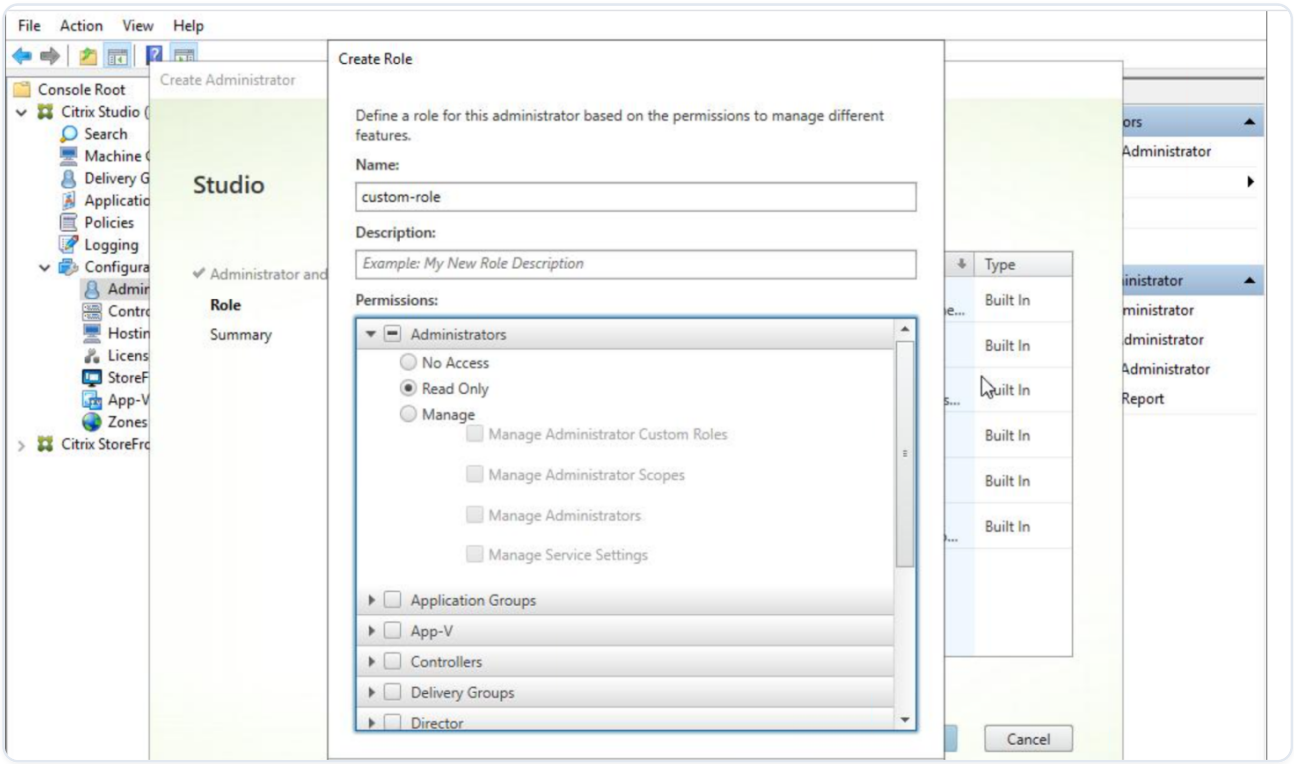
管理者役割	DIRECTORでの権限
	いるオブジェクトのみを表示できます。ユーザーのセッションをシャドウし、そのユーザーのコマンドを実行できます。メンテナンスモード操作を実行できます。シングルセッションOSマシンに対して電源制御オプションを使用できます。ダッシュボード、トレンド、アラート、またはフィルタービューにはアクセスできません。マルチセッションOSマシンに対して電源制御オプションを使用することはできません。
マシンカタログ管理者	マシン詳細ページ（マシンベース検索）のみにアクセスできます。
ホスト管理者	アクセスできません。この管理者はDirectorではサポートされておらず、データを表示できません。

Director管理者用のカスタム役割を構成する

Studioでは、組織の要件により厳密に一致させ、権限をより柔軟に委任するために、Director固有のカスタム役割を構成することもできます。たとえば、組み込みのヘルプデスク管理者役割を制限して、この管理者がセッションをログオフできないようにすることができます。

Director権限を持つカスタム役割を作成する場合、その役割に他の一般的な権限も付与する必要があります。

- Delivery Controller™ にログオンするための権限 - 管理者ノードで少なくとも読み取り専用アクセス
- Directorでそれらのデリバリーグループに関連するデータを表示するためのデリバリーグループへの権限 - 少なくとも読み取り専用アクセス

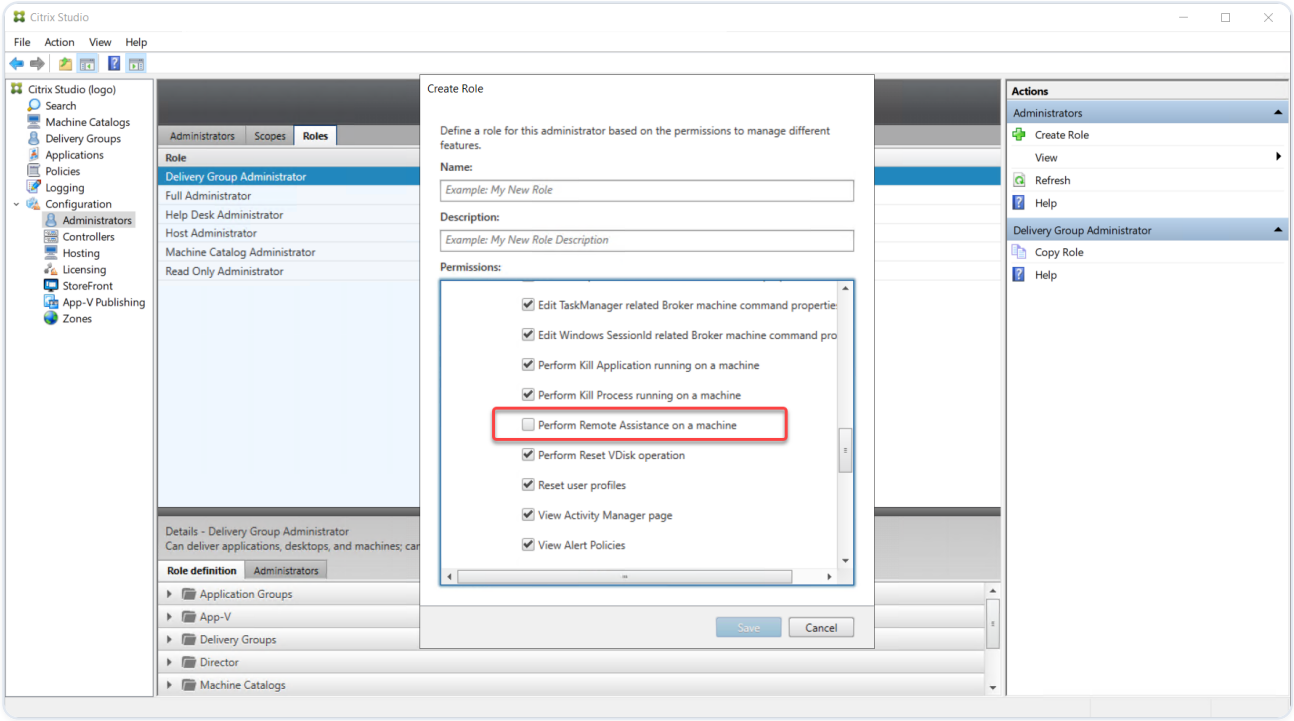


または、既存のロールをコピーして、さまざまなビューの追加の権限を含めることで、カスタムロールを作成できます。たとえば、ヘルプデスクロールをコピーして、ダッシュボードまたはフィルターページを表示する権限を含めることができます。

カスタムロールのDirector権限を選択します。これには以下が含まれます。

- マシン上で実行中のアプリケーションの強制終了を実行する
- マシン上で実行中のプロセスの強制終了を実行する
- マシン上でリモートアシスタンスを実行する
- ユーザープロファイルをリセットする
- クライアント詳細ページを表示
- ダッシュボードページの表示
- フィルターページを表示する
- マシン詳細ページを表示
- トレンドページの表示
- ユーザー詳細ページを表示

この例では、シャドウイング（マシンでリモートアシスタンスを実行）はオフになっています。



権限は、UIで適用可能になるために他の権限に依存する場合があります。たとえば、**マシン上で実行中のアプリケーションの強制終了を実行する**権限を選択すると、ロールに権限があるパネルでのみ**アプリケーションの終了**機能が有効になります。次のパネル権限を選択できます。

- フィルターページを表示する
- ユーザー詳細ページを表示
- マシン詳細ページを表示
- クライアント詳細ページを表示

さらに、他のコンポーネントの権限リストから、デリバリーグループの以下の権限を検討してください。

- デリバリーグループのメンバーシップを使用して、マシンのメンテナンスモードを有効/無効にする。
- デリバリーグループのメンバーシップを使用して、Windowsデスクトップマシンで電源操作を実行する。
- デリバリーグループのメンバーシップを使用して、マシンでセッション管理を実行する。

Directorの展開を保護する

この記事では、Directorの展開および構成時にシステムセキュリティに影響を与える可能性のある領域について説明します。

マイクロソフト インターネット インフォメーション サービス (IIS) の構成

制限されたIIS構成でDirectorを構成できます。

アプリケーションプールのリサイクル制限

次のアプリケーションプールのリサイクル制限を設定できます。

- 仮想メモリ制限: 4,294,967,295
- プライベートメモリ制限: StoreFront™サーバーの物理メモリのサイズ
- 要求制限: 4,000,000,000

ファイル名拡張子

一覧にないファイル名拡張子を許可しないように設定できます。

Directorは、要求フィルタリングで次のファイル名拡張子を必要とします。

- .エイエスピーエックス
- 「.css」
- .エイチティーエムエル
- .js
- ．png
- ．svc
- ．gif
- ドットジェイソン
- ドットウォフ
- ドットウォフ2
- ドットティーティーエフ

Directorは、要求フィルタリングで次のHTTP動詞を必要とします。リストにない動詞を許可しないように設定できます。

- GET
- POST
- HEAD

Directorは以下を必要としません:

- ISAPIフィルター

- ISAPI拡張機能
- CGIプログラム
- FastCGIプログラム

> **重要:**
>
> - Director には完全な信頼が必要です。グローバルな .NET 信頼レベルを High 以下に設定しないでください。
> - Director は個別のアプリケーションプールを維持します。Director の設定を変更するには、Director サイトを選択して変更します。

ユーザー権限の構成

Directorがインストールされると、そのアプリケーションプールには以下が付与されます。

- **サービスとしてログオン**のログオン権限
- **プロセスに対するメモリクォータの調整**、**セキュリティ監査の生成**、および**プロセスレベルトークンの置き換え**の特権

言及されている権限と特権は、アプリケーションプールが作成される際の通常のインストール動作です。

これらのユーザー権限を変更する必要はありません。これらの特権は Director では使用されず、自動的に無効になります。

Directorの通信

本番環境では、Director とサーバー間でやり取りされるデータを保護するために、インターネットプロトコルセキュリティ (IPsec) または HTTPS プロトコルを使用してください。

IPsec は、インターネットプロトコルに対する標準拡張機能のセットであり、データの整合性とリプレイ保護を備えた認証済みおよび暗号化された通信を提供します。IPsec はネットワーク層プロトコルセットであるため、上位レベルのプロトコルは変更なしでそれを使用できます。HTTPS は、トランスポート層セキュリティ (TLS) プロトコルを使用して強力なデータ暗号化を提供します。

> **注:**

- Citrix® は、Directorコンソールへのアクセスをイントラネット内に制限することを強く推奨します。
- Citrix は、本番環境で Director へのセキュリティで保護されていない接続を有効にしないことを強く推奨します。
- Director からの安全な通信には、接続ごとに個別の構成が必要です。
- SSL プロトコルは推奨されません。代わりに、より安全な TLS プロトコルを使用してください。
- IPsec ではなく TLS を使用して、Citrix ADC との通信を保護してください。

Director と Citrix Virtual Apps and Desktops サーバー間の通信（監視およびレポート用）を保護するには、Data Access Security を参照してください。

Director と Citrix ADC 間の通信（Citrix Insight 用）を保護するには、Configure network analysis を参照してください。

Director とライセンスサーバー間の通信を保護するには、Secure the License Administration Console を参照してください。

Director のセキュリティ分離

Director と同じ Web ドメイン（ドメイン名とポート）に任意の Web アプリケーションを展開できます。ただし、それらの Web アプリケーションにセキュリティ上のリスクがある場合、Director の展開のセキュリティが低下する可能性があります。より高度なセキュリティ分離が必要な場合は、Director を別の Web ドメインに展開することを Citrix は推奨します。

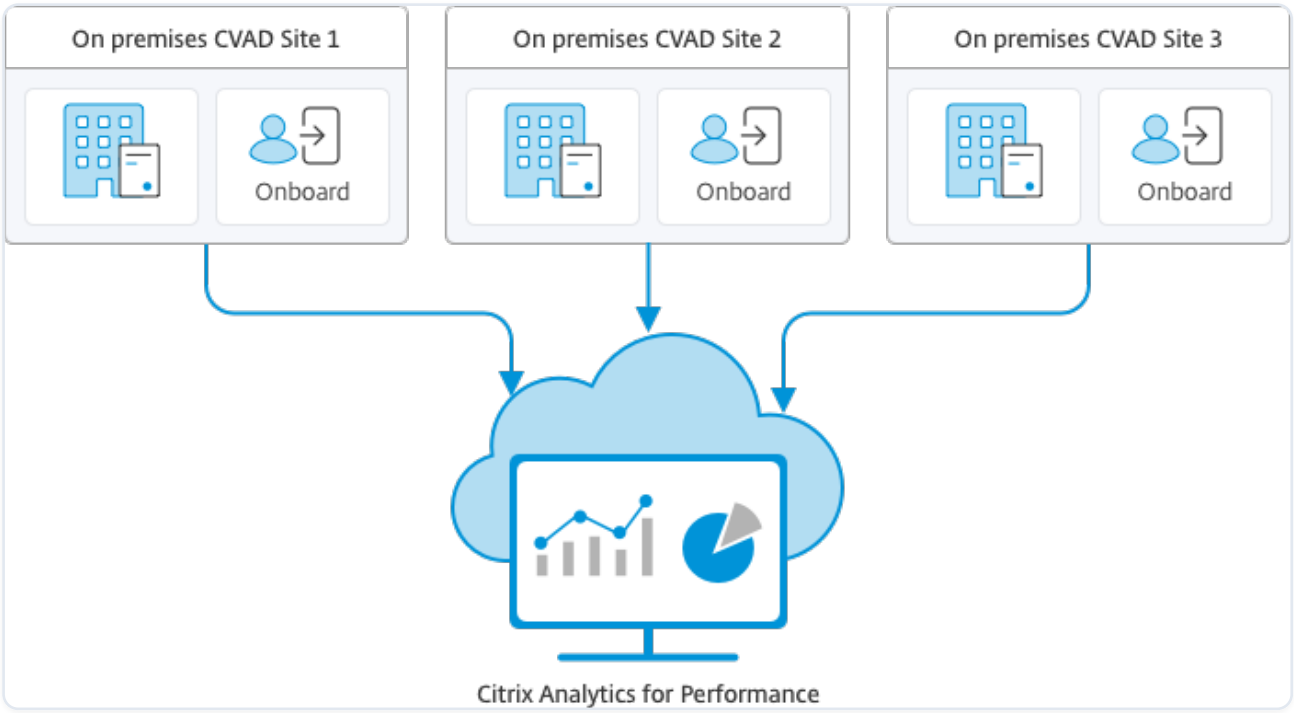
Citrix Analytics for Performance™ を使用したオンプレミスサイトの構成

Citrix Analytics for Performance (Performance Analytics) は、Citrix Analytics Cloud Service が提供する包括的なパフォーマンス監視ソリューションです。Performance Analytics は、パフォーマンスメトリックに基づいて構築された高度なインサイトと分析を提供します。Performance Analytics を使用すると、組織内の1つ以上のCitrix Virtual Apps and Desktops™サイトの使用状況とパフォーマンスメトリックを監視および表示できます。

Performance Analyticsの詳細については、Performance Analyticsの記事を参照してください。

サイトからCitrix Cloud™上のCitrix Analytics for Performanceにパフォーマンスデータを送信して、その高度なパフォーマンス分析機能を活用できます。Performance Analytics を表示および使

用するには、まず **Director** の **Analytics** タブからオンプレミスサイトをCitrix Analytics for Performanceで構成する必要があります。



Performance Analyticsは安全な方法でデータにアクセスし、Citrix Cloudからオンプレミス環境にデータが転送されることはありません。

前提条件

Director からCitrix Analytics for Performanceを構成するために、新しいコンポーネントをインストールする必要はありません。以下の要件が満たされていることを確認してください。

- Delivery Controller と Director がバージョン 1912 CU2 以降であること。詳細については、機能の互換性マトリックスを参照してください。

> **注:**
>
> - Delivery Controller で Microsoft .NET Framework のバージョン 4.8 より前のバージョンが実行されている場合、Director からオンプレミスサイトをCitrix Analytics for Performanceで構成できないことがあります。回避策として、Delivery Controller の .NET Framework をバージョン 4.8 にアップグレードしてください。LCM-9255。
> - Citrix Virtual Apps and Desktops バージョン 2012 を実行しているオンプレミスサイトを Director からCitrix Analytics for Performanceで構成すると、数時間後または Delivery Controller の Citrix Monitor Service の再起動後に構成が失敗する場合があります。この場合、Analytics タブには「未接続」ステータスが表示されます。回避策として、Delivery

> Controller のレジストリに Encryption フォルダーを作成します。場所: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor、フォルダー名: Encryption。CitrixMonitor アカウントが Encryption フォルダーに対してフルコントロールアクセス権を持っていることを確認してください。Citrix Monitor Service を再起動します。DIR-14324。

- この構成を実行するための **Analytics** タブへのアクセスは、フル管理者のみが利用できます。
- Performance Analytics がパフォーマンスメトリックにアクセスできるようにするには、すべての Delivery Controller および Director がインストールされているマシンでアウトバウンドインターネットアクセスが利用可能である必要があります。具体的には、次の URL へのアクセス可能性を確認してください。
  - Citrix キー登録: `https://*.citrixnetworkapi.net/`
  - シトリックスクラウド: `https://*.citrixworkspacesapi.net/`
  - シトリックス アナリティクス: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/` Delivery ControllerとDirectorマシンがイントラネット内にあり、アウトバウンドインターネットアクセスがプロキシサーバー経由である場合、以下を確認してください。
- プロキシサーバーは、上記のURLリストを許可する必要があります。
- Director web.config および citrix.monitor.exe.config ファイルに次の構成を追加します。この構成は **configuration** タグ内に追加してください。

```
&lt;system.net>

    &lt;defaultProxy>

        &lt;proxy  usesystemdefault = "false"  proxyaddress = "http://
&lt;your_proxyserver_address>:80" bypassonlocal = "true"  />

    &lt;/defaultProxy>

&lt;/system.net>
```

  - Director web.config は、Director がインストールされているマシンの `C:\inetpub\wwwroot\Director\web.config` にあります。

- citrix.monitor.exe.config は、Delivery Controller がインストールされているマシンの `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` にあります。

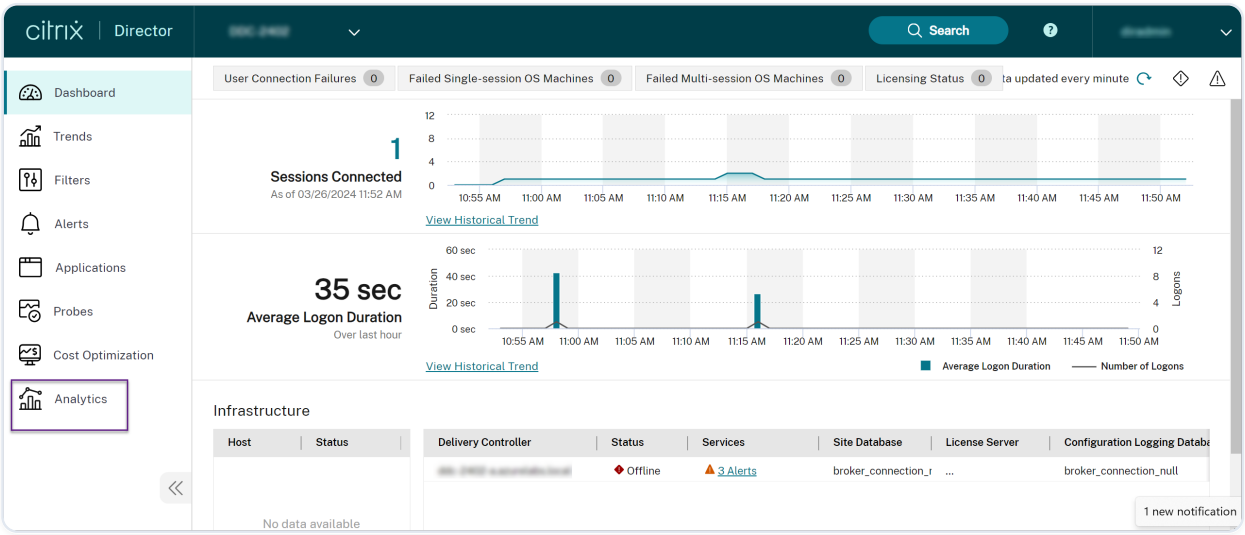
この設定は、IIS上のMicrosoftによって提供されます。詳細については、`https://docs.microsoft.com/ja-jp/dotnet/framework/network-programming/proxy-configuration`を参照してください。 構成ファイルの**defaultproxy**フィールドは、Directorおよび監視サービスのアウトバウンドアクセスを制御します。Performance Analyticsとの構成および通信には、**defaultproxy**フィールドを**true**に設定する必要があります。適用されているポリシーによってこのフィールドがfalseに設定されている可能性があります。この場合、フィールドを手動でtrueに設定する必要があります。変更を行う前に、構成ファイルのバックアップを取ってください。変更を有効にするには、Delivery Controller™で監視サービスを再起動してください。

- Citrix Analytics for PerformanceのCitrix Cloudエンタイトルメントがアクティブであること。
- Citrix Cloudアカウントが、製品登録エクスペリエンスに対する権限を持つ管理者アカウントであること。管理者権限の詳細については、「管理者権限の変更」を参照してください。

構成手順

前提条件を確認したら、次の手順を実行します。

1. Director にフル管理者としてサインインし、Performance Analytics で構成するサイトを選択します。Director ダッシュボードページが表示されます。



2. **Analytics** タブをクリックします。**Citrix Analytics の構成**ページが表示されます。

「開始」(/en-us/citrix-virtual-apps-desktops/2311/media/dir-onboardingstep3.png)

3. 手順を確認し、サービス規約を選択してから、**開始**をクリックします。**サイトの詳細**ページが表示されます。

「サイトを接続」(/en-us/citrix-virtual-apps-desktops/2311/media/dir-onboarding4.png)

4. 前提条件を確認し、満たされていることを確認します。サイトの詳細を確認します。
5. 構成プロセスを開始するには、**サイトの接続**をクリックします。

   このサイトをCitrix Cloudに登録するために使用される、一意の8桁の登録コードが生成されます。

   「登録コード」(/en-us/citrix-virtual-apps-desktops/2311/media/dir-onboarding5.png)
6. **Copy Code** をクリックしてコードをコピーし、**Register on Citrix Cloud** をクリックします。Citrix Cloudの登録URLにリダイレクトされます。
7. Citrix Cloudの資格情報でサインインし、顧客を選択します。
8. Citrix Cloudの「製品登録」ページに、コピーした登録コードを貼り付けます。登録するには、**［続行］**をクリックします。登録の詳細を確認し、［登録］**をクリックします。

   「Citrix Cloudに登録」(/en-us/citrix-virtual-apps-desktops/2311/media/dir-onboarding6.png)

   オンプレミスサイトがCitrix Cloudに登録されます。
9. **Director**から、**［Analytics］**タブの**［Analyticsに移動］**をクリックします。

   「Analyticsに移動」(/en-us/citrix-virtual-apps-desktops/2311/media/dir-onboarding7.png)

   Performance Analyticsがブラウザの新しいタブで開きます。 「Performance Analyticsダッシュボード」(/en-us/citrix-virtual-apps-desktops/2311/media/dir-onboarding-pa-dashboard.png)

   Citrix Cloudセッションの有効期限が切れている場合、Citrix.comまたはMy Citrixアカウントのログオンページにリダイレクトされることがあります。
10. 複数のサイトをPerformance Analyticsに登録するには、Directorから各サイトについて前述の構成手順を繰り返します。構成されているすべてのサイトのメトリックがPerformance Analyticsダッシュボードに表示されます。

    サイトごとに複数のDirectorインスタンスが実行されている場合は、いずれか1つのDirectorインスタンスから構成します。サイトに接続されている他のすべてのDirectorインスタンスは、構成プロセスの後の次回の更新時に更新されます。
11. サイトをCitrix Cloudから切断するには、 をクリックします。このオプションにより、既存の構成が削除されます。

> **注：**

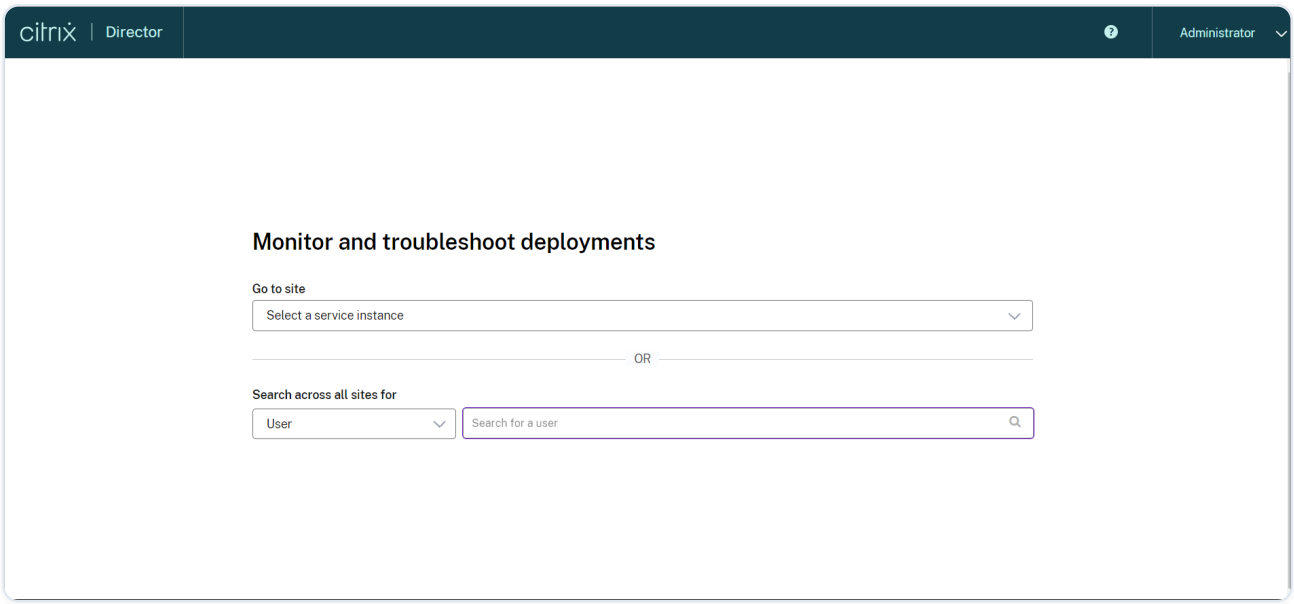
> サイトを初めて構成するとき、サイトからのイベントの処理には時間がかかる場合があり（約1時間）、Performance Analyticsダッシュボードにメトリックが表示されるまでに遅延が生じます。その後、イベントは定期的に更新されます。

> 切断後、新しいアカウントからのイベントが送信されるまで、古いアカウントからのデータ送信はしばらく継続されます。データ送信が停止してから約1時間、古いアカウントに関連する分析はPerformance Analyticsダッシュボードに表示されたままになります。

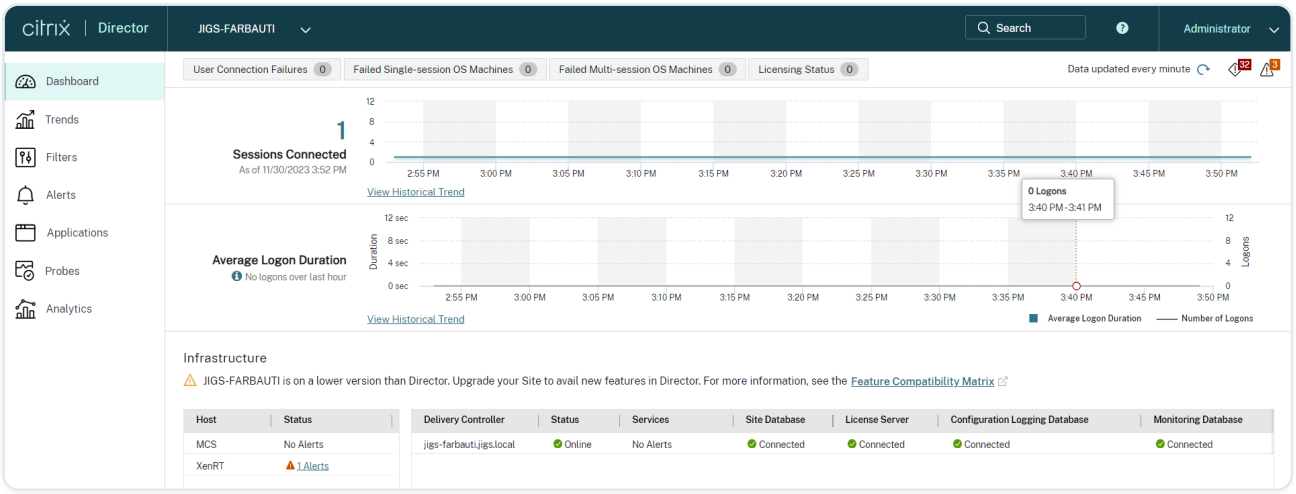
> Citrix Analyticsサービスのエンタイトルメントの有効期限が切れると、サイトメトリックがPerformance Analyticsに送信されなくなるまでに最大1日かかります。

サイト分析

Director を使用して、展開の健全性を監視できます。オンボードされたすべてのサイトでユーザー、エンドポイント、またはマシンを検索することで、パフォーマンスの問題をトラブルシューティングできます。



完全な管理者権限があれば、Directorを開くと、ダッシュボードは、サイトの健全性と使用状況を監視するための一元的な場所を提供します。



現在障害がなく、過去60分間に障害が発生していない場合、パネルは折りたたまれたままになります。障害が発生すると、特定の障害パネルが自動的に表示されます。

> **注:**
>
> 組織のライセンスと管理者権限によっては、一部のオプションまたは機能が利用できない場合があります。

Director ダッシュボードのパネル

ユーザー接続障害

過去60分間の接続障害。合計数の横にあるカテゴリをクリックすると、その種類の障害のメトリックが表示されます。隣接するテーブルでは、その数がデリバリーグループ別に分類されています。接続障害には、アプリケーション制限に達したことによる障害が含まれます。アプリケーション制限の詳細については、「アプリケーション」を参照してください。

失敗したシングルセッションOSマシンまたは失敗したマルチセッションOSマシン

過去60分間の合計障害数（デリバリーグループ別）。障害は、起動失敗、起動中に停止、未登録などの種類別に分類されます。マルチセッションOSマシンでは、障害には最大負荷に達したマシンも含まれます。

ライセンスステータス

ライセンスサーバーアラートは、ライセンスサーバーから送信されたアラートと、アラートを解決するために必要なアクションを表示します。License Server バージョン 11.12.1 以降が必要です。Delivery Controller アラートは、Controller が認識するライセンス状態の詳細を表示し、Controller から送信されます。XenApp 7.6 または XenDesktop 7.6 以降の Controller が必要です。Studio でアラートのしきい値を設定できます。**Delivery Controllers** > **Details** > **Product**

Editions > **PLT** に表示されるライセンスステータスは、**Premium** を示し、**Platinum** ではありません。

グレース状態

Directorは、以下のいずれかのグレース状態を表示します。この情報は、Delivery Controllerから取得されます。

1. **非アクティブ:** いずれの種類のライセンスキャッシュモードでもありません。通常のライセンス制限が適用されます。
2. **緊急グレース:** ライセンスサーバーに到達できない場合、または接続を仲介している間にライセンス情報を取得できない場合に有効になります。ユーザーには影響ありません。Directorに表示されるエラーは、ライセンスサーバーに到達可能になるまで閉じることができません。
3. **グレース期限切れ:** 緊急ライセンスキャッシュモードの有効期限が切れました。

詳しくは、ライセンスの超過およびライセンスバーストモードを参照してください。

接続されたセッション

過去60分間のすべてのデリバリーグループにおける接続されたセッション。

平均ログオン時間

過去60分間のログオンデータ。左側の大きな数字は、1時間あたりの平均ログオン時間です。XenDesktop 7.0より前のVDAのログオンデータは、この平均には含まれません。詳しくは、ユーザーログオンの問題の診断を参照してください。

インフラストラクチャ

サイトのインフラストラクチャ（ホストとコントローラー）を一覧表示します。XenServerまたはVMwareのインフラストラクチャの場合、パフォーマンスアラートを表示できます。たとえば、管理対象サーバーまたは仮想マシンでCPU、ネットワークI/O、またはディスクI/Oの使用率が指定されたしきい値を超えたときに、XenCenterがパフォーマンスアラートを生成するように構成できます。デフォルトでは、アラートの繰り返し間隔は60分ですが、これも構成できます。詳細については、XenServer製品ドキュメントの「XenCenterパフォーマンスアラート」セクションを参照してください。

> **注：**

特定のメトリックにアイコンが表示されない場合、そのメトリックは使用しているホストの種類でサポートされていないことを示します。たとえば、System Center Virtual Machine Manager (SCVMM) ホスト、AWS、CloudStackでは、健全性情報は利用できません。

以下のオプション（次のセクションで説明されています）を使用して、問題のトラブルシューティングを続行します。

- ユーザーマシンの電源を制御する(/ja-jp/citrix-virtual-apps-desktops/2311/director/site-analytics.html#control-user-machine-power-states)
- マシンへの接続を防止する(/ja-jp/citrix-virtual-apps-desktops/2311/director/site-analytics.html#prevent-connections-to-machines)

セッションの監視

セッションが切断されても、そのセッションはアクティブであり、アプリケーションは引き続き実行されますが、ユーザーデバイスはサーバーと通信しなくなります。

アクション	説明
ユーザーの現在接続されているマシンまたはセッションを表示する	アクティビティマネージャーとユーザー詳細ビューから、ユーザーの現在接続されているマシンまたはセッション、およびこのユーザーがアクセスできるすべてのマシンとセッションのリストを表示します。このリストにアクセスするには、ユーザータイトルバーのセッションスイッチャーアイコンをクリックします。詳細については、「セッションの復元」を参照してください。
すべてのデリバリーグループにわたる接続済みセッションの合計数を表示する	ダッシュボードの**接続済みセッション**ペインで、過去60分間のすべてのデリバリーグループにわたる接続済みセッションの合計数を表示します。次に、大きな合計数をクリックすると、フィルタービューが開き、選択したデリバリーグループと範囲、およびデリバリーグループ全体の使用状況に基づいてグラフィカルなセッションデータを表示できます。
アイドルセッションの終了	セッションフィルタービューには、すべてのアクティブなセッションに関連するデータが表示されます。関連ユーザー、デリバリーグルー

アクション	説明
	プ、セッション状態、およびしきい値期間を超えるアイドル時間に基づいてセッションをフィルター処理します。フィルター処理されたリストから、ログオフまたは切断するセッションを選択します。詳細については、「アプリケーションのトラブルシューティング」を参照してください。
より長期間のデータを表示する	トレンドビューで、**セッション**タブを選択すると、より長期間（つまり、過去60分よりも前のセッション合計）の接続済みセッションと切断済みセッションに関するより具体的な使用状況データにドリルダウンできます。この情報を表示するには、**履歴トレンドの表示**をクリックします。

注:

ユーザーデバイスがレガシーなVirtual Delivery Agent (VDA)（バージョン 7 以前の VDA や Linux VDA など）を実行している場合、Director はセッションに関する完全な情報を表示できません。代わりに、情報が利用できないことを示すメッセージが表示されます。

デスクトップ割り当てルールの制限事項: Web Studio では、異なるユーザーまたはユーザーグループに対して複数のデスクトップ割り当てルール (DAR) をデリバリーグループ内の単一の VDA に割り当てることができます。StoreFront™ は、ログインユーザーの DAR に従って、割り当てられたデスクトップを対応する**表示名**とともに表示します。しかし、Director は DAR をサポートしておらず、ログインユーザーに関係なく、デリバリーグループ名を使用して割り当てられたデスクトップを表示します。その結果、Director で特定のデスクトップをマシンにマッピングすることはできません。 StoreFront に表示される割り当てられたデスクトップを、Director に表示されるデリバリーグループ名にマッピングするには、次の PowerShell コマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq
```

```
"\&lt;Name on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property
Name, Uid
```

セッション転送プロトコル

現在のセッションの HDX 接続タイプで使用されているトランスポートプロトコルを、**セッションの詳細**パネルで表示します。この情報は、バージョン 7.13 以降の VDA で起動されたセッションで利用できます。

転送プロトコル (/en-us/citrix-virtual-apps-desktops/2311/media/sessions-transport-protocol.png)

- **HDX™** 接続タイプの場合、,
  - HDX 接続に EDT が使用されている場合、プロトコルは **UDP** と表示されます。
  - HDX 接続に TCP が使用されている場合、プロトコルは **TCP** と表示されます。
- **RDP** 接続タイプの場合、プロトコルは **n/a** と表示されます。

アダプティブトランスポートが構成されている場合、セッショントランスポートプロトコルはネットワークの状態に基づいて EDT (UDP 経由) と TCP の間で動的に切り替わります。EDT を使用して HDX セッションを確立できない場合、TCP プロトコルにフォールバックします。

アダプティブトランスポートの構成の詳細については、「アダプティブトランスポート」を参照してください。

レポートのエクスポート

定期的な使用状況および容量管理レポートを生成するために、トレンドデータをエクスポートできます。エクスポートは、PDF、Excel、CSV のレポート形式をサポートしています。PDF および Excel 形式のレポートには、グラフと表で表されたトレンドが含まれます。CSV 形式のレポートには、ビューを生成するために処理したり、アーカイブしたりできる表形式のデータが含まれます。

レポートをエクスポートするには：

1. **トレンド**タブに移動します。
2. フィルター条件と期間を設定し、**適用**をクリックします。傾向グラフと表にデータが入力されます。
3. **エクスポート**をクリックし、レポートの名前と形式を入力します。

Director は、選択したフィルター条件に基づいてレポートを生成します。フィルター条件を変更した場合は、**エクスポート**をクリックする前に**適用**をクリックしてください。

注:

大量のデータをエクスポートすると、Director サーバー、Delivery Controller、および SQL サーバーのメモリと CPU の消費量が大幅に増加します。最適なエクスポートパフォーマンスを実現するために、サポートされる同時エクスポート操作の数とエクスポートできるデータ量は、デフォルトの制限に設定されています。

サポートされるエクスポート制限

エクスポートされた PDF および Excel レポートには、選択されたフィルター条件の完全なグラフが含まれています。ただし、すべてのレポート形式の表形式データは、テーブル内の行数またはレコード数のデフォルト制限を超えると切り捨てられます。サポートされるレコードのデフォルト数は、レポート形式に基づいて定義されます。

Internet Information Services (IIS) の Director アプリケーション設定を構成することで、デフォルトの制限を変更できます。

レポート形式	サポートされるレコードのデフォルト数	DIRECTOR アプリケーション設定のフィールド	サポートされる最大レコード数
PDF	500	UI.ExportPdfDrilldownLimit	5000
エクセル	100,000	UI.ExportExcelDrilldownLimit	100,000
CSV	100,000 (「**セッション**」タブでは 10,000,000)	UI.ExportCsvDrilldownLimit	100,000

エクスポートできるレコード数の制限を変更するには、次のようにします。

1. IIS マネージャーコンソールを開きます。
2. デフォルトの Web サイトの下にある Director Web サイトに移動します。
3. 「**アプリケーション設定**」をダブルクリックします。
4. 必要に応じて、UI.ExportPdfDrilldownLimit、UI.ExportExcelDrilldownLimit、または UI.ExportCsvDrilldownLimit のフィールド設定を編集または追加します。

アプリケーション設定でこれらのフィールド値を追加すると、デフォルト値が上書きされます。

> **警告:**
>
> サポートされている最大レコード数を超えるフィールド値を設定すると、エクスポートのパフォーマンスに影響を与える可能性があり、サポートされていません。

エラー処理

このセクションでは、エクスポート操作中に発生する可能性のあるエラーの対処方法に関する情報を提供します。

- **Directorがタイムアウトしました**

このエラーは、ネットワークの問題、またはDirectorサーバーやMonitor Serviceでの高いリソース使用率が原因で発生する可能性があります。

デフォルトのタイムアウト期間は100秒です。Director Serviceのタイムアウト期間を長くするには、Internet Information Services (IIS) のDirectorアプリケーション設定で、**Connector.DataServiceContext.Timeout**フィールドの値を設定します。

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. **Application Settings**をダブルクリックします。
4. **Connector.DataServiceContext.Timeout**の値を編集します。

- **Monitorがタイムアウトしました**

このエラーは、ネットワークの問題、またはMonitor ServiceやSQLサーバーでの高いリソース使用率が原因で発生する可能性があります。

Monitor Serviceのタイムアウト期間を長くするには、Delivery Controllerで次のPowerShellコマンドを実行します。

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds &lt;timeout value>
```

- **同時エクスポートまたはプレビュー操作が最大数で進行中**

Directorはエクスポートまたはプレビューの1つのインスタンスをサポートします。「**Max concurrent Export or Preview operations ongoing**」エラーが発生した場合は、次のエクスポート操作を後でもう一度試してください。

同時実行できるエクスポートまたはプレビュー操作の数を増やすことは可能ですが、Directorのパフォーマンスに影響を与える可能性があり、サポートされていません。

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. 「**Application Settings**」をダブルクリックします。
4. 値「**UI.ConcurrentExportLimit**」を編集します。

- **「Directorのディスク容量不足」**

各エクスポート操作には、WindowsのTempフォルダーに最大2 GBのハードディスク容量が必要です。Directorサーバーの空き容量を確保するか、ハードディスク容量を追加してから、エクスポートを再試行してください。

ホットフィックスを監視する

特定のマシンVDA（物理またはVM）にインストールされているホットフィックスを表示するには、「**Machine Details**」ビューを選択します。

ユーザーマシンの電源状態を制御する

Directorで選択したマシンの状態を制御するには、電源制御オプションを使用します。これらのオプションは、シングルセッションOSマシンで利用できますが、マルチセッションOSマシンでは利用できない場合があります。

> **「注：」**：

> この機能は、物理マシンまたはリモートPCアクセスを使用するマシンでは利用できません。

コマンド	機能
再起動	VMの順序だった（ソフト）シャットダウンを実行し、VMを再起動する前に実行中のすべてのプロセスが個別に停止されます。たとえば、Directorで「起動に失敗しました」と表示されるマシンを選択し、このコマンドを使用して再起動します。
強制再起動	シャットダウン手順を最初に実行せずにVMを再起動します。このコマンドは、物理サーバーのプラグを抜き、再度差し込んで電源を入れるのと同じように機能します。
シャットダウン	VMの順序だった（ソフト）シャットダウンを実行します。実行中のすべてのプロセスが個別に停止されます。
強制シャットダウン	シャットダウン手順を最初に実行せずにVMをシャットダウンします。このコマンドは、物理サーバーのプラグを抜くのと同じように機能します。すべての実行中のプロセスが常にシャットダウンされるとは限らず、この方法でVMをシャットダウンするとデータが失われるリスクがあります。
一時停止	実行中のVMを現在の状態で一時停止し、その状態をデフォルトのストレージリポジトリのファイルに保存します。このオプションを使用すると、VMのホストサーバーをシャットダウンし、後で再起動した後、VMを再開して元の実行状態に戻すことができます。
再開	一時停止されたVMを再開し、元の実行状態に戻します。
起動	VMがオフの状態のときに起動します（コールドスタートとも呼ばれます）。

電源制御アクションが失敗した場合、アラートにマウスを重ねると、失敗の詳細を示すポップアップメッセージが表示されます。

マシンへの接続を防止する

適切な管理者がイメージのメンテナンス作業を実行している間、メンテナンスモードを使用して新しい接続を一時的に防止します。

マシンでメンテナンスモードを有効にすると、無効にするまで新しい接続は許可されません。ユーザーが現在ログオンしている場合、すべてのユーザーがログオフするとすぐにメンテナンスモードが有効になります。ログオフしないユーザーには、マシンが特定の時間にシャットダウンされることを通知するメッセージを送信し、電源制御を使用してマシンを強制的にシャットダウンします。

1. ユーザー詳細ビューからマシンを選択するか、フィルタービューでマシンのグループを選択します。
2. **メンテナンスモード**を選択し、オプションをオンにします。

ユーザーが割り当てられたデスクトップにメンテナンスモード中に接続しようとすると、デスクトップが利用できないことを示すメッセージが表示されます。メンテナンスモードを無効にするまで、新しい接続はできません。

アプリケーション分析

アプリケーションタブには、アプリケーションベースの分析が単一の統合ビューで表示され、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立ちます。サイトに公開されているすべてのアプリケーションの正常性と使用状況に関する貴重な洞察を得ることができます。プローブ結果、アプリケーションごとのインスタンス数、公開されたアプリケーションに関連する障害やエラーなどのメトリックが表示されます。詳細については、**アプリケーションのトラブルシューティング**のアプリケーション分析セクションを参照してください。

アラートと通知

アラートは、Directorのダッシュボードやその他の上位レベルのビューに、警告および重大なアラートシンボルとともに表示されます。アラートは**Premium**ライセンスサイトで利用できます。アラートは1分ごとに自動的に更新されます。オンデマンドでアラートを更新することもできます。

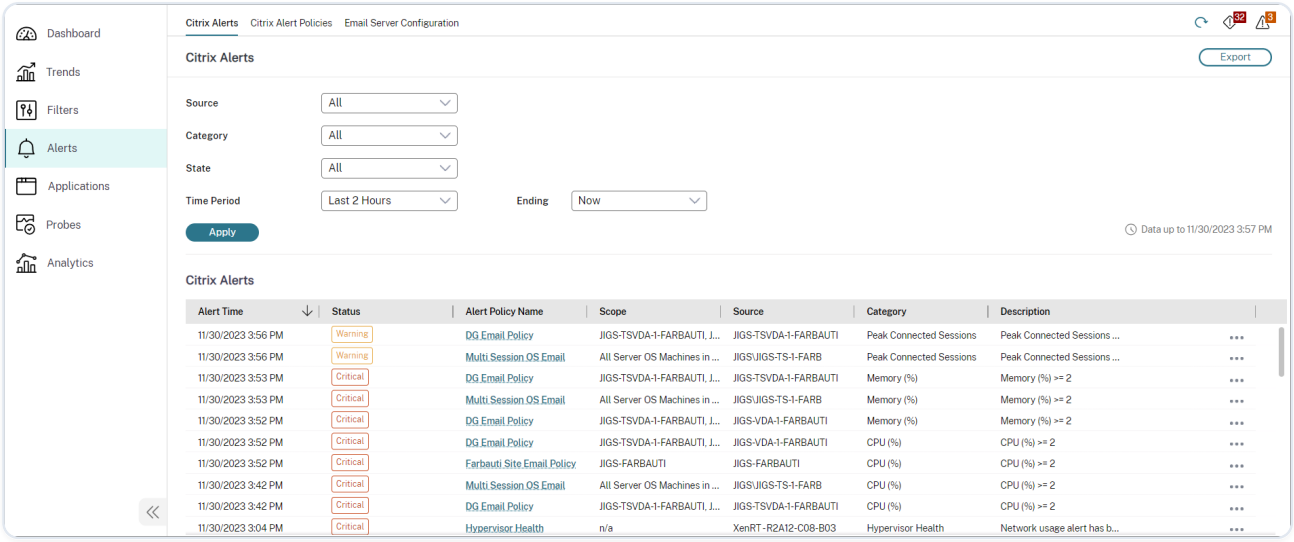
Directorアラート(/en-us/citrix-virtual-apps-desktops/2311/media/dir-alerts.png)

警告アラート（琥珀色の三角形）は、条件の警告しきい値に達したか、それを超えたことを示します。

重大なアラート（赤い円）は、条件の重大なしきい値に達したか、それを超えたことを示します。

アラートの詳細情報を表示するには、サイドバーからアラートを選択するか、サイドバーの下部にある**Go to Alerts**リンクをクリックするか、Directorページの上部から**Alerts**を選択します。

アラートビューでは、アラートをフィルター処理してエクスポートできます。たとえば、特定のデリバリーグループの過去1か月間の失敗したマルチセッションOSマシン、または特定のユーザーのすべてのアラートなどです。詳細については、「レポートのエクスポート」を参照してください。



Citrix®アラート

Citrixアラートは、Citrixコンポーネントから発信され、Directorで監視されるアラートです。Directorの**アラート** \> **Citrixアラートポリシー**でCitrixアラートを構成できます。構成の一部として、設定したしきい値を超過した場合に、個人やグループにメールで通知を送信するように設定できます。Citrixアラートの設定の詳細については、「アラートポリシーの作成」を参照してください。

> **注:**
>
> ファイアウォール、プロキシ、またはMicrosoft Exchange Serverがメールアラートをブロックしないことを確認してください。

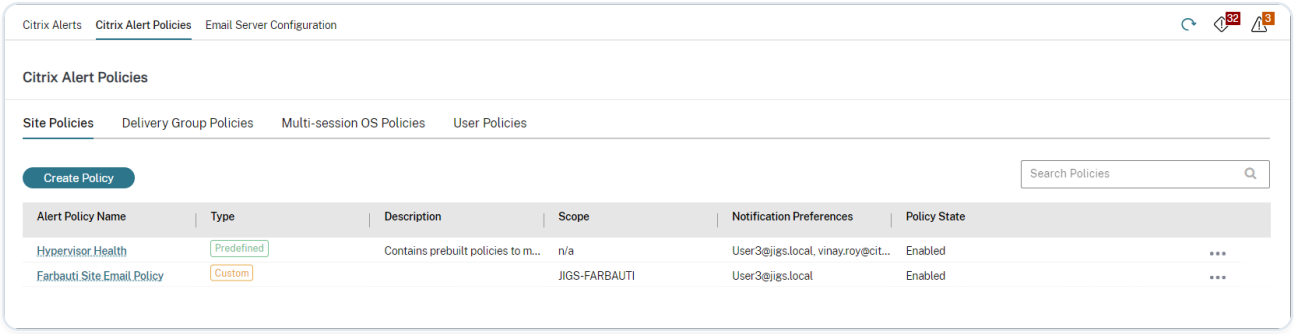
スマートアラートポリシー

デリバリーグループおよびマルチセッションOS VDAスコープ用に、事前定義されたしきい値を持つ一連の組み込みアラートポリシーが利用可能です。この機能には、Delivery Controllerバージョン7.18以降が必要です。組み込みアラートポリシーのしきい値パラメーターは、**アラート** \> **Citrixアラートポリシー**で変更できます。 これらのポリシーは、サイトに少なくとも1つのアラートター

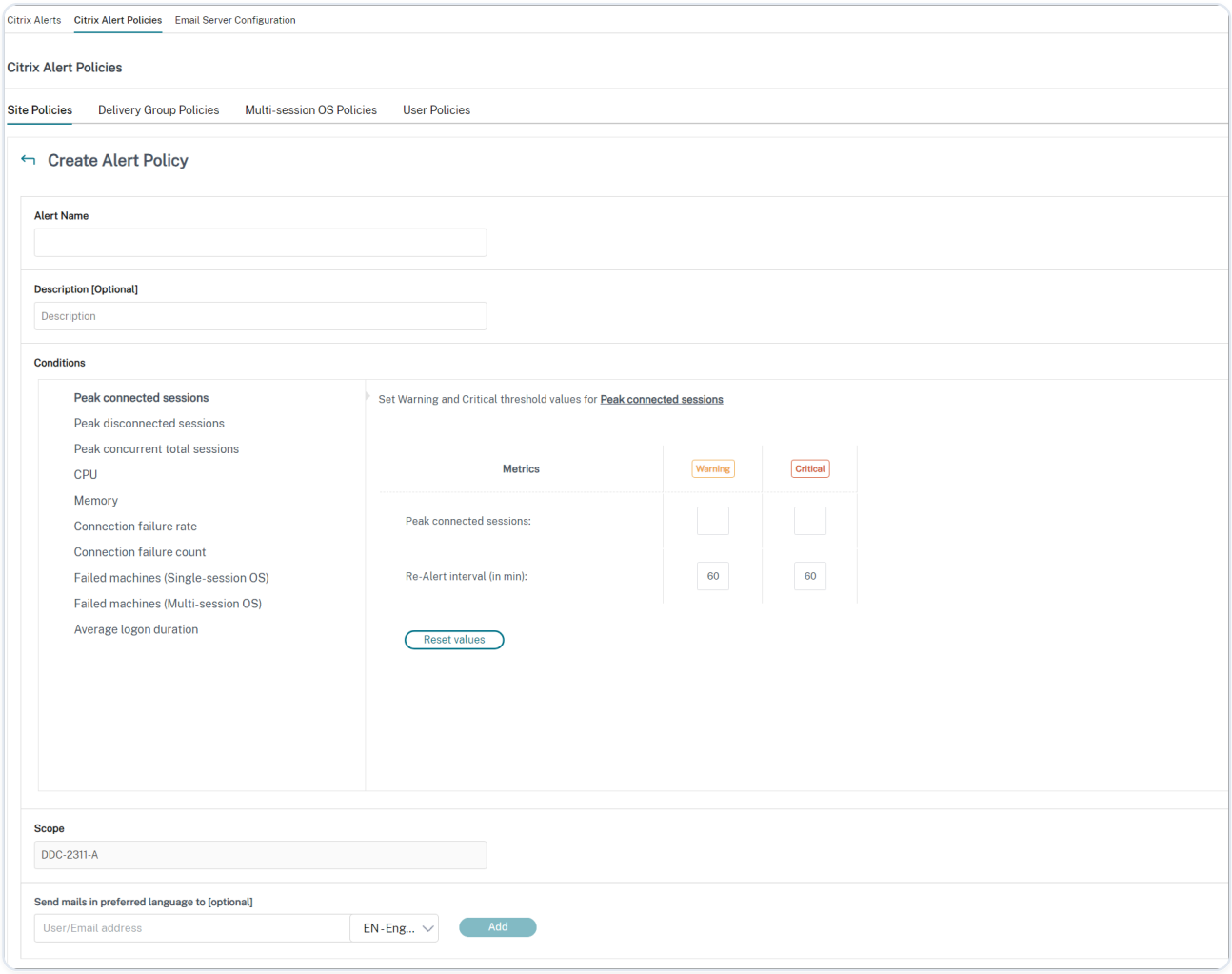
ゲット（デリバリーグループまたはマルチセッションOS VDA）が定義されている場合に作成されます。さらに、これらの組み込みアラートは、新しいデリバリーグループまたはマルチセッションOS VDAに自動的に追加されます。

Directorとサイトをアップグレードする場合、以前のDirectorインスタンスのアラートポリシーが引き継がれます。組み込みアラートポリシーは、Monitorデータベースに対応するアラートルールが存在しない場合にのみ作成されます。

組み込みのアラートポリシーのしきい値については、アラートポリシーの条件セクションを参照してください。



アラートポリシーを作成する



新しいアラートポリシーを作成するには、たとえば、特定のセッション数条件が満たされたときにアラートを生成するには、次の手順を実行します。

1. **アラート** > **Citrixアラートポリシー**に移動し、たとえば、マルチセッションOSポリシーを選択します。
2. **作成**をクリックします。
3. ポリシーに名前を付けて説明し、アラートがトリガーされるために満たす必要がある条件を設定します。たとえば、ピーク接続セッション、ピーク切断セッション、およびピーク同時合計セッションの警告数と重大数を指定します。警告値は重大値より大きくしてはいけません。詳細については、アラートポリシーの条件を参照してください。
4. 再アラート間隔を設定します。アラートの条件が引き続き満たされている場合、この時間間隔でアラートが再度トリガーされ、アラートポリシーで設定されている場合は、メール通知が生成されます。却下されたアラートは、再アラート間隔でメール通知を生成しません。
5. スコープを設定します。たとえば、特定のデリバリーグループに設定します。

6. 通知設定で、アラートがトリガーされたときに誰にメールで通知するかを指定します。アラートポリシーでメール通知設定を行うには、**メールサーバー構成**タブでメールサーバーを指定する必要があります。
7. **保存**をクリックします。

スコープに20以上のデリバリーグループが定義されたポリシーを作成すると、構成の完了に約30秒かかる場合があります。この間、スピナーが表示されます。

最大20の固有のデリバリーグループ（合計1000のデリバリーグループターゲット）に対して50を超えるポリシーを作成すると、応答時間が増加する可能性があります（5秒以上）。

アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、マシンパラメーターを使用して定義された誤ったデリバリーグループアラートがトリガーされる可能性があります。

> **注：** アラートポリシーを削除した後、そのポリシーによって生成されたアラート通知が停止するまでに最大30分かかる場合があります。

アラートポリシーの条件

以下に、アラートカテゴリ、アラートを軽減するための推奨アクション、および定義されている場合は組み込みポリシー条件を示します。組み込みのアラートポリシーは、アラートおよび再アラートの間隔が60分に設定されています。

接続セッションのピーク

- Directorのセッショントレンドビューで、接続セッションのピークを確認します。
- セッション負荷に対応する十分な容量があることを確認します。
- 必要に応じて新しいマシンを追加します

切断セッションのピーク

- Directorのセッショントレンドビューで、切断セッションのピークを確認します。
- セッション負荷に対応する十分な容量があることを確認します。
- 必要に応じて新しいマシンを追加します。
- 必要に応じて切断されたセッションをログオフします

同時実行セッションの合計ピーク

- Directorのセッショントレンドビューで、同時実行セッションのピークを確認します。

- セッション負荷に対応する十分な容量があることを確認します。
- 必要に応じて新しいマシンを追加します。
- 必要に応じて切断されたセッションをログオフします。

CPU

CPU使用率の割合は、プロセスを含むVDA全体のCPU消費量を示します。個々のプロセスによるCPU使用率の詳細については、対応するVDAの**マシン詳細**ページから確認できます。

- **［マシン詳細］>［履歴使用率の表示］>［上位10プロセス］** に移動し、CPUを消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、将来的に追加のCPUリソースを追加します。

> **注：**
>
> ポリシー設定の**リソース監視を有効にする**は、VDAがインストールされたマシンでのCPUおよびメモリパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリ条件のアラートはトリガーされません。詳細については、「監視ポリシー設定」を参照してください。

> **スマートポリシー条件：**
>
> - **スコープ：** デリバリーグループ、マルチセッションOSスコープ
> - **しきい値：** 警告 - 80%、重大 - 90%

メモリ

メモリ使用率の割合は、プロセスを含むVDA全体のメモリ消費量を示します。個々のプロセスによるメモリ使用量の詳細については、対応するVDAの**マシン詳細**ページから確認できます。

- 「**マシン詳細 > 履歴利用状況の表示 > 上位10プロセス**」に移動し、メモリを消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。

- すべてが期待どおりに機能している場合は、将来的に追加のメモリを追加します。

> **注：**
>
> ポリシー設定「**リソース監視を有効にする**」は、VDAがインストールされたマシン上のCPUおよびメモリのパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳細については、「監視ポリシー設定」を参照してください。

> **スマートポリシーの条件：**

- **スコープ：** デリバリーグループ、マルチセッションOSスコープ
- **しきい値：** 警告 - 80%、重大 - 90%

接続失敗率

過去1時間の接続失敗の割合。

- 試行された接続の総数に対する失敗の総数に基づいて計算されます。
- 構成ログから記録されたイベントについては、Directorの接続失敗トレンドビューを確認してください。
- アプリケーションまたはデスクトップに到達可能かどうかを判断します。

接続失敗数

過去1時間における接続失敗の数。

- 構成ログから記録されたイベントについて、Directorの接続失敗トレンドビューを確認します。
- アプリケーションまたはデスクトップに到達可能かどうかを判断します。

ICA® RTT (平均)

平均ICAラウンドトリップ時間。

- ICA RTTの内訳についてCitrix ADMを確認し、根本原因を特定します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、Directorのユーザー詳細ビューでICA RTTと遅延を確認し、ネットワークの問題か、アプリケーションまたはデスクトップの問題かを判断します。

ICA RTT (セッション数)

しきい値のICAラウンドトリップ時間を超えるセッションの数。

- 高いICA RTTを持つセッションの数についてCitrix ADMを確認します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 5セッション以上で300ミリ秒、重大 - 10セッション以上で400ミリ秒

ICA RTT (セッションの割合)

平均ICAラウンドトリップ時間を超えるセッションの割合。

- ICA RTTが高いセッションの数については、Citrix ADMを確認してください。詳細については、Citrix ADM ドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定してください。

ICA RTT (ユーザー)

指定されたユーザーによって起動されたセッションに適用されるICAラウンドトリップ時間。ICA RTTが少なくとも1つのセッションでしきい値を超えた場合、アラートがトリガーされます。

失敗したマシン（シングルセッションOS）

失敗したシングルセッションOSマシンの数。Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で障害が発生する可能性があります。

- Citrix Scout診断を実行して、根本原因を特定してください。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 1、重大 - 2

失敗したマシン (マルチセッションOS)

失敗したマルチセッションOSマシンの数。Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で障害が発生する可能性があります。

- Citrix Scout診断を実行して、根本原因を特定してください。

スマートポリシーの条件:

- **スコープ:** デリバリーグループ、マルチセッションOSスコープ
- **しきい値:** 警告 - 1、重大 - 2

失敗したマシン (%)

デリバリーグループ内の失敗したシングルセッションおよびマルチセッションOSマシンの割合で、失敗したマシンの数に基づいて計算されます。このアラート条件では、デリバリーグループ内の失敗したマシンの割合としてアラートしきい値を構成でき、30秒ごとに計算されます。 失敗は、Directorダッシュボードおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。根本原因を特定するには、Citrix Scout診断を実行します。詳細については、「ユーザーの問題のトラブルシューティング」を参照してください。

平均ログオン時間

過去1時間に発生したログオンの平均ログオン時間。

- Directorダッシュボードでログオン期間に関する最新のメトリックを確認します。短期間に多数のユーザーがログオンすると、ログオン期間が増加する可能性があります。
- ログオンのベースラインと内訳を確認して、原因を絞り込みます。詳細については、「ユーザーログオンの問題の診断」を参照してください。

  スマートポリシー条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 45秒、重大 - 60秒

ログオン時間 (ユーザー)

過去1時間に発生した、指定されたユーザーのログオンのログオン時間。

ロードエバリュエーターインデックス

過去5分間のロードエバリュエーターインデックスの値。

- ピーク負荷（最大負荷）が発生している可能性のあるマルチセッションOSマシンについて、Directorで確認します。ダッシュボード（障害）とトレンドの負荷評価インデックスレポートの両方を確認します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 80%、クリティカル - 90%

Webhook を使用してアラートポリシーを構成する

電子メール通知とは別に、Webhook を使用してアラートポリシーを構成できます。

注: この機能には、Delivery Controller バージョン 7.11 以降が必要です。

PowerShell コマンドレットを使用して、HTTP コールバックまたは HTTP POST でアラートポリシーを構成できます。これらは Webhook をサポートするように拡張されています。

新しいOctobluワークフローの作成と対応するWebhook URLの取得については、Octoblu Developer Hubを参照してください。

新しいアラートポリシーまたは既存のポリシーの Webhook URL を構成するには、次の PowerShell コマンドレットを使用します。

Webhook URLを使用して新しいアラートポリシーを作成します:

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -Description
<Policy description> -Enabled $true -Webhook <Webhook URL>
```

既存のアラートポリシーに Webhook URL を追加する:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

PowerShellコマンドに関するヘルプについては、PowerShellヘルプを使用してください（例：）。

```
Get-Help  <Set-MonitorNotificationPolicy>
```

アラートポリシーから生成された通知は、Webhook URL への POST 呼び出しで Webhook をトリガーします。POST メッセージには、JSON 形式の通知情報が含まれています。

```
{"NotificationId" : \<Notification Id\>,



"Target" : \<Notification Target Id\>,



"Condition" : \<Condition that was violated\>,
```

```
"Value" : \<Threshold value for the Condition\>,

"Timestamp": \<Time in UTC when notification was generated\>,

"PolicyName": \<Name of the Alert policy\>,

"Description": \<Description of the Alert policy\>,

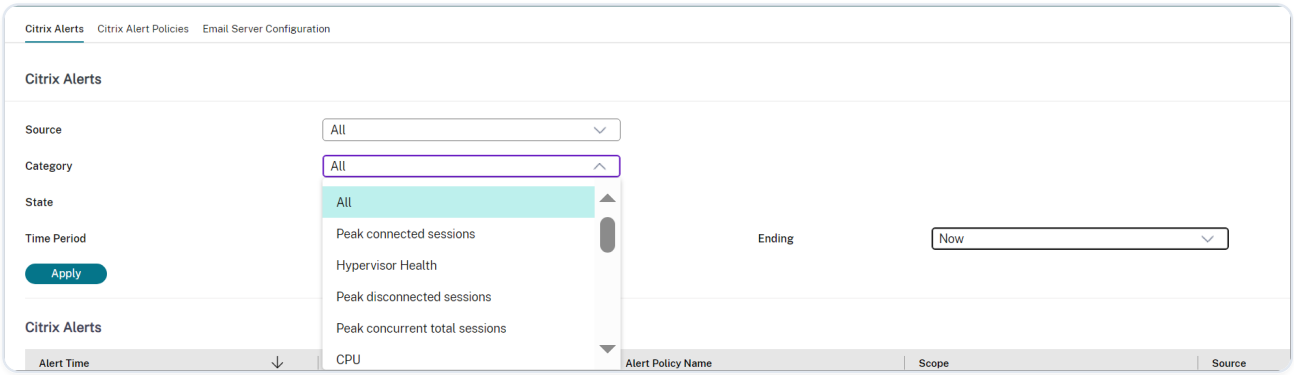
"Scope" : \<Scope of the Alert policy\>,

"NotificationState": \<Notification state critical, warning, healthy or
dismissed\>,

"Site" : \<Site name\>}
```

ハイパーバイザーアラートの監視

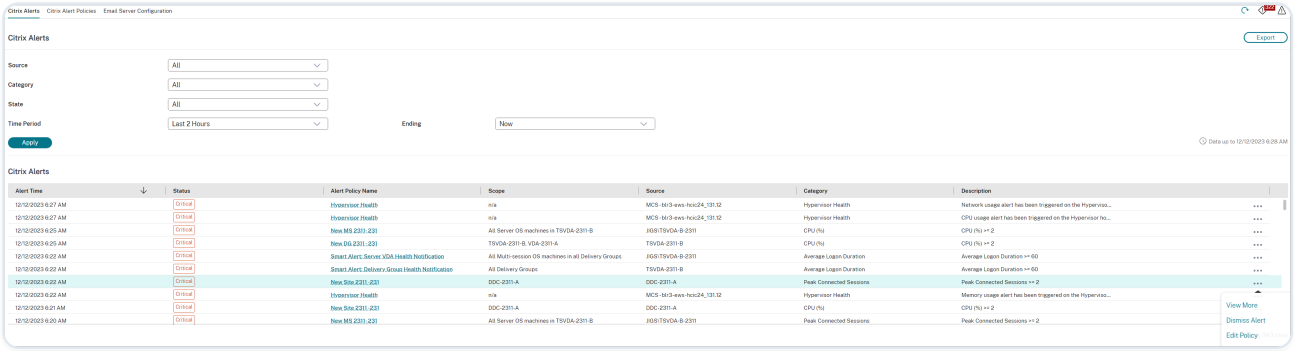
Director はハイパーバイザーの健全性を監視するためのアラートを表示します。XenServer® および VMware vSphere からのアラートは、ハイパーバイザーのパラメーターと状態の監視に役立ちます。ホストのクラスターまたはプールが再起動されたり利用できなくなったりした場合にアラートを提供するために、ハイパーバイザーへの接続ステータスも監視されます。



ハイパーバイザーアラートを受信するには、Web Studio でホスティング接続が作成されていることを確認してください。詳細については、「接続とリソース」を参照してください。ハイパーバイザーアラートについて監視されるのは、これらの接続のみです。

これらのアラートは、しきい値に達するか、それを超えると表示されます。ハイパーバイザーアラートには次のものがあります。

- 致命的 — ハイパーバイザーアラームポリシーの致命的なしきい値に達したか、それを超えた場合
- 警告 — ハイパーバイザーアラームポリシーの警告しきい値に達したか、それを超えた場合
- 却下済み — アラートがアクティブなアラートとして表示されなくなった場合



この機能には、Delivery Controller™ バージョン 7 1811 以降が必要です。Director の古いバージョンをサイト 7 1811 以降で使用している場合、ハイパーバイザーアラートの数のみが表示されます。アラートを表示するには、Director をアップグレードする必要があります。

次の表は、ハイパーバイザーアラートのさまざまなパラメーターと状態について説明しています。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
CPU使用率	ゼノサーバー、ブイエムウェア ブイスフィア	ハイパーバイザー	CPU使用率アラートのしきい値に達したか、超過した	アラートのしきい値はハイパーバイザーで構成

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
				する必要があります。
メモリ使用率	ゼノサーバー、ブイエムウェアブイスフィア	ハイパーバイザー	メモリ使用率アラートのしきい値に達したか、超過した	アラートのしきい値はハイパーバイザーで構成する必要があります。
ネットワーク使用率	ゼノサーバー、ブイエムウェアブイスフィア	ハイパーバイザー	ネットワーク使用率アラートのしきい値に達したか、超過した	アラートのしきい値はハイパーバイザーで構成する必要があります。
ディスク使用量	ヴイエムウェアヴイスフィア	ハイパーバイザー	ディスク使用量アラートのしきい値に達したか、超過しました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ホスト接続または電源状態	ヴイエムウェアヴイスフィア	ハイパーバイザー	ハイパーバイザーホストが再起動されたか、利用できません	アラートはVMware vSphereに組み込まれています。追加の構成は不要です。
ハイパーバイザー接続が利用できません	ゼノサーバー、ヴイエムウェアヴイスフィア	デリバリーコントローラー	ハイパーバイザー（プールまたはクラスター）への接続が失われたか、電源がオフになったか、再起動されました。このアラートは、接続が利用できない間、1	アラートはDelivery Controllerに組み込まれています。追加の構成は不要です。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
			時間ごとに生成されます。	

注記：

アラートの設定に関する詳細については、Citrix XenCenter Alertsを参照するか、VMware vCenter Alertsのドキュメントを確認してください。

電子メール通知の設定は、**Citrix Alerts Policy > Site Policy > Hypervisor Health**で構成できます。ハイパーバイザーアラートポリシーのしきい値条件は、Directorからではなく、ハイパーバイザーからのみ構成、編集、無効化、または削除できます。ただし、電子メール設定の変更やアラートの解除はDirectorで行うことができます。役割にインフラストラクチャの監視が含まれない場合は、アラートを無効にできます。

重要：

- ハイパーバイザーによってトリガーされたアラートは、Directorで取得され表示されます。ただし、ハイパーバイザーアラートのライフサイクル/状態の変更はDirectorには反映されません。
- ハイパーバイザーコンソールで正常、解除、または無効化されたアラートは、Directorに表示され続け、明示的に解除する必要があります。
- Directorで解除されたアラートは、ハイパーバイザーコンソールでは自動的に解除されません。

障害のトラブルシューティングのためにデータをフィルタリングする

ダッシュボードの数値をクリックするか、フィルターメニューから定義済みフィルターを選択すると、選択したマシンまたは障害の種類に基づいてデータを表示するフィルタービューが開きます。

定義済みフィルターは編集できませんが、定義済みフィルターをカスタムフィルターとして保存し、後で変更することができます。また、すべてのデリバリーグループにわたるマシン、接続、セッション、およびアプリケーションインスタンスのカスタムフィルタービューを作成することもできます。

1. ビューを選択します:

   - **マシン**。シングルセッションOSマシンまたはマルチセッションOSマシンを選択します。これらのビューには、構成されているマシンの数が表示されます。マルチセッションOSマシンのタブには、ロード評価インデックスも含まれており、これはパフォーマンスカウンターの分布を示し、リンクにカーソルを合わせるとセッション数のツールヒントが表示されます。
   - **セッション**。セッションビューからセッション数を確認することもできます。アイドル時間測定を使用して、しきい値期間を超えてアイドル状態になっているセッションを特定します。**関連ユーザー**をクリックすると、そのユーザーのActivity Managerが開きます。**エンドポイント**名をクリックすると、そのエンドポイントのActivity Managerが開きます。**詳細表示**をクリックすると、それぞれ**ユーザー詳細**または**エンドポイント詳細**ページが開きます。詳細については、「ユーザー詳細」を参照してください。
   - **接続**。過去60分、過去24時間、過去7日間など、さまざまな期間で接続をフィルターします。
   - **アプリケーションインスタンス**。このビューには、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスのプロパティが表示されます。マルチセッションOSのVDA上のアプリケーションインスタンスでは、セッションアイドル時間測定が利用可能です。

   注:

   Windows 10 1809コンピューターにインストールされたVDAでデスクトップセッションを起動した場合、DirectorのActivity Managerでは、Microsoft EdgeとOfficeがアクティブに実行されているアプリケーションとして表示されることがありますが、実際にはバックグラウンドでのみ実行されています。

2. **フィルター条件**で、基準を選択します。
3. 必要に応じて、各ビューの追加タブを使用してフィルターを完了します。
4. 必要に応じて、追加の列を選択してさらにトラブルシューティングを行います。
5. フィルターを保存して名前を付けます。

6. 複数のDirectorサーバーからフィルターにアクセスするには、それらのサーバーからアクセス可能な共有フォルダーにフィルターを保存します。

   - 共有フォルダーには、Directorサーバー上のアカウントに対する変更権限が必要です。
   - Directorサーバーは、共有フォルダーにアクセスできるように構成する必要があります。構成するには、**IIS マネージャー**を実行します。**サイト \> 既定の Web サイト \> Director\ > アプリケーション設定**で、**Service.UserSettingsPath**設定を共有フォルダーのUNCパスを反映するように変更します。

7. 後でフィルターを開くには、**フィルター**メニューからフィルターの種類（マシン、セッション、接続、またはアプリケーションインスタンス）を選択し、保存されたフィルターを選択します。
8. **エクスポート**をクリックして、データをCSV形式ファイルにエクスポートします。最大100,000レコードのデータをエクスポートできます。この機能は、Delivery Controller™バージョン1808以降で利用可能です。
9. 必要に応じて、**マシン**または**接続**ビューでは、フィルターされたリストで選択したすべてのマシンに対して電源制御を使用します。セッションビューでは、セッション制御またはメッセージ送信オプションを使用します。
10. **マシン**ビューと**接続**ビューで、失敗したマシンまたは接続の**失敗理由**をクリックすると、失敗の詳細な説明と、その失敗のトラブルシューティングに推奨されるアクションが表示されます。マシンおよび接続の失敗理由と推奨されるアクションは、Citrix Director の失敗理由とトラブルシューティングで確認できます。
11. **マシン**ビューで、マシン名リンクをクリックすると、対応する**マシン詳細**ページに移動します。このページには、マシンの詳細が表示され、電源制御が提供され、CPU、メモリ、ディスク監視、およびGPU監視グラフが表示されます。また、**履歴使用率の表示**をクリックすると、マシンのリソース使用率の傾向を確認できます。詳細については、マシンのトラブルシューティングを参照してください。
12. **アプリケーションインスタンス**ビューで、しきい値期間より長い**アイドル時間**に基づいて並べ替えまたはフィルター処理を行います。終了するアイドル状態のアプリケーションインスタンスを選択します。アプリケーションインスタンスのログオフまたは切断は、同じセッション内のすべてのアクティブなアプリケーションインスタンスを終了します。詳細については、アプリケーションのトラブルシューティングを参照してください。アプリケーションインスタンスフィルターページとセッションフィルターページでのアイドル時間測定は、Director、Delivery Controller、およびVDAがバージョン7.13以降の場合に利用可能です。

注: Web Studioでは、異なるユーザーまたはユーザーグループに対して複数のデスクトップ割り当てルール（DAR）をデリバリーグループ内の単一のVDAに割り当てることができます。StoreFront™は、ログインユーザーのDARに従って、対応する表示名を持つ割り当てられたデスクトップを表示します。ただし、DirectorはDARをサポートしておらず、ログインユーザーに関係なくデリバリーグループ名を使用して割り当てられたデスクトップを表示します。その結果、Directorで特定のデスクトップをマシンにマッピングすることはできません。StoreFrontに表示される割り当てられたデスクトップをDirectorに表示されるデリバリーグループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq "\<Name
on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

サイト全体の履歴トレンドを監視する

トレンドビューは、以下のパラメータについて、各サイトの履歴トレンド情報にアクセスします。

- セッション
- 接続障害
- マシン障害
- ログオンパフォーマンス
- 負荷評価
- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームイン・ドリルダウン機能を使用すると、期間をズームイン（グラフ内のデータポイントをクリック）してトレンドチャートをナビゲートし、トレンドに関連する詳細を確認できます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択してください。期間の利用可能性は、Directorの展開によって次のように異なります。

- 最大1年間（365日間）のトレンドレポートは、Premiumライセンスサイトで利用できます。
- 最大1か月間（31日間）のトレンドレポートは、Advancedライセンスサイトで利用できます。
- 最大7日間のトレンドレポートは、PremiumおよびAdvanced以外のライセンスサイトで利用できます。

注:

- すべてのDirector展開において、セッション、障害、ログオンパフォーマンスのトレンド情報は、期間が「先月」（**現在まで**）またはそれより短い期間に設定されている場合、グラフとテーブルとして利用できます。カスタム終了日を指定した「先月」または「昨年」として選択された期間の場合、トレンド情報はグラフとして利用でき、テーブルとしては利用できません。
- Monitor Serviceのグルーミング保持値がトレンドデータの可用性を制御します。デフォルト値については、データ粒度と保持を参照してください。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。
- IIS Managerの以下のパラメーターは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定されている特定のメトリックのグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能なトレンド

セッションの傾向を表示: 「**セッション**」タブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

セッションの自動再接続列には、セッション内の自動再接続の数が表示されます。自動再接続は、セッションの信頼性ポリシーまたはクライアントの自動再接続ポリシーが有効な場合に有効

になります。エンドポイントでネットワークの中断が発生した場合、以下のポリシーが有効になります。

- セッションの信頼性が有効になり (デフォルトで3分間)、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- クライアントの自動再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性やクライアントの自動再接続、タイムスタンプ、エンドポイントIP、Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントのタイムスタンプの降順でソートされます。この機能は、Windows用Citrix Workspaceアプリ、Mac用Citrix Workspaceアプリ、Windows用Citrix Receiver、およびMac用Citrix Receiverで利用できます。この機能には、Delivery Controller™バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続について詳しくは、セッションを参照してください。

ポリシーについて詳しくは、クライアントの自動再接続ポリシー設定およびセッションの信頼性ポリシー設定を参照してください。

自動再接続データがDirectorに表示されない場合があるのは、以下の理由によります。

- Workspaceアプリが自動再接続データをVDAに送信していません。
- VDAが監視サービスにデータを送信していません。
- Delivery Controllers は、対応するセッションを持っていない可能性があるため、VDA ペイロードを破棄します。

注:

特定の Citrix Gateway ポリシーが設定されている場合、クライアント IP アドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** 「障害」タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示する: シングルセッション OS マシン障害タブまたはマルチセッション OS マシンタブから、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のマシン障害に関する詳細情報を含むグラフを表示します。

ログオンパフォーマンスの傾向を表示する: ログオンパフォーマンスタブから、デリバリーグループと期間を選択すると、サイト全体のユーザーログオン時間の詳細情報と、ログオン数がパフォーマンスに影響するかどうかを示すグラフが表示されます。このビューには、ブローカー処理時間やVM起動時間など、ログオンフェーズの平均期間も表示されます。 このデータはユーザーログオンに特化したものであり、切断されたセッションから再接続しようとしているユーザーは含まれません。 グラフの下の表には、ユーザーセッションごとのログオン期間が表示されます。表示する列を選択し、任意の列でレポートを並べ替えることができます。 詳細については、「ユーザーログオンの問題の診断」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/user-issues/user-logon.html)

負荷評価の傾向を表示する: 負荷評価インデックスタブから、マルチセッション OS マシン間で分散される負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のマルチセッション OS マシン、マルチセッション OS マシン（デリバリーグループ内のマルチセッション OS マシンが選択されている場合にのみ利用可能）、および範囲が含まれます。

ホストされているアプリケーションの使用状況を表示する: この機能の利用可否は、組織のライセンスによって異なります。 **キャパシティ管理**タブから、**ホストされているアプリケーションの使用状況**タブを選択します。デリバリーグループと期間を選択して、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示す表を表示します。アプリケーションベースの使用状況の表から、特定のアプリケーションを選択して詳細と、そのアプリケーションを使用している、または使用したユーザーのリストを表示できます。

シングルセッションおよびマルチセッション OS の使用状況を表示する: ビューには、サイト別およびデリバリーグループ別のシングルセッション OS の使用状況が表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 ビューには、サイト別、デリバリーグループ別、およびマシン別のマルチセッション OS の使用状況も表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示する: マシン使用状況タブから、**シングルセッション OS マシンまたはマルチセッション OS マシン**を選択して、VM 使用状況のリアルタイムビューを取得し、サイトのキャパシティニーズを迅速に評価できるようにします。 シングルセッション OS の可用性 - サイト全体または特定のデリバリーグループの可用性別に、シングルセッション OS マシン (VDI) の現在の状態を表示します。 マルチセッション OS の可用性 - サイト全体または特定のデリバリーグループの可用性別に、マルチセッション OS マシンの現在の状態を表示します。

> **注:** に表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

> **リソース使用率を表示する: リソース使用率**タブから、**シングルセッション OS マシンまたはマルチセッション OS マシン**を選択して、各 VDI マシンの CPU およびメモリ使用量、IOPS およびディスク遅延に関する履歴傾向データを取得し、より適切なキャパシティプランニングに役立てます。 この機能には、Delivery Controllers および VDA **バージョン 7.11** 以降が必要です。 グラフには、平均 CPU、平均メモリ、平均 IOPS、ディスク遅延、およびピーク時の同時セッションのデータが表示されます。マシンにドリルダウンして、CPU を消費している上位 10 プロセスのデータとグラフを表示できます。

デリバリーグループと期間でフィルターします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去 2 時間、24 時間、7 日間、1 か月、および 1 年間で利用できます。平均 IOPS およびディスク遅延のグラフは、過去 24 時間、1 か月、および 1 年間で利用できます。

> **注:**
>
> - 履歴マシン使用率ページの「上位 10 プロセス」テーブルでデータを収集して表示するには、監視ポリシー設定の **プロセス監視を有効にする** を **許可** に設定する必要があります。このポリシーは、デフォルトでは **禁止** に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、**リソース監視を有効にする** ポリシー設定を使用して無効にできます。グラフの下の表には、マシンごとのリソース使用率データが表示されます。詳細については、「監視ポリシー設定」を参照してください。
> - 平均IOPSは日次平均を示します。ピークIOPSは、選択した時間範囲におけるIOPS平均の最高値として計算されます。(IOPS平均とは、VDAでその時間に収集されたIOPSの時間ごとの平均です)。

- マシンのドリルダウンには、平均CPU使用率または平均メモリ使用率が1%を超えるプロセスが一覧表示されます。これは、場合によっては10未満のプロセスしか表示されない可能性があることを意味します。

ネットワーク分析データの表示: この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controllerの**バージョン7.11**以降が必要です。

ネットワークタブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、デスクトップのコンテキストビューが提供されます。この機能により、DirectorはCitrix ADMからのHDX Insightレポートを通じて、展開環境におけるICAトラフィックの詳細な分析を提供します。詳細については、「ネットワーク分析の構成」を参照してください。

アプリケーション障害の表示: アプリケーション障害タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

この機能には、Delivery ControllerおよびVDA **バージョン7.15**以降が必要です。Windows Vista以降を実行するシングルセッションOS VDA、およびWindows Server 2008以降を実行するマルチセッションOS VDAがサポートされています。 詳細については、「履歴アプリケーション障害監視」を参照してください。

デフォルトでは、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳細については、「監視ポリシー設定」を参照してください。

プローブ結果の表示: プローブ結果タブには、構成ページでプローブ用に構成されたアプリケーションおよびデスクトップのプローブ結果が表示されます。ここでは、障害が発生した起動の段階が記録されます。

詳細については、「アプリケーションおよびデスクトップのプローブ」を参照してください。

カスタマイズされたレポートの作成: カスタムレポートタブは、監視データベースからのリアルタイムデータと履歴データを含むカスタムレポートを表形式で生成するためのユーザーインターフェイスを提供します。

この機能には、Delivery Controllers **バージョン7.12**以降が必要です。

以前に保存したカスタムレポートクエリのリストから、**実行してダウンロード**をクリックしてレポートをCSV形式でエクスポートしたり、**ODataをコピー**をクリックして対応するODataクエリをコピーして共有したり、**編集**をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できま

す。マシン、デリバリーグループ、期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューにはレポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存されたクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、ODataクエリオプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは後で実行するために保存できます。

> **注:** ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされておらず、英語で表示されます。

> グラフ上のフラグアイコンは、特定の時間範囲における重要なイベントまたはアクションを示します。フラグの上にマウスを移動し、クリックするとイベントまたはアクションが一覧表示されます。

> **注:**
>
> - HDX™接続ログオンデータは、VDA 7より前のバージョンでは収集されません。以前のVDAの場合、チャートデータは0と表示されます。
> - Citrix Studioで削除されたデリバリーグループは、それらに関連するデータが整理されるまで、Directorのトレンドフィルターで選択可能です。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータが表示されません。
> - アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの**リソース使用率と負荷評価インデックス**テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。

Autoscale管理マシンの監視

Autoscaleは、デリバリーグループ内の登録済みマルチセッションおよびシングルセッションOSマシンすべてのプロアクティブな電源管理を可能にする電源管理機能です。Web Studioで、選択したデリバリーグループのAutoscaleを構成できます。詳しくは、「Autoscale」(/ja-jp/citrix-virtual-

apps-desktops/2311/manage-deployment/autoscale.html)を参照してください。 Directorを使用して、Autoscaleが有効なマシンの主要なメトリックを監視できます。

マシン使用状況

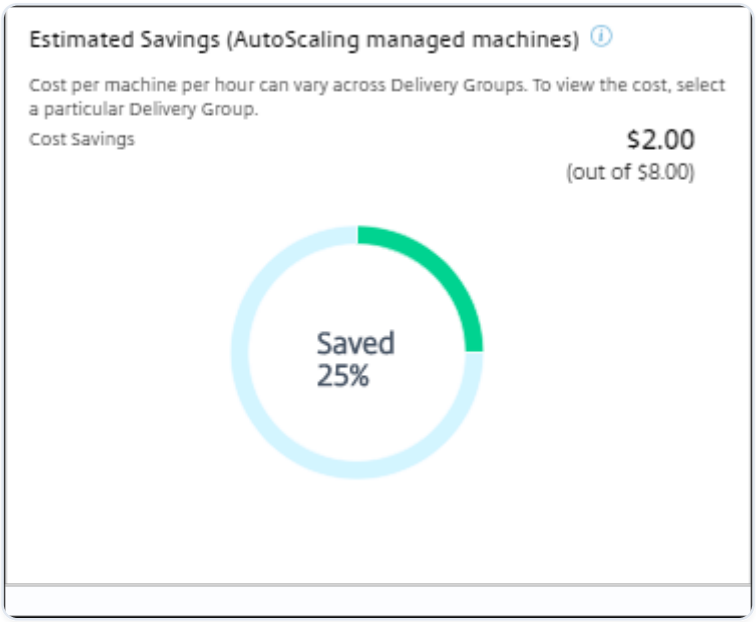
マシンの使用状況ページには、選択したデリバリーグループと期間において電源がオンになっているAutoscale対応のマルチセッションおよびシングルセッションOSマシンの総数が表示されます。このメトリックは、デリバリーグループ内のマシンの実際の使用状況を示します。 **シングルセッションOSマシン**タブまたは**マルチセッションOSマシン**タブから、デリバリーグループと期間を選択します。

このグラフには、次のメトリックが表示されます:

- **電源オンのマシン** - 電源がオンになっているAutoscale対応マシンの数
- **登録済みマシン** - 登録済みのマルチセッションまたはシングルセッションOSマシンの数
- **メンテナンス中のマシン** - メンテナンスモードがオンになっているマルチセッションまたはシングルセッションOSマシンの数

推定節約額

マシンの使用状況ページには、選択したデリバリーグループでAutoscaleを有効にすることで達成された推定コスト削減額も表示されます。



推定節約額は、**デリバリーグループの編集** > **Autoscale**で構成されている、マシン1台あたりの1時間あたりの節約額（米ドル）の割合として計算されます。マシンあたりの節約額の構成について詳しくは、「Autoscale」(/ja-jp/citrix-virtual-apps-desktops/2311/manage-deployment/autoscale.html)を参照してください。

すべてのデリバリーグループを選択すると、すべてのデリバリーグループにおける推定節約額の平均値が表示されます。

推定節約額は、管理者が既存のインフラストラクチャを統合し、容量を計画して、最大の節約と利用率を達成するのに役立ちます。

マシンとセッションのアラート通知

Directorダッシュボードには、アラート通知が表示されます。これらの通知はさらにドリルダウンできます。アラートの詳細は、**アラート**ページに表示されます。

- デリバリーグループでアラートポリシーを作成するには、**アラート** > **Citrixアラートポリシー** > **デリバリーグループポリシー**に移動します。
- ここでは、次の警告および重大なしきい値を設定できます。
  - 失敗したマシン（シングルセッションOS）および失敗したマシン（マルチセッションOS），
  - デリバリーグループ内のピーク接続セッション数、ピーク切断セッション数、およびピーク同時合計セッション数。
- デリバリーグループ内の対応するメトリックがしきい値に達すると、アラートが生成されます。

アラートポリシーの条件と新しいアラートポリシーの作成に関する詳細については、「アラートと通知」を参照してください。

マシンのステータス

- **フィルター** > **マシン**には、すべてのマシンの電源状態が表形式で表示されます。特定のデリバリーグループでフィルターできます。
- **フィルター** > **セッション**には、マシン名でフィルターして、関連するセッションとそのリアルタイムステータスが表示されます。
- **トレンド** > **セッション**で、デリバリーグループと期間を選択すると、セッションとその関連メトリックのトレンドが表示されます。

詳細については、「障害のトラブルシューティングのためのデータのフィルター」を参照してください。

負荷評価のトレンド

トレンド > **負荷評価インデックス**ページには、マルチセッションOSマシン間で分散される負荷に関する詳細情報を含むグラフが表示されます。このグラフのフィルターオプションには、デリバ

リーグループまたはデリバリーグループ内のマルチセッションOSマシン、マルチセッションOSマシン（デリバリーグループ内のマルチセッションOSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。負荷評価インデックスは、合計CPU、メモリ、ディスク、またはセッションの割合として表示され、最後の間隔での接続ユーザー数と比較して示されます。

展開のトラブルシューティング

アプリケーションのトラブルシューティング

アプリケーション分析

「**アプリケーション**」ビューには、アプリケーションベースの分析が単一の統合ビューで表示され、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立ちます。サイトで公開されているすべてのアプリケーションの正常性と使用状況に関する貴重な洞察を得ることができます。デフォルトビューは、最も多く実行されているアプリケーションを特定するのに役立ちます。 この機能には、Delivery Controllersバージョン7.16以降およびVDAバージョン7.15以降が必要です。

アプリケーションページ(/en-us/citrix-virtual-apps-desktops/2311/media/dir-app-analytics.png)

「**プローブ結果**」列には、過去24時間で実行されたアプリケーションプローブの結果が表示されます。プローブ結果リンクをクリックすると、「**傾向**」\>「**アプリケーションプローブ結果**」ページで詳細を確認できます。アプリケーションプローブの構成方法の詳細については、「アプリケーションおよびデスクトッププローブ」を参照してください。

「**インスタンス**」列には、アプリケーションの使用状況が表示されます。これは、現在実行中のアプリケーションインスタンスの数（接続済みインスタンスと切断済みインスタンスの両方）を示します。さらにトラブルシューティングを行うには、「**インスタンス**」フィールドをクリックして、対応する「**アプリケーションインスタンス**」フィルターページを表示します。ここで、ログオフまたは切断するアプリケーションインスタンスを選択できます。

> **注:**
>
> カスタムスコープ管理者向けに、Directorはアプリケーショングループの下に作成されたアプリケーションインスタンスを表示しません。すべてのアプリケーションインスタンスを表示するには、フル管理者である必要があります。詳細については、Knowledge Centerの記事CTX256001を参照してください。

「**アプリケーション障害**」列と「**アプリケーションエラー**」列を使用して、サイトで公開されているアプリケーションの正常性を監視します。これらの列には、過去1時間に該当するアプリケーションの起動中に発生した障害とエラーの合計数が表示されます。「**アプリケーション障害**」または「**アプリケーションエラー**」フィールドをクリックすると、選択したアプリケーションに対応する「**傾向**」\>「**アプリケーション障害**」ページで障害の詳細を確認できます。

アプリケーション障害ポリシー設定は、障害とエラーの可用性と表示を管理します。ポリシーとその変更方法の詳細については、「**監視ポリシー**」設定の「アプリケーション障害監視のポリシー」を参照してください。

リアルタイムアプリケーション監視

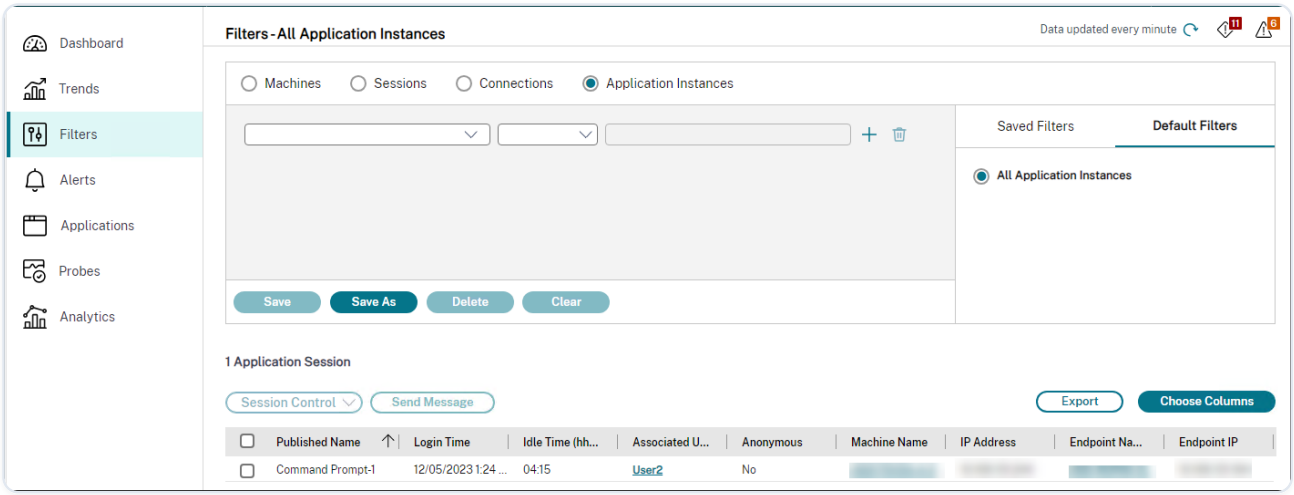
アイドル時間メトリックを使用すると、特定の時間制限を超えてアイドル状態になっているインスタンスを特定することで、アプリケーションとセッションのトラブルシューティングを行うことができます。

アプリケーションベースのトラブルシューティングの典型的なユースケースは、従業員がアプリケーションライセンスを共有する医療分野にあります。そこでは、アイドル状態のセッションとアプリケーションインスタンスを終了して、Citrix Virtual Apps and Desktops™環境をパージしたり、パフォーマンスの低いサーバーを再構成したり、アプリケーションを保守およびアップグレードしたりする必要があります。

「**アプリケーションインスタンス**」フィルターページには、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスが一覧表示されます。関連するアイドル時間測定値は、少なくとも10分間アイドル状態であったマルチセッションOSのVDA上のアプリケーションインスタンスに対して表示されます。

注： アプリケーションインスタンスのメトリックは、すべてのライセンスエディションのサイトで利用できます。

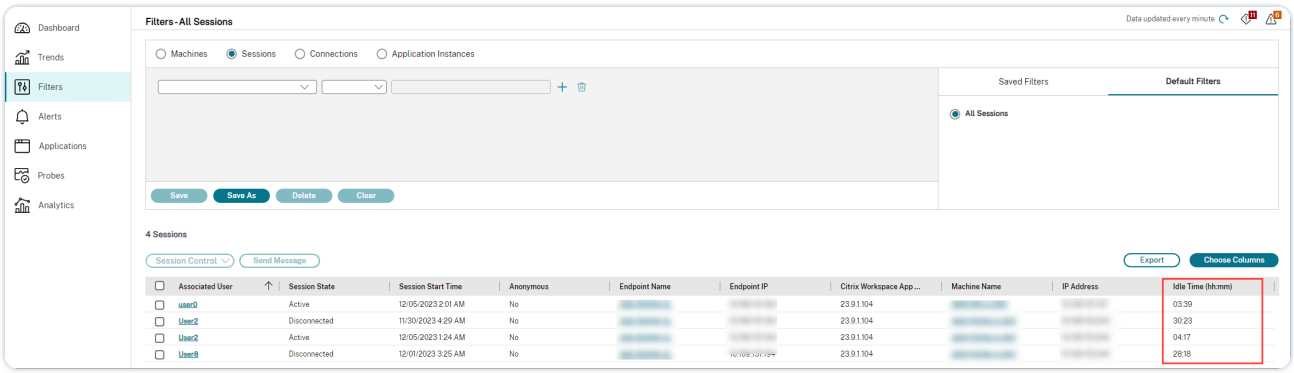
この情報を使用して、特定の期間を超えてアイドル状態になっているアプリケーションインスタンスを特定し、必要に応じてログオフまたは切断します。これを行うには、**フィルター** \> **アプリケーションインスタンス**を選択し、事前に保存されたフィルターを選択するか、**すべてのアプリケーションインスタンス**を選択して独自のフィルターを作成します。



フィルターの例は次のとおりです。**フィルター条件**として、**公開名**（アプリケーションの）と**アイドル時間**を選択します。次に、**アイドル時間**を特定の時間制限**以上**に設定し、再利用のためにフィルターを保存します。フィルターされたリストから、アプリケーションインスタンスを選択します。メッセージを送信するオプションを選択するか、**セッション制御**ドロップダウンから**ログオフ**または**切断**を選択してインスタンスを終了します。

> **注：** アプリケーションインスタンスをログオフまたは切断すると、現在のセッションがログオフまたは切断され、同じセッションに属するすべてのアプリケーションインスタンスが終了します。

セッションの状態とセッションアイドル時間メトリックを使用して、**セッション**フィルターページからアイドルセッションを特定できます。**アイドル時間**列で並べ替えるか、特定の時間制限を超えてアイドル状態になっているセッションを特定するためのフィルターを定義します。アイドル時間は、少なくとも10分間アイドル状態であったマルチセッションOSのVDA上のセッションに対して表示されます。



セッションまたはアプリケーションインスタンスが次の条件を満たす場合、**アイドル時間**は**N/A**と表示されます。

- 10分以上アイドル状態になっていない場合、,
- シングルセッションOSのVDAで起動されている場合、または

- Version 7.12以前のVDAで起動されます。

履歴アプリケーション障害監視

トレンド -\> **アプリケーション障害**タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

アプリケーション障害の傾向は、PremiumおよびAdvancedライセンスサイトでは過去2時間、24時間、7日間、および1か月間利用できます。その他のライセンスタイプでは、過去2時間、24時間、および7日間利用できます。「Application Errors」をソースとしてイベントビューアーにログ記録されたアプリケーション障害が監視されます。**エクスポート**をクリックして、CSV、Excel、またはPDF形式でレポートを生成します。

アプリケーション障害監視のグルーミング保持設定であるGroomApplicationErrorsRetentionDaysとGroomApplicationFaultsRetentionDaysは、Premiumおよび非Premiumライセンスサイトの両方で、デフォルトで1日に設定されています。この設定は、PowerShellコマンドを使用して変更できます。

```
Set-MonitorConfiguration -\<setting name\> \<value\>
```

アプリケーション障害の傾向(/en-us/citrix-virtual-apps-desktops/2311/media/dir_application_faults.png)

障害は、その重大度に基づいて**アプリケーション障害**または**アプリケーションエラー**として表示されます。アプリケーション障害タブには、機能またはデータの損失に関連する障害が表示されます。アプリケーションエラーは、直ちに関連しない問題を示します。これらは、将来問題を引き起こす可能性のある状態を示します。

公開アプリケーション名、**プロセス名**、**デリバリーグループ**、および**期間**に基づいて障害をフィルタリングできます。テーブルには、障害またはエラーコードと、障害の簡単な説明が表示されます。詳細な障害説明はツールチップとして表示されます。

> **注：** 対応するアプリケーション名を導出できない場合、公開されたアプリケーション名は「不明」と表示されます。これは通常、起動されたアプリケーションがデスクトップセッションで失敗した場合、または依存する実行可能ファイルによって引き起こされた未処理の例外が原因で失敗した場合に発生します。

> デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションの障害のみが監視されます。監視グループポリシー（アプリケーション障害の監視を有効にする、シ

> ングルセッションOS VDAでのアプリケーション障害の監視を有効にする、障害監視から除外されるアプリケーションのリスト）を通じて監視設定を変更できます。詳細については、監視ポリシー設定のアプリケーション障害監視のポリシーを参照してください。

トレンド \> アプリケーションプローブ結果ページには、過去24時間および7日間にサイトで実行されたアプリケーションプロービングの結果が表示されます。アプリケーションプローブの構成方法の詳細については、アプリケーションプロービングを参照してください。

マシンのトラブルシューティング

> **注:**
>
> **Citrix Health Assistant** は、未登録のVDAにおける構成の問題をトラブルシューティングするためのツールです。このツールは、VDA登録の失敗、セッション起動の問題、およびタイムゾーンリダイレクト構成における潜在的な根本原因を特定するために、いくつかのヘルスチェックを自動化します。ナレッジセンターの記事「Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch」には、**Citrix Health Assistant** ツールのダウンロードと使用方法が記載されています。

> Directorコンソールの **>** ビューには、サイトで構成されているマシンが表示されます。 タブには、ロード評価インデックスが表示され、パフォーマンスカウンターの分布と、リンクにカーソルを合わせるとセッション数のツールヒントが表示されます。

失敗したマシンの 列をクリックすると、障害の詳細な説明と、障害のトラブルシューティングに推奨されるアクションが表示されます。マシンおよび接続障害の障害理由と推奨されるアクションについては、「Citrix Director failure reasons and troubleshooting」を参照してください。

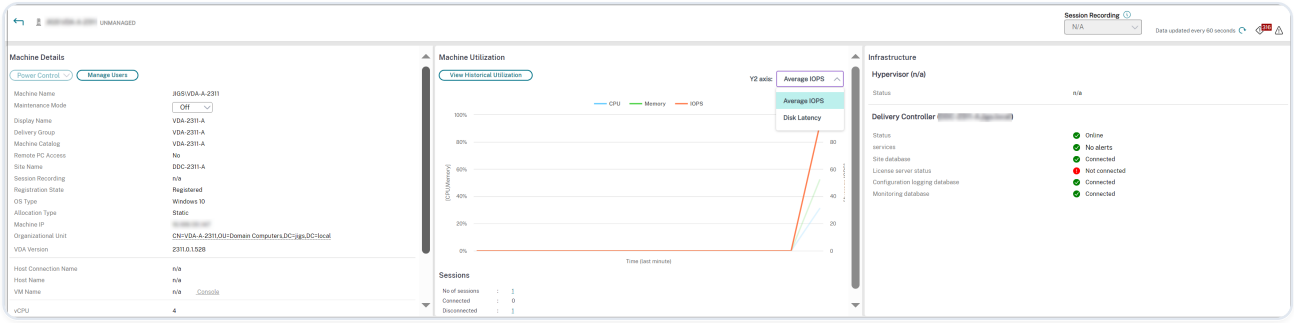
マシン名のリンクをクリックして、 ページに移動します。

マシン詳細ページには、マシンの詳細、インフラストラクチャの詳細、およびマシンに適用されたホットフィックスの詳細が一覧表示されます。

マシンベースのリアルタイムリソース使用率

パネルには、CPUとメモリのリアルタイム使用率を示すグラフが表示されます。さらに、Delivery ControllersとVDAのバージョンが**7.14**以降のサイトでは、ディスクとGPUの監視グラフが利用可能です。

ディスク監視グラフ、平均IOPS、およびディスク遅延は、VDAディスクに関連する問題を監視およびトラブルシューティングするのに役立つ重要なパフォーマンス測定値です。平均IOPSグラフは、ディスクへの読み取りと書き込みの平均回数を表示します。 を選択すると、データの要求からディスクからの返却までの遅延をミリ秒単位で測定したグラフが表示されます。



GPU使用率

を選択すると、GPU、GPUメモリ、エンコーダー、デコーダーの使用率がパーセンテージで表示され、マルチセッションおよびシングルセッションOS VDAにおけるGPU関連の問題をトラブルシューティングできます。

サポートされるGPUバージョン：

- Display Driverバージョン369.17以降を実行しているNVIDIA Tesla M60 GPU。詳細については、「NVIDIA vGPU Software」を参照してください。
- AMD Radeon Instinct MI25 GPU および AMD EPYC 7V12 (Rome) CPU。詳細については、「AMD Drivers and Support」を参照してください。

ドライバー:

適切なドライバーまたは拡張機能をVDAにインストールする必要があります。

- NVIDIA GPU の場合は、GRID ドライバーを手動で、または拡張機能経由でインストールします。詳細については、「NVIDIA vGPU Software」を参照してください。
  - NVIDIA の場合、GRID ドライバーのみがサポートされています。CUDA ドライバーは NVadsA10 v5 シリーズでは動作せず、サポートされていません。
  - Azure ベースのマシンに拡張機能経由でNvidia Grid GPUドライバーをインストールするプロセス例については、「NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines」を参照してください。
  - Nvidia Grid GPU ドライバーを手動でインストールするプロセス例については、「Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines」を参照してください。

- AMD GPU の場合は、AMD グラフィックドライバーを手動で、または拡張機能経由でインストールします。詳細については、「AMD Drivers and Support」を参照してください。
  - Azure ベースのマシンに拡張機能経由でAMD GPUドライバーをインストールするプロセス例については、「AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines」を参照してください。
  - Azure マシンにAMD GPUドライバーを手動でインストールするプロセス例については、「Install AMD GPU drivers on N-series VMs running Windows」を参照してください。

使用上の注意:

- GPU 使用率グラフは、64ビットWindowsを実行しているVDAでのみ利用できます。
- GPU アクセラレーションを提供するには、VDAでHDX 3D Proを有効にする必要があります。詳細については、「GPU acceleration for Windows Single-session OS」および「GPU acceleration for Windows Multi-session OS」を参照してください。
- VDAが複数のGPUにアクセスする場合、使用率グラフには個々のGPUから収集されたGPUメトリックの平均が表示されます。GPUメトリックは、個々のプロセスではなく、VDA全体に対して収集されます。
- AMDの場合、エンコーダーとデコーダーの使用は個別にサポートされていません。GPUを使用するエンコード/デコードワークロードは、GPU使用率の一般的な3D負荷として報告されます。
- インストール中にNVIDIA WMIをインストールしてください。このウィンドウは手動インストール中にのみ利用可能です。
- ドライバーがインストールされているのにDirectorがGPUを検出しない場合
  - タスクマネージャーを確認してください。ドライバーが適切にインストールされていれば、GPUがタスクマネージャーに表示されるはずです。
  - マシンが登録されているか確認してください。マシンがオンラインとして検出されるまでに時間がかかる場合があります。
- DirectorでGPU使用率にアクティビティが表示されない場合は、実行しているワークロードがGPUを使用していることを確認してください。グラフィックワークロードの場合、これは「設定」>「システム」>「ディスプレイ」>「グラフィック設定」>「アプリを選択して設定を優先」から有効にできます。「高パフォーマンス」をオンにしてください。システムデフォルトまたは省電力に設定されている場合、他の設定に基づいて、Windowsがグラフィックワークロードにを使用することがデフォルトになる場合があります。
- データは1分ごとに更新され、**GPU使用率**を選択してから1分以内にデータの視覚化が開始されます。

マシンベースの履歴リソース使用率

「**マシン使用率**」パネルで、「**履歴使用率の表示**」をクリックすると、選択したマシン上のリソースの履歴使用状況が表示されます。 使用率グラフには、CPU、メモリ、ピーク同時セッション、平均IOPS、ディスク遅延の重要なパフォーマンスカウンターが含まれます。

> **注:**
>
> 監視ポリシー設定の**プロセス監視を有効にする**は、履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集および表示するために、「許可」に設定する必要があります。収集はデフォルトで禁止されています。

> CPUとメモリの使用率、平均IOPS、ディスクの待機時間データはデフォルトで収集されます。**リソース監視を有効にする**ポリシー設定を使用して、この収集を無効にできます。



1. **マシン詳細**ビューの**マシン使用率**パネルから、**履歴使用率の表示**を選択します。
2. **履歴マシン使用率**ページで、**期間**を「過去2時間」、「24時間」、「7日間」、「月」、「年」に設定して使用状況を表示します。

> **注:**
>
> 平均IOPSとディスク遅延の使用状況データは、現在までの過去24時間、月、年についてのみ利用可能です。カスタム終了時刻はサポートされていません。

3. **適用**をクリックし、必要なグラフを選択します。
4. グラフの異なるセクションにカーソルを合わせると、選択した期間の詳細情報が表示されます。



たとえば、**過去2時間**を選択した場合、ベースライン期間は選択した時間範囲の前の2時間です。過去2時間とベースライン時間のCPU、メモリ、セッションの傾向を表示します。**先月**を選択した場合、ベースライン期間は前月です。先月とベースライン時間の平均IOPSとディスクの待機時間を表示するように選択します。

1. **エクスポート**をクリックして、選択した期間のリソース使用状況データをエクスポートします。詳細については、Monitor Deploymentsの「レポートのエクスポート」セクションを参照してください。
2. グラフの下には、CPUまたはメモリ使用率に基づいて上位10個のプロセスが表に表示されます。選択した時間範囲におけるアプリケーション名、ユーザー名、セッションID、平均CPU、ピークCPU、平均メモリ、ピークメモリを示す任意の列で並べ替えることができます。IOPSとディスク遅延の列は並べ替えることができません。

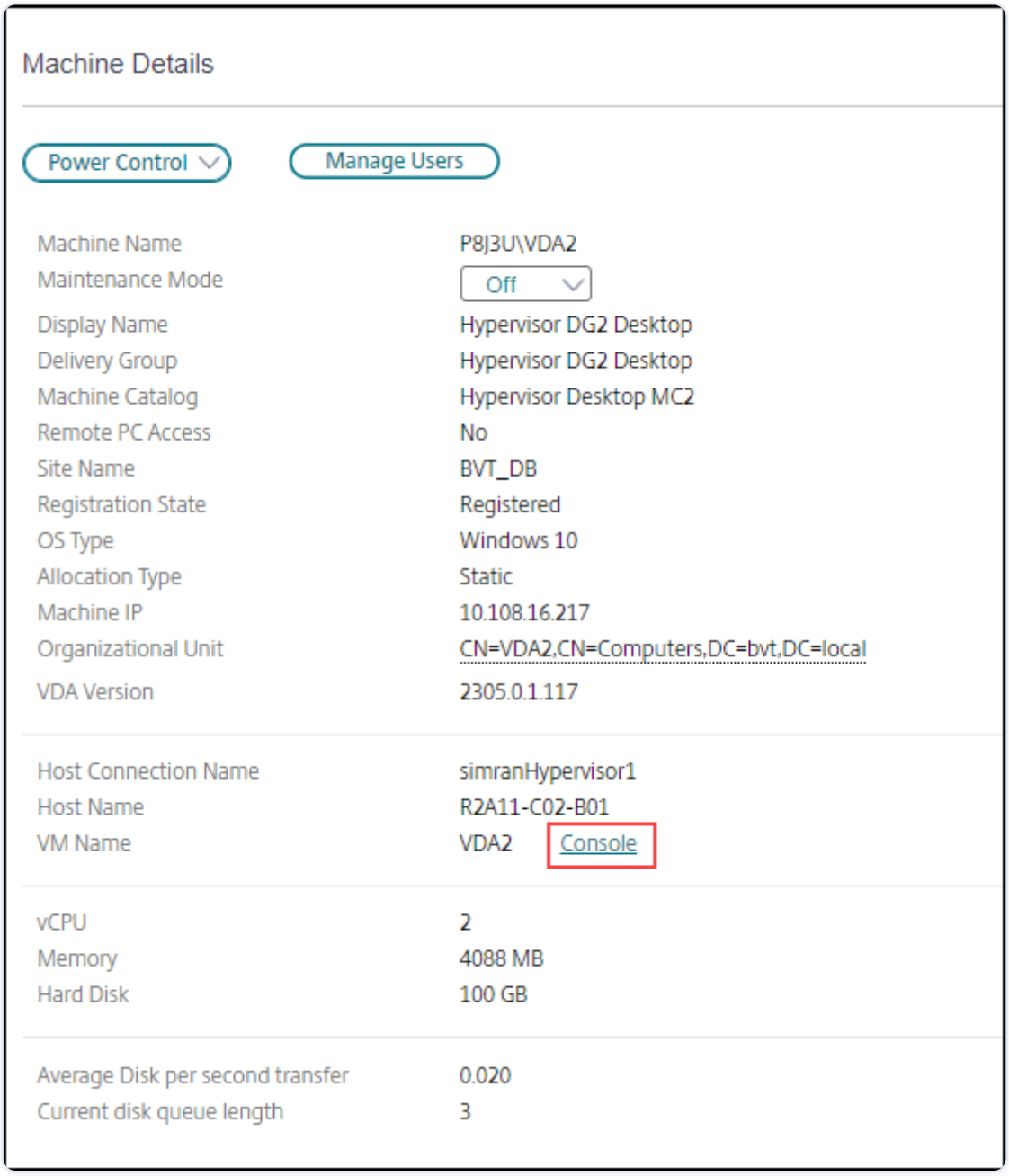
> **注:**
>
> システムプロセスのセッションIDは「0000」と表示されます。

3. 特定のプロセスのリソース消費の履歴傾向を表示するには、上位10個のプロセスのいずれかをドリルダウンします。

マシンコンソールへのアクセス

XenServerバージョン7.3以降でホストされているシングルセッションおよびマルチセッションOSマシンのコンソールには、Directorから直接アクセスできます。これにより、XenServerでホストされているVDAの問題をトラブルシューティングするためにXenCenterは必要ありません。この機能を利用するには：

- バージョン7.16以降のDelivery Controllerが必要です。
- マシンをホストするXenServerはバージョン7.3以降である必要があり、Director UIからアクセスできる必要があります。



マシンのトラブルシューティングを行うには、対応するマシン詳細パネルの**コンソール**リンクをクリックします。提供されたホスト資格情報が認証されると、WebベースのVNCクライアントで

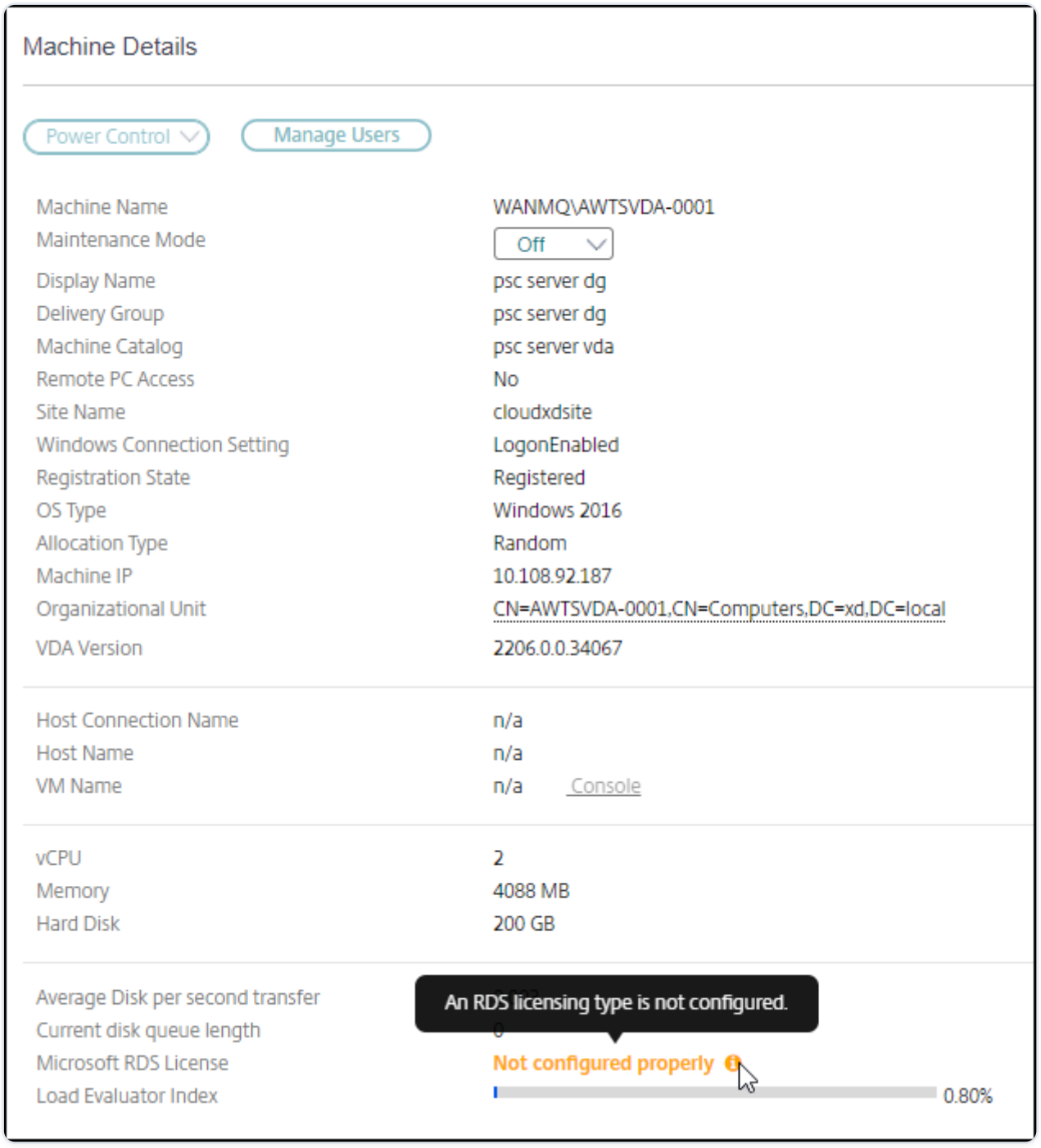
あるnoVNCを使用して、マシンコンソールが別のタブで開きます。これで、コンソールにキーボードとマウスでアクセスできるようになります。

注:

- この機能はInternet Explorer 11ではサポートされていません。
- マシンコンソール上のマウスポインターがずれている場合は、問題を解決するための手順についてCTX230727を参照してください。
- Directorは新しいタブでコンソールアクセスを起動します。ブラウザの設定でポップアップが許可されていることを確認してください。
- セキュリティ上の理由から、Citrix®はブラウザにSSL証明書をインストールすることを推奨しています。

Microsoft RDSライセンスの状態

マルチセッションOSマシンの**マシン詳細**および**ユーザー詳細**ページの「マシン詳細」パネルで、Microsoft RDSライセンスのステータスを表示できます。



次のいずれかのメッセージが表示されます。

- ライセンス利用可能
- 適切に構成されていません（警告）
- ライセンスエラー（エラー）
- 互換性のないVDAバージョン（エラー）

> **注:**

有効なライセンスを持つ猶予期間中のマシンのRDSライセンス健全性ステータスは、緑色で「**ライセンス利用可能**」メッセージを表示します。有効期限が切れる前にライセンスを更新してください。

警告メッセージとエラーメッセージについては、情報アイコンにカーソルを合わせると、以下の表に示す追加情報を表示できます。

メッセージの種類	DIRECTOR内のメッセージ
エラー	VDAバージョン7.16以降で利用可能です。
エラー	新しいRDS接続は許可されません。
エラー	RDSライセンスの猶予期間が過ぎました。
エラー	必要なOSレベルに対して、デバイスごとのクライアントアクセスライセンスの種類でライセンスサーバーが構成されていません。
エラー	構成されているライセンスサーバーは、デバイスごとのクライアントアクセスライセンスの種類でRDSホストOSレベルと互換性がありません。
警告	Personal Terminal Serverは、Citrix Virtual Apps and Desktops™展開において有効なRDSライセンスの種類ではありません。
警告	Remote Desktop for Administrationは、Citrix Virtual Apps and Desktops展開において有効なライセンスの種類ではありません。
警告	RDSライセンスの種類が構成されていません。
警告	ユーザーごとのクライアントアクセスRDSライセンスの種類では、ドメインコントローラーまたはライセンスサーバーに到達できません。
警告	デバイスごとのクライアントアクセスライセンスの種類では、必要なOSレベルのライセンス

メッセージの種類	DIRECTOR内のメッセージ
	サーバーに到達できないため、クライアントデバイスライセンスを判別できません。

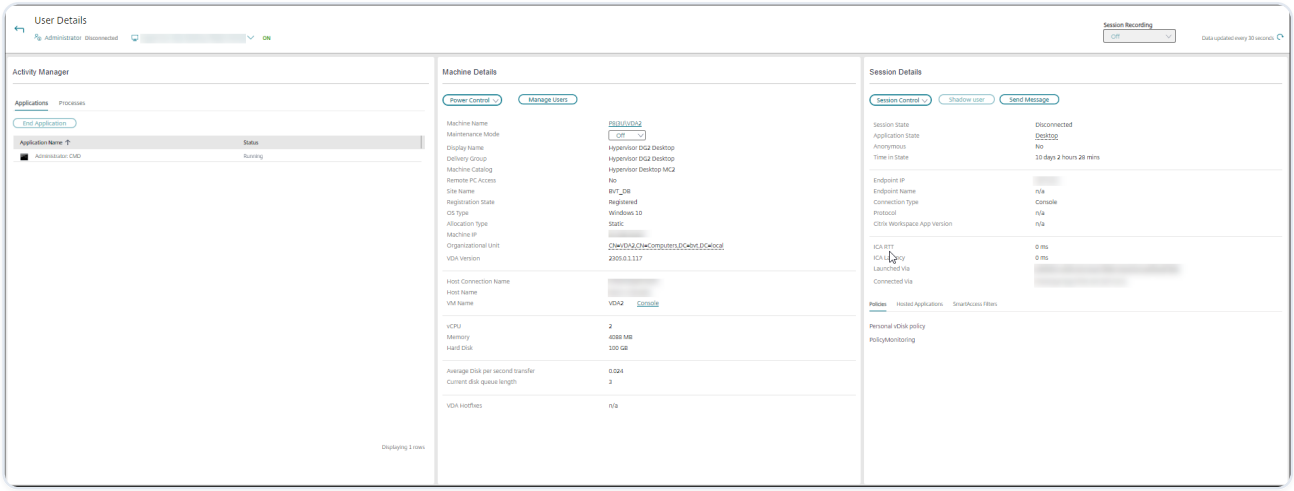
> **注:**
>
> この機能は、Microsoft RDS CAL (Client Access License) のみに適用されます。

ユーザーの問題のトラブルシューティング

Director の **ヘルプデスク** ビュー (**アクティビティマネージャー** ページ) を使用して、ユーザーまたはセッションに関する情報を表示します。

ユーザーの詳細(/en-us/citrix-virtual-apps-desktops/2311/media/dir-user-details-summary.png)

アクティビティマネージャーでユーザーの **詳細の表示** をクリックすると、**ユーザーの詳細** ページが開きます。 アクティビティマネージャーでエンドポイントの **詳細の表示** をクリックすると、**エンドポイントの詳細** ページが開きます。



セッションセレクター

ユーザーが複数のセッションを開始している場合、セッションセレクターはセッションの選択に役立ちます。

セッションセレクター(/en-us/citrix-virtual-apps-desktops/2311/media/dir-session-selector.png)

詳細を表示するセッションを選択します。

- セッション、ユーザーのサインインエクスペリエンス、セッションの起動、接続、およびアプリケーションに関する詳細を確認します。
- ユーザーのマシンをシャドウできます。
- ICA® セッションを記録します。

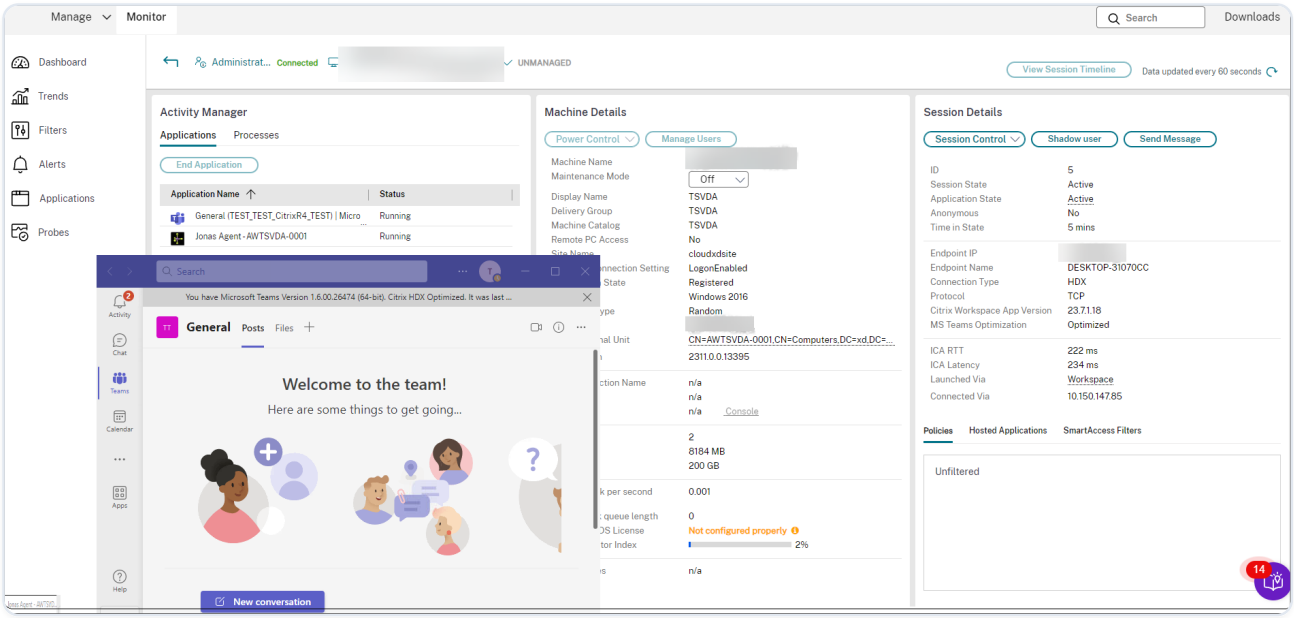
Microsoft Teams の最適化ステータス

Director は、**ユーザーの詳細** ページ > **セッションの詳細** パネル > **MS Teams の最適化** フィールドに、HDX™ セッションの Microsoft Teams の最適化ステータスを表示します。Microsoft Teams が最適化されていることは、クリアなオーディオやビデオなど、より良いユーザーエクスペリエンスのために重要です。Microsoft Teams の最適化ステータスの可視性は、チケットの解決にかかる時間を短縮するのに役立ち、管理者がトラブルシューティング中に重要なメトリックを特定するのに役立ちます。

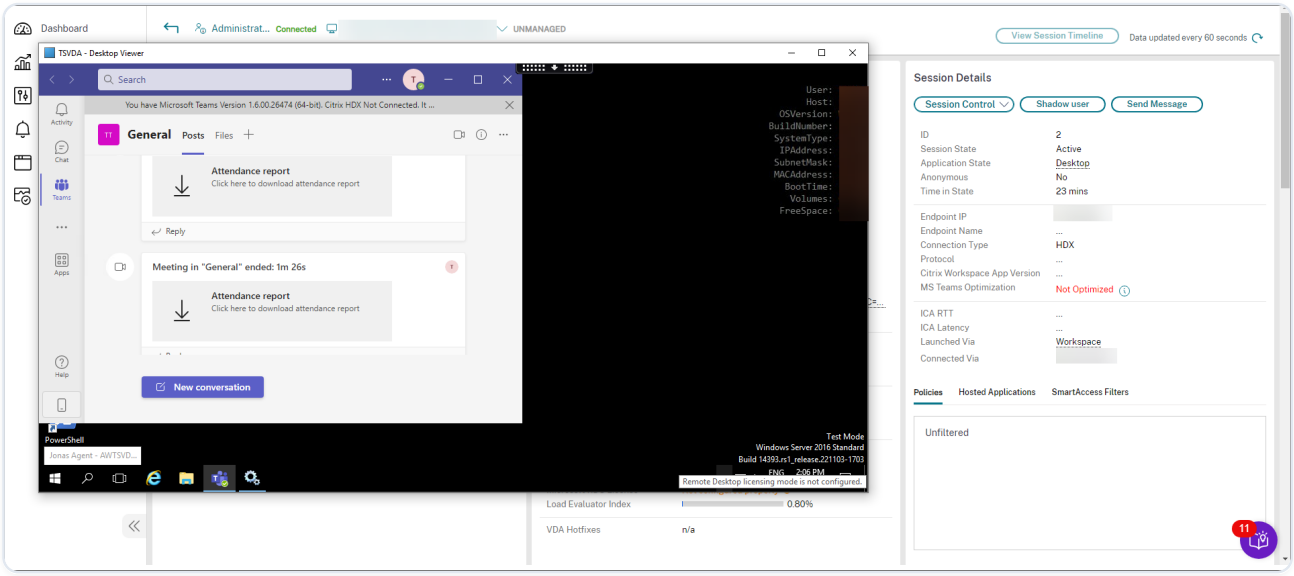
> **注:**
>
> Citrix Director は、バージョン 2.0 より前の Microsoft Teams を使用している場合にのみサポートされます。

前提条件:

- VDA はバージョン 2311 以降を実行しています。
- サポートされている Citrix Workspace アプリのバージョンは、Microsoft Teams の最適化 に記載されています。
- Microsoft Teams は、公開アプリケーションとして、または公開デスクトップ内で実行されます。
- Citrix HDX HTML5 ビデオリダイレクトサービスなどの重要なサービスが実行されています。



Microsoft Teams が最適化されていない場合、ツールヒントには、Microsoft Teams を最適化するためのヒントを含む、HDX からの外部トラブルシューティングライブ記事へのリンクが表示されます。HDX 最適化のトラブルシューティング。



トラブルシューティングのヒント

以下の表に記載されている推奨されるアクションで問題をトラブルシューティングし、必要に応じて適切な管理者に問題をエスカレートしてください。

ユーザーの問題	提案
ログオンに時間がかかる、または断続的または繰り返し失敗する	ユーザーログオンの問題を診断する

ユーザーの問題	提案
セッションの起動に時間がかかる、または断続的または繰り返し失敗する	セッション起動の問題を診断する
セッションの応答が遅い、または応答しない	セッションパフォーマンスの問題を診断する
アプリケーションが遅い、または応答しない	アプリケーションの障害を解決する
接続に失敗しました	デスクトップ接続を復元する
セッションが遅い、または応答しない	セッションを復元する
セッションを記録する	セッションを記録する
ビデオが遅い、または品質が低い	HDXチャネルシステムレポートを実行する

注: マシンがメンテナンスモードになっていないことを確認するには、 ビューから パネルを確認します。

セッションログオン

ユーザーの詳細ビュー > **セッションログオン**タブには、セッションログオンプロセスの包括的なビューが表示されます。このタブには、さまざまなログオンフェーズがプロットされたログオン期間フェーズチャートが含まれています。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。詳しくは、「ユーザーログオンの問題の診断」を参照してください。

セッションパフォーマンス

セッションパフォーマンスタブには、ユーザーセッション内の問題を特定するリアルタイムメトリックを関連付ける機能から始まる、強化されたトラブルシューティングワークフローがあります。**セッショントポロジ**パネルは、接続されたHDXセッションのセッション内パスを視覚的に表現します。**パフォーマンスメトリック**パネルは、ICARTT、ICA Latency、Frames Per Second、Output Bandwidth Available、Output Bandwidth Consumedなどのセッションメトリックの傾向を提供し、これらのメトリックが時間の経過とともにどのように実行されたかを示します。詳しくは、「セッションパフォーマンスの問題の診断」を参照してください。

検索のヒント

検索フィールドにユーザー名を入力すると、Directorは、Directorをサポートするように構成されているすべてのサイトのActive Directoryでユーザーを検索します。

検索フィールドにマルチユーザーマシンの名前を入力すると、Director は指定されたマシンのマシン詳細を表示します。

検索フィールドにエンドポイント名を入力すると、Directorは特定のEndpointに接続されている認証されていない（匿名）セッションと認証されたセッションを使用します。この検索により、認証されていないセッションのトラブルシューティングが可能になります。認証されていないセッションのトラブルシューティングを可能にするには、エンドポイント名が一意であることを確認してください。

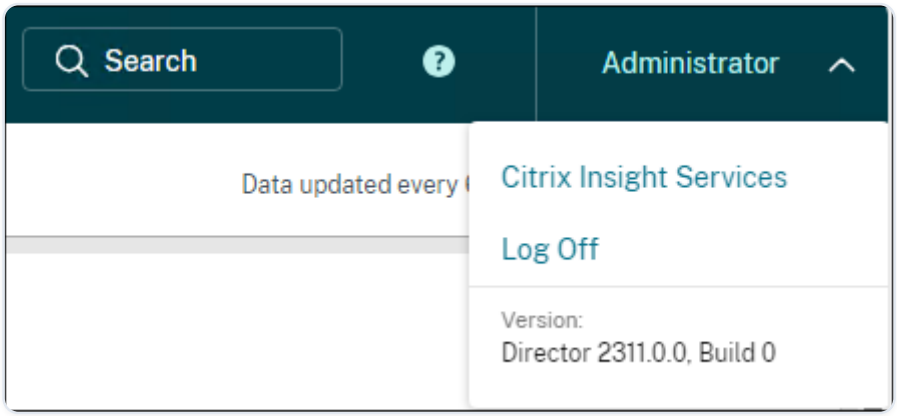
検索結果には、現在マシンを使用していない、またはマシンに割り当てられていないユーザーも含まれます。

- 検索では大文字と小文字は区別されません。
- 部分的な入力により、一致する可能性のあるリストが生成されます。
- スペースで区切られた2つの部分からなる名前の数文字を入力すると、両方の文字列に一致する結果が含まれます。2つの部分からなる名前の例としては、ユーザー名、姓と名、または表示名があります。たとえば、「jo rob」と入力すると、「John Robertson」や「Robert Jones」などの文字列が結果に含まれる場合があります。

ランディングページに戻るには、**Directorロゴ**をクリックします。

Citrix Insight Servicesへのアクセス

Directorの**ユーザー**ドロップダウンリストからCitrix Insight Services (CIS) にアクセスして、追加の診断インサイトにアクセスできます。CISで利用可能なデータは、Call HomeやCitrix Scoutなどのソースから取得されます。



トラブルシューティング情報をCitrixテクニカルサポートにアップロードする

選択したコンピューターのトラブルシューティングを行うために、単一のDelivery Controller™またはVDAからCitrix Scoutを実行し、主要なデータポイントとCitrix Diagnostics Facility (CDF) トレースをキャプチャします。Scoutは、Citrixテクニカルサポートのトラブルシューティングを支援

するために、データをCISプラットフォームに安全にアップロードする機能を提供します。Citrixテクニカルサポートは、CISプラットフォームを使用して、顧客から報告された問題の解決にかかる時間を短縮します。

Scoutは、Citrix Virtual Apps and Desktops™コンポーネントとともにインストールされます。Windowsのバージョンによっては、Citrix Virtual Apps and Desktopsをインストールまたはアップグレードすると、「**Windowsのスタート**」メニューまたはスタート画面にScoutが表示されます。

Scoutを起動するには、スタートメニューまたはスタート画面から「**Citrix \> Citrix Scout**」を選択します。

Scoutの使用方法と構成に関する情報、およびFAQについては、CTX130147を参照してください。

セッション起動の問題を診断する

ユーザーログオンの問題の診断セクションで述べられているログオンプロセスフェーズに加えて、Directorはセッション起動時間を表示します。これは、**ユーザー詳細**ページと**マシン詳細**ページで、Workspace Appセッション起動時間とVDAセッション起動時間に分けられます。これらの2つの期間には、起動時間も表示される個々のフェーズがさらに含まれています。このデータは、セッション起動時間が長い原因を理解し、トラブルシューティングするのに役立ちます。さらに、セッション起動に関わる各フェーズの所要時間は、個々のフェーズに関連する問題のトラブルシューティングに役立ちます。例えば、ドライブマッピング時間が長い場合、GPOまたはスクリプトですべての有効なドライブが正しくマッピングされているかを確認できます。この機能は、Delivery Controllerバージョン7 1906以降およびVDA 1903以降で利用可能です。

前提条件

セッション起動時間のデータが表示されるには、以下の前提条件が満たされていることを確認してください。

- デリバリーコントローラー™ 7 1906 以降。
- VDA 1903以降。
- Citrix End User Experience Monitoring (EUEM)サービスがVDAで実行されている必要があります。

制限事項

Directorがセッション起動時間のデータを表示する際には、以下の制限事項が適用されます。

- セッション起動時間は、HDX™セッションでのみ利用可能です。
- iOSおよびAndroid OSからのセッション起動の場合、VDA起動時間のみが利用可能です。

- ICA®ファイルダウンロード時間 (IFDCD) は、ブラウザから起動する際にWorkspace Appが検出された場合にのみ利用可能です。
- Mac OSからのセッション起動の場合、IFDCDはWorkspace App 1902以降でのみ利用可能です。
- Windows OSからのセッション起動の場合、IFDCDはWorkspace app 1902以降で利用可能です。それ以前のバージョンでは、IFDCDは、ブラウザから起動し、Workspace appが検出されたアプリ起動の場合にのみ表示されます。

注:

- 前提条件が満たされた後、セッション起動時間の表示に問題がある場合は、CTX130320に記載されているように、DirectorサーバーとVDAのログを確認してください。 共有セッション（同じセッションで複数のアプリケーションが起動されている場合）の場合、Workspace Appの起動メトリックは、最新の接続または最新のアプリケーション起動に対して表示されます。
- VDAセッション起動の一部のメトリックは、再接続時には適用されません。そのような場合、メッセージが表示されます。

セッション起動(/en-us/citrix-virtual-apps-desktops/2311/media/session_startup.png)

Workspace App セッション起動フェーズ

セッション起動クライアント期間 (SSCD)

このメトリックが高い場合、起動時間の長期化を引き起こしているクライアント側の問題を示しています。問題の根本原因を特定するために、後続のメトリックを確認してください。SSCDは、要求（マウスクリック）の時刻にできるだけ近い時点から開始されます。クライアントデバイスとVDA間のICA接続が確立されたときに終了します。共有セッションの場合、サーバーへの新しい接続の作成に関連するセットアップコストの多くが発生しないため、この期間ははるかに短くなります。次のレベルでは、いくつかの詳細なメトリックが利用可能です。

ICA ファイルダウンロード期間

これは、クライアントがサーバーから ICA ファイルをダウンロードするのにかかる時間です。全体的なプロセスは次のとおりです。

1. ユーザーがWorkspace Applicationでリソース（アプリケーションまたはデスクトップ）をクリックします。

2. ユーザーからの要求は、Citrix Gateway（構成されている場合）を介してStoreFront™に送信され、StoreFront™は要求をDelivery Controllerに送信します。
3. Delivery Controllerは、要求に対して利用可能なマシンを見つけ、マシン情報とその他の詳細をStoreFrontに送信します。また、StoreFrontはSecure Ticket Authorityからワンタイムチケットを要求し、受け取ります。
4. StoreFrontはICAファイルを生成し、Citrix Gateway（構成されている場合）を介してユーザーに送信します。

IFDCD は、完全なプロセス (ステップ 1〜4) にかかる時間を表します。IFDCD 期間は、クライアントが ICA ファイルを受信したときにカウントを停止します。

LPWD は、プロセスの StoreFront コンポーネントです。

IFDCD が高い (ただし LPWD が正常である) 場合、起動のサーバー側処理は成功しましたが、クライアントデバイスと StoreFront の間に通信の問題がありました。これは、2つのマシン間のネットワークの問題に起因します。したがって、まず潜在的なネットワークの問題をトラブルシューティングできます。

起動ページWEBサーバー期間 (LPWD)

これは、StoreFront で起動ページ (launch.aspx) を処理するのにかかる時間です。LPWD が高い場合、StoreFront にボトルネックがある可能性があります。

考えられる原因は次のとおりです。

- StoreFrontの負荷が高い。Internet Information Services (IIS) ログ、監視ツール、タスクマネージャー、パフォーマンスモニターなどを確認して、速度低下の原因を特定してください。
- StoreFrontがDelivery Controllerなどの他のコンポーネントとの通信に問題がある。StoreFrontとDelivery Controller間のネットワーク接続が遅いか、一部のDelivery Controllerがダウンしているか、過負荷になっていないかを確認してください。

名前解決WEBサーバー期間 (NRWD)

これは、Delivery Controllerが公開アプリケーション/デスクトップの名前をVDAマシンのIPアドレスに解決するのにかかる時間です。

このメトリックが高い場合、Delivery Controllerが公開アプリケーションの名前をIPアドレスに解決するのに時間がかかっていることを示します。

考えられる原因としては、クライアント側の問題、Delivery Controllerの過負荷などのDelivery Controllerに関する問題、またはそれらの間のネットワークリンクの問題が挙げられます。

チケット応答WEBサーバー期間 (TRWD)

この期間は、Secure Ticket Authority (STA) サーバーまたはDelivery Controllerからチケットを取得する (必要な場合) のにかかる時間を示します。この期間が高い場合、STAサーバーまたはDelivery Controllerが過負荷になっていることを示します。

セッション検索クライアント期間 (SLCD)

この期間は、要求された公開アプリケーションをホストするためにすべてのセッションを照会するのにかかる時間を表します。既存のセッションがアプリケーション起動要求を処理できるかどうかを判断するために、クライアントでチェックが実行されます。使用される方法は、セッションが新規か共有かによって異なります。

セッション作成クライアント期間 (SCCD)

この期間は、wfica32.exe (または同様の同等ファイル) が起動されてから接続が確立されるまでの、セッションを作成するのにかかる時間を表します。

VDAセッション起動フェーズ

セッション起動VDA期間 (SSVD)

この期間は、VDAが起動操作全体を実行するのにかかる時間を含む、高レベルのサーバー側接続起動メトリックです。このメトリックが高い場合、セッション起動時間を増加させるVDAの問題があることを示します。これには、VDAで起動操作全体を実行するのに費やされた時間が含まれます。

資格情報取得VDA期間 (COVD)

VDAがユーザー資格情報を取得するのにかかる時間。

ユーザーが時間内に資格情報を提供できない場合、この期間は人為的に増加する可能性があります。そのため、VDA起動期間には含まれません。この時間は、手動ログインが使用され、サーバー側の資格情報ダイアログが表示される場合（またはログイン開始前に法的通知が表示される場合）にのみ重要になる可能性があります。

資格情報認証VDA期間 (CAVD)

これは、VDAが認証プロバイダーに対してユーザーの資格情報を認証するのにかかる時間です。認証プロバイダーは、Kerberos、Active Directory、またはセキュリティサポートプロバイダーインターフェイス (SSPI) のいずれかです。

グループポリシーVDA期間 (GPVD)

この期間は、ログオン中にグループポリシーオブジェクトを適用するのにかかる時間です。

ログオンスクリプト実行VDA期間 (LSVD)

これは、VDAがユーザーのログオンスクリプトを実行するのにかかる時間です。

ユーザーまたはグループのログオンスクリプトを非同期にすることを検討してください。アプリケーション互換性スクリプトを最適化するか、代わりに環境変数を使用することを検討してください。

プロファイルロードVDA期間 (PLVD)

これは、VDAがユーザープロファイルをロードするのにかかる時間です。

この期間が長い場合は、ユーザープロファイルの設定を検討してください。ローミングプロファイルのサイズと場所は、セッションの開始が遅くなる原因となります。ユーザーがターミナルサービスローミングプロファイルとホームフォルダーが有効になっているセッションにログオンすると、ローミングプロファイルの内容とそのフォルダーへのアクセスがログオン中にマッピングされます。これには追加のリソースが必要です。場合によっては、これがCPU使用率の大部分を消費することがあります。この問題を軽減するには、リダイレクトされた個人フォルダーとともに**ターミナルサービスホーム**フォルダーの使用を検討してください。一般的に、Citrix環境でユーザープロファイルを管理するには、Citrix Profile Managementの使用を検討してください。Citrix Profile Managementを使用しており、ログオン時間が遅い場合は、アンチウイルスソフトウェアがCitrix Profile Managementツールをブロックしていないか確認してください。

プリンター作成VDA期間 (PCVD)

これは、VDAがユーザーのクライアントプリンターを同期的にマッピングするのにかかる時間です。プリンター作成が非同期的に実行されるように設定されている場合、セッション起動の完了に影響しないため、PCVDの値は記録されません。

プリンターのマッピングに過剰な時間が費やされるのは、多くの場合、プリンターの自動作成ポリシー設定が原因です。ユーザーのクライアントデバイスにローカルで追加されたプリンターの数と、印刷構成は、セッションの開始時間に直接影響を与える可能性があります。セッションが開始されると、Citrix Virtual Apps and Desktops™は、クライアントデバイス上のローカルにマッピングされたすべてのプリンターを作成する必要があります。特にユーザーが多くのローカルプリンターを持っている場合は、作成されるプリンターの数を減らすために、印刷ポリシーの再構成を検討してください。これを行うには、Delivery ControllerおよびCitrix Virtual Apps and Desktopsでプリンター自動作成ポリシーを編集します。

ドライブマッピングVDA期間 (DMVD)

これは、VDAがユーザーのクライアントドライブ、デバイス、ポートをマッピングするのにかかる時間です。

ICAプロトコルを最適化し、セッション全体のパフォーマンスを向上させるために、ベースポリシーに未使用の仮想チャネル（オーディオやCOMポートのマッピングなど）を無効にする設定が含まれていることを確認してください。

アプリケーション/デスクトップ起動VDA期間 (ALVD/DLVD)

このフェーズは、UserinitとShellの期間の組み合わせです。ユーザーがWindowsマシンにログオンすると、winlogonがuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してからExplorer.exeを開始します。Userinitは、userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。Shell期間は、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの時間です。

セッション作成VDA期間 (SCVD)

この時間には、VDAでのセッション作成時間におけるその他の遅延が含まれます。

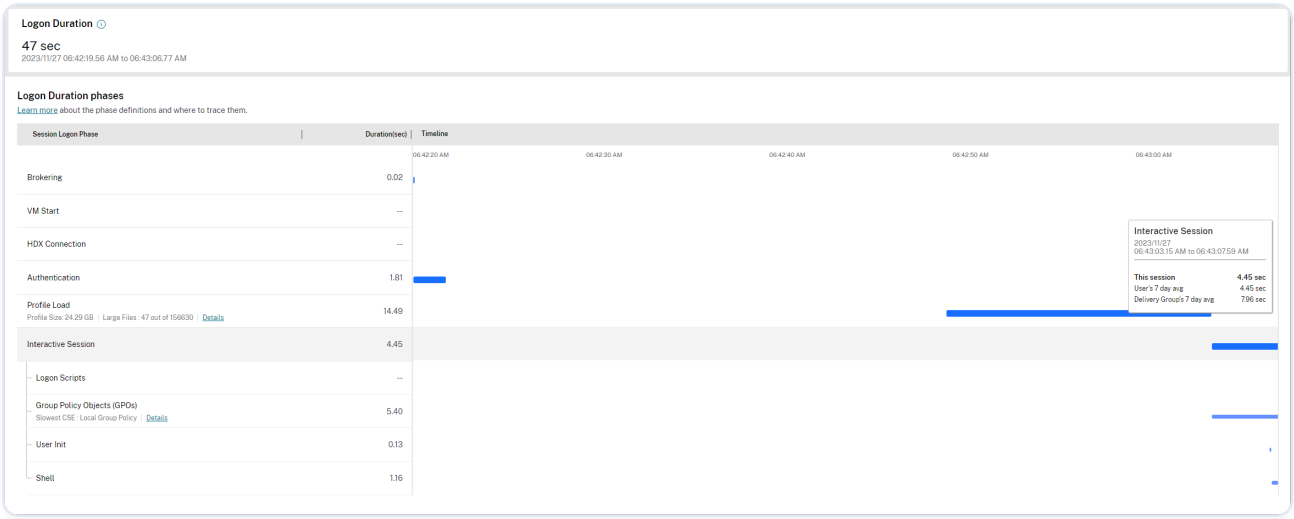
ユーザーログオンの問題を診断する

「**ユーザー詳細**」ビュー > 「**セッションログオン**」タブには、セッションログオンプロセスの包括的なビューが表示されます。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。

ログオン期間は、HDX を使用したデスクトップまたはアプリへの初回接続の場合にのみ測定されます。このデータには、リモートデスクトッププロトコルで接続しようとしているユーザーや、切断されたセッションから再接続しているユーザーは含まれません。具体的には、ユーザーが最初に非 HDX プロトコルを使用して接続し、HDX を使用して再接続する場合、ログオン期間は測定されません。

ユーザーがCitrix Virtual Apps and Desktops™にログオンすると、Monitor Serviceはログオンプロセスのフェーズを追跡します。フェーズは、ユーザーがCitrix Workspace™アプリから接続した時点から、アプリまたはデスクトップが使用可能になるまでの時間で始まります。

セッションログオンタブには、さまざまなログオンフェーズがプロットされたログオン期間フェーズチャートが含まれています。ログオン期間は、接続を確立し、Delivery Controller™ からアプリまたはデスクトップを取得するのに費やされた時間と、仮想アプリまたはデスクトップに認証してログオンするのに費やされた時間を表します。期間情報は秒（または秒の端数）で表示されます。



ログオン期間フェーズチャートは、さまざまなログオンフェーズとその開始時刻および終了時刻を明確に表示します。このチャートは、個々のログオンフェーズの重複を示します。合計ログオン時間は、個々のログオンフェーズの期間の合計ではない場合があります。これは、個々のフェーズが重複する可能性があり、すべてのログオンフェーズがこの表現の一部ではないためです。また、特定のフェーズは、ユーザーが仮想アプリまたはデスクトップとの対話を開始した後も延長される可能性があり、この期間は全体のログオン期間の一部として測定されません。

このビューを使用して、セッション起動の遅延を引き起こしている特定のログオンフェーズを特定します。各ログオンフェーズの定義と、情報を追跡できるイベントソースは、さらなるトラブルシューティングに役立ちます。チャートにカーソルを合わせると、現在のセッションのフェーズ期間、ユーザーの7日間平均、およびデリバリーグループの7日間平均を含むツールチップが表示されます。この情報は、現在のセッションログオン期間を7日間平均値と比較するのに役立ちます。GPOおよびプロファイルの詳細の場合、サブフェーズ測定にさらにドリルダウンできます。この視覚化は、ログオン期間関連の問題を簡単に理解し、トラブルシューティングするのに役立ちます。

前提条件

ログオン期間データとドリルダウンが表示されるように、次の前提条件が満たされていることを確認してください。

1. VDA に **Citrix User Profile Manager** と **Citrix User Profile Manager WMI Plugin** をインストールします。
2. Citrix Profile Management Service が実行されていることを確認します。
3. XenApp および XenDesktop サイト 7.15 以前の場合、GPO 設定 **レガシー実行リストを処理しない** を無効にします。
4. 対話型セッションのドリルダウンには、監査プロセス追跡を有効にする必要があります。
5. GPO ドリルダウンの場合、グループポリシーの運用ログのサイズを増やします。

注:

- ログオン期間は、デフォルトのWindowsシェル (explorer.exe) でのみサポートされ、カスタムシェルではサポートされません。
- Remote PC Accessのログオン期間は、Remote PC Accessのインストール中に**Citrix User Profile Manager**と**Citrix User Profile Manager WMI Plugin**が追加コンポーネントとしてインストールされている場合にのみ利用可能です。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2311/install-configure/remote-pc-access.html#configuration-sequence)の「Remote PC Accessの構成とシーケンスに関する考慮事項」のステップ4を参照してください。

ユーザーログオンの問題をトラブルシューティングする手順

1. **ユーザー詳細**ビュー > **セッションログオン**タブから、ログオン期間グラフを使用してログオン状態をトラブルシューティングします。
   - ユーザーがログオン中の場合、ビューにはログオンのプロセスが反映されます。
   - ユーザーがログオンしている場合、ログオン期間パネルには、ユーザーが現在のセッションにログオンするのにかかった時間が表示されます。
2. ログオンプロセスのフェーズを調べます。

ログオンプロセスのフェーズ

ブローカリング

ユーザーに割り当てるデスクトップを決定するのにかかった時間。

VMの起動

セッションがマシンの起動を必要とする場合、VM起動は仮想マシンを起動するのにかかった時間です。

HDX接続

クライアントから仮想マシンへのHDX接続をセットアップするのに必要な手順を完了するのにかかった時間。

認証

リモートセッションへの認証を完了するのにかかった時間。

GPO

仮想マシンでグループポリシー設定が有効になっている場合、これはログオン中にグループポリシーオブジェクトを適用するのにかかった時間です。CSE（クライアント側拡張）に従って各ポリシーを適用するのにかかった時間のドリルダウンは、GPOバーにカーソルを合わせるとツールヒントとして表示されます。



「**詳細**」をクリックすると、ポリシーのステータスと対応するGPO名を含むテーブルが表示されます。ドリルダウンの時間表示はCSEの処理時間のみを表し、GPOの合計時間には加算されません。ドリルダウンテーブルは、さらなるトラブルシューティングやレポートでの使用のためにコピーできます。ポリシーのGPO時間は、イベントビューアーログから取得されます。ログは、運用ログに割り当てられたメモリ（デフォルトサイズは4 MB）によって上書きされる可能性があります。運用ログのログサイズを増やす方法の詳細については、Microsoft TechNetの記事「イベントログの構成」を参照してください。

ログオンスクリプト

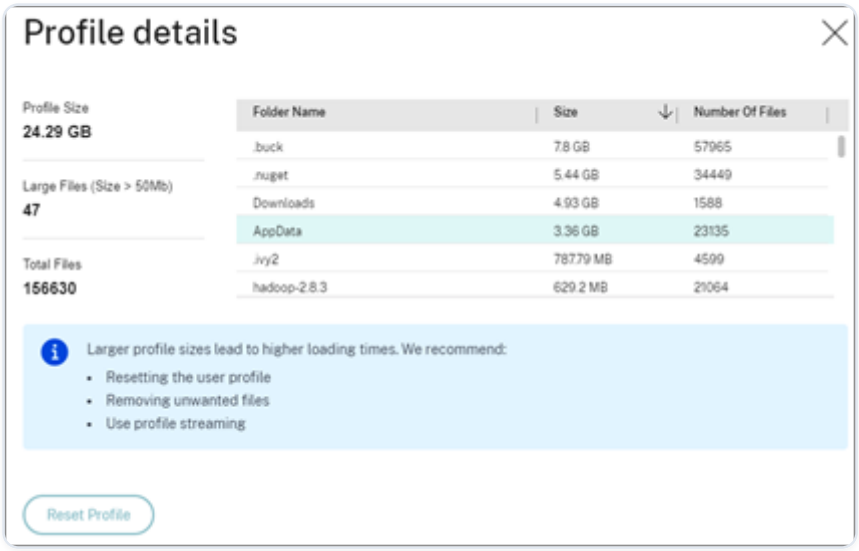
セッションにログオンスクリプトが構成されている場合、これはログオンスクリプトの実行にかかる時間です。

プロファイル読み込み

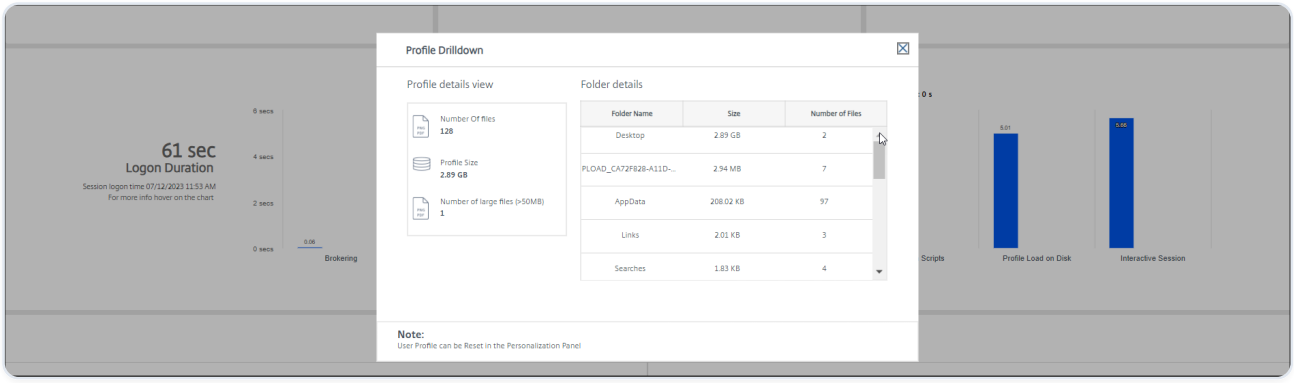
ユーザーまたは仮想マシンにプロファイル設定が構成されている場合、これはプロファイルの読み込みにかかる時間です。

Citrix Profile Managementが構成されている場合、プロファイルロードバーには、Citrix Profile Managementがユーザープロファイルを処理するのにかかった時間が含まれます。この情報は、管理者がプロファイル処理時間の長い問題をトラブルシューティングするのに役立ちます。Profile Managementが構成されている場合、プロファイルロードバーには増加した期間が表示されます。この増加は、この機能強化によって引き起こされるものであり、パフォーマンスの低下を反映するものではありません。この機能強化は、VDA 1903以降で利用可能です。

プロファイルロードバーにカーソルを合わせると、現在のセッションのユーザープロファイルの詳細を示すツールチップが表示されます。



「**詳細**」をクリックすると、プロファイルルートフォルダー内の個々のフォルダー（例：C:/Users/username）、そのサイズ、およびファイル数（ネストされたフォルダー内のファイルを含む）にさらにドリルダウンできます。



プロファイルドリルダウンは、Delivery Controllerバージョン7 1811以降およびVDA 1811以降で利用できます。プロファイルドリルダウン情報を使用すると、プロファイルロード時間が長いことに関する問題を解決できます。次のことができます。

- ユーザープロファイルをリセットする
- 不要な大きなファイルを削除してプロファイルを最適化する
- ネットワーク負荷を軽減するためにファイル数を減らす
- プロファイルストリーミングを使用する

デフォルトでは、プロファイルルート内のすべてのフォルダーがドリルダウンに表示されます。フォルダーの表示を非表示にするには、VDAマシンで次のレジストリ値を編集します。

> **警告:**

> レジストリを誤って追加または編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決されることを保証しません。レジストリエディターはご自身の責任において使用してください。編集する前に必ずレジストリをバックアップしてください。

1. VDAで、HKEY_LOCAL_MACHINE\Software\Citrix\Director\ に新しいレジストリ値 **ProfileFoldersNameHidden** を追加します。
2. 値を1に設定します。この値はDWORD（32ビット）値である必要があります。これでフォルダー名の表示が無効になります。
3. フォルダー名を再度表示するには、値を0に設定します。

> **注：** GPOまたはPowerShellコマンドを使用して、複数のマシンにレジストリ値の変更を適用できます。GPOを使用してレジストリの変更を展開する方法の詳細については、ブログを参照してください。

追加情報

- プロファイルドリルダウンは、リダイレクトされたフォルダーを考慮しません。
- ルートフォルダー内のNTUser.datファイルは、エンドユーザーには表示されない場合があります。ただし、これらはプロファイルドリルダウンに含まれ、**ルートフォルダー**のファイルリストに表示されます。
- AppDataフォルダー内の一部の隠しファイルは、プロファイルドリルダウンに含まれません。
- 特定のWindowsの制限により、ファイル数とプロファイルサイズデータがパーソナライゼーションパネルのデータと一致しない場合があります。

対話型セッション

対話型セッションとは、ユーザープロファイルが読み込まれた後、キーボードとマウスの制御をユーザーに「引き渡す」のにかかる時間です。通常、ログオンプロセスのすべてのフェーズの中で最も長い期間であり、**対話型セッション期間 = デスクトップ準備完了イベントのタイムスタンプ (VDA上のEventId 1000) - ユーザープロファイル読み込み完了イベントのタイムスタンプ (VDA上のEventId 2)** として計算されます。対話型セッションには、Pre-userinit、Userinit、Shellの3つのサブフェーズがあります。対話型セッションにカーソルを合わせると、次のツールヒントが表示されます。

- サブフェーズ

- 各サブフェーズにかかった時間
- これらのサブフェーズ間の合計累積時間遅延

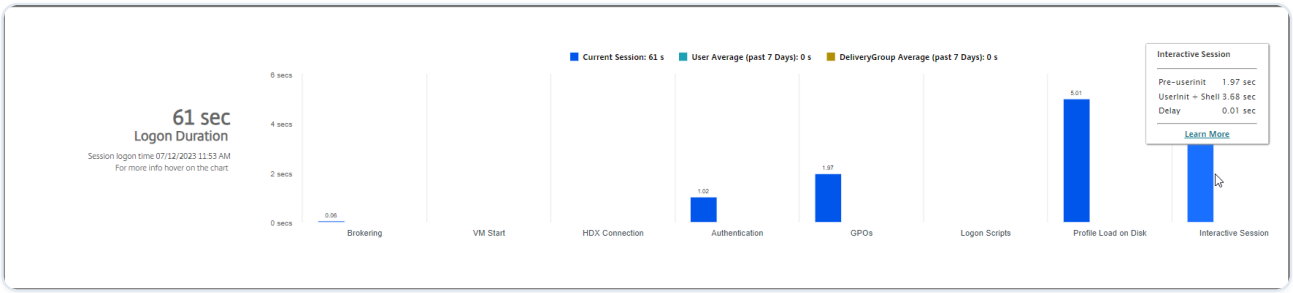
注:

この機能はVDA 1811以降で利用できます。7.18より前のサイトでセッションを起動し、その後7.18以降にアップグレードした場合、「サーバーエラーのためドリルダウンを利用できません」というメッセージが表示されます。ただし、アップグレード後にセッションを起動した場合は、エラーメッセージは表示されません。

各サブフェーズの期間を表示するには、VM (VDA) で監査プロセス追跡を有効にします。監査プロセス追跡が無効になっている場合 (デフォルト)、Pre-userinitの期間と、UserinitおよびShellの合計期間が表示されます。監査プロセス追跡は、グループポリシーオブジェクト (GPO) を使用して次のように有効にできます。

1. GPOを作成し、GPOエディターを使用して編集します。
2. **コンピューターの構成 > Windows の設定 > セキュリティの設定 > ローカル ポリシー > 監査ポリシー** に移動します。
3. 右側のペインで、**監査プロセス追跡** をダブルクリックします。
4. **成功** を選択し、OKをクリックします。
5. このGPOを必要なVDAまたはグループに適用します。

監査プロセス追跡とその有効化または無効化の詳細については、Microsoft ドキュメントの監査プロセス追跡を参照してください。



ユーザー詳細ビューのログオン時間パネル。

- **対話型セッション – Pre-userinit:** グループポリシーオブジェクトとスクリプトと重複する対話型セッションのセグメント。このサブフェーズは、GPOとスクリプトを最適化することで短縮できます。

- **対話型セッション – Userinit:** ユーザーがWindowsマシンにログオンすると、Winlogonはuserinit.exeを実行します。userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立し、その後Windowsユーザーインターフェイスであるexplorer.exeを起動します。対話型セッションのこのサブフェーズは、Userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。
- **対話型セッション – Shell:** 前のフェーズで、UserinitはWindowsユーザーインターフェイスの初期化を開始します。シェルサブフェーズは、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの期間を捕捉します。
- **遅延:** これは、**Pre-userinitとUserinit**サブフェーズ間、および**UserinitとShell**サブフェーズ間の累積時間遅延です。

合計ログオン時間は、これらのフェーズの正確な合計ではありません。たとえば、一部のフェーズは並行して発生し、一部のフェーズでは、合計よりも長いログオン時間につながる可能性のあるより多くの処理が発生します。 合計ログオン時間には、ICA®アイドル時間は含まれません。これは、ICAファイルのダウンロードとアプリケーションのICAファイル起動の間の時間です。 アプリケーション起動時にICAファイルを自動的に開くには、ICAファイルのダウンロード時にICAファイルを自動的に起動するようにブラウザを設定してください。詳細については、CTX804493を参照してください。

> **注:** ログオン時間グラフは、ログオンフェーズを秒単位で表示します。1秒未満の期間値はサブ秒値として表示されます。1秒を超える値は、最も近い0.5秒に丸められます。グラフは、Y軸の最大値が200秒になるように設計されています。200秒を超える値は、バーの上に実際の値が表示されます。

トラブルシューティングのヒント

グラフ内の異常な値や予期しない値を特定するには、現在のセッションの各フェーズにかかった時間を、このユーザーの過去7日間の平均期間、およびこのデリバリーグループの全ユーザーの過去7日間の平均期間と比較します。

必要に応じてエスカレートします。たとえば、VMの起動が遅い場合、問題はハイパーバイザーにある可能性があるため、ハイパーバイザー管理者にエスカレートできます。または、ブローカリング時間が遅い場合、サイト管理者に問題をエスカレートして、デリバリーコントローラーの負荷分散を確認できます。

以下を含む異常な相違点を調べます。

- 欠落している（現在の）ログオンバー
- 現在の期間とこのユーザーの平均期間との間の大きな不一致。原因は次のとおりです。

  - 新しいアプリケーションがインストールされた。
  - オペレーティングシステムの更新が行われた。
  - 設定変更が行われました。
  - ユーザーのプロファイルサイズが大きい。この場合、プロファイルロードが高くなります。

- ユーザーのログオン数値（現在および平均継続時間）とデリバリーグループの平均継続時間の間に大きな不一致がある。

必要に応じて、**再起動**をクリックしてユーザーのログオンプロセスを監視し、VM起動やブローカリングなどの問題をトラブルシューティングします。

セッションパフォーマンスの問題を診断する

ユーザー詳細ページの**セッションパフォーマンス**タブには、HDX™ユーザーセッション内の問題を特定するのに役立つトラブルシューティングワークフローが強化されています。セッショントポロジとパフォーマンスメトリックパネルは、セッションのコンポーネントビューと複数のパフォーマンスメトリックを単一のビューで関連付け、セッションエクスペリエンスの問題解決にかかる平均時間を短縮します。

セッションパフォーマンスビュー(/en-us/citrix-virtual-apps-desktops/2311/media/dir-session-performance.png)

エンドツーエンドのネットワークホップビュー

エンドツーエンドのネットワークホップビューは、トラブルシューティングワークフローを強化するための次のステップです。**ユーザー詳細** > **セッションパフォーマンス** > **セッショントポロジ**セクションでは、接続されたHDXセッションのエンドツーエンドのネットワークホップビューを視覚的に表現します。

接続されたセッションのセッショントポロジは、セッションパスに関与するコンポーネントとそのメタデータ、コンポーネント間のリンク、およびVDAで公開されているアプリケーションを示します。 さらに、セッションについて以下のセッションパフォーマンスメトリックが表示されます。

- ICA®遅延 - 遅延は基本的にネットワーク遅延です。このパラメーターは、ネットワークが遅いかどうかを示します。
- ICA RTT - ICARTTは、ユーザーのアクションと画面に表示されるグラフィック応答との間の時間間隔です。この測定には、ICA遅延、エンドポイント遅延、およびホスト遅延が含まれます。

このビューを使用して、セッションデータが流れるコンポーネントを理解し、パフォーマンスの問題を引き起こしている可能性のある特定のホップを特定できます。

セッショントポロジビューのパフォーマンスメトリックは、接続状態のHDXセッションでのみ利用可能です。

セッショントポロジのシナリオ

サイトの展開シナリオに応じて、セッションに関与するコンポーネントは、以下のすべてまたは一部です。

- エンドポイント上のCitrix Workspace™ app
- Gatewayサービス/オンプレミスGateway
- Cloud Connector – ハイブリッド接続の場合、GatewayはCloud Connectorを介してDaaSに接続されます。
- VDA

したがって、可能なネットワークトポロジは次のとおりです。

- エンドポイント上のCitrix Workspaceアプリは、Citrix WorkspaceおよびGateway Serviceを介してオンプレミスのVDAに接続します。VDAへの接続にCloud Connectorは使用されません。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2311/media/dir-session-topology1.png)

- エンドポイント上のCitrix Workspaceアプリは、Citrix WorkspaceおよびGateway Serviceを介して、Cloud Connector経由でオンプレミスのVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2311/media/dir-session-topology2.png)

- エンドポイント上のCitrix Workspaceアプリは、StoreFront™およびオンプレミスGatewayを介してオンプレミスVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2311/media/dir-session-topology3.png)

- エンドポイント上のCitrix Workspaceアプリは、StoreFrontを介してオンプレミスVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2311/media/dir-session-topology4.png)

パフォーマンスメトリック

パフォーマンスメトリックパネルでは、ユーザーセッション内の問題を特定するためにリアルタイムメトリックを関連付けることができます。セッションメトリックの傾向は、これらのメトリックが時間の経過とともにどのように機能したかを示すのに役立ちます。

セッションパフォーマンスメトリック(/en-us/citrix-virtual-apps-desktops/2311/media/dir-session-performance-trends.png)

> **注:**
>
> グラフは、セッションが接続されている期間のみプロットされます。
>
> ICARTTとICA Latencyの他に、以下のメトリックが利用可能です。

- Frames Per Second - Frames Per Second は、セッションの応答性を示す重要なメトリックです。 Output Bandwidth Available - Output Bandwidth Available は、VDA からエンドポイントにデータを送信するために利用可能な総帯域幅の測定値です。
- Output Bandwidth Consumed (出力帯域幅消費量) - Output Bandwidth Consumedは、ユーザーにセッションを表示するためにVDAからエンドポイントに送信された実際のデータ量を示します。

Output Bandwidth AvailableとOutput Bandwidth Consumedを分析することで、セッションを提供するために十分な帯域幅が利用可能であるか、またセッションが帯域幅不足の影響を受けているかを検出するのに役立ちます。

シャドウユーザー

Directorから、シャドウユーザー機能を使用して、ユーザーの仮想マシンまたはセッションを直接表示したり操作したりできます。Windows VDAとLinux VDAの両方をシャドウできます。シャドウするマシンにユーザーが接続している必要があります。これは、ユーザーのタイトルバーに表示されているマシン名を確認することで検証できます。

Directorは新しいタブでシャドウを開始します。DirectorのURLからのポップアップを許可するようにブラウザ設定を更新してください。

シャドウイング機能は、**ユーザーの詳細**ビューからアクセスします。ユーザーセッションを選択し、アクティビティマネージャービューまたはセッションの詳細パネルで**シャドウ**をクリックします。

Linux VDAのシャドウ

シャドウイングは、RHEL7.3またはUbuntuバージョン16.04のLinuxディストリビューションを実行している、バージョン7.16以降のLinux VDAで利用できます。

注:

- シャドウイングが機能するには、VDAがDirector UIからアクセス可能である必要があります。したがって、シャドウイングはDirectorクライアントと同じイントラネット内のLinux VDAでのみ可能です。
- Directorは、ターゲットのLinux VDAに接続するためにFQDNを使用します。Directorクライアントが Linux VDAのFQDNを解決できることを確認してください。
- VDAには、python websockifyおよびx11vncパッケージがインストールされている必要があります。
- VDAへのnoVNC接続はWebSocketプロトコルを使用します。デフォルトでは、**ws://** WebSocketプロトコルが使用されます。セキュリティ上の理由から、Citrixは安全な **wss://**プロトコルを使用することを推奨します。各DirectorクライアントとLinux VDAにSSL証明書をインストールしてください。

シャドウイング用にVDAを構成するには、セッションシャドウイングの手順に従ってください。

1. **シャドウ**をクリックすると、シャドウイング接続が初期化され、ユーザーデバイスに確認プロンプトが表示されます。
2. マシンまたはセッションの共有を開始するには、ユーザーに**はい**をクリックするよう指示してください。
3. 管理者はシャドウされたセッションを表示することしかできません。

Windows VDA のシャドウイング

Windows VDA セッションは、Windows リモートアシスタンスを使用してシャドウされます。VDAのインストール中に、**ユーザー Windows リモートアシスタンス**機能を有効にします。詳細については、「機能の有効化または無効化」を参照してください。

1. **シャドウ**をクリックすると、シャドウ接続が初期化され、.msrc インシデントファイルを開くか保存するかを求めるダイアログボックスが表示されます。

2. デフォルトで選択されていない場合は、リモートアシスタンスビューアでインシデントファイルを開きます。ユーザーデバイスに確認プロンプトが表示されます。
3. ユーザーに**はい**をクリックして、マシンまたはセッションの共有を開始するように指示します。
4. さらに制御するには、ユーザーにキーボードとマウスの制御を共有するように依頼します。

シャドウイングのために MICROSOFT INTERNET EXPLORER ブラウザを効率化する

Microsoft Internet Explorer ブラウザを構成して、ダウンロードした Microsoft Remote Assistance (.msra) ファイルをリモートアシスタンスクライアントで自動的に開くようにします。

これを行うには、グループポリシーエディターで「ファイルのダウンロード時に自動的にプロンプトを表示する」設定を有効にする必要があります。

コンピューターの構成 \> 管理用テンプレート \> Windows コンポーネント \> Internet Explorer \> インターネットコントロールパネル \> セキュリティページ \> インターネットゾーン \> ファイルのダウンロード時に自動的にプロンプトを表示する。

デフォルトでは、このオプションはローカルイントラネットゾーンのサイトに対して有効になっています。Director サイトがローカルイントラネットゾーンにない場合は、このゾーンにサイトを手動で追加することを検討してください。

セッションを復元する

セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはサーバーと通信しなくなります。

ユーザー詳細ビューで、**セッションの詳細**パネルでセッションの障害をトラブルシューティングします。セッションIDで示される現在のセッションの詳細を表示できます。

アクション	説明
応答しないアプリケーションまたはプロセスを終了する	**アプリケーション**タブをクリックします。応答しないアプリケーションを選択し、**アプリケーションの終了**をクリックします。同様に、応答しない対応するプロセスを選択し、**プロセスの終了**をクリックします。また、異常に大量のメモリまたはCPUリソースを消費しているプロセスを終了します。これにより、CPUが使用不能になる可能性があります。

アクション	説明
Windowsセッションを切断する	**セッション制御**をクリックし、**切断**を選択します。このオプションは、ブローカーされたマルチセッションOSマシンでのみ利用可能です。ブローカーされていないセッションの場合、このオプションは無効になります。
ユーザーのセッションからログオフする	**セッション制御**をクリックし、**ログオフ**を選択します。

セッションをテストするには、ユーザーはセッションに再度ログオンを試みることができます。このセッションをより詳細に監視するために、ユーザーをシャドウすることもできます。

ユーザープロファイルをリセットする

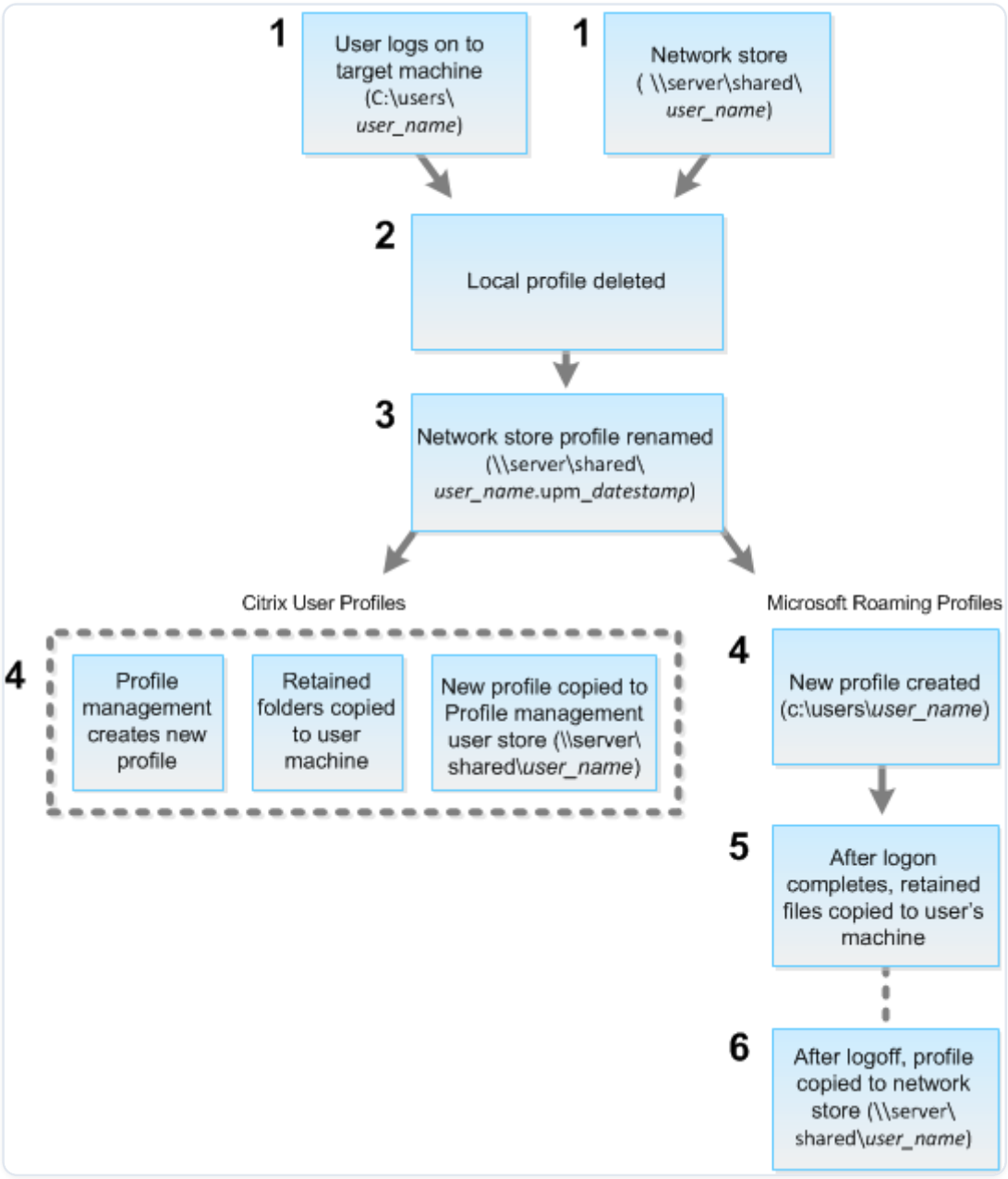
> **注意:**
>
> プロファイルがリセットされると、ユーザーのフォルダーとファイルは保存され、新しいプロファイルにコピーされます。ただし、ほとんどのユーザープロファイルデータは失われます（たとえば、レジストリがリセットされ、アプリケーション設定が削除される可能性があります）。

> Profile Management 2106以降、Citrix Managementプロファイルコンテナベースのユーザープロファイルソリューションでリセット機能が利用可能になりました。

リセットされたプロファイルの処理方法

任意のCitrixユーザープロファイルまたはMicrosoftローミングプロファイルをリセットできます。ユーザーがログオフし、リセットコマンド（DirectorまたはPowerShell SDKを使用して）を選択すると、Directorはまず使用中のユーザープロファイルを識別し、適切なリセットコマンドを発行します。Directorは、プロファイルサイズ、種類、ログオン時間などの情報を含むProfile Managementを介して情報を受け取ります。

この図は、ユーザープロファイルがリセットされた後のユーザーログオンに続くプロセスを示しています。



Directorによって発行されたリセットコマンドは、プロファイルの種類を指定します。その後、Profile Managementサービスはその種類のプロファイルをリセットしようとし、適切なネットワーク共有（ユーザーストア）を探します。ユーザーがProfile Managementによって処理されているにもかかわらず、ローミングプロファイルコマンドを受け取った場合、それは拒否されます（またはその逆）。

1. ローカルプロファイルが存在する場合、それは削除されます。
2. ネットワークプロファイルの名前が変更されます。
3. 次のアクションは、リセットされるプロファイルがCitrixユーザープロファイルかMicrosoftローミングプロファイルかによって異なります。

Citrixユーザープロファイルの場合、新しいプロファイルはProfile Managementのインポートルールを使用して作成されます。フォルダーはネットワークプロファイルにコピーされ、ユーザーは通常どおりログオンできます。リセットにローミングプロファイルが使用される場合、ローミングプロファイル内のレジストリ設定はリセットされたプロファイルに保持されます。必要に応じて、テンプレートプロファイルがローミングプロファイルを上書きするようにProfile Managementを構成できます。

Microsoftローミングプロファイルの場合、Windowsはプロファイルを作成し、ユーザーがログオンすると、フォルダーはユーザーデバイスにコピーされます。ユーザーが再度ログオフすると、新しいプロファイルはネットワークストアにコピーされます。

Directorでユーザープロファイルをリセットするには

Citrix Virtual Desktops™ (Desktop VDA) を使用している場合は、次の操作を行います。

1. **Director** で、プロファイルをリセットするユーザーを検索し、そのユーザーのセッションを選択します。
2. をクリックします。
3. ユーザーにすべてのセッションからログオフするよう指示します。
4. ユーザーに再度ログオンするよう指示します。 ユーザーのプロファイルから保存されたフォルダーとファイルは、新しいプロファイルにコピーされます。

Citrix Virtual Desktops (Server VDA) を使用している場合、プロファイルのリセットを実行するにはログオンしている必要があります。その後、ユーザーはログオフし、再度ログオンしてプロファイルのリセットを完了する必要があります。

> **重要:**

> ユーザーが複数のプラットフォーム（Windows 8やWindows 7など）にプロファイルを持っている場合は、ユーザーが問題として報告したのと同じデスクトップまたはアプリに最初に再度ログオンするよう指示します。このログオン操作により、正しいプロファイルがリセットされます。プロファイルがCitrixユーザープロファイルの場合、ユーザーのデスクトップが表示されるまでにプロファイルはすでにリセットされています。プロファイルがMicrosoftローミングプロファイルの場合、フォルダーの復元が短時間進行中の可能性があります。ユーザーは復元が完了するまでログオンしたままにする必要があります。

> プロファイルが正常にリセットされない場合（たとえば、ユーザーがマシンに正常に再度ログオンできない、または一部のファイルが不足している場合）は、元のプロファイルを手動で復元する必要があります。

次の点に注意してください。

- ユーザープロファイルソリューションとしてユーザーストアが有効になっている場合、新しいプロファイルには元のユーザープロファイルから次の個人用フォルダーが含まれます。
  - デスクトップ
  - クッキー
  - お気に入り
  - ドキュメント
  - ピクチャ
  - ミュージック
  - ビデオ
- Citrix Management プロファイルコンテナがユーザープロファイルソリューション全体として有効になっている場合、新しいプロファイルには上記の個人用フォルダーは含まれません。
- Windows 8以降では、プロファイルがリセットされると、クッキーは新しいプロファイルにコピーされません。

リセットが失敗した後でプロファイルを手動で復元するには

1. ユーザーにすべてのセッションからログオフするよう指示します。
2. ローカルプロファイルが存在する場合は削除します。
3. フォルダー名に日付と時刻が追加された、.upm_datestamp拡張子を持つネットワーク共有上のアーカイブされたフォルダーを見つけます。
4. 現在のプロファイル名を削除します。つまり、upm_datestamp拡張子のないものです。
5. 元のプロファイル名を使用してアーカイブされたフォルダーの名前を変更します。つまり、日付と時刻の拡張子を削除します。これで、プロファイルはリセット前の元の状態に戻りました。

PowerShell SDKを使用してプロファイルをリセットするには

Broker PowerShell SDKを使用してプロファイルをリセットできます。

NEW-BROKERMACHINECOMMAND

特定のユーザー、セッション、またはマシンへの配信のためにキューに入れられたコマンドを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/>`を参照してください。

例

プロファイルをリセットするためにPowerShellコマンドレットを使用する方法の詳細については、以下の例を参照してください。

Profile Management プロファイルをリセットする

- user1 のプロファイルをリセットするとします。New-BrokerMachineCommand PowerShell コマンドを使用します。例:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

> **重要:**
>
> `CommandData $byteArray`は次の形式である必要があります: `<SID>[,<backup path>]`。バックアップパスを指定しない場合、Profile Managementは現在の日時で名前が付けられたバックアップフォルダーを生成します。

Windowsローミングプロファイルをリセットする

- user1 のローミングプロファイルをリセットするとします。New-BrokerMachineCommand PowerShell コマンドを使用します。例:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

セッションを記録する

Director の 画面と 画面にあるセッション記録コントロールを使用して、ICA® セッションを記録できます。この機能は、**Premium** サイトのお客様が利用できます。

動的セッション記録

画面にあるセッション記録コントロールを使用して、現在アクティブなセッションを記録できます。動的セッション記録の詳細については、セッション記録サービス の記事を参照してください。

ポリシーベースのセッション記録

DirectorConfig ツールを使用して Director でポリシーベースのセッション記録を構成するには、セッション記録ポリシーの構成 の「**Director でセッション記録サーバーを使用するように構成する**」セクションを参照してください。 セッション記録コントロールは、ログインしているユーザーがセッション記録ポリシーを変更する権限を持っている場合にのみ Director で利用できます。この権限は、ユーザーの承認 で説明されているように、セッション記録承認コンソールで設定できます。

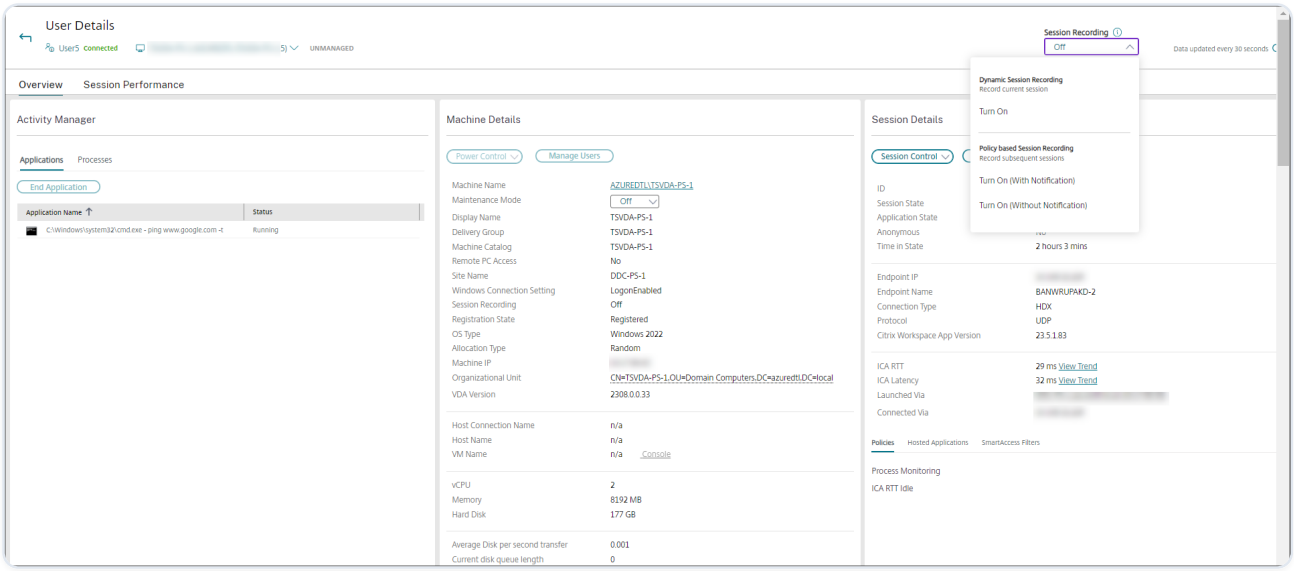
> **注：** Director またはセッション記録ポリシーコンソールを通じてセッション記録設定に加えられた変更は、次回の ICA セッションから有効になります。

Director のセッション記録コントロール

> アクションを使用して、現在または以降のセッションを記録できます。

- 動的セッション記録をオンにする - 現在のセッションが記録されます。
- オンにする（通知あり） - 以降のセッションが記録され、ユーザーが ICA セッションにログオンしたときにセッションが記録されていることが通知されます。
- オンにする（通知なし） - 以降のセッションが記録され、ユーザーに通知することなくセッションがサイレントに記録されます。
- オフにする - ユーザーのセッション記録を無効にします。

パネルには、アクティブなセッション記録ポリシーの名前が表示されます。



マシン詳細パネルには、マシンのセッション記録ポリシーのステータスが表示されます。

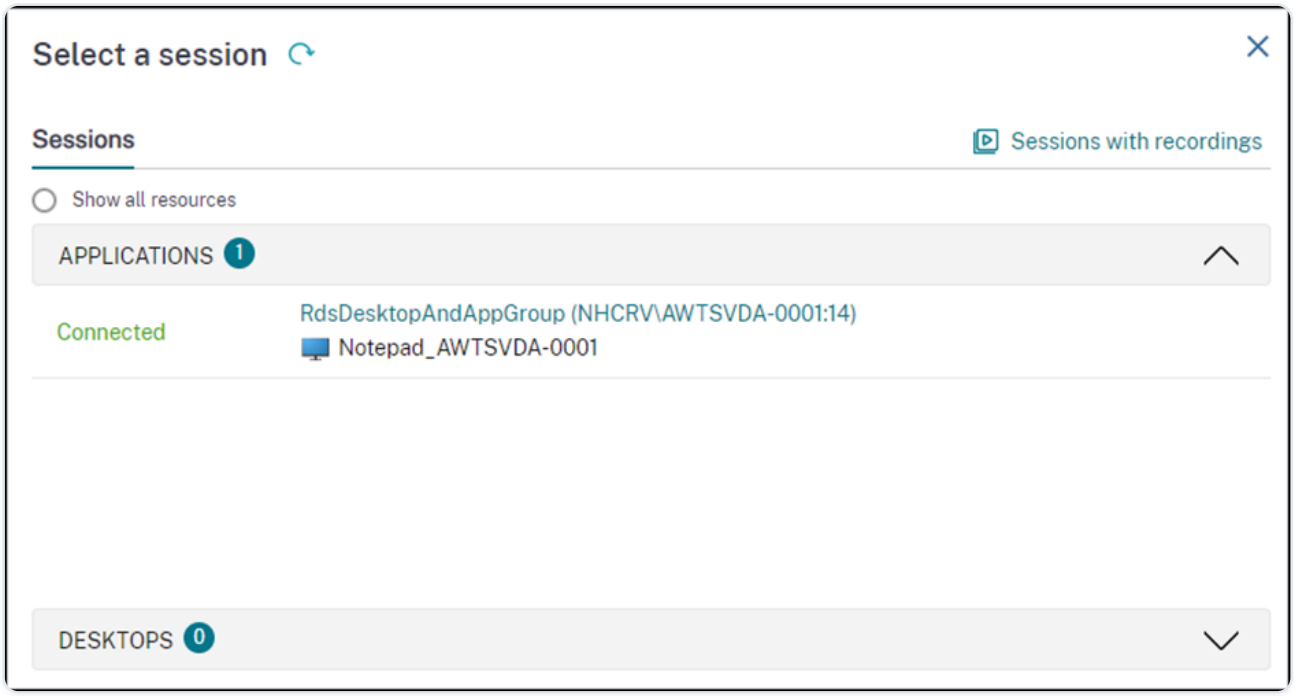
ライブセッションと録画セッションを再生する

記録されたユーザーセッションとライブユーザーセッションを再生して、ユーザーが遭遇した問題を理解できます。Directorコンソール内で記録とセッション関連のメトリックにすぐにアクセスできるため、複数のセッション記録サーバーで記録を検索したり、記録を表示するためのサードパーティ製アプリを探したりする必要がなくなります。これにより、記録で発見された問題とパフォーマンスメトリックを関連付けることができます。

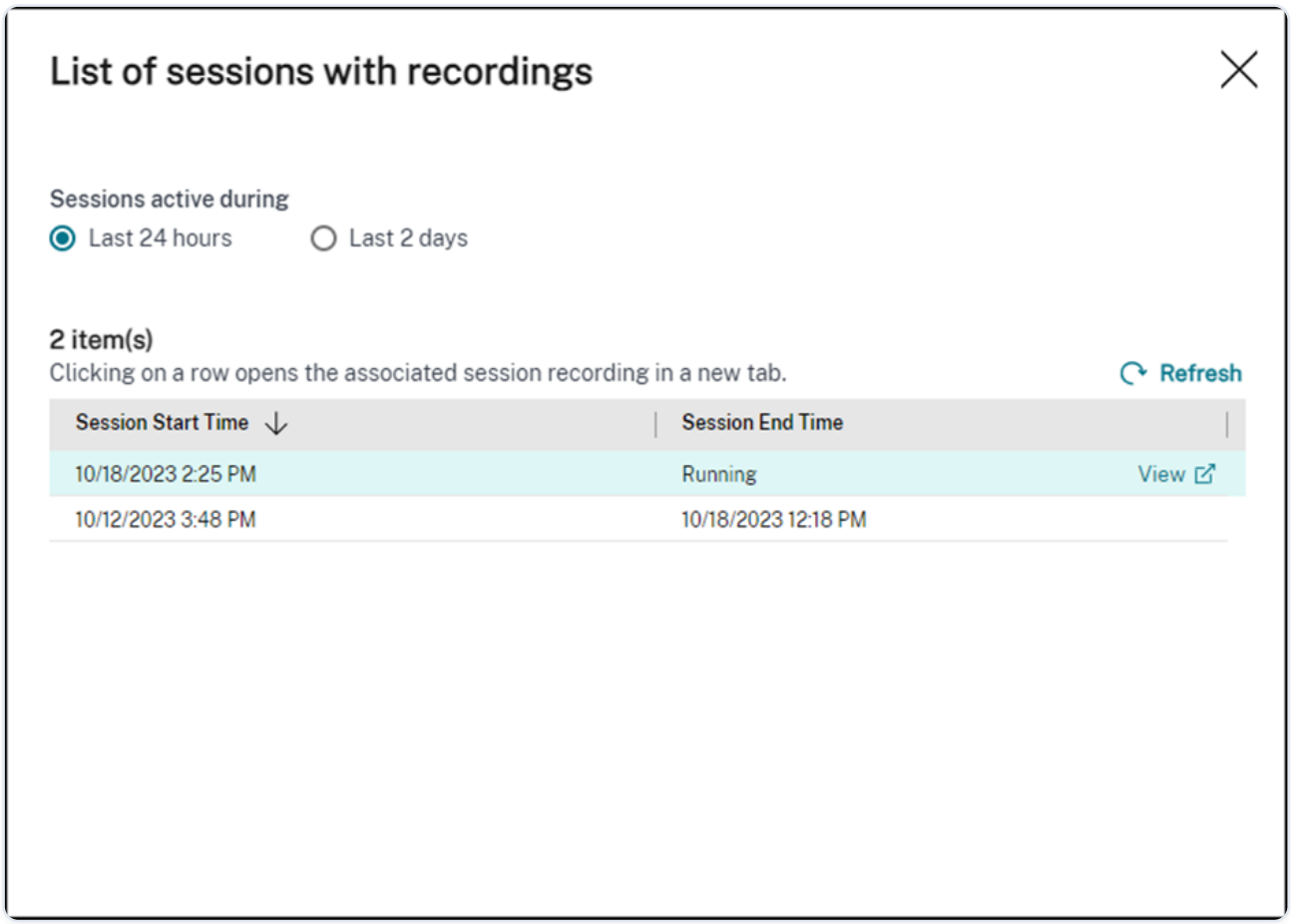
この機能には、以下が必要です。

- VDAおよびセッション記録サーバーはバージョン2308以降であること。
- Delivery Controller™およびDirectorはバージョン2311以降であること。

Directorはセッション記録を一元的なリポジトリに保存します。「**セッションセレクター**」モーダル > 「**記録のあるセッション**」リンクをクリックすると、ユーザーに属する記録のリストが表示されます。



過去24時間または過去2日間にアクティブだったセッションの録画を表示することを選択できます。現在アクティブなセッションのライブ録画は、「**Session End Time**」が「**Running**」と表示されます。



「**表示**」リンクをクリックすると、Citrix Session Recording再生サーバーを使用して新しいタブで記録が再生されます。

機能互換性マトリックス

Citrix Director 7 2203 は以下と互換性があります。

- Citrix Virtual Apps and Desktops™ 7 2112 以降
- Citrix Virtual Apps and Desktops 7 1912 LTSR

各サイト内で、Delivery Controller™ の以前のバージョンでDirectorを使用できますが、Directorの最新バージョンのすべての機能が利用できない場合があります。Citrixは、Director、Delivery Controller、およびVDAを同じバージョンにすることを推奨します。

注：

Delivery Controllerをアップグレードした後、Studioを開くと、サイトのアップグレードを促されます。詳細については、展開のアップグレード の「**アップグレードシーケンス**」セクションを参照してください。

Director のアップグレード後に初めてログインすると、構成済みのサイトでバージョンチェックが実行されます。いずれかのサイトが Director より古いバージョンの Controller を実行している場合、Director コンソールにサイトのアップグレードを推奨するメッセージが表示されます。さらに、サイトのバージョンが Director より古い間は、この不一致を示すメモが Director ダッシュボードに表示され続けます。

注：

以前のバージョンのCitrix Directorでは、最近のVDAバージョンで実行されているユーザーセッションに適用されたポリシーは表示されません。Citrix Director 1912以前のバージョンでは、VDAバージョン2003以降で実行されているユーザーセッションに適用されたポリシーは表示されません。これらのポリシーを表示するには、Citrix Directorバージョン2003以降を使用してください。

必要なDelivery Controller (DC)、VDA、およびその他の依存コンポーネントの最小バージョンとライセンスエディションを含む、特定のDirector機能は以下のとおりです。

DIRECTORのバージョン	機能	依存関係 - 必要な最小バージョン	エディション
2311	ライブおよび録画されたセッションの再生(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/user-issues/record-sessions#play-back-live-and-recorded-sessions)	VDA 2308 および DDC 2311	すべて
2311	セッショントポロジ(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/user-issues/session-performance#session-topology)	なし	すべて
2311	最適な画面解像度(/ja-jp/citrix-virtual-apps-desktops/2311/system-requirements#citrix-director)	なし	すべて
2311	MS Teams の最適化(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/user-issues#microsoft-teams-optimization-status)	VDA 2311 および DDC 最新版	すべて
2311	プローブの概要の機能強化	なし	すべて

DIRECTORのバージョン	機能	依存関係 - 必要な最小バージョン	エディション
2311	セッションログオン期間ビューの刷新	なし	すべて
2308	プローブの概要とドリルダウン	なし	すべて
2308	Citrix Gateway多要素認証に対するCitrix Probe Agentのサポート	シトリックス ゲートウェイ	すべて
2308	ハイパーバイザーアラートの無効化	なし	すべて
2308	セッションエクスペリエンスメトリックの傾向	なし	すべて
2305	Citrix Gateway を介した認証のサポート	なし	すべて
2305	DirectorでのAutoscale管理	なし	すべて
2303	失敗したマシンのアラート	DC 7 2303	プレミアム
2203	TLS 1.3のサポート	-	すべて
2212	AMD GPUで利用可能なリアルタイムGPU使用率	DC 7.14およびVDA 7.14 (64ビットWindowsを実行し、HDX 3D Proが有効になっている)	すべて
2212	「高度なプローブスケジューリング」(/ja-jp/citrix-virtual-apps-desktops/2311/director/probes.html)	DC 7 1906 と Citrix Probe Agent 2209 の組み合わせ	プレミアム

DIRECTORのバージョン	機能	依存関係 - 必要な最小バージョン	エディション
1909	「Citrix Analytics for Performance を使用したオンプレミスサイトの構成」(/ja-jp/citrix-virtual-apps-desktops/2311/director/install-and-configure/onboarding.html)	DC 7 1906 および VDA 1906	すべて
1906	「セッションの自動再接続」(/ja-jp/citrix-virtual-apps-desktops/2311/director/site-analytics/trends.html#available-trends)	DC 7 1906 および VDA 1906	すべて
1906	「セッション起動時間」(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/user-issues/session-startup.html)	DC 7 1906 および VDA 1903	すべて
1906	デスクトッププロービング	DC 7 1906 と Citrix Probe Agent 1903 の組み合わせ	プレミアム
7.9以降	プロファイル読み込みにおけるCitrix Profile Managementの期間	VDA 1903	すべて
1811	プロファイルドリルダウン	DC 7 1811および VDA 1811	すべて

DIRECTORのバージョン	機能	依存関係 - 必要な最小バージョン	エディション
1811	ハイパーバイザーアラート監視	DC 7 1811	プレミアム
1811	アプリケーションプロービング	DC 7 1811 および シトリックス アプリケーション プローブ エージェント 1811	プレミアム
1811	Microsoft RDS ライセンスの正常性	DC 7 1811 および VDA 7.16	すべて
1811	主要な RTOP データ表示	DC 7 1811 および VDA 1808	プレミアム
1808	フィルターデータのエクスポート(/ja-jp/citrix-virtual-apps-desktops/2311/director/site-analytics/filters-data.html)	DC 7 1808	すべて
1808	対話型セッションのドリルダウン(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/user-issues/user-logon.html)	DC 7 1808 および VDA 1808	すべて
1808	GPOのドリルダウン(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/user-issues/user-logon.html)	DC 7 1808 および VDA 1808	すべて

DIRECTORのバージョン	機能	依存関係 - 必要な最小バージョン	エディション
1808	OData API を使用して利用可能なマシンの履歴データ(https://developer-docs.citrix.com/projects/monitor-service-odata-api/en/)	DC 7 1808	すべて
7.18	アプリケーションプロービング	DC 7.18	Premium (以前の Platinum)
7.18	スマートアラートポリシー	DC 7.18	Premium (以前の Platinum)
7.18	ヘルスアシスタントリンク	なし	すべて
7.18	インタラクティブセッションのドリルダウン	なし	すべて
7.17	PIV スマートカード認証	なし	すべて
7.16	アプリケーション分析	DC 7.16 および VDA 7.15	すべて
7.16	OData API バージョン4	DC 7.16	すべて
7.16	Linux VDA ユーザーのシャドウイング	VDA 7.16	すべて
7.16	ドメインローカルグループのサポート(/ja-jp/citrix-virtual-apps-desktops/2311/director/install-and-configure/advanced-configuration.html#d	なし	すべて

DIRECTORのバージョン	機能	依存関係 - 必要な最小バージョン	エディション
	omain-local-group-configuration)		
7.16	マシンコンソールアクセス(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/machines.html#machine-console-access)	DC 7.16	すべて
7.15	アプリケーション障害監視(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/applications.html#real-time-application-monitoring)	DC 7.15およびVDA 7.15	すべて
7.14	アプリケーション中心のトラブルシューティング(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/applications.html)	DC 7.13 および VDA 7.13	すべて
7.14	ディスク監視(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/applications.html#real-time-application-monitoring)	DC 7.14 および VDA 7.14	すべて

DIRECTORのバージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.14	GPU 監視(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/applications.html#real-time-application-monitoring)	DC 7.14 および VDA 7.14	すべて
7.13	セッション詳細パネル上のトランスポートプロトコル(/ja-jp/citrix-virtual-apps-desktops/2311/director/site-analytics.html#session-transport-protocol)	DC 7.x および VDA 7.13	すべて
7.12	ユーザーフレンドリーな接続とマシンの障害説明(/ja-jp/citrix-virtual-apps-desktops/2311/director/site-analytics/filters-data.html)	DC 7.12およびVDA 7.x	すべて
7.12	Enterpriseエディションでの履歴データ可用性の向上(/ja-jp/citrix-virtual-apps-desktops/2311/director/site-analytics/trends.html)	DC 7.12およびVDA 7.x	エンタープライズ
7.12	カスタムレポート(/ja-jp/citrix-virtual-apps-desktops/2311/director/site-analytics/trends.html)	DC 7.12およびVDA 7.x	プレミアム (旧 Platinum)

DIRECTORのバージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.11	リソース使用率レポート(/ja-jp/citrix-virtual-apps-desktops/2311/director/site-analytics/trends.html)	DC 7.11およびVDA 7.11	すべて
7.11	CPU、メモリ、ICA RTT条件に対するアラート機能の拡張	DC 7.11およびVDA 7.11	Premium (以前は Platinum)
7.11	レポートのエクスポート機能の改善	DC 7.11およびVDA 7.x	すべて
7.11	Citrix ADMとの統合	DC 7.11、VDA 7.x、およびMASバージョン11.1ビルド49.16	Premium (以前は Platinum)
7.9	ログオン期間の内訳	DC 7.9 および VDA 7.x	すべて
7.7	プロアクティブな監視とアラート	DC 7.7 および VDA 7.x	プレミアム (旧 プラチナ)
7.7	Windows認証統合	DC 7.x および VDA 7.x	すべて
7.7	シングルセッションおよびマルチセッションOSの使用状況	DC 7.7 および VDA 7.x	プレミアム (旧 プラチナ)
7.6.300	Framehawk仮想チャネルのサポート(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/user-issues/hdx-channel-reports.html)	DC 7.6 と VDA 7.6	すべて

DIRECTORのバージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.6.200	セッション記録の統合(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/user-issues/record-sessions.html)	DC 7.6 と VDA 7.x	プレミアム (旧プラチナ)
7	HDX Insightの統合(/ja-jp/citrix-virtual-apps-desktops/2311/director/install-and-configure/hdx-insight.html)	DC 7.6、VDA 7.x、および Citrix ADM	プレミアム (旧プラチナ)

データの粒度と保持

データ値の集計

Monitor Service は、ユーザーセッションの使用状況、ユーザーログオンパフォーマンスの詳細、セッションの負荷分散の詳細、および接続とマシンの障害情報など、さまざまなデータを収集します。データはカテゴリに応じて異なる方法で集計されます。OData Method API を使用して提示されるデータ値の集計を理解することは、データを解釈するために不可欠です。例:

- 接続されたセッションとマシンの障害は一定期間に発生します。したがって、それらは一定期間の最大値として公開されます。
- ログオン期間は時間の長さを測定するものであり、したがって、一定期間の平均として公開されます。
- ログオン数と接続障害は一定期間の発生回数であるため、したがって、一定期間の合計として公開されます。

同時データ評価

セッションは同時と見なされるために重複している必要があります。ただし、時間間隔が1分の場合、その1分間のすべてのセッション（重複しているかどうかに関わらず）は同時と見なされます。間隔のサイズが非常に小さいため、精度を計算するのに伴うパフォーマンスオーバーヘッド

は、追加される価値に見合いません。セッションが同じ時間内に発生しても、同じ分内に発生しない場合、それらは重複しているとは見なされません。

サマリーテーブルと生データの相関関係

データモデルはメトリックを2つの異なる方法で表します。

- サマリーテーブルは、分、時間、日ごとの時間粒度でメトリックの集計ビューを表します。
- 生データは、セッション、接続、アプリケーション、およびその他のオブジェクトで追跡される個々のイベントまたは現在の状態を表します。

API呼び出し間またはデータモデル自体内でデータを関連付けようとするときは、以下の概念と制限を理解することが重要です。

- **部分的な間隔のサマリーデータはありません。** メトリックのサマリーは、長期間にわたる履歴トレンドのニーズを満たすように設計されています。これらのメトリックは、完全な間隔でサマリーテーブルに集計されます。データ収集の開始時（利用可能な最も古いデータ）または終了時の部分的な間隔には、サマリーデータはありません。1日の集計（Interval=1440）を表示する場合、これは最初と最新の不完全な日にはデータがないことを意味します。これらの部分的な間隔には生データが存在する可能性がありますが、それは決して要約されません。特定のデータ粒度について、最も早い集計間隔と最も遅い集計間隔は、特定のサマリーテーブルから最小および最大の SummaryDate を取得することで判断できます。SummaryDate 列は間隔の開始を表します。Granularity 列は、集計データの期間の長さを表します。
- **時間による相関。** メトリックは、前述のセクションで説明されているように、完全な間隔でサマリーテーブルに集計されます。これらは履歴トレンドに使用できますが、生イベントはトレンド分析のために要約されたものよりも現在の状態に近い場合があります。サマリーと生データの時間ベースの比較では、発生する可能性のある部分的な間隔や期間の開始と終了にはサマリーデータがないことを考慮する必要があります。
- **見逃されたイベントと潜在的なイベント。** 集計テーブルに集約されるメトリックは、イベントが見逃されたり、集計期間に対して潜在的であったりする場合、わずかに不正確になる可能性があります。Monitor Serviceは正確な現在の状態を維持しようとしますが、見逃されたイベントや潜在的なイベントのために、集計テーブルの集計を再計算するために過去に遡ることはありません。
- **接続の高可用性。** 接続の高可用性中、現在の接続のサマリーデータカウントにはギャップが生じますが、セッションインスタンスは引き続き生データで実行されます。
- **データ保持期間。** サマリーテーブルのデータは、生イベントデータのスケジュールとは異なるデータ整理スケジュールで保持されます。データがサマリーテーブルまたは生テーブルから整理されたために、データが欠落している可能性があります。保持期間は、サマリーデータの異

なる粒度によっても異なる場合があります。粒度の低いデータ（分単位）は、粒度の高いデータ（日単位）よりも早く整理されます。データがデータ整理のためにある粒度から欠落している場合、より高い粒度で見つかる可能性があります。API呼び出しは要求された特定の粒度のみを返すため、ある粒度でデータが受信されないからといって、同じ期間のより高い粒度でデータが存在しないという意味ではありません。

- **タイムゾーン。** メトリックはUTCタイムスタンプで保存されます。サマリーテーブルは、時間単位のタイムゾーン境界で集約されます。時間単位の境界に該当しないタイムゾーンの場合、データが集約される場所に関して多少の不一致が生じる可能性があります。

粒度と保持

Directorが取得する集約データの粒度は、要求された時間 (T) スパンの関数です。ルールは次のとおりです。

- 0 \< T \<= 1時間 - 分単位の粒度を使用
- 0 \< T \<= 30日 - 時間単位の粒度を使用
- T \> 31日 - 日単位の粒度を使用

集約データから取得されない要求データは、生のセッションおよび接続情報から取得されます。このデータは急速に増加する傾向があるため、独自のデータ整理設定があります。データ整理により、関連データのみが長期的に保持されます。データ整理は、レポートに必要な粒度を維持しながら、より良いパフォーマンスを保証します。Premiumライセンスサイトのお客様は、データ整理保持期間を希望する保持日数に変更できます。変更しない場合は、デフォルトが使用されます。サイトデータベースとの接続が失われた場合、Monitor Serviceは以下の表で指定されているPremiumエンタイトルメントのデフォルトの保持日数を使用します。

設定にアクセスするには、Delivery Controller™で次のPowerShellコマンドを実行します。

```
asnp Citrix.*

 Get-MonitorConfiguration

 Set-MonitorConfiguration -<setting name> <value>
```

	設定名	影響を受けるデータ整理	PREMIUMの保持日数	ADVANCEDの保持日数
1	GroomSessionsRetentionDays	セッション終了後のセッション	90	31

	設定名	影響を受けるデータ整理	PREMIUMの保持日数	ADVANCEDの保持日数
		および接続レコードの保持		
2	GroomFailuresRetentionDays	MachineFailureLog および ConnectionFailureLog レコード	90	31
3	GroomLoadIndexesRetentionDays	LoadIndex レコード	90	31
4	GroomDeletedRetentionDays	「Deleted」の LifecycleState を持つ Machine、Catalog、DesktopGroup、および Hypervisorエンティティ。この設定は、関連するSession、SessionDetail、Summary、Failure、または LoadIndexレコードも削除します。	90	31
5	GroomSummariesRetentionDays	DesktopGroupSummary、FailureLogSummary、および LoadIndexSummaryレコード。集計データ - 日次粒度。	365	31

	設定名	影響を受けるデータ整理	PREMIUMの保持日数	ADVANCEDの保持日数
6	GroomMachineHotfixLogRetentionDays	VDAおよびControllerマシンに適用されたホットフィックス	90	31
7	GroomMinuteRetentionDays	集計データ - 分単位の粒度	3	3
8	GroomHourlyRetentionDays	集計データ - 時間単位の粒度	32	31
9	GroomApplicationInstanceRetentionDays	アプリケーションインスタンス履歴	90	該当なし
10	GroomNotificationLogRetentionDays	通知ログレコード	90	該当なし
11	GroomResourceUsageRawDataRetentionDays	リソース使用率データ - 生データ	3	3
12	GroomResourceUsageMinuteDataRetentionDays	リソース使用率サマリーデータ - 分単位の粒度	7	7
13	GroomResourceUsageHourDataRetentionDays	リソース使用率サマリーデータ - 時間単位の粒度	30	30
14	GroomResourceUsageDayDataRetentionDays	リソース使用率サマリーデータ - 日単位の粒度	365	31

	設定名	影響を受けるデータ整理	PREMIUMの保持日数	ADVANCEDの保持日数
15	GroomProcessUsageRawDataRetentionDays	プロセス使用率データ - 生データ	1	1
16	GroomProcessUsageMinuteDataRetentionDays	プロセス使用率データ - 分単位の粒度	3	3
17	GroomProcessUsageHourDataRetentionDays	プロセス使用率データ - 時間単位の粒度	7	7
18	GroomProcessUsageDayDataRetentionDays	プロセス使用率データ - 日単位の粒度	30	30
19	GroomSessionMetricsDataRetentionDays	セッションメトリックデータ	1	1
20	GroomMachineMetricDataRetentionDays	マシンメトリックデータ	3	3
21	GroomMachineMetricDaySummaryDataRetentionDays	マシンメトリックサマリーデータ	365	31
22	GroomApplicationErrorsRetentionDays	アプリケーションエラーデータ	1	1
23	GroomApplicationFaultsRetentionDays	アプリケーション障害データ	1	1

注意:

> Monitor Serviceデータベースの値を変更した場合、新しい値を有効にするにはサービスを再起動する必要があります。Monitor Serviceデータベースへの変更は、Citrixサポートの指示の下でのみ行うことをお勧めします。

> GroomProcessUsageRawDataRetentionDays、GroomResourceUsageRawDataRetentionDays、およびGroomSessionMetricsDataRetentionDaysの設定は、デフォルト値の1に制限されており、GroomProcessUsageMinuteDataRetentionDaysはデフォルト値の3に制限されています。これらの値を設定するPowerShellコマンドは、プロセス使用状況データが急速に増加する傾向があるため、無効になっています。 また、ライセンスベースの保持設定は次のとおりです。

- **Premiumライセンスサイト -** すべての設定のグルーミング保持期間は1000日に制限されています（Citrixは365日を推奨）。
- **Advancedライセンスサイト -** すべての設定のグルーミング保持期間は31日に制限されています。
- **その他のすべてのサイト -** すべての設定のグルーミング保持期間は7日間に制限されます。

例外:

- GroomApplicationInstanceRetentionDaysは、Premiumライセンスサイトでのみ設定できます。
- GroomApplicationErrorsRetentionDaysおよびGroomApplicationFaultsRetentionDaysは、Premiumライセンスサイトでは31日間に制限されます。

長期間データを保持すると、テーブルサイズに以下の影響があります:

- **時間単位のデータ。** 時間単位のデータを最大2年間データベースに保持できるようにすると、1000のデリバリーグループを持つサイトでは、データベースが次のように増加する可能性があります。

  1000のデリバリーグループ x 24時間/日 x 365日/年 x 2年 = 17,520,000行のデータ。集計テーブルにこれほど大量のデータがあると、パフォーマンスへの影響は甚大です。ダッシュボードデータはこのテーブルから取得されるため、データベースサーバーへの要件は大きくなる可能性があります。過度に大量のデータは、パフォーマンスに劇的な影響を与える可能性があります。
- **セッションおよびイベントデータ。** セッションが開始され、接続/再接続が行われるたびに収集されるデータです。大規模なサイト（10万ユーザー）の場合、このデータは急速に増加します。たとえば、これらのテーブルの2年分のデータは1TBを超えるデータとなり、ハイエンドのエンタープライズレベルのデータベースが必要になります。

Citrix Director の障害理由とトラブルシューティング

以下の表は、さまざまな障害カテゴリ、その理由、および問題を解決するために必要なアクションについて説明しています。詳細については、「列挙型、エラーコード、および説明」を参照してください。

接続障害エラー

カテゴリ	理由	問題	アクション
該当なし	[0] 不明。このエラーコードはマッピングされていません。	監視サービスは、ブローカリングサービスから共有された情報から、報告された起動または接続障害の理由を判断できません。	コントローラーでCDFログを収集し、Citrixサポートに連絡してください。
[0] なし	[1] なし	なし	該当なし
[2] マシン障害	[2] セッション準備	デリバリーコントローラーからVDAへのセッション準備要求が失敗しました。考えられる原因: コントローラーとVDA間の通信の問題、準備要求の作成中にBroker Serviceで発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題。	コントローラーとVDA間の通信の問題を引き起こす一般的な問題については、ナレッジセンターの記事「Citrix Virtual Apps and Desktopsにおけるデリバリーコントローラーへの Virtual Delivery Agent登録のトラブルシューティング」に記載されているトラブルシューティング手順を参照してください。
[2] マシン障害	[3] 登録タイムアウト	VDAは電源がオンになっていましたが、デリバリーコントローラーへの登録を試行中にタイムアウトが発生しました。	デリバリーコントローラーでCitrix Broker Serviceが実行されていること、およびVDAでDesktop Serviceが実

カテゴリ	理由	問題	アクション
			行されていることを確認します。停止している場合は、それぞれを開始します。
[1] クライアント接続障害	[4] 接続タイムアウト	VDAがセッション起動の準備を完了した後、クライアントがVDAに接続しませんでした。セッションは正常に仲介されましたが、クライアントがVDAに接続するのを待っている間にタイムアウトが発生しました。考えられる原因: ファイアウォール設定、ネットワークの中断、またはリモート接続を妨げる設定。	Directorコンソールで、クライアントが現在アクティブな接続を持っているかどうかを確認します。これは、ユーザーに影響がないことを意味します。セッションが存在しない場合は、クライアントとVDAのイベントログでエラーがないか確認します。クライアントとVDA間のネットワーク接続に関する問題を解決します。
[4] 利用可能なライセンスなし	[5] ライセンス	ライセンス要求が失敗しました。考えられる原因: ライセンス数が不足している、またはライセンスサーバーが30日以上ダウンしている。	ライセンスサーバーがオンラインで到達可能であることを確認します。ライセンスサーバーへのネットワーク接続の問題を解決するか、ライセンスサーバーが誤動作しているように見える場合は再起動します。環境内に十分なライセンスがあることを確認し、必要に応じて追加で割り当てます。

カテゴリ	理由	問題	アクション
[1] ClientConnectionFailure	[6] チケット対応	チケット発行中にエラーが発生しました。これは、VDA へのクライアント接続が仲介された要求と一致しないことを示しています。起動要求チケットは Broker によって準備され、ICA® ファイルで配信されます。ユーザーがセッションを起動しようとすると、VDA は ICA ファイル内の起動チケットを Broker と照合して検証します。考えられる原因：ICA ファイルが破損しているか、ユーザーが不正な接続を試みている。	デリバリーグループで定義されているユーザーグループに基づいて、ユーザーがアプリケーションまたはデスクトップにアクセスできることを確認します。ユーザーにアプリケーションまたはデスクトップを再起動するよう指示し、これが一時的な問題であるかどうかを判断します。問題が再度発生する場合は、クライアントデバイスのイベントログでエラーを確認します。ユーザーが接続しようとしているVDAが登録されていることを確認します。未登録の場合は、VDA のイベントログを確認し、登録に関する問題を解決します。
[1] ClientConnectionFailure	[7] その他	クライアントが最初に VDA に接続した後、接続シーケンスが完了する前に、セッションが VDA から終了したと報告されました。	起動前にユーザーによってセッションが終了されていないか確認します。セッションの再起動を試み、問題が解決しない場合は、CDF ログを収集して Citrix サポートに連絡してください。

カテゴリ	理由	問題	アクション
[1] ClientConnectionFailure	[8] GeneralFail	セッションの起動に失敗しました。考えられる原因：Brokerが起動中または初期化中に仲介された起動が要求された、または起動の仲介フェーズ中に内部エラーが発生した。	Citrix Broker Serviceが実行されていることを確認し、セッションの起動を再試行します。
[5] 設定	[9] MaintenanceMode	VDA、またはVDAが属するデリバリーグループがメンテナンスモードに設定されています。	メンテナンスモードが必要かどうかを判断します。不要な場合は、該当するデリバリーグループまたはマシンでメンテナンスモードを無効にし、ユーザーに再接続を試みるよう指示します。
[5] 構成	[10] アプリケーション無効	アプリケーションは管理者によって無効にされているため、エンドユーザーはアクセスできません。	アプリケーションが本番環境で使用される予定である場合は、アプリケーションを有効にし、ユーザーに再接続するよう指示します。
[4] 利用可能なライセンスなし	[11] ライセンス機能拒否	使用されている機能は、既存のライセンスではカバーされていません。	既存のCitrix Virtual Apps and Desktops™ライセンスのエディションとタイプでカバーされている機能を確認するには、Citrixの営業担当者にお問い合わせください。
[3] 利用可能な容量なし	[13] セッション制限に到達	すべてのVDAが使用中であり、これ以上	メンテナンスモードになっているVDAが

カテゴリ	理由	問題	アクション
		セッションをホストする容量がありません。考えられる原因：すべてのVDAが使用中である（シングルセッションOS VDAの場合）、またはすべてのVDAが設定された最大同時セッション数に達している（マルチセッションOS VDAの場合）。	ないか確認します。容量を増やすために不要な場合は、メンテナンスモードを無効にします。Citrixポリシー設定の**最大セッション数**の値を増やして、サーバーVDAあたりのセッション数を増やすことを検討してください。マルチセッションOS VDAを追加することを検討してください。シングルセッションOS VDAを追加することを検討してください。
[5] 構成	[14] DisallowedProtocol	ICAおよびRDPプロトコルは許可されていません。	デリバリーコントローラーで **Get-BrokerAccessPolicyRule** PowerShellコマンドを実行し、**AllowedProtocols** の値に目的のプロトコルがすべてリストされていることを確認します。この問題は、設定ミスがある場合にのみ発生します。
[5] 構成	[15] ResourceUnavailable	ユーザーが接続しようとしているアプリケーションまたはデスクトップは利用できません。このアプリケーションまたはデスクトップが存在しないか、実行でき	アプリケーションまたはデスクトップがまだ公開されており、VDAがメンテナンスモードではないことを確認します。マルチセッションOS VDAがフルロード状

カテゴリ	理由	問題	アクション
		るVDAがありません。考えられる原因: アプリケーションまたはデスクトップが非公開になっている、または、アプリケーションまたはデスクトップをホストしているVDAが最大負荷に達している、または、アプリケーションまたはデスクトップがメンテナンスモードに設定されている。	態であるかどうかを判断します。もしそうであれば、さらにマルチセッションOS VDAをプロビジョニングします。接続に利用できるシングルセッションOS VDAがあることを確認します。必要に応じて、さらにシングルセッションOS VDAをプロビジョニングします。
[5] 構成	[16] ActiveSessionReconnectDisabled	ICAセッションはアクティブで、別のエンドポイントに接続されています。ただし、**Active Session Reconnection** が無効になっているため、クライアントはアクティブなセッションに接続できません。	デリバリーコントローラーで、**Active Session Reconnection** が有効になっていることを確認します。レジストリの **HKEY_LOCAL_MACHINE\Software\Citrix\Desktop\Server** の下にある **DisableActiveSessionReconnect** の値が0に設定されていることを確認します。
[2] MachineFailure	[17] NoSessionToReconnect	クライアントは特定のセッションに再接続しようとしましたが、セッションは終了しました。	ワークスペースコントロールの再接続を再試行してください。
[2] MachineFailure	[18] SpinUpFailed	セッション起動のためにVDAの電源をオ	マシンの電源がまだオフになっている場

カテゴリ	理由	問題	アクション
		ンにできません。これはハイパーバイザーが報告した問題です。	合は、Citrix Studioからマシンの起動を試みてください。これが失敗した場合は、ハイパーバイザーの接続と権限を確認してください。VDAがPVSプロビジョニングされたマシンの場合は、PVSコンソールでマシンが実行中であることを確認してください。そうでない場合は、マシンにPersonal vDiskが割り当てられていることを確認し、ハイパーバイザーにログインしてVMをリセットしてください。
[2] MachineFailure	[19] 拒否	デリバリーコントローラーは、エンドユーザーからの接続に備えるようVDAに要求を送信しますが、VDAはこの要求を積極的に拒否します。	pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認してください。通信できない場合は、ファイアウォールまたはネットワークルーティングの問題を解決してください。
[2] MachineFailure	[20] 構成セットの失敗	デリバリーコントローラーは、セッション起動中にポリシー設定やセッション情報などの必要な構成データをVDAに送信しませんでし	-

カテゴリ	理由	問題	アクション
		た。考えられる原因：コントローラーとVDA間の通信の問題、構成セット要求の作成中にBroker Serviceで発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題。	
[3] NoCapacityAvailable	[21] MaxTotalInstancesExceeded	アプリケーションのインスタンスの最大数に達しました。VDA上でアプリケーションの追加インスタンスを開くことはできません。この問題は、アプリケーション制限機能に関連しています。	ライセンスが許す場合、アプリケーション設定の「**同時に実行するインスタンスの数を制限する**」をより高い値に増やすことを検討してください。
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	ユーザーがアプリケーションの複数のインスタンスを開こうとしていますが、アプリケーションはユーザーごとに1つのインスタンスのみを許可するように構成されています。この問題は、アプリケーション制限機能に関連しています。	デフォルトでは、ユーザーごとにアプリケーションのインスタンスは1つのみ許可されています。ユーザーごとに複数のインスタンスが必要な場合は、アプリケーション設定の「**ユーザーごとに1つのインスタンスに制限する**」設定をクリアすることを検討してください。
[1] ClientConnectionFailure	[23] 通信エラー	デリバリーコントローラーは、接続の準備要求などの情報をVDAに送信しよう	既に開始されている場合は、VDA上のデスクトップサービスを再起動して登録プ

カテゴリ	理由	問題	アクション
		としましたが、通信中にエラーが発生しました。これはネットワーク障害が原因である可能性があります。	ロセスを再開し、VDAが正常に登録されていることを確認してください。アプリケーションイベントログの詳細を通じて、VDA用に構成されたデリバリーコントローラーが正確であることを確認してください。
[3] NoCapacityAvailable	[100] NoMachineAvailable 監視サービスは [12] NoDesktopAvailable をこのエラーコードに変換します。	セッションを起動するために割り当てられたVDAが無効な状態であるか、利用できません。考えられる原因：VDAの電源状態が不明または利用できない、VDAが前回のユーザーセッション以降に再起動されていない、現在のセッションで有効にする必要があるにもかかわらずセッション共有が無効になっている、またはVDAがデリバリーグループまたはサイトから削除された。	VDAがデリバリーグループ内にあることを確認してください。そうでない場合は、適切なデリバリーグループに追加してください。公開された共有デスクトップまたはユーザーが要求したアプリケーションを起動できるように、十分なVDAが登録され、準備状態にあることを確認してください。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認してください。
[2] MachineFailure	[101] MachineNotFunctional. 監視サービスは [12] NoDesktopAvailable をこのエラーコードに変換します。	VDAが動作していません。考えられる原因：VDAがデリバリーグループから削除された、VDAが登録解除されている、VDAの電源状態が利	VDAがデリバリーグループに属していることを確認します。属していない場合は、適切なデリバリーグループに追加します。Citrix Studio

カテゴリ	理由	問題	アクション
		用できない、またはVDAが内部的な問題を抱えている。	でVDAが電源オンとして表示されていることを確認します。複数のマシンの電源状態が不明な場合は、ハイパーバイザーへの接続に関する問題またはホストの障害を解決します。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認します。これらの問題が解決されたら、VDAを再起動します。

マシン障害の種類

エラーコード	エラーコードID	問題	アクション
不明	-	-	-
未登録	3	-	-
MaxCapacity (Directorでは最大負荷として表示)	4	マシンが最大容量、つまり最大負荷インデックスに達していると報告しています	すべてのハイパーバイザーの電源がオンになっていることを確認します。ハイパーバイザーの容量を増やすか、ハイパーバイザーを追加することで、影響を受けるデリバリーグループにマシンを追加します。
StuckOnBoot	2	VMが起動シーケンスを完了せず、ハイ	VMがハイパーバイザー上で正常に起動したことを確認しま

エラーコード	エラーコードID	問題	アクション
		パーバイザーと通信していません。	す。OSの問題など、VM上の他のメッセージを確認します。ハイパーバイザーツールがVMにインストールされていることを確認します。VDAがVMにインストールされていることを確認します。
FailedToStart	1	VMがハイパーバイザー上で起動しようとしたときに問題が発生しました。	ハイパーバイザーのログを確認します。
なし	0	-	-

マシンの登録解除理由 (障害の種類が「未登録」または「不明」の場合に適用)

エラーコード	エラーコードID	問題	アクション
AgentShutdown	0	VDAが正常にシャットダウンされました。	既存の電源管理ポリシーに基づいてVDAがオフになっていることが予期されない場合は、VDAの電源をオンにしてください。イベントログでエラーを確認してください。
AgentSuspended	1	VDAは休止状態またはスリープモードです。	VDAを休止モードから解除してください。電源設定を介してCitrix Virtual Apps and Desktops VDAの休止状態を無効にす

エラーコード	エラーコードID	問題	アクション
			ることを検討してください。
IncompatibleVersion	100	Citrixプロトコルバージョンの不一致により、VDAがデリバリーコントローラーと通信できません。	VDAとデリバリーコントローラーのバージョンを合わせてください。
AgentAddressResolutionFailed	101	デリバリーコントローラーがVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は修正します。広範囲にわたる場合は、デリバリーコントローラーのDNS設定を検証します。コントローラーから`nslookup`コマンドを実行してDNS解決を確認します。
[Cloud]:AgentAddressResolutionFailed	101	デリバリーコントローラーがVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は修正します。
AgentNotContactable	102	デリバリーコントローラーとVDA間で	pingを使用して、デリバリーコントロー

エラーコード	エラーコードID	問題	アクション
		通信の問題が発生しました。	ラーとVDAが正常に通信できることを確認します。通信できない場合は、ファイアウォールまたはネットワークの問題を解決します。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
[Cloud]: AgentNotContactable	102	デリバリーコントローラーとVDAの間で通信の問題が発生しました。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手

エラーコード	エラーコードID	問題	アクション
			順を参照してください。Citrixサポートにお問い合わせください。
AgentWrongActiveDirectoryOU	103	Active Directoryの検出設定に誤りがあります。VDAレジストリで構成されているサイト固有のOU（サイトコントローラー情報がADに保存されている場所）が、別のサイト用になっています。	Active Directoryの設定が正しいことを確認するか、レジストリ設定を確認してください。
EmptyRegistrationRequest	104	VDAからデリバリーコントローラーに送信された登録要求が空でした。これは、VDAソフトウェアのインストールが破損していることが原因である可能性があります。	登録プロセスを再開するには、VDA上のDesktopサービスを再起動し、アプリケーションイベントログを介してVDAが正しく登録されていることを確認してください。
MissingRegistrationCapabilities	105	VDAのバージョンがデリバリーコントローラーと互換性がありません。	VDAをアップグレードするか、VDAを削除してから再インストールします。
MissingAgentVersion	106	VDAのバージョンがデリバリーコントローラーと互換性がありません。	問題がすべてのマシンに影響している場合は、VDAソフトウェアを再インストールしてください。
InconsistentRegistrationCapabilities	107	VDAはBrokerにその機能を伝えることができません。これは、VDAとデリバ	VDAとデリバリーコントローラーのバー

エラーコード	エラーコードID	問題	アクション
		リーコントローラーのバージョン間の非互換性が原因である可能性があります。バージョンごとに変更される登録機能は、登録要求と一致しない形式で表現されています。	ジョンを合わせます。
NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixライセンスエディションを確認するか、VDAを削除してから再インストールしてください。
[Cloud]: NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixサポートにお問い合わせください。
サポートされていないCredentialSecurityバージョン	109	VDAとデリバリーコントローラーが同じ暗号化メカニズムを使用していません。	VDAとデリバリーコントローラーのバージョンを合わせてください。
無効な登録要求	110	VDAがブローカーに登録要求を行いましたが、要求の内容が破損しているか無効です。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手

エラーコード	エラーコードID	問題	アクション
			順を参照してください。
シングル/マルチセッションの不一致	111	VDAのオペレーティングシステムタイプは、マシンカタログまたはデリバリーグループと互換性がありません。	VDAを、適切なマシンカタログタイプまたは同じオペレーティングシステムを持つマシンを含むデリバリーグループに追加してください。
カタログに対して機能レベルが低すぎます	112	マシンカタログが、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのマシンカタログ機能レベルがVDAの機能レベルと一致していることを確認してください。マシンカタログをVDAの機能レベルに合わせてアップグレードまたはダウングレードしてください。
FunctionalLevelTooLowForDesktopGroup	113	デリバリーグループが、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのデリバリーグループ機能レベルがVDAの機能レベルと一致していることを確認してください。マシンカタログをVDAの機能レベルに合わせてアップグレードまたはダウングレードしてください。
PowerOff	200	VDAが正常にシャットダウンされませんでした。	VDAが電源オンの状態であるべき場合、Citrix StudioからVDAを起動し、正常に起動して登録されることを確認してください。起動または登録

エラーコード	エラーコードID	問題	アクション
			に関する問題があればトラブルシューティングを行ってください。VDAが復旧したら、イベントログを確認してシャットダウンの根本原因を特定するのに役立ててください。
AgentRejectedSettingsUpdate	203	Citrixポリシーなどの設定が変更または更新されましたが、VDAへの更新の送信中にエラーが発生しました。これは、更新がインストールされているVDAバージョンと互換性がない場合に発生する可能性があります。	必要に応じてVDAをアップグレードしてください。適用された更新がVDAバージョンでサポートされているかどうかを確認してください。
SessionPrepareFailure	206	ブローカーは、VDAで実行されているセッションの監査を完了しませんでした。	広範囲にわたる場合は、デリバリーコントローラーでCitrix Broker Serviceを再起動してください。
[Cloud]: SessionPrepareFailure	206	ブローカーは、VDAで実行されているセッションの監査を完了しませんでした。	Citrixサポートに連絡してください。
ContactLost	207	デリバリーコントローラーはVDAとの接続を失いました。これはネットワークの中断によって引き起こされる可能性があります。	デリバリーコントローラーでCitrix Broker Serviceが実行されており、VDAでDesktopサービスが実行されていることを確認します。停

エラーコード	エラーコードID	問題	アクション
			止している場合はそれぞれを開始します。すでに開始されている場合は、VDAでDesktopサービスを再起動して登録プロセスを再開し、VDAが正常に登録されることを確認します。アプリケーションイベントログの詳細を通じて、VDA用に構成されたデリバリーコントローラーが正確であることを確認します。pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認します。そうでない場合は、ファイアウォールまたはネットワークの問題を解決します。
[Cloud]: ContactLost	207	デリバリーコントローラーはVDAとの接続を失いました。これはネットワークの中断によって引き起こされる可能性があります。	VDA上でDesktopサービスが実行されていることを確認します。停止している場合は開始します。
BrokerRegistrationLimitReached	301	デリバリーコントローラーは、同時に登録できるVDAの構成済み最大数に達しました。デフォルトでは、デリバリーコントローラーは	サイトにデリバリーコントローラーを追加するか、サイトを作成することを検討してください。また、**HKEY_LOCAL_MA**

エラーコード	エラーコードID	問題	アクション
		10,000の同時VDA登録を許可します。	**CHINE\Software\Citrix\DesktopServer\MaxWorkers** レジストリキーを介して、デリバリーコントローラーに同時に登録できるVDAの数を増やすこともできます。詳細については、Knowledge Centerの記事「Registry Key Entries Used by Citrix Virtual Apps and Desktops (CTX117446)」を参照してください。この数を増やすと、コントローラーにより多くのCPUおよびメモリリソースが必要になる場合があります。
SettingsCreationFailure	208	Brokerは、VDAに送信する設定と構成のセットを構築しませんでした。Brokerがデータを収集できない場合、登録は失敗し、VDAは未登録になります。	デリバリーコントローラーのイベントログでエラーがないか確認してください。ログに特定の問題が明らかでない場合は、Broker Serviceを再起動してください。Broker Serviceが再起動されたら、影響を受けるVDAでDesktopサービスを再起動し、それらが正常に登録されることを確認してください。

エラーコード	エラーコードID	問題	アクション
[Cloud]: SettingsCreationFailure	208	Brokerは、VDAに送信する設定と構成のセットを構築しませんでした。Brokerがデータを収集できない場合、登録は失敗し、VDAは未登録になります。	影響を受けるVDAでDesktopサービスを再起動し、それらが正常に登録されることを確認してください。Citrixサポートに連絡してください。
SendSettingsFailure	204	BrokerがVDAに設定および構成データを送信しませんでした。Brokerがデータを収集できても送信できない場合、登録は失敗します。	単一のVDAに限定される場合は、VDA上のDesktopサービスを再起動して再登録を強制し、アプリケーションイベントログを介してVDAが正常に登録されることを確認します。発生したエラーをトラブルシューティングします。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。

エラーコード	エラーコードID	問題	アクション
AgentRequested	2	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
DesktopRestart	201	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
DesktopRemoved	202	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
SessionAuditFailure	205	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
UnknownError	300	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
RegistrationStateMismatch	302	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
不明	-	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。

サードパーティ通知

Citrix Virtual Apps and Desktops™ のこのリリースには、以下のドキュメントに定義されている条件に基づいてライセンス供与されたサードパーティ製ソフトウェアが含まれる場合があります。

- Citrix Virtual Apps and Desktops サードパーティ通知(/ja-jp/citrix-virtual-apps-desktops/2311/downloads/third-party-notices-apps-and-desktops.pdf) (PDFダウンロード)
- FlexNet Publisher 2017 (11.15.0.0) の非商用ソフトウェア開示(/ja-jp/citrix-virtual-apps-desktops/2311/downloads/fnp-licensing-11-15-0-ncsd-summary.pdf) (PDFダウンロード)
- FlexNet Publisher 11.15.0 で使用されている FlexNet Publisher ドキュメント補足 サードパーティおよびオープンソースソフトウェア (PDFダウンロード)

SDKとAPIの概要

このリリースでは、いくつかのSDKとAPIが利用可能です。SDKとAPIにアクセスするには、Build anything with Citrixにアクセスしてください。そこから、**Citrix Workspace**を選択して、Citrix Virtual Apps and Desktopsおよび関連コンポーネントのプログラミング情報にアクセスします。

> **注:**
>
> Citrix Virtual Apps and Desktops™ SDKとCitrix Group Policy SDKは、モジュールまたはスナップインとしてインストールできます。いくつかのコンポーネントSDK（Citrix Licensing、Citrix Provisioning、StoreFrontなど）は、スナップインのみを使用してインストールされます。

> この製品はPowerShellバージョン3から5をサポートしています。

Citrix Virtual Apps and Desktops ソフトウェア開発キット

このSDKは、Delivery Controller™またはStudioをインストールすると、PowerShellモジュールとして自動的にインストールされます。これにより、スナップインを追加することなく、このSDKのコマンドレットを使用できます。（このSDKをスナップインとしてインストールすることを選択した場合の指示は以下に記載されています。）

権限

Citrix管理権限を持つIDを使用してシェルまたはスクリプトを実行する必要があります。Controller上のローカル管理者グループのメンバーは、Citrix Virtual AppsまたはCitrix Virtual Desktops™をインストールするための完全な管理権限を自動的に持っていますが、Citrixは、通常の運用では、ローカル管理者アカウントを使用するのではなく、適切な権限を持つCitrix管理者を作成することを推奨します。

コマンドレットにアクセスして実行する

1. PowerShellでシェルを起動します。Studioを開き、**PowerShell**タブを選択し、**Launch PowerShell**をクリックします。

2. スクリプト内でSDKコマンドレットを使用するには、PowerShellで実行ポリシーを設定します。PowerShellの実行ポリシーについては、Microsoftのドキュメントを参照してください。
3. モジュールではなくスナップインを使用したい場合は、`Add-PSSnapin`（または`asnp`）コマンドレットを使用してスナップインを追加します。

   V1とV2はスナップインのバージョンを示します。XenDesktop 5のスナップインはバージョン1です。Citrix Virtual Apps and Desktops、および以前のXenDesktop 7バージョンのスナップインはバージョン2です。例えば、Citrix Virtual Apps and Desktopsスナップインをインストールするには、`Add-PSSnapin Citrix.ADIdentity.Admin.V2`と入力します。すべてのコマンドレットをインポートするには、次のように入力します: `Add-PSSnapin Citrix.*.Admin.V*`

これでコマンドレットとヘルプファイルを使用できます。

- このSDKのヘルプファイルにアクセスするには、Categoriesリストで製品またはコンポーネントを選択し、**Citrix Virtual Apps and Desktops SDK**を選択します。
- PowerShellのガイダンスについては、Windows PowerShell Integrated Scripting Environment (ISE)を参照してください。

グループポリシーSDK

Citrixグループポリシー SDKを使用すると、グループポリシーの設定とフィルターを表示および構成できます。このSDKは、PowerShellプロバイダーを使用して、マシンおよびユーザーの設定とフィルターに対応する仮想ドライブを作成します。このプロバイダーは、`New-PSDrive`の拡張機能として表示されます。

Group Policy SDKを使用するには、StudioまたはCitrix Virtual Apps and Desktops SDKのいずれかがインストールされている必要があります。

Citrix Group Policy PowerShell プロバイダーは、モジュールまたはスナップインとして利用できます。

- モジュールを使用する場合、追加の作業は不要です。
- スナップインを追加するには、`Add-PSSnapin citrix.common.grouppolicy` と入力します。

ヘルプにアクセスするには、次のように入力します: `help New-PSDrive -path localgpo:/`。

仮想ドライブを作成し、設定をロードするには、`New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>`と入力します。ここで、Controller文字列は、接続して設定をロードしたいサイト内のControllerの完全修飾ドメイン名です。

シトリックス バーチャル アプリケーションズ アンド デスクトップ REST API群

Citrix Virtual Apps and Desktops REST API を使用すると、Citrix Virtual Apps and Desktops 展開内のリソースの管理を自動化できます。

Citrix Virtual Apps and Desktops REST APIは `<https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis>` で利用できます。Citrix Virtual Apps and Desktopsに適用されないAPIは、その旨がマークされています。そこにあるガイダンスに従って、APIサービスへのアクセスを構成し、APIを使用してリソースを管理および最適化してください。

モニターサービス OData

Monitor API を使用すると、OData API のバージョン 3 または 4 を使用して Monitor Service データにアクセスできます。Monitor Service データからクエリされたデータに基づいて、カスタマイズされた監視およびレポートダッシュボードを作成できます。OData V.4 は ASP.NET Web API に基づいており、集計クエリをサポートしています。

詳細については、Monitor Service OData API を参照してください。

__index__

サイト全体の履歴トレンドを監視する

トレンドビューは、以下のパラメータについて、各サイトの履歴トレンド情報にアクセスします。

- セッション
- 接続障害
- マシン障害
- ログオンパフォーマンス
- 負荷評価
- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームイン・ドリルダウン機能を使用すると、期間をズームイン（グラフ内のデータポイントをクリック）してトレンドチャートをナビゲートし、トレンドに関連する詳細を確認できます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択してください。期間の利用可能性は、Directorの展開によって次のように異なります。

- 最大1年間（365日間）のトレンドレポートは、Premiumライセンスサイトで利用できます。
- 最大1か月間（31日間）のトレンドレポートは、Advancedライセンスサイトで利用できます。
- 最大7日間のトレンドレポートは、PremiumおよびAdvanced以外のライセンスサイトで利用できます。

> **注:**

- すべてのDirector展開において、セッション、障害、ログオンパフォーマンスのトレンド情報は、期間が「先月」（**現在まで**）またはそれより短い期間に設定されている場合、グラフとテーブルとして利用できます。カスタム終了日を指定した「先月」または「昨年」として選択された期間の場合、トレンド情報はグラフとして利用でき、テーブルとしては利用できません。
- Monitor Serviceのグルーミング保持値がトレンドデータの可用性を制御します。デフォルト値については、データ粒度と保持を参照してください。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。
- IIS Managerの以下のパラメーターは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定されている特定のメトリックのグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能なトレンド

セッションの傾向を表示: 「**セッション**」タブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

セッションの自動再接続列には、セッション内の自動再接続の数が表示されます。自動再接続は、セッションの信頼性ポリシーまたはクライアントの自動再接続ポリシーが有効な場合に有効になります。エンドポイントでネットワークの中断が発生した場合、以下のポリシーが有効になります。

- セッションの信頼性が有効になり (デフォルトで3分間)、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- クライアントの自動再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性やクライアントの自動再接続、タイムスタンプ、エンドポイントIP、Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントのタイムスタンプの降順でソートされます。この機能は、Windows用Citrix Workspaceアプリ、Mac用Citrix Workspaceアプリ、Windows用Citrix Receiver、およびMac用Citrix Receiverで利用できます。この機能には、Delivery Controller™バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続について詳しくは、セッションを参照してください。

ポリシーについて詳しくは、クライアントの自動再接続ポリシー設定およびセッションの信頼性ポリシー設定を参照してください。

自動再接続データがDirectorに表示されない場合があるのは、以下の理由によります。

- Workspaceアプリが自動再接続データをVDAに送信していません。
- VDAが監視サービスにデータを送信していません。
- Delivery Controllers は、対応するセッションを持っていない可能性があるため、VDA ペイロードを破棄します。

> **注:**
>
> 特定の Citrix Gateway ポリシーが設定されている場合、クライアント IP アドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** 「障害」タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示する: シングルセッション OS マシン障害タブまたはマルチセッション OS マシンタブから、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のマシン障害に関する詳細情報を含むグラフを表示します。

ログオンパフォーマンスの傾向を表示する: ログオンパフォーマンスタブから、デリバリーグループと期間を選択すると、サイト全体のユーザーログオン時間の詳細情報と、ログオン数がパフォーマンスに影響するかどうかを示すグラフが表示されます。このビューには、ブローカー処理時間やVM起動時間など、ログオンフェーズの平均期間も表示されます。 このデータはユーザーログオンに特化したものであり、切断されたセッションから再接続しようとしているユーザーは含まれません。 グラフの下の表には、ユーザーセッションごとのログオン期間が表示されます。表示する列を選択し、任意の列でレポートを並べ替えることができます。 詳細については、「ユーザーログオンの問題の診断」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2311/director/troubleshoot-deployments/user-issues/user-logon.html)

負荷評価の傾向を表示する: 負荷評価インデックスタブから、マルチセッション OS マシン間で分散される負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のマルチセッション OS マシン、マルチセッション OS マシン（デリバリーグループ内のマルチセッション OS マシンが選択されている場合にのみ利用可能）、および範囲が含まれます。

ホストされているアプリケーションの使用状況を表示する: この機能の利用可否は、組織のライセンスによって異なります。 **キャパシティ管理**タブから、**ホストされているアプリケーションの使用状況**タブを選択します。デリバリーグループと期間を選択して、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示す表を表示します。アプリケーションベースの使用状況の表から、特定のアプリケーションを選択して詳細と、そのアプリケーションを使用している、または使用したユーザーのリストを表示できます。

シングルセッションおよびマルチセッション OS の使用状況を表示する: ビューには、サイト別およびデリバリーグループ別のシングルセッション OS の使用状況が表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 ビューには、サイト別、デリバリーグループ別、およびマシン別のマルチセッション OS の使用状況も表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示する: マシン使用状況タブから、**シングルセッション OS マシンまたはマルチセッション OS マシン**を選択して、VM 使用状況のリアルタイムビューを取得し、サイトのキャパシティニーズを迅速に評価できるようにします。 シングルセッション OS の可用性 - サイト全体または特定のデリバリーグループの可用性別に、シングルセッション OS マシン (VDI) の現在の状態を表示します。 マルチセッション OS の可用性 - サイト全体または特定のデリバリーグループの可用性別に、マルチセッション OS マシンの現在の状態を表示します。

注: に表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

リソース使用率を表示する: リソース使用率タブから、**シングルセッション OS マシンまたはマルチセッション OS マシン**を選択して、各 VDI マシンの CPU およびメモリ使用量、IOPS およびディスク遅延に関する履歴傾向データを取得し、より適切なキャパシティプランニングに役立てます。 この機能には、Delivery Controllers および VDA **バージョン 7.11** 以降が必要です。 グラフには、平均 CPU、平均メモリ、平均 IOPS、ディスク遅延、およびピーク時の同時セッションのデータが表示されます。マシンにドリルダウンして、CPU を消費している上位 10 プロセスのデータとグラフを表示できます。

デリバリーグループと期間でフィルターします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去 2 時間、24 時間、7 日間、1 か月、および 1 年間で利用できます。平均 IOPS およびディスク遅延のグラフは、過去 24 時間、1 か月、および 1 年間で利用できます。

注:

- 履歴マシン使用率ページの「上位 10 プロセス」テーブルでデータを収集して表示するには、監視ポリシー設定の **プロセス監視を有効にする** を **許可** に設定する必要があります。このポリシーは、デフォルトでは **禁止** に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、**リソース監視を有効にする** ポリシー設定を使用して無効にできます。グラフの下の表には、マシンごとのリソース使用率データが表示されます。詳細については、「監視ポリシー設定」を参照してください。
- 平均IOPSは日次平均を示します。ピークIOPSは、選択した時間範囲におけるIOPS平均の最高値として計算されます。(IOPS平均とは、VDAでその時間に収集されたIOPSの時間ごとの平均です)。
- マシンのドリルダウンには、平均CPU使用率または平均メモリ使用率が1%を超えるプロセスが一覧表示されます。これは、場合によっては10未満のプロセスしか表示されない可能性があることを意味します。

ネットワーク分析データの表示: この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controllerの**バージョン7.11**以降が必要です。

ネットワークタブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、デスクトップのコンテキストビューが提供されます。この機能により、

DirectorはCitrix ADMからのHDX Insightレポートを通じて、展開環境におけるICAトラフィックの詳細な分析を提供します。詳細については、「ネットワーク分析の構成」を参照してください。

アプリケーション障害の表示: アプリケーション障害タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

この機能には、Delivery ControllerおよびVDA **バージョン7.15**以降が必要です。Windows Vista以降を実行するシングルセッションOS VDA、およびWindows Server 2008以降を実行するマルチセッションOS VDAがサポートされています。 詳細については、「履歴アプリケーション障害監視」を参照してください。

デフォルトでは、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳細については、「監視ポリシー設定」を参照してください。

プローブ結果の表示: プローブ結果タブには、構成ページでプローブ用に構成されたアプリケーションおよびデスクトップのプローブ結果が表示されます。ここでは、障害が発生した起動の段階が記録されます。

詳細については、「アプリケーションおよびデスクトップのプローブ」を参照してください。

カスタマイズされたレポートの作成: カスタムレポートタブは、監視データベースからのリアルタイムデータと履歴データを含むカスタムレポートを表形式で生成するためのユーザーインターフェイスを提供します。

この機能には、Delivery Controllers **バージョン7.12**以降が必要です。

以前に保存したカスタムレポートクエリのリストから、**実行してダウンロード**をクリックしてレポートをCSV形式でエクスポートしたり、**ODataをコピー**をクリックして対応するODataクエリをコピーして共有したり、**編集**をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューにはレポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存されたクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、ODataクエリオプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは後で実行するために保存できます。

注: ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされておらず、英語で表示されます。

グラフ上のフラグアイコンは、特定の時間範囲における重要なイベントまたはアクションを示します。フラグの上にマウスを移動し、クリックするとイベントまたはアクションが一覧表示されます。

注:

- HDX™接続ログオンデータは、VDA 7より前のバージョンでは収集されません。以前のVDAの場合、チャートデータは0と表示されます。
- Citrix Studioで削除されたデリバリーグループは、それらに関連するデータが整理されるまで、Directorのトレンドフィルターで選択可能です。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータが表示されません。
- アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの**リソース使用率と負荷評価インデックス**テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。

アプリケーションおよびデスクトップのプローブ

アプリケーションおよびデスクトップのプローブは、StoreFront を使用してサイトに公開されているアプリとデスクトップをテスト起動することで、それらの正常性を確認するプロセスを自動化します。プローブの結果は Director で確認できます。

要件

- アプリケーションプローブの場合は Delivery Controller バージョン 7.18 以降、デスクトッププローブの場合はバージョン 1906 以降が動作していること。
- プローブエージェントを実行するエンドポイントマシンは、アプリケーションプローブの場合は Citrix Workspace™ app for Windows バージョン 1808 以降、デスクトッププローブの場合はバージョン 1906 以降がインストールされた Windows マシンであること。Unified Windows Platform (UWP) 用の Workspace アプリはサポートされていません。

- Citrix Probe Agent は、Active Directory 資格情報を使用した StoreFront および Citrix Workspace 経由の認証をサポートしています。エンドポイントデバイスが Citrix Gateway 経由で StoreFront / Workspace に接続されている場合、Citrix Gateway ドメイン資格情報または多要素認証 (MFA) を使用して認証できます。Citrix Probe Agent は、シングルサインオン (SSO) などの他の認証方法をサポートしていません。
- Probe Agent をインストールするエンドポイントマシンに Microsoft .NET Framework バージョン 4.7.2 以降がインストールされていることを確認してください。

プローブの実行に必要なユーザーアカウント/権限:

- 各エンドポイントマシンでプローブを実行するための固有の StoreFront ユーザー。StoreFront ユーザーは管理者である必要はありません。プローブは非管理者コンテキストで実行できます。
- エンドポイントマシンに Citrix Probe Agent をインストールおよび構成するための Windows 管理者権限を持つユーザーアカウント
- 既存のユーザーアカウントをプローブに再利用すると、ユーザーのアクティブなセッションからログオフされる可能性があります。以下の権限を持つフル管理者ユーザーアカウントまたはカスタムロール:
    - デリバリーグループの権限:
        - 読み取り専用
    - Director の権限:
        - アラートメールサーバー構成の作成\\編集\\削除 - メールサーバーがまだ構成されていない場合
        - プローブ構成の作成\編集\削除
        - 構成の表示ページ
        - トレンドの表示ページ

構成

複数の地域で、オフピーク時間中にプローブを実行するようにスケジュールできます。包括的なプローブ結果は、ユーザーが問題を経験する前に、アプリケーション、ホストマシン、または接続に関連する問題のトラブルシューティングに役立ちます。

Citrix Probe Agent バージョン 2103 以降は、サイト集約をサポートしています。Citrix Probe Agent を構成するときに、Workspace (StoreFront) Site Aggregation Enabled オプションを選択し

て、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にします。次のサイトの組み合わせがサポートされています。

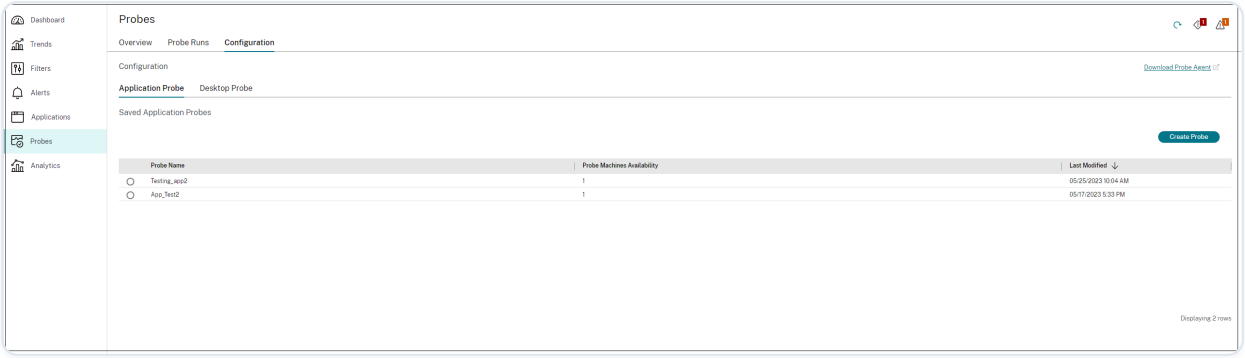
- 1つのStoreFront URLを持つ複数のオンプレミスサイト。
- StoreFrontまたはWorkspace URLのいずれかを持つオンプレミスサイトとクラウドサイト。
- 1つのWorkspace URLを持つ複数のクラウドサイト。
- Citrix Gateway経由でStoreFrontまたはWorkspaceに接続されたオンプレミスサイト。

> **注：**
>
> 1つのサイトにのみアクセスできるプローブを構成するには、個別の管理者またはユーザーを作成する必要があります。

ステップ1：Citrix Probe Agentをインストールして構成する

Citrix Probe Agentは、StoreFrontを介したユーザーによる実際のアプリケーションまたはデスクトップの起動をシミュレートするWindows実行可能ファイルです。Directorで構成された起動をテストし、その結果をDirectorに報告します。

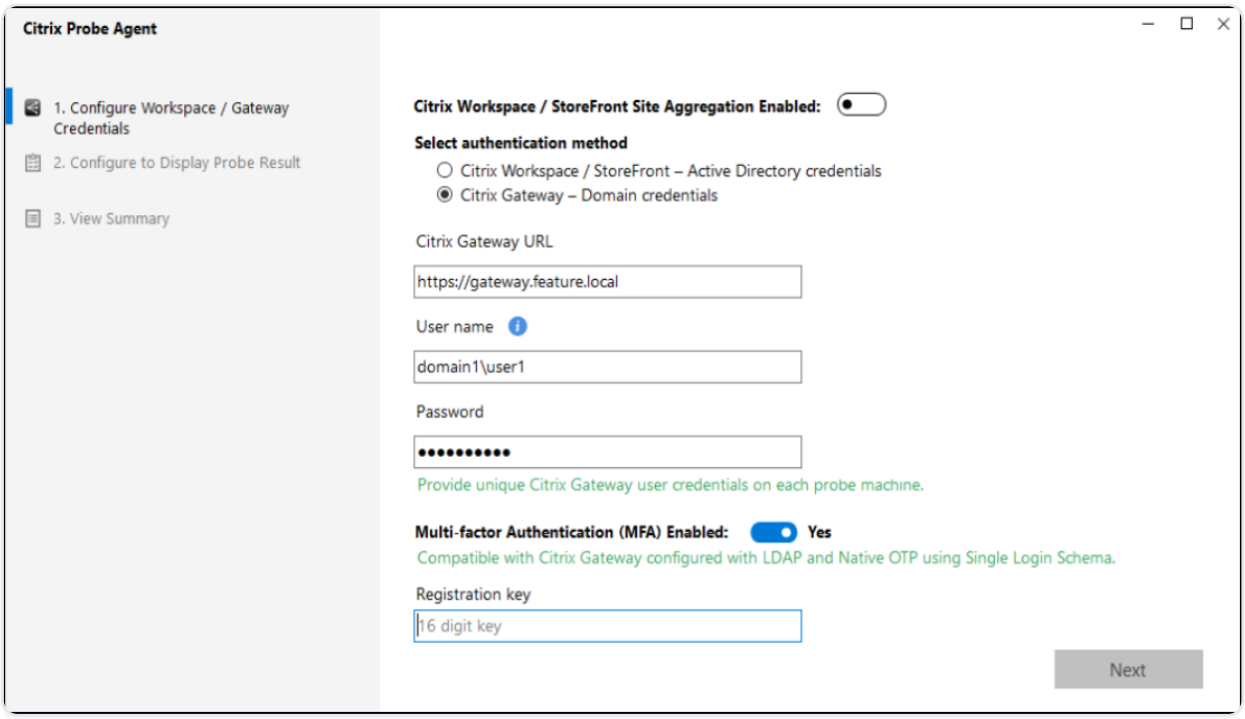
1. プロービングを実行するエンドポイントマシンを特定します。
2. 管理者権限を持つユーザーは、エンドポイントマシンに Citrix Probe Agent をインストールして構成できます。`<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>` で入手可能な Citrix Probe Agent 実行可能ファイルをダウンロードしてください。ダウンロードリンクは、Director の タブでも利用できます。



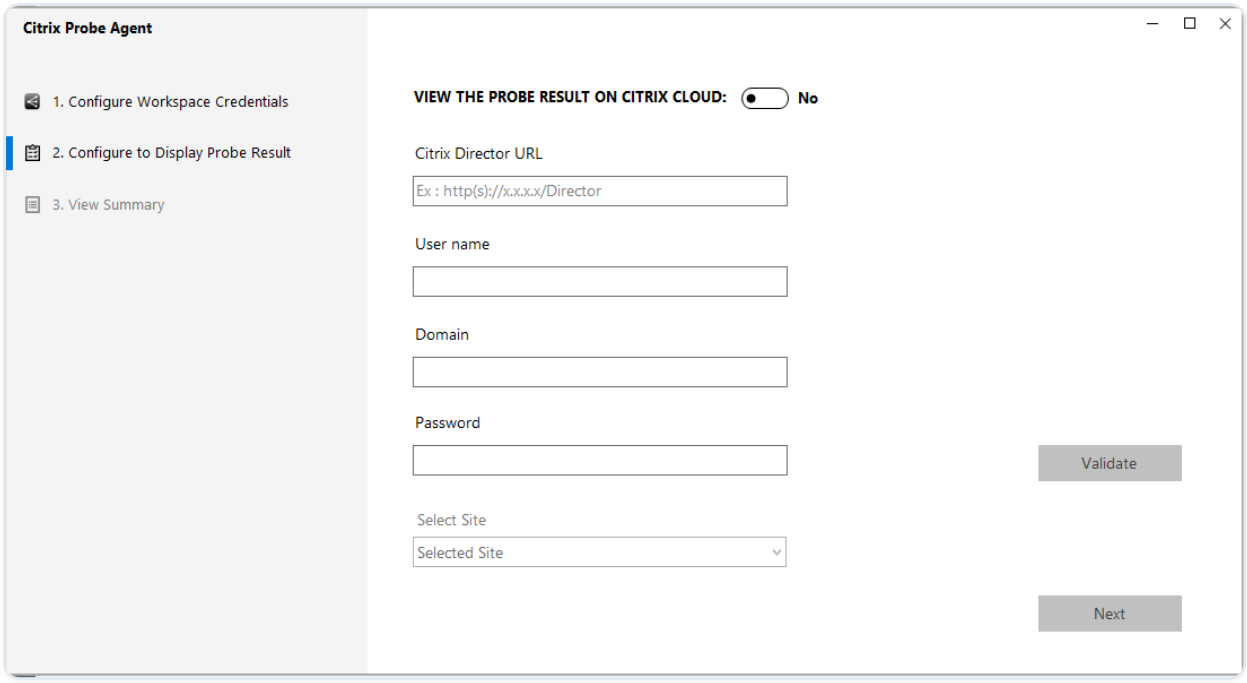
。

3. 集約されたサイトがある場合は、Workspace (StoreFront) サイト集約有効オプションを選択して、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にします。

4. 認証方法を選択し、関連する資格情報を入力します。資格情報は暗号化され、安全に保存されます。
5. StoreFront Active Directoryの資格情報で構成します。各エンドポイントマシンで一意のWorkspace (StoreFront) ユーザーを構成します。
6. エンドポイントがCitrix Gatewayを介してStoreFrontに接続されている場合は、Citrix Gatewayオプションを選択し、Citrix Gatewayドメインの資格情報で構成します。



7. ゲートウェイが多要素認証をサポートしている場合は、多要素認証オプションを選択し、16桁の認証キーを入力します。これは、LDAPとシングルログインスキーマを使用したネイティブOTPで構成されたCitrix Gatewayでのみ利用可能です。
8. **プローブ結果表示の構成**タブで、Directorの資格情報を入力し、**Validate**をクリックします。



9. サイトを選択し、**Next**をクリックします。
10. **概要の表示**タブで、構成された詳細が正確であることを確認します。変更が必要な場合は、該当するタブに移動して更新を行ってください。

> **注：**
>
> Automating Citrix Probe Agent Installation and Configuration に含まれるPowerShellスクリプトを使用して、Citrix Probe Agentのインストールと構成を自動化できます。

ステップ2：Directorでのプロービングの構成

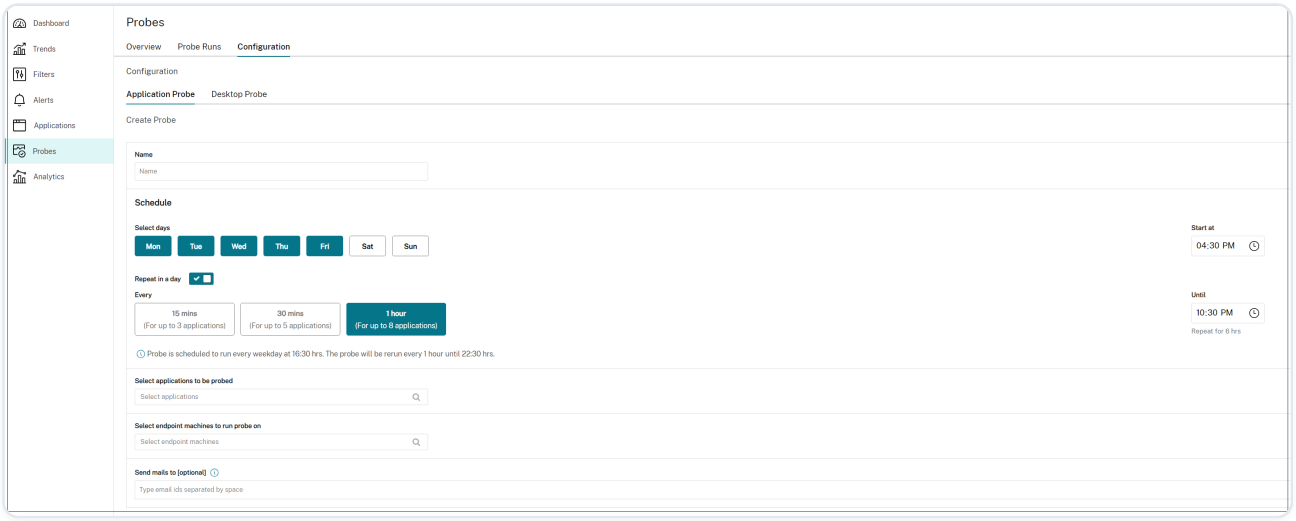
> **制限事項:**
>
> 対話型ログオンメッセージバナーが有効になっているWindows VDAからアプリケーションまたはデスクトップがテスト起動されると、プロービングは失敗します。これは、対話型ログオンメッセージの承認を待機しているためにタイムアウトが発生するためです。 サーバーVDAでログオンメッセージを無効にするには、 > > > > に移動します。
>
> 以下のフィールドのテキストを削除し、Microsoftポリシーを更新します。

- 対話型ログオン: ログオンしようとするユーザーへのメッセージテキスト
- 対話型ログオン: ログオンしようとするユーザーへのメッセージタイトル

プローブがアプリケーションまたはデスクトップの起動状態を通過できるように、対話型ログオンメッセージバナーを無効にして、この特定のサーバーVDAにプローブユーザーを割り当てます。

詳細については、`<https://learn.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`を参照してください。

1. **プローブ** \> **アプリケーションプローブ**または**デスクトッププローブ**に移動し、**プローブの作成**をクリックします。
2. 「**プローブの作成**」ページで、プローブの名前を入力します。
3. スケジュールを選択します。
   a. プローブを実行する曜日を選択します。
   b. プローブを実行する開始時刻を入力します。
   c. さらに、**1日あたりの繰り返し**オプションを選択できます。終了時刻と、1日の中でプローブを繰り返す間隔を入力します。たとえば、以下の構成は、月曜日、水曜日、木曜日、日曜日に、12:08から16:34まで30分ごとにアプリケーションプローブを実行するのに役立ちます。
4. 間隔に応じて、プローブするアプリケーションまたはデスクトップの推奨数を選択します。
5. プローブを実行する必要があるエンドポイントマシンを選択します。
6. 失敗したプローブの結果を送信する管理者のメールアドレスを入力します。メールサーバーは、**アラート** > **メールサーバーの構成**で構成します。



この構成では、毎週月曜日、水曜日、木曜日、日曜日に、アプリケーションセッションが12:08、12:38、13:08といった具合に16:08まで起動します。

注:

- 構成後、エージェントは次の時間から構成されたプローブを実行します。
- **1日あたりの繰り返し**オプションが導入される前に設定されたプローブは、スケジュールされた時間に引き続き実行されます。これらのプローブでは、**1日あたりの繰り返し**オプションがデフォルトで無効になっています。
- 重複を防ぐため、各実行が5分間隔になるようにプローブを構成することをお勧めします。

ステップ3：プローブの実行

エージェントは、Directorから定期的に取得するプローブ構成に従ってプロービングを実行します。

StoreFrontを使用して、選択されたアプリケーションを順次起動します。エージェントは、Monitorデータベースを介してDirectorに結果を報告します。失敗は5つの特定の段階で報告されます。

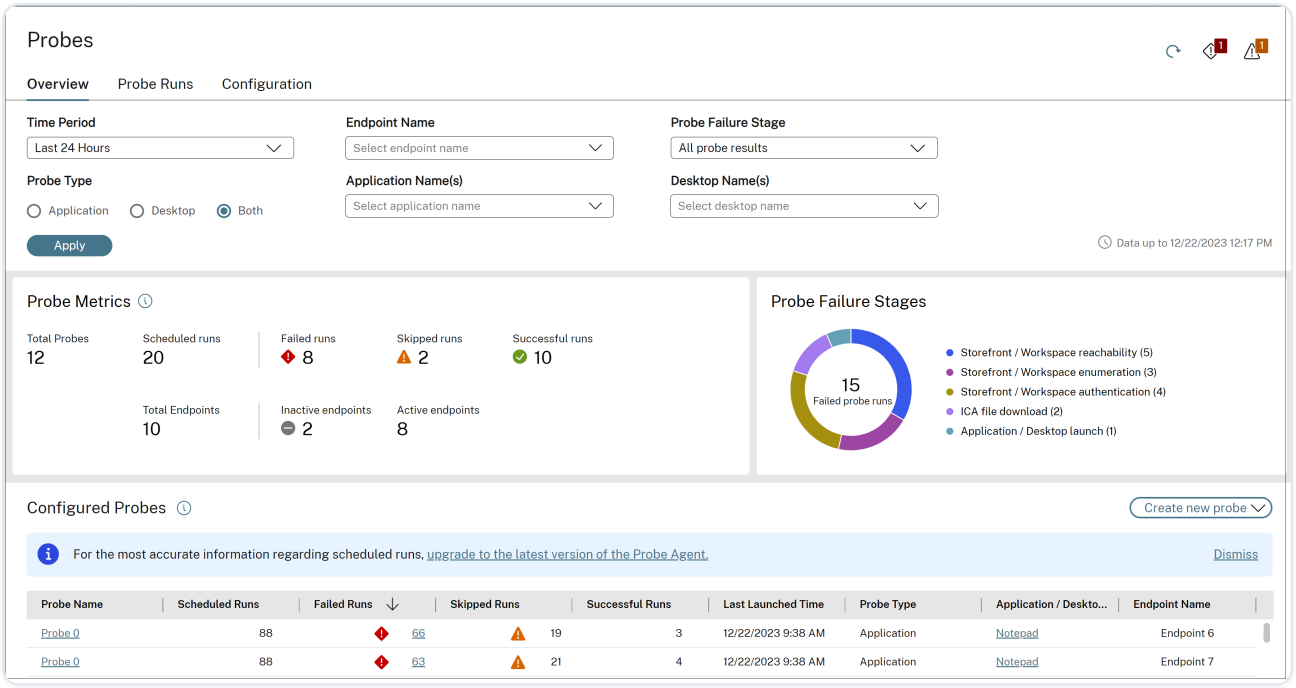
- **StoreFront到達可能性** - 構成されたStoreFront URLに到達できません。
- **StoreFront認証** - 構成されたStoreFront資格情報が無効です。
- **StoreFront列挙** - StoreFrontのアプリケーション列挙リストに、プローブ対象のアプリケーションまたはデスクトップが含まれていません。
- **ICA®ダウンロード** - ICAファイルが利用できません。

- **アプリケーション/デスクトップの起動** – アプリケーションまたはデスクトップを起動できませんでした。

ステップ4：プローブ結果の表示

プローブでプローブ結果を確認できます。プローブビューでは、プローブ結果の包括的な概要が示されます。これらの結果は、問題をプロアクティブに分析およびトラブルシューティングし、ユーザーのセッション起動エクスペリエンスをよりスムーズにするのに役立ちます。

概要タブには、構成されているすべてのプローブの概要が1つのビューに表示されます。



プローブは、時間範囲、プローブの種類、エンドポイント名、アプリケーション名、デスクトップ名、プローブ結果の種類に基づいてフィルタリングできます。フィルタ条件に一致するプローブは、プローブ、アプリケーション/デスクトップ、エンドポイントごとに以下の詳細とともに表示されます。

プローブメトリックには、スケジュール済み、計画済み、スキップ済み、成功、失敗した実行の数が表示されます。

- 完了した実行 – 完了まで実行されたプローブ実行の数。
- 失敗した実行 – 失敗したプローブ実行の数。
- スキップされた実行 – エンドポイントが非アクティブであるか、サービスが利用できないために完了まで実行されなかった実行の数。
- 成功した実行 – アプリ/デスクトップ起動中のどの段階でも失敗することなく、正常に完了したプローブの数。

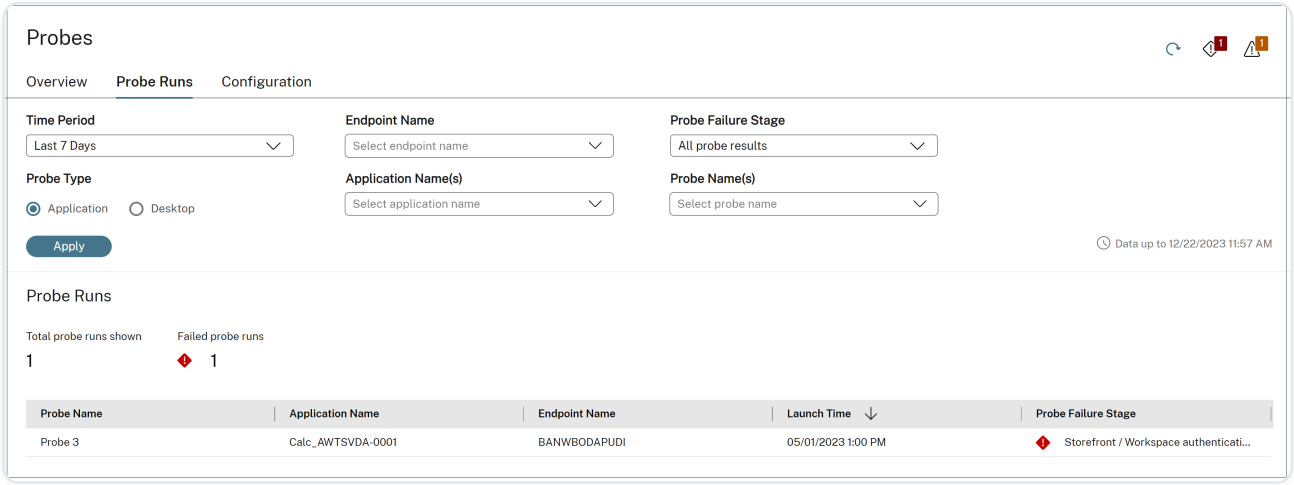
アクティブおよび非アクティブなマシンの数とともに、エンドポイントマシンの総数も表示されます。

プローブ失敗ステージは、各失敗グループの失敗分布を視覚的に分類して表示します。ほとんどの失敗が発生したステージを分析することで、プローブ結果の解釈と問題のトラブルシューティングが容易になります。グラフィカル表示では、アプリケーション/デスクトップの起動、ICAファイルのダウンロード、Storefront/Workspaceの列挙、Storefront/Workspaceの到達可能性、Storefront/Workspaceの認証における失敗したプローブ実行の数が示されます。

ほとんどの失敗が発生したステージを分析するのに役立ちます。この情報は、プローブ結果を迅速に理解し、トラブルシューティングを行うのに役立ちます。

エンドポイントが非アクティブであるか、サービスが利用できないために、一部のプローブ実行が完了しない場合があります。

プローブ実行タブには、完了したプローブ実行の結果が詳細に表示されます。選択したプローブの個々の実行の詳細を確認するためにドリルダウンできます。重要なピボットポイントに基づいて、さらにフィルタリングおよび分析できます。



期間、プローブの種類、エンドポイント名、アプリケーション名、デスクトップ名、およびプローブ失敗ステージに基づいて、プローブの実行をフィルタリングできます。プローブ失敗ステージには、プローブが失敗したステージが表示されます。プローブ名、スケジュールされた実行、失敗した実行、アプリケーション/デスクトップ名のリンクをクリックすると、フィルタ条件に一致するプローブ実行のリストが表示されるプローブ実行ページに移動します。

フレームホーク

> **重要:**

> Citrix Virtual Apps and Desktops 7 1903以降、Framehawkはサポートされなくなりました。代わりに、アダプティブトランスポートを有効にしたThinwireを使用してください。

> Framehawkは、高いパケット損失が発生しやすいブロードバンドワイヤレス接続（Wi-Fiおよび4G/LTEセルラーネットワーク）を使用するモバイルワーカー向けの特殊なディスプレイリモートテクノロジーです。Framehawkは、スペクトル干渉とマルチパス伝播の課題を克服します。Framehawkは、ラップトップやタブレットなどのWindowsおよびiOSモバイルデバイスで仮想アプリとデスクトップを使用するユーザーに、スムーズでインタラクティブなユーザーエクスペリエンスを提供します。サーバーのスケーラビリティを最大化し、ネットワーク帯域幅の消費を最小限に抑えるため、Framehawkは上記の特定のユースケースでのみ使用することをお勧めします。その他のすべてのユースケースでは、データスループットを最大化するために多くのFramehawkコンセプトを組み込んだアダプティブトランスポートをお勧めします。

Citrix®ポリシーテンプレートを使用して、組織に適した方法で、特定のユーザーセットとアクセスシナリオに対してFramehawkを実装できます。Framehawkは、ラップトップやタブレットなどのシングルスクリーンモバイルユースケースを対象としています。リアルタイムのインタラクティブなパフォーマンスのビジネス価値が、サーバーリソースの追加コストとブロードバンド接続の要件を正当化する場合に、Framehawkを使用してください。

Framehawkがスムーズなユーザーエクスペリエンスを維持する方法

Framehawkは、フレームバッファの内容を見て、画面上のさまざまな種類のコンテンツを識別する、人間の目のソフトウェア実装と考えてください。ユーザーにとって何が重要でしょうか？ビデオや動くグラフィックのように画面の領域が急速に変化する場合、一部のピクセルが失われても人間の目には問題ありません。それらの領域は新しいデータで迅速に上書きされます。

しかし、画面の静的な領域に関しては、人間の目は気難しいものです。たとえば、通知領域やツールバーのアイコン、またはユーザーが読み始めたい場所にスクロールした後のテキストなどです。ユーザーは、これらの領域がピクセルパーフェクトであることを期待します。「**1と0**」の観点から技術的に正確であることを目指すプロトコルとは異なり、Framehawkはテクノロジーを使用する人間にとって関連性があることを目指しています。

Framehawkには、次世代のサービス品質信号増幅器と、ワークロードをよりきめ細かく効率的に識別するための時間ベースのヒートマップが含まれています。データ圧縮に加えて、自律的で自己修復型の変換を使用し、データの再送信を回避して、クリック応答、線形性、一貫したケイデンスを維持します。損失の多いネットワーク接続では、Framehawkは補間によって損失を隠すことができ、ユーザーはよりスムーズなエクスペリエンスを楽しみながら、良好な画質を認識できます。さらに、Framehawkアルゴリズムは、異なる種類のパケット損失をインテリジェントに区別

します。たとえば、ランダムな損失（補償のためにより多くのデータを送信する）と輻輳による損失（チャネルがすでに詰まっているため、より多くのデータを送信しない）などです。

Citrix Workspace™アプリのFramehawkインテントエンジンは、上下スクロール、ズーム、左右移動、読み取り、入力、およびその他の一般的なアクションを区別します。このエンジンは、共有辞書を使用してVirtual Delivery Agent (VDA)への通信も管理します。ユーザーが読み取ろうとしている場合、テキストの視覚品質は優れている必要があります。ユーザーがスクロールしている場合、それは迅速かつスムーズでなければなりません。そして、中断可能である必要があり、ユーザーがアプリケーションまたはデスクトップとのインタラクションを常に制御できるようにします。

ネットワーク接続上のケイデンス（自転車のチェーンの張力に例えられる「**ギアリング**」）を測定することで、Framehawkロジックはより迅速に反応し、高遅延接続で優れたエクスペリエンスを提供します。このユニークで特許取得済みのギアリングシステムは、ネットワーク状況に関する常に最新のフィードバックを提供し、Framehawkが帯域幅、遅延、損失の変化に即座に反応できるようにします。

ThinwireとFramehawkを使用する際の設計上の考慮事項

Framehawkは、User Datagram Protocol (UDP)の上に構築されたデータ転送層を使用します。FramehawkのパフォーマンスをUDPベースのプロトコルと比較するとわかるように、UDPはFramehawkが損失を克服する方法の小さな部分です。UDPは、Framehawkを際立たせる人間中心の技術に重要な基盤を提供します。

Framehawkにはどのくらいの帯域幅が必要ですか？

ブロードバンドワイヤレスの意味は、接続を共有しているユーザー数、接続の品質、使用されているアプリなど、いくつかの要因に依存します。最適なパフォーマンスを得るために、Citrixは、4 Mbpsまたは5 Mbpsをベースとし、同時ユーザーあたり約150 Kbpsを追加することを推奨しています。

Thinwireの帯域幅の推奨事項は、通常、ベースとして1.5 Mbpsに加えてユーザーあたり150 Kbpsです。詳細については、Citrix Virtual Apps and Desktopsの帯域幅に関するブログを参照してください)。パケット損失が3%の場合、TCP経由のThinwireは、良好なユーザーエクスペリエンスを維持するためにFramehawkよりもはるかに多くの帯域幅を必要とすることがわかります。

Thinwireは、ICA®プロトコルにおける主要なディスプレイリモートチャネルであり続けています。Framehawkはデフォルトで無効になっています。Citrixは、組織内のブロードバンドワイヤレスアクセスシナリオに対処するために、選択的に有効にすることをお勧めします。FramehawkはThinwireよりもはるかに多くのサーバーリソース（CPUとメモリ）を必要とすることに注意してください。

要件と考慮事項

Framehawkには、VDA 7.6.300およびGroup Policy Management 7.6.300が最低限必要です。

エンドポイントには、Workspace app for Windows 1808、またはCitrix Receiver for Windows 4.3.100、Workspace app for iOS 1808、またはCitrix Receiver for iOS 6.0.1が最低限必要です。

デフォルトでは、Framehawkは双方向のUser Datagram Protocol (UDP) ポート範囲（3224から3324）を使用して、Citrix WorkspaceアプリとFramehawkディスプレイチャネルデータを交換します。この範囲は、**Framehawk display channel port range**というポリシー設定でカスタマイズできます。クライアントと仮想デスクトップ間の同時接続ごとに一意のポートが必要です。Citrix Virtual Apps™サーバーのようなマルチユーザーOS環境では、最大数の同時ユーザーセッションをサポートするのに十分なポートを定義してください。VDIデスクトップのようなシングルユーザーOSの場合、単一のUDPポートを定義するだけで十分です。Framehawkは、最初に定義されたポートから、範囲で指定された最後のポートまで使用を試みます。これは、Citrix Gatewayを介して接続する場合と、StoreFrontサーバーへの直接内部接続の両方に適用されます。

リモートアクセスの場合、Citrix Gatewayを展開する必要があります。デフォルトでは、Citrix GatewayはクライアントのCitrix WorkspaceアプリとGateway間の暗号化された通信にUDPポート443を使用します。このポートは、双方向の安全な通信を許可するために、すべての外部ファイアウォールで開いている必要があります。この機能はDatagram Transport Security (DTLS)として知られています。

> **注:**
>
> Framehawk/DTLS接続はFIPSアプライアンスではサポートされていません。

> 暗号化されたFramehawk接続は、NetScaler Gatewayバージョン11.0.62およびNetScaler Unified Gatewayバージョン11.0.64.34以降でサポートされています。

NetScaler High Availabilityは、XenAppおよびXenDesktop 7.12以降でサポートされています。

Framehawkを実装する前に、以下の推奨事項を考慮してください。

- Framehawk用に定義されたUDPポートがファイアウォールで開いていることを確認するために、セキュリティ管理者に連絡してください。インストールプロセスでは、ファイアウォールは自動的に構成されません。
- 多くの場合、Citrix GatewayはDMZにインストールされ、外部と内部の両側にファイアウォールが配置されていることがあります。外部ファイアウォールでUDPポート443が開いているこ

とを確認してください。環境がデフォルトのポート範囲を使用している場合は、内部ファイアウォールでUDPポート3224から3324が開いていることを確認してください。

構成

> **注意:**
>
> Citrixは、高いパケット損失が発生する可能性のあるユーザーに対してのみFramehawkを有効にすることを推奨しています。また、サイト内のすべてのオブジェクトに対してFramehawkをユニバーサルポリシーとして有効にしないことを推奨します。
>
> Framehawkはデフォルトで無効になっています。有効にすると、サーバーはユーザーグラフィックと入力にFramehawkを使用しようとします。何らかの理由で前提条件が満たされない場合、接続はデフォルトモード（Thinwire）を使用して確立されます。

以下のポリシー設定がFramehawkに影響します。

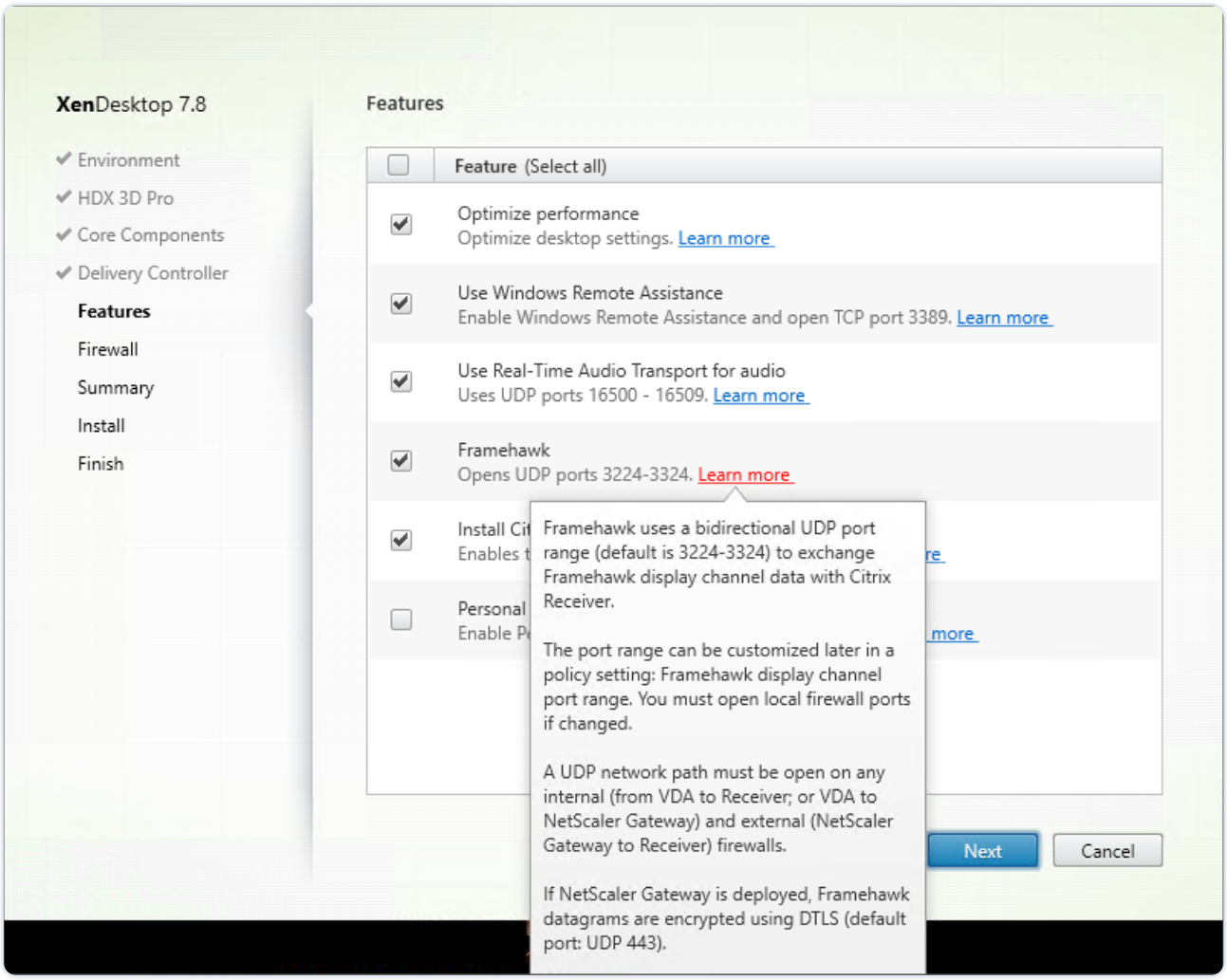
- Framehawkディスプレイチャネル: この機能を有効または無効にします。
- Framehawkディスプレイチャネルポート範囲: VDAがユーザーデバイスとFramehawkディスプレイチャネルデータを交換するために使用するUDPポート番号の範囲（最小ポート番号から最大ポート番号まで）を指定します。VDAは、最小ポート番号から開始し、その後の試行ごとにインクリメントして、各ポートを使用しようとします。このポートは、インバウンドおよびアウトバウンドトラフィックを処理します。

Framehawkディスプレイチャネル用のポートを開く

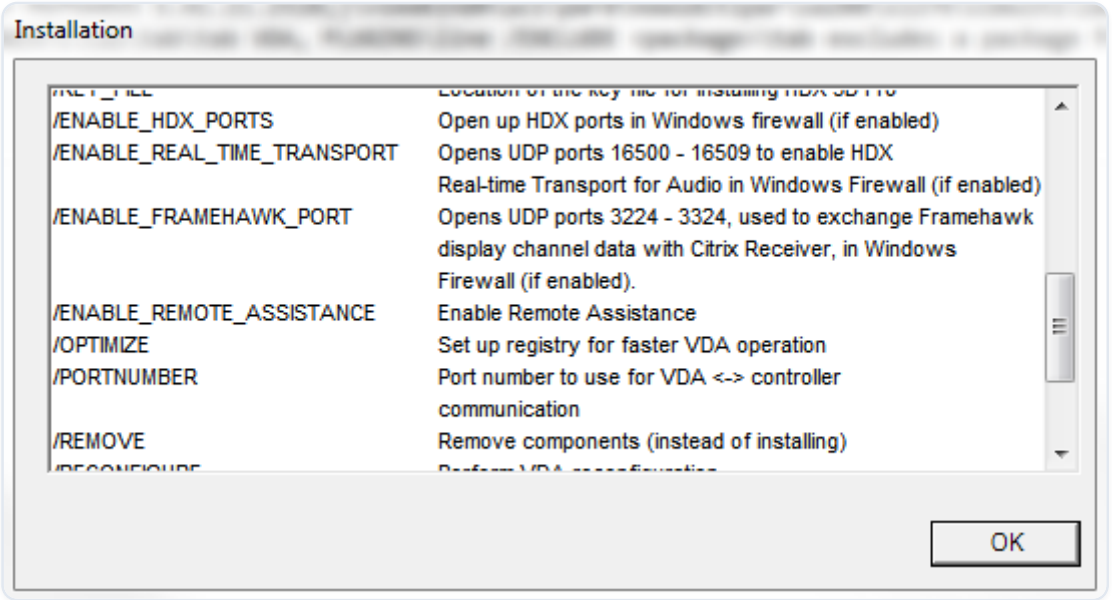
XenAppおよびXenDesktop 7.8以降では、VDAインストーラーの**機能**ステップ中にファイアウォールを再構成するオプションが利用可能です。このチェックボックスを選択すると、Windowsファイアウォールで UDPポート3224から3324が開きます。特定の状況では、手動でのファイアウォール構成が必要です。

- 任意のネットワークファイアウォールの場合。 または
- デフォルトのポート範囲がカスタマイズされている場合。

これらの UDP ポートを開くには、 チェックボックスをオンにします。

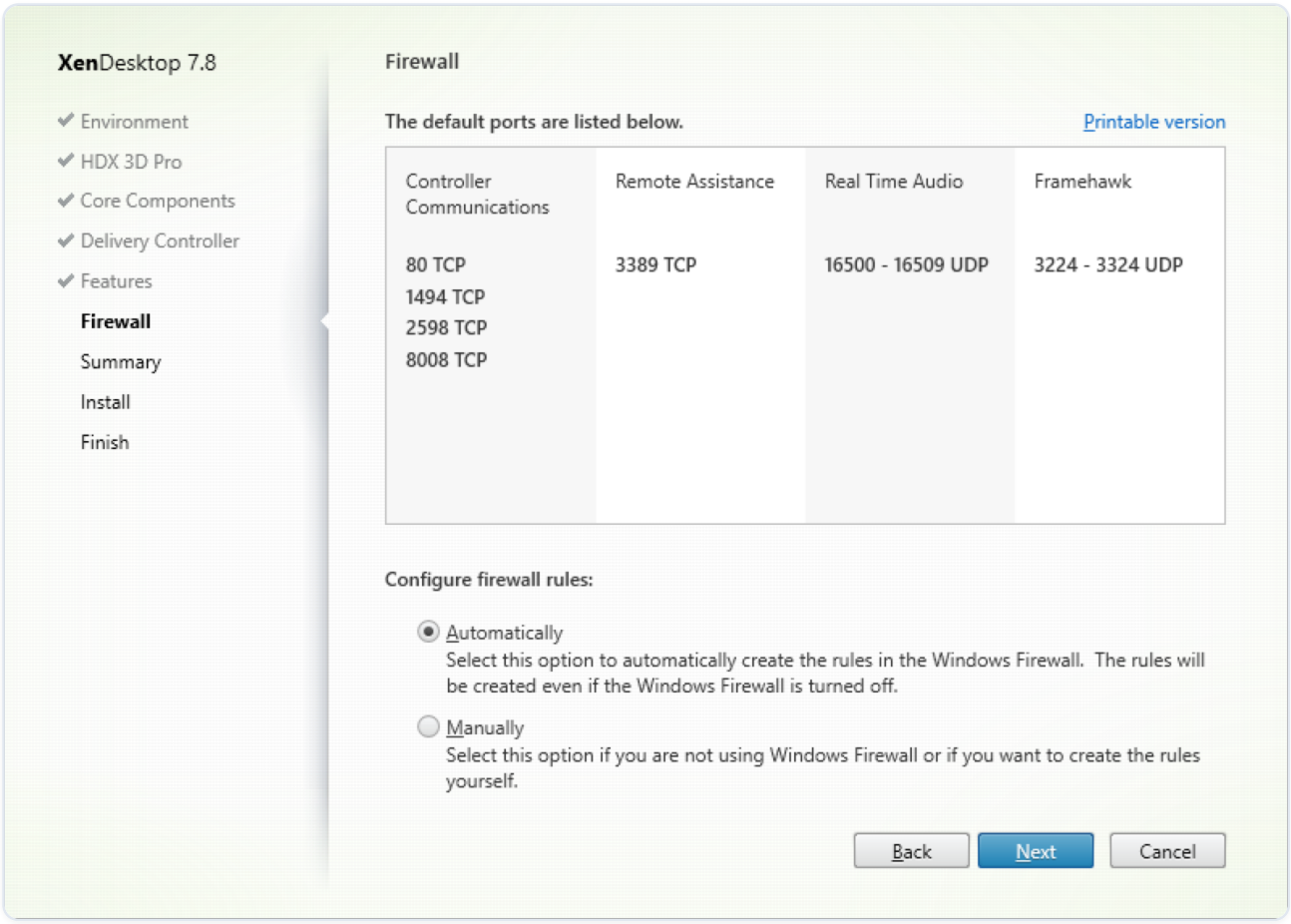


コマンドラインを使用して、**/ENABLE_FRAMEHAWK_PORT**でFramehawk用のUDPポートを開くこともできます。

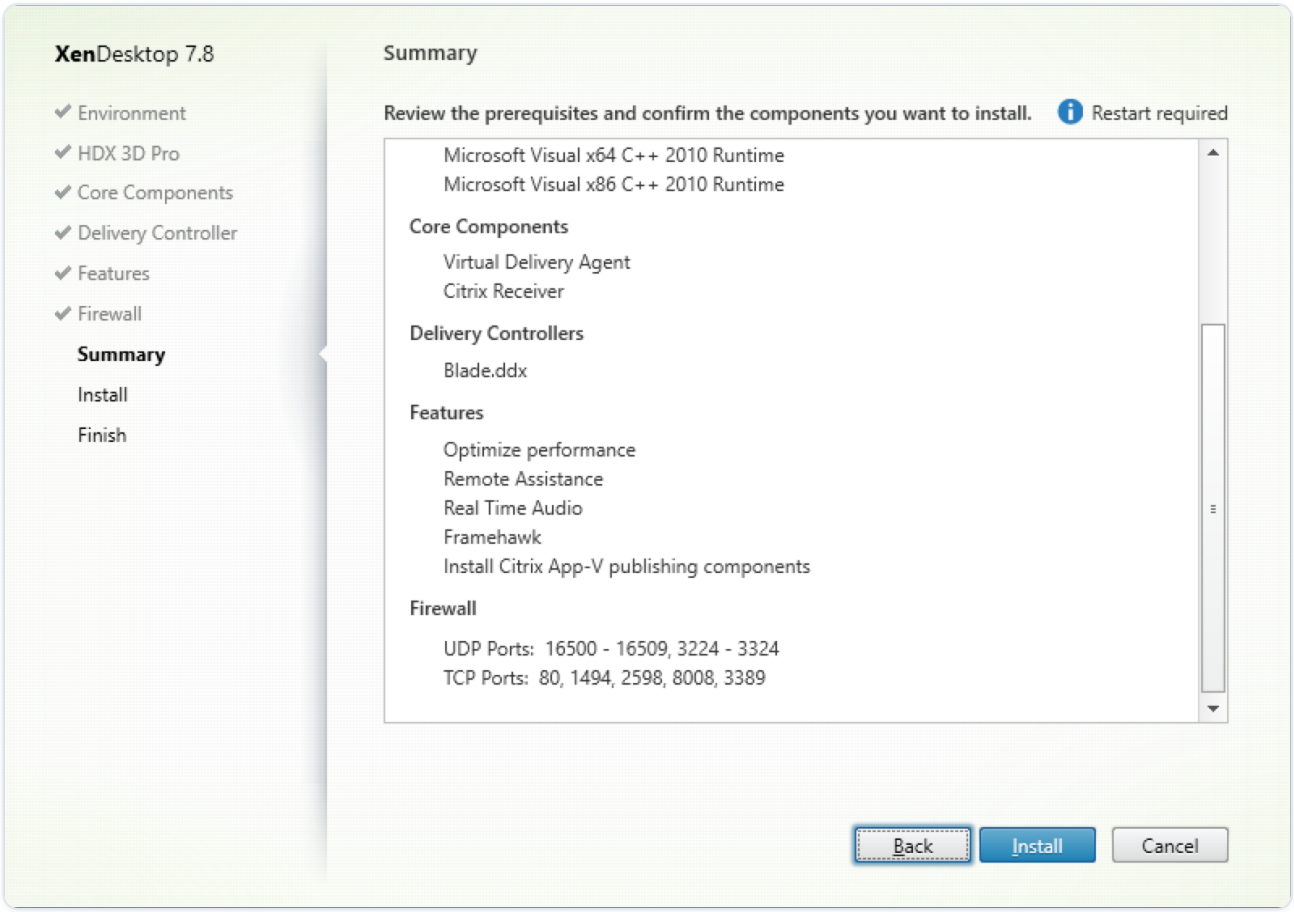


Framehawk UDP ポートの割り当ての確認

インストール中に、 画面で Framehawk に割り当てられている UDP ポートを確認できます。



画面には、Framehawk 機能が有効になっているかどうかが表示されます。



Framehawk の Citrix Gateway サポート

暗号化された Framehawk トラフィックは、Citrix Gateway 1808 以降、NetScaler Gateway 11.0.62.10 以降、Citrix Unified Gateway 1808、および NetScaler Unified Gateway 11.0.64.34 以降でサポートされています。

- Citrix Gatewayとは、Gateway VPN仮想サーバーがエンドユーザーデバイスから直接アクセスできる展開アーキテクチャを指します。つまり、VPN仮想サーバーにはパブリックIPアドレスが割り当てられており、ユーザーはこのIPアドレスに直接接続します。
- Unified Gatewayを使用するCitrix Gatewayとは、Gateway VPN仮想サーバーがコンテンツスイッチング仮想サーバー（CS）のターゲットとしてバインドされている展開を指します。この展開では、CS仮想サーバーがパブリックインターネットプロトコルアドレスを持ち、Gateway VPN仮想サーバーはダミーのインターネットプロトコルアドレスを持ちます。

Citrix GatewayでFramehawkサポートを有効にするには、Gateway VPN仮想サーバーレベルのDTLSパラメーターを有効にする必要があります。パラメーターが有効になり、Citrix Virtual AppsまたはCitrix Virtual Desktops™のコンポーネントが正しく更新されると、Framehawkのオーディオ、ビデオ、およびインタラクティブトラフィックはGateway VPN仮想サーバーとユーザーデバイス間で暗号化されます。

Citrix Gateway、Unified Gateway、および Citrix Gateway + グローバルサーバー負荷分散は Framehawk でサポートされています。

以下のシナリオはFramehawkではサポートされていません。

- HDX™ インサイト
- IPv6 モードの Citrix Gateway
- Citrix Gateway ダブルホップ
- クラスター設定の Citrix Gateway

シナリオ	FRAMEHAWK のサポート
シトリックス ゲートウェイ	はい
Citrix Gateway + グローバルサーバー負荷分散	はい
Unified Gatewayを使用したCitrix Gateway	はい。**注：**Unified Gatewayバージョン11.0.64.34以降がサポートされています。
HDXインサイト	いいえ

シナリオ	FRAMEHAWK のサポート
IPv6モードのCitrix Gateway	いいえ
Citrix Gatewayダブルホップ	いいえ
Citrix Gateway 上の複数のセキュアチケットオーソリティ	はい
Citrix Gatewayと高可用性	はい
Citrix Gatewayとクラスター設定	いいえ

FramehawkサポートのためのCitrix Gatewayの構成

Citrix GatewayでFramehawkサポートを有効にするには、Gateway VPN *仮想サーバー* レベルでDTLSパラメーターを有効にします。パラメーターが有効になり、Citrix Virtual Apps and Desktops™のコンポーネントが正しく更新されると、Framehawkのオーディオ、ビデオ、およびインタラクティブトラフィックはGateway VPN仮想サーバーとユーザーデバイスの間で暗号化されます。

リモートアクセス用にCitrix GatewayでUDP暗号化を有効にする場合、この構成が必要です。

FramehawkサポートのためにCitrix Gatewayを構成する際：

- 外部ファイアウォールでUDPポート443が開いていることを確認します
- 外部ファイアウォールでCGPポート（デフォルト2598）が開いていることを確認します
- VPN仮想サーバーの設定でDTLSを有効にします
- SSL証明書とキーのペアをアンバインドして再バインドします。Citrix Gateway 1808以降またはNetScalerバージョン11.0.64.34以降を使用している場合、この手順は必要ありません。

FramehawkサポートのためにCitrix Gatewayを構成するには：

1. Citrix Gatewayを展開して、StoreFront™と通信し、Citrix Virtual Apps and Desktopsのユーザーを認証するように構成します。
2. 「Citrix Gateway構成」タブでCitrix Gatewayを展開し、「**仮想サーバー**」を選択します。
3. 「**編集**」を選択してVPN仮想サーバーの基本設定を表示し、DTLS設定の状態を確認します。
4. 「**詳細**」を選択してその他の構成オプションを表示します。

5. 「**DTLS**」を選択してFramehawkなどのデータグラムプロトコルに通信セキュリティを提供します。「**OK**」をクリックします。VPN仮想サーバーの基本設定領域に、DTLSフラグが「**True**」に設定されていることが表示されます。
6. サーバー証明書バインド画面を再度開き、「**+**」をクリックして証明書キーペアをバインドします。
7. 以前の証明書キーペアを選択し、「**選択**」をクリックします。
8. サーバー証明書バインドへの変更を保存します。
9. 保存後、証明書キーペアが表示されます。「**バインド**」をクリックします。
10. 「**SSL仮想サーバー/サービスに構成された使用可能な暗号はありません**」という警告メッセージが表示された場合は無視します。

以前のNetScaler® Gatewayバージョンの手順

NetScaler Gatewayのバージョンが11.0.64.34より古い場合：

1. サーバー証明書バインド画面を再度開き、「+」をクリックして証明書キーペアをバインドします。
2. 以前の証明書キーペアを選択し、「**選択**」をクリックします。
3. サーバー証明書バインドへの変更を保存します。
4. 保存後、証明書キーペアが表示されます。「**バインド**」をクリックします。
5. 「**SSL vserver/serviceに、使用可能な暗号が設定されていません**」という警告メッセージが表示された場合は、無視してください。

FramehawkをサポートするようにUnified Gatewayを構成するには：

1. Unified Gatewayがインストールされ、適切に構成されていることを確認してください。詳細については、Citrix製品ドキュメントサイトのUnified Gatewayを参照してください。
2. VPN *virtual server*でDTLSパラメーターを有効にします。これは、ターゲット *virtual server*としてCS *virtual server*にバインドされています。

制限事項

クライアントデバイスにCitrix Gateway仮想サーバーの古いDNSエントリがある場合、アダプティブトランスポートとFramehawkはUDPトランスポートではなくTCPトランスポートにフォールバックする可能性があります。TCPトランスポートへのフォールバックが発生した場合は、クライアントのDNSキャッシュをフラッシュし、再接続してUDPトランスポートを使用してセッションを確立してください。

Framehawkは、PTC Creoなどのアプリケーションに見られる32ビットマウスカーソルをサポートしていません。

Framehawkは、シングルモニターを使用するラップトップやタブレットなどのモバイルデバイス向けに設計されており、デュアル/マルチモニター構成ではThinwireに戻ります。

その他のVPN製品のサポート

Citrix Gatewayは、Framehawkが必要とするUDP暗号化をサポートする唯一のSSL VPN製品です。別のSSL VPNまたは誤ったバージョンのCitrix Gatewayが使用されている場合、Framehawkポリシーが適用されない可能性があります。従来のIPsec VPN製品は、変更なしでFramehawkをサポートします。

Framehawkの監視

Citrix DirectorからFramehawkの使用状況とパフォーマンスを監視できます。HDX仮想チャネルの詳細ビューには、任意のセッションでFramehawkのトラブルシューティングと監視に役立つ情報が含まれています。Framehawk関連のメトリックを表示するには、「**Graphics-Framehawk**」を選択します。

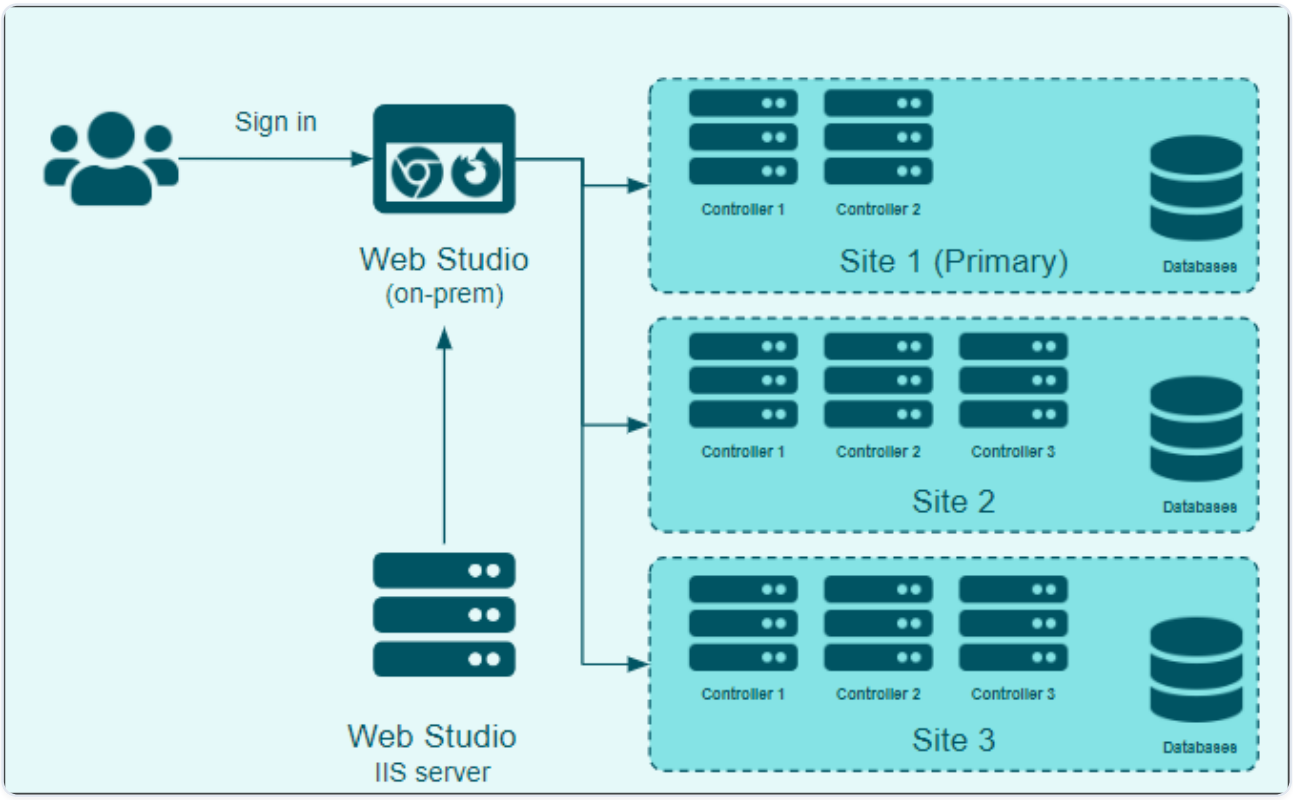
Framehawk接続が確立されると、詳細ページに「**Provider = VD3D**」と「**Connected = True**」が表示されます。仮想チャネルの状態がアイドルであるのは正常です。これは、初期ハンドシェイク中にのみ使用されるシグナリングチャネルを監視するためです。このページには、接続に関するその他の有用な統計も表示されます。

問題が発生した場合は、Framehawkトラブルシューティングブログを参照してください。

複数サイト管理を有効にする

デフォルトでは、1つのWeb Studioコンソールは単一のCitrix Virtual Apps and Desktops™サイトにマッピングされますが、必要に応じて、Web Studioコンソールを複数のサイトを管理するように構成できます。これにより、すべてのサイトを構成および管理するために、Web Studioを1つだけインストールすればよくなります。

次の図は、単一のWeb Studio展開が複数の独立したCitrix Virtual Apps and Desktopsサイトを管理する、複数サイトアーキテクチャを示しています。



利点

- 統合されたシングルサインオンエクスペリエンスで複数のサイトを管理する際の効率が向上します。
- すべての構成が1つのコンソールからアクセスできるため、トラブルシューティングが容易になります。

考慮事項

サイトを構成および展開する際は、次の点に留意してください。

- 必須バージョン:
  - シトリックス 仮想アプリおよびデスクトップ 2311 以降。
  - Delivery Controller™のバージョンは、Web Studioのバージョンと一致するか、それ以前のバージョンである必要があり、最低要件は2311以降です。
  - この機能はWeb Studio（Webベース）専用であり、Citrix Studio（Windowsベース）では利用できません。
- シングルサインオンをサポートするには、すべてのサイトを信頼されたドメインに展開します。
- 統合されたWeb Studioコンソールを使用して、最大10個のCitrix Virtual Apps and Desktopsサイトを管理できます。

ワークフロー

始める前に

- プライマリサイトを決定し、Web Studioコンソールがプライマリサイト管理にアクセス可能であることを確認します。

  > **注:**
  >
  > - プライマリサイトを設計する際は、追加されたサイトのアクセシビリティがプライマリサイトの可用性に依存することに注意してください。プライマリサイトのパフォーマンスの問題は、追加されたサイトへのアクセスに影響を与える可能性があります。
  > - Web Studioがインストールされていない場合は、「Web Studioのインストール」を参照してください。

- Web Studioで管理する予定のサイトがすでに設定されていることを確認してください。
  - 新しいサイトを作成するには、「サイトの作成」を参照してください。
- (推奨) コンソールでサイト間を切り替える際にシングルサインオンを有効にするには、すべてのサイトで統合Windows認証 (IWA) を有効にします。IWAが有効になっていないサイトでは、ログイン資格情報を使用してサインインすることもできます。

ステップ1：Web Studioコンソールにサインインする

1. Webブラウザを開きます。`https://<address of the server hosting Web Studio>/Citrix/Studio`を入力します。
2. Web Studioにサインインして、プライマリサイトを管理します。

   > **注:**
   >
   > インストール時に使用するDelivery Controllerのアドレスによってサイトが識別されます。Delivery Controllerがプライマリサイトのものである場合、そのサイトにサインインします。

ステップ2：Web Studioを使用してサイトを追加する

1. 「**設定** > **サイト管理の一元化**」に移動し、「**追加**」をクリックします。

サイト管理の一元化(/en-us/citrix-virtual-apps-desktops/2311/media/centralize-site-mgmt-add.png)

2. **Virtual Apps and Desktopsサイトの追加**ページで、**サイトの追加**をクリックします。

   サイトの追加(/en-us/citrix-virtual-apps-desktops/2311/media/add-cvad-sites.png)

3. デリバリーコントローラーを追加するには、次のいずれかの操作を実行します。

   - 「**コントローラーの追加**」をクリックし、FQDNを入力します。接続をテストするには、「**テスト**」をクリックします。
   - 「**検出**」をクリックします。

     a. 「**サイト検出**」ページで、サイト内に存在するコントローラーのアドレスを選択または入力します。

     b. コントローラーに対する完全な権限を持つ管理者の資格情報を、「**ユーザー名**」フィールドと「**パスワード**」フィールドに入力します。

     c. 「**完了**」をクリックします。

   サイト検出(/en-us/citrix-virtual-apps-desktops/2311/media/site-discovery.png)

   > **注:**
   >
   > 検出機能は、入力したデリバリーコントローラーのアドレスに基づいて、サイト内で到達可能なデリバリーコントローラーを自動的に追加します。

4. 「**保存**」をクリックします。

   サイト構成を管理または編集するには、「**設定** > **サイト管理の一元化**」に移動し、「**管理**」をクリックします。「**管理**」オプションは、プライマリサイトでのみ有効になります。

   集中サイトの管理(/en-us/citrix-virtual-apps-desktops/2311/media/centralize-site-mgmt-manage.png)

ステップ3：サイト設定の管理

サイト構成の変更を反映させるには、ブラウザを更新してください。サイト選択ボックスは、コンソールの右上隅に表示されます。

設定ページで、**更新**アイコンの横にある右上のドロップダウンメニューからサイトを選択します。コンソールには、選択したサイトの構成が表示されます。

注:

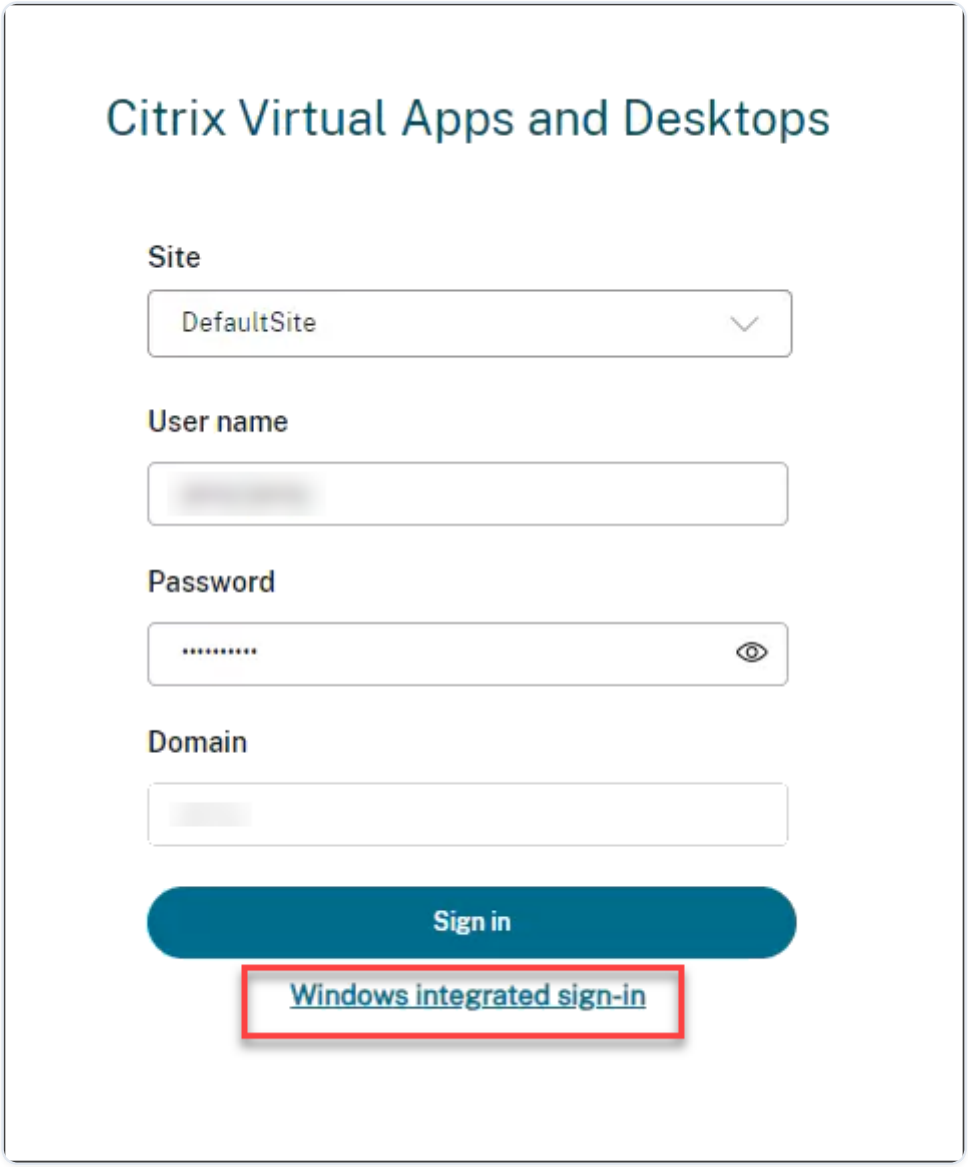
- プライマリサイトに到達できない場合、それに関連付けられている他のサイトにアクセスすることはできません。
- 別のサイトに切り替える際は、サインインに必要なアクセス許可またはアクセス資格情報があることを確認してください。

サイト構成後のサインインエクスペリエンス

1. Webブラウザを開きます。`https://<address of the server hosting Web Studio>/Citrix/Studio`と入力します。
2. **サイト**フィールドからサイトを選択します。
3. **Windows統合サインイン**を選択するか、**ユーザー名**と**パスワード**を入力してサインインします。

注:

Windows統合サインインは、選択したサイトで有効になっている場合にのみ利用できます。統合Windows認証の詳細については、「認証の管理」を参照してください。

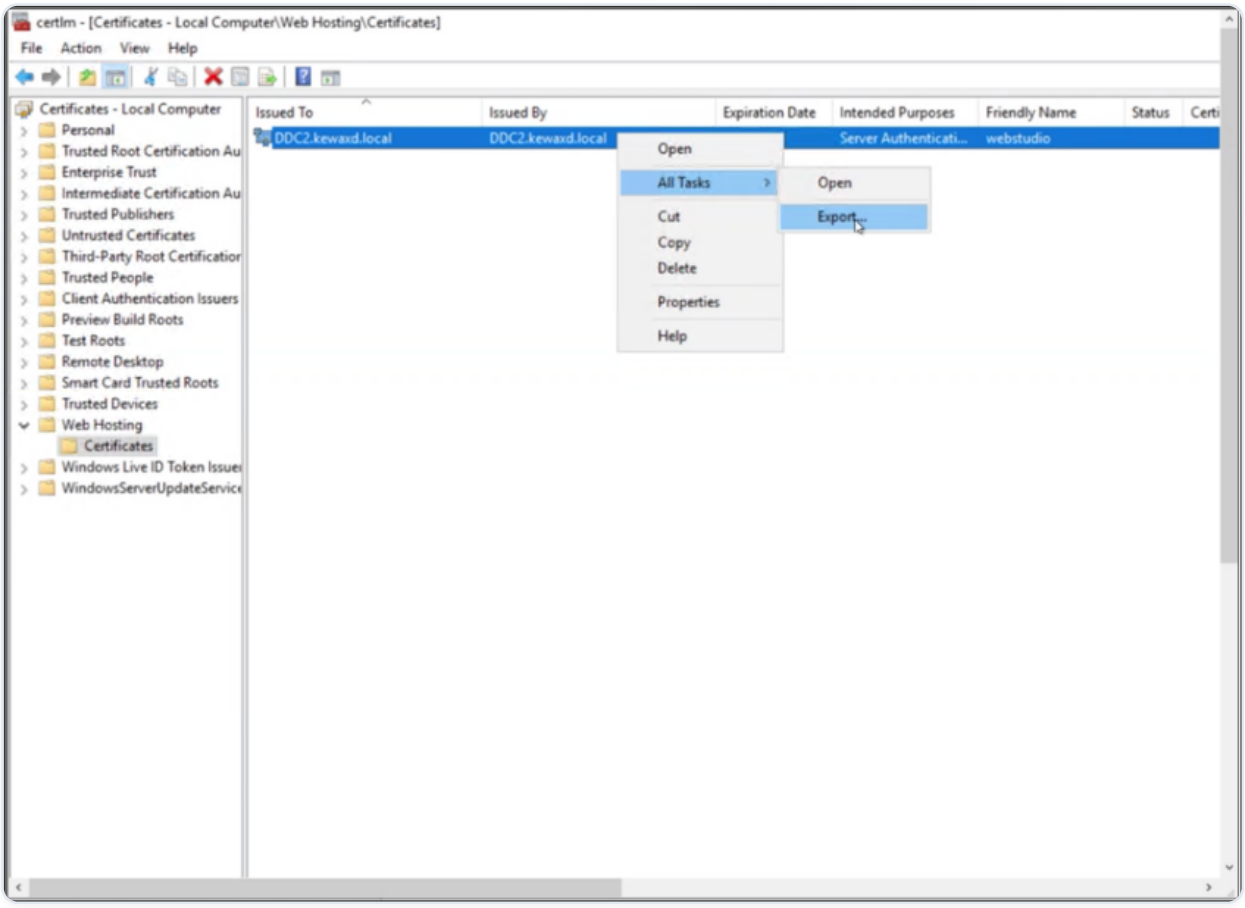


Web Studio展開の保護 (オプション)

Delivery Controller™ と一緒に Web Studio をインストールすると、インストーラーは、現在のサーバーの `443` ポートにバインドされた自己署名証明書を作成します。Web Studio と Delivery Controller は、その証明書を TLS 証明書として使用します。別のマシンからアクセスする場合、Web Studio にアクセスできないか、Web Studio のログオン画面にエラーが表示されることがあります。

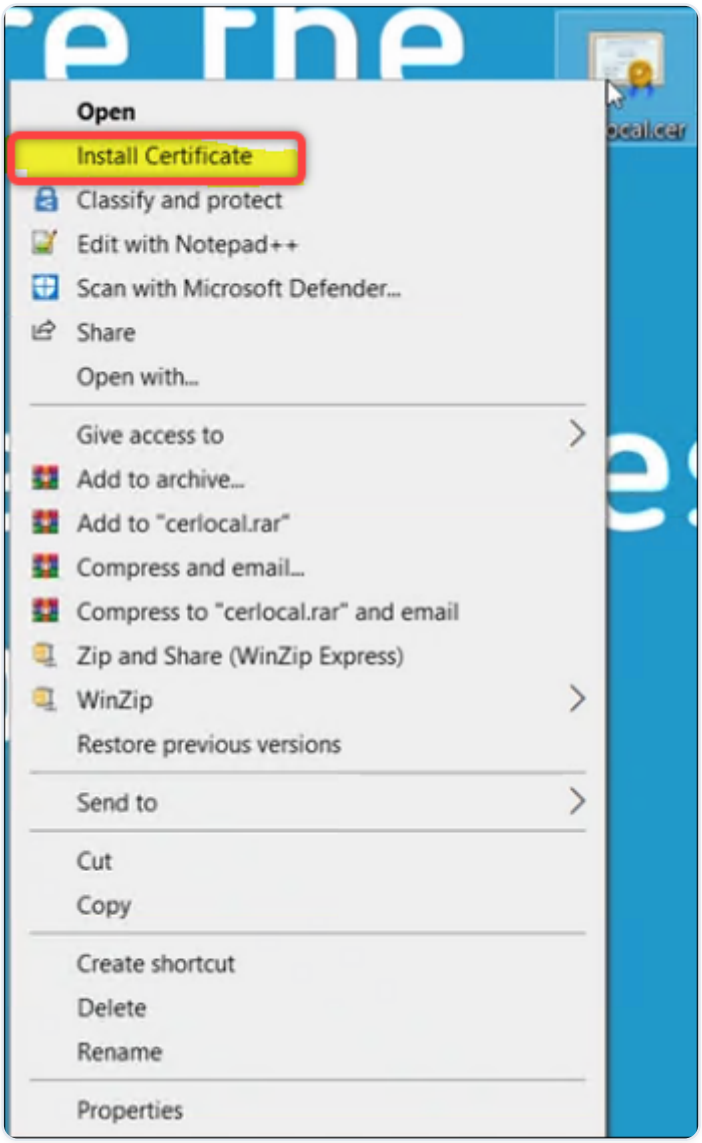
別のマシンから Web Studio にアクセスしたい場合は、次の操作を実行できます。

1. Delivery Controller から自己署名証明書をエクスポートします。



- **秘密キーのエクスポート**については、**いいえ、秘密キーをエクスポートしません**を選択します。
- **エクスポートファイル形式**については、**DER encoded binary X.509 (.CER)**を選択します。

2. Web Studio にアクセスしたいマシンに移動し、証明書をインストールします。



- 「**ストアの場所**」で、「**ローカルコンピューター**」を選択します。

Delivery Controller から離れた専用サーバーに Web Studio をインストールすることを選択した場合、2つのタスクを実行する必要があります。

- **タスク 1**: Web Studio サーバーと Delivery Controller から、それぞれ証明書をエクスポートします。
- **タスク 2**: Web Studio にアクセスしたいマシンに2つの証明書をインストールします。

> **注:**
>
> ベストプラクティスとして、外部の公開信頼証明書またはエンタープライズ CA の証明書を使用して Web Studio 展開を保護することをお勧めします。

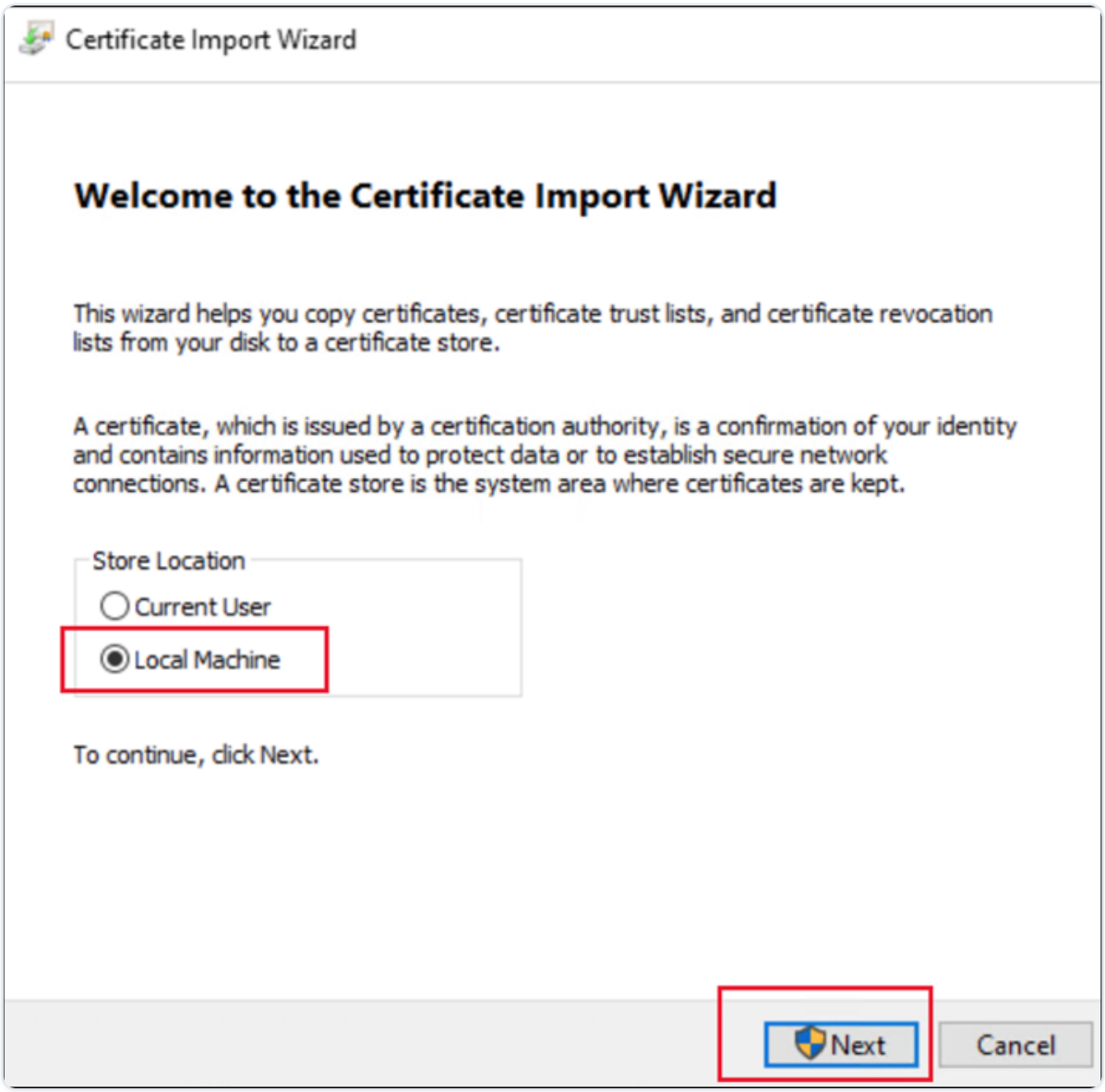
外部の公開信頼証明書を使用する

次の3つの方法のいずれかを使用して、外部の公開信頼証明書を Web Studio サーバーにインポートできます。

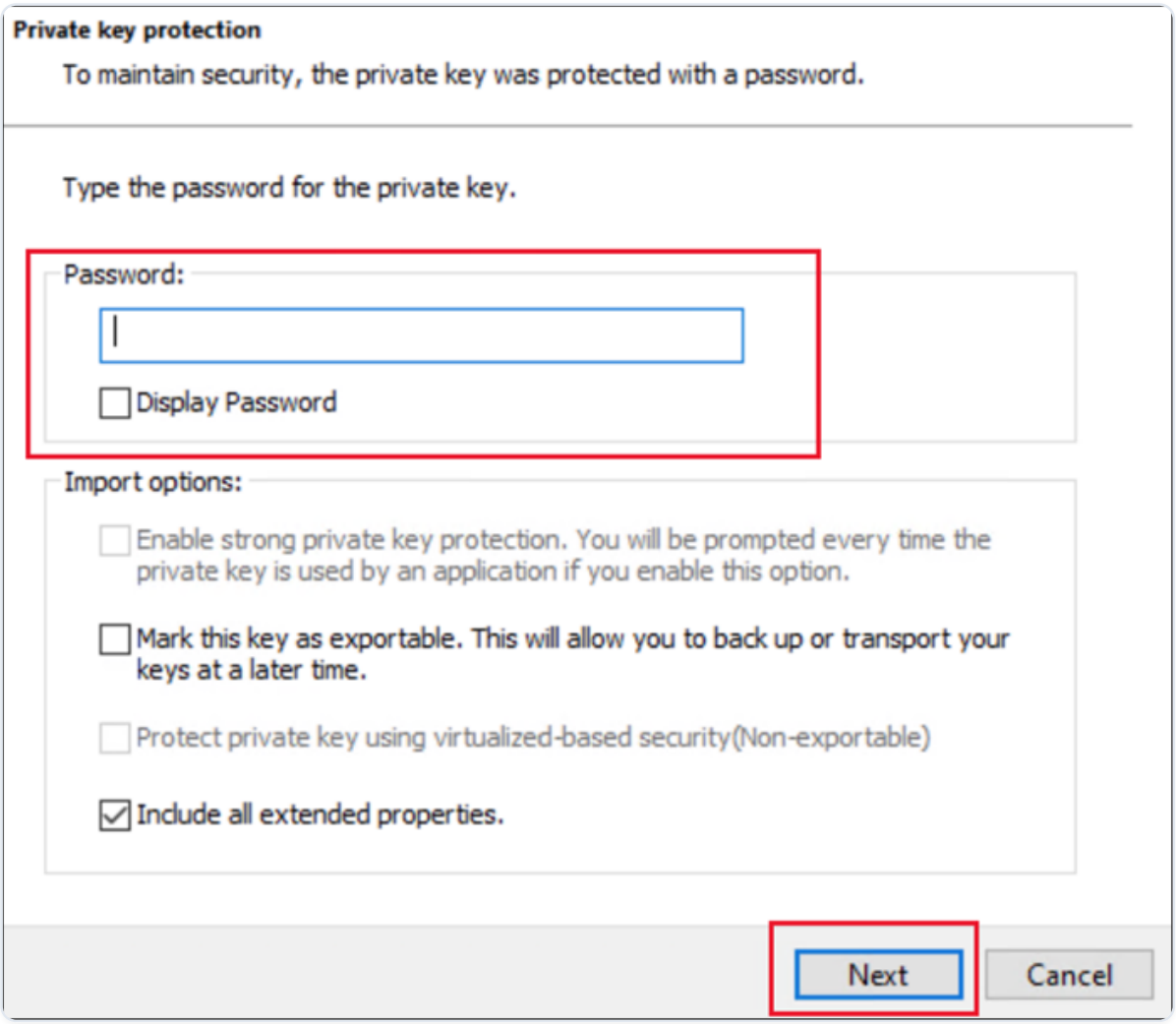
- **PFXファイルをインストールします。**

  a. PFXファイルをダブルクリックします。

  b. 「**ストアの場所**」で、「**ローカルコンピューター**」を選択します。



  c. 必要に応じてパスワードを入力します。



d. **証明書ストア**には、**個人**を選択します。

証明書ストア(/en-us/citrix-virtual-apps-desktops/2311/media/certificate-store.png)

- **コンピューター証明書の管理コンソールを使用します。**

a. コンピューター証明書の管理コンソールを開き、**個人 > 証明書 > すべてのタスク > インポート**に移動します。

コンピューター証明書の管理コンソール(/en-us/citrix-virtual-apps-desktops/2311/media/manage-computer-certificates-console.png)

b. PFXファイルを選択し、必要に応じてパスワードを入力します。

- **PowerShellを使用します。**

```
Import-PfxCertificate -Password $(ConvertTo-SecureString -String
"123456" -AsPlainText -Force) -CertStoreLocation Cert:\LocalMachine\My\
-FilePath .\Desktop\certificate.pfx
```

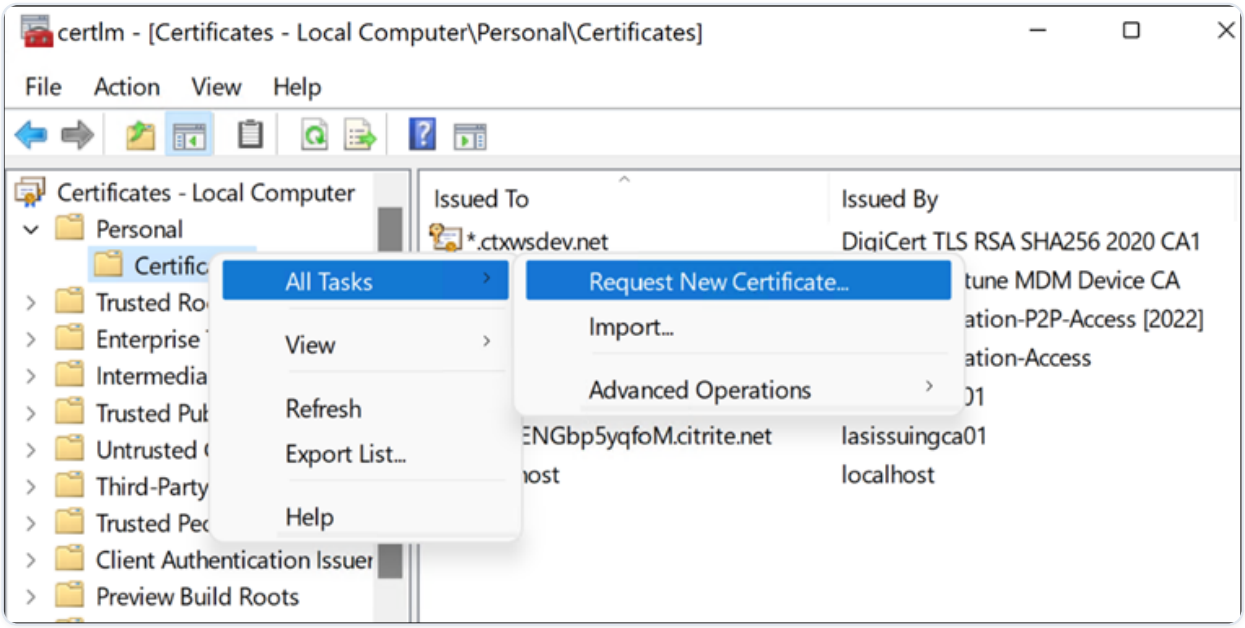
その後、証明書を`443`ポートにバインドします。これは、インストールまたはアップグレードの前、あるいはインストールまたはアップグレードの後に行うことができます。`443`ポートに証明書バインディングが構成されている場合、インストーラーは何も行いません。詳細については、「インストールまたはアップグレードの前に」(#before-installation-or-upgrade)を参照してください。

エンタープライズCAからの証明書を使用する

開始する前に、エンタープライズ証明機関（CA）サーバーがドメインに展開されていることを確認してください。

証明書を要求するには、次の手順を実行します。

1. サーバーで、**コンピューター証明書の管理コンソール**を開きます。
2. **個人 > 証明書 > すべてのタスク > 新しい証明書の要求**に移動します。



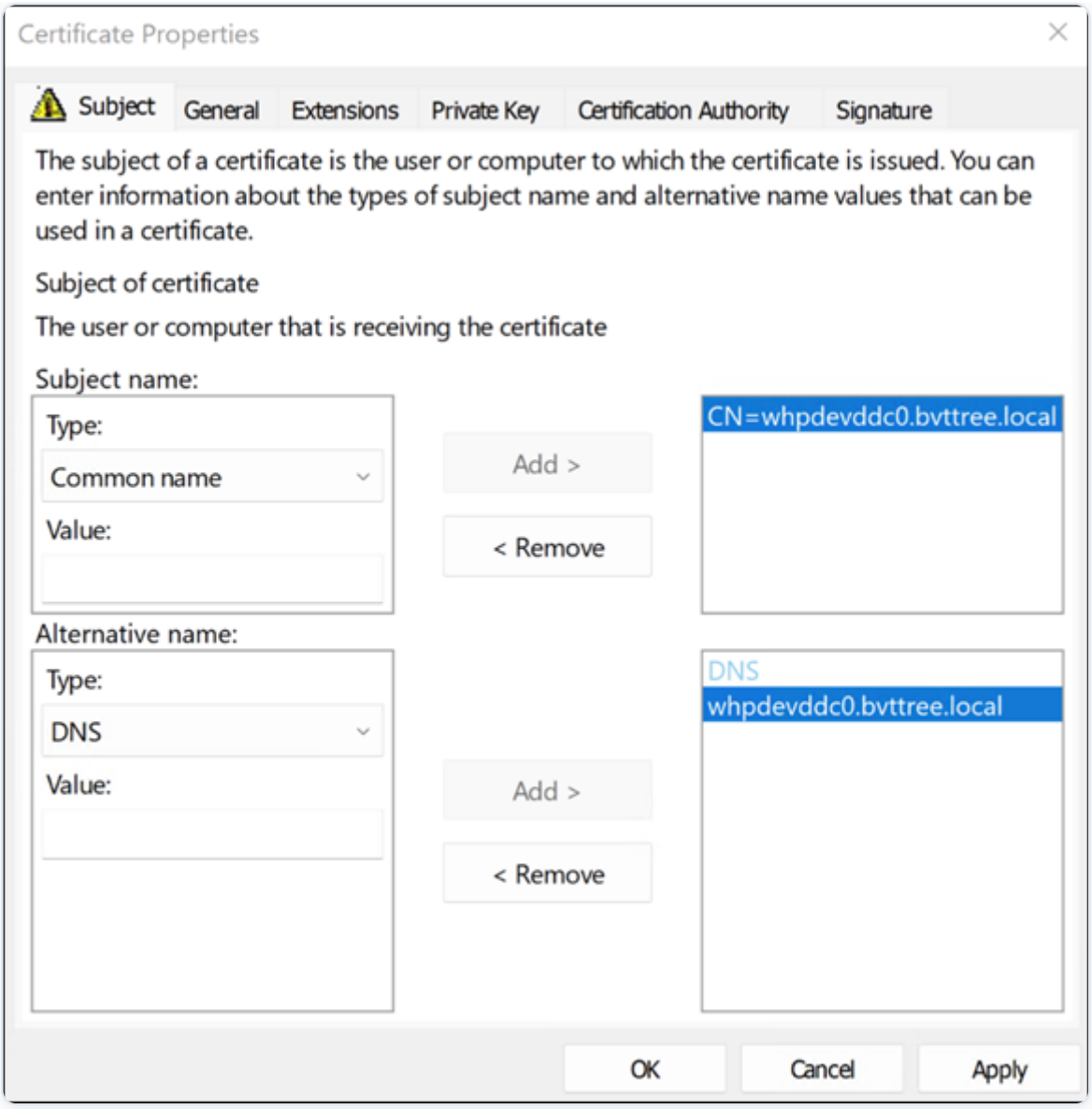
3. **証明書の登録**に移動し、Webサーバーを選択して、警告メッセージをクリックして必要な情報を入力します。

   証明書の登録(/en-us/citrix-virtual-apps-desktops/2311/media/certificate-enrollment.png)

4. サブジェクト名タイプとして**共通名**を選択し、FQDNまたはDNSを入力します。また、代替名も入力します。

> **注:**

ワイルドカード証明書が必要な場合は、サブジェクト名に`CN=*.bvttree.local`を、代替DNS名に`*.bvttree.local and bvttree.local`を入力できます。



証明書は**個人 > 証明書**の下にあります。

個人 > 証明書(/en-us/citrix-virtual-apps-desktops/2311/media/personal-certificates.png)

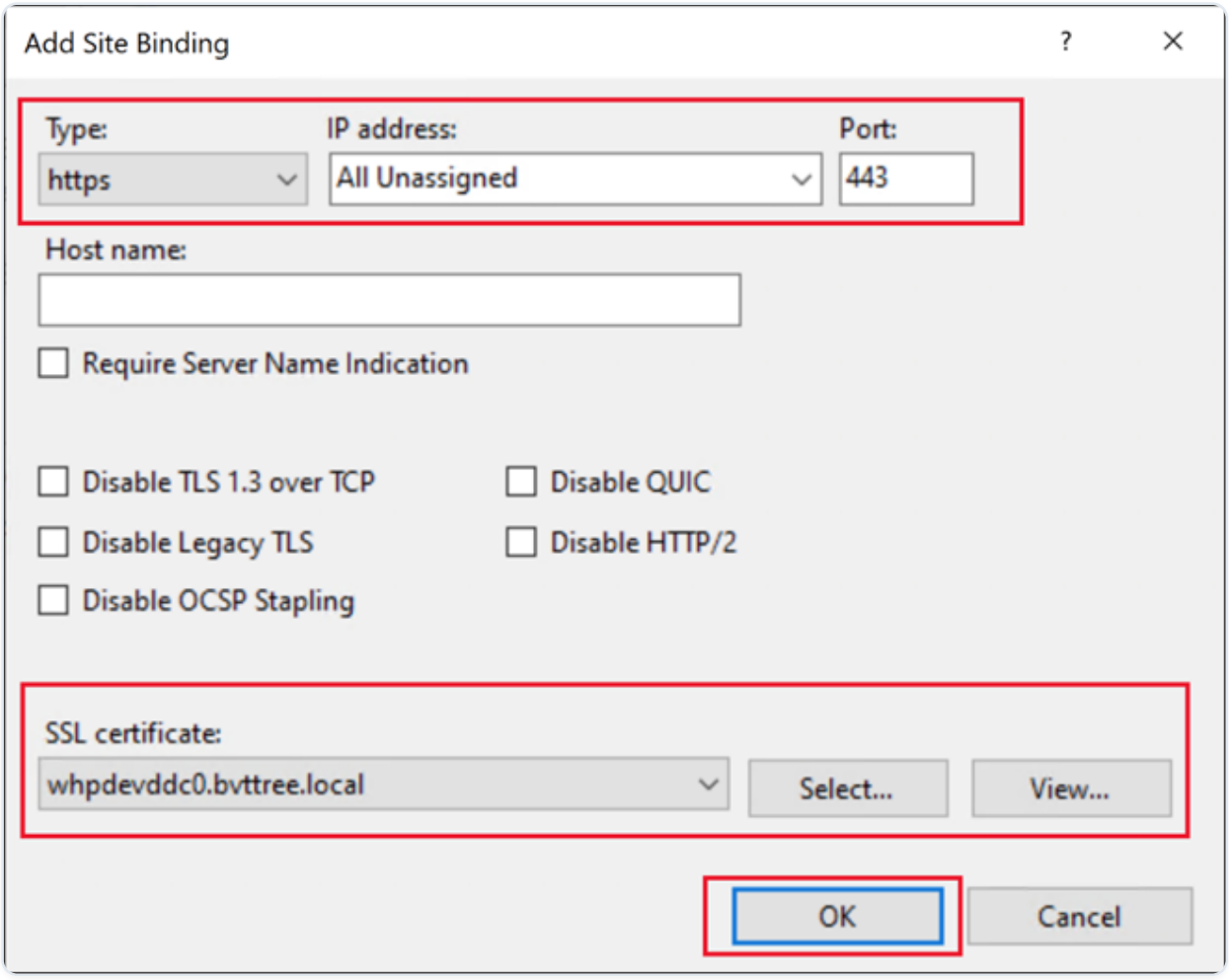
その後、証明書を`443`ポートにバインドします。これは、インストールまたはアップグレードの前、あるいはインストールまたはアップグレードの後に行うことができます。`443`ポートに証明書バインディングが構成されている場合、インストーラーは何も行いません。

インストールまたはアップグレードの前

証明書を`443`ポートにバインドするには、次の手順を実行します（`443`に証明書バインディングがまだ構成されておらず、サーバーでIISが有効になっている場合）。

1. 管理者としてWeb Studioサーバーにログオンします。
2. IISマネージャーを開き、**サイト > 既定のWebサイト > バインド**の順に参照します。
3. **サイトバインド**で、**追加**をクリックします。

   サイトバインド 2(/en-us/citrix-virtual-apps-desktops/2311/media/site-bindings-2.png)
4. **サイトバインドの追加**で、タイプを`https`に、ポートを443に設定し、CAから要求したSSL証明書を選択して、**OK**をクリックします。



Web Studioをインストールすると、Web StudioとDelivery Controllerは、証明書を使用して接続を保護するように自動的に構成されます。

または、PowerShellを使用して証明書を変更することもできます。

```
$certSName = 'CN=whpdevddc0.bvttree.local'  # The subject name of the
certificate

$certificate = Get-ChildItem -Path Cert:\LocalMachine\My\ | ? {$_.Subject
-eq $certSName}
```

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=$
($certificate.Thumbprint) certstorename=My appid="$($(New-
Guid).ToString("B"))"
```

インストールまたはアップグレード後

Web Studioサーバーに移動し、IISマネージャーを使用して証明書を変更します。 または、PowerShellを使用して証明書を変更することもできます。

```
$certSName = 'CN=whpdevddc0.bvttree.local' # The Enterprise CA certificate
subject.

$certificate = Get-ChildItem -Path Cert:\LocalMachine\My\ | ? {$_.Subject
-eq $certSName}

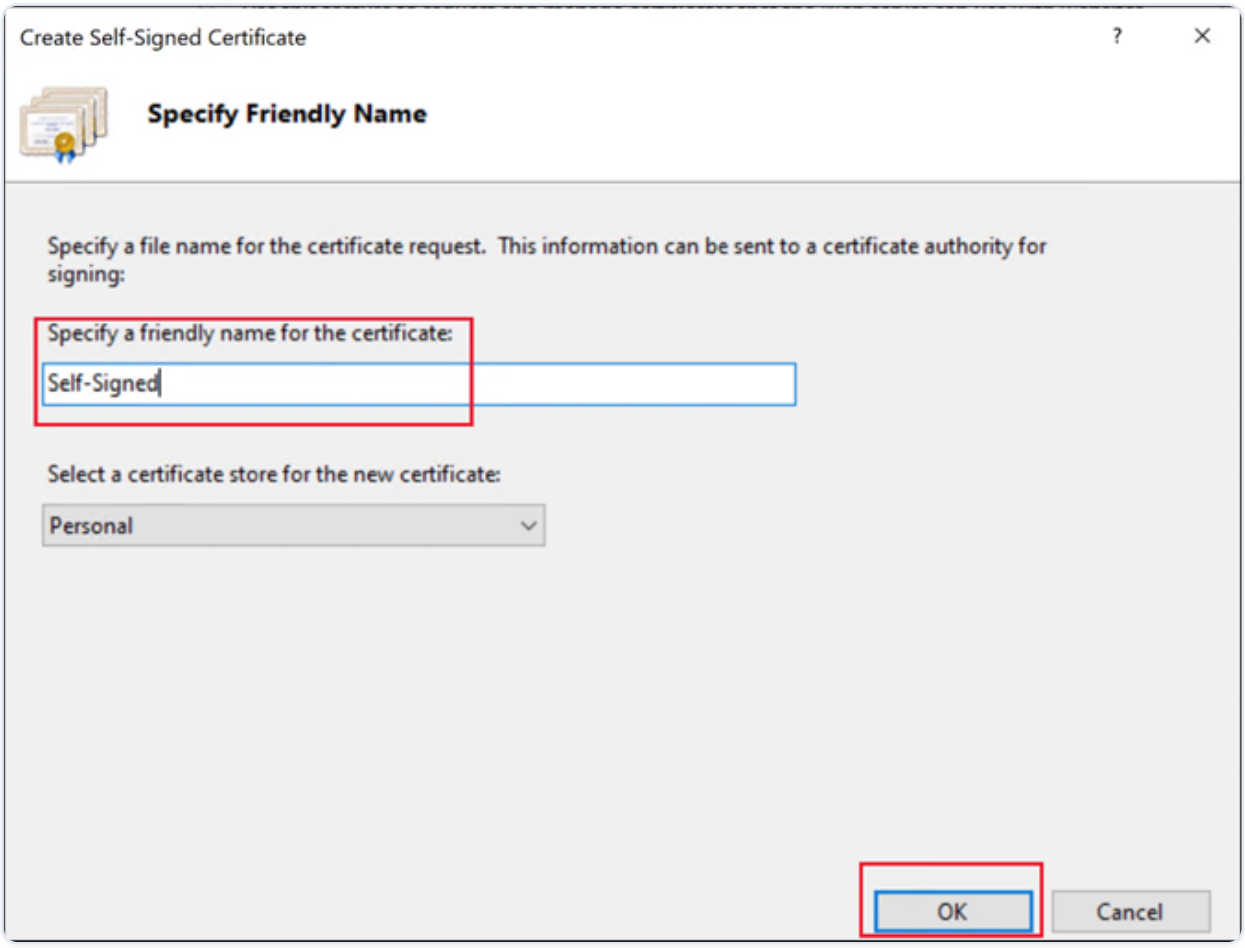
netsh http update sslcert ipport=0.0.0.0:443 certhash=$
($certificate.Thumbprint)
```

新しい自己署名証明書を使用する

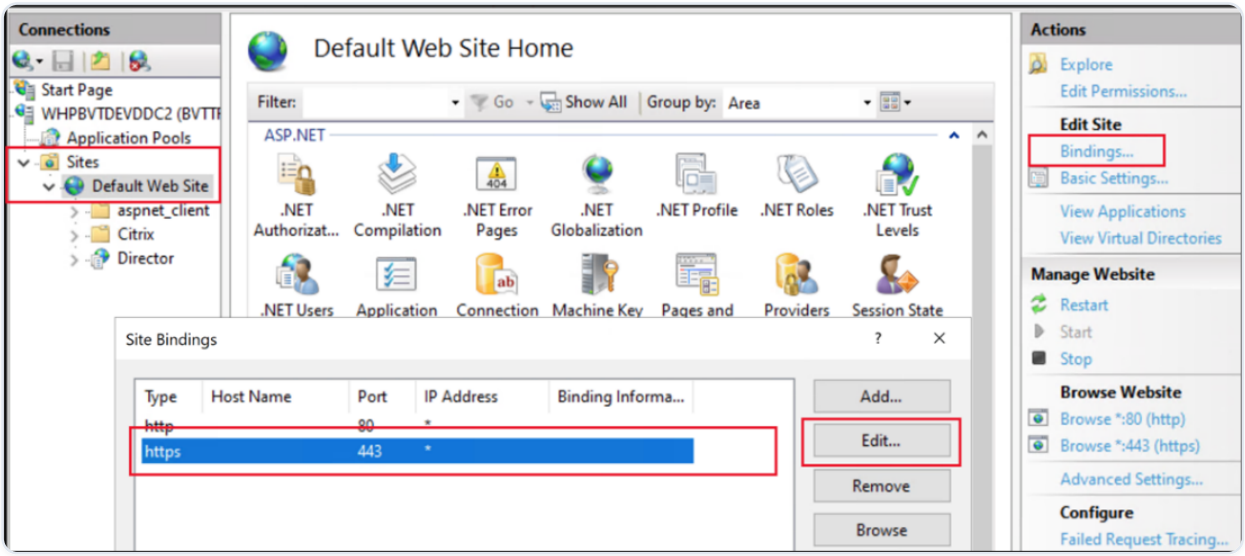
新しい自己署名証明書を生成し、既存の証明書と置き換えることができます。次の手順を実行します。

1. Web Studioサーバーに管理者としてログオンします。
2. IISマネージャーを開き、**サーバー証明書**に移動し、**操作**ペインで**自己署名証明書の作成**を選択します。

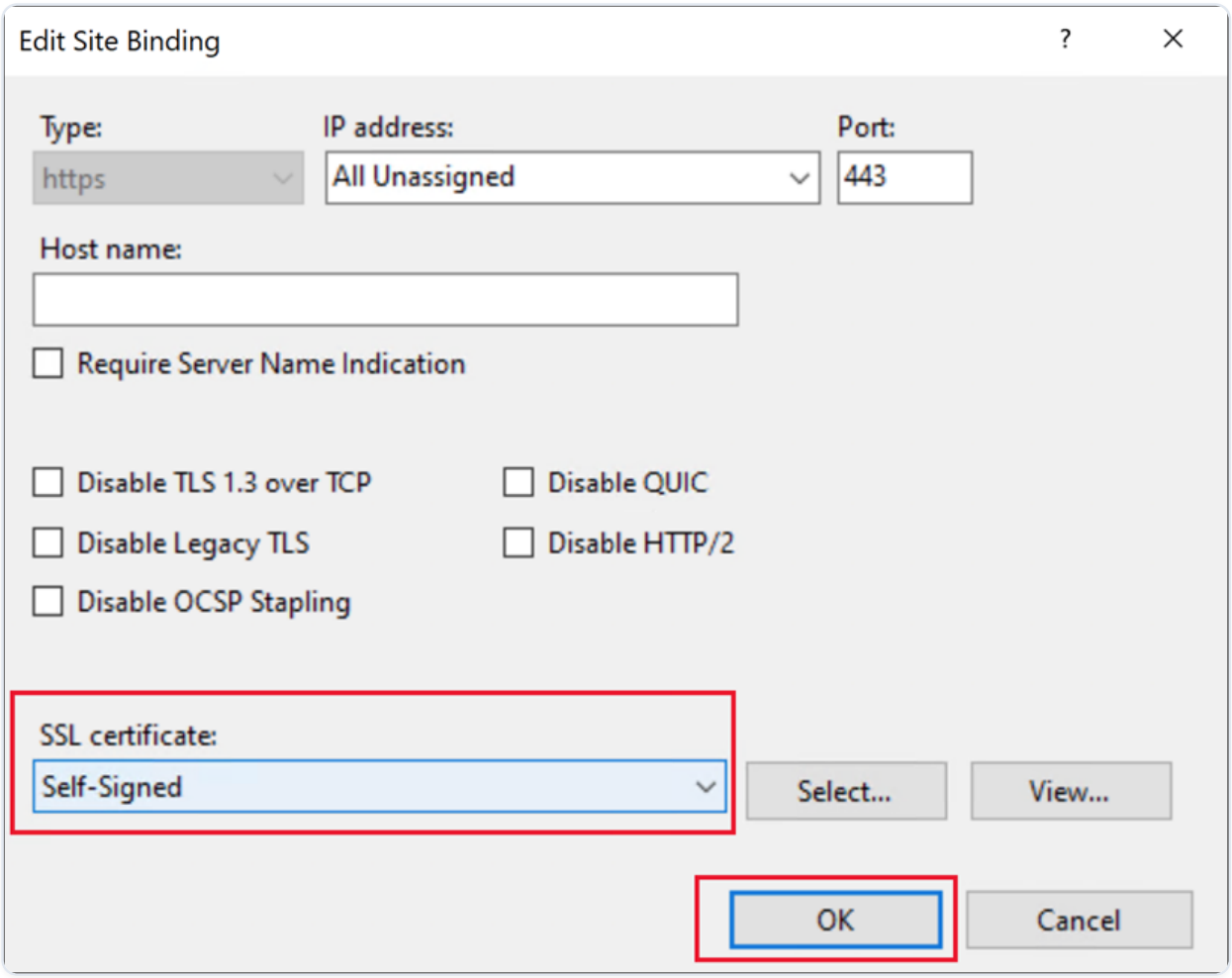
   サーバー証明書(/en-us/citrix-virtual-apps-desktops/2311/media/server-certificates.png)
3. 「**自己署名証明書の作成**」で、証明書の名前を入力し、「**OK**」をクリックします。自己署名証明書が作成されます。



4. **サイト > 既定のWebサイト**に移動し、**操作**ペインで**バインド**を選択し、`https`エントリを選択して、**編集**を選択します。



5. **サイトバインドの編集**で、リストから証明書を選択し、**OK**をクリックします。



これで証明書の変更は完了です。

または、PowerShellを使用して証明書を変更することもできます。

```
$certSubject = "CN=WHPBVTDEVDDC2.BVTTREE.LOCAL" # The FQDN of the server.

$frindlyName = "Self-Signed-3"

$expireYears = 5



## new self-signed certificate under LocalMachine\My

$certificate = New-SelfSignedCertificate -Subject $certSubject
-CertStoreLocation "Cert:\LocalMachine\My\" -KeyExportPolicy Exportable
-KeySpec Signature -KeyLength 2048 -KeyAlgorithm RSA -HashAlgorithm SHA256
-FriendlyName $frindlyName -NotAfter $
([System.DateTime]::Now.AddYears($expireYears))
```

```
Remove-Item -Path $Env:TEMP\tempCertificate.cer -Force -ErrorAction
SilentlyContinue



## Import this certificate into LocalMachine\Root to let this OS trust
this certificate

Export-Certificate -Type CERT -Force -Cert $certificate -FilePath
$Env:TEMP\tempCertificate.cer -NoClobber

Import-Certificate -FilePath $Env:TEMP\tempCertificate.cer
-CertStoreLocation "Cert:\LocalMachine\Root\"



## Update bind the 0.0.0.0:443 with this certificate

Invoke-Command -ScriptBlock { Param ($param1) netsh http update sslcert
ipport=0.0.0.0:443 certhash=$param1 } -ArgumentList
@($certificate.Thumbprint)
```

Call Home の主要データポイント

Call Home は以下の主要データポイントを収集します。

(M) = 手動収集時のみ取得 (PowerShell コマンドレット `Start-CitrixCallHomeUpload`)

ファイル名	カテゴリ	データグループ
		マシン
		XDサイト
		サイト情報
		Broker DB 情報 (M)
		インストールされている DB バージョン (M)

		Broker サービスステータス (M)
		登録済みサービスインスタンス (M)
		ブローカーライセンステスト (M)
		アクティブなHDX™セッション (M)
		ブローカー管理者
		ブローカー管理者権限
		RDS構成 (LicensingSettings、SessionSettings、SpecifiedLicenseServers、RegisteredLicenseServersを含む)
		監視サービス (M) (MonitorConfiguration、MonitorDataStore、MonitorDBConnection、MonitorDBSchemaVersion、MonitorService、MonitorServiceAddedCapability、MonitorServiceInstance、MonitorServiceStatus、MonitorInstalledDBVersionを含む)
		構成ログ
		接続ログ
		ハイパーバイザー接続 (M)
		ブローカーハイパーバイザー接続

		ハイパーバイザーアラート
		カタログ
		マルチセッションOSエージェント (M)
		シングルセッションOSエージェント (M)
		公開アプリケーション
		デリバリー グループ
		構成済みデリバリーエージェント

		Citrixインストール済みコンポーネント
		Citrix ブローカー サービス情報
		Broker Service構成ファイル
		Machine Creation Services™ 構成ファイル
		Host Service構成ファイル
		AD Identity Service構成ファイル
		Configuration Service構成ファイル
		Configuration Logging Service構成ファイル
		Delegated Administration Service構成ファイル

		環境テストサービス構成ファイル
		監視サービス構成ファイル
		Storefront™ サービス構成ファイル
		ワークステーションエージェント構成ファイル
		Citrix VDA情報
		Citrix XD ホットフィックス
		Citrix_VirtualChannel_Graphics_Enum
		Citrix_VirtualChannel_Flash_Enum
		Citrix_VirtualChannel_Printer_Enum

		コンピューター
		BIOS
		メモリ情報
		プロセッサ
		PNP デバイス
		デバイス
		ディスクドライブ
		論理ドライブ
		ページファイル使用状況
		ネットワークアダプター

		ネットワークアダプター構成
		ipConfig
		ビデオコントローラー
		IDE コントローラー
		SCSI コントローラー

		HKLM:\Software\Wow6432Node\Citrix
		HKLM:\System\CurrentControlSet\Control\Citrix
		HKLM:\SOFTWARE\Policies\Citrix
		HKLM:\Software\Microsoft\Cryptography
		HKLM:\Software\Wow6432Node\Microsoft\Cryptography
		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Windows
		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
		HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

		HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\SYSTEM\CurrentControlSet\Control\Print\Environments
		HKLM:\System\CurrentControlSet\Control\セッション マネージャー
		HKLM:\System\CurrentControlSet\Control\ターミナル サーバー
		HKCU:\Control Panel\Desktop
		HKLM:\SOFTWARE\Classes\ShockwaveFlash.ShockwaveFlash\CurVer
		HKLM:\SYSTEM\CurrentControlSet\Control\SystemInformation
		HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem
		HKLM:\SYSTEM\CurrentControlSet\Control\Windows
		HKLM:\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

		ドライバー
		EnvVariables
		OS
		プロセス
		サービス
		サービスパック
		ジーピーリザルト
		Microsoft ホットフィックス
		ネットスタット
		PNP ドライバー

		システムイベントログ
		AOT (常時オンのトレース)
		クラッシュダンプ

		アップタイム
		メモリ
		コンピューターシステム
		プロセッサ
		ビデオコントローラー
		ディスクドライブ
		ブラウザ情報
		再起動回数

		メモリ使用量
		ディスク使用量
		ICAセッション解像度
		ICAカラー深度
		メタインストーラーCEIPマシンID

		ストア数
		サーバーグループ内のサーバー数
		ストアあたりのDelivery Controller™数
		HTTPS有効
		Citrix Receiver™ のクラシックエクスペリエンスが有効
		Citrix レシーバーの HTML5 レシーバー設定
		Citrix Receiver のワークスペースコントロールが有効
		ストアのリモートアクセスが有効
		ゲートウェイ数
		統合された NetScaler® 認証用の明示的な JSON サービス

プロファイルコンテナのポリシー設定

プロファイルコンテナ

ユーザープロファイルに関連付けられた大きなフォルダーは、ログオンの遅延を引き起こします。Citrix Profile Managementは、プロファイルディスク（VHDXファイル）に含めるフォルダーを指定できるVHDXベースのプロファイルソリューションを提供します。このソリューションは、指定されたフォルダーをネットワークに保存されているプロファイルディスクにマッピングすることで、ログオン時間を短縮します。プロファイルコンテナは、ログオン時にこれらのフォルダーを含むプロファイルディスクをアタッチするため、フォルダーのコピーをローカルプロファイルに保存する必要がなくなります。これにより、ログオン時間が短縮されます。

プロファイルコンテナのローカルキャッシュを有効にする

このポリシーは、Citrix Profile Managementプロファイルコンテナのローカルキャッシュサポートを有効にします。ポリシーが**有効**に設定されている場合、各ローカルプロファイルは、そのCitrix Profile Managementプロファイルコンテナのローカルキャッシュとして機能します。プロファイルストリーミングが使用されている場合、ローカルにキャッシュされたファイルはオンデマンドで作成されます。それ以外の場合は、ユーザーログオン時に作成されます。ローカルキャッシュ機能を使用するには、ユーザープロファイル全体をCitrix Profile Managementプロファイルコンテナに配置します。

プロファイルコンテナから除外するフォルダー

Citrix Profile Managementプロファイルコンテナから除外するフォルダーのリスト。

プロファイルコンテナに含めるフォルダー

親フォルダーが除外されている場合に、Citrix Profile Managementプロファイルコンテナに保持するフォルダーのリスト。

このリストのフォルダーは、除外されたフォルダーのサブフォルダーである必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナに含めるファイル

Citrix Profile Managementプロファイルコンテナに含めるファイルのリスト。

このリストのファイルは、除外されたフォルダー内にある必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナから除外するファイル

Citrix Profile Managementプロファイルコンテナから除外するファイルのリスト。

VHDディスクの圧縮を有効にする

Profile Management の VHD ディスク圧縮を有効にできます。有効にすると、特定の条件が満たされた場合に、ユーザーのログオフ時に VHD ディスクが自動的に圧縮されます。このポリシーにより、プロファイルコンテナ、OneDriveコンテナ、およびミラーフォルダコンテナによって消費されるストレージスペースを節約できます。

必要に応じて、詳細設定にある「**VHDディスク圧縮をトリガーする空き領域の比率**」、「**VHDディスク圧縮をトリガーするログオフ回数**」、「**VHDディスク圧縮のデフラグを無効にする**」の各ポリシーを使用して、デフォルトのVHD圧縮設定と動作を調整できます。

プロファイルコンテナのVHD自動拡張を有効にする

プロファイルコンテナのVHD自動拡張を有効にするかどうかを指定できます。有効にすると、すべてのVHD自動拡張設定がプロファイルコンテナに適用されます。

構成の優先順位:

- ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
- ここでも.iniファイルでもこのポリシーが構成されていない場合、無効になります。

VHDコンテナへの排他的アクセスを有効にする

デフォルトでは、VHDコンテナは同時アクセスを許可します。この設定を有効にすると、一度に1つのアクセスのみが許可されます。この機能は、プロファイルコンテナとOneDriveコンテナに適用されます。

> **注:**

> コンテナベースのプロファイルソリューションでプロファイルコンテナに対してこの設定を有効にすると、「*プロファイルコンテナのマルチセッション書き戻しを有効にする*」設定が自動的に無効になります。

> 構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。

2. ここでも.iniファイルでもこのポリシーが構成されていない場合、この設定は無効になります。

ログオン時にプロファイルコンテナが利用できない場合にユーザーをログオフする

ユーザーログオン時にプロファイルコンテナが利用できない場合に、ユーザーを強制的にログオフさせ、(オプションで)ユーザーに表示されるエラーメッセージをカスタマイズできます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、この設定は無効になります。

プロファイルコンテナにアクセスするユーザーとグループ

プロファイルコンテナに対して`Read & Execute`権限を持つADドメインユーザーとグループを指定できます。デフォルトでは、プロファイルコンテナはその所有者のみがアクセスできます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの設定が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、プロファイルコンテナはその所有者のみがアクセスできます。

シトリックス バーチャル アプリ アンド デスクトップ 7 2411

> **重要:**

> 現在のリリース (CR) および長期サービスリリース (LTSR) の製品ライフサイクル戦略については、ライフサイクルマイルストーンに記載されています。

> Citrix Virtual Apps and Desktops は、データセキュリティを強化し、コストを削減し、生産性を向上させながら、あらゆるデバイスに、あらゆるネットワーク経由でアプリケーションおよびデスクトップを配信するための仮想化ソリューションを提供します。

Citrix Virtual Apps and Desktops の長期サービスリリース (LTSR) プログラムは、Citrix Virtual Apps and Desktops リリースに安定性と長期サポートを提供します。

累積更新プログラム 5 (CU5) は、2203 LTSR の最新の更新プログラムです。LTSR は、Citrix Virtual Apps and Desktops 1912 でも利用可能です。

- ユースケース情報については、`<https://www.citrix.com/products/citrix-virtual-apps-and-desktops/>`を参照してください。
- Citrix Virtual Apps and Desktops の展開におけるコンポーネントとテクノロジーについて学ぶには、技術概要を参照してください。

以前のリリース

現在利用可能なその他のリリースのドキュメントは、Citrix Virtual Apps and Desktopsにあります。

さらに以前のリリースについては、ドキュメントはLegacy Documentationにアーカイブされています。

シトリックス クラウド™ におけるシトリックス バーチャル アップス アンド デスクトップス

Citrix Cloud Virtual Apps and Desktops の提供サービスは Citrix DaaS です。詳細については、Citrix DaaSを参照してください。

役立つリンク

- Citrix サポーナビリティパック
- LTSR FAQ
- Citrix Virtual Apps and Desktops サービスオプション
- 製品ライフサイクル日付
- Citrix Workspace app 向け LTSRプログラム