XenApp et XenDesktop 7.9

Aug 22, 2016

Nouveautés

Problèmes résolus

Problèmes connus

Fonctionnalités absentes de cette version

Avis de tiers

Configuration système requise

Vue d'ensemble technique

Concepts et composants

Active Directory

Bases de données

Méthodes de mise à disposition

Architectures de référence

Guides de conception

Guides d'implémentation

Installer et configurer

Préparer l'installation

Installer à l'aide de l'interface graphique

Installer à l'aide de la ligne de commande

Installer les VDA à l'aide de scripts

Installer des VDA Red Hat Linux

Installer des VDA SUSE Linux

Créer un site

Créer des catalogues de machines

Gérer les catalogues de machines

Créer des groupes de mise à disposition

Gérer les groupes de mise à disposition

Créer des groupes d'applications

Gérer des groupes d'applications

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Remote PC Access

App-V

AppDisks

Local App Access et redirection d'adresse URL

XenApp Secure Browser

Server VDI

Personal vDisk

Supprimer des composants

Mettre à niveau et migrer

Mettre un déploiement à niveau

Migrer XenApp 6.x

Migrer XenDesktop 4

Sécuriser

Considérations de sécurité et meilleures pratiques

Délégation de l'administration

Cartes à puce

Transport Layer Security (TLS)

Service d'authentification fédérée

Imprimer

Exemple de configuration de l'impression

Recommandations, considérations en matière de sécurité et opérations par défaut

Stratégies et préférences d'impression

Provisionner les imprimantes

Gérer l'environnement d'impression

HDX

Mode de compatibilité Thinwire

Canal virtuel Framehawk

HDX 3D Pro

Redirection Flash

Accélération GPU pour OS de bureau Windows

Accélération GPU pour OS de serveur Windows

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Accélération logicielle OpenGL

Fonctionnalités audio

Priorités du trafic réseau

Considérations USB et de lecteur client

Stratégies

Utilisation des stratégies

Modèles de stratégie

Créer des stratégies

Comparer, donner un ordre de priorité, modéliser et résoudre les problèmes des stratégies

Paramètres de stratégie par défaut

Référence des paramètres de stratégie

Gérer

Système de licences

Applications

Zones

Connexions et ressources

Location de connexions

Adresses IP virtuelles et bouclage virtuel

Delivery Controller

Sessions

Utiliser la fonction de recherche dans Studio

Balises

Prise en charge de IPv4/IPv6

Redirection de dossiers clients

Profils utilisateur

Citrix Insight Services

Surveiller

Enregistrement de session

Journalisation de la configuration

Surveiller les Personal vDisks

Director

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration avancée

Surveiller les déploiements

Alertes et notifications

Administration déléguée et Director

Sécuriser le déploiement de Director

Configurer les permissions pour VDA antérieurs à XenDesktop 7.

Configurer HDX Insight

Résoudre les problèmes utilisateur

Kits de développement (SDK) et API

API Monitor Service OData

Exemples de déploiement FIPS

Citrix SCOM Management Pack pour XenApp et XenDesktop

Citrix SCOM Management Pack pour Serveur de licences

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Nouveautés

Jul 07, 2016

Dans cet article :

À propos de cette version

XenApp et XenDesktop 7.9

Virtual Delivery Agent (VDA) 7.9

StoreFront 3.6

Provisioning Services 7.9

AppDNA 7,9

À propos de cette version

La version 7.9 de XenApp et XenDesktop comprend les nouvelles versions des VDA Windows et les nouvelles versions de plusieurs composants principaux de XenApp et XenDesktop. Vous pouvez :

- **Installer ou mettre à niveau un site XenApp ou XenDesktop**

  Utilisez le fichier ISO de cette version pour installer ou mettre à niveau tous les composants principaux et les VDA. Cela vous permet d'utiliser les dernières fonctionnalités, décrites ci-dessous. Pour obtenir des instructions, veuillez consulter l'article Préparer l'installation ou Mettre un déploiement à niveau.

- **Installer ou mettre à niveau les VDA dans un site existant**

  Si vous disposez d'un déploiement XenApp ou XenDesktop, et que vous n'êtes pas prêt à mettre à niveau les composants principaux, vous pouvez toujours utiliser plusieurs des dernières fonctionnalités HDX en installant (ou en effectuant une mise à niveau vers) un nouveau VDA. C'est souvent utile lorsque vous voulez tester les améliorations dans un environnement de non production. Les fonctions nouvelles et mises à jour dans le VDA sont décrites ci-dessous. Pour de plus amples informations, consultez les articles suivants :

  Installer ou mettre à niveau les VDA à l'aide de l'interface graphique du programme d'installation VDA autonome

  Installer ou mettre à niveau les VDA à partir de l'interface de ligne de commande du programme d'installation VDA autonome

Les pages de téléchargement de XenApp et de XenDesktop pour cette version incluent également des versions mises à jour des logiciels suivants. Pour obtenir des informations sur les fonctionnalités et des instructions d'installation, consultez la documentation du composant.

StoreFront

Provisioning Services

AppDNA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenApp et XenDesktop 7.9

Cette version comprend les fonctionnalités nouvelles et améliorées suivantes.

Cette section résume les modifications apportées à l'installation et à la configuration de XenApp et XenDesktop dans cette version.

- Des données d'analyse sont collectées et stockées localement lorsque vous installez les composants.
- Si vous installez un VDA et que vous ne spécifiez aucune adresse de Controller, un rappel vous indique que le VDA ne peut pas s'enregistrer tant que des adresses de Controller ne sont pas fournies.
- Si vous spécifiez une ou plusieurs adresses de Controller lorsque vous installez un VDA, le programme d'installation vérifie si une connexion peut être établie entre le VDA et le Controller et rend compte du résultat.
- Les assistants d'installation ne permettent plus de s'inscrire au Programme d'amélioration de l'expérience utilisateur Citrix ; vous êtes inscrit d'office.
- Les assistants d'installation des composants principaux et des VDA permettent maintenant de s'inscrire au programme Call Home.
- Vous pouvez maintenant installer le Service d'authentification fédérée à partir de l'interface graphique du programme d'installation du produit complet.

Les modifications suivantes sont implémentées en vue d'une utilisation dans les versions futures.

- Microsoft SQL Express LocalDB 2014 est installé automatiquement lorsque vous installez un Delivery Controller. Ce logiciel n'est pas utilisé pour les bases de données de site, de journalisation et de surveillance. Aucune interaction avec cette base de données n'est requise de la part de l'administrateur. Pour empêcher son installation, installez le Controller à l'aide de la commande XenDesktopServerSetup.exe avec l'option /exclude "Microsoft SQL Server 2014 Express LocalD".
- Lorsque vous créez un site, si vous choisissez d'installer la base de données SQL Server Express en tant que base de données du site (ce qui est le paramètre par défaut), la machine sera redémarrée après l'installation du logiciel de base de données Ce redémarrage ne se produit pas si vous choisissez de ne pas installer le logiciel SQL Server Express en tant que base de données du site.

Lors d'une mise à niveau, le programme d'installation ne détecte plus ou ne met plus à niveau Citrix Receiver pour Windows Enterprise, Offline Plug-in pour Windows ou XenApp Plugin pour applications en streaming. Pour de plus amples informations, consultez l'article Mettre un déploiement à niveau

Lorsque vous créez une connexion à un hyperviseur ou à un fournisseur de service de cloud qui sera utilisée pour héberger des machines créées avec Machine Creation Services (MCS), vous pouvez maintenant spécifier les emplacements de stockage pour différents types de données :

- Données du système d'exploitation, ce qui comprend les images principales.
- Données temporaires, ce qui comprend toutes les données non persistantes écrites sur les machines provisionnées avec MCS, les fichiers de pages Windows, les données du profil utilisateur et les données qui sont synchronisées avec ShareFile. Ces données sont supprimées chaque fois qu'une machine redémarre.
- Données stockées sur les Personal vDisks.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

La mise à disposition d'espaces de stockage distincts pour chaque type de données peut réduire la charge et améliorer les performances IOPS (opérations E/S par seconde) sur chaque périphérique de stockage, ce qui permet d'utiliser les ressources disponibles de l'hôte de manière optimale. Cela permet également d'utiliser un stockage approprié pour les différents types de données : la persistance et la résilience sont des facteurs plus importants pour certaines données que pour d'autres.

Lorsque vous choisissez un stockage partagé par les hyperviseurs, vous pouvez choisir d'utiliser le stockage local pour les données temporaires de la machine. Lorsque vous créez un catalogue de machines qui utilise cette connexion, vous pouvez activer et configurer des valeurs autres que les valeurs par défaut pour la taille de disque et de mémoire pour chaque VM.

Lorsque vous choisissez un stockage local sur l'hyperviseur, vous pouvez choisir d'utiliser un stockage partagé pour les Personal vDisks (si vous utilisez des Personal vDisks).

Pour de plus amples informations, consultez les articles Connexions et ressources et Créer des catalogues de machines.

Si vous prévoyez d'utiliser Nutanix Acropolis pour héberger des VM provisionnées, installez le plug-in Nutanix sur les Delivery Controller pour activer la configuration des connexions Nutanix dans Studio.

Lorsque vous utilisez Studio pour créer une connexion à Nutanix et un catalogue de machines qui utilise une image Nutanix, les assistants vous permettent de spécifier des informations de configuration standard et spécifiques à Nutanix.

Pour plus d'informations, veuillez consulter l'article Environnements de virtualisation Nutanix.

Les groupes d'applications vous permettent de gérer des collections d'applications. Vous pouvez créer des groupes d'applications pour les applications qui sont partagées entre différents groupes de mise à disposition ou utilisées par un sous-ensemble d'utilisateurs au sein de groupes de mise à disposition.

Les groupes d'applications sont facultatifs ; ils offrent une alternative à l'ajout des mêmes applications sur plusieurs groupes de mise à disposition. Les groupes de mise à disposition peuvent être associés à plus d'un groupe d'applications, et un groupe d'applications peut être associé à plus d'un groupe de mise à disposition.

Pour de plus amples informations, consultez les articles Créer des groupes d'application et Gérer des groupes d'applications.

L'introduction de groupes d'applications affecte plusieurs autres zones de Studio. Par exemple, lorsque vous modifiez les propriétés d'une application, son appartenance à un groupe peut inclure des groupes de mise à disposition et/ou des groupes d'applications. Précédemment, une application devait être associée à au moins un groupe de mise à disposition ; maintenant, elle doit être associée à au moins un groupe de mise à disposition ou groupe d'applications. Pour de plus amples informations sur la gestion des applications, consultez la section Applications.

Le Service d'authentification fédérée de Citrix est un composant doté de privilèges conçu pour s'intégrer avec votre autorité de certification Microsoft. Il émet des certificats pour les utilisateurs de manière dynamique, ce qui leur permet de se connecter à un environnement Citrix comme s'ils avaient une carte à puce. Cela permet à StoreFront d'utiliser un éventail plus large d'options d'authentification, telles que les assertions SAML (Security Assertion Markup Language).

Pour plus d'informations, veuillez consulter l'article Service d'authentification fédérée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour de plus amples informations sur les fonctionnalités de télémétrie, y compris sur les modalités de participation, consultez l'article Citrix Insight Services.

Analyse du programme d'installation

Lorsque vous utilisez le programme d'installation du produit complet, des données analytiques sont collectées et stockées localement lorsque vous installez les composants XenApp et XenDesktop. Si vous rencontrez des problèmes durant l'installation, Citrix peut vous aider à charger des données à des fins d'analyse.

Call Home

La participation au programme Call Home (y compris le suivi permanent) est proposée dans le programme d'installation du produit complet. Vous pouvez également modifier votre inscription, créer des programmes de chargement personnalisés et charger manuellement les packages à l'aide d'applets de commande PowerShell.

Programme d'amélioration de l'expérience du client Citrix (CEIP)

La participation au programme d'amélioration de l'expérience du client Citrix est maintenant automatiquement activée lorsque vous créez un site. Vous n'avez pas besoin de vous inscrire dans l'assistant de création de site. Vous pouvez modifier votre participation après la création du site.

Director comprend les nouvelles fonctionnalités et fonctionnalités améliorées suivantes :

- **Améliorations apportées à la durée d'ouverture de session**. Lorsque vous sélectionnez un point de données dans le diagramme Performances d'ouverture de session, les données des info-bulles sont plus claires et plus faciles à interpréter. En outre, le nombre d'ouvertures de session est représenté par un graphique à barres (un graphique en courbes était précédemment utilisé). Le nombre d'ouvertures de session et la période de référence précédente peuvent être activés/désactivés sur le graphique. Un nouveau tableau affiche la durée de connexion par session utilisateur pour la période sélectionnée ; il est affiché en dessous du graphique Performances d'ouverture de session. L'administrateur peut rechercher des utilisateurs et choisir les colonnes et l'ordre de tri à afficher. Pour de plus amples informations, consultez la section Surveiller les déploiements.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Virtual Delivery Agent (VDA) 7.9

La version 7.9 du VDA pour OS de serveur et du VDA pour OS de bureau inclut les améliorations suivantes à l'impression, aux technologies HDX et à la prise en charge de plates-formes :

- **Équilibrage de charge pour le serveur d'impression universelle Citrix (UPS)**. Les administrateurs peuvent ajouter plusieurs serveurs d'impression dont la charge est équilibrée à l'aide de deux nouveaux paramètres de stratégie, Serveurs d'impression universelle d'équilibrage de la charge et Seuil au-delà duquel les serveurs d'impression universelle sont hors service. Ces dernières permettent aux sessions XenApp et XenDesktop sur un VDA de mapper des imprimantes de session vers différents serveurs d'impression au moment de l'ouverture de session. Pour de plus amples informations, consultez Paramètres de stratégie Serveur d'impression universelle et Équilibrer la charge des serveurs d'impression universelle dans l'article Gérer l'environnement d'impression.
- **Sélection de l'agrafage et de l'alimentation papier pour le pilote d'impression universelle Citrix XPS**. Le pilote d'imprimante universelle Citrix XPS prend en charge les fonctionnalités d'impression avancées, telles que l'agrafage et la sélection de l'alimentation papier. Pour de plus amples informations, consultez la section Provisionner des imprimantes.
- **Serveur d'impression universelle et CEIP**. L'inscription au programme CEIP est automatique lorsque vous installez le serveur d'impression universelle. Aucune donnée n'est collectée durant les sept premiers jours. Durant cette période, ou à n'importe quel moment dans le futur, vous pouvez désactiver la participation au programme CEIP pour UPS à l'aide d'un paramètre de registre. Pour de plus amples informations, consultez Provisionner des imprimantes et Citrix Insight Services.
- **Paramètres de stratégie de redirection des ports LPT et COM dans Studio**. Les paramètres de ports LPT et COM sont maintenant configurables dans Studio. Dans les versions 7.0 à 7.8 du VDA, ces paramètres étaient uniquement configurables à l'aide du Registre. Pour de plus amples informations, consultez la section Paramètres de stratégie de redirection de port et Paramètres de stratégie de bande passante.
- **Prise en charge de HDX 3D Pro étendue aux processeurs Intel avec Intel Iris Pro Graphics**. Permet d'utiliser les technologies d'accélération des graphiques HDX 3D Pro avec des processeurs Intel de 5ème et 6ème génération avec Intel Iris Pro Graphics. Cette version prend en charge plusieurs moniteurs (maximum de trois), l'occultation de la console, une résolution personnalisée et une haute fréquence d'images. Les programmes d'installation des VDA comprennent un nouveau fichier, GfxDisplayTool.exe, destiné à prendre en charge cette fonctionnalité. Pour de plus amples informations, consultez la section Accélération GPU pour OS de bureau Windows.
- **Prise en charge de Windows 10 dans le VDA HDX 3D Pro**. Cette version prend en charge Windows 10 dans la version HDX 3D Pro du VDA pour OS de bureau Windows.
- **Prise en charge du démarrage sécurisé pour Remote PC Access sur Windows 10**. Le Virtual Delivery Agent (VDA) pour OS de bureau prend en charge le démarrage sécurisé pour XenDesktop Remote PC Access sur Windows 10 et Windows 8.1.
- **Nouveau paramètre par défaut pour Utiliser codec vidéo pour la compression**. Utiliser un codec vidéo au choix est la nouvelle valeur par défaut du paramètre de stratégie pour les graphiques, Utiliser codec vidéo pour la compression. Cette modification a pour but de prendre en charge l'utilisation du mode de compatibilité Thinwire par le VDA. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie des graphiques.
- **Améliorations du VDA Linux pour Red Hat et SUSE.** Ajout de la prise en charge de VC CDM et CentOS (version 6.7, 7.2) avec de nombreuses améliorations pour résoudre les problèmes signalés par les clients. Pour de plus amples informations, consultez les articles Red Hat/CentOS et SUSE.
- **Redirection USB générique pour les périphériques de stockage de masse sur XenApp**. La redirection USB générique (USB Plug and Play) pour les périphériques de stockage de masse est maintenant prise en charge dans XenApp et XenDesktop. Les utilisateurs XenApp peuvent interagir avec les périphériques de stockage de masse dans une session XenApp comme si le périphérique de stockage était physiquement connecté. Pour utiliser cette fonctionnalité dans

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenApp, vous devez tout d'abord installer la mise à jour de sécurité Microsoft KB3155784. Dans cette version, cette fonctionnalité est désactivée par défaut pour XenApp et activée avec une clé de registre.

Pour activer les périphériques de stockage USB pour la redirection USB générique dans XenApp, créez un nom de valeur **UsbStorageEnabled** sous la clé **HKLM\SOFTWARE\Citrix\Portica\GenericUSB** et définissez sa valeur sur **1**.

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

StoreFront 3.6

StoreFront comprend les nouvelles fonctionnalités suivantes :

- **Équilibrage de la charge de batteries non identiques.** Dans les versions précédentes de StoreFront, lors de la création d'ensembles de batteries similaires à l'aide d'une configuration multisite, toutes les ressources devaient être publiées par chaque Delivery Controller pour que l'équilibrage de charge fonctionne. Le processus d'énumération des ressources par le biais duquel StoreFront obtenait une liste des ressources disponibles ne contactait qu'un seul Delivery Controller dans l'ensemble de batteries similaires. Dans StoreFront 3.6, certaines de vos ressources peuvent être communes à tous les Delivery Controller dans l'ensemble de batteries similaires et certaines peuvent être publiées uniquement par des Delivery Controller spécifiques. Vous pouvez maintenant configurer StoreFront pour énumérer les ressources provenant de tous ces Delivery Controller.
- **Domaine Active Directory non requis pour les déploiements sur un seul serveur.** Pour diverses raisons, il se peut que vous ne souhaitiez pas ajouter vos serveurs à un domaine Active Directory. Cette version évite l'obligation d'utiliser un domaine Active Directory pour les déploiements sur un seul serveur et vous permet d'installer StoreFront sur un serveur qui n'est pas joint à un domaine.
- **API REST StoreFront.** Nous avons créé une API REST StoreFront que NetScaler Gateway peut interroger pour déterminer la configuration de passerelle actuelle du cluster StoreFront. La console d'administration de NetScaler crée un fichier de configuration de passerelle combinant les paramètres de StoreFront et de NetScaler. Vous pouvez importer le fichier de configuration dans StoreFront à l'aide de la console de gestion StoreFront ou PowerShell.

Pour plus d'informations, veuillez consulter la documentation de StoreFront 3.6.

Provisioning Services 7.9

Provisioning Services comprend les nouvelles fonctionnalités suivantes :

- **Programme d'amélioration de l'expérience du client Citrix (CEIP)**. CEIP collecte des données de configuration et d'utilisation anonymes à partir de Provisioning Services et les envoie automatiquement à Citrix. Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de Provisioning Services.
- **Prise en charge de BDM pour UEFI via l'assistant d'installation de XenDesktop**. La prise en charge UEFI BDM inclut désormais l'intégration avec l'assistant d'installation de XenDesktop, qui vous permet de définir l'option de démarrage BDM sur le firmware UEFI cible. Avec cette prise en charge, PVS prend en charge le démarrage à partir de :
  - ISO

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- USB
- partitions de démarrage

- **Mise à jour d'une partition BDM**. Provisioning Services 7.9 ajoute une fonctionnalité qui vous permet d'effectuer la mise à niveau de la partition BDM en fonction de l'adresse IP du serveur dans le bootstrap du serveur PVS auquel vous êtes connecté. Une partition BDM peut être mise à niveau de l'une des trois manières suivantes :
  - par une collecte
  - par un groupe de machines sélectionnées
  - par une seul machine

Pour de plus amples informations, consultez la documentation Provisioning Services 7.9.

AppDNA 7,9

AppDNA comprend les nouvelles fonctionnalités suivantes :

- **Améliorations du workflow d'importation d'applications**. Les améliorations apportées au workflow d'importation d'applications ajoutent des informations sur l'état d'avancement du traitement côté serveur et la possibilité d'ajouter et d'annuler des importations.
- **Module Compliance Manager**. Le module Compliance Manager vous aide à déterminer si les applications que vous souhaitez déployer dans votre infrastructure informatique peuvent présenter des risques de sécurité. Ce module contient un jeu initial d'algorithmes et de rapports, qui sera étendu à l'avenir. Cette fonctionnalité est disponible à des fins d'évaluation dans cette version et ne doit pas être utilisée pour prendre des décisions sur le déploiement d'applications dans l'environnement de production.
- **Accès du client Web aux formulaires des attributs d'application**. Cette version ajoute un accès aux formulaires des attributs d'application à partir du client Web AppDNA. Depuis le client Web, sélectionnez Applications, sélectionnez une application, puis sélectionnez Properties.

Pour plus d'informations, veuillez consulter la documentation de AppDNA 7.9.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problèmes résolus

Jul 13, 2016

Les problèmes suivants ont été résolus depuis la version 7.8 :

AppDNA	Provisioning Services
Citrix Director	StoreFront
Stratégie Citrix	Serveur d'impression universelle
Citrix Studio	VDA pour OS de bureau
Controller	VDA pour OS de serveur
Redirection HDX MediaStream Flash	Composants Virtual Desktop : autres

- Lors de la tentative d'exportation d'une grande quantité de données au format PDF, la consommation d'UC et de mémoire du serveur peut s'approcher de 100 % et le message d'erreur suivant s'affiche :

  « L'action a échoué. La source de données ne répond pas ou a signalé une erreur. Consultez les journaux d'événements du serveur pour plus d'informations. »

  Cette correction ajoute une limite configurable pour l'exportation de format PDF, ce qui permet d'obtenir au moins une partie du rapport.

  Après l'installation de cette solution, vous devez configurer le fichier web.config dans le dossier wwwroot\Director comme suit :

  Ajoutez la ligne suivante à la section « appSettings » :

  La limite dépend de la capacité du serveur, par exemple la taille de la mémoire. La valeur spécifie le nombre de lignes dans le rapport PDF.

  [#LC4108]

- Les tentatives d'exportation de rapports dans tout format de fichier peuvent échouer avec le message d'erreur suivant :

  « L'action a échoué. Erreur serveur inattendue. Consultez les journaux d'événements du serveur pour plus d'informations. »

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LC4281]

- Si un serveur XenApp dispose de deux adresses IP et que le serveur DNS ne peut pas résoudre la première adresse IP, les tentatives de connexion à Citrix Director par un administrateur peuvent échouer avec le message d'erreur suivant :

  « Le système est actuellement indisponible. Réessayez ultérieurement ou contactez votre administrateur. »

  [#LC4411]

- Lors de la tentative d'exportation d'une grande quantité de données au format CSV, un délai d'expiration peut s'appliquer et l'exportation peut échouer avec le message d'erreur suivant :

  « L'action a échoué. La source de données ne répond pas ou a signalé une erreur. Consultez les journaux d'événements du serveur Director pour plus d'informations. »

  Cette solution vous permet de configurer la valeur du délai d'expiration pour l'exportation de données.

  Après l'installation de cette solution, vous devez configurer le fichier web.config dans le dossier wwwroot\Director comme suit :

  Ajoutez la ligne suivante à la section « appSettings » :
  où la valeur spécifie le délai d'expiration en secondes.

  [#LC4467]

- Lorsque vous sélectionnez un utilisateur pour afficher les informations de session de cet utilisateur, le nom de l'utilisateur qui s'affiche dans le coin supérieur gauche peut être « NULL ».

  [#LC4589]

- Si le nom de domaine NetBios contient une esperluette (&), l'observation à partir de la console Citrix Director peut échouer. Ce problème se produit car le caractère esperluette est réservé dans XML et peut provoquer l'échec de l'analyse pour l'ouverture de session.

  [#LC4633]

- Citrix Director avec authentification intégrée Windows (WIA) risque de ne pas fonctionner avec une configuration de délégation Kerberos contrainte.

  [#LC5196]

- Les administrateurs Citrix Director peuvent ne pas être en mesure d'afficher les stratégies Citrix dans les détails de la session.

  [#LC3941]

- Si vous essayez d'ajouter plusieurs imprimantes de session à un groupe de machines utilisateur sous la fenêtre « Attributions d'imprimantes », la barre de défilement ne se développe pas et ne s'affiche pas. Par conséquent, les tentatives d'ajout de plusieurs imprimantes de session à un groupe de machines utilisateur peuvent échouer.

  [#LC4658]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Les administrateurs Citrix Director peuvent ne pas être en mesure d'afficher les stratégies Citrix dans les détails de la session.

  [#LC4956]

- Lors de l'utilisation de Machine Creation Services pour cataloguer les VDA pour OS de serveur, le manque de disponibilité de stockage Personal vDisk peut définir de manière incorrecte la propriété « CleanOnBoot » du catalogue sur « False ». Par conséquent, la mise à jour du catalogue peut échouer.

  [#LC2959]

- La création de plusieurs applications dans plusieurs dossiers sous Groupes de mise à disposition dans Citrix Studio peut entraîner une structure de dossiers importante. La première fois que vous ouvrez Citrix Studio, lorsque vous cliquez sur des dossiers ou des applications, les dossiers ou applications peuvent être déplacés au lieu d'être sélectionnés. L'objet sélectionné est déplacé, ce qui entraîne un changement de la structure de dossier ou d'application.

  [#LC3705]

- Si des utilisateurs qui ne sont pas membres du groupe d'utilisateurs administrateurs de la base de données essaient d'ouvrir Citrix Studio, cela peut entraîner des erreurs d'autorisation sur le serveur SQL Server.

  [#LC4127]

- Les tentatives de provisionner des ressources supplémentaires à une offre multi-locataire dans App Orchestration 2.6 peuvent échouer si l'offre contient déjà plusieurs locataires.

  [#LC4170]

- Lorsqu'un Delivery Controller est déconnecté ou devient indisponible pour toute autre raison, Citrix Studio peut fonctionner lentement.

  [#LC4481]

- Les tentatives d'ajout de machines à un catalogue de machines à partir de Citrix Studio peuvent échouer et un message d'erreur s'afficher. Ce problème ne se produit pas lorsque vous ajoutez des machines à l'aide de l'assistant d'installation de XenDesktop.

  [#LC5030]

- Effectuer un redémarrage programmé d'un VDA pour OS de serveur qui est connecté à un hyperviseur VMware Vsphere peut entraîner l'arrêt du serveur qui reste alors à l'état arrêté.

  - Pour activer cette correction, définissez la clé de registre suivante :
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer\RebootSchedule
    Nom : ShutdownTimeoutRecovery
    Type : DWORD
    Valeur : 1

  - Pour désactiver cette correction, définissez la clé de registre suivante :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer\RebootSchedule
Nom : ShutdownTimeoutRecovery
Type : DWORD
Valeur : 0

Après la définition de la valeur, vous devez redémarrer le service Broker.

[#LC3807]

- Si des utilisateurs qui ne sont pas membres du groupe d'utilisateurs administrateurs de la base de données essaient d'ouvrir Citrix Studio, cela peut entraîner des erreurs d'autorisation sur le serveur SQL Server.

  [#LC4127]

- Lorsque le paramètre « SupportMultipleForest » est activé sur le Controller pour autoriser l'authentification NTLM, Linux VDA peut ne pas parvenir à effectuer le processus d'enregistrement car son nom de service principal (SPN) peut ne pas être défini dans le EndpointReference de Windows Communication Foundation (WCF).

  [#LC4235]

- Lorsqu'un Delivery Controller est déconnecté ou devient indisponible pour toute autre raison, Citrix Studio peut fonctionner lentement.

  [#LC4481]

- La réponse WaitForTask entraîne l'exception VimApi.MissingProperty qui n'autorise pas la mise à jour des catalogues de machines.

  [#LC4573]

- Lors de l'exécution de la commande PowerShell « Get-LogSummary » pour une plage de dates qui inclut le passage à l'heure d'été ou d'hiver, le message d'erreur suivant s'affiche :

  « Un élément avec la même clé a déjà été ajouté. »

  Le problème se produit lorsque l'heure d'été introduit des dates ou des heures locales ambigües. Des doublons d'entrées sont créés dans le HashMap et une exception se produit.

  Cette correction ajoute un message qui indique aux utilisateurs de diviser la période en fonction du moment où l'heure d'été commence ou se termine.

  [#LC4612]

- Les tentatives de mise à jour des catalogues de machines dans les environnements Amazon Web Services (AWS) peuvent échouer par intermittence. Pour activer le correctif, vous devez exécuter la commande « Set-ProvServiceConfigurationData –Name ImageManagementPrep_DoImagePreparation –Value $false » pour que la phase de préparation d'image soit ignorée lors de la mise à jour du catalogue de machines.

  [#LC4709]

- Les Controller peuvent parfois perdre leur connexion avec la base de données lorsqu'il existe un nombre élevé d'applications et de processus VDA en cours d'exécution. Lorsque cela se produit, les VDA restent à l'état d'initialisation

© 1999-2017 Citrix Systems, Inc. All rights reserved.

et les applications ne sont pas disponibles.

[#LC4848]

- Les tentatives d'ajout de machines à un catalogue de machines à partir de Citrix Studio peuvent échouer et un message d'erreur s'afficher. Ce problème ne se produit pas lorsque vous ajoutez des machines à l'aide de l'assistant d'installation de XenDesktop.

  [#LC5030]

- Cette correction résout un problème qui empêche le provisioning de Machine Creation Services de fonctionner dans Amazon Web Services lorsque le Controller est isolé des points de terminaison API publics d'Amazon par le biais d'un proxy Web.

  [#LC5109]

- Lorsque HDX MediaStream pour Flash est activé, l'ouverture et la fermeture de plusieurs onglets dans Internet Explorer avec du contenu Flash peut provoquer la fermeture inattendue d'Internet Explorer.

  [#LA3065]

- Lorsque HDX MediaStream pour Flash est activé, l'ouverture et la fermeture de plusieurs onglets dans Internet Explorer peut provoquer la fermeture inattendue d'Internet Explorer.

  [#LC1141]

- Lorsque la redirection Flash HDX MediaStream est activée, Microsoft Internet Explorer peut se fermer de manière inattendue lorsqu'il exécute pseudoserverinproc2.dll.

  Pour appliquer la modification, créez la clé de registre suivante :

  - *Sur les systèmes Windows 32 bits* :
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
    Nom : AllowCOMObjectTrack
    Type : DWORD
    Valeur : 0

  - *Sur les systèmes Windows 64 bits* :
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
    Nom : AllowCOMObjectTrack
    Type : DWORD
    Valeur : 0

  [#LC1885]

- Lorsque vous parcourez des sites Web avec la redirection Flash HDX MediaStream activée, la fonctionnalité de redirection Flash échoue si la valeur de registre HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs est définie sur « mfaphook.dll » ou « mfaphook64.dll » au lieu du chemin

© 1999-2017 Citrix Systems, Inc. All rights reserved.

d'accès complet vers « mfaphook.dll » ou « mfaphook64.dll ».

[#LC4388]

Redirection de

Port

Redirection de

- L'application NextGen peut parfois échouer lors de la tentative d'impression vers le Serveur d'impression universelle.

  [#LC4246]

Port

- L'impression par lots à l'aide de l'API d'impression Microsoft GDI peut échouer avec la dernière page qui ne s'imprime pas. Le message d'erreur suivant s'affiche :

  « Dispatch::CDriverTripSummary::PrintReport, Error Occured While Printing....Check Printer »

  [#LC3920]

- Cette correction introduit la prise en charge de Citrix UPS Print Driver Certification Tool pour le serveur d'impression universelle 7.6.300. Pour obtenir davantage d'informations, veuillez consulter l'article CTX142119 du centre de connaissances.

  [#LC4265]

Cartes à puce

Redirection HDX Mediastream Windows Media

Exceptions système

Impression

Expérience utilisateur

Session/Connexion

Interface utilisateur

Redirection HDX Mediastream Windows Media

- Si vous lisez un fichier .avi avec Windows Media Player dans une session ICA (ou session de bureau publié), puis démarrez la lecture d'un autre fichier .avi sans arrêter le premier, les trames vidéo peuvent ne pas être correctement dirigées vers la

© 1999-2017 Citrix Systems, Inc. All rights reserved.

machine utilisateur. Par conséquent, l'utilisation de l'UC du processus mmvdhost.exe peut être supérieure à la normale et la vidéo peut ne pas être restituée correctement sur la machine utilisateur.

[#LC4260]

- Lorsque la redirection HDX MediaStream Windows Media est activée, certains lecteurs tiers peuvent se fermer de manière inattendue lors de la restitution des fichiers sur un VDA qui est exécuté sur Windows 10.

  [#LC5110]

Impression

- Le service Spouleur d'impression Citrix peut s'arrêter de façon inattendue.

  [#LC4180]

- La stratégie « Créer automatiquement les imprimantes clientes » peut ne pas parvenir à définir correctement les imprimantes par défaut dans une application publiée et Microsoft XPS Document Writer est défini comme imprimante par défaut.

  [#LC4696]

Session/Connexion

- La stratégie Règles de redirection des périphériques USB clients peut ne pas s'appliquer. Le problème se produit lorsque le nombre de caractères saisis par l'utilisateur dans la stratégie dépasse 1002.

  [#LC1144]

- Lorsque plusieurs webcams ou périphériques de capture vidéo sont installés sur un point de terminaison, un seul de ces périphériques est mappé dans la session cliente. En outre, le périphérique est mappé en tant que caméra Web Citrix HDX, sans aucune indication sur le périphérique qui est mappé.

  [#LC1919]

- Certaines applications publiées tierces peuvent ne pas parvenir à démarrer sur des serveurs XenApp. Par conséquent, le processus wfshell.exe peut se fermer de manière inattendue. Lorsque cette erreur se produit, aucune indication que la session est en cours de démarrage ni aucun message d'erreur ne s'affiche sur la machine utilisateur.

  [#LC3766]

- Après libération de la barre d'outils Thomson Reuters Eikon dans une session comportant plusieurs moniteurs, l'espace occupé par la barre d'outils n'est pas récupéré par la session.

  Dans les configurations dans lesquelles le moniteur principal n'est pas situé dans le coin supérieur gauche du tableau, vous devez également installer le correctif #LC1599, qui est inclus dans Receiver pour Windows 4.4 et versions ultérieures.

  [#LC3773]

- Lorsque le paramètre de configuration App-V « EnablePublishingRefreshUI » est activé sur l'hôte de session et que la persistance de session est également activée, les tentatives de fermeture d'une application sur un appareil iOS peuvent entraîner une fenêtre noire qui reste sur l'écran de l'appareil.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LC3800]

- Si vous effectuez un arrêt ou forcez un ordinateur distant à redémarrer lors d'une session ICA, tous les pilotes audio peuvent être désactivés lors du redémarrage de l'ordinateur distant.

  [#LC4071]

- Après avoir installé la correction ICAWS760WX64032 et activé SSL, les tentatives de reconnexion à un VDA échouent par intermittence. Le problème se produit si le service ICA Citrix s'arrête de manière inattendue, ou ne répond plus en raison d'un échec d'écoute SSL.

  [#LC4438]

- Après une interruption du réseau entre le VDA et Citrix Receiver, vous ne pouvez pas lire de fichier .avi sur le lecteur Windows Media.

  [#LC4670]

- Les tentatives de reconnexion à une session VDA après une interruption du réseau peuvent échouer. Le problème se produit après la mise à niveau de VDA vers la version 7.8.

  [#LC5040]

- Cette correction résout un problème qui rompt la récupération de contenu côté client pour les applications basées sur DirectShow, ce qui empêche les vidéos d'être restituées.

  [#LC5098]

Cartes à puce

- Dans Microsoft Internet Explorer, l'interface utilisateur pour les ouvertures de session par carte à puce sur certains sites Web peut être parfois indisponible.

  [#LC3988]

- L'option Connexion ne s'affiche pas sur les VDA 7.6.300 et versions ultérieures exécutées sous Windows 10 Build 10586 et versions ultérieures. Par conséquent, les ouvertures de session par carte à puce ne sont pas disponibles.

  [#LC4778]

Exceptions système

- Le système d'exploitation rencontre une erreur sur ctxad.sys et un écran bleu s'affiche avec le code d'erreur 0xD1.

  [#LC4007]

- Lorsque vous exécutez de manière répétée un fichier .avi sur le Lecteur Windows Media, la consommation en mémoire du processus wfica32.exe peut continuer à augmenter jusqu'à ce que le processus se termine de manière inattendue.

  [#LC4335]

- Si la clé de registre HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\Thinwire\DisableOssForProcesses est définie, les tentatives de redémarrage du VDA et le lancement d'un bureau publié peuvent entraîner un écran bleu.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LC4597]

- Un processus d'application publiée peut se fermer de manière inattendue avec une exception « c000041d » sur MobileDesktopHook64.dll.

  [#LC4821]

Expérience utilisateur

- Lorsque vous passez d'un bureau publié tactile à un bureau publié standard, le bouton Démarrer :
  - Ne se met pas en surbrillance lorsque vous le survolez
  - Affiche le bureau local au lieu du bureau publié

  [#LC3466]

Interface utilisateur

- Après la publication d'applications transparentes, l'icône Citrix Receiver générique s'affiche à la place de l'icône de l'application publiée dans la barre des tâches.

  [#LC4757]

Redirection HDX Mediastream Windows Media	Cartes à puce
Impression	Exceptions système
Administration d'un serveur/d'un site	Expérience utilisateur
Session/Connexion	Interface utilisateur

Redirection HDX Mediastream Windows Media

- Si vous lisez un fichier .avi avec Windows Media Player dans une session ICA (ou session de bureau publié), puis démarrez la lecture d'un autre fichier .avi sans arrêter le premier, les trames vidéo peuvent ne pas être correctement dirigées vers la machine utilisateur. Par conséquent, l'utilisation de l'UC du processus mmvdhost.exe peut être supérieure à la normale et la vidéo peut ne pas être restituée correctement sur la machine utilisateur.

  [#LC4260]

- Lorsque la redirection HDX MediaStream Windows Media est activée, certains lecteurs tiers peuvent se fermer de manière inattendue lors de la restitution des fichiers sur un VDA qui est exécuté sur Windows 10.

  [#LC5110]

Impression

- Le service Spouleur d'impression Citrix peut s'arrêter de façon inattendue.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LC4180]

- Lorsque les noms d'imprimante d'ancienne génération sont activés, les imprimantes créées automatiquement peuvent ne pas être disponibles pour une utilisation dans une application publiée lorsque plusieurs sessions sont établies sur un serveur unique pour le même utilisateur.

  [#LC4517]

- La redirection d'imprimante peut échouer par intermittence.

  [#LC4584]

- La stratégie « Créer automatiquement les imprimantes clientes » peut ne pas parvenir à définir correctement les imprimantes par défaut dans une application publiée et Microsoft XPS Document Writer est défini comme imprimante par défaut.

  [#LC4696]

Administration d'un serveur/d'un site

- Si les utilisateurs basculent entre des sessions se trouvant sur des sous-réseaux différents, la liste des imprimantes contient des imprimantes provenant des deux sous-réseaux, plutôt que du sous-réseau auquel les utilisateurs sont actuellement connectés.

  [#LC2308]

- Plusieurs tentatives simultanées de connexion Bureau à distance (RDP) à un VDA depuis différentes machines utilisateur peuvent entraîner l'annulation de l'enregistrement du VDA.

  [#LC4014]

Session/Connexion

- Lorsque les stratégies Redirection audio du client ou Windows Media Redirection sont désactivées, l'icône de contrôle du volume (Haut-parleur) dans la zone de notification de la session de bureau publié peut afficher un état incorrect de l'audio.

  [#LC2538]

- Par défaut, les raccourcis d'accès rapide Windows pour « Bureau » et « Téléchargements » sont recréés dans %userprofile%\Links lors de l'ouverture de session, même si vous les avez supprimés manuellement auparavant. Ce comportement n'est pas conseillé dans tous les scénarios. Cette correction prend en charge la clé de registre suivante, qui si elle est définie sur 0 (zéro), empêche la recréation automatique de ces deux raccourcis :

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell
  Nom : CreateShortcutLinks
  Type : REG_DWORD
  Données : 0

  [#LC3274]

- Cette correction résout un problème qui entraîne l'altération occasionnelle des fichiers qui sont écrits sur des lecteurs clients mappés.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LC3684]

- Certaines applications publiées tierces peuvent ne pas parvenir à démarrer sur des serveurs XenApp. Par conséquent, le processus wfshell.exe peut se fermer de manière inattendue. Lorsque cette erreur se produit, aucune indication que la session est en cours de démarrage ni aucun message d'erreur ne s'affiche sur la machine utilisateur.

  [#LC3766]

- Après libération de la barre d'outils Thomson Reuters Eikon dans une session comportant plusieurs moniteurs, l'espace occupé par la barre d'outils n'est pas récupéré par la session.

  Dans les configurations dans lesquelles le moniteur principal n'est pas situé dans le coin supérieur gauche du tableau, vous devez également installer le correctif #LC1599, qui est inclus dans Receiver pour Windows 4.4 et versions ultérieures.

  [#LC3773]

- Lorsque Excelhook est activé, si plusieurs classeurs Excel sont ouverts et que vous les réduisez, vous risquez de ne pas pouvoir afficher les classeurs dans le focus.

  [#LC3799]

- Lorsque le paramètre de configuration App-V « EnablePublishingRefreshUI » est activé sur l'hôte de session et que la persistance de session est également activée, les tentatives de fermeture d'une application sur un appareil iOS peuvent entraîner une fenêtre noire qui reste sur l'écran de l'appareil.

  [#LC3800]

- Même lorsque la stratégie Redirection audio du client est activée, la lecture des fichiers audio (.wav) peut échouer. Le problème se produit dans les sessions où l'ID de session est réutilisé et la stratégie Redirection audio du client a été désactivée pour la session précédente.

  [#LC3882]

- Sur les systèmes avec correctif #LC2702 (inclus dans Hotfix Rollup Pack 6), les applications peuvent ne pas s'enregistrer sur les lecteurs clients mappés et générer des fichiers endommagés.

  [#LC3976]

- Avec des instances de Microsoft Internet Explorer, les tentatives de téléchargement d'un fichier à partir d'un site Web et son enregistrement sur un lecteur client mappé (« Enregistrer sous... ») peuvent échouer.

  [#LC4300]

- Le fichier icaendpoint.dll peut fermer le service audio Windows de manière inattendue.

  [#LC4356]

- Si un autre processus contient le même verrou que picadm.sys, les utilisateurs ne peuvent pas se déconnecter de la session et la session reste dans un état déconnecté.

  [#LC4415]

- Sur les systèmes avec correctif #LC0615 installé, les fermetures de session peuvent prendre plus de temps que prévu.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LC4674]

- Le lancement d'un processus avec WinDbg.exe peut échouer lorsque Streaming Profiler ou Offline Plug-in est installé. Le problème se produit car RadeAPHook effectue un hooking sur le paramètre pour HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ <*nomprocessus*> et HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<*nomprocessus*>.

  Pour appliquer la modification, créez la clé de registre suivante :

  - *Pour Windows 32 bits :*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\StreamingHook
    Nom : EnableReadImageFileExecOptionsExclusionList
    Type : Reg_SZ
    Valeur : < *Liste d'exécutables à exclure du hooking pour le paramètre Image File Execution Options, séparée par des virgules sans espaces. Par exemple, windbg.exe, application_1.exe.*>

  - *Pour Windows 64 bits pour les applications 32 bits :*
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StreamingHook
    Nom : EnableReadImageFileExecOptionsExclusionList
    Type : Reg_SZ
    Valeur : < *Liste d'exécutables à exclure du hooking pour le paramètre Image File Execution Options, séparée par des virgules sans espaces. Par exemple, windbg.exe,application_1.exe.*>

  [#LC4750]

- Cette correction résout un problème qui rompt la récupération de contenu côté client pour les applications basées sur DirectShow, ce qui empêche les vidéos d'être restituées.

  [#LC5098]

Cartes à puce

- Dans Microsoft Internet Explorer, l'interface utilisateur pour les ouvertures de session par carte à puce sur certains sites Web peut être parfois indisponible.

  [#LC3988]

- L'option Connexion ne s'affiche pas sur les VDA 7.6.300 et versions ultérieures exécutées sous Windows 10 Build 10586 et versions ultérieures. Par conséquent, les ouvertures de session par carte à puce ne sont pas disponibles.

  [#LC4778]

Exceptions système

- Lorsque vous exécutez de manière répétée un fichier .avi sur le Lecteur Windows Media, la consommation en mémoire du processus wfica32.exe peut continuer à augmenter jusqu'à ce que le processus se termine de manière inattendue.

  [#LC4335]

- Si la clé de registre HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\Thinwire\DisableOssForProcesses est définie, les

© 1999-2017 Citrix Systems, Inc. All rights reserved.

tentatives de redémarrage du VDA et le lancement d'un bureau publié peuvent entraîner un écran bleu.

[#LC4597]

- Un processus d'application publiée peut se fermer de manière inattendue avec une exception « c000041d » sur MobileDesktopHook64.dll.

  [#LC4821]

Expérience utilisateur

- Lorsque vous passez d'un bureau publié tactile à un bureau publié standard, le bouton Démarrer :
  - Ne se met pas en surbrillance lorsque vous le survolez
  - Affiche le bureau local au lieu du bureau publié

  [#LC3466]

- Lorsque vous tentez de déplacer une fenêtre Microsoft Excel dans une session transparente à deux moniteurs, la fenêtre peut rencontrer un délai lors de sa regénération dans le nouvel emplacement.

  [#LC4441]

Interface utilisateur

- Après la publication d'applications transparentes, l'icône Citrix Receiver générique s'affiche à la place de l'icône de l'application publiée dans la barre des tâches.

  [#LC4757]

Composants Virtual Desktop : autres

- Les applications qui utilisent l'intégration App-V peuvent ne pas parvenir à démarrer si le répertoire de travail configuré n'existe pas.

  [#LC4839]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problèmes connus

Aug 22, 2016

L'avertissement suivant s'applique à toute solution qui suggère de modifier une entrée de registre :

> **Avertissement** : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

XenApp et XenDesktop

La version 7.9 de XenApp et de XenDesktop contient les problèmes suivants :

- Lors de l'utilisation d'un périphérique de stockage de masse USB sur le point de terminaison, et que la stratégie de redirection USB est activée, un message d'erreur « Périphérique en cours d'utilisation » peut s'afficher lorsque vous essayez d'éjecter l'appareil.
  - Dans un environnement Remote PC Access, réinstallez le VDA à partir de la ligne de commande. Ceci empêchera l'erreur de se produire.
  - Dans les autres environnements, essayez l'une des solutions suivantes :
    - Utilisez la redirection de canal virtuel optimisé plutôt que générique. Cela permet au périphérique USB d'être éjecté sur la machine cliente. Consultez les articles CTX137939 et Redirection de périphérique USB.
    - Sur le périphérique USB, utilisez Windows pour désactiver le cache en écriture et optimiser le périphérique pour un retrait rapide. Reportez-vous à la documentation Microsoft pour plus d'informations. [#628442]
- Si SQL Server Express 2008 R2 est déjà installé sur le serveur sur lequel vous avez installé le Delivery Controller (sans aucun Service Pack), Studio échoue lors de la création du site. (Ce problème se produit même si vous n'utilisez pas cette base de données pour la base de données de site, de journalisation et de surveillance). Pour éviter ce problème, effectuez l'une des tâches suivantes avant d'installer le Controller : installez SQL Server Express 2008 R2 service pack ou désinstallez SQL Server Express 2008 R2 avant d'installer le Controller. [#632483]
- Si une machine utilisée pour la création d'un AppDisk ne dispose pas d'une liste ListOfDDCs actuelle (liste des Delivery Controller), toute demande de création d'un AppDisk initiée par un Controller risque de ne pas être traitée et d'échouer. La fonctionnalité de mise à jour automatique normale ne fonctionnera pas pour ces machines ; vous devez mettre à jour manuellement la liste ListOfDDCs au travers des paramètres de stratégie ou du registre (consultez l'article Delivery Controller). [#633341]
- Lorsque vous créez un site, si vous choisissez d'installer la base de données SQL Server Express en tant que base de données du site (ce qui est le paramètre par défaut), la machine sera redémarrée après l'installation du logiciel de base de données Ce redémarrage ne se produit pas si vous choisissez de ne pas installer le logiciel SQL Server Express en tant que base de données du site. [#634316]
- L'installation d'un VDA sur un OS de serveur Windows peut échouer si les dernières mises à jour Windows ne sont pas installées sur la machine. (Les mises à jour Windows Server 2008 R2 doivent inclure celles comprises dans le correctif KB2685811 ; ces mises à jour sont déjà installées sur les systèmes d'exploitation plus récents pris en charge). [#635456]
- Si vous sélectionnez Configuration > Gestion des licences dans le panneau de navigation de Studio, puis cliquez sur **Ouvrir une session** dans le panneau Actions, le composant logiciel enfichable de Studio s'arrête si vous n'êtes pas autorisé à utiliser le serveur de licences Citrix. Pour récupérer, redémarrez Studio. (Vous pouvez gérer le serveur de licences directement à partir de la console License Administration Console) [#640925]
- Une fois que vous avez configuré les serveurs App-V dans Studio, la console Microsoft Management Console (MMC) peut se bloquer lorsque vous fermez Studio. [#652949]
- Si vous utilisez un stockage local pour votre cache de système d'exploitation et votre cache en écriture, assurez-vous que le même stockage est utilisé pour les deux. Si la liste de stockage pour le cache en écriture contient un stockage qui n'est pas disponible pour le stockage de système d'exploitation, l'erreur « Unable to find file [Datastore] » peut s'afficher lors de la création d'un catalogue. [#637430]
- Lors de la création de AppDisks à l'aide d'une machine Windows 10, le processus de scellement peut échouer. Pour contourner le problème, supprimez le AppDisk (à l'aide de l'applet de commande PowerShell Remove-AppLibAppDisk), puis recréez le AppDisk. [#633998]
- La mise à niveau de StoreFront à l'aide du programme d'installation du produit entier XenApp et XenDesktop peut échouer. Pour éviter que ce problème se reproduise, redémarrez le serveur StoreFront pour supprimer les verrous de fichier, puis exécutez le programme d'installation sans ouvrir de console de gestion Citrix ou de sessions PowerShell. [#641242]
- Après la mise à niveau de la version 7.5 (ou 7.6 s'il s'agit déjà d'une mise à niveau de la version 7.5), le démarrage de Studio ou du kit de développement de haut niveau peut échouer. Solution : Effectuez une installation de réparation du MSI Studio ([XDInstallerRoot]\x64\DesktopStudio\DesktopStudio_x64.msi) ou du MSI SDK haut niveau ([XDInstallerRoot]\x64\Citrix Desktop Delivery Controller\XDPoshSnapin.msi). [#617897]
- Dans un site de grande taille, certains des problèmes de performances dans Studio et Director peuvent être causés par des statistiques SQL obsolètes et des index fragmentés. Pour éviter ce problème, l'administrateur de votre base de données doit exécuter un plan de maintenance SQL Server durant les heures creuses ; ce plan doit inclure la reconstruction des index et des statistiques sur les bases de données du site, de contrôle et de journalisation de la configuration.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour de plus amples informations, consultez la documentation relative à votre plan de maintenance pour votre version de SQL Server. [#641889]

- Les valeurs de durée d'ouverture de session pour un groupe de mise à disposition supprimé s'affichent comme n/a dans le graphique et la ligne n'est pas affichée dans le tableau si le groupe de mise à disposition est supprimé et que ce groupe de mise à disposition est sélectionné. [#615106]
- Le tri par Durée d'utilisation ou Utilisateurs distincts sous **Tendances** > **Gestion de la capacité** > **Utilisation d'applications hébergées** entraîne une erreur. Pour contourner ce problème, redémarrez Director. [#640508]
- L'utilisation de la roulette de la souris pour cliquer à l'intérieur d'une session Framehawk peut ne pas donner les résultats attendus. [#625408]
- Après la déconnexion d'un VDA HDX 3D Pro dans un déploiement Remote PC Access qui utilise des processeurs Intel avec Intel Iris Pro Graphics, la luminosité de l'écran de la console est réduite. Il s'agit d'un problème de tiers. La solution consiste à redémarrer la machine Remote PC Access pour restaurer la luminosité de l'écran. [#633101]
- Dans un déploiement Remote PC Access Windows 10 (32 bits uniquement) avec HDX 3D Pro, la machine Remote PC Access ne se lance plus après l'installation d'un pilote Intel version 20.19.15.9999. Il s'agit d'un problème de tiers. La solution consiste à utiliser les pilotes de Windows Update. [#637294] **Remarque** : pour Remote PC Access, le VDA est généralement configuré à l'aide de l'option VDA standard. Pour de plus amples informations sur la configuration du VDA en mode standard ou HDX 3D Pro, consultez l'article Préparer l'installation.
- XenApp et XenDesktop interrompt l'installation après l'installation de .NET 4.5.2. Ce problème a été observé sur Windows Server 2008 R2. La solution consiste à installer manuellement .NET 4.5.2, avant de recommencer l'installation. [633721]
- Lorsque vous déconnectez un périphérique d'interface utilisateur (HID) USB comme un touchpad durant une session Remote PC à laquelle plusieurs périphériques de ce type sont attachés (à l'exception des claviers et de la souris), puis que vous le reconnectez après la déconnexion et reconnexion à la session, le HID USB reste désactivé. Pour contourner ce problème, activez manuellement le périphérique HID dans Device Manager. [#638766]
- Une altération graphique peut se produire lors du déplacement d'une vidéo sur plusieurs moniteurs (observé dans les sessions à moniteurs multiples avec trois moniteurs ou plus) en mode de compatibilité Thinwire. [#640437]
- Si un utilisateur arrête Surface Pro, lorsqu'il est rallumé, les connexions HDX utilisant Remote PC Access peuvent ne pas fonctionner. La solution consiste à redémarrer la machine. [#634830]
- Lors d'une connexion à une machine Surface Pro avec Windows 8.1, la session peut sembler être lente pendant environ une minute lorsque le démarrage sécurisé est activé. [#634382]
- Si vous activez Remote PC Access, lorsque vous installez un VDA à l'aide du programme d'installation du produit entier avec interface graphique, des composants supplémentaires (Machine Creation Services et Profile Management) sont installés [#637741]. Dans cette version, utilisez uniquement la ligne de commande pour les déploiements Remote PC Access et ne changez pas l'ordre de syntaxe pour /components et /remotepc. Par exemple :

```
VDAWorkstationSetup.exe /components vda /controllers "example.delivery.controller.net" /remotepc /EXCLUDE "AppDisks VDA Plug-in" /enable_hdx_ports /noreboot /quiet
```

Si l'option /remotepc est utilisée avant /composants, l'option /remotepc est ignorée. Pour de plus amples informations sur les options de ligne de commande, consultez la section Installer à l'aide de la ligne de commande.

Vous pouvez accéder à une liste des problèmes identifiés lors de l'utilisation de cette version de XenApp et XenDesktop avec Windows Server 2016 Tech Preview dans le forum Windows Server 2016 Tech Preview (connexion au compte Citrix requise).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Autres composants

Des composants disponibles séparément sur les pages de téléchargement de XenApp et XenDesktop présentent les problèmes connus suivants.

- L'installation des composants du serveur d'enregistrement de session échoue avec les codes d'erreur 2503 et 2502. Résolution : vérifiez la liste de contrôle d'accès (ACL) du dossier C:\windows\Temp pour vous assurer que **Utilisateurs et groupes locaux > Groupes > Utilisateurs** ont un accès en écriture à ce dossier. Si ce n'est pas le cas, ajoutez manuellement les autorisations en écriture. [#611487]
- Étant donné que l'enregistrement de session ne prend pas en charge le mode d'affichage Framehawk, les sessions en mode d'affichage Framehawk ne peuvent pas être enregistrées et lues correctement. Les sessions enregistrées dans ce mode peuvent ne pas contenir les activités de session. [#622085]
- Vous ne pouvez pas enregistrer les sessions de bureau Windows 7 correctement lorsque **Mode graphique d'ancienne génération** est activé par la stratégie de site XenDesktop et **Disk-based Caching** est activé par la stratégie Citrix Receiver pour Windows. Ces enregistrements affichent un écran noir. Solution : désactivez **Disk-based Caching** en déployant avec un objet de stratégie de groupe vers les machines sur lesquelles vous avez installé Citrix Receiver pour Windows. Pour de plus amples informations sur la désactivation de **Disk-based Caching**, consultez http://support.citrix.com/article/CTX123169 et http://docs.citrix.com/en-us/receiver/windows/4-4/ica-overview-receiver-config/ica-import-icaclient-template-v2.html. [#618237]
- Le paramètre de reprise ne s'applique pas aux sessions de bureau VDI pour XenDesktop 7.8, XenDesktop 7.9 et l'agent d'enregistrement de session. Dans ce cas, chaque fichier d'enregistrement a une limite de taille maximale de 1 Go et les activités ne sont pas enregistrées une fois que cette limite est atteinte. [#584890]
- Lorsque Machine Creation Services (MCS) ou Provisioning Services crée plusieurs VDA avec une image principale configurée et que Microsoft Message Queuing (MSMQ) est installé, ces VDA disposent de la même QMId. Cela peut entraîner différents problèmes, tels que :
  - Les sessions peuvent ne pas être enregistrées, même si l'accord d'enregistrement est accepté.
  - Le signal de fermeture de session peut ne pas être reçu par le serveur d'enregistrement de session, par conséquent l'état de la session est toujours Actif. [#528678]

    La solution pour créer une QMId unique et persistante pour chaque VDA varie selon les méthodes de déploiement.

    Aucune action supplémentaire n'est requise si des VDA avec OS de bureau sur lesquels un agent d'enregistrement de session est installé seront créés avec PVS 7.7 ou version ultérieure en mode de bureau statique ; par exemple, configurés pour rendre toutes les modifications persistantes avec un Personal vDisk ou disque local distinct du VDA.

    Pour les VDA avec OS de serveur créés par MCS ou PVS ou les VDA avec OS de bureau dédiés créés par MCS en mode de bureau statique, par exemple, configurés pour rendre toutes les modifications persistantes avec un Personal vDisk ou disque local distinct du VDA, utilisez un script (GenQMID.ps1) pour modifier la QMId au démarrage du système.

    Pour les VDA avec OS de bureau créés par MCS ou PVS et configurés pour supprimer toutes les modifications lorsque l'utilisateur ferme sa session, utilisez un script (GenRandomQMID.ps1) pour modifier la QMId au démarrage du système. Modifiez la stratégie de gestion de l'alimentation pour vous assurer qu'un nombre

© 1999-2017 Citrix Systems, Inc. All rights reserved.

suffisant de VDA sont en cours d'exécution avant les tentatives de connexion des utilisateurs.

Pour utiliser le script, procédez comme suit :

1. Vérifiez que la stratégie d'exécution est définie sur RemoteSigned ou Unrestricted dans PowerShell.

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

2. Créez une tâche planifiée et définissez le déclencheur sur Au démarrage du système et exécutez le compte SYSTEM sur la machine avec l'image principale Provisioning Services ou MCS.

3. Ajoutez la commande en tant que tâche de démarrage.

   ```
   powershell.exe -file C:\GenQMID.ps1
   SOIT
   powershell .exe -file C:\GenRandomQMID.ps1
   ```

Résumé du GenQMID.ps1 :

1. Générez la QMId en fonction de la valeur de hachage de l'identificateur unique universel de la machine.
2. Arrêtez les services associés, notamment CitrixSmAudAgent et MSMQ.
3. Démarrez les services arrêtés précédemment pour appliquer les modifications apportées à la QMId.

```
function ConvertHexStringToByte($theString)

{

    $bytes = New-Object Byte[] ($theString.Length / 2)

    for ($i = 0; $i -lt $theString.Length; $i += 2) {

        $bytes[$i / 2] = [System.Convert]::ToByte($theString.Substring($i, 2), 16)

    }

    return $bytes

}


Try {

    # Get UUID of machine

    $strUUID = (Get-WmiObject -Class Win32_ComputerSystemProduct | Select-Object -Property UUID).UUID
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    # Remove "-"
    $strUUID = $strUUID.ToString().Replace("-", "")

    # Convert string to bytes
    $UUID = ConvertHexStringToByte($strUUID)

    # Set UUID as QMId
    $new_QMID = $UUID
}
Catch {
    # IF exception occurred, just use MD5 digest of FQDN as QMID

    # Get FQDN
    $fqdn = [System.Net.Dns]::GetHostByName(($env:computerName)).HostName

    # Calculate MD5 hash of FQDN
    $md5 = new-object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider

    # Set md5 digest as QMID
    $utf8 = new-object -TypeName System.Text.UTF8Encoding
    $new_QMID = $md5.ComputeHash($utf8.GetBytes($fqdn))
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
# Write new_QMID into registry

Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\MachineCache -Name "QMId" -Value $new_QMID


# Restart MSMQ to adopt new QMId


# Get dependent services

$depServices = Get-Service -name MSMQ -dependentservices | Select -Property Name

Restart-Service -force MSMQ


# Start dependent services

if ($depServices -ne $null) {

    foreach ($depService in $depServices) {

        $startMode = Get-WmiObject win32_service -filter "NAME = '$($depService.Name)'" | Select -Property StartMode

        if ($startMode.StartMode -eq "Auto") {

            Start-Service $depService.Name

        }

    }

}
```

Résumé du GenRandomQMID.ps1 :

1. Supprimez la QMId actuelle du registre.
2. Ajoutez SysPrep = 1 dans HKLM\Software\Microsoft\MSMQ\Parameters.
3. Arrêtez les services associés, notamment CitrixSmAudAgent et MSMQ.
4. Démarrez les services arrêtés précédemment pour générer une QMId aléatoire.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
# Remove old QMId from registry and set SysPrep flag for MSMQ

Remove-Itemproperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\MachineCache -Name QMId -Force

Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -Name "SysPrep" -Type DWord -Value 1

# Get dependent services

$depServices = Get-Service -name MSMQ -dependentservices | Select -Property Name

# Restart MSMQ to get a new QMId

Restart-Service -force MSMQ

# Start dependent services

if ($depServices -ne $null) {

    foreach ($depService in $depServices) {

        $startMode = Get-WmiObject win32_service -filter "NAME = '$($depService.Name)'" | Select -Property StartMode

        if ($startMode.StartMode -eq "Auto") {

            Start-Service $depService.Name

        }

}

}
```

- Lors de l'enregistrement d'une session avec une résolution supérieure ou égale à 4 096 x 4 096, des fragments peuvent apparaître dans l'apparence de l'enregistrement. [#524973]
- Lorsque vous modifiez votre type de licence XenApp ou XenDesktop, cette modification ne prend pas effet immédiatement pour l'enregistrement de session. Solution : redémarrez la machine VDA. [#532393]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Limitation de l'enregistrement de session concernant la prise en charge des sessions d'application pré-lancées [#561109]
  - Problème :
    - Si la stratégie active tente d'effectuer une correspondance avec le nom de l'application, la correspondance avec l'application lancée dans la session de pré-lancement n'est pas établie, ce qui entraîne l'échec de l'enregistrement de la session.
    - Si la stratégie active enregistre chaque application, lorsque l'utilisateur ouvre la session Receiver pour Windows (au même moment où la session de pré-lancement est ouverte), une notification d'enregistrement apparaît et la session vide et toute application lancée ultérieurement dans cette session sont enregistrées.
  - Solution :
    - Publiez les applications dans des groupes de mise à disposition séparés en fonction de leur stratégie d'enregistrement. N'utilisez pas le nom de l'application en tant que condition d'enregistrement. Ceci permet de vous assurer que les sessions de pré-lancement seront enregistrées. Toutefois, les notifications continueront à s'afficher.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Fonctionnalités absentes de cette version

Jul 07, 2016

Conseil : si votre expérience la plus récente est avec XenApp 6.5 (ou les versions antérieures de XenApp), nous vous conseillons également de consulter les différences en termes d'architecture, de terminologie et de composants décrites ici.

Les fonctionnalités suivantes ne sont actuellement pas fournies ou ne sont plus prises en charge.

- **Démarrer un bureau tactile :** ce paramètre a été désactivé pour les machines Windows 10. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie Expérience mobile.
- **Cryptage ICA Sécurisé en-dessous de 128 bits** : dans les versions antérieures à 7.x, Secure ICA pouvait crypter les connexions clientes pour le cryptage de base, 40 bits, 56 bits et 128 bits. Dans les versions 7.x, le cryptage Secure ICA est uniquement disponible pour le cryptage 128 bits.
- **Impression d'ancienne génération** : les fonctionnalités d'impression suivantes ne sont plus prises en charge dans les versions 7.x :
  - Rétrocompatibilité pour les clients DOS et les imprimantes 16 bits, y compris le nom d'imprimante cliente d'ancienne génération.
  - Prise en charge des imprimantes connectées aux systèmes d'exploitation Windows 95 et Windows NT, y compris les propriétés d'imprimante étendues et Win32FavorRetainedSetting.
  - Possibilité d'activer ou désactiver les imprimantes conservées et restaurées automatiquement.
  - DefaultPrnFlag, un paramètre de registre pour les serveurs qui est utilisé pour activer ou désactiver des imprimantes conservées et restaurées automatiquement, qui sont stockées dans les profils utilisateur sur le serveur.
- **Secure Gateway** : dans les versions antérieures à 7.x, Secure Gateway était une option pour sécuriser les connexions entre le serveur et les machines utilisateur. NetScaler Gateway est l'option de remplacement pour sécuriser les connexions externes.
- **Observation des utilisateurs** : dans les versions antérieures à la version 7.x, les administrateurs définissaient des stratégies pour contrôler l'observation utilisateur-utilisateur. Dans les versions 7.x, l'observation des utilisateurs finaux est une fonctionnalité intégrée du composant Director, qui utilise Microsoft Remote Assistance pour autoriser les administrateurs à observer et résoudre les problèmes de mise à disposition des applications transparentes et des bureaux virtuels.
- **Gestion de la capacité et de la consommation** : dans les versions antérieures à la version 7.x, la fonctionnalité de gestion de la capacité et de la consommation pouvait être utilisée pour vous aider à réduire la consommation d'énergie et gérer la capacité du serveur. Microsoft Configuration Manager est l'outil de remplacement de cette fonction.
- **Redirection Flash v1** : les clients qui ne prennent pas en charge la redirection Flash de deuxième génération (y compris les versions Citrix Receiver pour Windows antérieures à la version 3.0, Citrix Receiver pour Linux antérieures à la version 11.100 et Citrix Online Plug-in 12.1) retourneront à la restitution côté serveur pour les fonctionnalités de redirection Flash d'ancienne génération. Les VDA inclus avec les versions 7.x prennent en charge les fonctionnalités de redirection Flash de deuxième génération.
- **Écho local du texte** : cette fonctionnalité était utilisée avec une version antérieure des technologies d'application Windows pour accélérer l'affichage du texte saisi sur les machines utilisateur sur des connexions à latence élevée. Elle n'est pas incluse dans les versions 7.x à cause des améliorations apportées au sous-système graphique et SuperCodec HDX.
- **Smart Auditor** : dans les versions antérieures à la version 7.x, Smart Auditor vous permettait d'enregistrer les activités à l'écran de la session de l'utilisateur. À compter de 7.6 Feature Pack 1, cette fonctionnalité est fournie par l'enregistrement de session.
- **Single Sign-On** : cette fonctionnalité, qui fournit le mot de passe de sécurité, n'est pas pris en charge pour les

© 1999-2017 Citrix Systems, Inc. All rights reserved.

environnements Windows 8 et Windows Server 2012. Elle est toujours prise en charge pour les environnements Windows 2008 R2 et Windows 7, mais n'est pas incluse dans les versions 7.x. Vous pouvez la rechercher sur le site Web de téléchargement Citrix : http://citrix.com/downloads.

- **Prise en charge de base de données Oracle** : les versions 7.x nécessitent une base de données SQL Server.
- **Suivi et rétablissement de l'état (HMR)** : dans les versions antérieures à la version 7.x, HMR peut effectuer des tests sur les serveurs d'une batterie de serveurs afin de contrôler leur état et détecter tout problème éventuel. Dans les versions 7.x, Director offre une vue centralisée de l'intégrité du système en présentant l'analyse et les alertes de l'ensemble de l'infrastructure à partir de la console Director.
- **Fichiers ICA personnalisés** : les fichiers ICA personnalisés étaient utilisés pour activer les connexions directes à partir des machines utilisateur (avec le fichier ICA) pour une machine spécifique. Dans les versions 7.x, cette fonctionnalité est désactivée par défaut, mais peut être activée pour l'utilisation normale à l'aide d'un groupe local ou peut être utilisée en mode haute disponibilité si le Controller devient non disponible.
- **Pack d'administration de System Center Operations Manager (SCOM) 2007** : le pack d'administration, qui surveille l'activité des batteries de serveurs à l'aide de SCOM, ne prend pas en charge les versions 7.x.
- **Fonction CNAME** : la fonction CNAME était activée par défaut dans les versions antérieures à 7.x. Les déploiements qui dépendent des enregistrements CNAME pour le nouveau routage FQDN et l'utilisation de noms NETBIOS peut échouer. Dans les versions 7.x, la mise à jour automatique de Delivery Controller est la fonctionnalité de remplacement qui met à jour la liste de Controller dynamiquement et notifie automatiquement les VDA lorsque les Controller sont ajoutés et supprimés du site. La fonctionnalité de mise à jour automatique du Controller est activée par défaut dans les stratégies Citrix, mais peut être désactivé en créant une stratégie. Sinon, vous pouvez activer à nouveau la fonction CNAME dans le Registre pour continuer avec votre déploiement existant et autoriser le nouveau routage FQDN et l'utilisation de noms NETBIOS. Pour obtenir davantage d'informations, veuillez consulter la section CTX137960.
- **Assistant de déploiement rapide** : dans les versions de Studio antérieures à la version 7.x, cette option permettait le déploiement rapide d'un déploiement XenDesktop complètement installé. La nouvelle installation simplifiée et workflow de configuration dans les versions 7.x élimine la nécessité d'utiliser l'option de l'assistant de déploiement rapide.
- **Fichier de configuration et fichier de script PowerShell pour l'administration automatique du service Remote PC** : Remote PC est désormais intégré dans Studio et le Controller.
- **Workflow Studio** : dans les versions antérieures à la version 7.x, Workflow Studio était l'interface graphique pour la composition du flux de travail pour XenDesktop. La fonctionnalité n'est pas prise en charge dans les versions 7.x.
- **Nombre de couleurs**: dans les versions de Studio antérieures à 7.6, vous spécifiez le nombre de couleurs dans les paramètres utilisateur d'un groupe de mise à disposition. À compter de la version 7.6, le nombre de couleurs pour le groupe de mise à disposition peut être défini à l'aide de l'applet de commande PowerShell New-BrokerDesktopGroup ou Set-BrokerDesktopGroup.
- **Lancement de programmes non publiés lors de la connexion du client** : dans les versions antérieures à 7.x, ce paramètre de stratégie Citrix spécifiait si les applications initiales ou les applications publiées devaient être lancées via ICA ou RDP sur le serveur. Dans les versions 7.x, ce paramètre spécifie uniquement si les applications initiales ou publiées doivent être lancées via RDP sur le serveur.
- **Démarrages de bureaux** : dans les versions antérieures à la version 7.x, ce paramètre de stratégie Citrix spécifiait si les utilisateurs non administrateurs pouvaient se connecter à une session de bureau. Dans les versions 7.x, les utilisateurs qui ne sont pas des administrateurs doivent appartenir au groupe d'utilisateurs DirectAccess d'une machine VDA pour se connecter à des sessions sur ce VDA. Le paramètre **Démarrages de bureaux** permet aux utilisateurs qui ne sont pas des administrateurs d'un groupe d'utilisateurs DirectAccess dans un VDA de se connecter au VDA à l'aide d'une connexion ICA. Le paramètre **Démarrages de bureaux** n'a aucun effet sur les connexions RDP ; les utilisateurs d'un groupe d'utilisateurs DirectAccess dans un VDA peuvent se connecter au VDA à l'aide d'une connexion Bureau à distance que ce paramètre soit activé ou non.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Mappage des ports COM** : le mappage de port COM permet ou empêche l'accès aux ports COM sur la machine utilisateur. Le mappage de port COM était précédemment activé par défaut. Dans les versions 7.x de XenDesktop et XenApp, le mappage des ports COM est désactivé par défaut. Pour de plus amples informations, consultez la section Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.
- **Mappage de port LPT** : le mappage de port LPT contrôle l'accès aux applications d'ancienne génération sur des ports LPT. Le mappage de port LPT était précédemment activé par défaut. Dans les versions 7.x, le mappage des ports LPT est désactivé par défaut.
- **Codec audio PCM** : seuls les clients HTML5 prennent en charge le codec audio PCM dans les versions 7.x.
- **Prise en charge de Microsoft ActiveSync**
- **Prise en charge de proxy pour les versions plus anciennes** : cela inclut :
  - Microsoft Internet Security et Acceleration (ISA) 2006 (Windows Server 2003)
  - Oracle iPlanet Proxy Server 4.0.14 (Windows Server 2003)
  - Serveur proxy Squid 3.1.14 (serveur Linux Ubuntu 11.10)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Avis de tiers

Jul 07, 2016

Cette version de XenApp et XenDesktop peut inclure un logiciel tiers distribué sous une licence selon les conditions définies dans les documents suivants :

- XenApp 7.9 et XenDesktop 7.9 - Avis de tiers
- Supplément à la documentation FLEXnet Publisher : Logiciels tiers et open source utilisés dans FlexNet Publisher 11.13.1
- Linux Virtual Desktop version 1.2 - Avis de tiers

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration système requise

Aug 22, 2016

Dans cet article :

- Delivery Controller
- Bases de données
- Citrix Studio
- Citrix Director
- Virtual Delivery Agent (VDA) pour système d'exploitation de bureau
- Virtual Delivery Agent (VDA) pour système d'exploitation de serveur
- Hôtes et ressources de virtualisation
- Niveaux fonctionnels Active Directory
- HDX
- Enregistrement de session
- Serveur d'impression universelle
- Autre

Introduction

La configuration système requise détaillée dans ce document est valide lors de la publication de cette version du produit ; des mises à jour sont apportées régulièrement. La configuration système requise des composants non couverts dans ce document (telles que StoreFront, systèmes hôte, Citrix Receiver et plug-ins, et Provisioning Services) est décrite dans leur documentation respective.

Important : consultez la section Préparer l'installation avant de procéder à l'installation.

Sauf spécification contraire, le programme d'installation du composant déploie automatiquement les composants logiciels requis (tels que les packs .NET et C++) si les versions requises ne sont pas détectées sur la machine. Le support d'installation Citrix contient également certains de ces logiciels requis.

Le support d'installation contient plusieurs composants tiers. Avant d'utiliser le logiciel Citrix, recherchez des mises à jour de sécurité à partir des composants tiers et installez-les.

Les valeurs d'espace disque sont uniquement des estimations, et existent en plus de l'espace nécessaire pour l'image du produit, du système d'exploitation et d'autres logiciels.

Si vous installez tous les composants principaux (Controller avec SQL Server Express, Studio, Director, StoreFront et le système de licences) sur un serveur unique, vous devez disposer d'un minimum de 4 Go de RAM pour évaluer le produit ; il est recommandé de disposer d'une plus grande quantité de RAM lors de l'exécution d'un environnement pour les utilisateurs. Les performances peuvent varier en fonction de votre configuration, y compris le nombre d'utilisateurs, d'applications, de bureaux et d'autres facteurs.

Pour obtenir davantage d'informations sur la globalisation, veuillez consulter la section CTX119253.

Delivery Controller

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Systèmes d'exploitation pris en charge :

- Technical Preview actuelle de Windows Server 2016 : la prise en charge de ce système d'exploitation dans cette version est disponible à des fins d'évaluation uniquement et n'est pas destinée à un environnement de production.
- Windows Server 2012 R2, édition Standard et Datacenter.
- Windows Server 2012, édition Standard et Datacenter.
- Windows Server 2008 R2 SP1, éditions Standard, Entreprise et Datacenter.

Configuration requise :

- Microsoft .NET Framework 3.5.1 (Windows Server 2008 R2 uniquement).
- Microsoft .NET Framework 4.5.2 (4.6 est également pris en charge).
- Windows PowerShell 2.0 (compris avec Windows Server 2008 R2) ou 3.0 (compris avec Windows Server 2016 Technology Preview, Windows Server 2012 R2 et Windows Server 2012).
- Visual C++ 2008 SP1 Redistributable Package.
- Espace disque : 100 Mo.

  L'utilisation de fonctionnalités optionnelles augmente les besoins en espace disque. Par exemple, la quantité d'espace disponible pour la location de connexion (activée par défaut) dépend du nombre d'utilisateurs, d'applications et du mode : 100 000 utilisateurs RDS avec 100 applications récemment utilisées requièrent approximativement 3 Go pour la connexion des baux ; les déploiements comportant un plus grand nombre d'applications peuvent nécessiter plus d'espace. Pour les bureaux VDI dédiés, 40 000 bureaux requièrent au moins 400 à 500 Mo d'espace. Dans tous les cas, Citrix suggère de prévoir plusieurs Go d'espace supplémentaire.

Bases de données

Les versions de Microsoft SQL Server prises en charge pour les bases de données de configuration de site, de journalisation de la configuration et de surveillance :

- SQL Server 2016, éditions Express, Standard et Entreprise.
- SQL Server 2014 à SP2, éditions Express, Standard et Entreprise.
- SQL Server 2012 à SP3, éditions Express, Standard et Entreprise. Par défaut, SQL Server 2012 SP2 Express est installé lors de l'installation du Controller, si une installation de SQL Server prise en charge existante n'est pas détectée.
- SQL Server 2008 R2 SP2 et SP3 : éditions Express, Standard, Entreprise et Datacenter.

Les fonctionnalités de base de données suivantes sont prises en charge (à l'exception de SQL Server Express qui prend uniquement en charge le mode autonome) :

- Instances en cluster de SQL Server
- Miroir SQL Server
- Groupes de disponibilité AlwaysOn SQL Server 2012

L'authentification Windows est requise pour les connexions entre le Controller et la base de données SQL Server.

Pour de plus amples informations, consultez l'article Bases de données et CTX114501.

Citrix Studio

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Systèmes d'exploitation pris en charge :

- Windows 10, éditions Professionnelle, Entreprise et Éducation.
- Windows 8.1, éditions Professionnelle et Entreprise.
- Windows 8, éditions Professionnelle et Entreprise.
- Windows 7 éditions Professionnelle, Entreprise et Intégrale.
- Technical Preview actuelle de Windows Server 2016 : la prise en charge de ce système d'exploitation dans cette version est disponible à des fins d'évaluation uniquement et n'est pas destinée à un environnement de production.
- Windows Server 2012 R2, édition Standard et Datacenter.
- Windows Server 2012, édition Standard et Datacenter.
- Windows Server 2008 R2 SP1, éditions Standard, Entreprise et Datacenter.

Configuration requise :

- Espace disque : 75 Mo.
- Microsoft .NET Framework 4.5.2 (4.6 est également pris en charge)
- Microsoft .NET Framework 3.5 SP1 (Windows Server 2008 R2 et Windows 7 uniquement)
- Microsoft Management Console 3.0 (incluse avec tous les systèmes d'exploitation pris en charge).
- Windows PowerShell 2.0 (compris avec Windows 7 et Windows Server 2008 R2) ou 3.0 (compris avec Windows 10, Windows 8.1, Windows 8, Windows Server 2016 Technology Preview, Windows Server 2012 R2 et Windows Server 2012).

Citrix Director

Systèmes d'exploitation pris en charge :

- Technical Preview actuelle de Windows Server 2016 : la prise en charge de ce système d'exploitation dans cette version est disponible à des fins d'évaluation uniquement et n'est pas destinée à un environnement de production.
- Windows Server 2012 R2, édition Standard et Datacenter.
- Windows Server 2012, édition Standard et Datacenter.
- Windows Server 2008 R2 SP1, éditions Standard, Entreprise et Datacenter.

Configuration requise :

- Espace disque : 140 Mo.
- Microsoft .NET Framework 4.5.2 (4.6 est également pris en charge).
- Microsoft .NET Framework 3.5 SP1 (Windows Server 2008 R2 uniquement)
- Microsoft Internet Information Services (IIS) 7.0 et ASP.NET 2.0 Assurez-vous que le service de rôle Contenu statique est installé sur le serveur IIS. S'ils ne sont pas déjà installés, vous êtes invité à insérer le support d'installation Windows Server et ils sont installés pour vous.

L'intégration de System Center Operations Manager (SCOM) requiert :

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager

Navigateurs pris en charge pour l'affichage de Director :

- Internet Explorer 11. Vous pouvez utiliser Internet Explorer 10, mais Microsoft prend en charge la version 11 (et Citrix vous recommande d'utiliser cette version). Le mode de compatibilité n'est pas pris en charge pour Internet Explorer. Vous

© 1999-2017 Citrix Systems, Inc. All rights reserved.

devez utiliser les paramètres de navigateur recommandés pour accéder à Director. Lorsque vous installez Internet Explorer, acceptez la valeur par défaut pour utiliser les paramètres de sécurité et de compatibilité recommandés. Si vous avez déjà installé le navigateur et que vous avez choisi de ne pas utiliser les paramètres recommandés, rendez-vous dans Outils > Options Internet > Avancé > Réinitialiser et suivez les instructions.
- Microsoft Edge.
- Firefox ESR (version de prise en charge étendue).
- Chrome.

La résolution d'écran recommandée pour afficher Director est 1366 × 1024.

Virtual Delivery Agent (VDA) pour système d'exploitation de bureau

Systèmes d'exploitation pris en charge :

- Windows 10, éditions Professionnelle, Entreprise et Éducation Les fonctionnalités suivantes ne sont pas prises en charge sur Windows 10 : l'accélération GPU pour un VDA configuré en mode standard, la redirection Desktop Composition, le mode graphique d'ancienne génération, le démarrage sécurisé (uniquement pris en charge pour Remote PC Access), la publication d'applications Windows universelles à l'aide de VM Hosted Apps.
- Windows 8.1, éditions Professionnelle et Entreprise.
- Windows 8, éditions Professionnelle et Entreprise.
- Windows 7 SP1, éditions Professionnelle, Entreprise et Intégrale.

Pour utiliser la fonctionnalité Server VDI, vous pouvez utiliser l'interface de ligne de commande pour l'installation d'un VDA pour OS Windows Desktop sur un système d'exploitation serveur pris en charge ; consultez l'article Server VDI pour plus d'informations.

- Technical Preview actuelle de Windows Server 2016 : la prise en charge de ce système d'exploitation dans cette version est disponible à des fins d'évaluation uniquement et n'est pas destinée à un environnement de production.
- Windows Server 2012 R2, édition Standard et Datacenter.
- Windows Server 2012, édition Standard et Datacenter.
- Windows Server 2008 R2 SP1, éditions Standard, Entreprise et Datacenter.

Configuration requise :

- Microsoft .NET Framework 4.5.2 (4.6 est également pris en charge)
- Microsoft .NET Framework 3.5.1 (Windows 7 uniquement).
- Microsoft Visual C++ 2008 SP1, 2010 SP1 et 2013 Runtimes (32 bits et 64 bits)

Remote PC Access utilise ce VDA, que vous installez sur les PC de bureau physiques.

Ce Virtual Delivery Agent (VDA) prend en charge le démarrage sécurisé pour XenDesktop Remote PC Access sur 10 et Windows 8.1.

Plusieurs fonctionnalités d'accélération multimédia (telles que la redirection Windows Media HDX Mediastream) requièrent que Microsoft Media Foundation soit installé sur la machine sur laquelle vous installez le VDA. Si la machine ne possède pas Media Foundation installé, les fonctionnalités d'accélération multimédia ne seront pas installées et ne fonctionneront pas. Ne supprimez pas Media Foundation de la machine après l'installation du logiciel Citrix ; sinon, les utilisateurs ne pourront pas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ouvrir une session sur la machine. Sur la plupart des éditions d'OS de bureau Windows prises en charge, la prise en charge Media Foundation est déjà installée et ne peut pas être supprimée. Toutefois, N éditions n'incluent pas certaines technologies multimédia ; vous pouvez obtenir ce logiciel depuis Microsoft ou un composant tiers.

Lors de l'installation de VDA, vous pouvez choisir d'installer la version HDX 3D Pro du VDA pour OS de bureau Windows. Cette version convient tout particulièrement aux applications exploitant DirectX et OpenGL, ainsi qu'aux données multimédia riches telles que la vidéo. Consultez la section HDX 3D Pro pour plus de détails.

Vous ne pouvez pas installer une version actuelle du VDA sur une machine exécutant Windows XP ou Windows Vista ; vous pouvez cependant installer une version antérieure de Virtual Desktop Agent sur ces systèmes d'exploitation, si nécessaire. Pour de plus amples informations, veuillez consulter l'article CTX140941. La version de Remote PC Access disponible dans cette version n'est pas prise en charge sur les systèmes d'exploitation Windows Vista.

Virtual Delivery Agent (VDA) pour système d'exploitation de serveur

Systèmes d'exploitation pris en charge :

- Technical Preview actuelle de Windows Server 2016 : la prise en charge de ce système d'exploitation dans cette version est disponible à des fins d'évaluation uniquement et n'est pas destinée à un environnement de production.
- Windows Server 2012 R2, édition Standard et Datacenter.
- Windows Server 2012, édition Standard et Datacenter.
- Windows Server 2008 R2 SP1, éditions Standard, Entreprise et Datacenter.

Le programme d'installation déploie automatiquement la configuration requise, qui est également disponible sur le support d'installation Citrix dans les dossiers Support :

- Microsoft .NET Framework 4.5.2 (4.6 est également pris en charge)
- Microsoft .NET Framework 3.5.1 (Windows Server 2008 R2 uniquement).
- Microsoft Visual C++ 2008 SP1, 2010 SP1 et 2013 Runtimes (32 bits et 64 bits)

Le programme d'installation installe et active automatiquement et les services de rôle des services Bureau à distance, s'ils ne sont pas déjà installés et activés.

Plusieurs fonctionnalités d'accélération multimédia (telles que la redirection Windows Media HDX Mediastream) requièrent que Microsoft Media Foundation soit installé sur la machine sur laquelle vous installez le VDA. Si la machine ne possède pas Media Foundation installé, les fonctionnalités d'accélération multimédia ne seront pas installées et ne fonctionneront pas. Ne supprimez pas Media Foundation de la machine après l'installation du logiciel Citrix ; sinon, les utilisateurs ne pourront pas ouvrir une session sur la machine. Sur la plupart des éditions Windows Server 2012 R2, Windows Server 2012 et Windows Server 2008 R2 éditions, la fonctionnalité de Media Foundation est installée via le Gestionnaire de serveur (pour Windows Server 2012 R2 et Windows Server 2012 : ServerMediaFoundation, pour Windows Server 2008 R2 : DesktopExperience). Toutefois, N éditions n'incluent pas certaines technologies multimédia ; vous pouvez obtenir ce logiciel depuis Microsoft ou un composant tiers.

Hôtes et ressources de virtualisation

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Certaines des fonctionnalités de XenApp et XenDesktop peuvent ne pas être prises en charge sur toutes les plates-formes hôte ou toutes les versions de plate-forme. Par exemple, les AppDisks sont pris en charge avec les hôtes XenServer et VMware. Pour de plus amples informations, consultez la documentation relative aux fonctionnalités.

L'article CTX131239 contient des informations supplémentaires sur les versions d'hyperviseur prises en charge.

Plates-formes hôte prises en charge :

XenServer

- XenServer 6.5 et SP1
- XenServer 6.2 SP1 plus corrections à chaud (vous devez appliquer SP1 pour activer l'application de futurs correctifs)
- XenServer 6.1

VMware vSphere. aucune prise en charge n'est fournie pour l'opération vSphere vCenter Linked Mode.

- VMware vSphere 6.0 et mises à jour 1 et 2
- VMware vSphere 5.5 et mises à jour 1 à 3
- VMware vSphere 5.1 mises à jour 2 et 3
- VMware vSphere 5.0 mises à jour 2 et 3
- Boîtier VMware vCenter 5.5/6

System Center Virtual Machine Manager : comprend toute version d'Hyper-V qui peut s'inscrire auprès des versions prises en charge de System Center Virtual Machine Manager.

- System Center Virtual Machine Manager 2012 R2
- System Center Virtual Machine Manager 2012 SP1
- System Center Virtual Machine Manager 2012

Nutanix Acropolis 4.5. Plusieurs fonctionnalités XenApp et XenDesktop ne sont pas disponibles lors de l'utilisation de cette plate-forme ; consultez l'article CTX202032 pour de plus amples informations. Pour plus d'informations sur l'utilisation du produit avec Acropolis, visitez https://portal.nutanix.com/#/page/docs.

Environnements de cloud pris en charge :

services Web Amazon (AWS)

- Vous pouvez configurer des applications et des bureaux sur les systèmes d'exploitation Windows pris en charge.
- SQL Server 2012 Enterprise n'est pas disponible sur AWS.
- AWS ne prend pas en charge les instances de système d'exploitation de bureau.
- Le service Amazon de la base de données relationnelle (RDS) n'est pas pris en charge.
- Consultez la section Citrix XenDesktop sur AWS pour des informations supplémentaires.

Citrix CloudPlatform

- La version minimale prise en charge est 4.2.1 avec des corrections à chaud 4.2.1-4
- Les déploiements ont été testés à l'aide de XenServer 6.2 (avec Service Pack 1 et correction à chaud XS62ESP1003) et hyperviseurs vSphere 5.1
- CloudPlatform ne prend pas en charge les hyperviseurs Hyper-V.
- CloudPlatform 4.3.0.1 prend en charge VMware vSphere 5.5.
- Consultez la documentation de CloudPlatform (y compris les notes de publication pour votre version CloudPlatform) pour

© 1999-2017 Citrix Systems, Inc. All rights reserved.

des informations supplémentaires.

Microsoft Azure

La fonctionnalité Remote PC Access Wake on LAN requiert Microsoft System Center Configuration Manager 2012.

Niveaux fonctionnels Active Directory

Les niveaux fonctionnels de la forêt et du domaine Active Directory sont pris en charge :

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003
- Windows 2000 natif (non pris en charge pour les contrôleurs de domaine)

HDX

L'audio UDP pour Multi-Stream ICA est pris en charge sur Receiver pour Windows et Citrix Receiver pour Linux 13.

L'annulation de l'écho est prise en charge sur Citrix Receiver pour Windows.

Consultez la prise en charge et la configuration requise pour chaque fonctionnalité HDX spécifique ci-dessous.

La machine utilisateur Windows ou un client léger doit prendre en charge ou contenir :

- DirectX 9
- Pixel Shader 2.0 (pris en charge dans le matériel)
- 32 bits par pixel
- Processeur 1,5 GHz 32 bits ou 64 bits
- 1 Go de RAM
- 128 Mo de mémoire vidéo sur la carte graphique ou sur le processeur graphique intégré

HDX interroge la machine Windows pour vérifier qu'elle possède des capacités GPU et retourne automatiquement à la composition de bureau côté serveur si ce n'est pas le cas. Répertoriez les machines Windows avec les capacités de processeur graphique requise, qui ne répondent pas aux spécifications de vitesse de processeur ou de mémoire vive (RAM) doivent être répertoriées dans le groupe de l'objet de stratégie de groupe pour les appareils exclus de la Redirection Desktop Composition.

La valeur minimale de bande passante disponible est de 1,5 Mbps, la bande passante recommandée est de 5 Mbps. Ces valeurs intègrent la latence de bout en bout.

Les clients suivants sont pris en charge pour la récupération de contenu côté client Windows Media, la redirection Windows Media, le transcodage multimédia en temps réel de Windows Media : Citrix Receiver pour Windows, Citrix Receiver pour iOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

et Citrix Receiver pour Linux.

Pour utiliser la récupération de contenu côté client Windows Media sur des machines Windows 8, définissez Citrix Multimedia Redirector comme programme par défaut : dans le **Panneau de configuration > Programmes > Programmes par défaut > Choisir les programmes par défaut**, sélectionnez **Citrix Multimedia Redirector** et cliquez sur **Définir ce programme comme programme par défaut** ou **Choisir les paramètres par défaut pour ce programme**. Un transcodage GPU requiert un processeur graphique compatible NVIDIA CUDA avec Compute Capability 1.1 ou version ultérieure ; voir http://developer.nvidia.com/cuda/cuda-gpus.

Les clients suivants et Adobe Flash Player sont pris en charge :

- Citrix Receiver pour Windows (pour les fonctionnalités de redirection Flash de deuxième génération) : les fonctionnalités de redirection Flash de deuxième génération nécessitent Adobe Flash Player pour d'autres navigateurs, parfois appelé NPAPI (Netscape Plugin Application Programming Interface) de Flash Player
- Citrix Receiver pour Linux (pour les fonctionnalités de redirection Flash de deuxième génération) : les fonctionnalités de redirection Flash de deuxième génération nécessitent Adobe Flash Player pour Linux ou Adobe Flash Player pour Ubuntu.
- Citrix Online Plug-in 12.1 (pour les fonctionnalités de redirection Flash d'ancienne génération) : les fonctionnalités de redirection Flash d'ancienne génération nécessitent Adobe Flash Player pour Windows Internet Explorer (parfois appelé lecteur ActiveX).

le numéro de version majeur du lecteur Flash Player sur la machine utilisateur doit être supérieur ou égal au numéro de version majeur du lecteur Flash Player sur le serveur. Si une version antérieure de Flash Player est installée sur la machine utilisateur, ou si le lecteur Flash Player ne peut pas être installé sur la machine utilisateur, le contenu Flash est restitué sur le serveur.

Les machines exécutant VDA requièrent :

- Adobe Flash Player pour Windows Internet Explorer (le lecteur ActiveX) ;
- Internet Explorer 11 (en mode UI non-moderne). Vous pouvez utiliser Internet Explorer versions 7-10, mais Microsoft prend en charge la version 11 (et Citrix vous recommande d'utiliser cette version). la redirection Flash requiert Internet Explorer sur le serveur ; avec d'autres navigateurs, le contenu Flash est restitué sur le serveur.
- Le mode protégé désactivé dans Internet Explorer (Outils > Options Internet > onglet Sécurité > case à cocher Activer le mode protégé désactivée). Redémarrez Internet Explorer pour appliquer la modification.

Si vous installez un VDA pour OS de bureau Windows, vous pouvez choisir d'installer la version HDX 3D Pro.

La machine physique ou virtuelle qui héberge l'application peut utiliser la fonctionnalité GPU Passthrough de traitement graphique (GPU) ou virtuel (vGPU) :

- GPU Passthrough est disponible avec Citrix XenServer. GPU Passthrough est également disponible avec VMware vSphere et VMware ESX, où il est appelé accélération graphique virtuelle (vDGA).
- vGPU est disponible avec Citrix XenServer et VMware vSphere ; voir www.citrix.com/go/vGPU (informations d'identification de votre compte Citrix requises).

Citrix recommande que l'ordinateur hôte dispose au minimum de 4 Go de mémoire vive et d'une UC à quadruple cœur offrant une vitesse d'horloge de 2,3 GHz ou plus.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Unité de traitement graphique (GPU) :

- Pour la compression basée sur l'UC, y compris la compression sans perte, HDX 3D Pro prend en charge toute carte vidéo sur l'ordinateur hôte compatible avec l'application que vous mettez à disposition.
- Pour optimiser l'accès à la mémoire tampon de trame GPU à l'aide de NVIDIA GRID API, HDX 3D Pro peut être utilisé avec des cartes NVIDIA prises en charge (voir NVIDIA GRID). Le NVIDIA GRID offre une haute fréquence d'images, ce qui entraîne une expérience utilisateur hautement interactive.
- Pour optimiser l'accès à la mémoire tampon de trame GPU à l'aide de du SDK Intel Media, HDX 3D Pro peut être utilisé avec les plates-formes matérielles Intel et processeurs Intel Iris Pro Graphics pris en charge. Les processeurs Intel pris en charge comprennent les Processeurs Intel Core de 5ème génération et les Processeurs Intel Core de 6ème génération.
- Pour vGPU utilisant XenServer, la configuration requise HDX 3D Pro comprend des cartes NVIDIA GRID K1 et K2 (voir NVIDIA GRID).

Machine utilisateur :

- HDX 3D Pro prend en charge toutes les résolutions de moniteur prises en charge par le processeur graphique de l'ordinateur hôte. Toutefois, pour des performances optimales avec les spécifications minimales recommandées pour la machine utilisateur et le processeur graphique, Citrix recommande de ne pas dépasser, sur la machine utilisateur, la résolution de 1920 x 1200 pixels pour les connexions en réseau local et de 1280 x 1024 pixels pour les connexions en réseau étendu.
- Citrix recommande qu'au minimum, les machines utilisateur disposent de 1 Go de mémoire vive et d'une UC avec une vitesse d'horloge de 1,6 GHz ou plus. L'utilisation du codec de compression profonde par défaut, qui est requis sur les connexions à faible bande passante, requiert un processeur plus puissant à moins que le décodage ne soit effectué dans le matériel. Pour des performances optimales, Citrix recommande que les machines utilisateur soient équipées de 2 Go de mémoire vive et d'un processeur double cœur offrant une vitesse d'horloge de 3 GHz ou plus.
- Pour accéder à plusieurs moniteurs, Citrix recommande que les machines utilisateur soient équipées d'UC quadruple cœur.
- Les machines utilisateur n'ont pas besoin d'un processeur graphique pour accéder aux bureaux ou aux applications mises à disposition avec HDX 3D Pro.
- Citrix Receiver doit être installé.

Pour de plus amples informations, consultez les articles HDX 3D Pro et www.citrix.com/xenapp/3d.

Clients pris en charge : Citrix Receiver pour Windows, Citrix Receiver pour Mac et Citrix Receiver pour Linux.

Applications de visioconférence prises en charge :

- Adobe Connect
- Cisco WebEx
- Citrix GoToMeeting HD Faces
- Google + Hangouts
- IBM Sametime
- Applications vidéo Media Foundation sur Windows 8.x, Windows Server 2012 et Windows Server 2012 R2
- Microsoft Lync 2010 et 2013
- Microsoft Office Communicator
- Microsoft Skype 6.7

Pour utiliser Skype sur un client Windows, modifiez le registre sur le client et le serveur :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Clé de Registre cliente HKEY_CURRENT_USER\Software\Citrix\HdxRealTime

Name: DefaultHeight , Type: REG_DWORD, Data: 240

Nom : DefaultWidth, Type : REG_DWORD, Données : 320

Clé de Registre serveur HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Compatibility

Name: skype.exe, Type: REG_DWORD, Data: Set to 0

Autres configurations requises pour la machine utilisateur :

- Un matériel approprié pour produire des sons.
- une webcam compatible DirectShow (utilisez les paramètres par défaut de la webcam) ; Des webcams avec encodeur matériel réduisent l'utilisation de l'UC du côté client.
- Les pilotes de webcam, obtenus à partir du fournisseur de caméra si possible.

Enregistrement de session

Cette section présente la configuration système requise pour :

Composants de l'administration d'enregistrement de session

Agent d'enregistrement de session

Lecteur d'enregistrement de session

Les composants de l'administration d'enregistrement de session (base de données d'enregistrement de session, serveur d'enregistrement de session et console de stratégie d'enregistrement de session) peuvent aussi bien être installés sur un serveur unique que sur différents serveurs.

Base de données d'enregistrement de session

Systèmes d'exploitation pris en charge :

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

Versions de Microsoft SQL Server prises en charge :

- Microsoft SQL Server 2014 éditions Enterprise, Express et Standard
- Microsoft SQL Server 2012 SP2 éditions Enterprise et Express
- Microsoft SQL Server 2008 R2 SP3 éditions Enterprise et Express

Configuration requise : .NET Framework version 3.5 SP1 (Windows Server 2008 R2 uniquement) ou .NET Framework version 4.5.2 ou 4.6.

Serveur d'enregistrement de session

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Systèmes d'exploitation pris en charge :

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

Vous devez installer les composants requis avant d'installer le serveur d'enregistrement de session. Dans le Gestionnaire de serveur, ajoutez le rôle IIS et sélectionnez les options suivantes :

- Développement d'applications > ASP.NET 4.5 sur Server 2012 et Server 2012 R2, ASP.NET sur Server 2008 R2. Les autres composants sont automatiquement sélectionnés ; cliquez sur **Ajouter** pour accepter les rôles requis.
- Sécurité > Authentification Windows
- Outils de gestion > Compatibilité avec la gestion IIS 6 : compatibilité avec la métabase de données IIS 6, compatibilité avec le service WMI IIS 6, outils de script IIS 6, console de gestion IIS 6

Autres éléments requis :

- .NET Framework version 3.5 SP1 (Windows Server 2008 R2 uniquement) ou .NET Framework version 4.5.2 ou 4.6.
- Si le serveur d'enregistrement de session utilise HTTPS comme protocole de communication, ajoutez un certificat valide. L'enregistrement de session utilise HTTPS par défaut, selon les recommandations de Citrix.
- Microsoft Message Queuing (MSMQ), avec intégration Active Directory désactivée et la prise en charge de MSMQ HTTP activée.

Console de stratégie d'enregistrement de session

Systèmes d'exploitation pris en charge :

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

Configuration requise : .NET Framework version 3.5 SP1 (Windows Server 2008 R2 uniquement) ou .NET Framework version 4.5.2 ou 4.6.

L'installation de l'agent d'enregistrement de session s'effectue sur chaque serveur XenApp et XenDesktop pour lequel vous souhaitez enregistrer des sessions.

Systèmes d'exploitation pris en charge :

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10
- Microsoft Windows 8,1
- Microsoft Windows 8
- Microsoft Windows 7 SP1

Configuration requise :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- XenApp 7.8 ou XenDesktop 7.8 avec licence Platinum
- .NET Framework version 4.5.2 ou 4.6
- Microsoft Message Queuing (MSMQ), avec intégration Active Directory désactivée et la prise en charge de MSMQ HTTP activée.

Systèmes d'exploitation pris en charge :

- Microsoft Windows 10
- Microsoft Windows 8,1
- Microsoft Windows 8
- Microsoft Windows 7 SP1

Configuration requise : .NET Framework version 3.5 SP1 (Windows 7 uniquement), 4.5.2 ou 4.6.

Pour obtenir des résultats optimaux, installez le lecteur d'enregistrement de session sur une station de travail disposant des caractéristiques suivantes :

- Résolution d'écran de 1024 x 768.
- Profondeur de couleur d'au moins 32 bits.
- 1 Go de RAM minimum ; des ressources supplémentaires en RAM et UC/GPU peuvent améliorer les performances lors de la lecture d'enregistrements riches en graphiques ; plus particulièrement si les enregistrements contiennent beaucoup d'animations.

Le délai de réponse de la recherche dépend de la taille de l'enregistrement et des spécifications matérielles de votre ordinateur.

Serveur d'impression universelle

Le serveur d'impression universelle comprend les composants client et serveur. Le composant UpsClient est inclus dans l'installation du VDA. Vous installez le composant UpsServer sur chaque serveur d'impression où les imprimantes partagées résident que vous souhaitez provisionner avec le pilote d'impression universelle Citrix dans les sessions utilisateur.

Le composant UpsServer est pris en charge sur :

- Windows Server 2012 R2 et 2012.
- Windows Server 2008 R2 SP1
- Windows Server 2003 32 bits

Configuration requise : Microsoft Visual C++ 2013 Runtime

Pour les VDA pour OS Windows Server, l'authentification de l'utilisateur lors des opérations d'impression nécessite que le Serveur d'impression universelle appartienne au même domaine que le VDA.

Des packs de composants client et serveur autonomes peuvent également être téléchargés.

Pour plus d'informations, veuillez consulter l'article Provisionner les imprimantes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Autre

Résolutions mixtes avec plusieurs moniteurs. L'utilisation de différentes résolutions entre les moniteurs n'est pas prise en charge dans les environnements Citrix XenDesktop et XenApp. Vous pouvez vérifier la résolution (% de mise à l'échelle) sous Panneau de configuration de Windows > Affichage. Si vous utilisez une machine cliente Windows 8.1 ou Windows 10, l'activation de l'option « Me laisser choisir un niveau de mise à l'échelle pour tous mes affichages » dans le Panneau de configuration de Windows > Affichage configure les moniteurs de manière appropriée. Pour de plus amples informations, consultez la section CTX201696. Citrix vous recommande d'installer ou de mettre à niveau les versions logicielles du composant fournies sur le support d'installation de cette version.

- StoreFront requiert 2 Go de mémoire. Consultez la documentation StoreFront pour la configuration système requise. StoreFront 2.6 est la version minimale prise en charge avec cette version.
- Lors de l'utilisation de Provisioning Services avec cette version, la version minimale de Provisioning Services prise en charge est la version 7.0.
- Le serveur de licences Citrix requiert 40 Mo d'espace disque. Consultez la documentation relative au système de licences pour une configuration système requise. Seul le serveur de licences Citrix pour Windows est pris en charge. La version minimale prise en charge est la version 11.13.1.

Microsoft Group Policy Management Console (GPMC) est nécessaire si vous stockez les informations de stratégie Citrix dans Active Directory au lieu de la base de données de configuration de site. Pour plus d'informations, veuillez consulter la documentation Microsoft.

Plusieurs cartes d'interface réseau sont prises en charge.

Par défaut, Citrix Receiver pour Windows est installé lorsque vous installez un VDA. Pour plus d'informations, consultez la documentation Citrix Receiver pour Windows.

Consultez l'article App-V pour les versions prises en charge de Microsoft App-V.

Consultez l'article Local App Access pour des informations sur les navigateurs pris en charge pour Local App Access.

Redirection de dossiers clients : systèmes d'exploitation pris en charge :

- Serveur : Windows Server 2008 R2 SP1, Windows Server 2012 et Windows Server 2012 R2
- Client (avec la dernière version de Citrix Receiver pour Windows) : Windows 7, Windows 8 et Windows 8.1

Résolutions mixtes avec plusieurs moniteurs. L'utilisation de différentes résolutions entre les moniteurs n'est pas prise en charge dans les environnements Citrix XenDesktop et XenApp. Vous pouvez vérifier la résolution (% de mise à l'échelle) sous Panneau de configuration de Windows > Affichage. Si vous utilisez une machine cliente Windows 8.1 ou Windows 10, l'activation de l'option **Me laisser choisir un niveau de mise à l'échelle pour tous mes affichages** dans le Panneau de configuration de Windows > Affichage configure les moniteurs de manière appropriée. Pour obtenir davantage d'informations, veuillez consulter la section CTX201696.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Vue d'ensemble technique

Aug 22, 2016

XenApp et XenDesktop sont des solutions de virtualisation qui fournissent au personnel informatique un contrôle des machines virtuelles, des applications, des licences et de la sécurité tout en offrant un accès à n'importe quel appareil.

XenApp et XenDesktop permettent :

- Aux utilisateurs d'exécuter des applications et des bureaux indépendamment du système d'exploitation et de l'interface de l'appareil.
- Aux administrateurs de gérer le réseau et fournir ou restreindre l'accès à partir d'appareils sélectionnés ou depuis tous les appareils.
- Aux administrateurs de gérer l'ensemble d'un réseau à partir d'un centre de données unique.

XenApp et XenDesktop partagent une architecture unifiée appelée FlexCast Management Architecture (FMA). Les fonctionnalités clé de FMA comprennent la possibilité d'exécuter plusieurs versions de XenApp ou XenDesktop à partir d'un site unique et un provisioning intégré.

Composants principaux de FMA

Un environnement XenApp ou XenDesktop typique est constitué de plusieurs composants technologiques clé, qui interagissent lorsque les utilisateurs se connectent à des applications et des bureaux, et des données du journal sur l'activité du site.

Citrix Receiver : un client logiciel qui est installé sur la machine utilisateur, fournit la connexion à la machine virtuelle via le port TCP 80 ou 443, et communique avec StoreFront à l'aide de l'API du service StoreFront.

Citrix StoreFront : l'interface qui permet d'authentifier les utilisateurs, de gérer les applications et les bureaux, et qui héberge le magasin d'applications. StoreFront communique avec le Delivery Controller à l'aide de XML.

Delivery Controller : le composant de gestion centralisée d'un site XenApp ou XenDesktop qui comprend des services qui gèrent des ressources, des applications et des bureaux, et optimisent et équilibrent les charges des connexions utilisateur.

Virtual Delivery Agent (VDA) : un agent qui est installé sur des machines exécutant Windows Server ou des systèmes d'exploitation de bureau Windows qui permettent à ces machines et aux ressources qu'ils hébergent d'être mise à la disposition des utilisateurs. Les machines installées sur des VDA exécutant le système d'exploitation Windows Server autorisent la machine à héberger plusieurs connexions pour plusieurs utilisateurs et sont connectés à des utilisateurs sur les ports suivants :

- port TCP 80 ou 443 si TLS est activé
- Port TCP 2598, si le protocole CGP (Citrix Gateway Protocol) est activé, ce qui active la fiabilité de session
- Port TCP 1494 si CGP est désactivé ou si l'utilisateur se connecte à l'aide d'un client d'ancienne génération

Service de Broker : un service Delivery Controller qui contrôle quels utilisateurs sont connectés et depuis quel endroit, quelles ressources de session les utilisateurs possèdent-ils et si les utilisateurs doivent se reconnecter aux applications existantes. Le service de Broker exécute PowerShell et communique avec l'agent Broker sur le port TCP 80. Il n'est pas possible d'utiliser le port TCP 443.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Agent Broker : un agent qui héberge de multiples plug-ins et collecte des données en temps réel. L'agent Broker est situé sur le VDA et est connecté au Controller à l'aide du port TCP 80. Il n'est pas possible d'utiliser le port TCP 443.

Service Moniteur : un composant de Delivery Controller qui collecte des données d'historique et les place dans la base de données du site par défaut. Le service Moniteur communique sur le port TCP 80 ou 443.

Fichier/pile ICA : informations utilisateur groupées qui sont requises pour se connecter au VDA.

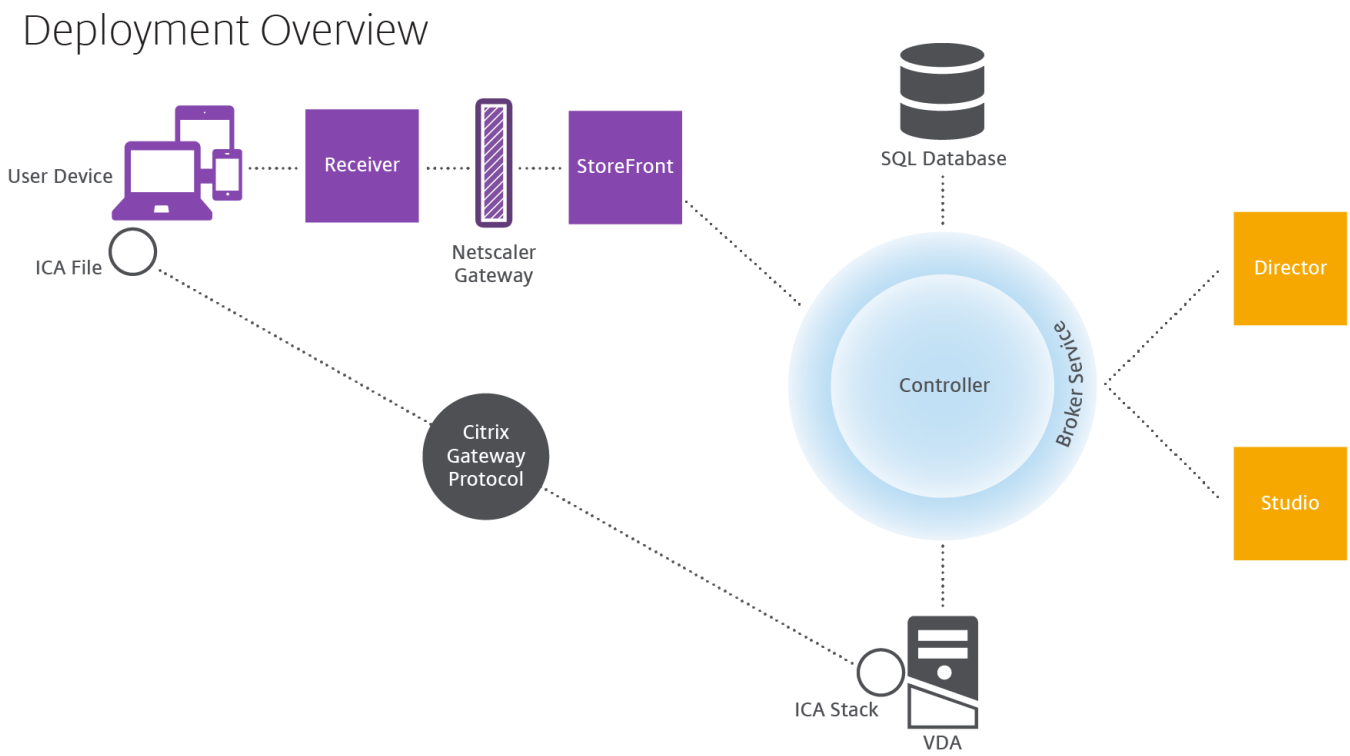
Base de données du site : une base de données Microsoft SQL qui stocke les données pour le Delivery Controller, telles que les stratégies de site, les catalogues de machines et les groupes de mise à disposition.

NetScaler Gateway : une solution data-access offre un accès sécurisé à l'intérieur ou à l'extérieur du pare-feu du réseau local avec d'autres informations d'identification.

Citrix Director : un outil Web qui permet l'accès aux données en temps réel pour les administrateurs et le personnel d'assistance à partir de l'agent Broker, les données d'historique de la base de données du site, et les données HDX de NetScaler pour le dépannage et le support. Director communique avec le Controller sur le port TCP 80 ou 443.

Citrix Studio : une console d'administration qui permet aux administrateurs de configurer et de gérer des sites et permet d'accéder à des données en temps réel à partir de l'agent Broker. Studio communique avec le Controller sur le port TCP 80.

Les sites XenApp et XenDesktop sont composés de machines avec des rôles dédiés qui permettent de garantir une certaine évolutivité, une haute disponibilité, la capacité de basculement, et fournir une solution qui est sécurisé par nature. Un site XenApp ou XenDesktop comprend des serveurs et des machines de bureau installés sur un VDA, ainsi que le Delivery Controller, qui gère l'accès.



Le VDA permet aux utilisateurs de se connecter à des bureaux et des applications. Il est installé sur des machines de serveur

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ou de bureaux dans le centre de données pour la plupart des méthodes de mise à disposition, mais il peut également être installé sur des ordinateurs physiques pour Remote PC Access.

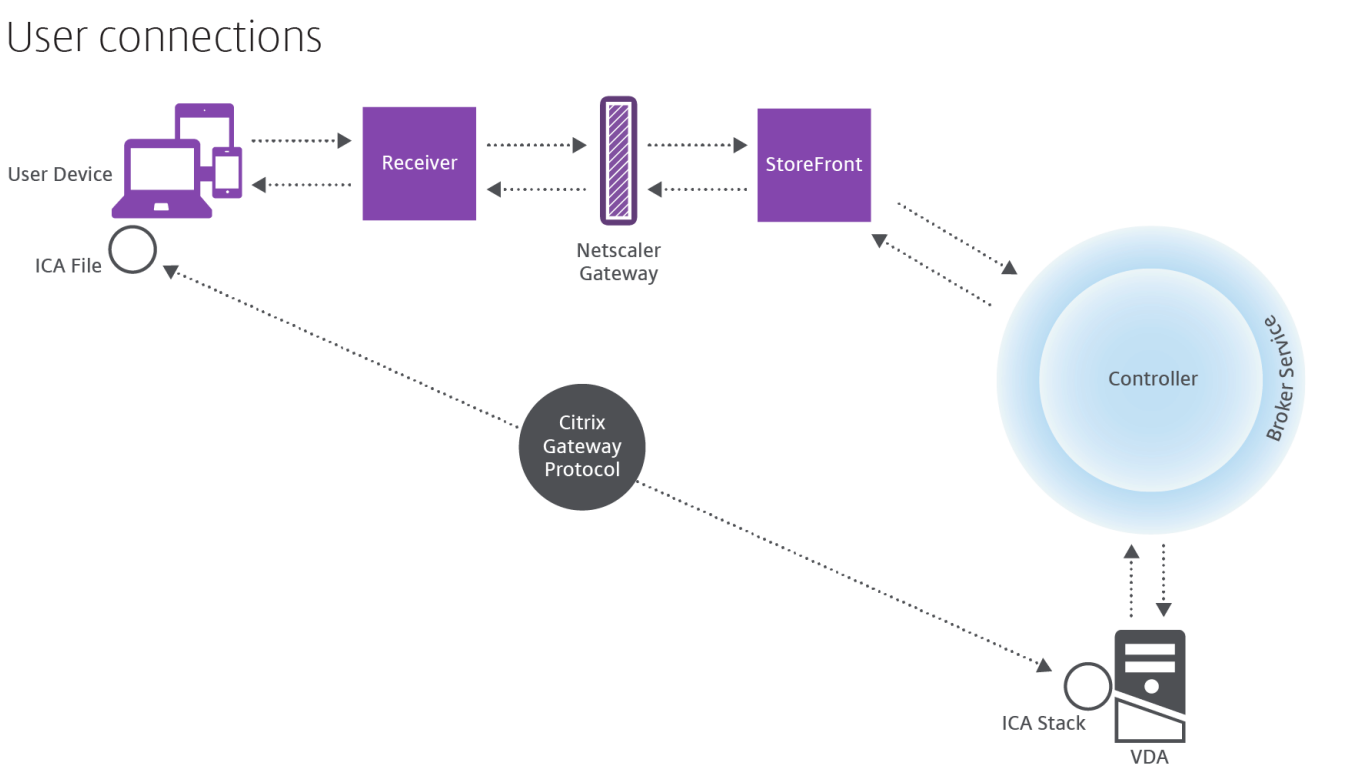
Le Controller est constitué de services Windows indépendants qui permettent de gérer les ressources, les applications et les bureaux, et optimiser et équilibrer les connexions utilisateur. Chaque site possède un ou plusieurs Controller, et, parce que les sessions sont dépendantes de la latence, de la bande passante et de fiabilité du réseau, tous les Controller devraient idéalement se trouver sur le même réseau local.

Les utilisateurs n'accèdent jamais directement au Controller. Le VDA est utilisé en tant que intermédiaire entre les utilisateurs et le Controller. Lorsque les utilisateurs ouvrent une session sur le site à l'aide de StoreFront, leurs informations d'identification sont transmises via le service Broker, qui obtient leurs profils et les ressources disponibles en fonction des stratégies définies pour ces derniers.

Pour démarrer une session XenApp ou XenDesktop, l'utilisateur se connecte, soit via Citrix Receiver, qui est installé sur la machine utilisateur, soit par le biais de Citrix Receiver pour Web (RFW).

Dans Citrix Receiver, l'utilisateur sélectionne les bureaux virtuels ou physiques ou l'application virtuelle nécessaire(s).

Les informations d'identification de l'utilisateur passent par le biais de cette piste pour accéder au Controller, qui détermine quelles ressources sont nécessaires à la communication avec un service Broker. Il est recommandé que les administrateurs placent un certificat SSL sur StoreFront pour chiffrer les informations d'identification provenant de Receiver.



Le Service Broker détermine la nature des bureaux et des applications que l'utilisateur est autorisé à accéder.

Une fois les informations d'identification vérifiées, les informations sur les applications ou les bureaux disponibles sont envoyées à l'utilisateur au travers de la piste StoreFront-Citrix Receiver. Lorsque l'utilisateur sélectionne des applications ou des bureaux depuis cette liste, ces informations retournent à la piste vers le Delivery Controller, qui détermine le VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

approprié pour héberger les applications ou les bureaux spécifiques.

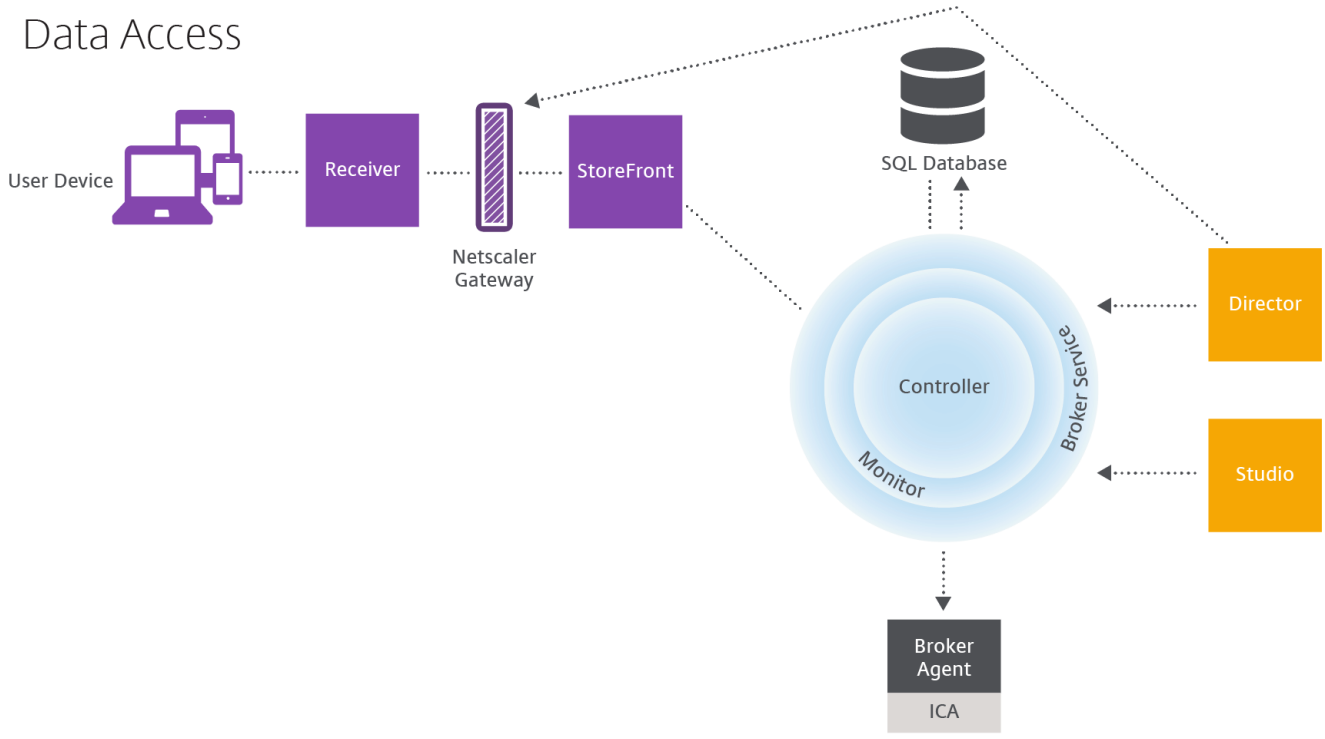
Le Controller envoie un message au VDA avec les informations d'identification de l'utilisateur et envoie toutes les données à propos de l'utilisateur et de la connexion au VDA. Le VDA accepte la connexion et renvoie les informations vers les mêmes pistes jusqu'au Citrix Receiver. Citrix Receiver regroupe toutes les informations qui ont été générées dans la session pour créer le fichier ICA (Independent Computing Architecture) sur la machine de l'utilisateur si Citrix Receiver est installé localement ou sur Citrix RFW si accessible via le Web. Tant que le site a été correctement configuré, les informations d'identification sont chiffrées dans ce processus.

Le fichier ICA est copié vers la machine de l'utilisateur et établit une connexion directe entre le périphérique et la pile ICA en cours d'exécution sur le VDA. Cette connexion ignore l'infrastructure de gestion : Citrix Receiver, StoreFront et Controller.

La connexion entre Citrix Receiver et le VDA utilise Citrix Gateway Protocol (CGP). Si une connexion est interrompue, la fonction de fiabilité de session permet à l'utilisateur de se reconnecter au VDA plutôt que d'avoir à redémarrer via l'infrastructure de gestion. La fiabilité de session peut être activée ou désactivée dans Studio.

Une fois que le client se connecte au VDA, le VDA avertit le Controller que l'utilisateur a ouvert une session, et le Controller envoie ces informations à la base de données du site et démarre la journalisation des données dans la base de données de surveillance.

Chaque session XenApp ou XenDesktop génère des données auxquelles le service informatique peut accéder au travers de Studio ou Director. Studio permet aux administrateurs d'accéder à des données en temps réel à partir de l'agent Broker afin de mieux gérer les sites. Director a accès aux mêmes données en temps réel et données d'historique stockées dans la base de données de surveillance ainsi que les données HDX de NetScaler Gateway à des fins de dépannage et de support technique.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dans le Controller, le service Broker signale des données de session pour chaque session sur la machine virtuelle fournissant des données en temps réel. Le service Moniteur suit également les données en temps réel et les stocke en tant que données d'historique dans la base de données de surveillance.

Studio peut uniquement communiquer avec le service Broker ; par conséquent, il a uniquement accès aux données en temps réel. Director communique avec le service Broker (via un plug-in dans l'agent Broker) pour accéder à la base de données du site.

Director peut également accéder à NetScaler Gateway pour obtenir des informations sur les données HDX.

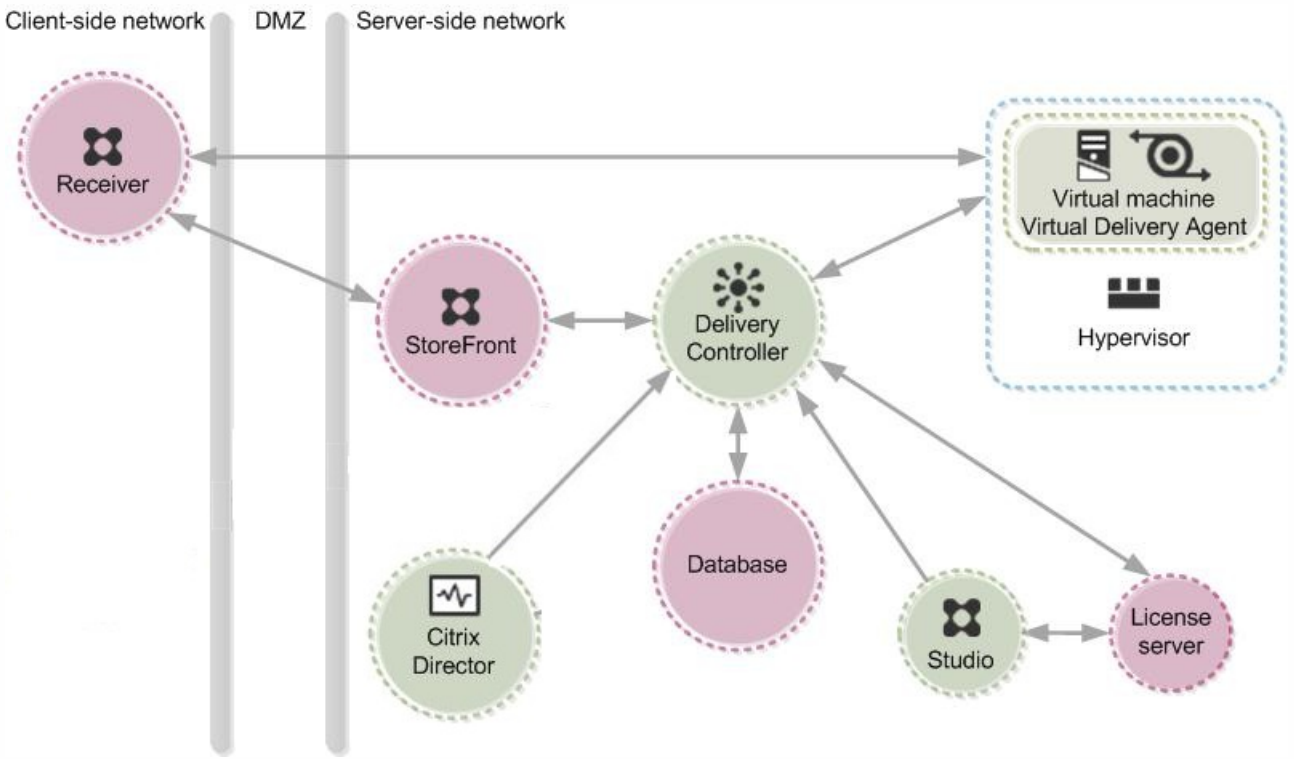
- Concepts et composants
- Méthodes de mise à disposition

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Concepts et composants

Jul 07, 2016

Cette illustration affiche les composants principaux d'un déploiement XenApp ou XenDesktop typique, qui est appelé un *site*.



Les composants de cette illustration sont les suivants :

- **Delivery Controller** : Delivery Controller est le composant de gestion centralisée de tout site XenApp ou XenDesktop. Chaque site possède un ou plusieurs Delivery Controller. Il est installé sur au moins un serveur dans le centre de données. (Pour la fiabilité et la disponibilité du site, installez le Controller sur plusieurs serveurs). Si votre déploiement comprend des machines virtuelles hébergées sur un hyperviseur ou service de cloud, les services Controller communiquent avec l'hyperviseur pour distribuer les applications et les bureaux, authentifier et gérer l'accès utilisateur, négocier les connexions entre les utilisateurs et leurs applications et bureaux virtuels, optimiser l'utilisation de connexions et répartir la charge de ces connexions.
  Chaque donnée du service est stockée dans la base de données du site.

  Le Controller gère l'état des bureaux, les démarre ou les arrête à la demande et en fonction de la configuration de l'administration. Dans certaines éditions, le Controller permet d'installer Profile Management pour gérer les paramètres de personnalisation des utilisateurs dans des environnements Windows physiques ou virtualisés.

- **Base de données** : au moins une base de données Microsoft SQL Server est requise pour chaque site XenApp ou XenDesktop pour stocker toutes les informations de configuration et de session. Cette base de données stocke les données collectées et gérés par les services qui constituent le Controller. Installez la base de données dans votre centre de données et assurez-vous qu'elle possède une connexion permanente au Controller.
- **Virtual Delivery Agent (VDA)** : le VDA est installé sur chaque machine physique ou virtuelle de votre site que vous

© 1999-2017 Citrix Systems, Inc. All rights reserved.

voulez rendre disponible aux utilisateurs. Il permet aux machines de s'enregistrer auprès du Controller, qui permet à la machine et aux ressources qu'elle héberge d'être mise à la disposition des utilisateurs. Les VDA établissent et gèrent la connexion entre la machine et la machine utilisateur, vérifiez qu'une licence Citrix est disponible pour l'utilisateur ou la session, et appliquez toute stratégie qui a été configurée pour la session. Le VDA communique des informations de session au service Broker dans le Controller via l'agent Broker inclus dans le VDA.
Les VDA sont disponibles pour les systèmes d'exploitation de serveur et de bureau Windows. Les VDA pour les systèmes d'exploitation de serveur Windows Server autorisent plusieurs utilisateurs à se connecter au serveur à un moment donné. Les VDA pour les systèmes d'exploitation de bureau Windows ne permettent qu'à un seul utilisateur de se connecter au bureau à la fois.

- **Citrix StoreFront** : StoreFront authentifie les utilisateurs sur les sites hébergeant les ressources et gère les magasins de bureaux et d'applications auxquels les utilisateurs accèdent. Il héberge votre magasin d'applications d'entreprise qui vous permet de fournir aux utilisateurs un accès en libre-service à des bureaux et des applications que vous mettez à leur disposition. Il permet également d'effectuer le suivi des abonnements aux applications des utilisateurs, des noms de raccourci et d'autres données pour vous assurer qu'ils ont une expérience cohérente sur de multiples périphériques.
- **Citrix Receiver** : installé sur les machines utilisateur et autres points de terminaison, tels que les bureaux virtuels, Citrix Receiver offre aux utilisateurs un accès en libre-service, rapide et sécurisé aux documents, applications et bureaux à partir de tout appareil utilisateur, y compris les smartphones, tablettes et PC. Citrix Receiver offre également un accès à la demande aux applications Windows, Web et SaaS (Software as a Service). Pour les périphériques qui ne peuvent pas installer le logiciel Citrix Receiver, Citrix Receiver pour HTML5 offre une connexion via un navigateur Web compatible HTML5.
- **Citrix Studio** : Studio est la console de gestion qui vous permet de configurer et de gérer votre déploiement, en éliminant le besoin de consoles de gestion distinctes pour gérer la mise à disposition d'applications et de bureaux. Studio offre différents assistants pour vous guider dans le processus de définition de votre environnement, créer des charges de travail pour héberger les applications et bureaux, et attribuer des applications et des bureaux aux utilisateurs. Vous pouvez également utiliser Studio pour allouer et suivre les licences Citrix pour votre site.
Studio obtient les informations qu'il s'affiche depuis le service Broker dans le Controller.

- **Citrix Director** : Director est un outil Web qui permet aux équipes d'assistance et de support informatique de surveiller un environnement, de résoudre les problèmes avant qu'ils ne deviennent critiques pour le système et de réaliser des tâches d'assistance pour les utilisateurs finaux. Vous pouvez utiliser un déploiement Director auquel vous connecter et contrôler plusieurs sites XenApp ou XenDesktop. Director affiche les informations de session et de site à partir de ces sources :

  - Données de session en temps réel à partir du service Broker dans le Controller, qui comprennent des données que le service Broker obtient depuis l'agent broker dans le VDA.
  - Données de site historiques provenant du service Monitoring dans le Controller.
  - Données de trafic HDX (également appelé trafic ICA) capturé par HDX Insight depuis NetScaler, si votre déploiement comprend un boîtier NetScaler et votre édition XenApp ou XenDesktop comprend HDX Insights.

  Vous pouvez également afficher et interagir avec les sessions d'un utilisateur à l'aide de l'Assistance à distance Windows.

- **Serveur de licences Citrix** : le serveur de licences gère les licences de vos produits. Il communique avec le Controller pour gérer les licences pour chaque session utilisateur et avec Studio pour allouer les fichiers de licences. Vous devez créer au moins un serveur de licences pour stocker et gérer vos fichiers de licences.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Hyperviseur** : l'hyperviseur héberge les machines virtuelles dans votre site. Celui-ci peut être la machine virtuelle que vous utilisez pour héberger les applications et les bureaux, ainsi que la machine virtuelle que vous utilisez pour héberger les composants de XenApp et XenDesktop. Un hyperviseur est installé sur un ordinateur hôte entièrement dédié à l'exécution de l'hyperviseur et l'hébergement des machines virtuelles.
  L'hyperviseur Citrix XenServer est inclus avec XenApp et XenDesktop ; vous pouvez utiliser d'autres hyperviseurs pris en charge, tels que Microsoft Hyper-V ou VMware vSphere.

  Bien que de nombreuses implémentations de XenApp et XenDesktop requièrent un hyperviseur, vous n'avez pas besoin de fournir l'accès au PC à distance ou lorsque vous utilisez Provisioning Services (inclus avec certaines éditions de XenApp et XenDesktop) à la place de MCS pour provisionner la machine virtuelle.

Ces composants supplémentaires, non affichés dans le diagramme ci-dessus, peuvent également être inclus dans les déploiements XenApp ou XenDesktop typiques :

- **Provisioning Services** : Provisioning Services est un composant de XenApp et XenDesktop facultatif, disponible dans certaines éditions. Il offre une alternative à MCS pour le provisioning des machines virtuelles. Alors que MCS permet de créer des copies d'une image principale, Provisioning Services livre l'image principale en streaming vers la machine utilisateur. Provisioning Services ne nécessite pas d'hyperviseur pour effectuer cette opération, vous pouvez donc l'utiliser pour héberger des machines physiques. Si Provisioning Services est inclus dans un site, il communique avec le Controller afin de fournir aux utilisateurs des ressources.
- **NetScaler Gateway** : lorsque les utilisateurs se connectent en dehors du pare-feu d'entreprise, cette version peut utiliser la technologie Citrix NetScaler Gateway (anciennement Access Gateway) pour sécuriser les connexions avec le protocole TLS. Le boîtier virtuel NetScaler Gateway ou NetScaler VPX est un boîtier SSL VPN déployé dans la zone démilitarisée (DMZ) pour fournir un point d'accès sécurisé unique via le pare-feu de l'entreprise.
- **Citrix CloudBridge** : dans les déploiements dans lesquels des bureaux virtuels sont mis à disposition auprès des utilisateurs dans des emplacements distants, des succursales par exemple, la technologie Citrix CloudBridge (anciennement Citrix Branch Repeater ou WANScaler) peut être utilisée pour optimiser les performances. Les répéteurs accélèrent les performances sur les réseaux étendus, de sorte que les utilisateurs des succursales bénéficient des performances d'un réseau local sur le réseau étendu. CloudBridge permet de définir des priorités dans l'expérience des utilisateurs, par exemple pour éviter une dégradation des performances au niveau de la succursale en cas d'envoi de fichiers volumineux ou de tâches d'impression importantes sur le réseau. L'optimisation WAN HDX avec CloudBridge assure une compression avec système de jetons et déduplication des données, réduisant considérablement les besoins en bande passante tout en améliorant les performances. Pour plus d'informations, consultez la documentation Citrix CloudBridge.

Configuration et affectation des ressources : catalogues de machines et groupes de mise à disposition

Vous pouvez configurer les ressources que vous souhaitez offrir aux utilisateurs avec des catalogues de machines, mais vous indiquez quels utilisateurs ont accès à ces ressources avec des groupes de mise à disposition.

Catalogues de machines

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Les catalogues de machines sont des collections de machines physiques ou virtuelles que vous gérez comme une seule entité. Ces machines, et les applications ou les bureaux virtuels sur celles-ci, sont les ressources que vous souhaitez mettre à la disposition de vos utilisateurs. Toutes les machines d'un catalogue de machines ont le même système d'exploitation et VDA installé. Elles possèdent également les mêmes applications ou bureaux virtuels disponibles sur ces dernières. En général, vous créez une image principale et vous l'utilisez pour créer des machines virtuelles identiques dans le catalogue. Lorsque vous créez un catalogue de machines, vous spécifiez le type de machine et la méthode de provisioning pour les machines de ce catalogue.

- **Machines avec OS de serveur** : des machines virtuelles ou physiques basées sur le système d'exploitation de serveur utilisé pour mettre à disposition des applications publiées XenApp, également appelées applications hébergées sur un serveur, et les bureaux publiés XenApp, également appelés bureaux hébergés sur un serveur. Ces machines autorisent plusieurs utilisateurs à se connecter à un moment donné.
- **Machines avec OS de bureau** : des machines virtuelles ou physiques basées sur le système d'exploitation de bureau utilisé pour la mise à disposition de bureaux VDI (des bureaux exécutant les systèmes d'exploitation de bureau qui peuvent être complètement personnalisés, en fonction des options que vous choisissez), et d'applications hébergées sur une machine virtuelle (applications provenant de systèmes d'exploitation de bureau), et de bureaux physiques hébergés. Un seul utilisateur à la fois peut se connecter à chacun de ces bureaux.
- **Remote PC Access** : machines utilisateur qui sont incluses dans une liste blanche, permettant aux utilisateurs d'accéder aux ressources sur leurs ordinateurs de bureau à distance, à partir de n'importe quelle machine exécutant Citrix Receiver. Remote PC Access vous permet de gérer l'accès aux PC de bureau via votre déploiement XenDesktop.

Méthodes de provisioning

- **Machine Creation Services (MCS)** : collection de services qui permettent de créer à la demande des bureaux et des serveurs virtuels à partir d'une image principale, d'optimiser l'utilisation du stockage et de fournir une machine virtuelle aux utilisateurs chaque fois qu'ils se connectent. MCS est complètement intégré et administré dans Citrix Studio.
- **Provisioning Services :** permet aux ordinateurs d'être provisionnés et provisionnés à nouveau en temps réel depuis une image disque partagée unique. Provisioning Services vous permet de gérer des machines cibles en tant que collection de machines. Le bureau et les applications sont mis à disposition à partir d'une image vDisk Provisioning Services créée à partir d'une machine cible principale, et qui vous permet de tirer parti de la puissance de traitement du matériel ou des machines virtuelles existant(es). Provisioning Services est géré par le biais de sa propre console.
- **Images existantes :** s'applique à des bureaux et des applications que vous avez déjà fait migrer vers des machines virtuelles dans le centre de données. Vous devez gérer les machines cibles individuellement ou collectivement à l'aide d'outils de distribution logiciel électronique tiers (ESD).

Groupes de mise à disposition

Les groupes de mise à disposition sont des collections d'utilisateurs accédant à un groupe commun de ressources. Les groupes de mise à disposition contiennent les machines de vos catalogues de machines et les utilisateurs Active Directory qui ont accès à votre site. Souvent, il est souhaitable d'attribuer des utilisateurs à vos groupes de mise à disposition en fonction de leur groupe Active Directory, car les groupes Active Directory et les groupes de mise à disposition représentent des modes de regroupement des utilisateurs ayant les mêmes spécifications. Chaque groupe de mise à disposition peut contenir des machines provenant de plusieurs catalogues de machines et chaque catalogue de machines peut contribuer des machines à plus d'un groupe de mise à disposition, mais chaque machine individuelle ne peut appartenir qu'à un seul groupe de mise à disposition à la fois. Vous pouvez configurer un groupe de mise à disposition pour mettre des applications, des bureaux, ou les deux à disposition. Vous définissez les ressources auxquelles les utilisateurs dans le groupe de mise à disposition peuvent accéder. Par exemple, si vous voulez mettre à disposition des applications différentes pour différents utilisateurs, une manière de le faire est d'installer toutes les applications que vous souhaitez mettre à disposition sur l'image

© 1999-2017 Citrix Systems, Inc. All rights reserved.

principale pour un catalogue de machines et créer suffisamment de machines dans ce catalogue à répartir sur plusieurs groupes de mise à disposition. Vous devez ensuite configurer chaque groupe de mise à disposition pour fournir un sous-ensemble différent d'applications installées sur les machines.

Différences entre XenApp/XenDesktop 7.x et XenApp 6.5 et versions précédentes

Si vous êtes familiarisé avec XenApp 6.5 et les versions précédentes de XenApp, il peut être utile de voir les versions 7.x de XenApp et XenDesktop en fonction de la façon dont elles diffèrent de ces versions.

> **REMARQUE :** dans cette section, 7.x fait référence aux versions 7.5 ou ultérieures de XenApp et aux versions 7 ou ultérieures de XenDesktop.

Bien qu'ils ne soient pas totalement équivalents, le tableau suivant permet de mapper des éléments de fonctionnalité de XenApp 6.5 et des versions précédentes de XenApp 7.x et XenDesktop 7.x :

Au lieu de cela, dans XenApp 6.5 et versions antérieures :	Pensez à ceci dans XenApp et XenDesktop 7.x :
Independent Management Architecture (IMA)	FlexCast Management Architecture (FMA)
Batterie	Site
Groupe de tâches	Catalogue de machines Groupe de mise à disposition
Tâche	Virtual Delivery Agent (VDA) Machine avec OS de serveur, VDA avec OS de serveur Machine avec OS de bureau, VDA avec OS de bureau
Machine Services Bureau à distance (RDS) ou Services Terminal Server	Machine avec OS de serveur, VDA avec OS de serveur
Collecteur de zone et de données	Delivery Controller
Delivery Services Console	Citrix Studio et Citrix Director
Publication d'applications	Mise à disposition des applications

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Magasin de données	Base de données
Calculateur de charge	Stratégie de gestion de charge
Administrateur	Administrateur délégué Rôle Étendue

XenApp 7.x et XenDesktop 7.x sont basées sur FlexCast Management Architecture (FMA). FMA est une architecture orientée services qui permet l'interopérabilité et la gestion de modularité sur les technologies Citrix. FMA fournit une plate-forme pour la mise à disposition d'applications, la mobilité, les services, le provisioning flexible et le cloud.

FMA remplace le service IMA (Independent Management Architecture) utilisé dans XenApp 6.5 et versions antérieures.

Ces éléments représentent les éléments clé de FMA en termes de la façon dont ils sont liés aux éléments de XenApp 6.5 et versions précédentes :

- **Sites de mise à disposition :** les batteries sont des objets de niveau supérieur dans XenApp 6.5 et versions antérieures. Dans XenApp 7.x et XenDesktop 7.x, le site représente l'élément de plus haut niveau. Les sites offrent des bureaux et des applications aux groupes d'utilisateurs. FMA requiert que vous vous trouviez dans un domaine pour déployer un site. Par exemple, pour installer les serveurs, votre compte doit disposer des privilèges d'administrateur local et être un utilisateur de domaine dans Active Directory.
- **Catalogues de machines et groupes de mise à disposition :** les machines hébergeant des applications dans XenApp 6.5 et versions précédentes appartenaient à des groupes de tâches pour une gestion efficace des applications et du logiciel serveur. Les administrateurs peuvent gérer toutes les machines d'un groupe de tâches comme une unité unique pour leurs besoins de gestion d'application et d'équilibrage de charge. Des dossiers étaient utilisés pour organiser les applications et les machines. Dans XenApp 7.x et XenDesktop 7.x, vous pouvez utiliser une combinaison de catalogues de machines et de groupes de mise à disposition pour gérer les machines, l'équilibrage de charge et les applications ou les bureaux hébergés. Vous pouvez également utiliser des dossiers d'applications.
- **Virtual Delivery Agents (VDA) :** dans XenApp 6.5 et versions précédentes, les machines de travail des groupes de tâches exécutaient les applications pour l'utilisateur et communiquaient avec les collecteurs de données. Dans XenApp 7.x et XenDesktop 7.x, le VDA communique avec les Delivery Controller qui gèrent les connexions utilisateur.
- **Delivery Controller :** dans XenApp 6.5 et versions précédentes, il existait une zone principale responsable des requêtes de connexion utilisateur et des communications avec les hyperviseurs. Dans XenApp 7.x et XenDesktop 7.x, les Controller du site distribuent et gèrent les demandes de connexion. Dans XenApp 6.5 et versions précédentes, les zones fournies de manière à agréger les serveurs et répliquer des données entre des connexions de réseau étendu. Bien que les zones n'aient pas d'équivalent exact dans XenApp 7.x et XenDesktop 7.x, la fonctionnalité des zones 7.x aide les utilisateurs situés dans des régions éloignées à se connecter à des ressources sans que leurs connexions soient obligées de traverser des segments important de réseau étendu.
- **Citrix Studio et Citrix Director :** utilisez la console Studio pour configurer vos environnements et fournir aux utilisateurs un accès aux applications et aux bureaux. Studio remplace la console Delivery Services Console dans XenApp 6.5 et versions antérieures. Les administrateurs peuvent utiliser Director pour contrôler l'environnement, observer les machines des utilisateurs et résoudre les problèmes informatiques. Pour observer les utilisateurs, l'Assistance à distance Windows doit être activée ; elle est activée par défaut lorsque le VDA est installé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Mise à disposition d'applications** : XenApp 6.5 et versions précédentes utilise l'assistant de publication d'application pour préparer les applications et les mettre à la disposition des utilisateurs. Dans XenApp 7.x et XenDesktop 7.x, vous utilisez Studio pour créer et ajouter des applications afin de les mettre à disposition auprès des utilisateurs qui sont inclus dans un groupe de mise à disposition. À l'aide de Studio, vous devez tout d'abord configurer un site, créer et spécifier des catalogues de machines, puis créer des groupes de mise à disposition qui utilisent les machines de ces catalogues. Les groupes de mise à disposition déterminent quels utilisateurs ont accès aux applications que vous mettez à disposition.
- **Base de données** : XenApp 7.x et XenDesktop 7.x n'utilisent pas le magasin de données IMA pour obtenir des informations de configuration. Ils utilisent une base de données Microsoft SQL Server pour stocker les informations de configuration et de session.
- **Stratégie de gestion de charge** : dans XenApp 6.5 et versions précédentes, les calculateurs de charge utilisent des mesures prédéfinies pour déterminer la charge sur une machine. Les connexions utilisateur peuvent être associées aux machines possédant moins de charge. Dans XenApp 7.x et XenDesktop 7.x, utilisez les stratégies de gestion de la charge pour l'équilibrage de charge entre les machines.
- **Administration déléguée** : dans XenApp 6.5 et versions précédentes, vous pouvez créer des administrateurs personnalisés et leur attribuer des autorisations basées sur des dossiers et des objets. Dans XenApp 7.x et XenDesktop 7.x, les administrateurs personnalisés sont basés sur des rôles et des paires d'étendues. Un rôle représente une fonction de tâche et possède des permissions définies qui lui sont associées afin de permettre la délégation. Une étendue représente une collection d'objets. Les rôles d'administrateur intégré possèdent des ensembles de permissions spécifiques, tels que l'assistance technique, des applications, l'hébergement et les catalogues. Par exemple, les administrateurs de bureaux d'assistance ne peuvent fonctionner qu'avec des utilisateurs individuels sur des sites spécifiques, alors que les administrateurs complets peuvent contrôler la totalité du déploiement et résoudre les problèmes du service informatique.

La transition vers FMA signifie également que certaines fonctionnalités disponibles dans XenApp 6.5 et versions précédentes sont implémentées différemment ou nécessitent que vous utilisiez d'autres fonctionnalités, composants, ou outils pour obtenir les mêmes objectifs.

Au lieu de cela, dans XenApp 6.5 et versions antérieures :	Utilisez ceci dans XenApp et XenDesktop 7.x :
Pré-lancement de session et persistance de session configurées avec des paramètres de stratégie	Le pré-lancement de session et la persistance de session sont configurés en modifiant les paramètres du groupe de mise à disposition. Comme dans XenApp 6.5, ces fonctionnalités permettent aux utilisateurs de se connecter à des applications plus rapidement, en démarrant des sessions avant qu'elles ne soient requises (pré-lancement de session) et en gardant les sessions actives après qu'un utilisateur ferme toutes les applications (persistance de session). Dans XenApp 7.x et XenDesktop 7.x, vous activez ces fonctionnalités pour les utilisateurs spécifiés en configurant ces paramètres pour les groupes de mise à disposition existants. Consultez la section Configurer le pré-lancement de session et la persistance de session.
Prise en charge des utilisateurs non authentifiés (anonymes) fournie lors de l'octroi de droits à l'utilisateur	Prise en charge des utilisateurs non authentifiés (anonymes) fournie par la configuration de cette option lors de la définition des propriétés de l'utilisateur d'un groupe de mise à disposition. Consultez la section Utilisateurs.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

anonyme lors de la définition des propriétés des applications publiées	
Le cache d'hôte local permet à un serveur de tâches de fonctionner même lorsqu'une connexion au magasin de données n'est pas disponible	La location de connexion permet aux utilisateurs de se connecter et de se reconnecter à leurs applications et bureaux les plus récemment utilisés, même lorsque la base de données du site n'est pas disponible. La fonctionnalité de location de connexion complète les meilleures pratiques de de haute disponibilité de SQL Server. Consultez la section Location de connexion.
Streaming d'application	App-V met à disposition des applications livrées en streaming, gérées à l'aide de Studio.
Interface Web	Citrix vous recommande d'effectuer la transition vers StoreFront.
SmartAuditor	Utilisez l'enregistrement de session. Vous pouvez également utiliser la journalisation de la configuration pour consigner toutes les activités de session d'un point de vue administratif.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Active Directory

Jul 07, 2016

Active Directory est requis pour l'authentification et l'autorisation. L'infrastructure Kerberos dans Active Directory est utilisée pour garantir l'authenticité et la confidentialité des communications avec les Delivery Controller. Pour de plus amples informations sur Kerberos, veuillez consulter la documentation Microsoft.

L'article Configuration système requise répertorie les niveaux fonctionnels pris en charge de la forêt et du domaine. Pour utiliser la modélisation de stratégie, le contrôleur de domaine doit s'exécuter sur Windows Server 2003 à Windows Server 2012 R2 ; cela n'affecte pas le niveau fonctionnel du domaine.

Ce produit prend en charge ce qui suit :

- Déploiements dans lesquels les comptes d'utilisateurs et les comptes d'ordinateurs existent dans les domaines d'une forêt Active Directory unique. Les comptes d'utilisateurs et d'ordinateurs peuvent exister dans des domaines arbitraires d'une forêt unique. Tous les niveaux fonctionnels de domaine et de forêt sont pris en charge dans ce type de déploiement.
- Déploiements dans lesquels les comptes d'utilisateurs existent dans une forêt Active Directory qui est différente de celle contenant les comptes d'ordinateurs des contrôleurs et des bureaux virtuels. Dans ce type de déploiement, les domaines contenant les comptes d'ordinateurs des contrôleurs et des bureaux virtuels doivent établir l'approbation des domaines dans lesquels figurent les comptes d'utilisateurs. Des approbations de forêt ou des approbations externes peuvent être utilisées. Tous les niveaux fonctionnels de domaine et de forêt sont pris en charge dans ce type de déploiement.
- Déploiements dans lesquels les comptes d'ordinateurs des contrôleurs figurent dans une forêt Active Directory différente d'une ou de plusieurs forêts Active Directory supplémentaires contenant les comptes d'ordinateurs des bureaux virtuels. Dans ce type de déploiement, une approbation bilatérale doit exister entre les domaines contenant les comptes d'ordinateurs des contrôleurs et l'ensemble des domaines contenant les comptes d'ordinateurs des bureaux virtuels. Dans ce type de déploiement, tous les domaines contenant les comptes d'ordinateurs des contrôleurs ou des bureaux virtuels doivent figurer au niveau fonctionnel « natif de Windows 2000 » ou supérieur. Tous les niveaux fonctionnels de forêt sont pris en charge.
- Contrôleurs de domaine accessibles en écriture. Les contrôleurs de domaine en lecture seule ne sont pas pris en charge.

Facultativement, les VDA (Virtual Delivery Agents) peuvent utiliser des informations publiées dans Active Directory pour déterminer les Controller avec lesquels ils peuvent s'enregistrer (découverte). Cette méthode est principalement prise en charge pour la rétrocompatibilité, et est uniquement disponible si les VDA se trouvent dans la même forêt Active Directory que les Controller. Pour de plus amples informations sur cette méthode de découverte, veuillez consulter les articles Delivery Controller et CTX118976.

Conseil : ne modifiez pas le nom de l'ordinateur ou l'appartenance à un domaine d'un Controller une fois que le site est configuré.

Remarque : ces informations s'appliquent à XenDesktop 7.1 et XenDesktop 7.5 (versions minimum). Elles ne s'appliquent pas aux versions antérieures de XenDesktop ou XenApp.
Dans un environnement Active Directory avec plusieurs forêts, si des approbations à sens unique ou bidirectionnelles sont en place, vous pouvez utiliser les redirecteurs DNS pour la recherche de nom et l'enregistrement. Pour autoriser les utilisateurs Active Directory appropriés à créer des comptes d'ordinateurs, utilisez l'Assistant Délégation de contrôle. Référez-vous à la documentation Microsoft pour plus d'informations sur cet assistant.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Aucune zone DNS inversée n'est nécessaire dans l'infrastructure DNS si des redirecteurs DNS appropriés sont en place entre les forêts.

La clé SupportMultipleForest n'est nécessaire que si le VDA et le Controller se trouvent dans des forêts différentes que les noms Active Directory et NetBios soient différents ou non. La clé SupportMultipleForest est uniquement nécessaire sur le VDA. Utilisez les informations suivantes pour ajouter la clé de registre :
Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

- HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest
  - Nom : SupportMultipleForest
  - Type : REG_DWORD
  - Données : 0x00000001 (1)

Vous aurez peut-être besoin d'utiliser une configuration DNS inversée si l'espace de noms DNS est différent de celui d'Active Directory.

Si des approbations externes sont en place au cours de l'installation, la clé de registre ListOfSIDs est requise. La clé de registre ListOfSIDs est également nécessaire si le nom de domaine complet (FQDN) Active Directory est différent du FQDN DNS ou si le domaine contenant le contrôleur de domaine porte un nom NetBIOS autre que le FQDN Active Directory. Pour ajouter la clé de registre, utilisez les informations suivantes :

- Pour un VDA 32 bits ou 64 bits, accédez à la clé de registre : HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs
  - Nom : ListOfSIDs
  - type : REG_SZ
  - Données : identificateur de sécurité (SID) des Controller

Lorsque des approbations externes sont en place, apportez les modifications suivantes sur le VDA :

1. Recherchez le fichier \Citrix\Virtual Desktop Agent\brokeragentconfig.exe.config
2. Créez une copie de sauvegarde du fichier.
3. Ouvrez le fichier dans un éditeur de texte tel que le Bloc-notes.
4. Recherchez le texte allowNtlm="false" et modifiez le texte en allowNtlm="true".
5. Enregistrez le fichier.

Après l'ajout de la clé de registre ListOfSIDs et la modification du fichier brokeragent.exe.config, redémarrez le service Citrix Desktop pour appliquer les modifications.

Le tableau suivant dresse la liste des types de prise en charge de l'approbation :

Type d'approbation	Transitivité	Direction	Pris en charge dans cette version
Parent et enfant	Transitive	Bidirectionnelle	Oui
Racine d'arborescence	Transitive	Bidirectionnelle	Oui
Externe	Non transitive	Unidirectionnelle ou bidirectionnelle	Oui

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Type d'approbation	Transitivité	Direction	Pris en charge dans cette version
Forêt	Transitive	Unidirectionnelle ou bidirectionnelle	Oui
Raccourci	Transitive	Unidirectionnelle ou bidirectionnelle	Oui
Domaine	Transitive ou non transitive	Unidirectionnelle ou bidirectionnelle	Non

Pour de plus amples informations sur les environnements Active Directory complexes, consultez l'article CTX134971.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Bases de données

Jul 15, 2016

Un site XenApp ou XenDesktop utilise trois bases de données SQL Server :

- **Site** : (également appelé Configuration de site) stocke les données de configuration du site, ainsi que les informations sur l'état de la session et la connexion.
- **Journalisation de la configuration** : (également appelée Journalisation) stocke des informations sur les modifications apportées à la configuration du site et les activités administratives. Cette base de données est utilisée lorsque la fonction Journalisation de la configuration est activée (valeur par défaut=activée).
- **Contrôle** : stocke les données utilisées par Director, telles que les informations de session et de connexion.

Chaque Controller communique avec la base de données du site ; l'authentification Windows est requise entre le Controller et les bases de données. Il est possible de déconnecter un Controller ou de le mettre hors tension sans affecter les autres Controller du site. L'unique point de défaillance reste par conséquent la base de données. Si le serveur de base de données échoue, les connexions existantes continuent de fonctionner jusqu'à ce que l'utilisateur ferme sa session ou se déconnecte. Si le serveur de la base de données est indisponible, aucune nouvelle connexion ne peut être établie, sauf dans certains cas si la location de connexion est configurée.

Citrix vous recommande de sauvegarder régulièrement les bases de données afin de pouvoir la restaurer en cas de défaillance du serveur de base de données. La stratégie de sauvegarde pour chaque base de données peut différer. Pour obtenir des instructions, consultez l'article CTX135207.

Si votre site contient plus d'une zone, la base de données du site doit toujours se trouver dans la zone principale. Les Controller de chaque zone communiquent avec cette base de données.

Haute disponibilité

Il existe trois solutions de haute disponibilité à considérer pour garantir le basculement automatique :

- **Groupes de disponibilité AlwaysOn** : cette solution à haute disponibilité et reprise après sinistre introduite dans SQL Server 2012 vous permet d'optimiser la disponibilité pour une ou plusieurs bases de données. Les Groupes de disponibilité AlwaysOn nécessitent que les instances SQL Server résident les nœuds WSFC (Windows Server Failover Clustering). Pour de plus amples informations, consultez l'article http://msdn.microsoft.com/en-us/library/hh510230.
- **Mise en miroir de la base de données SQL Server** : la mise en miroir de la base de données garantit qu'en cas d'indisponibilité soudaine du serveur de base de données actif, le basculement automatique se produit au bout de quelques secondes seulement, évitant généralement toute gêne pour les utilisateurs. Cette méthode est plus coûteuse que d'autres solutions car les licences complètes de SQL Server sont requises sur chaque serveur de base de données ; vous ne pouvez pas utiliser SQL Server édition Express pour un environnement de mise en miroir.
- **Mise en cluster SQL** : la technologie de mise en cluster SQL de Microsoft peut être utilisée pour permettre à un serveur d'assurer automatiquement la reprise des tâches et des responsabilités d'un autre serveur en échec. Toutefois, cette solution est plus complexe à mettre en place et le basculement automatique est généralement plus lent qu'avec les autres méthodes, comme la mise en miroir SQL.
- **À l'aide des fonctionnalités de haute disponibilité de l'hyperviseur** : avec cette méthode, vous déployez la base de données en tant que machine virtuelle et utilisez les fonctions de haute disponibilité de votre hyperviseur. Cette solution est moins coûteuse que la mise en miroir du fait qu'elle utilise votre logiciel d'hyperviseur et que vous pouvez

© 1999-2017 Citrix Systems, Inc. All rights reserved.

également utiliser l'édition SQL Server Express. Cependant, le processus de basculement automatique est plus lent car il faut un certain temps pour qu'une nouvelle machine démarre pour la base de données, avec le risque d'interrompre le service fourni aux utilisateurs.

Remarque : l'installation d'un Controller sur un nœud dans une installation de mise en cluster SQL ou mise en miroir SQL n'est pas prise en charge.

La fonctionnalité de location de connexion complète les meilleures pratiques de la haute disponibilité du serveur SQL Server en permettant aux utilisateurs de se connecter et de se reconnecter à leurs applications et bureaux les plus récemment utilisés, même lorsque la base de données du site n'est pas disponible. Pour plus d'informations, veuillez consulter l'article *Location de connexion*.

Si tous les Controller d'un site échouent, vous pouvez configurer les VDA pour fonctionner en mode haute disponibilité de sorte à ce que les utilisateurs puissent continuer à accéder à leurs bureaux et applications et les utiliser. En mode haute disponibilité, le VDA accepte des connexions ICA directes provenant des utilisateurs, plutôt que des connexions négociées par le Controller. Cette fonctionnalité n'est à utiliser que lors de rares occasions lorsque les communications avec tous les Controller échouent ; cela ne constitue pas une alternative aux autres solutions de haute disponibilité. Pour plus d'informations, veuillez consulter l'article CTX127564.

Installer le logiciel de base de données

Par défaut, l'édition SQL Server Express est installée lorsque vous installez le premier Delivery Controller, si une autre instance SQL Server n'est pas détectée sur ce serveur. Cette installation par défaut est généralement suffisante pour les déploiements de preuve de concept ou de pilote ; cependant, SQL Server Express ne prend pas en charge les fonctionnalités de haute disponibilité de Microsoft.

Cette installation utilise les comptes de service et autorisations Windows par défaut. Reportez-vous à la documentation Microsoft pour de plus amples informations sur ces défauts, y compris l'ajout de comptes de service Windows au rôle sysadmin. Le Controller utilise le compte de service réseau de cette configuration. Le Controller ne requiert aucun rôle ni autorisation SQL Server supplémentaire.

Le cas échéant, vous pouvez sélectionner **Masquer l'instance** pour l'instance de base de données. Lors de la configuration de l'adresse de la base de données dans Studio, entrez le numéro de port statique de l'instance plutôt que son nom. Reportez-vous à la documentation Microsoft pour de plus amples informations sur le masquage d'une instance du moteur de base de données SQL Server.

La plupart des déploiements de production, et tout déploiement qui utilise les fonctionnalités de haute disponibilité de Microsoft, devraient utiliser des éditions non-Express prises en charge de SQL Server installées sur des machines autres que le serveur sur lequel le premier Delivery Controller est installé. L'article Configuration système requise répertorie les versions prises en charge de SQL Server. Les bases de données peuvent résider sur une ou plusieurs machines.

Assurez-vous que le logiciel SQL Server est installé avant de créer un site. Vous n'avez pas besoin de créer la base de données, mais si vous le faites, elle doit être vide. La configuration de technologies haute disponibilité de Microsoft est également recommandée.

Utilisez Windows Update pour conserver SQL Server à jour.

Configurer les bases de données à partir de l'assistant

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de création de site

Indiquez le nom et l'adresse des bases de données (emplacement) sur la page **Bases de données** dans l'assistant de création de site ; consultez la section *Formats d'adresse de base de données* ci-dessous. Pour éviter des erreurs lorsque Director interroge le service Monitor, n'utilisez pas d'espaces dans le nom de la base de données de contrôle.

La page **Bases de données** offre deux options pour configurer les bases de données : automatiquement et à l'aide de scripts. En général, vous pouvez utiliser l'option automatique si vous (utilisateur de Studio et administrateur de Citrix) disposez des privilèges de base de données requis ; veuillez consulter la section Autorisations requises pour configurer les bases de données ci-dessous.

Vous pouvez modifier l'emplacement de la base de données plus tard, après avoir créé le site ; consultez la section *Modifier l'emplacement des bases de données* ci-dessous.

Pour configurer un site pour utiliser une base de données mise en miroir, effectuez les étapes suivantes, puis passez à la procédure de configuration automatique ou à l'aide d'un script.

1. Installez le logiciel SQL Server sur deux serveurs, A et B
2. Sur le serveur A, créez la base de données destinée à être utilisée comme base de données principale. Sauvegardez la base de données sur le serveur A, puis copiez-la sur le serveur B.
3. Sur le serveur B, restaurez le fichier de sauvegarde.
4. Démarrez la mise en miroir sur le serveur A.

Conseil : pour vérifier la mise en miroir après la création du site, exécutez le cmdlet PowerShell **get-configdbconnection** pour vous assurer que le partenaire de basculement a été défini dans la chaîne de connexion pour le miroir.

Si vous ajoutez, déplacez ou supprimez un Delivery Controller dans un environnement de base de données mise en miroir ultérieurement, consultez l'article Delivery Controller.

Si vous possédez les privilèges de base de données requis, sélectionnez l'option Créer et configurer les bases de données à partir de Studio sur la page **Bases de données** de l'assistant de création de site, puis fournissez les noms et adresses des bases de données principales.

Si une base de données existe sur une adresse spécifiée, elle doit être vide. Si les bases de données n'existent pas sur une adresse spécifiée, vous êtes informé qu'aucune base de données n'a été détectée, puis vous êtes invité à indiquer si vous souhaitez que la base de données soit créée pour vous. Lorsque vous confirmez, Studio crée automatiquement les bases de données, le cas échéant, puis applique les scripts d'initialisation pour les bases de données principales et les copies.

Si vous ne disposez pas des privilèges de base de données requis, un utilisateur avec ces autorisations, tel qu'un administrateur de base de données, doit vous aider. Voici la séquence :

1. Dans l'assistant de création de site, sélectionnez l'option **Générer des scripts**. Six scripts sont générés : deux pour chacune des trois de bases de données, une pour chaque base de données principale et une autre pour chaque copie. Vous pouvez indiquer l'emplacement de stockage des scripts.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Donnez ces scripts à votre administrateur de base de données. L'assistant de création de site s'arrête automatiquement à ce stade ; vous serez invité lorsque vous y reviendrez plus tard à continuer la création de site.

L'administrateur de base de données crée alors les bases de données. Chaque base de données doit présenter les caractéristiques suivantes :

- Utilisez un classement qui se termine par « _CI_AS_KS ». Citrix vous recommande d'utiliser un classement qui se termine par « _100_CI_AS_KS ».
- Pour des performances optimales, activez l'option Capture instantanée Read Committed de SQL Server. Pour plus d'informations, veuillez consulter l'article CTX 137161.
- Les fonctionnalités haute disponibilité doivent être configurées, le cas échéant.
- Pour configurer la mise en miroir, vous devez tout d'abord définir la base de données pour utiliser le modèle de récupération complet (le modèle simple est la valeur par défaut). Sauvegardez la base de données principale dans un fichier et copiez-la sur le serveur miroir. Sur la base de données miroir, restaurez le fichier de sauvegarde sur le serveur miroir. Ensuite, démarrez la mise en miroir sur le serveur principal.

L'administrateur de base de données utilise l'utilitaire de ligne de commande SQLCMD ou SQL Server Management Studio dans le mode SQLCMD pour exécuter chacun des scripts xxx_Replica.sql sur les instances de base de données SQL Server haute disponibilité (si la haute disponibilité est configurée), puis exécute chacun des scripts xxx_Principal.sql sur les instances de base de données SQL Server principales. Consultez la documentation Microsoft sur SQLCMD pour plus de détails.

Lorsque tous les scripts sont terminés, l'administrateur de la base de données donne à l'administrateur Citrix les trois adresses de base de données principale.

Dans Studio, vous serez invité à continuer la création de site et renvoyé à la page **Bases de données**. Entrez les adresses. Si l'un des serveurs hébergeant une base de données ne peut pas être contacté, un message d'erreur s'affiche.

Autorisations requises pour configurer les bases de données

Vous devez être un administrateur local et un utilisateur du domaine pour créer et initialiser les bases de données (ou modifier l'emplacement de la base de données). Vous devez également disposer de certaines autorisations SQL Server. Les autorisations suivantes peuvent être explicitement configurées ou acquises par l'appartenance à un groupe Active Directory. Si vos informations d'identification d'utilisateur Studio ne comprennent pas ces autorisations, vous êtes invité à entrer les informations d'identification d'utilisateur SQL Server.

Opération	Objectif	Rôle de serveur	Rôle de base de données
Créer une base de données	Créer une base de données vide appropriée	dbcreator	
Créer un schéma	Créer tous les schémas spécifiques au service et ajouter le premier Controller au site	securityadmin *	db_owner

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ajouter un Controller	Ajouter un Controller (autre que le premier) au site	securityadmin *	db_owner
Ajouter un Controller (serveur miroir)	Ajouter une connexion Controller au serveur de base de données assumant actuellement le rôle de miroir d'une base de données en miroir	securityadmin *	
Mettre à jour un schéma	Appliquer les mises à jour ou correctifs au schéma		db_owner

* Bien qu'il soit plus restrictif techniquement, en pratique, le rôle de serveur securityadmin doit être considéré comme équivalent au rôle de serveur sysadmin.

Lorsque vous utilisez Studio pour effectuer ces opérations, le compte d'utilisateur doit être un membre du rôle de serveur sysadmin.

Formats d'adresse de base de données

Vous pouvez spécifier une adresse de base de données dans l'un des formats suivants :

- NomServeur
- NomServeur\NomInstance
- NomServeur,NuméroPort

Pour un groupe de disponibilité AlwaysOn, spécifiez l'écouteur du groupe dans le champ d'emplacement.

Modifier l'emplacement des bases de données

Une fois que vous avez créé un site, vous pouvez modifier l'emplacement des bases de données. Lorsque vous modifiez l'emplacement d'une base de données :

- Les données provenant de la base de données précédente ne sont pas importées vers la nouvelle base de données.
- Les journaux ne peuvent pas être regroupés pour les deux bases de données lors de la récupération des journaux.
- La première entrée du journal dans la nouvelle base de données indique qu'une modification a été apportée dans une base de données, mais elle n'identifie pas la base de données précédente.

Vous ne pouvez pas modifier l'emplacement de la base de données de journalisation de la configuration lorsque la journalisation obligatoire est activée.

Pour modifier l'emplacement d'une base de données :

1. Assurez-vous qu'une version prise en charge de Microsoft SQL Server est installée sur le serveur sur lequel vous souhaitez que la base de données réside. Configurez les fonctionnalités de haute disponibilité en fonction de vos besoins.
2. Sélectionnez **Configuration** dans le volet de navigation Studio.
3. Sélectionnez la base de données pour laquelle vous souhaitez spécifier un autre emplacement, puis

© 1999-2017 Citrix Systems, Inc. All rights reserved.

sélectionnez **Modifier la base de données** dans le volet Actions.

4. Spécifiez le nouvel emplacement et le nom de la base de données.
5. Si vous souhaitez que Studio crée la base de données et que vous possédez les autorisations appropriées, cliquez sur **OK**. Lorsque vous y êtes invité, cliquez sur **OK** et Studio va créer la base de données automatiquement. Studio tente d'accéder à la base de données à l'aide de vos informations d'identification ; si la tentative échoue, vous êtes invité à entrer les informations d'identification de l'utilisateur de la base de données. Studio télécharge ensuite le schéma de base de données vers la base de données. Les informations d'identification ne sont conservées que durant la création de la base de données.
6. Si vous ne souhaitez pas que Studio crée la base de données, ou si vous ne disposez pas des autorisations suffisantes, cliquez sur **Générer script**. Les scripts générés contiennent des instructions permettant de créer manuellement la base de données et une base de données miroir, si nécessaire. Avant le chargement du schéma, assurez-vous que la base de données est vide et qu'au moins un utilisateur est autorisé à accéder et modifier la base de données.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Méthodes de mise à disposition

Jul 07, 2016

Il est difficile de répondre aux besoins de chaque utilisateur avec un déploiement de virtualisation. XenApp et XenDesktop permettent aux administrateurs de personnaliser l'expérience de l'utilisateur avec une variété de méthodes parfois appelées modèles FlexCast.

Cette collection de méthodes de mise à disposition, chacune avec ses propres avantages et inconvénients respectifs : fournit la meilleure expérience utilisateur dans un scénario au cas par cas.

Les périphériques à écran tactile, tels que les tablettes et les smartphones, sont maintenant standard en mobilité. Ces périphériques peuvent entraîner des problèmes lors de l'exécution d'applications Windows qui utilisent les écrans en plein écran et s'appuient sur les entrées utilisant le bouton droit de la souris pour une fonctionnalité totale.

XenApp avec Citrix Receiver offre une solution sécurisée qui permet aux utilisateurs de périphériques mobiles un accès à toutes les fonctionnalités dans leurs applications Windows sans le coût de réécriture de ces applications pour les plateformes mobiles natives.

La méthode de mise à disposition des applications publiées XenApp utilise la technologie HDX Mobile qui résout les problèmes associés à la mobilisation des applications Windows. Cette méthode permet aux applications Windows d'être restructurées pour une expérience tactile tout en gérant des fonctionnalités telles que les gestes multitouch, les commandes de menu natif et GPS, la caméra et les fonctions GPS. De nombreuses fonctions tactiles sont disponibles en mode natif dans XenApp et XenDesktop et ne requièrent aucune activation des modifications du code source de l'application.

Ces fonctionnalités comprennent :

- Affichage automatique du clavier de l'appareil lorsqu'un champ modifiable est actif
- Plus grand contrôle de sélecteur pour remplacer le contrôle de la zone combinée Windows
- Gestes multitouch, comme l'action de pincer et de zoom
- Défilement lié à l'inertie
- Navigation via touchpad ou directement via le curseur

La mise à niveau des machines physiques est une tâche difficile à laquelle de nombreuses entreprises doivent faire face tous les trois à cinq ans, spécialement si votre entreprise doit gérer les versions les plus récentes des systèmes d'exploitation et des applications. Les entreprises en croissance font également face à des frais généraux impressionnants d'ajout de nouvelles machines à leur réseau.

La méthode de mise à disposition VDI Personal vDisk offre des systèmes d'exploitation de bureaux complètement personnalisés à des utilisateurs uniques sur n'importe quelle machine ou client fin utilisant des ressources serveur. Les administrateurs peuvent créer des machines virtuelles dont les ressources, tels que le traitement, la mémoire et le stockage, sont stockés dans le centre de données du réseau.

Cela peut prolonger la durée de vie des machines plus anciennes, permettre de garder le logiciel à jour, et réduire les temps d'arrêt lors des mises à niveau.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

La sécurité du réseau est un problème grandissant, plus particulièrement lorsque vous travaillez avec les fournisseurs, partenaires et autres travailleurs de contingent tiers qui nécessitent un accès aux applications et données d'une entreprise. Il se peut que les utilisateurs nécessitent également des ordinateurs portables ou autres périphériques en prêt, ce qui entraîne des problèmes de coût supplémentaires.

Les données, applications et bureaux sont stockés derrière le pare-feu du réseau sécurisé avec XenDesktop et XenApp, et la seule chose transmise par l'utilisateur final correspond à des entrées et sorties effectuées sur le périphérique utilisateur, telles que les frappes clavier, des clics souris, et des mises à jour audio et de l'écran. En effectuant la gestion de ces ressources dans un centre de données, XenDesktop et XenApp offre une solution d'accès à distance plus sécurisée que d'utiliser VPN SSL typique.

Avec un déploiement VDI avec Personal vDisk, les administrateurs peuvent utiliser des clients légers ou des périphériques personnels utilisateurs en créant une machine virtuelle sur un serveur réseau et en fournissant un système d'exploitation de bureau mono-utilisateur. Ceci permet au département informatique de maintenir la sécurité des travailleurs tiers sans devoir acquérir d'équipement coûteux.

Lors du basculement vers un nouveau système d'exploitation, le service informatique peut faire face à un test de mise à disposition d'applications d'ancienne génération et non compatibles.

Avec les applications hébergées sur des machines virtuelles, les utilisateurs peuvent exécuter des applications plus anciennes par le biais de Citrix Receiver sur la machine virtuelle mise à niveau sans aucun problème de compatibilité. Ceci laisse au service informatique du temps supplémentaire pour résoudre et tester les problèmes de compatibilité, faciliter la transition des utilisateurs et rendre plus efficace les appels au service d'assistance.

Les autres avantages de l'utilisation de XenDesktop pendant la migration comprennent :

- La réduction de la complexité des bureaux
- L'amélioration du contrôle informatique
- L'amélioration de la flexibilité de l'utilisateur en termes de l'utilisation des périphériques et l'emplacement de l'espace de travail

De nombreuses entreprises de conception et de fabrication reposent fortement sur des applications graphiques 3D professionnelles. Ces entreprises font face à des contraintes financières découlant de coûts matériel élevés pour prendre en charge ce type de logiciel ainsi que les problèmes logistiques qui se produisent éventuellement avec le partage de fichiers de conception importants via FTP, e-mail et des méthodes similaires appropriées.

La méthode de mise à disposition du bureau physique hébergé de XenDesktop offre une seule image de bureau aux stations de travail et aux serveurs lames, sans que des hyperviseurs aient à exécuter d'applications 3D gourmandes en graphiques sur un système d'exploitation natif.

Tous les fichiers sont enregistrés dans un centre de données central au sein du réseau, ainsi le partage de fichiers volumineux avec d'autres utilisateurs du réseau est plus rapide et plus sécurisé car les fichiers ne sont pas transférés d'une station de travail à une autre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Les entreprises nécessitant des centres d'appel à grande échelle font face à des difficultés à grande échelle de gestion de personnel adéquate lors des périodes de pointe tout en n'effectuant de provisioning supplémentaire des machines lors des heures creuses.

La méthode de mise à disposition VDI regroupés fournit l'accès à un bureau standard à plusieurs utilisateurs de manière dynamique à un coût minimum lors du provisioning d'un grand nombre d'utilisateurs. Les machines regroupées sont attribuées session par session, premier arrivé, premier servi.

La gestion quotidienne de ces machines virtuelles est allégée, car toute modification effectuée au cours de la session est supprimée lorsque l'utilisateur ferme sa session. Cela augmente également la sécurité.

La méthode de mise à disposition des bureaux hébergés XenApp est une autre option viable de transformation des centres d'appels. Cette méthode héberge de multiples bureaux utilisateur sur un seul système d'exploitation de serveur.

Cette méthode est plus rentable que VDI regroupés, mais avec les bureaux hébergés XenApp, les utilisateurs sont restreints à l'installation d'applications, à la modification des paramètres système et au démarrage du serveur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Applications et bureaux publiés XenApp

Jul 07, 2016

Utilisez les machines avec OS de serveur pour mettre à disposition des applications publiées XenApp et des bureaux publiés.

Cas d'utilisation

- Une mise à disposition peu onéreuse sur le serveur pour réduire le coût de mise à disposition des applications pour un grand nombre d'utilisateurs, tout en offrant une expérience utilisateur haute définition en toute sécurité.
- Vos utilisateurs effectuent des tâches clairement définies, et qui ne requièrent aucune personnalisation ou accès en mode déconnecté aux applications. Les utilisateurs peuvent inclure les travailleurs productifs, tels que des opérateurs de centre d'appel et des travailleurs au détail, ou des utilisateurs qui partagent des stations de travail.
- Types d'application : toute application.

Avantages et considérations

- Solution gérable et évolutive dans votre centre de données.
- Solution de mise à disposition des applications la moins onéreuse.
- Les applications hébergées sont gérées de manière centralisée et les utilisateurs ne peuvent pas modifier l'application, offrant une expérience utilisateur cohérente, sécurisée et fiable.
- Les utilisateurs doivent être en ligne pour accéder à leurs applications.

Expérience utilisateur

- L'utilisateur demande une ou plusieurs applications depuis StoreFront, leur menu Démarrer ou une adresse URL que vous leur fournissez.
- Les applications sont mises à disposition virtuellement et s'affichent en toute transparence en haute définition sur les machines utilisateur.
- En fonction des paramètres de profil, les modifications apportées par l'utilisateur sont enregistrées lorsque la session applicative de l'utilisateur prend fin. Sinon, les modifications sont supprimées.

Traiter, héberger et mettre à disposition des applications

- Le traitement de l'application a lieu sur les machines hôtes, plutôt que sur les machines utilisateur. La machine hôte peut être une machine physique ou virtuelle.
- Les applications et les bureaux résident sur une machine équipée d'un système d'exploitation serveur.
- Les machines deviennent disponibles au travers des catalogues de machines.
- Les machines présentes dans des catalogues de machines sont organisées en groupes de mise à disposition qui mettent à disposition le même ensemble d'applications vers des groupes d'utilisateurs.
- Les machines avec système d'exploitation serveur prennent en charge les groupes de mise à disposition qui hébergent des applications ou bureaux, ou les deux.

Gestion et attribution de sessions

- Les machines équipées d'un système d'exploitation serveur exécutent plusieurs sessions à partir d'une seule machine pour mettre à disposition plusieurs applications et bureaux vers de multiples utilisateurs connectés simultanément. Chaque utilisateur requiert une seule session depuis laquelle ils peuvent exécuter toutes leurs applications hébergées.

  Par exemple, un utilisateur ouvre une session et requiert une application. Une session sur cette machine devient

© 1999-2017 Citrix Systems, Inc. All rights reserved.

indisponible pour d'autres utilisateurs. Un second utilisateur ouvre une session et requiert une application que cette machine héberge. Une seconde session sur la même machine est maintenant disponible. Si les deux utilisateurs demandent des applications supplémentaires, aucune des sessions supplémentaires n'est requise, car un utilisateur peut exécuter de multiples applications à l'aide de la même session. Si deux utilisateurs ou plus ouvrent une session et demandent des bureaux, et deux sessions sont disponibles sur la même machine, cette machine unique utilise maintenant quatre sessions pour héberger quatre utilisateurs différents.

- Dans le groupe de mise à disposition auquel un utilisateur est attribué, une machine sur le serveur le moins chargé est sélectionnée. Une machine avec une session de disponibilité est attribuée de manière aléatoire pour mettre à disposition les applications à un utilisateur lorsque ce dernier ouvre une session.

Pour mettre à disposition des applications et bureaux publiés XenApp :

1. Installez les applications que vous souhaitez mettre à disposition sur une image principale exécutant un système d'exploitation de serveur Windows pris en charge.
2. Créez un catalogue de machines pour cette image principale ou mettre à jour un catalogue existant avec l'image principale.
3. Créez un groupe de mise à disposition pour mettre à disposition les applications et bureaux auprès des utilisateurs. Si vous effectuez la mise à disposition d'applications, sélectionnez les applications que vous souhaitez mettre à disposition.

Veuillez consulter les articles de configuration et d'installation pour plus de détails.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VM hosted Apps

Jul 07, 2016

Utilisez les machines avec OS de bureau pour mettre à disposition des applications hébergées sur une machine virtuelle.

Cas d'utilisation

- Vous recherchez une solution de mise à disposition d'applications basée sur client qui soit sécurisée, offre une gestion centralisée et prenne en charge un grand nombre d'utilisateurs par serveur hôte (ou hyperviseur), tout en offrant aux utilisateurs des applications qui s'affichent en haute définition.
- Vos utilisateurs sont des sous-traitants internes ou externes, des collaborateurs tiers et autres membres d'équipe provisoire. Vos utilisateurs ne requièrent aucun accès à des applications hébergées en mode déconnecté.
- Types d'application : applications qui risquent de ne pas fonctionner correctement avec d'autres applications ou qui peuvent interagir avec le système d'exploitation, telles que .NET Framework. Ces types d'applications sont idéaux pour l'hébergement sur des machines virtuelles.

  Les applications exécutées sur des systèmes d'exploitation plus anciens tels que Windows XP ou Windows Vista, et des architectures plus anciennes, telles que 32 bits ou 16 bits. En isolant chaque application sur sa propre machine virtuelle, si une machine échoue, elle n'affecte pas les autres utilisateurs.

Avantages et considérations

- Les applications et les bureaux sur l'image principale sont hébergés, gérés et exécutés en toute sécurité sur les machines de votre centre de données, qui fournissent une solution de mise à disposition d'applications la moins onéreuse.
- Dès l'ouverture de session, les utilisateurs peuvent être attribués à une machine de manière aléatoire au sein d'un groupe de mise à disposition qui est configuré pour héberger la même application. Vous pouvez également attribuer une machine unique pour mettre une application une application vers un seul utilisateur chaque fois que l'utilisateur ouvre une session. Les machines attribuées de manière statique permettent aux utilisateurs d'installer et de gérer leurs propres applications sur la machine virtuelle.
- L'exécution de plusieurs sessions n'est pas prise en charge sur des machines équipées d'un système d'exploitation de bureau. Par conséquent, chaque utilisateur utilise une seule machine au sein d'un groupe de mise à disposition lorsqu'il ouvre une session, et les utilisateurs doivent être en ligne pour accéder à leurs applications.
- Cette méthode peut augmenter la quantité de ressources serveur pour le traitement des applications et augmenter la quantité de stockage pour les Personal vDisks des utilisateurs.

Expérience utilisateur

La même expérience d'application transparente que l'hébergement des applications partagées sur les machines équipées d'un système d'exploitation serveur.

Traiter, héberger et mettre à disposition des applications

Le même que les machines équipées d'un système d'exploitation serveur, mis à part qu'elles sont des machines de systèmes d'exploitation de bureau virtuel.

Gestion et attribution de sessions

- Les machines équipées d'un système d'exploitation de bureau exécutent une seule session de bureau à partir d'une seule machine. Lors de l'accès à des applications uniquement, un seul utilisateur peut utiliser plusieurs applications (et n'est pas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

limité à une seule application), car le système d'exploitation accède à chaque application comme une nouvelle session.
- Dans un groupe de mise à disposition, lorsque les utilisateurs ouvrent une session, ils peuvent accéder à une machine affectée de manière statique (à chaque fois que l'utilisateur ouvre une session sur la même machine) ou une machine affectée de manière aléatoire qui est sélectionnée en fonction de la disponibilité de session.

Pour mettre à disposition des applications hébergées sur une machine virtuelle :

1. Installez les applications que vous souhaitez mettre à disposition sur une image principale exécutant un système d'exploitation de bureau Windows pris en charge.
2. Créez un catalogue de machines pour cette image principale ou mettre à jour un catalogue existant avec l'image principale.
3. Lors de la définition de l'expérience de bureau pour le catalogue de machines, déterminez si vous souhaitez que les utilisateurs se connectent à une nouvelle VM ou se connectent à la même machine chaque fois qu'ils ouvrent une session.
4. Créez un groupe de mise à disposition pour mettre à disposition l'application auprès des utilisateurs.
5. À partir de la liste des applications installées, sélectionnez l'application que vous souhaitez mettre à disposition.

Veuillez consulter les articles de configuration et d'installation pour plus de détails.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Bureaux VDI

Jul 07, 2016

Utilisez des machines avec OS de bureau pour mettre à disposition des bureaux VDI.

Les bureaux VDI sont hébergés sur des machines virtuelles et fournissent à chaque utilisateur un système d'exploitation de bureau.

Les bureaux VDI requièrent plus de ressources que les bureaux publiés XenApp, mais n'exigent pas que les applications installées sur ceux-ci prennent en charge des systèmes d'exploitation serveur. De plus, selon le type de bureau VDI que vous choisissez, ces bureaux peuvent être affectés à des utilisateurs individuels et permettre à ces utilisateurs un haut degré de personnalisation.

Lorsque vous créez un catalogue de machines pour les bureaux VDI, vous créez un de ces types de bureaux :

- Bureaux aléatoires non persistants, également appelé bureaux VDI regroupés. Chaque fois qu'un utilisateur ouvre une session sur l'un de ces bureaux, ils se connectent à un bureau sélectionné de manière dynamique dans un groupe de bureaux basés sur une image principale unique. Toutes les modifications apportées au bureau sont perdues lorsque la machine redémarre.
- Bureau statique non persistant. La première fois qu'un utilisateur ouvre une session pour utiliser l'un de ces bureaux, l'utilisateur se voit attribuer un bureau depuis un groupe de bureaux basés sur une image principale unique. Après la première utilisation, chaque fois qu'un utilisateur ouvre une session pour utiliser l'un de ces bureaux, l'utilisateur se connecte au même bureau auquel l'utilisateur a été affecté lors de la première utilisation. Toutes les modifications apportées au bureau sont perdues lorsque la machine redémarre.
- Statique persistant, également appelé VDI avec Personal vDisk. À l'inverse d'autres types de bureaux VDI, ces bureaux peuvent être entièrement personnalisés par les utilisateurs. La première fois qu'un utilisateur ouvre une session pour utiliser l'un de ces bureaux, l'utilisateur se voit attribuer un bureau depuis un groupe de bureaux basés sur une image principale unique. Après la première utilisation, chaque fois qu'un utilisateur ouvre une session pour utiliser l'un de ces bureaux, l'utilisateur se connecte au même bureau auquel l'utilisateur a été affecté lors de la première utilisation. Les modifications apportées aux bureaux sont conservées lorsque la machine redémarre, car ils sont stockés dans un Personal vDisk.

Pour mettre à disposition des bureaux VDI :

1. Créer une image principale exécutant un système d'exploitation de bureau Windows pris en charge.
2. Créez un catalogue de machines pour cette image principale ou mettre à jour un catalogue existant avec l'image principale. Lors de la définition de l'expérience de bureau pour le catalogue de machines, déterminez si vous souhaitez que les utilisateurs se connectent à une nouvelle VM à chaque ouverture de session ou se connectent à la même machine chaque fois qu'ils ouvrent une session et spécifiez comment les modifications apportées au bureau sont conservées.
3. Créez un groupe de mise à disposition pour mettre à disposition les bureaux auprès des utilisateurs.

Veuillez consulter les articles de configuration et d'installation pour plus de détails.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Installer et configurer

Jul 15, 2016

Consultez les articles référencés avant de démarrer chaque étape de déploiement, de façon à être informé sur ce que vous voyez et sélectionnez lors du déploiement.

Utilisez la séquence suivante pour déployer XenApp ou XenDesktop.

Préparer

Consultez l'article Préparer l'installation et effectuez toutes les tâches nécessaires. Parmi lesquelles :

- Se familiariser avec XenApp et XenDesktop : cet article vous explique où trouver des informations sur les concepts, les fonctionnalités, les différences avec les versions antérieures, la configuration système requise et les bases de données.
- Configurer l'environnement de virtualisation, d'hébergement ou d'assistance, si vous en utilisez un.
- Configurer les machines sur lesquelles vous installerez les composants.
- Configurer l'environnement Active Directory.

Cet article présente également les informations que vous devez sélectionner ou spécifier lorsque vous installez les composants et fonctionnalités.

Si vous installez des VDA Linux, veillez à consulter VDA Red Hat Linux et VDA SUSE Linux avant de procéder à l'installation.

Installer les composants principaux

Installez Delivery Controller, Citrix Studio, Citrix Director, le serveur de licences et Citrix StoreFront. Vous pouvez utiliser une interface graphique basée sur assistant ou d'une interface de ligne de commande, qui permet d'effectuer l'installation à partir d'un script. Les deux méthodes installent la plupart composants requis automatiquement.

Créer un site

Après avoir installé les composants principaux et démarré Studio, vous êtes automatiquement invité à créer un site à l'aide de l'assistant de création de site.

Installer un ou plusieurs Virtual Delivery Agents (VDA)

Installez un VDA sur une machine exécutant un système d'exploitation Windows, soit sur une image principale utilisée pour créer les machines virtuelles soit directement sur chaque machine. Vous pouvez utiliser une interface graphique ou de commande. Des exemples de scripts sont également fournis si vous souhaitez installer le VDA à l'aide d'Active Directory.

Pour les machines avec un système d'exploitation Linux, suivez les instructions pour l'installation d'un VDA Red Hat Linux ou d'un VDA SUSE Linux.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour un déploiement Remote PC Access, installez un VDA pour OS de bureau sur chaque PC de bureau ; pour une meilleure efficacité, utilisez l'interface de ligne de commande du programme d'installation de VDA autonome et vos méthodes de distribution électronique de logiciels existantes.

Installer les autres composants facultatifs

Si vous prévoyez d'utiliser le serveur d'impression universelle Citrix, installez son composant serveur sur vos serveurs d'impression. Vous pouvez utiliser une interface graphique ou de commande. Pour de plus amples informations, consultez la section Provisionner des imprimantes.

Pour permettre à StoreFront d'utiliser des options d'authentification telles que les assertions SAML, installez le Service d'authentification fédérée de Citrix, de préférence sur un serveur qui ne contient pas d'autres composants Citrix.

Si vous le souhaitez, vous pouvez intégrer d'autres composants Citrix dans votre déploiement XenApp ou XenDesktop. Par exemple :

- Provisioning Services est un composant facultatif de XenApp et XenDesktop qui provisionne les machines en livrant en streaming une image principale vers les machines cibles. Consultez la documentation Provisioning Services.
- Citrix NetScaler Gateway est une solution garantissant un accès sécurisé aux applications. Grâce à des stratégies de contrôle d'accès et d'action avancées, elle permet aux administrateurs de renforcer l'accès aux applications et données. Consultez la documentation NetScaler Gateway.
- Citrix CloudBridge est un ensemble de boîtiers qui permet d'optimiser les performances du réseau étendu. Consultez la documentation Citrix CloudBridge.

Pour obtenir des instructions d'installation, consultez la documentation accompagnant ces composants, fonctionnalités et technologies.

Créer un catalogue de machines

Lorsque vous créez un site dans Studio, vous êtes guidé dans la création d'un catalogue de machines.

Un catalogue peut contenir des machines physiques ou virtuelles (VM). Les machines virtuelles peuvent être créées à partir d'une image principale. Si vous utilisez un hyperviseur ou un service de cloud pris en charge pour fournir des machines virtuelles, vous devez d'abord créer une image principale sur cet hôte. Ensuite, lorsque vous créez le catalogue, vous spécifiez cette image, qui sera utilisée lors de la création de machines virtuelles.

Créer un groupe de mise à disposition

Lorsque vous créez votre premier catalogue de machines dans Studio, vous êtes guidé dans la création d'un groupe de mise à disposition.

Un groupe de mise à disposition spécifie quels utilisateurs peuvent accéder aux machines dans un catalogue de machines spécifique et les applications disponibles pour ces utilisateurs.

Créer un groupe d'applications (facultatif)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Lorsque vous créez un groupe de mise à disposition, vous pouvez également créer un groupe d'applications. Vous pouvez créer des groupes d'applications pour les applications qui sont partagées entre différents groupes de mise à disposition ou utilisées par un sous-ensemble d'utilisateurs au sein de groupes de mise à disposition.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Préparer l'installation

Jul 15, 2016

Dans cet article :

- Instructions d'installation générales
- Que spécifier lors de l'installation des composants principaux
- Instructions d'installation d'un VDA
- Que spécifier lors de l'installation d'un VDA

Instructions d'installation générales

- Si vous ne connaissez pas le produit et ses composants, veuillez consulter les articles Vue d'ensemble technique. Si votre déploiement actuel est XenApp 6.5 ou version antérieure, l'article Concepts et composants décrit les différences dans les versions 7.x de XenApp et XenDesktop.
- Lors de la planification de votre déploiement, consultez les articles de sécurité.
- Lisez l'article Problèmes connus afin de prendre connaissance des problèmes d'installation que vous êtes susceptibles de rencontrer.
- Si vous utilisez un hyperviseur ou un service de cloud pris en charge pour fournir des machines virtuelles pour les applications et bureaux, vous pouvez configurer la première connexion à cet hôte lorsque vous créez un site, après avoir installé les composants. Toutefois, vous pouvez configurer l'environnement de virtualisation à tout moment avant cette configuration. Consultez les sources d'informations répertoriées ici.
- Si vous utilisez Microsoft System Center Configuration Manager pour gérer l'accès aux applications et bureaux, consultez cet article.
- Si un composant requiert .NET, le programme d'installation déploie la version .NET requise si elle n'est pas présente. L'installation de .NET peut nécessiter un redémarrage de la machine.
- Consultez l'article Bases de données pour en apprendre davantage sur les bases de données du système et leur configuration. Lors de l'installation du Controller, vous pouvez choisir d'installer Microsoft SQL Server 2012 Express sur le même serveur. Vous configurez la plupart des informations de base de données lorsque vous créez un site, après avoir installé les composants principaux.
- Lorsque vous installez le serveur de licences Citrix, ce compte d'utilisateur est automatiquement converti en administrateur complet sur le serveur de licences. Consultez l'article Administration déléguée pour plus de détails.
- Lorsque vous créez des objets avant, pendant et après l'installation, il est recommandé de spécifier des noms uniques pour chaque objet : par exemple réseaux, groupes, catalogues et ressources.
- Si un composant n'est pas installé correctement, le processus s'arrête et un message d'erreur s'affiche. Les composants installés correctement sont conservés ; vous n'avez pas besoin de les réinstaller.
- Citrix Studio démarre automatiquement après son installation. Lors de l'utilisation de l'interface graphique, vous pouvez désactiver cette action sur la dernière page de l'assistant.
- Vous pouvez utiliser le programme d'installation inclus dans le fichier ISO du produit pour installer les composants principaux et les Virtual Delivery Agents (VDA) ; ce programme est appelé « programme d'installation du produit entier ». Pour installer des VDA, vous pouvez utiliser le programme d'installation du produit entier ou le programme d'installation VDA autonome, qui est disponible sur le site de téléchargement du produit. Les deux programmes d'installation offrent des interfaces graphique et de ligne de commande.
- Le support d'installation du produit contient des exemples de scripts qui permettent d'installer, mettre à niveau ou supprimer les VDA pour les groupes de machines dans Active Directory. Vous pouvez également appliquer les scripts à des

© 1999-2017 Citrix Systems, Inc. All rights reserved.

machines individuelles, et les utiliser pour gérer les images principales utilisées par Machine Creation Services et Provisioning Services. Pour de plus amples informations, consultez l'article Installer les VDA à l'aide de scripts.

- Vous pouvez utiliser le programme d'installation du produit entier pour installer le composant serveur (UpsServer) du serveur d'impression universelle sur vos serveurs d'impression, soit à l'aide de l'interface graphique ou de l'interface de ligne de commande. Le site de téléchargement du produit peut également contenir des packs de téléchargement UpsServer. Pour de plus amples informations, consultez la section Provisionner des imprimantes.
- Vous pouvez utiliser le programme d'installation du produit entier pour installer le Service d'authentification fédérée.
- Des données d'analyse sont collectées lorsque vous installez les composants. En outre, lorsque vous utilisez l'interface graphique du programme d'installation du produit entier pour installer un Delivery Controller ou un VDA, vous pouvez indiquer si vous souhaitez ou non participer à la fonctionnalité Citrix Call Home. Pour de plus amples informations sur ces fonctionnalités, consultez l'article Citrix Insight Services.
- Le fichier ISO du produit ne comprend plus les versions de Citrix Receiver pour Mac et Citrix Receiver pour Linux. Vous (ou vos utilisateurs) pouvez télécharger et installer Citrix Receiver à partir du site Web de Citrix. Éventuellement, vous pouvez mettre à disposition ces logiciels Citrix Receiver à partir de votre serveur StoreFront (veuillez consulter la section Mettre à disposition des fichiers d'installation Citrix Receiver sur le serveur dans la documentation de StoreFront 3.0.x ou le contenu équivalent dans la version de StoreFront que vous utilisez).

Vous devez être un utilisateur du domaine et un administrateur local sur les machines sur lesquelles vous installez les composants.

Vous devez disposer de privilèges d'administrateur avant de démarrer l'installation ou utiliser **Exécuter en tant qu'administrateur**.

Configurez votre domaine Active Directory avant de procéder à l'installation.

- L'article Configuration système requise répertorie les niveaux fonctionnels d'Active Directory pris en charge. L'article Active Directory contient des informations supplémentaires.
- Vous devez disposer d'au moins un contrôleur de domaine exécutant les services de domaine Active Directory.
- N'essayez pas d'installer les composants sur un contrôleur de domaine.
- N'utilisez pas de barre oblique (/) lorsque vous spécifiez les noms d'unité d'organisation dans Studio.
- Consultez la documentation Microsoft pour obtenir des instructions de configuration Active Directory.

Choisissez l'emplacement d'installation des composants, puis préparez les machines et les systèmes d'exploitation.

- Consultez l'article Configuration système requise pour connaître les systèmes d'exploitation et les versions pris en charge de Controller, Studio, Citrix Director, des ressources virtuelles (hôtes) et des VDA. La plupart des composants requis sont installés automatiquement ; les exceptions sont indiquées dans cet article. Consultez les documents relatifs à Citrix StoreFront et au serveur de licences Citrix pour connaître les plates-formes prises en charge.
- Vous pouvez installer les composants principaux sur le même serveur ou sur des serveurs différents. Par exemple, pour gérer un déploiement de petite taille à distance, vous pouvez installer Studio sur une autre machine que le serveur sur lequel vous avez installé le Controller. Pour prendre en charge une expansion future, pensez à installer des composants sur des serveurs distincts ; par exemple, installez le serveur de licences et Director sur des serveurs différents.
- Vous pouvez installer Delivery Controller et Virtual Delivery Agent pour système d'exploitation Windows Server sur le même serveur. Pour cela, lancez le programme d'installation et sélectionnez le Delivery Controller (ainsi que tout autre composant que vous voulez installer sur cette machine) ; puis lancez de nouveau le programme d'installation et

© 1999-2017 Citrix Systems, Inc. All rights reserved.

sélectionnez le Virtual Delivery Agent pour système d'exploitation Windows Server.

- N'installez pas les composants sur un contrôleur de domaine.
- L'installation d'un Controller sur un nœud dans une installation de mise en cluster SQL Server, de mise en miroir SQL Server où sur un serveur exécutant Hyper-V n'est pas prise en charge.
- N'installez pas Studio sur un serveur exécutant XenApp 6.5 Feature Pack 2 pour Windows Server 2008 R2 ou toute version antérieure de XenApp.
- Assurez-vous que chaque système d'exploitation dispose des dernières mises à jour.
- Assurez-vous que les horloges système de toutes les machines sont synchronisées. La synchronisation est requise par l'infrastructure Kerberos qui sécurise la communication entre les machines.

Que spécifier lors de l'installation des composants principaux

Les sections suivantes expliquent ce que vous verrez et devrez spécifier lors de l'installation. Elles suivent la séquence de l'assistant avec interface graphique ; les options de ligne de commande équivalentes sont également fournies. Les articles sur l'installation fournissent plus de détails sur la manière de lancer les assistants et d'émettre des commandes avec les options.

Les composants sont installés par défaut dans C:\Program Files\Citrix. Vous pouvez spécifier un autre emplacement sur la page **Composants principaux**, mais ce dernier doit disposer d'autorisations d'exécution pour le service réseau. (option de ligne de commande : /installdir pour spécifier un répertoire différent)

Sélectionnez ou spécifiez si vous souhaitez installer Microsoft SQL Server Express. Si vous n'avez pas d'expérience avec les bases de données, consultez l'article Bases de données. (option de ligne de commande : /nosql pour empêcher l'installation)

Lorsque vous installez Director, l'Assistance à distance Windows est installée automatiquement. Vous pouvez choisir d'activer l'observation dans l'Assistance à distance Windows pour l'utiliser avec l'observation utilisateur de Director et d'ouvrir le port TCP 3389. Par défaut, cette option est activée. (option de ligne de commande : /no_remote_assistance)

Par défaut, les ports suivants sont ouverts automatiquement si le service Pare-feu Windows est en cours d'exécution, même si le pare-feu n'est pas activé. Vous pouvez désactiver cette action par défaut et ouvrir les ports manuellement si vous utilisez un pare-feu tiers ou aucun pare-feu, ou si vous préférez le faire vous-même. Pour des informations de port complètes sur ce produit et d'autres produits Citrix, consultez l'article CTX101810. (Option de ligne de commande : /configure_firewall)

- Controller : TCP 80, 443
- Director : TCP 80, 443
- Serveur de licences : TCP 7279, 8082, 8083, 27000
- StoreFront : TCP 80, 443

Instructions d'installation d'un VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Les programmes d'installation de VDA offrent des interfaces graphique et de ligne de commande.
- Consultez l'article Configuration système requise pour connaître les systèmes d'exploitation et versions pris en charge pour les VDA. La plupart des composants requis sont installés automatiquement ; les exceptions sont indiquées dans cet article. Lorsque vous installez un VDA pour système d'exploitation de serveur Windows, les services de rôle des services Bureau à distance sont automatiquement installés et activés (s'ils ne sont pas déjà installés et activés).
- Si vous installez un VDA sur Windows 7 ou Windows Server 2008 R2, assurez-vous que .NET 3.5.1 est installé avant de démarrer l'installation du VDA. La section Redémarrages ci-dessous contient des informations supplémentaires sur l'installation des composants requis.
- Le service Spouleur d'impression est activé par défaut sur les serveurs Windows pris en charge. Si vous désactivez ce service, vous ne pouvez pas installer correctement un VDA pour OS de serveur Windows ; assurez-vous donc que ce service est activé avant d'installer un VDA.
- La gestion de profil est automatiquement installée lors de l'installation de l'Agent Virtual Desktop. Bien que vous puissiez exclure cette fonctionnalité si vous utilisez l'interface de ligne de commande, cette exclusion affectera la surveillance et la résolution des problèmes de VDA avec Director.
- Lorsque vous installez le VDA, un nouveau groupe d'utilisateurs locaux appelé Direct Access Users est créé automatiquement. Sur un VDA pour OS de bureau Windows, ce groupe s'applique uniquement aux connexions RDP ; sur un VDA pour OS de serveur Windows, ce groupe s'applique aux connexions ICA et RDP.
- Pour les configurations Remote PC Access, installez le VDA pour OS de bureau Windows sur chaque PC de bureau physique auquel les utilisateurs accèderont à distance. N'activez pas la fonctionnalité d'optimisation.
- Si vous installez un VDA sur une machine exécutant un système d'exploitation Linux pris en charge, consultez la section Red Hat Linux VDA ou SUSE Linux VDA pour des informations essentielles.
- Le VDA doit avoir des adresses Controller valides avec lesquelles communiquer ; sinon, les sessions ne peuvent pas être établies. Vous pouvez spécifier les adresses Controller lorsque vous installez le VDA ou ultérieurement ; mais surtout n'oubliez pas, car cette opération est indispensable ! Pour de plus amples informations, consultez la section Adresses Delivery Controller.
- Après installation d'un VDA pour OS de serveur sur un système Windows Server 2012 R2, utilisez l'outil Kerberos Enable Tool (XASsonKerb.exe) pour garantir le bon fonctionnement de l'authentification Citrix Kerberos. L'outil est situé dans le dossier Support > Tools > XASsonKerb sur le support d'installation, vous devez disposer des privilèges d'administrateur local pour utiliser l'outil. Exécutez **xassonkerb.exe –install** à partir d'une invite de commande sur le serveur. Si vous appliquez plus tard une mise à jour qui modifie l'emplacement du registre HKLM\System\CurrentControlSet\Control\LSA\OSConfig, réexécutez la commande. Pour afficher toutes les options d'outils, exécutez la commande avec le paramètre –help.

Vous pouvez installer un VDA à l'aide du programme d'installation du produit entier ou un pack d'installation autonome. Les deux programmes offrent des interfaces graphique et de ligne de commande.

Le programme d'installation du produit entier détecte automatiquement votre système d'exploitation et vous permet d'installer uniquement le VDA Windows pris en charge sur ce système : VDA pour système d'exploitation de serveur Windows ou VDA pour système d'exploitation de bureau Windows.

Pack d'installation VDA autonome

Ce pack autonome de taille plus petite convient aux déploiements faisant appel à des packs ESD (mise à disposition électronique du logiciel) qui sont préparés ou copiés localement et qui disposent de machines physiques ou de bureaux distants. Le pack autonome est principalement destiné aux déploiements utilisant l'installation par ligne de commande (silencieuse) ; il prend en charge les mêmes paramètres de ligne de commande que le programme d'installation du produit

© 1999-2017 Citrix Systems, Inc. All rights reserved.

entier. Le pack offre également une interface graphique équivalente au programme d'installation du produit complet.

Comment utiliser l'interface graphique du programme d'installation VDA autonome.

Comment utiliser l'interface de ligne de commande du programme d'installation VDA autonome.

Deux packs d'installation VDA autonomes auto-extractibles sont disponibles : un pour l'installation sur les machines avec OS de serveur et un autre pour l'installation sur les machines avec OS de bureau.

Par défaut, les fichiers du pack sont extraits dans le dossier Temp. L'espace disque nécessaire sur la machine lors de l'extraction sur le dossier Temp est plus important que lors de l'utilisation du programme d'installation du produit entier. Les fichiers extraits sur le dossier Temp ne sont pas automatiquement supprimés, mais vous pouvez les supprimer manuellement (sur C:\Windows\Temp\Ctx-*, où * est un identificateur global unique aléatoire) une fois l'installation terminée. Vous pouvez aussi utiliser la commande /extract avec un chemin d'accès absolu.

Si votre déploiement utilise Microsoft System Center Configuration Manager, l'installation d'un VDA peut sembler avoir échoué avec le code de sortie 3, bien que le VDA ait été installé avec succès. Pour éviter ce message erroné, vous pouvez wrapper votre installation dans un script CMD ou modifier les codes de réussite dans votre pack Configuration Manager. Pour de plus amples informations, consultez le forum de discussion http://discussions.citrix.com/topic/350000-sccm-install-of-vda-71-fails-with-exit-code-3/.

Un redémarrage est requis à la fin de l'installation du VDA.

Si vous souhaitez réduire le nombre de redémarrages supplémentaires requis durant l'installation :

- Assurez-vous qu'une version de .NET Framework prise en charge est installée avant d'installer le VDA.
- Pour les machines équipées d'un OS de serveur Windows, installez et activez les services de rôle RDS avant d'installer le VDA.

Les autres composants requis ne requièrent pas le redémarrage de la machine, vous pouvez donc laisser le programme d'installation s'en occuper.

Si vous n'installez pas les composants requis avant de commencer l'installation du VDA, et que vous spécifiez l'option /noreboot pour une installation par ligne de commande, vous devez gérer les redémarrages. À titre d'exemple, lors du déploiement automatique des composants requis, le programme d'installation s'arrêtera après l'installation de RDS, en attente d'un redémarrage ; n'oubliez pas d'exécuter de nouveau la commande après le redémarrage pour poursuivre l'installation du VDA.

La dernière version de VDA n'est pas prise en charge sur Windows XP ou Windows Vista ; de plus, certaines des fonctionnalités disponibles dans cette version et d'autres versions récentes ne peuvent pas être utilisées sur ces systèmes d'exploitation. Citrix vous recommande de remplacer ces systèmes par des versions de systèmes d'exploitation de bureau Windows prises en charge et d'installer un VDA à partir de cette version. Si vous continuez à recevoir des machines exécutant Windows XP ou Windows Vista, vous pouvez installer une version antérieure de Virtual Desktop Agent (5.6 FP1 avec certaines corrections à chaud). Pour de plus amples informations, veuillez consulter l'article CTX140941. Gardez à l'esprit que :

- Vous ne pouvez pas installer de composants principaux (par exemple, Controller, Studio, Director, StoreFront, le serveur de licences) sur un système Windows XP ou Windows Vista.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Si vous utilisez les systèmes Windows XP ou Windows Vista, lorsque vous créez un catalogue de machines contenant ces machines, assurez-vous de choisir l'entrée 5.6 FP1 dans la liste « Sélectionnez la version de VDA installée... » sur la page Image principale.
- Remote PC Access n'est pas pris en charge sur Windows Vista.
- La prise en charge de Citrix pour Windows XP s'est terminée le 8 avril 2014 lorsque Microsoft a mis fin à la prise en charge de son assistance.
- Le fait de continuer à utiliser une version plus ancienne de VDA peut affecter la disponibilité des fonctionnalités de l'enregistrement VDA auprès du Controller ; voir Considérations d'environnement mixte.

Que spécifier lors de l'installation d'un VDA

Les sections suivantes expliquent ce que vous devrez spécifier lors de l'installation. Elles suivent la séquence de l'assistant avec interface graphique ; les options de ligne de commande équivalentes sont également fournies. Les articles sur l'installation fournissent plus de détails sur la manière de lancer les assistants ou d'émettre des commandes avec les options.

Consultez Instructions d'installation d'un VDA pour connaître les tâches qui peuvent être nécessaires après l'installation d'un VDA.

L'environnement de VDA détermine la manière dont vous utilisez le VDA :

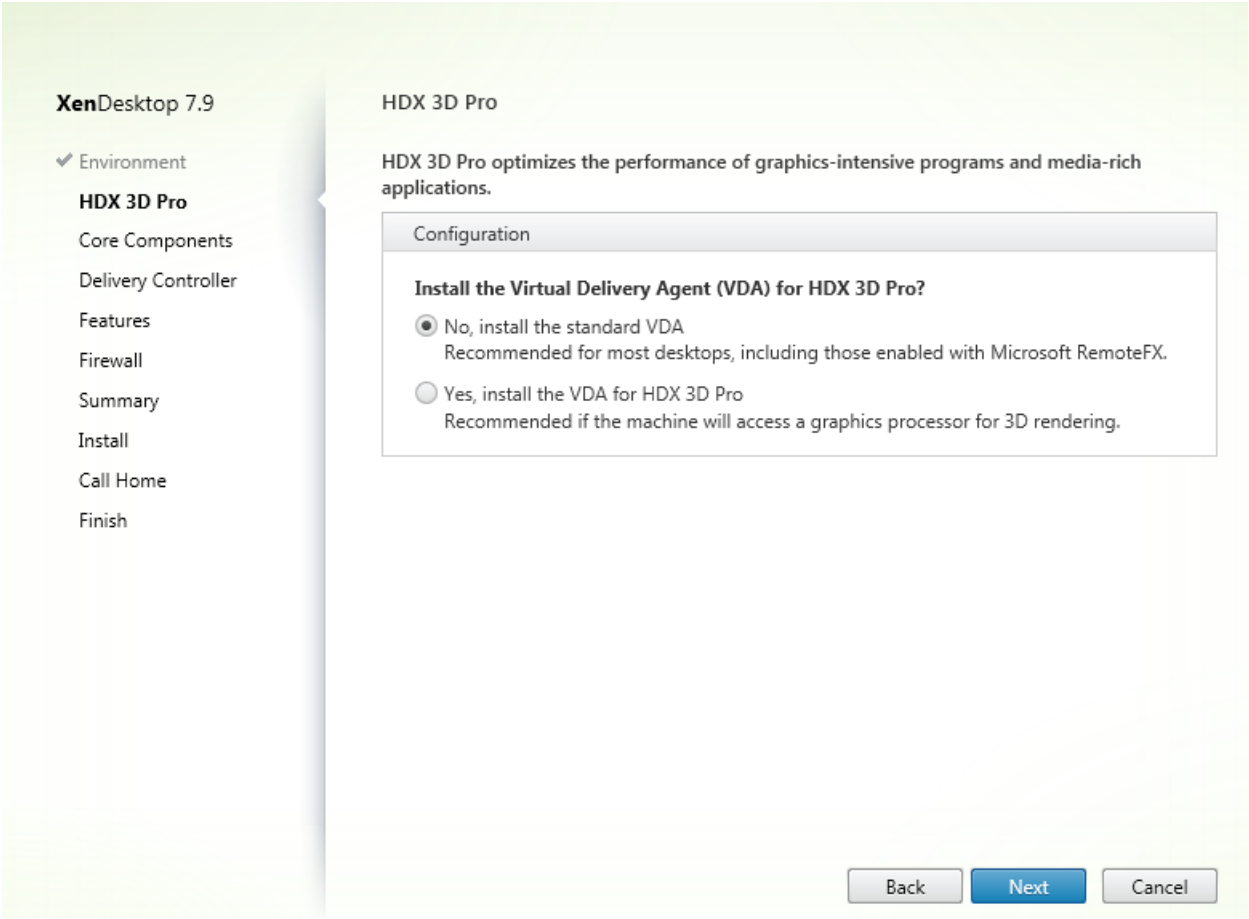
- L'option « image principale » par défaut indique que vous allez utiliser Machine Creation Services (MCS) ou Provisioning Services pour créer des machines virtuelles basées sur une image principale créée dans un hyperviseur ou un service de cloud. Installez le VDA sur l'image principale. (option de ligne de commande : /masterimage)
- L'option « Remote PC Access » indique que vous allez installer le VDA sur une machine physique ou sur une VM qui a été provisionnée sans VDA.

> **Important**
>
> Dans XenApp et XenDesktop 7.9, utilisez uniquement la ligne de commande pour les déploiements Remote PC Access. Pour de plus amples informations, consultez les sections Installer à l'aide de la ligne de commande et Problèmes connus [#637741].

Lorsque vous installez un VDA à l'aide de l'interface graphique, cette page s'affiche uniquement lors de l'installation d'un VDA sur une machine avec OS de bureau (et non sur une machine avec OS de serveur). Choisissez de configurer le VDA en mode standard ou HDX 3D Pro.

- Le mode de VDA standard est recommandé pour la plupart des bureaux, y compris ceux activés avec Microsoft RemoteFX. Ce mode est configuré par défaut.
- Le VDA pour mode HDX 3D Pro optimise les performances des programmes gourmands en graphique et des applications riches en multimédia. Il est recommandé si la machine aura accès au processeur graphique pour la restitution 3D. (option de ligne de commande uniquement valide sur les machines avec OS de bureau : /enable_hdx_3d_pro)

© 1999-2017 Citrix Systems, Inc. All rights reserved.



VDA standard	VDA pour HDX 3D Pro

• Recommandé en général pour les bureaux virtuels sans accélération graphique matérielle et pour Remote PC Access.
• Prend en charge l'accélération GPU avec tout processeur graphique, avec certaines limitations de compatibilité applicative :
  • Sur Windows 7, 8 et 8.1, accélération GPU pour niveaux de fonctionnalité DirectX jusqu'à 9.3. Certaines applications DirectX 10, 11 et 12 risquent de ne pas s'exécuter si elles ne gèrent pas le retour sur DirectX 9.
  • Sur Windows 10, l'accélération GPU est limitée aux applications DirectX 10, 11, 12 en mode fenêtré (sans mode plein écran) ; les applications DirectX 9 et plein écran sont rendues par logiciel (WARP).
  • Accélération des applications OpenGL dans les sessions distantes si prise en charge par le fournisseur GPU (NVIDIA uniquement pour le moment).
	• Recommandé en général pour les bureaux de centre de données avec accélération graphique matérielle, sauf si plus de quatre moniteurs sont requis.
	• Prend en charge l'accélération GPU avec tout processeur graphique ; toutefois l'occultation de console, les résolutions d'écran non standard et la prise en charge de moniteurs multiples réelle requièrent NVIDIA GRID ou Intel Iris Pro Graphics.
	• Utilise le pilote du fournisseur de graphiques pour une compatibilité applicative optimale.
	  • Toutes les API 3D (DirectX ou OpenGL) que le processeur graphique prend en charge.
	  • Prise en charge d'applications 3D plein écran avec Intel Iris Pro (Win10 uniquement) et NVIDIA GRID.
	  • Prise en charge d'API et d'extensions de pilote personnalisées. Par exemple, CUDA ou OpenCL.
	• Prend en charge jusqu'à quatre moniteurs.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

• Utilise le pilote d'affichage Citrix WDDM, avec prise en charge de résolutions de moniteur arbitraires (jusqu'à 4K) et jusqu'à 8 moniteurs. • Option Redirection Desktop Composition pour accès haut débit aux bureaux Windows 7 et 8.x Aero. • Composition de bureau Windows transférée à la machine utilisateur (Windows ou Mac).	

Remote PC Access et mode HDX 3D Pro

Pour Remote PC Access, le VDA est généralement configuré à l'aide de l'option VDA standard. Lorsque Remote PC Access est configuré avec HDX 3D Pro, l'occultation de moniteur est prise en charge avec Intel Iris Pro Graphics et Intel HD Graphics 5300 et supérieur (Processeurs Intel Core 5ème Génération et Processeurs Intel Core i5 6ème Génération), et NVIDIA Quadro et NVIDIA GRID

Les VDA sont installés par défaut dans C:\Program Files\Citrix. Vous pouvez spécifier un autre emplacement au cours de l'installation, mais ce dernier doit disposer d'autorisations d'exécution pour le service réseau. (option de ligne de commande : /installdir pour spécifier un répertoire différent)

Par défaut, Citrix Receiver pour Windows est installé avec le VDA. Vous pouvez désactiver cette action par défaut. (option de ligne de commande : utilisez /components vda pour empêcher l'installation de Citrix Receiver)

Vous pouvez spécifier les adresses (nom de domaine complet, FQDN) des Controller installés lorsque vous installez le VDA (recommandé) ou ultérieurement. Bien qu'il ne soit pas nécessaire de spécifier les adresses Controller lorsque vous installez un VDA, n'oubliez pas qu'un VDA ne peut pas s'enregistrer auprès d'un Controller sans ces informations. Si les VDA ne peuvent pas s'enregistrer, les utilisateurs sur des machines contenant ces VDA ne pourront pas accéder à leurs applications et bureaux. (Option de ligne de commande : /controllers)

- Si vous spécifiez les noms de domaine complets des Controller lorsque vous installez le VDA, le programme d'installation tente de se connecter aux adresses spécifiées. Si la connexion échoue, le programme d'installation contient des messages d'information.
- Si vous choisissez de spécifier les adresses des Controller ultérieurement, le programme d'installation vous le rappelle. Si vous installez un VDA sans spécifier d'adresse de Controller, vous pouvez soit exécuter de nouveau le programme d'installation ultérieurement soit utiliser la stratégie de groupe Citrix.

Si vous spécifiez les adresses des Controller à la fois lors de l'installation du VDA et dans la stratégie de groupe, les paramètres de la stratégie remplacent les paramètres fournis au cours de l'installation.

N'oubliez pas que l'enregistrement du VDA requiert également que les ports de pare-feu utilisés pour les communications avec le Controller soient ouverts.

Une fois que vous avez initialement spécifié l'emplacement des Controller (au cours de l'installation du VDA ou ultérieurement), vous pouvez utiliser la fonctionnalité de mise à jour automatique pour mettre les VDA à jour lorsque d'autres Controller sont installés.

Pour de plus amples informations sur la façon dont les VDA découvrent et s'enregistrent auprès de Controller, consultez

© 1999-2017 Citrix Systems, Inc. All rights reserved.

l'article Delivery Controller.

Vous pouvez activer ou désactiver les fonctionnalités suivantes, utilisées avec les VDA :

- **Optimisation des performances :** (par défaut = activée) lorsque cette fonctionnalité est sélectionnée, l'outil d'optimisation est utilisé pour les VDA exécutés sur une machine virtuelle d'un hyperviseur. L'optimisation de VM comprend la désactivation des fichiers en mode déconnecté, la désactivation de la défragmentation en arrière-plan et la réduction de la taille du journal d'événements. Pour obtenir davantage d'informations, veuillez consulter l'article CTX125874. N'activez pas cette option si vous prévoyez d'utiliser Remote PC Access. (option de ligne de commande : /optimize)
- **Assistance à distance Windows :** (par défaut = activée) lorsque cette fonctionnalité est sélectionnée, l'Assistance à distance Windows est utilisée avec la fonctionnalité d'observation utilisateur de Director, et Windows ouvre automatiquement le port TCP 3389 dans le pare-feu, même si vous choisissez d'ouvrir les ports du pare-feu manuellement. (option de ligne de commande : /enable_remote_assistance)
- **Utiliser Real-Time Audio Transport pour l'audio :** (par défaut = activé) lorsque cette fonctionnalité est sélectionnée, le protocole UDP est utilisé pour les paquets audio, ce qui peut améliorer les performances audio. (option de ligne de commande : /enable_real_time_transport)
- **Framehawk :** (par défaut= activé) lorsque cette fonctionnalité est sélectionnée, les ports UDP bidirectionnels 3224-3324 sont ouverts (vous pouvez modifier la plage de ports ultérieurement avec le paramètre de stratégie Citrix « Plage de ports du canal d'affichage Framehawk » ; vous devez ouvrir les ports de pare-feu locaux). Un chemin réseau UDP doit être ouvert sur les pare-feux internes (VDA vers Citrix Receiver ou VDA vers NetScaler Gateway) et externes (NetScaler Gateway vers Citrix Receiver). Si NetScaler Gateway est déployé, les datagrammes Framehawk sont cryptés à l'aide de DTLS (port UDP 443 par défaut). Pour plus d'informations, veuillez consulter l'article Framehawk. (option de ligne de commande : /enable_framehawk_port)
- **Installer les composants de publication Citrix App-V :** (valeur par défaut : activé) sélectionnez cette fonctionnalité si vous prévoyez d'utiliser des applications à partir de Microsoft App-V. Pour plus d'informations, veuillez consulter l'article App-V. (option de ligne de commande : /no_appv pour empêcher l'installation des composants)
- **Personal vDisk :** (par défaut = activé, disponible uniquement lors de l'installation d'un VDA pour OS de bureau sur une VM). Lorsque cette fonctionnalité est sélectionnée, les Personal vDisks peuvent être utilisés avec une image principale. Pour de plus amples informations, consultez les articles Personal vDisk. (option de ligne de commande : /baseimage)

Par défaut, les ports suivants sont ouverts automatiquement si le service Pare-feu Windows est en cours d'exécution, même si le pare-feu n'est pas activé. Vous pouvez désactiver cette action par défaut et ouvrir les ports manuellement si vous utilisez un pare-feu tiers ou aucun pare-feu, ou si vous préférez le faire vous-même. pour accéder à des informations complètes sur les ports, consultez l'article CTX101810. (option de ligne de commande : /enable_hdx_ports)

- Communications Controller : TCP 80, 1494, 2598, 8008 Pour les communications entre les machines utilisateur et les bureaux virtuels, configurez TCP entrant sur les ports 1494 et 2598 en tant qu'exceptions de ports. Pour des raisons de sécurité, Citrix vous recommande de ne pas utiliser ces ports pour autre chose que le protocole ICA et CGP. Pour les communications entre les Controller et les bureaux virtuels, configurez le port 80 entrant en tant qu'exception de port.
- Assistance à distance : TCP 3389. Windows ouvre ce port automatiquement si la fonctionnalité Assistance à distance Windows a été activée sur la page précédente, même si vous choisissez d'ouvrir les ports manuellement.
- Real-Time Audio : UDP 16500-16509.
- Framehawk : UDP 3224-3324.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Une fois que vous avez passé en revue les informations présentées et cliqué sur **Installer**, l'affichage indique la progression de l'installation. Une fois l'installation terminée, un redémarrage de machine est nécessaire avant que le VDA puisse être utilisé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Environnements de virtualisation VMware

Jul 07, 2016

Suivez ce guide si vous utilisez VMware pour fournir des machines virtuelles.

Installer et configurer votre hyperviseur

Étape 1. Installez vCenter Server et les outils de gestion appropriés. (Aucune prise en charge n'est fournie pour l'opération vSphere vCenter Linked Mode.)

Étape 2. Créez un compte d'utilisateur VMware avec, au minimum, les permissions suivantes au niveau du centre de données. ce compte dispose d'autorisations pour créer des VM et est utilisé pour communiquer avec vCenter.

Kit de développement	Interface utilisateur
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
System.Anonymous, System.Read et System.View	Ajouté automatiquement.
Task.Create	Tasks > Create task
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU Count

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Config.Resource	Virtual machine > Configuration > Change resource
VirtualMachine.Config.Settings	Virtual machine > Configuration > Settings
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Inventory.Register	Virtual machine > Inventory > Register
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine
VirtualMachine.Provisioning.CloneTemplate	Virtual machine > Provisioning > Clone template
VirtualMachine.Provisioning.DiskRandomAccess	Virtual machine > Provisioning > Allow disk access
VirtualMachine.Provisioning.GetVmFiles	Virtual machine > Provisioning > Allow virtual machine download
VirtualMachine.Provisioning.PutVmFiles	Virtual machine > Provisioning > Allow virtual machine files upload
VirtualMachine.Provisioning.DeployTemplate	Virtual machine > Provisioning > Deploy template
VirtualMachine.Provisioning.MarkAsVM	Virtual machine > Provisioning > Mark as virtual machine

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VirtualMachine.State.CreateSnapshot	vSphere 5.0 Update 2 et vSphere 5.1, Update 1: Machine virtuelle > État > Créer l'instantané vSphere 5.5 : Machine virtuelle > Gestion des captures instantanées > Créer l'instantané
VirtualMachine.State.RemoveSnapshot	vSphere 5.0 Update 2 et vSphere 5.1, Update 1: Machine virtuelle > État > Supprimer l'instantané vSphere 5.5 : Machine virtuelle > Gestion des captures instantanées > Supprimer l'instantané
VirtualMachine.State.RevertToSnapshot	vSphere 5.0 Update 2 et vSphere 5.1, Update 1 : Machine virtuelle > État > Restaurer l'instantané vSphere 5.5 : Machine virtuelle > Gestion des captures instantanées > Restaurer l'instantané

Étape 3. Si vous voulez que les VM que vous créez soient balisées, ajoutez les permissions suivantes pour le compte d'utilisateur :

Kit de développement	Interface utilisateur
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Set custom attribute

Pour vous assurer que vous utilisez une nouvelle image de base pour créer de nouvelles VM, identifiez les VM créées avec Machine Creation Services pour les exclure de la liste des VM disponibles à utiliser en tant qu'images de base.

Étape 4. Pour créer des AppDisks, le compte utilisateur doit disposer des autorisations supplémentaires suivantes :

- SDK : VirtualMachine.Config.EditDevice
- Interface utilisateur : Virtual machine > Configuration > Modify Device Settings

Obtenir et importer un certificat

Pour protéger les communications vSphere, Citrix vous recommande d'utiliser HTTPS plutôt que HTTP. HTTPS requiert des certificats numériques. Citrix vous recommande d'utiliser un certificat numérique émis par une autorité de certification conformément à la stratégie de sécurité de votre organisation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si vous ne pouvez pas utiliser un certificat numérique émis par une autorité de certification et que la stratégie de sécurité de votre organisation le permet, vous pouvez utiliser le certificat auto-signé installé par VMware. Ajoutez le certificat VMware vCenter à chaque Controller. Suivez cette procédure :

1. Ajoutez le nom de domaine complet (FQDN) de l'ordinateur exécutant vCenter Server dans le fichier hôtes de ce serveur, situé à l'emplacement %SystemRoot%/WINDOWS/system32/Drivers/etc/. Cette étape est uniquement nécessaire que si le nom de domaine complet de l'ordinateur exécutant vCenter Server n'est pas déjà présent dans le DNS.
2. Obtenez le certificat vCenter à l'aide de l'une des méthodes suivantes :
   - Depuis le serveur vCenter :
     1. Copiez le fichier rui.crt depuis le serveur vCenter vers un emplacement accessible sur vos Delivery Controller.
     2. Sur le Controller, naviguez vers l'emplacement du certificat exporté et ouvrez le fichier rui.crt.
   - Téléchargez le certificat à l'aide d'un navigateur Web. Si vous utilisez Internet Explorer, selon votre compte utilisateur, il se peut que vous deviez cliquer avec le bouton droit de la souris sur Internet Explorer et choisir Exécuter en tant qu'administrateur pour pouvoir télécharger et installer le certificat.
     1. Ouvrez votre navigateur Web et créez une connexion Web sécurisée vers le serveur vCenter ; par exemple https://serveur1.domaine1.com
     2. Acceptez les avertissements relatifs à la sécurité.
     3. Cliquez sur la barre d'adresse sur laquelle l'erreur de certificat est affichée.
     4. Affichez le certificat puis cliquez sur l'onglet Détails.
     5. Sélectionnez Copier dans un fichier puis effectuez l'exportation au format .CER, en fournissant un nom lorsque vous êtes invité à le faire.
     6. Enregistrez le certificat exporté.
     7. Naviguez vers l'emplacement du certificat exporté et ouvrez le fichier .CER.
   - Importez directement depuis Internet Explorer exécuté en tant qu'administrateur :
     1. Ouvrez votre navigateur Web et créez une connexion Web sécurisée vers le serveur vCenter ; par exemple https://serveur1.domaine1.com
     2. Acceptez les avertissements relatifs à la sécurité.
     3. Cliquez sur la barre d'adresse sur laquelle l'erreur de certificat est affichée.
     4. Affichez le certificat.
   - Importez le certificat dans le magasin de certificats sur chacun de vos Controller :
     1. Cliquez sur Installer le certificat, sélectionnez Ordinateur local, puis cliquez sur Suivant.
     2. Sélectionnez Placer tous les certificats dans le magasin suivant, puis cliquez sur Parcourir.
     3. Si vous utilisez Windows Server 2008 R2 :
        1. Cochez la case Afficher les magasins physiques.
        2. Développez Personnes autorisées.
        3. Sélectionnez Ordinateur local.
        4. Cliquez sur Suivant, puis cliquez sur Terminer.

        Si vous utilisez Windows Server 2012 ou Windows Server 2012 R2 :

        1. Sélectionnez Personnes autorisées, puis cliquez sur OK.
        2. Cliquez sur Suivant, puis cliquez sur Terminer.

   Important : si vous modifiez le nom du serveur vSphere après l'installation, vous devez générer un nouveau certificat auto-signé sur ce serveur avant d'importer le nouveau certificat.

Utilisez une VM principale pour fournir les bureaux et les applications des utilisateurs. Sur votre hyperviseur :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Installez un VDA sur la VM principale, en sélectionnant l'option d'optimisation du bureau, ce qui améliore les performances.
2. Réalisez un instantané de la VM principale à utiliser comme sauvegarde.

Si vous utilisez Studio pour créer des VM, plutôt que de sélectionner un catalogue de machines existant, spécifiez les informations suivantes lors de la configuration de votre infrastructure d'hébergement pour créer des bureaux virtuels.

1. Sélectionnez le type d'hôte VMware vSphere.
2. Entrez l'adresse du point d'accès pour le kit de développement vCenter.
3. Entrez les informations d'identification du compte d'utilisateur VMware configuré précédemment qui dispose des permissions nécessaires à la création de nouvelles VM. Spécifiez le nom d'utilisateur au format domaine/nomutilisateur.

Empreinte numérique SSL VMware

La fonctionnalité d'empreinte numérique SSL VMware résout une erreur fréquemment signalée lors de la création d'une connexion hôte sur un hyperviseur VMware vSphere. Précédemment, les administrateurs devaient créer manuellement une relation d'approbation entre les Delivery Controller du site et le certificat de l'hyperviseur avant de créer une connexion. La fonctionnalité d'empreinte numérique SSL VMware élimine cette opération manuelle : l'empreinte numérique du certificat non approuvé est stockée dans la base de données du site, de façon à ce que l'hyperviseur puisse être continuellement identifié comme approuvé par XenApp ou XenDesktop, même s'il ne l'est pas par les Controller.

Lors de la création d'une connexion hôte vSphere dans Studio, une boîte de dialogue vous permet d'afficher le certificat de la machine à laquelle vous vous connectez. Vous pouvez alors choisir de l'approuver.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Environnements de virtualisation Microsoft System Center Virtual Machine Manager

Jul 15, 2016

Suivez ce guide si vous utilisez Hyper-V avec Microsoft System Center Virtual Machine Manager (VMM) pour fournir des machines virtuelles.

Cette version prend en charge :

- VMM 2012 : fournit des capacités de gestion améliorées, ce qui vous permet de gérer la totalité du data center virtualisé ainsi que les machines virtuelles. Cette version orchestre maintenant l'application de correctifs à l'hôte de cluster ainsi que l'intégration avec Windows Server Update Services, ce qui vous permet de définir les critères de base des correctifs requis par chaque hôte.
- VMM 2012 SP1 : offre des améliorations des performances pour Machine Creation Services (MCS) lors de l'utilisation de SMB 3.0 sur des serveurs de fichiers avec des volumes partagés en cluster et des réseaux de zone de stockage (SAN). Ces partages de fichiers fournissent un cache peu onéreux et réduisent des E/S sur le stockage SAN améliorant les performances.
- VMM 2012 R2 : permet une gestion à l'échelle des principales fonctionnalités Windows Server 2012 R2, y compris des instantanés des VM en cours d'exécution, un redimensionnement VHDX dynamique et des espaces de stockage.

Cette version prend en charge uniquement les machines virtuelles de génération 1 avec VMM 2012 R2. Lors de la création de VM avec MCS, les VM de deuxième génération n'apparaissent pas dans la liste de sélection d'une VM principale ; ils disposent de Secure Boot activé par défaut, ce qui empêche le VDA de fonctionner correctement.

- Mise à niveau de VMM 2012 vers VMM 2012 SP1 ou VMM 2012 R2
  Pour la configuration requise pour les hôtes VMM et Hyper-V, consultez http://technet.microsoft.com/fr-fr/library/gg610649.aspx. Pour la configuration requise pour la console VMM, consultez http://technet.microsoft.com/fr-fr/library/gg610640.aspx.

  Un cluster Hyper-V mixte n'est pas pris en charge. Un exemple de cluster mixte est un cluster dans lequel la moitié du cluster exécute Hyper-V 2008 et l'autre moitié exécute Hyper-V 2012.

- Mettre à niveau VMM 2008 R2 vers VMM 2012 SP1.
  Si vous effectuez une mise à niveau depuis XenDesktop 5.6 sur VMM 2008 R2, suivez cette séquence pour éviter l'interruption de XenDesktop.
  1. Mettre à niveau VMM 2012 (désormais exécutant XenDesktop 5,6 et VMM 2012) ;
  2. Mettre à niveau XenDesktop vers la version la plus récente (désormais exécutant la dernière version de XenDesktop et de VMM 2012)
  3. Mettre à niveau VMM de 2012 à 2012 SP1 (exécutant désormais XenDesktop et VMM 2012 SP1)
- Mettre à niveau VMM 2012 SP1 vers VMM 2012 R2.
  Si vous démarrez depuis XenDesktop ou XenApp 7.x sur VMM 2012 SP1, suivez cette séquence pour éviter l'interruption de XenDesktop.
  1. Mettre à niveau XenDesktop ou XenApp vers la dernière version (désormais exécutant la dernière version de XenDesktop ou XenApp, et VMM 2012 SP1)
  2. Mettre à niveau VMM 2012 SP1 vers 2012 R2 (désormais exécutant XenDesktop ou XenApp, et VMM 2012 R2)

1. Installez et configurez un hyperviseur.
   1. Installez Microsoft Hyper-V Server et VMM sur vos serveurs. Tous les Delivery Controller doivent se trouver dans la même forêt que les serveurs VMM.
   2. Installez la console System Center Virtual Machine Manager Console sur tous les Controller.
   3. Vérifiez les informations de compte suivantes :
      - Le compte que vous utilisez pour spécifier des hôtes dans Studio est un administrateur VMM ou un administrateur VMM délégué pour les machines Hyper-V appropriées. Si ce compte possède uniquement le rôle d'administrateur délégué dans VMM, les données de stockage ne sont pas répertoriées dans Studio lors du processus de création de l'hôte.
      - Le compte d'utilisateur utilisé pour l'intégration de Studio doit également être un membre du groupe de sécurité Administrateurs local sur chaque serveur Hyper-V pour prendre en charge la gestion du cycle de vie des VM (telles que pour la création, la mise à jour et la suppression de VM).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Remarque : l'installation du Controller sur un serveur exécutant Hyper-V n'est pas prise en charge.

2. Créer une VM principale
   1. Installez Virtual Desktop Agent sur la VM principale, et sélectionnez l'option d'optimisation du bureau. Cela améliore les performances.
   2. Réalisez un instantané de la VM principale à utiliser comme sauvegarde.
3. Créez des bureaux virtuels. Si vous utilisez MCS pour créer des VM, lors de la création d'un site ou d'une connexion.
   1. sélectionnez le type d'hôte de virtualisation Microsoft.
   2. Entrez l'adresse en tant que nom de domaine complet du serveur hôte.
   3. Entrez les informations d'identification du compte d'administrateur créé préalablement disposant des permissions requises pour créer de nouvelles VM.
   4. Dans la boîte de dialogue Détails d'hôte, sélectionnez le cluster ou l'hôte autonome à utiliser pour créer vos nouvelles VM.
      Important : recherchez et sélectionnez un cluster ou un hôte autonome, même si vous utilisez un déploiement d'hôte Hyper-V unique.

Pour les catalogues de machines créés avec MCS sur des partages de fichiers SMB 3 pour le stockage de VM, assurez-vous que les informations d'identification sont définies comme suit pour que des appels provenant de Hypervisor Communications Library (HCL) d'un Controller puissent se connecter avec succès au stockage SMB :

- Les informations d'identification de l'utilisateur VMM doivent inclure un accès en écriture complet au stockage SMB.
- Les opérations de disque virtuel de stockage pendant les événements du cycle de vie des VM sont effectuées par le biais du serveur Hyper-V à l'aide des informations d'identification de l'utilisateur VMM.

Lorsque vous utilisez SMB comme stockage, activez Authentication Credential Security Support Provider (CredSSP) du Controller sur différentes machines Hyper-V individuelles lors de l'utilisation de VMM 2012 SP1 avec Hyper-V sur Windows Server 2012. Pour obtenir davantage d'informations, veuillez consulter la section CTX137465.

À l'aide d'une session à distance PowerShell V3 standard, le HCL utilise CredSSP pour ouvrir une connexion à la machine Hyper-V. Cette fonctionnalité transmet des informations d'identification de l'utilisateur cryptées avec Kerberos à la machine Hyper-V, et les commandes PowerShell dans la session sur la machine Hyper-V distante exécutée avec les informations d'identification fournies (dans ce cas, celles de l'utilisateur VMM), de façon à ce que les commandes de communication vers le stockage fonctionnent correctement.

Les tâches suivantes utilisent des scripts PowerShell constituées initialement dans le HCL et sont alors envoyées à la machine Hyper-V pour agir sur le stockage SMB 3.0.

- **Consolider l'image principale** : une image principale crée un nouveau schéma de provisioning MCS (catalogue de machines). Il clone et écrase la VM principale en préparation pour la création de nouvelles VM à partir du nouveau disque créé (et supprime une dépendance sur la VM principale originale).
  ConvertVirtualHardDisk sur l'espace de noms root\virtualization\v2

  Exemple :
  $ims = Get-WmiObject -class $class -namespace "root\virtualization\v2"; $result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext) $result
- **Créer un disque de différence** : crée un disque de différence à partir de l'image principale générée par la consolidation de l'image principale. Le disque de différence est alors attaché à une nouvelle VM.
  CreateVirtualHardDisk sur l'espace de noms root\virtualization\v2

  Exemple :
  $ims = Get-WmiObject -class $class -namespace "root\virtualization\v2"; $result = $ims.CreateVirtualHardDisk($vhdastext); $result
- **Télécharger des disques d'identité** : le HCL ne peut pas directement télécharger le disque d'identité vers le stockage SMB. Par conséquent, la machine Hyper-V doit télécharger et copier le disque d'identité vers le stockage. Étant donné que la machine Hyper-V ne peut pas lire le disque à partir du Controller, HCL doit tout d'abord copier le disque d'identité via la machine Hyper-V comme suit.
  1. HCL télécharge l'identité de la machine Hyper-V via le partage d'administrateur.
  2. La machine Hyper-V copie le disque vers le stockage SMB via un script PowerShell exécuté dans la session à distance PowerShell. Un dossier est créé sur la machine Hyper-V et les permissions sur ce dossier sont verrouillées pour l'utilisateur VMM uniquement (via la connexion PowerShell distante).
  3. HCL supprime le fichier à partir du partage de l'administrateur.
  4. Lorsque le HCL termine le téléchargement du disque d'identité vers la machine Hyper-V, la session PowerShell distante copie les disques d'identité vers le stockage SMB puis le supprime de la machine Hyper-V.
     Le dossier du disque d'identité est recréé s'il est supprimé de façon à ce qu'il soit disponible pour une éventuelle réutilisation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Télécharger des disques d'identité** : comme les téléchargements, les disques d'identité transfèrent vers le HCL via la machine Hyper-V. Le processus suivant permet de créer un dossier qui ne possède que des permissions utilisateur VMM sur le serveur Hyper-V s'il n'existe pas.
  1. La machine Hyper-V copie le disque à partir du stockage SMB vers le stockage Hyper-V local au travers d'un script PowerShell en cours d'exécution dans la session à distance PowerShell V3.
  2. HCL lit le disque depuis le partage administrateur de la machine Hyper-V dans la mémoire.
  3. HCL supprime le fichier à partir du partage de l'administrateur.
- **Création de Personal vDisk** : si l'administrateur crée les VM dans un catalogue de machine Personal vDisk, vous devez créer un disque vide (PvD).

  L'appel pour créer un disque vide ne nécessite pas d'accès direct au stockage. Si vous possédez des disques PvD qui résident sur différents stockages que le disque du système d'exploitation ou le système d'exploitation principal, puis utiliser le PowerShell à distance pour créer le disque PvD dans un dossier de répertoire qui a le même nom que la VM à partir de laquelle il a été créé. Pour CSV ou LocalStorage, n'utilisez pas de PowerShell à distance. La création du répertoire avant de créer un disque vide évite l'échec de la commande VMM.

  À partir de la machine Hyper-V, réalisez un mkdir sur le stockage.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Environnements de virtualisation Microsoft Azure

Jul 07, 2016

Configuration des connexions

Lorsque vous utilisez Studio pour créer une connexion Microsoft Azure, vous devez disposer d'informations contenues dans le fichier des paramètres de publication Microsoft Azure. Les informations contenues dans ce fichier XML pour chaque abonnement sont similaires à l'exemple ci-dessous (votre certificat de gestion sera beaucoup plus long) :

```
ServiceManagementUrl="https://management.core.windows.net"
Id="o1455234-0r10-nb93-at53-21zx6b87aabb7p"
Name="Test1"
ManagementCertificate=";alkjdflaksdjfl;akjsdfl;akjsdfl; sdjfklasdfilaskjdfkluqweiopruaiopdfaklsdjfjsdilfasdkl;fjerioup" />
```

La procédure ci-dessous suppose que vous créez une connexion à partir de Studio, et que vous avez démarré l'assistant de création de site ou l'assistant de création de connexion.

1. Dans un navigateur, accédez à https://manage.windowsazure.com/publishsettings/index.
2. Téléchargez le fichier de paramètres de publication.
3. Dans Studio, sur la page **Connexion** de l'assistant, lorsque vous sélectionnez le type de connexion Microsoft Azure, cliquez sur Importer.
4. Si vous disposez de plusieurs abonnements, vous êtes invité à sélectionner l'abonnement.

L'ID et le certificat sont automatiquement et de manière silencieuse importés dans Studio.

Les actions d'alimentation utilisant une connexion sont soumises à des seuils. En général, les valeurs par défaut sont appropriées et ne devraient pas être modifiées. Toutefois, vous pouvez modifier une connexion et les modifier (vous ne pouvez pas modifier ces valeurs lorsque vous créez la connexion). Pour de plus amples informations, consultez la section Modifier une connexion.

Machines virtuelles

Lors de la création d'un catalogue de machines dans Studio, la sélection de la taille de chaque machine virtuelle dépend des options présentées par Studio, du coût et des performances du type d'instance de VM sélectionné et de la capacité à monter en charge.

Studio affiche toutes les options d'instance de VM que Microsoft Azure met à disposition dans une région sélectionnée ; Citrix ne peut pas les modifier. Par conséquent, vous devez bien connaître vos applications et leurs besoins en UC, en mémoire et en E/S. Plusieurs options sont disponibles à des niveaux de prix et de performance différents ; veuillez consulter les articles Microsoft suivants afin de mieux comprendre les options.

- MSDN – Tailles de machines virtuelles et de services cloud pour Microsoft Azure : https://msdn.microsoft.com/en-us/library/azure/dn197896.aspx
- Tarification des machines virtuelles : http://azure.microsoft.com/en-us/pricing/details/virtual-machines

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Niveau de base : les machines virtuelles portant le préfixe « Basic » représentent le disque de base. Elles sont limitées principalement par le niveau IOPS Microsoft de 300. Elles ne sont pas recommandées pour les charges de travail OS de serveur (RDSH) ou OS de bureau (VDI).

Niveau standard : les VM de niveau standard apparaissent sous forme de 4 séries : A, D, DS et G.

Série	Affichage dans Studio
A	Très petite, petite, moyenne, grande, très grande, A5, A6, A7, A8, A9, A10, A11. « moyenne » et « grande » sont les options recommandées pour tester les charges de travail avec OS de bureau (VDI) ou OS de serveur (RDSH), respectivement.
D	Standard_D1, D2, D3, D4, D11, D12, D13, D14. Ces machines virtuelles proposent un SSD pour le stockage temporaire.
DS	Standard_DS1, DS2, DS3, DS4, DS11, DS12, DS13, DS14. Ces machines virtuelles proposent un stockage SSD local pour tous les disques.
G	Standard_G1 – G5. Ces machines virtuelles sont destinées à des opérations informatiques haute performance.

Lors du provisioning de machines dans un stockage Premium Azure, veillez à sélectionner une taille de machine qui est prise en charge dans un compte de stockage Premium.

Pour la tarification aux États-Unis, le coût de chaque type d'instance VM par heure est disponible sur http://azure.microsoft.com/en-us/pricing/details/virtual-machines/.

Lorsque vous travaillez avec des environnements de cloud, il est important de bien comprendre vos besoins informatiques réels. Pour les déploiements de preuve de concept ou autres activités de test, il peut être tentant d'avoir recours à des types d'instance de VM haute performance. Il peut également être tentant d'utiliser des VM de moindre performance pour réduire les coûts. La meilleure option est d'utiliser une VM appropriée pour la tâche. Démarrer avec les machines les plus performantes peut ne pas donner les résultats escomptés et s'avérer coûteux dans le temps, au bout d'une semaine dans certains cas. Avec les types d'instance de VM moins performants et moins coûteux, les performances et la convivialité peuvent ne pas être appropriées pour la tâche.

Pour les charges de travail avec OS de bureau (VDI) ou OS de serveur (RDSH), des tests effectués avec LoginVSI et sa charge de travail moyenne ont révélé que les types d'instance Moyenne (A2) et Grande (A3) offraient le meilleur équilibre entre le prix et les performances.

Moyenne (A2) et Grande (A3 ou A5) représentent le meilleur équilibre coût/performances pour les charges de travail d'évaluation. Les niveaux inférieurs ne sont pas recommandés. Des séries de VM plus performantes peuvent proposer à vos applications ou à vos utilisateurs les performances et la convivialité dont ils ont besoin ; cependant, il est préférable de se baser sur l'un de ces trois types d'instance pour déterminer si le coût plus élevé d'une instance de VM plus performante est justifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Plusieurs contraintes affectent la capacité à monter en charge des catalogues d'une unité d'hébergement. Certaines contraintes, telles que le nombre de cœurs d'UC dans un abonnement Azure, peuvent être éliminées en contactant l'assistance Microsoft Azure pour augmenter la valeur par défaut (20). D'autres, telles que le nombre de machines virtuelles dans un réseau virtuel par abonnement (2048), ne peuvent pas être modifiées.

Actuellement, Citrix prend en charge 40 VM dans un catalogue.

Pour augmenter le nombre de VM dans un catalogue ou un hôte, contactez l'assistance Microsoft Azure. Les limites par défaut de Microsoft Azure empêchent l'extension au-delà d'un certain nombre de machines virtuelles ; cependant, ces limites changent souvent, il est donc recommandé de vérifier les dernières informations : http://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/.

Un réseau virtuel Microsoft Azure prend en charge jusqu'à 2 048 VM.

Microsoft recommande une limite de 40 images de VM avec disque standard par service cloud. Lors d'une extension, prenez en compte le nombre de services de cloud requis pour le nombre de VM de l'ensemble de la connexion. Prenez aussi en compte les VM nécessaires pour fournir les applications hébergées.

Contactez l'assistance Microsoft Azure pour déterminer si les limitations par défaut d'UC doivent être augmentées pour vos charges de travail.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Environnements Microsoft System Center Configuration Manager

Jul 07, 2016

Les sites qui utilisent System Center Configuration Manager (Configuration Manager) 2012 pour gérer l'accès aux applications et bureaux sur les machines physiques peuvent étendre cette utilisation à XenApp ou XenDesktop via ces options d'intégration.

- **Citrix Connector 7.5 pour Configuration Manager 2012** : Citrix Connector offre un pont entre Configuration Manager et XenApp ou XenDesktop. Le Connector vous permet d'unifier les opérations quotidiennes sur les environnements physiques que vous gérez avec Configuration Manager et les environnements virtuels que vous gérez avec XenApp ou XenDesktop. Pour de plus amples informations sur Connector, consultez Citrix Connector 7.5 pour System Center Configuration Manager 2012.
- **Fonctionnalité Configuration Manager Wake Proxy** : si votre environnement comprend ou non Citrix Connector, l'utilisation de la fonctionnalité Remote PC Access Wake on LAN requiert Configuration Manager. Pour de plus amples informations, consultez la section ci-dessous.
- Propriété XenApp et XenDesktop : les propriétés XenApp et XenDesktop vous permettent d'identifier les bureaux virtuels Citrix pour la gestion au travers de Configuration Manager. Ces propriétés sont automatiquement utilisées par Citrix Connector, mais elles peuvent également être configurées manuellement, comme décrit dans la section suivante.

Propriétés disponibles pour Microsoft System Center Configuration Manager 2012 et 2012 R2 pour gérer des bureaux virtuels.

Les propriétés booléennes affichées dans Configuration Manager 2012 peuvent apparaître sous la forme de 1 ou 0 au lieu de true ou false.

Les propriétés sont disponibles pour la classe Citrix_virtualDesktopInfo dans l'espace de noms Root\Citrix\DesktopInformation. Les noms des propriétés proviennent du fournisseur WMI (Windows Management Instrumentation) :

Propriété	Description
AssignmentType	Définit la valeur de IsAssigned. Les valeurs autorisées sont : • ClientIP • ClientName • Aucun(e) • User : définit la valeur True à IsAssigned
BrokerSiteName	Site ; renvoie la même valeur que HostIdentifier.
DesktopCatalogName	Catalogue de machines associé au bureau.
DesktopGroupName	Groupe de mise à disposition associé au bureau.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Propriété	Description
HostIdentifier	Site renvoie la même valeur que BrokerSiteName.
IsAssigned	True pour attribuer le bureau à un utilisateur, False pour un bureau aléatoire
IsMasterImage	Permet de prendre des décisions sur l'environnement. Par exemple, vous pouvez installer des applications sur l'image principale et non sur les machines provisionnées, particulièrement si ces machines sont dans un état propre au démarrage des machines. Les valeurs autorisées sont : • True sur une VM qui est utilisé comme une image principale (cette valeur est définie lors de l'installation basée sur une sélection). • Cleared sur une VM qui est provisionnée à partir de cette image.
IsVirtualMachine	True pour une machine virtuelle, False pour une machine physique.
OSChangesPersist	False si l'image du système d'exploitation du bureau est réinitialisée à un nouvel état chaque fois qu'elle est redémarrée, sinon True.
PersistentDataLocation	Emplacement dans lequel le Gestionnaire de configuration stocke les données permanentes. Ceci n'est pas accessible aux utilisateurs.
PersonalvDiskDriveLetter	Pour un bureau comprenant un Personal vDisk, la lettre de lecteur que vous attribuez au Personal vDisk.
BrokerSiteName, DesktopCatalogName, DesktopGroupName et HostIdentifier	Déterminé lorsque le bureau s'enregistre auprès du Controller, ils ont la valeur de Null pour un bureau qui ne s'est pas complètement enregistré.

Pour collecter les propriétés, exécutez un inventaire matériel dans Configuration Manager. Pour afficher les propriétés, utilisez l'Explorateur de ressources Configuration Manager. Dans ce cas, il se peut que les noms incluent des espaces ou varient légèrement des noms de propriété. Par exemple, il se peut que **BrokerSiteName** s'affiche en tant que Broker Site Name. Pour de plus amples informations sur les tâches suivantes, consultez la section http://support.citrix.com/article/ctx140905.

- Configurer Configuration Manager pour collecter les propriétés Citrix WMI du VDA Citrix
- Créer des collections de machines basées sur une requête à l'aide des propriétés Citrix WMI
- Créer des conditions globales basées sur les propriétés Citrix WMI
- Utilisez les conditions globales pour définir les spécifications du type de déploiement de l'application

Vous pouvez également utiliser les propriétés Microsoft dans la classe Microsoft CCM_DesktopMachine dans l'espace de noms Root\ccm_vdi. Pour plus d'informations, veuillez consulter la documentation Microsoft.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour configurer la fonctionnalité Remote PC Access Wake on LAN, procédez comme suit avant d'installer un VDA sur le PC de bureau et utilisez Studio pour créer ou mettre à jour le déploiement Remote PC Access :

- Configurez Configuration Manager 2012 au sein de l'organisation, puis déployez le client Configuration Manager sur toutes les machines Remote PC Access, tout en allouant un délai suffisant pour l'exécution du cycle d'inventaire SCCM programmé (ou en forcer un manuellement, si nécessaire). Les informations d'identification d'accès que vous avez spécifiez dans Studio pour configurer la connexion à Configuration Manager doivent inclure des collections dans l'étendue et le rôle d'opérateur des outils à distance.
- Pour activer la prise en charge d'Intel Active Management Technology (AMT) :
  - La version minimale prise en charge sur le PC doit être AMT 3.2.1.
  - Configurez le PC pour l'utilisation d'AMT avec des certificats et des processus de provisioning associés.
- Pour la prise en charge Configuration Manager Wake Proxy et/ou paquet magique :
  - Configurez Wake on LAN dans chacun des paramètres BIOS du PC.
  - Pour une prise en charge de Configuration Manager Wake Proxy, activez l'option dans Configuration Manager. Pour chaque sous-réseau de l'organisation contenant les PC qui utiliseront la fonctionnalité Remote PC Access Wake on LAN, vérifiez que trois machines ou plus peuvent servir de machines sentinelles.
  - Pour une prise en charge de paquet magique, configurez des routeurs réseau et des pare-feu pour autoriser l'envoi des paquets magiques, en utilisant soit une diffusion dirigée vers un sous-réseau, soit une monodiffusion.

Une fois que vous avez installé le VDA sur les PC de bureau, activez ou désactivez la gestion de l'alimentation lorsque vous créez le déploiement Remote PC Access dans Studio.

- Si vous activez la gestion de l'alimentation, spécifiez les détails de connexion : l'adresse Configuration Manager et les informations d'identification d'accès et un nom.
- Si vous n'activez pas la gestion de l'alimentation, vous pouvez ajouter une connexion de gestion de l'alimentation (Configuration Manager) ultérieurement, puis modifier un catalogue de machines Remote PC Access pour activer la gestion de l'alimentation et spécifier la nouvelle connexion de gestion de l'alimentation.

Vous pouvez modifier la connexion de gestion de l'alimentation pour configurer l'utilisation de Configuration Manager Wake Proxy et des paquets magiques, ainsi que modifier la méthode de transmission des paquets.

Consultez l'article Remote PC Access pour plus d'informations.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Environnements de virtualisation Nutanix

Aug 22, 2016

Suivez ces instructions lors de l'utilisation de Nutanix Acropolis pour fournir des machines virtuelles dans votre déploiement XenApp ou XenDesktop. Le processus d'installation comprend les tâches suivantes :

- Installer et enregistrer le plug-in Nutanix dans votre environnement XenApp ou XenDesktop.
- Créer une connexion à l'hyperviseur Nutanix Acropolis.
- Créer un catalogue de machines qui utilise un instantané d'une image principale que vous avez créée sur l'hyperviseur Nutanix.

Pour de plus amples informations, consultez le Guide d'installation de plugin Nutanix Acropolix MCS, disponible sur le portail d'assistance Nutanix : https://portal.nutanix.com.

Installer et enregistrer le plug-in Nutanix

Après avoir installé les composants XenApp ou XenDesktop, complétez la procédure suivante pour installer et enregistrer le plug-in Nutanix sur les Delivery Controller. Vous pourrez ensuite utiliser Studio pour créer une connexion à l'hyperviseur Nutanix, puis créer un catalogue de machines qui utilise un instantané de l'image principale que vous avez créée dans l'environnement Nutanix.

1. Obtenez le plug-in Nutanix auprès de Nutanix, et installez-le sur les Delivery Controller.
2. Vérifiez qu'un dossier Nutanix Acropolis a été créé dans C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0.
3. Exécutez **C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugin.exe –PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"**.
4. Redémarrez les services suivants : Citrix Host Service, Citrix Broker Service et Citrix Machine Creation Service.
5. Exécutez les applets de commande PowerShell suivantes pour vérifier que le plug-in Nutanix Acropolis a bien été enregistré :

```
Add-PSSnapin Citrix*
Get-HypHypervisorPlugin
```

Créer une connexion à Nutanix

Consultez les articles Créer un site et Connexions et ressources pour des informations complètes sur les pages dans les assistants de création d'une connexion.

Dans l'assistant Création d'un site ou Ajouter une connexion et des ressources, sélectionnez le type de connexion **Nutanix** sur la page **Connexion**, puis spécifiez l'adresse et les informations d'identification de l'hyperviseur, ainsi qu'un nom pour la connexion. Sur la page **Réseau**, sélectionnez un réseau pour l'unité d'hébergement.

Créer un catalogue de machines à l'aide d'un

© 1999-2017 Citrix Systems, Inc. All rights reserved.

instantané Nutanix

Ces informations étayent les instructions disponibles dans l'article Créer des catalogues de machines. Elles décrivent uniquement les champs qui sont uniques à Nutanix.

L'instantané que vous sélectionnez représente le modèle qui sera utilisé pour créer les machines virtuelles dans le catalogue de machines. Avant de créer le catalogue de machines, créez des images et des instantanés dans Nutanix.

- Pour de plus amples informations sur les images principales en général, consultez l'article Créer des catalogues de machines.
- Pour consulter les procédures Nutanix de création d'images et d'instantanés, reportez-vous à la documentation Nutanix référencée ci-dessus.

Les pages **Système d'exploitation** et **Gestion des machines** ne contiennent aucune information spécifique à Nutanix. Suivez les instructions de l'article Créer des catalogues de machines.

Sur la page **Conteneur**, qui est unique Nutanix, sélectionnez le conteneur où les disques des VM seront placés.

Sur la page **Image principale**, sélectionnez l'instantané d'image.

Sur la page **Machines virtuelles**, indiquez le nombre de processeurs virtuels et le nombre de cœurs par vCPU.

Les pages **Cartes réseau**, **Comptes d'ordinateurs** et **Résumé** ne contiennent aucune information spécifique à Nutanix. Suivez les instructions de l'article Créer des catalogues de machines.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Installer à l'aide de l'interface graphique

Jul 07, 2016

Remarque : cet article s'applique à l'installation de composants sur des machines avec systèmes d'exploitation Windows. Pour de plus amples informations sur les VDA pour systèmes d'exploitation Linux, consultez les sections VDA Red Hat Linux et VDA SUSE Linux.

Dans cet article :

- Introduction
- Utiliser le programme d'installation du produit entier
- Utiliser le programme d'installation de VDA autonome.
- Personnaliser un VDA

Introduction

Important : avant de procéder à l'installation, consultez l'article Préparer l'installation qui répertorie les programmes d'installation et les éléments que vous devez connaître avant l'installation. Il vous guide également à travers les éléments que vous verrez et devrez spécifier dans l'interface graphique. Cet article explique comment démarrer l'interface graphique dans un programme d'installation du produit.

Vous pouvez utiliser l'interface graphique pour :

- Installer un ou plusieurs composants principaux : Delivery Controller, Citrix Studio, Citrix Director, le serveur de licences et StoreFront.
- Installer Virtual Delivery Agent (VDA) sur une image principale ou sur une machine physique ou virtuelle. Vous pouvez également personnaliser les scripts fournis sur le support, puis les utiliser pour installer et supprimer des VDA dans Active Directory.
- Personnaliser un VDA précédemment installé.
- Installer le composant serveur d'un serveur d'impression universelle. Le Controller dispose déjà de la fonctionnalité client du serveur d'impression universelle ; vous devez installer uniquement le composant UpsServer sur les serveurs d'impression dans votre environnement. Après avoir installé le composant, suivez les instructions de configuration dans l'article Configurer des imprimantes.
- Mettre à niveau les composants ; consultez l'article Mettre à niveau un déploiement.

Le programme d'installation du produit entier et le programme d'installation de VDA autonome proposent tous les deux une interface graphique.

Utiliser le programme d'installation du produit entier

Vous pouvez utiliser le programme d'installation du produit entier pour installer les composants principaux, les VDA et le composant serveur du serveur d'impression universelle.

1. Téléchargez le pack du produit auprès de Citrix. Des informations d'identification de compte Citrix sont requises pour accéder au site de téléchargement.
2. Décompressez le fichier. Éventuellement, gravez un DVD du fichier ISO.
3. Ouvrez une session sur le serveur sur lequel vous installez les composants, à l'aide d'un compte d'administrateur local.
4. Insérez le DVD dans le lecteur ou montez le fichier ISO. Si le programme d'installation ne démarre pas automatiquement,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

cliquez deux fois sur l'application **Sélection automatique** ou montez le lecteur.
5. Choisissez si vous souhaitez installer XenApp ou XenDesktop.
6. Sélectionnez le composant que vous souhaitez installer :

- Si vous venez juste de démarrer, sélectionnez **Delivery Controller** dans la colonne de gauche. Dans l'écran suivant de l'assistant, vous pouvez choisir les composants à installer sur la machine sur laquelle vous exécutez le programme d'installation (Delivery Controller, Studio, Director, StoreFront, le serveur de licences).
- Si vous avez déjà installé certains composants et souhaitez étendre votre déploiement, cliquez sur le composant que vous souhaitez installer dans la colonne de droite. Cette colonne propose les composants principaux et le serveur d'impression universelle.
- Pour installer un VDA, cliquez sur l'entrée VDA disponible dans la colonne du milieu : le programme d'installation détermine automatiquement celui qui convient au système d'exploitation sur lequel vous exécutez le programme d'installation.

Suivez les instructions de l'assistant. Rappel : l'article Préparer l'installation fournit des explications sur les informations affichées et à spécifier dans l'assistant. Si vous installez un VDA, un redémarrage automatique est activé par défaut lorsque l'installation est terminée ; le redémarrage est nécessaire avant que le VDA puisse être utilisé dans un site.

Utiliser le programme d'installation de VDA autonome.

Important : l'article Préparer l'installation fournit des explications sur les informations que vous voyez et spécifiez lors de l'installation, plus particulièrement sur la gestion des redémarrages et l'espace d'extraction disponible lors de l'utilisation du programme d'installation de VDA autonome.

Des informations d'identification de compte Citrix sont requises pour accéder au site de téléchargement. Vous devez soit disposer de privilèges d'administrateur avant de démarrer l'installation, soit utiliser l'option **Exécuter en tant qu'administrateur**. Désactivez le contrôle de compte d'utilisateur (UAC).

1. Téléchargez le pack approprié à partir de Citrix : **VDAServerSetup.exe** (pour les machines avec OS de serveur) ou **VDAWorkstationSetup.exe** (pour les machines avec OS de bureau). Pour les déploiements d'un OS de serveur auprès d'un utilisateur unique, (par exemple, la mise à disposition de Windows Server 2012 à un utilisateur pour développement Web), utilisez le pack VDAWorkstationSetup.exe. Pour plus d'informations, veuillez consulter l'article Server VDI.
2. Cliquez avec le bouton droit sur le pack et choisissez **Exécuter en tant qu'administrateur**.
3. Suivez les instructions de l'assistant. Un redémarrage automatique est activé par défaut lorsque l'installation est terminée ; le redémarrage est nécessaire avant que le VDA puisse être utilisé dans un site.

Personnaliser un VDA

Si vous voulez personnaliser un VDA que vous avez déjà installé :

1. À partir de la fonctionnalité Windows de suppression ou modification des programmes, sélectionnez **Citrix Virtual Delivery Agent <*version*>**, puis cliquez avec le bouton droit et sélectionnez **Modifier**.
2. Sélectionnez **Personnaliser les paramètres Virtual Delivery Agent**. Lorsque le programme d'installation démarre, vous pouvez changer les adresses Controller, le port TCP/IP auprès duquel s'enregistrer avec le Controller (valeur par défaut = 80), ou si vous souhaitez ouvrir automatiquement les exceptions de port du pare-feu Windows.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Installer à l'aide de la ligne de commande

Jul 13, 2016

Remarque : cet article s'applique à l'installation de composants sur des machines avec systèmes d'exploitation Windows. Pour de plus amples informations sur les VDA pour systèmes d'exploitation Linux, consultez les sections VDA Red Hat Linux et VDA SUSE Linux.

Dans cet article :

- Introduction
- Utiliser le programme d'installation du produit entier
- Utiliser le programme d'installation de VDA autonome.
- Personnaliser un VDA à l'aide de la ligne de commande
- Options de ligne de commande pour l'installation des composants principaux
- Options de ligne de commande pour l'installation d'un VDA
- Installer le Serveur d'impression universelle à l'aide de la ligne de commande

Introduction

Important : avant de procéder à l'installation, consultez l'article Préparer l'installation qui répertorie les programmes d'installation et les éléments que vous devez connaître avant l'installation. Il vous présente également les options que vous pouvez inclure avec une commande. Cet article explique comment démarrer l'interface de ligne de commande dans le programme d'installation d'un produit.

Vous pouvez utiliser une interface de ligne de commande pour :

- Installer un ou plusieurs composants principaux : Delivery Controller, Citrix Studio, Citrix Director, le serveur de licences et StoreFront.
- Installer Virtual Delivery Agent (VDA) sur une image principale ou sur une machine physique ou virtuelle. Vous pouvez également personnaliser les scripts fournis sur le support, puis les utiliser pour installer et supprimer des VDA dans Active Directory.
- Personnaliser un VDA précédemment installé.
- Installer un serveur d'impression universelle, qui provisionne les imprimantes réseau de session. Le Controller dispose déjà de la fonctionnalité Serveur d'impression universelle ; vous devez installer uniquement le Serveur d'impression universelle sur les serveurs d'impression dans votre environnement.
- Mettre à niveau les composants ; consultez l'article Mettre à niveau un déploiement.

Vous pouvez également supprimer des composants de cette version que vous avez précédemment installé, à l'aide des options /remove ou /removeall. Pour de plus amples informations, veuillez consulter l'article Supprimer des composants.

Pour pouvoir suivre la progression de l'exécution de la commande en cours et des valeurs de retour, vous devez être l'administrateur d'origine ou utiliser l'option **Exécuter en tant qu'administrateur**. Pour plus d'informations, veuillez consulter la documentation des commandes Microsoft.

Le programme d'installation du produit entier et le programme d'installation de VDA autonome proposent tous les deux une interface de ligne de commande.

Si vous utilisez les scripts fournis pour installer, mettre à niveau ou supprimer des VDA dans Active Directory, vous pouvez spécifier les options de configuration de VDA répertoriées ci-dessous dans la section Options de ligne de commande pour l'installation d'un VDA. Pour de plus amples informations sur les exemples de scripts, consultez l'article Installer les VDA à

© 1999-2017 Citrix Systems, Inc. All rights reserved.

l'aide de scripts.

Utiliser le programme d'installation du produit entier

Vous pouvez installer les composants principaux et les VDA avec le programme d'installation du produit entier.

- Téléchargez le pack du produit auprès de Citrix. Des informations d'identification de compte Citrix sont requises pour accéder au site de téléchargement.
- Décompressez le fichier. Éventuellement, gravez un DVD du fichier ISO.
- Ouvrez une session sur le serveur sur lequel vous installez les composants, à l'aide d'un compte d'administrateur local.
- Insérez le DVD dans le lecteur ou montez le fichier ISO.
- À partir du répertoire \x64\XenDesktop Setup du support d'installation :

  Pour installer les composants principaux, exécutez la commande **XenDesktopServerSetup.exe**. Utilisez les options répertoriées dans la section Options de ligne de commande pour l'installation des composants principaux ci-dessous.

  Pour installer un VDA, exécutez la commande **XenDesktopVDASetup.exe**. Utilisez les options répertoriées dans la section Options de ligne de commande pour l'installation d'un VDA ci-dessous.

Exemple 1 : la commande suivante installe un Controller XenDesktop, Studio, le système de licences Citrix et SQL Server Express sur le serveur. Les ports requis pour les communications de composants seront ouverts automatiquement.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver
/configure_firewall
```

Exemple 2 : la commande suivante installe un Controller XenApp, Studio, et SQL Server Express sur le serveur. Les ports requis pour la communication de composants seront ouverts automatiquement.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components  controller,desktopstudio
/configure_firewall
```

Exemple 1 : la commande suivante installe un VDA pour OS de bureau Windows et Citrix Receiver à l'emplacement par défaut sur une VM. Ce VDA sera utilisé comme une image principale. Le VDA s'enregistrera initialement auprès du Controller sur le serveur appelé « Contr-Main » dans le domaine « mondomaine », et utilisera des Personal vDisks, la fonctionnalité d'optimisation et l'Assistance à distance Windows.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components  vda,plugins /controllers "Contr-
Main.mydomain.local" /enable_hdx_ports /optimize  /masterimage /baseimage /enable_remote_assistance
```

Exemple 2 : la commande suivante installe un VDA pour OS de bureau Windows et Citrix Receiver à l'emplacement par défaut sur un PC de bureau qui sera utilisé avec Remote PC Access. La machine ne sera pas redémarrée une fois que le VDA est installé ; toutefois un redémarrage est nécessaire avant que le VDA puisse être utilisé. Le VDA s'enregistrera initialement auprès du Controller sur le serveur appelé « Contr-East » dans le domaine « mondomaine », et utilisera UDP pour les paquets audio. Les ports HDX seront ouverts si le service Pare-feu Windows est détecté.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet  /components vda,plugins /controllers "Contr-
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

East.mydomain.local" /enable_hdx_ports /enable_real_time_transport /noreboot

Utiliser le programme d'installation de VDA autonome.

Important : l'article Préparer l'installation fournit des explications sur les informations que vous voyez et spécifiez lors de l'installation, plus particulièrement sur la gestion des redémarrages et l'espace d'extraction disponible lors de l'utilisation du programme d'installation de VDA autonome.

Des informations d'identification de compte Citrix sont requises pour accéder au site de téléchargement. Vous devez soit disposer de privilèges d'administrateur avant de démarrer l'installation, soit utiliser l'option **Exécuter en tant qu'administrateur**.

1. Téléchargez le pack approprié à partir de Citrix : **VDAServerSetup.exe** (pour les machines avec OS de serveur) ou **VDAWorkstationSetup.exe** (pour les machines avec OS de bureau). Pour les déploiements d'un OS de serveur auprès d'un utilisateur unique, (par exemple, la mise à disposition de Windows Server 2012 à un utilisateur pour développement Web), utilisez le pack VDAWorkstationSetup.exe. Pour plus d'informations, veuillez consulter l'article Server VDI.
2. Vous pouvez extraire les fichiers du pack, puis exécuter la commande d'installation, ou uniquement exécuter le pack.

   Pour extraire les fichiers avant l'installation, utilisez **/extract** avec le chemin d'accès absolu ; par exemple, .\VDAWorkstationSetup.exe /extract %temp%\CitrixVDAInstallMedia. Puis dans une commande séparée, exécutez la commande **XenDesktopVdaSetup.exe** à partir du répertoire contenant le contenu extrait (dans l'exemple ci-dessus, CitrixVDAInstallMedia). Utilisez les options répertoriées dans la section Options de ligne de commande pour l'installation d'un VDA ci-dessous.

   Pour simplement exécuter le pack téléchargé, exécutez son nom : **VDAServerSetup.exe** ou **VDAWorkstationSetup.exe**. Utilisez les options répertoriées dans la section Options de ligne de commande pour l'installation d'un VDA ci-dessous. (Si vous êtes familiarisé avec le programme d'installation du produit : exécutez le pack autonome téléchargé comme s'il s'agissait de la commande XenDesktop VdaSetup.exe. sauf pour le nom.)

La commande d'installation suivante est souvent utilisée pour Remote PC Access. Elle installe un VDA sur un PC de bureau physique, sans installer Citrix Receiver ou Citrix Profile Manager. La machine ne sera pas redémarrée automatiquement une fois que le VDA est installé ; toutefois un redémarrage est nécessaire avant que le VDA puisse être utilisé. Lors de sa première exécution, le VDA s'enregistrera auprès du Controller sur le serveur appelé 'Contr-East'. Les ports seront ouverts si le service Pare-feu Windows est détecté.

VDAWorkstationSetup.exe /quiet /components vda /exclude "Citrix User Profile Manager" /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot

> ## Remarque
>
> L'exclusion de Citrix User Profile Manager à partir de l'installation de ces paramètres affecte la surveillance et la résolution des problèmes des VDA avec Citrix Director. Sur les pages Détails de l'utilisateur et Point de terminaison, les panneaux Personnalisation et Durée de l'ouverture de session échoueront. Sur les pages Tableau de bord et Tendances, le panneau Durée moyenne d'ouverture de session affichera les données uniquement pour les machines sur lesquelles Profile Management est installé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Personnaliser un VDA à l'aide de la ligne de commande

Une fois que vous avez installé un VDA, vous pouvez personnaliser plusieurs paramètres. À partir du répertoire \x64\XenDesktop Setup du support du produit, exécutez la commande **XenDesktopVdaSetup.exe**, à l'aide d'une ou plusieurs des options suivantes, qui sont décrites dans la section Options de ligne de commande pour l'installation d'un VDA ci-dessous.

- /reconfigure : cette option est requise lors de la personnalisation d'un VDA
- /h ou/help
- /quiet
- /noreboot
- /controllers
- /portnumber port
- /enable_hdx_ports

Options de ligne de commande pour l'installation des composants principaux

Le tableau suivant dresse la liste des options valides pour la commande **XenDesktopServerSetup.exe**.

Option	Description
/components composant [,composant] ...	Liste séparée par des virgules des composants à installer ou supprimer. Les valeurs autorisées sont : • CONTROLLER – Controller • DESKTOPSTUDIO – Studio • DESKTOPDIRECTOR – Director • LICENSESERVER - Serveur de licences Citrix • STOREFRONT – StoreFront Si cette option est omise, tous les composants sont installés (ou supprimés, si l'option /remove est également spécifiée).
/configure_firewall	Ouvre tous les ports du pare-feu Windows requis par les composants installés, si le service Pare-feu Windows est en cours d'exécution, même si le pare-feu n'est pas activé. Si vous utilisez un pare-feu tiers ou aucun pare-feu, vous devez ouvrir les ports manuellement.
/help ou/h	Affiche la commande d'aide.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

/installdir répertoire	Répertoire vide existant où les composants seront installés. Valeur par défaut : c:\Program Files\Citrix.
/logpath chemin	Emplacement du fichier journal. Le dossier spécifié doit déjà exister ; il n'est pas créé par le programme d'installation. Valeur par défaut = "%TEMP%\Citrix\XenDesktop Installer"
/no_remote_assistance	(Valide uniquement lors de l'installation de Director.) Désactive la fonctionnalité d'observation utilisateur qui utilise l'Assistance à distance Windows.
/noreboot	Empêche un redémarrage après l'installation. (Pour la plupart des composants principaux, aucun redémarrage n'est activé par défaut).
/nosql	Empêche l'installation de Microsoft SQL Server Express sur le serveur sur lequel vous installez le Controller. Si cette option est omise, SQL Server Express sera installé.
/quiet ou /passive	Aucune interface utilisateur ne s'affiche lors de l'installation. La seule preuve de l'installation est dans le Gestionnaire des tâches Windows. Si cette option n'est pas utilisée, l'interface graphique démarre.
/remove	Supprime les principaux composants spécifiés avec l'option /components.
/removeall	Supprime tous les principaux composants installés.
/tempdir répertoire	Répertoire qui contient les fichiers temporaires durant l'installation. Valeur par défaut = c:\Windows\Temp.
/xenapp	Installe XenApp. Si cette option est omise, XenDesktop est installé.

Options de ligne de commande pour l'installation d'un VDA

Le tableau suivant dresse la liste des options valides pour la commande **XenDesktopVDASetup.exe**.

Lors de l'installation de Virtual Desktop Agent en vue d'une utilisation avec Remote PC Access, spécifiez uniquement des options qui sont valides sur des machines physiques (pas de VM ou des images principales) et pour les VDA pour système d'exploitation de bureau Windows.

Sauf spécification contraire, les options s'appliquent aux machines physiques et virtuelles, et aux VDA pour OS de bureau

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Windows et OS de serveur Windows.

Important

Dans XenApp et XenDesktop 7.9, utilisez uniquement la ligne de commande pour les déploiements **Remote PC Access** et ne changez pas l'ordre de syntaxe pour /components et /remotepc. Par exemple :

VDAWorkstationSetup.exe /components vda /controllers "example.delivery.controller.net" /remotepc /EXCLUDE "AppDisks VDA Plug-in" /enable_hdx_ports /noreboot /quiet

Si l'option /remotepc est utilisée avant /composants, l'option /remotepc est ignorée.

Option	Description
/baseimage	(Valide uniquement lors de l'installation d'un VDA pour OS de bureau Windows sur une VM). Permet l'utilisation de Personal vDisks avec une image principale. Pour de plus amples informations, consultez les articles Personal vDisk.
/components component[,component]	Liste séparée par des virgules des composants à installer ou supprimer. Les valeurs autorisées sont : • VDA : installe le VDA • PLUGINS : installe Citrix Receiver pour Windows (CitrixReceiver.exe) Par exemple, pour installer le VDA, mais pas Citrix Receiver, spécifiez l'option /components vda. Si cette option est omise, tous les composants sont installés.
/controllers "contrôleur [contrôleur] [...]"	Noms de domaines complets (FQDN) séparés par des virgules des Controller avec lesquels le VDA peut communiquer, entourés de guillemets. Ne spécifiez pas à la fois les options /site_guid et /controllers.
/enable_framehawk_port	Ouvre les ports UDP utilisés par Framehawk. Valeur par défaut = false
/enable_hdx_3d_pro	Installe le VDA pour HDX 3D Pro. Pour plus d'informations, veuillez consulter l'article HDX 3D Pro.
/enable_hdx_ports	Ouvre les ports du pare-feu Windows requis par le Controller et les fonctionnalités que vous avez spécifiées (assistance à distance Windows, transport en temps réel et optimisation), si le service Pare-feu Windows est détecté, même si le pare-feu n'est pas activé. Si vous utilisez un autre pare-feu ou aucun pare-feu, vous devez configurer le pare-feu manuellement.
/enable_real_time_transport	Active ou désactive l'utilisation d'UDP pour les paquets audio (Real-Time Audio Transport pour l'audio). L'activation de cette fonctionnalité peut améliorer les performances audio. (Incluez l'option /enable_hdx_ports si vous souhaitez que les ports UDP soient ouverts automatiquement si le service Pare-feu Windows est détecté.)
/enable_remote_assistance	Active la fonctionnalité d'observation dans l'Assistance à distance Windows pour l'utiliser avec Director. Si vous spécifiez cette option, Windows ouvre le port TCP 3389 dans le pare-feu, même si vous omettez l'option /enable_hdx_ports.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

/exclude "component"[,"component"]	Empêche l'installation d'un ou de plusieurs composants facultatifs séparés par des virgules, entourés de guillemets. Par exemple, l'installation ou la mise à niveau d'un VDA sur une image qui n'est pas gérée par Machine Creation Services ne nécessite pas les composants Personal vDisk ou Machine Identity Service. Les valeurs autorisées sont : • Personal vDisk • Machine Identity Service • Citrix User Profile Manager L'exclusion de Citrix User Profile Manager de l'installation de VDA affecte la surveillance et la résolution des problèmes des VDA avec Citrix Director. Sur les pages Détails de l'utilisateur et Point de terminaison, les panneaux Personnalisation et Durée de l'ouverture de session échoueront. Sur les pages Tableau de bord et Tendances, le panneau Durée moyenne d'ouverture de session affichera les données uniquement pour les machines sur lesquelles Profile Management est installé.
/h ou/help	Affiche la commande d'aide.
/installdir répertoire	Répertoire vide existant où les composants seront installés. Valeur par défaut : c:\Program Files\Citrix.
/logpath chemin	Emplacement du fichier journal. Le dossier spécifié doit déjà exister ; il n'est pas créé par le programme d'installation. (Cette option n'est pas disponible dans l'interface graphique.) Valeur par défaut = "%TEMP%\Citrix\XenDesktop Installer"
/masterimage	(Valide uniquement lors de l'installation d'un VDA sur une VM) Définit le VDA en tant qu'image principale.
/no_appv	Empêche l'installation des composants Citrix App-V. Pour plus d'informations, veuillez consulter l'article App-V.
/nocitrixwddm	(Valide uniquement sur les machines Windows 7 qui ne contiennent pas un pilote WDDM). Cette option désactive l'installation du pilote Citrix WDDM.
/nodesktopexperience	(Valide uniquement lors de l'installation d'un VDA pour OS de serveur Windows). Empêche l'activation de la fonctionnalité Enhanced Desktop Experience. Cette fonctionnalité est contrôlée par le paramètre de stratégie Citrix Expérience de bureau améliorée.
/noreboot	Empêche un redémarrage après l'installation. Le VDA ne sera entièrement disponible qu'après un redémarrage.
/optimize	Permet l'optimisation des VDA exécutés dans une VM sur un hyperviseur. L'optimisation de VM comprend la désactivation des fichiers en mode déconnecté, la désactivation de la défragmentation en arrière-plan et la réduction de la taille du journal d'événements. Ne spécifiez pas cette option pour Remote PC Access. Pour plus d'informations sur l'outil d'optimisation, veuillez consulter l'article CTX125874.
/portnumber port	(Valide uniquement si l'option /reconfig est spécifiée.) Numéro de port à activer pour les communications entre le VDA et le Controller. Le port précédent configuré est désactivé, à moins qu'il s'agisse du port 80.
/quiet ou /passive	Aucune interface utilisateur ne s'affiche lors de l'installation. La seule preuve de l'installation et de la configuration est dans le Gestionnaire des tâches Windows. Si cette option n'est pas utilisée, l'interface graphique démarre.
/reconfig	Personnalise les paramètres VDA précédemment configurés lorsqu'il est utilisé avec les options /portnumber,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	/controllers ou /enable_hdx_ports. Si vous spécifiez cette option sans spécifier également l'option/quiet, l'interface graphique de personnalisation de VDA démarre.
/remotepc	Empêche l'installation des composants suivants sur un OS de bureau (poste de travail) : • Composant App V : Citrix Personalization for App-V - VDA • Composant Upm : Citrix User Profile Manager • Composant UpmVdaPlugin : Citrix User Profile Manager WMI Plugin • Composant Mps : Machine Identity Service • Composant VDisk : Personal vDisk Durant une mise à niveau, si l'un de ces composants est installé, il sera détecté et mis à niveau par le programme d'installation.
/remove	Supprime les composants spécifiés avec l'option /components.
/removeall	Supprime tous les composants VDA installés.
/servervdi	Installe un VDA pour OS Windows Desktop sur un Windows Server pris en charge. Évitez cette option lors de l'installation d'un VDA pour OS Windows Server sur un Windows Server. Avant d'utiliser cette option, consultez l'article Server VDI. (Cette option n'est pas disponible dans l'interface graphique.)
/site_guid guid	Identificateur global unique (GUID) de l'unité d'organisation Active Directory du site. Associe un bureau virtuel à un site lorsque vous utilisez Active Directory pour la découverte (la mise à jour automatique est la méthode recommandée et la méthode de découverte par défaut). Le GUID du site est une propriété de site affichée dans Studio. Ne spécifiez pas à la fois les options /site_guid et /controllers.
/tempdir répertoire	Répertoire sur lequel stocker les fichiers temporaires durant l'installation. (Cette option n'est pas disponible dans l'interface graphique.) Valeur par défaut = c:\Windows\Temp.
/virtualmachine	(Valide uniquement lors de l'installation d'un VDA sur une VM) Remplace la détection par le programme d'installation d'une machine physique, où les informations du BIOS transmises aux VM les font passer pour des machines physiques.
/xa_server_location url	URL du serveur des applications du serveur Windows.

Installer le Serveur d'impression universelle à l'aide de la ligne de commande

Remarque : si vous installez le composant UpsServer sur un serveur Windows 2008 32 bits, suivez les étapes décrites dans Avant d'installer le serveur d'impression universelle sur un serveur Windows 2008 32 bits.

Exécutez l'une des commandes suivantes sur chaque serveur d'impression :

- Sur un système d'exploitation 32 bits pris en charge : à partir du répertoire \x86\Universal Print Server\ sur le support

© 1999-2017 Citrix Systems, Inc. All rights reserved.

d'installation Citrix, exécutez **UpsServer_x86.msi**.
- Sur un système d'exploitation 64 bits pris en charge : à partir du répertoire \x64\Universal Print Server\ sur le support d'installation Citrix, exécutez **UpsServer_x64.msi**.

Après avoir installé le composant du serveur d'impression universelle sur vos serveurs d'impression, configurez ce dernier à l'aide des instructions de l'article Provisionner les imprimantes.

Avant de déployer UpsServer_x86.msi sur une machine Windows 2008 32 bits, vous devez régler la version minimum pour Windows Installer pour les fichiers cdf_x86.msi et UpsServer_x86.msi, soit à l'aide de scripts Visual Basic ou d'un outil tel que Orca.

1. Copiez les versions 32 bits des fichiers msi CDF et UPS (**cdf_x86.msi** et **UpsServer_x86.msi**) dans un dossier temporaire.
2. Installez le script WiSumInf.vbs ou l'outil Orca, disponibles dans le package Windows SDK Components for Windows Installer Developers. Pour de plus amples informations sur le script, consultez l'article MSDN Manage Summary Information.
3. Modifiez la version minimum pour Windows Installer à l'aide de l'une des méthodes ci-dessous :

   À l'aide du script WiSumInf.vbs : copiez WiSumInf.vbs dans le même dossier temporaire que les deux msi de Citrix. Ensuite, exécutez le script pour chaque package avec les paramètres **WiSumInf.vbs cdf_x86.msi Pages=405** et **WiSumInf.vbs UpsServer_x86.msi Pages=405**.

   Utilisation de l'outil Orca : ouvrez chacun des packages cdf_x86.msi et UpsServer_x86.msi, accédez au menu View > Summary Information et définissez la valeur de la zone de texte **Schema** sur **405**.

Après avoir effectué la procédure ci-dessus, installez le serveur d'impression universelle sur le serveur d'impression.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Installer les VDA à l'aide de scripts

Jul 07, 2016

Remarque : cet article s'applique à l'installation de composants sur des machines avec systèmes d'exploitation Windows. Pour de plus amples informations sur les VDA pour systèmes d'exploitation Linux, consultez les sections VDA Red Hat Linux et VDA SUSE Linux.

Le support d'installation contient des exemples de scripts qui permettent d'installer, mettre à niveau ou supprimer les VDA pour les groupes de machines dans Active Directory. Vous pouvez également appliquer les scripts à des machines individuelles, et les utiliser pour gérer les images principales utilisées par Machine Creation Services et Provisioning Services.

Accès requis :

- Les scripts doivent disposer d'un accès en lecture Tout le monde sur le partage réseau sur lequel figure la commande d'installation. La commande d'installation est XenDesktopVdaSetup.exe à partir de l'image ISO du produit complet ou VDAWorkstationSetup.exe ou VDAServerSetup.exe depuis le programme d'installation autonome.
- Les informations de journalisation sont stockées sur chaque machine locale. Si vous souhaitez consigner les résultats de manière centralisée à des fins de vérification et d'analyse, les scripts doivent disposer d'un accès en lecture et écriture Tout le monde sur le partage réseau approprié.

Pour vérifier les résultats de l'exécution d'un script, examinez le partage du journal central. Les journaux consignés incluent le journal du script, le journal du programme d'installation et les journaux d'installation MSI. Chaque tentative d'installation ou de suppression est enregistrée dans un dossier horodaté. Le titre du dossier indique si l'opération a réussi avec le préfixe PASS ou FAIL. Plutôt que d'effectuer une recherche locale sur les machines cibles, vous pouvez utiliser les outils de recherche d'annuaire standard pour trouver rapidement une installation ayant échoué ou une suppression dans le journal central.

Important : avant de commencer l'installation, lisez et complétez les tâches décrites dans l'article Préparer l'installation.

Pour installer ou mettre à niveau des VDA à l'aide du script

1. Obtenez le script exemple InstallVDA.bat à partir de \Support\AdDeploy\ sur le support d'installation. Citrix vous recommande d'effectuer une sauvegarde du script d'origine avant de le personnaliser.
2. Modifiez le script :
   - Spécifiez la version du VDA à installer : SET DESIREDVERSION. Par exemple, la version 7 peut être spécifiée en tant que 7.0 ; la valeur totale peut être localisée sur le support d'installation dans le fichier ProductVersion.txt (par exemple 7.0.0.3018) ; toutefois, une correspondance totale n'est pas requise.
   - Spécifiez l'emplacement du partage réseau à partir duquel le programme d'installation va être appelé. Pointez vers la racine de la structure (point le plus haut de l'arborescence) : la version appropriée du programme d'installation (32 bits ou 64 bits) sera automatiquement appelée lorsque le script s'exécute. Par exemple : SET DEPLOYSHARE =\\fileserver1\share1.
   - Si vous le souhaitez, vous pouvez spécifier un emplacement de partage réseau pour le stockage des journaux centralisés. Par exemple : SET LOGSHARE=\\fileserver1\log1.
   - Spécifiez les options de configuration VDA comme décrit dans l'article Installer à l'aide de la ligne de commande. Les options /quiet et /noreboot sont incluses par défaut dans le script et sont requises : SET COMMANDLINEOPTIONS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

=/QUIET /NOREBOOT.

3. À l'aide de scripts de démarrage de stratégie de groupe, attribuez le script à l'unité d'organisation dans Active Directory où vos machines se trouvent. Cette unité d'organisation doit uniquement contenir les machines sur lesquelles vous souhaitez installer le VDA. Lorsque les machines dans l'unité d'organisation sont redémarrées, le script s'exécute sur toutes ces machines, et installer un VDA sur chaque machine équipée d'un système d'exploitation pris en charge.

Pour supprimer des VDA à l'aide du script

1. Obtenez le script exemple UninstallVDA.bat à partir de \Support\AdDeploy\ sur le support d'installation. Citrix vous recommande d'effectuer une sauvegarde du script d'origine avant de le personnaliser.
2. Modifiez le script :
   - Spécifiez la version du VDA à supprimer : SET CHECK_VDA_VERSION. Par exemple, la version 7 peut être spécifiée en tant que 7.0 ; la valeur totale peut être localisée sur le support d'installation dans le fichier ProductVersion.txt (par exemple 7.0.0.3018) ; toutefois, une correspondance totale n'est pas requise.
   - Si vous le souhaitez, vous pouvez spécifier un emplacement de partage réseau pour le stockage des journaux centralisés.
3. À l'aide de scripts de démarrage de stratégie de groupe, attribuez le script à l'unité d'organisation dans Active Directory où vos machines se trouvent. Cette unité d'organisation doit uniquement contenir les machines sur lesquelles vous souhaitez supprimer le VDA. Lorsque les machines dans l'unité d'organisation sont redémarrées, le script s'exécute sur toutes ces machines et supprime un VDA de chaque machine.

Résolution des problèmes

Le script génère des fichiers journaux internes qui décrivent la progression de l'exécution du script. Le script copie un journal Kickoff_VDA_Startup_Script sur le partage de journal central quelques secondes après le démarrage du déploiement sur la machine, de façon à ce que vous puissiez vérifier que le processus fonctionne. Si ce journal n'est pas copié sur le partage de journal central comme prévu, vous pouvez trouver davantage d'informations de dépannage en inspectant la machine locale : le script place deux fichiers journaux de débogage dans le dossier %temp% de chaque machine à des fins de dépannage anticipé :

- Kickoff_VDA_Startup_Script_.log
- VDA_Install_ProcessLog_.log

Vérifiez le contenu de ces journaux pour vous assurer que le script :

- S'exécute comme prévu.
- Détecte correctement le système d'exploitation cible.
- Est correctement configuré pour pointer vers le ROOT du partage DEPLOYSHARE (contient le fichier appelé AutoSelect.exe).
- Est capable de s'authentifier auprès des partages DEPLOYSHARE et LOG.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Installer des VDA Red Hat Linux

Jul 07, 2016

Vous pouvez créer des bureaux virtuels Linux basés sur la distribution Red Hat/CentOS. Préparez les machines virtuelles Linux, installez-y le nouveau logiciel, configurez le Delivery Controller, puis utilisez Studio pour mettre les bureaux à la disposition des utilisateurs.

Pour plus de détails, veuillez consulter les informations contenues dans cet article.

> **Remarque**
>
> Nous avons vérifié que les commandes shell Linux utilisées dans ce document fonctionnaient avec le shell GNU Bash.

Cet article comprend les sections suivantes :

- Configuration système requise
- Configurer des Delivery Controller
- Préparer les machines Linux pour l'installation de VDA
- Configurer un catalogue et un groupe de mise à disposition de machines Linux
- Installer le logiciel VDA Linux
- Exécuter le logiciel VDA
- Désinstaller le logiciel VDA Linux
- Résolution des problèmes
- Problèmes connus
- Glossaire

Configuration système requise

Les distributions Linux suivantes sont prises en charge par le produit Linux Virtual Desktop :

- SUSE Linux Enterprise :
  - Desktop 11 Service Pack 4
  - Desktop 12 Service Pack 1
  - Server 11 Service Pack 4
  - Server 12 Service Pack 1
- Red Hat Enterprise Linux
  - Workstation 6.7
  - Workstation 7.2
  - Server 6.7
  - Server 7.2
- CentOS Linux
  - CentOS 6.7

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- CentOS 7.2

> **Remarque**
>
> Dans tous les cas, l'architecture de processeur prise en charge est x86-64.

> **Conseil**
>
> CentOS Linux est pris en charge depuis la version 1.3. Les informations d'installation contenues dans cet article s'appliquent également à CentOS.

Les versions suivantes de XenDesktop sont prises en charge par le VDA Linux :

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7,9

Le processus de configuration pour les VDA Linux diffère légèrement des VDA Windows. Toutefois, toute batterie de Delivery Controller est capable de négocier les connexions aux bureaux Windows et Linux.

> **Remarque**
>
> Le VDA Linux n'est pas compatible avec la version XenDesktop 7.0 ou une version antérieure.

Les versions suivantes de Citrix Receiver sont prises en charge :

- Citrix Receiver pour Windows version 4.4 ou version ultérieure (correspond à la version v14.4 de wfica32.exe)
- Citrix Receiver pour Linux version 13.3 ou version ultérieure
- Citrix Receiver pour Mac OS X version 12.1 ou version ultérieure
- Citrix Receiver pour Android version 3.8 ou version ultérieure
- Citrix Receiver pour iOS version 6.1.4 ou version ultérieure
- Citrix Receiver pour Chrome/HTML5 version 2.0 (uniquement via Access Gateway)

Les hyperviseurs suivants sont pris en charge pour l'hébergement des VM invité de VDA Linux :

- XenServer

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- VMware ESX et ESXi
- Microsoft Hyper-V

L'hébergement de bare metal est également pris en charge.

> **Conseil**
>
> Reportez-vous à la documentation du fabricant de l'hyperviseur pour obtenir la liste des plates-formes prises en charge.

Les produits ou packages d'intégration d'Active Directory suivants sont pris en charge par le VDA Linux :

- Samba Winbind
- Services d'authentification Quest v4.1 ou version ultérieure
- Centrify DirectControl

> **Conseil**
>
> Reportez-vous à la documentation du fabricant du package d'intégration d'Active Directory pour obtenir la liste des plates-formes prises en charge.

Les hyperviseurs, distributions Linux et GPU NVIDIA GRID™ suivants sont requis pour la prise en charge de HDX 3D Pro.

Hyperviseurs

Les hyperviseurs suivants sont pris en charge :

- XenServer
- VMware ESX et ESXi

Distributions Linux

La distribution Linux suivante prend en charge HDX 3D Pro :

- Red Hat Enterprise Linux - Workstation 7.2

Processeur graphique

Les GPU suivants sont pris en charge :

- NVIDIA GRID™ 3.0 - Tesla M60
- NVIDIA GRID™ - K2

Configurer des Delivery Controller

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenDesktop 7.7 ou version ultérieure contient les modifications nécessaires à la prise en charge de Linux Virtual Desktop ; cependant, pour les versions précédentes, un correctif ou un script de mise à jour est requis. Leur installation et leur vérification sont décrites dans cette section.

Pour XenDesktop 7.6 SP2, appliquez le correctif Update 2 pour mettre à jour le broker pour Linux Virtual Desktop. Les correctifs Update 2 sont disponibles ici :

- CTX142438 : Correctif Update 2 - Pour Delivery Controller 7.6 (32 bits) – Anglais
- CTX142439 : Correctif Update 2 - Pour Delivery Controller 7.6 (64 bits) – Anglais

Pour les versions antérieures de XenDesktop, un script PowerShell nommé **Update-BrokerServiceConfig.ps1** est fourni ; il met à jour la configuration du service de broker. Il est disponible dans le package suivant :

- citrix-linuxvda-scripts-1.3.0.zip

Répétez les étapes suivantes sur *chaque* Delivery Controller de la batterie :

1. Copiez le script **Update-BrokerServiceConfig.ps1** sur la machine Delivery Controller.
2. Ouvrez une console Windows PowerShell dans le contexte de l'administrateur local.
3. Accédez au dossier contenant le script.
4. Exécutez le script :

```
.\Update-BrokerServiceConfig.ps1
```

> ## Remarque
>
> Par défaut, PowerShell est configuré pour empêcher l'exécution des scripts PowerShell. Si le script ne réussit pas à s'exécuter, il se peut que vous deviez modifier la stratégie d'exécution PowerShell avant d'essayer à nouveau :
>
> ```
> Set-ExecutionPolicy Unrestricted
> ```

Le script **Update-BrokerServiceConfig.ps1** met à jour le fichier de configuration du service Broker avec de nouveaux points de terminaison WCF requis par le VDA Linux et redémarre le service de broker. Le script détermine automatiquement l'emplacement du fichier de configuration du service de broker. Une copie de sauvegarde du fichier de configuration d'origine est créée dans le même répertoire avec l'extension **.prelinux**.

Ces modifications n'ont pas d'impact sur la négociation des VDA Windows configurés pour utiliser la même batterie de Delivery Controller. Cela permet d'utiliser une seule batterie pour gérer et négocier les sessions pour les VDA Windows et Linux en toute facilité.

Pour vous assurer que les modifications de configuration requises ont été appliquées à un Delivery Controller, vérifiez si la chaîne **EndpointLinux** apparaît bien cinq fois dans le fichier :

```
%PROGRAMFILES%\Citrix\Broker\Service\BrokerService.exe.config
```

À partir de l'invite de commande de Windows, connecté en tant qu'administrateur local :

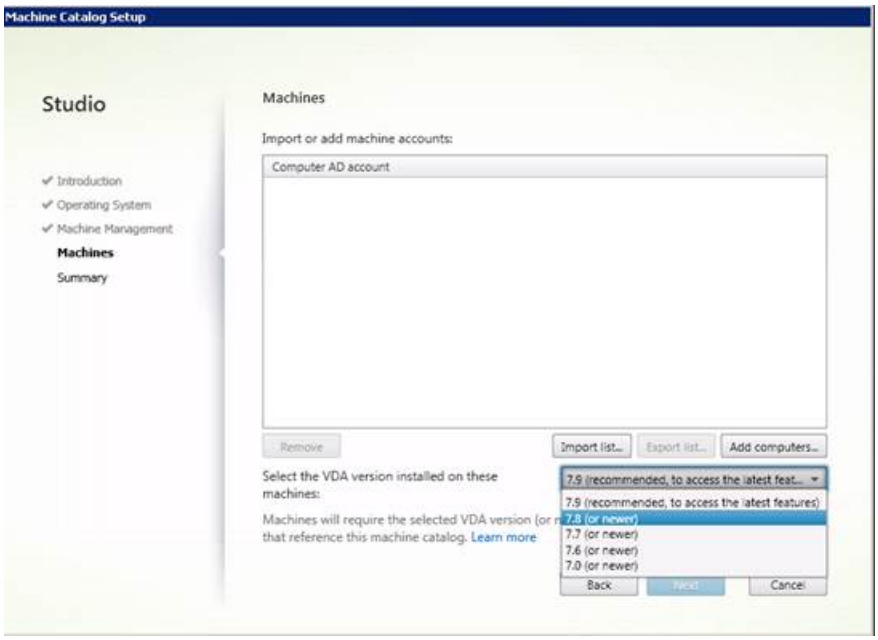
© 1999-2017 Citrix Systems, Inc. All rights reserved.

cd "%PROGRAMFILES%"\Citrix\Broker\Service\

findstr EndpointLinux BrokerService.exe.config

Important

À partir de la version 1.3, l'agent broker du VDA Linux est défini sur XenApp/XenDesktop 7.8. Toutefois, lors de l'ajout d'un catalogue de machines à l'aide de l'écran **Création d'un catalogue de machines** de Studio, la valeur par défaut est automatiquement définie sur la version 7.9. Vous devez définir explicitement la version du VDA installée sur **7.8 (ou ultérieure)**. Référez-vous à l'image ci-dessous.



Préparer la machine Linux pour l'installation de VDA

Citrix recommande que le réseau soit connecté et correctement configuré avant de continuer.

RHEL 6 uniquement : définir le nom de l'hôte

Pour vous assurer que le nom d'hôte de la machine est indiqué correctement, modifiez le fichier **/etc/sysconfig/network** pour qu'il contienne uniquement le nom d'hôte de la machine.

HOSTNAME=**nom d'hôte**

RHEL 7 uniquement : définir le nom de l'hôte

Pour vous assurer que le nom d'hôte de la machine est indiqué correctement, modifiez le fichier **/etc/hostname** pour qu'il contienne uniquement le nom d'hôte de la machine.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Attribuer une adresse de bouclage au nom de l'hôte

Pour vous assurer que le nom de domaine DNS et le nom de domaine complet (FQDN) de la machine sont indiqués correctement, modifiez la ligne suivante du fichier **/etc/hosts** pour qu'elle inclue le nom de domaine complet et le nom d'hôte dans les deux premières entrées :

127.0.0.1 **hostname-fqdn hostname** localhost localhost.localdomain localhost4 localhost4.localdomain4

Par exemple :

127.0.0.1 vda01.example.com vda01 localhost localhost.localdomain localhost4 localhost4.localdomain4

Supprimez toute autre référence à **hostname-fqdn** ou **hostname** des autres entrées du fichier.

Remarque

Le VDA Linux ne prend actuellement pas en charge la troncation du nom NetBIOS ; par conséquent, le nom de l'hôte ne doit pas comporter plus de 15 caractères.

Conseil

Utilisez uniquement les caractères a-z, 0-9 et tiret (-). Évitez le caractère de soulignement (_), les espaces et autres symboles. Ne démarrez pas un nom de l'hôte par un chiffre et ne le terminez pas par un tiret.

Vérifier le nom de l'hôte

Vérifiez que le nom d'hôte est correctement configuré :

hostname

Doit renvoyer uniquement le nom d'hôte de la machine et non pas son nom de domaine complet (FQDN).

Vérifiez que le nom de domaine complet est correctement configuré :

hostname -f

Doit renvoyer le nom de domaine complet de la machine.

Vérifier la résolution de nom et l'accessibilité du service

Vérifiez que vous pouvez résoudre le nom de domaine complet et effectuer un sondage ping sur le contrôleur de domaine et le Delivery Controller XenDesktop :

nslookup **domain-controller-fqdn**

ping **domain-controller-fqdn**

nslookup **delivery-controller-fqdn**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ping **delivery-controller-fqdn**

Si vous ne pouvez pas résoudre le nom de domaine complet ou effectuer un sondage ping sur l'une de ces machines, reprenez les étapes avant de continuer.

Il est très important de maintenir la synchronisation de l'horloge entre les VDA, les contrôleurs XenDesktop et les contrôleurs de domaine. L'hébergement du VDA Linux en tant que machine virtuelle peut entraîner des problèmes de décalage d'horloge. Pour cette raison, il est recommandé de synchroniser l'heure avec un service de temps à distance.

RHEL 6.x et versions antérieures utilisent le démon NTP (ntpd) pour la synchronisation d'horloge, tandis qu'un environnement RHEL 7.x par défaut utilise le démon Chrony le plus récent (chronyd). Le processus de configuration et de fonctionnement entre les deux services est similaire.

RHEL 6 uniquement : configurer le service NTP

En tant que root, modifiez **/etc/ntp.conf** et ajoutez une entrée de serveur pour chaque serveur de temps distant :

server **peer1-fqdn-or-ip-address** iburst

server **peer2-fqdn-or-ip-address** iburst

Dans un déploiement type, l'heure doit être synchronisée depuis les contrôleurs de domaine locaux et non pas directement depuis des serveurs de pool NTP publics. Ajoutez une entrée de serveur pour chaque contrôleur de domaine Active Directory du domaine.

Supprimez toute autre entrée **server** répertoriée, y compris les entrées d'adresse IP de bouclage, localhost et ***.pool.ntp.org** de serveur public.

Enregistrez les modifications et redémarrez le démon NTP :

sudo /sbin/service ntpd restart

RHEL 7 uniquement : service Chrony

En tant que root, modifiez **/etc/chrony.conf** et ajoutez une entrée de serveur pour chaque serveur de temps distant :

server **peer1-fqdn-or-ip-address** iburst

server **peer2-fqdn-or-ip-address** iburst

Dans un déploiement type, l'heure doit être synchronisée depuis les contrôleurs de domaine locaux et non pas directement depuis des serveurs de pool NTP publics. Ajoutez une entrée de serveur pour chaque contrôleur de domaine Active Directory du domaine.

Supprimez toute autre entrée server répertoriée, y compris les entrées d'adresse IP de bouclage, localhost et ***.pool.ntp.org** de serveur public.

Enregistrez les modifications et redémarrez le démon Chrony :

sudo /sbin/service chronyd restart

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Il s'agit d'un problème spécifique à RHEL 6 : les utilisateurs reçoivent un message les invitant à entrer le mot de passe racine après avoir ouvert une session.

Pour résoudre ce problème, en tant que root, créez le fichier **/etc/polkit-1/localauthority/30-site.d/20-no-show-proxy-dialog.pkla** dans un éditeur de texte et ajoutez le contenu suivant :

```
[No Show Proxy Dialog]

Identity=unix-user:*

Action=org.freedesktop.packagekit.system-network-proxy-configure

ResultAny=no

ResultInactive=no

ResultActive=no
```

> ## Conseil
>
> Pour de plus amples informations sur ce problème, consultez la page de solutions RedHat ici. La solution appropriée est décrite dans la section des commentaires.

Le VDA Linux dépend de OpenJDK. L'environnement d'exécution doit avoir été installé dans le cadre de l'installation du système d'exploitation.

RHEL 6 uniquement : OpenJDK 1,7

Vérifiez que la version est correcte avec :

```
sudo yum info java-1.7.0-openjdk
```

Le OpenJDK préconditionné peut être une version antérieure. Mettez à jour vers la dernière version :

```
sudo yum -y update java-1.7.0-openjdk
```

Définissez la variable d'environnement **JAVA_HOME** en ajoutant la ligne suivante au fichier **~/.bashrc** :

```
export JAVA_HOME=/usr/lib/jvm/java
```

Ouvrez un nouveau shell et vérifiez la version de Java :

```
java –version
```

RHEL 7,0 uniquement : OpenJDK 1,8

Vérifiez que la version est correcte avec :

```
sudo yum info java-1.8.0-openjdk
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Le OpenJDK préconditionné peut être une version antérieure. Mettez à jour vers la dernière version :

```
sudo yum -y update java-1.8.0-openjdk
```

Définissez la variable d'environnement **JAVA_HOME** en ajoutant la ligne suivante au fichier **~/.bashrc** :

```
export JAVA_HOME=/usr/lib/jvm/java
```

Ouvrez un nouveau shell et vérifiez la version de Java :

```
java –version
```

> ## Conseil
>
> Pour éviter les problèmes, assurez-vous que vous avez uniquement installé OpenJDK version 1.7.0 ou 1.8.0. Supprimez toutes les autres versions de Java de votre système.

Le VDA Linux requiert PostgreSQL 8.4 ou version ultérieure sur RHEL 6 ou PostgreSQL version 9.2 ou version ultérieure sur RHEL 7.

Installez les packages suivants :

```
sudo yum -y install postgresql-server
```

```
sudo yum -y install postgresql-jdbc
```

L'étape de post-installation suivante est requise pour initialiser la base de données et s'assurer que le service est lancé au démarrage. Cette opération crée les fichiers de base de données sous **/var/lib/pgsql/data**. Cette commande diffère entre PostgreSQL 8 et 9.

RHEL 6 uniquement : PostgreSQL 8

```
sudo /sbin/service postgresql initdb
```

RHEL 7 uniquement : PostgreSQL 9

```
sudo postgresql-setup initdb
```

Démarrer PostgreSQL

Pour les deux versions de PostgreSQL, configurez le service pour qu'il soit lancé au démarrage et pour qu'il soit lancé maintenant :

```
sudo /sbin/chkconfig postgresql on
```

```
sudo /sbin/service postgresql start
```

Vérifiez la version de PostgreSQL avec :

```
psql --version
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Vérifiez que le répertoire de données est défini à l'aide de l'utilitaire de ligne de commande **psql** :

```
sudo -u postgres psql -c 'show data_directory'
```

Le VDA Linux requiert le package motif ou openmotif, selon la distribution.

RHEL 6 uniquement : Open Motif

```
sudo yum -y install openmotif
```

RHEL 7 uniquement : Motif

```
sudo yum -y install motif
```

Le VDA Linux requiert les filtres cups et foomatic.

RHEL 6 uniquement : prise en charge de l'impression

```
sudo yum –y install cups
```

```
sudo yum -y install foomatic
```

RHEL 7 uniquement : prise en charge de l'impression

```
sudo yum –y install cups
```

```
sudo yum -y install foomatic-filters
```

Installez les autres packages requis :

```
sudo yum -y install redhat-lsb-core
```

```
sudo yum -y install ImageMagick
```

Certaines modifications sont requises pour l'exécution du VDA Linux en tant que machine virtuelle sur un hyperviseur pris en charge. Apportez les modifications suivantes en fonction de la plateforme d'hyperviseur utilisée. Aucune modification n'est requise si vous utilisez la machine Linux sur un matériel bare metal.

Corriger la synchronisation de l'heure sur Citrix XenServer

Si la fonctionnalité de synchronisation de l'heure de XenServer est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée car XenServer et NTP tenteront de gérer l'horloge du système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, l'horloge du système de chaque invité Linux doit être synchronisée avec NTP. Pour cela, la synchronisation de l'heure de l'hôte doit être désactivée. Aucune modification n'est requise en mode HVM.

Sur certaines distributions Linux, si vous utilisez un noyau Linux paravirtualisé avec XenServer Tools installé, vous pouvez

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

vérifier si la fonctionnalité de synchronisation de l'heure de XenServer est présente et activée à partir de la VM Linux :

```
su -

cat /proc/sys/xen/independent_wallclock
```

Cette commande renvoie une de ces valeurs :

- 0 - La fonctionnalité de synchronisation de l'heure est activée, et doit être désactivée.
- 1 - La fonctionnalité de synchronisation de l'heure est désactivée, et aucune action n'est requise.

Si le fichier /proc/sys/xen/indepent_wallclock n'est pas présent, les étapes suivantes ne sont pas requises.

Si cette option est activée, désactivez la fonctionnalité de synchronisation de l'heure en indiquant 1 dans le fichier :

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

Pour rendre cette modification permanente et persistante après le redémarrage, modifiez le fichier /etc/sysctl.conf en ajoutant la ligne suivante :

```
xen.independent_wallclock = 1
```

Pour vérifier ces modifications, redémarrez le système :

```
reboot
```

Après le redémarrage, vérifiez que cette configuration est correcte :

```
su -

cat /proc/sys/xen/independent_wallclock
```

Cette commande doit renvoyer la valeur 1.

Corriger la synchronisation de l'heure sur Microsoft Hyper-V

Les VM Linux sur lesquelles Hyper-V Integration Services est installé peuvent tirer parti de la fonctionnalité de synchronisation de l'heure Hyper-V pour utiliser l'heure du système d'exploitation hôte. Pour vous assurer que l'horloge du système est toujours précise, cette fonctionnalité doit être activée avec les services NTP.

Depuis le système d'exploitation de gestion :

1. Ouvrez la console du gestionnaire Hyper-V.
2. Pour les paramètres d'une VM Linux, sélectionnez **Integration Services**.
3. Assurez-vous que **Synchronisation date/heure** est sélectionné.

> ### Remarque
>
> Cette approche diffère de XenServer et VMware, pour lesquels la synchronisation de l'heure est désactivée pour éviter tout conflit avec NTP. La synchronisation de l'heure Hyper-V peut co-exister avec la synchronisation de l'heure NTP.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Corriger la synchronisation de l'heure sur ESX et ESXi

Si la fonctionnalité de synchronisation de l'heure de VMware est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée car l'hyperviseur et NTP tenteront de gérer l'horloge du système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, l'horloge du système de chaque invité Linux doit être synchronisée avec NTP. Pour cela, la synchronisation de l'heure de l'hôte doit être désactivée.

Si vous exécutez un noyau Linux paravirtualisé sur lequel VMware Tools est installé :

1. Ouvrez vSphere Client.
2. Modifiez les paramètres pour la VM Linux.
3. Dans la boîte de dialogue **Virtual Machine Properties** , ouvrez l'onglet **Options**.
4. Sélectionnez **VMware Tools**.
5. Dans la zone **Advanced**, désélectionnez **Synchronize guest time with host** (Synchroniser l'heure de l'invité avec l'hôte).

Il existe un certain nombre de méthodes pour ajouter des machines Linux au domaine Active Directory qui sont prises en charge par XenDesktop pour Linux :

- Samba Winbind
- Service d'authentification Quest
- Centrify DirectControl

Suivez les instructions ci-dessous pour la méthode choisie.

Samba Winbind

Installer ou mettre à jour les packages

Installez ou mettez à jour les packages requis :

```
sudo yum -y install samba-winbind \
    samba-winbind-clients \
    krb5-workstation \
    authconfig \
    oddjob-mkhomedir
```

Activer le lancement du démon Winbind au démarrage

Le démon Winbind doit être configuré pour être lancé au démarrage :

```
sudo /sbin/chkconfig winbind on
```

Configurer l'authentification Winbind

Configurez la machine pour l'authentification Kerberos à l'aide de Winbind :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
sudo authconfig \
    --disablecache \
    --disablesssd \
    --disablesssdauth \
    --enablewinbind \
    --enablewinbindauth \
    --disablewinbindoffline \
    --smbsecurity=ads \
    --smbworkgroup=domain \
    --smbrealm=REALM \
    --krb5realm=REALM \
    --krb5kdc=fqdn-of-domain-controller \
    --winbindtemplateshell=/bin/bash \
    --enablemkhomedir --updateall
```

Où **REALM** est le nom du domaine Kerberos en majuscules et **domain** est le nom NetBIOS court du domaine Active Directory.

Si des recherches DNS sur le nom de domaine et de serveur KDC sont requises, ajoutez les options suivantes à la commande ci-dessus :

```
--enablekrb5kdcdns --enablekrb5realmdns
```

Ignorez les erreurs renvoyées par la commande **authconfig** sur l'échec du démarrage du service winbind. C'est parce que authconfig essaie de démarrer le service winbind sans que la machine ait rejoint le domaine.

Ouvrez **/etc/samba/smb.conf** et ajoutez les entrées suivantes dans la section **[Global]**, mais après la section générée par l'outil authconfig.

```
kerberos method = secrets and keytab
winbind refresh tickets = true
```

Le fichier keytab système **/etc/krb5.keytab** est requis par le VDA Linux pour s'authentifier et s'enregistrer auprès du Delivery Controller. Le paramètre **kerberos method** ci-dessus force Winbind à créer le fichier keytab système lorsque la machine rejoint le domaine.

Rejoindre un domaine Windows

Votre contrôleur de domaine doit être accessible et vous devez disposer d'un compte utilisateur Active Directory avec les autorisations nécessaires pour ajouter des ordinateurs au domaine.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
sudo net ads join REALM -U user
```

Où REALM est le nom de domaine Kerberos en majuscules, et user est un utilisateur de domaine disposant des autorisations nécessaires pour ajouter les ordinateurs au domaine.

Configurer PAM pour Winbind

Par défaut, la configuration du module Winbind PAM **(pam_winbind)** n'active pas la mise en cache de ticket Kerberos ni la création du répertoire de base. Ouvrez **/etc/security/pam_winbind.conf** et ajoutez ou modifiez les entrées suivantes dans la section **[Global]** :

```
krb5_auth = yes

krb5_ccache_type = FILE

mkhomedir = yes
```

Assurez-vous que les points-virgules de début de chaque paramètre sont supprimés. Ces modifications requièrent un redémarrage du démon Winbind :

```
sudo /sbin/service winbind restart
```

> **Conseil**
>
> Le démon winbind ne reste en cours d'exécution que si la machine est associée à un domaine.

Ouvrez **/etc/krb5.conf** et modifiez le paramètre suivant dans la section [libdefaults], remplacez le type KEYRING par le type FILE :

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

Vérifier l'appartenance à un domaine

Le contrôleur XenDesktop requiert que toutes les machines VDA, Windows ou Linux, aient un objet ordinateur dans Active Directory.

Vérifiez que la machine est associée à un domaine à l'aide de la commande **net ads** de Samba :

```
sudo net ads testjoin
```

Il est possible de vérifier les informations supplémentaires de domaine et d'objet ordinateur avec :

```
sudo net ads info
```

Vérifier la configuration de Kerberos

Pour vérifier que Kerberos est correctement configuré pour être utilisé avec le VDA Linux, vérifiez que le fichier keytab système a été créé et contient des clés valides :

```
sudo klist -ke
```

Cette commande doit afficher la liste des clés disponibles pour les différentes combinaisons de noms principaux et de suites

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de chiffrement. Exécutez la commande **kinit** Kerberos pour authentifier la machine auprès du contrôleur de domaine à l'aide de ces clés :

sudo kinit -k **MACHINE**\$@**REALM**

Les noms de machine et de domaine doivent être spécifiés en majuscules, et le signe dollar ($) doit être placé dans une séquence d'échappement avec une barre oblique inverse (\) pour empêcher le remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom de domaine Kerberos ; assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

Vérifiez que le ticket TGT pour le compte de machine a été mis en cache à l'aide de :

sudo klist

Examinez les détails du compte de machine à l'aide de :

sudo net ads status

Vérifier l'authentification utilisateur

Utilisez l'outil **wbinfo** pour vérifier que les utilisateurs de domaine peuvent s'authentifier auprès du domaine :

wbinfo --krb5auth=**domain****username**%**password**

Le domaine spécifié ici est le nom de domaine Active Directory, et non le nom de domaine Kerberos. Pour le shell bash, la barre oblique inverse (\) doit être placée dans une séquence d'échappement avec une autre barre oblique inverse. Cette commande renvoie un message indiquant la réussite ou l'échec.

Pour vérifier que le module PAM Winbind est correctement configuré, ouvrez une session localement à l'aide d'un compte d'utilisateur de domaine qui ne s'est pas connecté à la machine précédemment.

ssh localhost -l **domain****username**

id -u

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le uid renvoyé par la commande **id -u** :

ls /tmp/krb5cc_**uid**

Vérifiez que les tickets dans le cache d'identification de Kerberos de l'utilisateur sont valides et n'ont pas expiré :

klist

Quittez la session :

exit

Le même test peut être réalisé en ouvrant une session directement sur la console KDE ou Gnome.

Service d'authentification Quest

Configurer Quest sur le contrôleur de domaine

Cette procédure suppose que vous avez installé et configuré le logiciel Quest sur les contrôleurs de domaine Active

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Directory et disposez des droits Administrateur pour créer des objets ordinateur dans Active Directory.

Autoriser les utilisateurs de domaine à ouvrir une session sur des machines VDA Linux

Pour chaque utilisateur de domaine qui doit établir des sessions HDX sur une machine VDA Linux :

1. Dans la console de gestion Utilisateurs et ordinateurs Active Directory, ouvrez les propriétés de l'utilisateur Active Directory pour ce compte d'utilisateur.
2. Sélectionnez l'onglet **Unix Account**.
3. Sélectionnez la case **Unix-enabled**.
4. Définissez **Primary GID Number** sur l'ID d'un groupe d'utilisateurs de domaine.

> ## Remarque
>
> Ces instructions sont les mêmes que pour la configuration d'utilisateurs de domaine pour l'ouverture de session à l'aide de la console, RDP, SSH ou tout autre protocole de communication à distance.

Configurer Quest sur un VDA Linux

Solution à l'application forcée de la stratégie SELinux

L'environnement RHEL par défaut applique entièrement SELinux. Cela interfère avec les mécanismes IPC de socket de domaine Unix utilisés par Quest et empêche les utilisateurs de domaine d'ouvrir une session.

> ## Conseil
>
> Il existe plusieurs solutions indiquées ici.

La plus facile consiste à désactiver SELinux. En tant que root, modifiez le paramètre SELinux dans /etc/selinux/config :

```
SELINUX=disabled
```

Cette modification nécessite un redémarrage :

```
reboot
```

> ## Important
>
> Utilisez ce paramètre avec précaution. La réactivation de l'application forcée de la stratégie SELinux après sa désactivation peut entraîner un verrouillage complet, même pour l'utilisateur root et d'autres utilisateurs locaux.

Configurer le démon VAS

Le renouvellement automatique des tickets Kerberos doit être activé et déconnecté ; l'authentification (ouverture de session en mode déconnecté) doit être désactivée :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
sudo /opt/quest/bin/vastool configure vas vasd \
                auto-ticket-renew-interval 32400
sudo /opt/quest/bin/vastool configure vas vas_auth \
                allow-disconnected-auth false
```

Ces commandes définissent l'intervalle de renouvellement sur 9 heures (32400 secondes), ce qui est une heure de moins que la valeur par défaut de 10 heures pour la durée de vie de ticket. Définissez ce paramètre sur une valeur inférieure sur les systèmes avec une durée de vie de ticket plus courte.

Configuration de PAM et de NSS

Quest requiert la configuration manuelle de PAM et NSS pour permettre la connexion d'utilisateur de domaine via HDX et d'autres services tels que su, ssh et RDP. Pour configurer PAM et NSS :

```
sudo /opt/quest/bin/vastool configure pam
sudo /opt/quest/bin/vastool configure nss
```

Rejoindre un domaine Windows

Associez la machine Linux au domaine Active Directory à l'aide de la commande vastool de Quest :

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

L'utilisateur est un utilisateur de domaine disposant des autorisations nécessaires pour associer des ordinateurs au domaine Active Directory. Le nom de domaine est le nom DNS du domaine ; par exemple, exemple.com.

Vérifier l'appartenance à un domaine

Le contrôleur XenDesktop requiert que toutes les machines VDA, Windows ou Linux, aient un objet ordinateur dans Active Directory. Pour vérifier qu'une machine Linux associée à Quest se trouve sur le domaine :

```
sudo /opt/quest/bin/vastool info domain
```

Si la machine est associée à un domaine, cette commande renvoie le nom de domaine. Si elle n'est pas associée, vous voyez le message d'erreur suivant :

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
default_realm not configured in vas.conf. Computer may not be joined to domain
```

Vérifier l'authentification utilisateur

Pour vérifier que Quest peut authentifier les utilisateurs de domaine à l'aide de PAM, ouvrez une session à l'aide d'un compte d'utilisateur de domaine qui ne s'est pas connecté à la machine précédemment.

```
ssh localhost -l domain\\username
id -u
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le uid renvoyé par la commande **id -u** :

ls /tmp/krb5cc_uid

Vérifiez que les tickets dans le cache d'identification de Kerberos de l'utilisateur sont valides et n'ont pas expiré :

/opt/quest/bin/vastool klist

Quittez la session :

exit

Le même test peut être réalisé en ouvrant une session directement sur la console KDE ou Gnome.

Centrify DirectControl

Rejoindre un domaine Windows

Avec le Centrify DirectControl Agent installé, associez la machine Linux au domaine Active Directory à l'aide de la commande **adjoin** Centrify :

su –

adjoin -w -V -u **user domain-name**

Le paramètre **user** est un utilisateur de domaine Active Directory disposant des autorisations nécessaires pour associer des ordinateurs au domaine Active Directory. Le paramètre de nom de domaine est le nom du domaine auquel associer la machine Linux.

Vérifier l'appartenance à un domaine

Le contrôleur XenDesktop requiert que toutes les machines VDA, Windows ou Linux, aient un objet ordinateur dans Active Directory. Pour vérifier qu'une machine Linux associée à Centrify se trouve sur le domaine :

su –

adinfo

Vérifiez que la valeur **Joined to domain** est valide et que **CentrifyDC mode** renvoie **connected**. Si le mode reste bloqué à l'état de démarrage, le client Centrify rencontre des problèmes de connexion au serveur ou d'authentification.

Des informations plus complètes sur le système et les diagnostics sont disponibles à l'aide de :

adinfo --sysinfo all

adinfo –diag

Pour tester la connectivité avec les différents services Active Directory et Kerberos :

adinfo --test

Installer les pilotes NVIDIA GRID

Pour activer HDX 3D Pro, des étapes d'installation supplémentaires sont requises pour installer les pilotes graphiques nécessaires sur l'hyperviseur, ainsi que sur les machines VDA.

Configurez ce qui suit :

1. Citrix XenServer
2. VMware ESX

Suivez les instructions pour l'hyperviseur choisi.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix XenServer

Cette section détaillée décrit l'installation et la configuration des pilotes NVIDIA GRID sur Citrix XenServer.

VMware ESX

Suivez les informations contenues dans ce guide pour installer et configurer les pilotes NVIDIA GRID de VMware ESX.

Machines VDA

Suivez ces étapes pour installer et configurer les pilotes pour chaque invité VM Linux :

1. Avant de commencer, assurez-vous que la VM Linux est arrêtée.
2. Dans XenCenter, ajoutez un processeur graphique en mode GPU Passthrough à la VM.
3. Démarrez la VM RHEL.

Pour préparer la machine pour les pilotes NVIDIA GRID, les étapes suivantes sont requises :

```
# yum install gcc

# yum install "kernel-devel-uname-r == $(uname -r)"

# systemctl set-default multi-user.target
```

Une fois terminé, suivez les étapes décrites dans le document Red Hat Enterprise Linux pour installer les pilotes NVIDIA GRID.

> **Remarque**
>
> Pendant l'installation du pilote GPU, sélectionnez la valeur par défaut (no) pour chaque question.

> **Important**
>
> Une fois que la fonctionnalité GPU Passthrough a été activée, la VM Linux n'est plus accessible via XenCenter, vous devez donc utiliser SSH pour vous connecter.

Afin de vérifier si le pilote graphique NVIDIA GRID™ est correctement installé, exécutez « nvidia-smi » ; les résultats doivent ressembler à :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
nvidia-smi

+-----------------------------------------------------+
| NVIDIA-SMI 352.70     Driver Version: 352.70        |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|===============================+======================+======================|
|   0  Tesla M60           Off  | 0000:00:05.0     Off |                  Off |
| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU Memory |
|  GPU       PID  Type  Process name                               Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

Définissez la configuration correcte pour la carte :

etc/X11/ctx-nvidia.sh

Pour bénéficier des résolutions élevées et des capacités multi-écrans, vous aurez besoin d'une licence NVIDIA valide. Pour appliquer la licence, suivez les instructions de la documentation du produit, GRID Licensing Guide.pdf - DU-07757-001 Septembre 2015.

Configurer un catalogue et un groupe de mise à disposition de machines Linux

Le processus de création de catalogues de machines et d'ajout de machines VDA Linux est très similaire à l'approche traditionnelle avec les VDA Windows. Reportez-vous à la documentation du produit Citrix en ligne pour obtenir une description complète de la méthode à utiliser pour effectuer ces tâches.

Pour la création de catalogues de machines contenant des machines VDA Linux, il existe quelques restrictions qui différencient ce processus de la création de catalogues de machines pour VDA Windows :

- Pour le système d'exploitation, sélectionnez :
  - Système d'exploitation de serveur Windows ou OS de serveur pour un modèle de mise à disposition de bureaux partagés hébergés.
  - Système d'exploitation de bureau Windows ou OS de bureau pour un modèle de mise à disposition de bureaux dédiés VDI.
- Assurez-vous que les machines sont définies avec alimentation non gérée.
- PVS et MCS n'étant pas pris en charge pour les VDA Linux, choisissez la méthode de déploiement **Autre service ou technologie** (images existantes).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Ne combinez pas de machines VDA Linux et Windows dans le même catalogue de machines.

> ## Remarque
>
> Les versions antérieures de Citrix Studio ne prenaient pas en charge la notion de système d'exploitation Linux ; toutefois, la sélection de l'option Système d'exploitation de serveur Windows ou OS de serveur implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l'option Système d'exploitation de bureau Windows ou OS de bureau implique un modèle de mise à disposition d'un utilisateur XenDesktop unique par machine.

La documentation Citrix pour la création de catalogues de machines est référencée ci-dessous :

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7,9

Les versions antérieures de XenDesktop ne sont pas prises en charge.

> ## Conseil
>
> Si une machine quitte et rejoint le domaine Active Directory, la machine devra être supprimée et ajoutée de nouveau au catalogue de machines.

Le processus de création d'un groupe de mise à disposition et d'ajout de catalogues de machines contenant des machines VDA Linux est presque identique aux machines VDA Windows. Reportez-vous à la documentation du produit Citrix en ligne pour obtenir une description complète de la méthode à utiliser pour effectuer ces tâches.

Lors de la création de groupes de mise à disposition qui contiennent des catalogues de machines VDA Linux, les restrictions suivantes s'appliquent :

- Pour le type de mise à disposition, sélectionnez Bureaux. Les machines VDA Linux ne prennent pas en charge la mise à disposition d'applications.
- Assurez-vous que les utilisateurs et les groupes AD que vous sélectionnez ont été correctement configurés pour l'ouverture de session sur les machines VDA Linux.
- N'autorisez pas l'ouverture de session d'utilisateurs non authentifiés (anonymes).
- Ne combinez pas le groupe de mise à disposition avec des catalogues de machines contenant des machines Windows.

La documentation Citrix pour la création de groupes de mise à disposition est référencée ci-dessous :

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7,9

Les versions antérieures de XenDesktop ne sont pas prises en charge.

Installer le logiciel VDA Linux

Si vous avez déjà installé une version de VDA Linux antérieure à la version 1.0, désinstallez-la avant d'installer la nouvelle version.

Arrêtez les services VDA Linux :

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
```

Désinstallez le package :

```
sudo rpm -e XenDesktopVDA
```

> **Important**
>
> La mise à niveau à partir de la Tech Preview vers les versions 1.0, 1.1, 1.2 ou 1.3 n'est pas prise en charge.
>
> Pour RHEL 6.0, Citrix recommande de conserver Xorg-x11-server-Xorg version 1.155 ; ne mettez pas à niveau ce package.

> **Remarque**
>
> À compter de la version 1.3, le chemin d'accès d'installation est différent. Dans les versions précédentes, les composants d'installation se trouvaient dans **/usr/local/** ; le nouvel emplacement est **/opt/Citrix/VDA/**.
>
> Pour exécuter une commande, le chemin d'accès complet est nécessaire ; vous pouvez ajouter **/opt/Citrix/VDA/sbin** et **/opt/Citrix/VDA/bin** au chemin du système.

Installer le VDA Linux

Installez le logiciel VDA Linux à l'aide du gestionnaire de package RPM :

Pour RHEL 6 :

```
sudo rpm -i XenDesktopVDA-1.3.0.312-1.el6.x86_64.rpm
```

Pour RHEL 7,2 :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

sudo rpm -i XenDesktopVDA-1.3.0.312-1.el7.x86_64.rpm

Si vous avez déjà installé la version 1.1 ou 1.2 du VDA Linux, mettez à niveau le logiciel VDA Linux à l'aide du gestionnaire de package RPM :

Pour RHEL 6 :

sudo rpm -U XenDesktopVDA-1.3.0.312-1.el6.x86_64.rpm

Pour RHEL 7,2 :

sudo rpm -U XenDesktopVDA-1.3.0.312-1.el7.x86_64.rpm

> ## Important
>
> Vous devez redémarrer la machine Linux VDA après la mise à niveau.

Après l'installation du package, vous devez configurer le VDA Linux en exécutant le script ctxsetup.sh. Si vous avez mis à niveau le package, vous devez exécuter le script ctxsetup.sh pour finaliser la mise à niveau. Avant d'apporter des modifications, ce script va vérifier l'environnement et s'assurer que toutes les dépendances sont installées. Si nécessaire, ce script peut être réexécuté à tout moment pour modifier les paramètres.

Le script peut être exécuté manuellement avec invites ou automatiquement avec réponses pré-configurées. Consultez l'aide sur ce script avant de continuer :

sudo /opt/Citrix/VDA/sbin/ctxsetup.sh –help

Configuration avec invites

Exécutez une configuration manuelle avec questions :

sudo /opt/Citrix/VDA/sbin/ctxsetup.sh

Configuration automatique

Pour une installation automatique, les options requises par le script d'installation peuvent être fournies avec des variables d'environnement. Si toutes les variables requises sont présentes, le script n'invite pas l'utilisateur à entrer les informations, ce qui permet d'exécuter le processus d'installation à l'aide d'un script.

Les variables d'environnement prises en charge sont les suivantes :

- CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N - Le Virtual Delivery Agent prend en charge la spécification d'un nom de Delivery Controller à l'aide d'un enregistrement DNS CNAME. Il est généralement configuré sur N.
- CTX_XDL_DDC_LIST = list-ddc-fqdns – Le Virtual Delivery Agent requiert une liste séparée par des espaces de noms de domaines complets de Delivery Controller
- à utiliser pour s'enregistrer auprès d'un Delivery. Au moins un alias de nom de domaine complet (FQDN) ou CNAME doit

© 1999-2017 Citrix Systems, Inc. All rights reserved.

être spécifié.

- CTX_XDL_VDA_PORT = port-number – Le Virtual Delivery Agent communique avec les Delivery Controller à l'aide d'un port TCP/IP. Il s'agit généralement du port 80.
- CTX_XDL_REGISTER_SERVICE = Y | N - Les services Linux Virtual Desktop prennent en charge le lancement lors du démarrage. Généralement configuré sur Y.
- CTX_XDL_ADD_FIREWALL_RULES = Y | N – Les services Linux Virtual Desktop requièrent que les connexions réseau entrantes soient autorisées via le pare-feu du système. Vous pouvez ouvrir automatiquement les ports requis (par défaut, les ports 80 et 1494) dans le pare-feu du système pour Linux Virtual Desktop. Généralement configuré sur Y.
- CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 – Le Virtual Delivery Agent requiert que les paramètres de configuration Kerberos s'authentifient auprès des Delivery Controller. La configuration de Kerberos est déterminée depuis l'outil d'intégration d'Active Directory installé et configuré sur le système. Spécifiez la méthode d'intégration d'Active Directory prise en charge à utiliser :
  - 1 - Samba Winbind
  - 2 - Service d'authentification Quest
  - 3 - Centrify DirectControl
- CTX_XDL_HDX_3D_PRO= Y | N – Linux Virtual Desktop prend en charge HDX 3D Pro, un ensemble de technologies d'accélération des graphiques conçues pour optimiser la virtualisation des applications riches en graphiques. HDX 3D Pro nécessite l'installation d'une carte graphique NVIDIA Grid compatible. Si HDX 3D Pro est sélectionné, le Virtual Delivery Agent doit être configuré pour le mode Bureaux VDI (session unique) – (c'est-à-dire, CTX_XDL_VDI_MODE=Y). Ceci n'est pas pris en charge avec SUSE. Assurez-vous que cette valeur est définie sur N.
- CTX_XDL_VDI_MODE= Y | N - Indiquer si la machine est configurée comme modèle de mise à disposition de bureaux dédiés (VDI) ou comme modèle de mise à disposition de bureaux partagés hébergés. Pour les environnements HDX 3D Pro, doit être défini sur Y. Il est généralement configuré sur N.
- CTX_XDL_SITE_NAME= dns-name – Le Virtual Delivery Agent découvre les serveurs LDAP à l'aide de DNS en interrogeant les enregistrements du service LDAP. Pour limiter les résultats de recherche DNS à un site local, un nom de site DNS peut être spécifié. Ce paramètre est généralement vide [none].
- CTX_XDL_LDAP_LIST= list-ldap-servers – Le Virtual Delivery Agent interroge par défaut le DNS pour découvrir les serveurs LDAP, mais si le DNS ne peut pas fournir les enregistrements du service LDAP, vous pouvez fournir une liste séparée par des espaces des noms de domaine complets (FQDN) LDAP avec le port LDAP (ex. ad1.masociété.com:389). Ce paramètre est généralement vide [none].
- CTX_XDL_SEARCH_BASE= search-base – Le Virtual Delivery Agent interroge par défaut LDAP à l'aide d'une base de recherche définie sur la racine du domaine Active Directory (ex. DC=masociété,DC=com), toutefois une base de recherche peut être spécifiée pour améliorer les performances (ex. OU=VDI,DC=masociété,DC=com). Ce paramètre est généralement vide [none].
- CTX_XDL_START_SERVICE = Y | N - Indiquer si les services VDA Linux sont lancés lorsque la configuration du VDA Linux est terminée. Généralement configuré sur Y.

Définissez la variable d'environnement et exécutez le script de configuration :

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
export CTX_XDL_AD_INTEGRATION=1|2|3

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Vous devez fournir l'option -E avec sudo pour transmettre les variables d'environnement au nouveau shell créé. Citrix vous recommande de créer un fichier de script shell à partir des commandes ci-dessus avec #!/bin/bash sur la première ligne.

Vous pouvez aussi spécifier tous les paramètres avec une seule commande :

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST=list-ddc-fqdns \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST=list-ldap-servers \

CTX_XDL_SEARCH_BASE=search-base \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
```

Supprimer les modifications de configuration

Dans certains scénarios, il peut être nécessaire de supprimer les modifications de configuration effectuées par le script **ctxsetup.sh** sans désinstaller le package VDA Linux.

Consultez l'aide sur ce script avant de continuer :

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour supprimer les modifications de configuration :

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

> **Important**
>
> Ce script supprimera toutes les données de configuration de la base de données et empêchera VDA Linux de fonctionner.

Journaux de configuration

Les scripts **ctxsetup.sh** et **ctxcleanup.sh** affichent les erreurs dans la console, avec des informations supplémentaires consignées dans un fichier journal de configuration :

```
/tmp/xdl.configure.log
```

Redémarrez les services de VDA Linux pour que les modifications prennent effet.

Exécuter le logiciel VDA

Une fois que vous avez configuré le VDA Linux à l'aide du script ctxsetup.sh, utilisez les commandes suivantes pour contrôler le VDA Linux.

Pour démarrer les services VDA Linux :

```
sudo /sbin/service ctxhdx start
sudo /sbin/service ctxvda start
```

Pour arrêter les services VDA Linux :

```
sudo /sbin/service ctxvda stop
sudo /sbin/service ctxhdx stop
```

Pour redémarrer les services VDA Linux :

```
sudo /sbin/service ctxvda stop
sudo /sbin/service ctxhdx restart
sudo /sbin/service ctxvda start
```

Pour vérifier l'état de fonctionnement des services du VDA Linux :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status

Désinstaller le logiciel VDA Linux

Pour vérifier que le VDA Linux est installé et pour afficher la version du package installé :

rpm -q XenDesktopVDA

Pour afficher des informations plus détaillées :

rpm –qi XenDesktopVDA

> ## Remarque
>
> La désinstallation du logiciel VDA Linux supprimera le PostgreSQL associé et d'autres données de configuration. Toutefois, le package PostgreSQL et les autres packages dépendants qui ont été installés avant l'installation du VDA Linux ne seront pas supprimés.

Cet article ne traite pas de la suppression des packages dépendants, y compris PostgreSQL.

Résolution des problèmes

Vérifier que le codage H.264 est utilisé

Linux VDA v1.3 ajoute H264 et une valeur HardwareEncoding dans le chemin d'accès de registre HKLM\Software\Citrix\Ica\Session\\Graphics pour faciliter la résolution des problèmes graphiques rencontrés avec le VDA.

Exécutez la commande suivante pour publier le codage H.264 dans un Linux VDA avant le lancement d'une session :

/opt/Citrix/VDA/bin/ctxreg create -k

"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v

"AdvertiseH264" -d "0x00000001" --force

Lancez la session et vérifiez si la clé H264 est créée dans le chemin d'accès de registre. Si tel est le cas, le codage H.264 est utilisé.

/opt/Citrix/VDA/bin/ctxreg list -k

"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"

Vérifier que le codage matériel pour 3D Pro est en cours d'utilisation

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Le codage matériel 3D Pro est désactivé par défaut, utilisez la commande ci-dessous pour activer la fonction :

```
/opt/Citrix/VDA/bin/ctxreg create -k

"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v

"HardwareEncoding" -d "0x00000001" --force
```

Lancez la session et vérifiez la valeur de « HardwareEncoding » dans le chemin d'accès du Registre ; 0 signifie que le codage matériel n'est pas utilisé, 1 signifie qu'il est utilisé.

```
/opt/Citrix/VDA/bin/ctxreg list -k

"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"
```

Utilisez la commande ci-dessous pour interroger votre ID de session :

```
/opt/Citrix/VDA/bin/ctxqsession
```

Personnaliser l'environnement de bureau pour chaque utilisateur

Actuellement, Linux VDA ne permet pas aux utilisateurs de choisir l'environnement de bureau lors de l'ouverture de session ; pour contourner ce problème, l'utilisateur peut configurer un fichier (par exemple, .xsession) pour la distribution Linux afin de définir l'environnement de bureau par défaut pour chaque utilisateur. Reportez-vous aux documents accompagnant la distribution Linux pour plus d'informations.

Pour définir KDE comme environnement par défaut :

```
#! /usr/bin/env bash

exec startkde
```

Pour définir GNOME comme environnement de bureau par défaut :

```
#! /usr/bin/env bash

exec gnome-session
```

Vérifier que la machine Linux a été correctement préparée

La plupart des problèmes proviennent d'une configuration incorrecte de la machine Linux, principalement des paramètres réseau, de la configuration du serveur de temps NTP ou de l'appartenance à un domaine Active Directory. Corriger la configuration de la machine Linux résout souvent les problèmes rencontrés avec le logiciel VDA.

Configurer la journalisation et le traçage

L'agent broker et le service HDX consignent les entrées de journal dans syslog. L'équipe d'assistance de Citrix dispose d'un ensemble d'outils permettant un traçage supplémentaire lors d'un appel.

Journalisation du service HDX

Le service HDX est configuré pour consigner les entrées de journal dans syslog et aucune configuration supplémentaire n'est requise.

Journalisation de l'agent broker

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

L'agent broker (également appelé service ctxvda) écrit les données de journal dans syslog via des sockets réseau. Ce comportement n'est peut-être pas configuré initialement. Pour définir la journalisation de l'agent broker dans syslog, la configuration suivante est requise.

Ajoutez les lignes suivantes dans le fichier /etc/rsyslog.conf :

```
$ModLoad imudp

$UDPServerRun 514
```

Enregistrez et fermez le fichier rsyslog.conf. Redémarrez le service rsyslog pour que les modifications prennent effet :

```
sudo /sbin/service rsyslog restart
```

Solutions possibles si les sessions HDX ne démarrent pas

Vérifiez qu'aucun processus orphelin n'empêche les nouvelles sessions de démarrer :

```
sudo pkill -9 ctxhdx

sudo pkill -9 ctxgfx

sudo pkill -9 ctxlogin

sudo pkill -9 ctxvfb
```

Redémarrez les services VDA Linux et réessayez.

Vérifier les autorisations et les propriétaires des fichiers et répertoires principaux

Vérifiez le propriétaire et les autorisations des fichiers et répertoires suivants :

- /var - Owner: root, Group: root, Permissions: 0755
- /var/xdl - Owner: ctxsrvr, Group: ctxadm, Permissions: 0755
- /var/xdl/.isacagent - Owner: root, Group: root, Permissions: 0666
- /var/xdl/.winsta - Owner: ctxsrvr, Group: ctxadm, Permissions: 0777
- /var/xdl/vda - Owner: root, Group: root, Permissions: 0755

Problèmes d'actualisation des multi-écrans HDX 3D Pro

Si vous rencontrez des problèmes d'actualisation des écrans autres que l'écran principal, vérifiez que la licence NVIDIA GRID est disponible.

Le son n'est pas audible

Vérifiez que le volume sur la machine exécutant Citrix Receiver et le bureau Linux n'est pas désactivé ou réglé sur un niveau bas.

Vérifiez que l'audio est activé sur le VDA Linux. Utilisez l'outil ctxreg pour interroger la valeur de l'élément de configuration fDisableCam :

```
sudo ctxreg read -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam
```

Une valeur de 0x1 signifie que l'audio est désactivé. Pour l'activer, définissez fDisableCam sur 0x0 :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
sudo ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam -d 0x00000000
```

Si l'audio n'est toujours pas audible, vérifiez que le récepteur audio Citrix est chargé par pulseaudio. Ce module PulseAudio est chargé dans le démon pulseaudio au démarrage de la session. Utilisez l'outil pacmd pour vérifier si le récepteur audio Citrix est chargé :

```
pacmd list-sinks
```

Si le récepteur audio Citrix est chargé, le résultat doit être :

```
name:

driver:
```

Si le récepteur audio Citrix n'est pas chargé, arrêtez le processus ctxaudio et redémarrez-le.

Le son n'est pas enregistré

Vérifiez que l'audio est activé sur le VDA Linux et que l'enregistrement audio est activé sur le client ICA. Si l'audio n'est toujours pas enregistré, vérifiez que la source audio Citrix est chargée par pulseaudio. Si l'enregistrement audio est activé sur le client ICA, ce module PulseAudio sera chargé dans le démon pulseaudio au démarrage de la session. Utilisez l'outil pacmd pour vérifier si la source audio Citrix est chargée :

```
pacmd list-sources
```

Si la source audio Citrix est chargée, le résultat doit être :

```
name:

driver:
```

Si la source audio Citrix n'est pas chargée, arrêtez le processus ctxaudio et redémarrez-le.

Impossible d'imprimer

Il existe un certain nombre d'éléments à vérifier si l'impression ne fonctionne pas correctement. Le démon d'impression est un processus par session et doit être en cours d'exécution pour la durée de la session. Vérifiez que le démon d'impression est en cours d'exécution.

```
ps –ef | grep ctxlpmngt
```

Si le processus ctxlpmngt n'est pas exécuté, démarrez manuellement ctxlpmngt à partir d'une ligne de commande.

Si l'impression ne fonctionne toujours pas, l'élément suivant à vérifier est l'infrastructure CUPS. Le service ctxcups est pour la gestion d'imprimante et communique avec l'infrastructure Linux CUPS. Il s'agit d'un processus unique par machine qui peut être vérifié par :

```
service ctxcups status
```

Si le service n'est pas exécuté, démarrez-le manuellement :

```
service ctxcups start
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Journal supplémentaire pour le système d'impression CUPS

En tant que composant du VDA Linux, la méthode permettant d'obtenir le journal d'un composant d'impression est similaire à d'autres composants.

Pour Red Hat, certaines étapes supplémentaires sont nécessaires pour configurer le fichier du service CUPS. Sinon, certains journaux ne peuvent pas être consignés dans hdx.log.

```
sudo service cups stop

sudo vi /etc/systemd/system/printer.target.wants/cups.service

PrivateTmp=false

sudo service cups start

sudo systemctl daemon-reload
```

Cette configuration sert uniquement à collecter le journal d'impression complet lorsqu'un problème survient. En général, cette configuration n'est pas recommandée car cette opération enfreint la sécurité CUPS.

L'impression est illisible

Une impression illisible peut être causée par un pilote d'imprimante incompatible. Une configuration pilote par utilisateur est disponible et peut être configurée en modifiant le fichier de configuration ~/.CtxlpProfile.

```
[DEFAULT_PRINTER]

printername=

model=

ppdpath=

drivertype=
```

printername est un champ contenant le nom de l'imprimante par défaut actuelle du côté client. Il s'agit d'une valeur en lecture seule qui ne doit pas être modifiée.

> **Important**
>
> Les champs **ppdpath**, **model** et **drivertype** ne doivent pas être définis en même temps car un seul est appliqué pour l'imprimante mappée.

Si le pilote d'imprimante universel n'est pas compatible avec l'imprimante cliente, le modèle du pilote d'imprimante natif peut être configuré avec l'option model=. Le nom du modèle de l'imprimante peut être obtenu avec la commande lpinfo.

```
lpinfo –m

...

xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

...

Le modèle peut être défini pour correspondre à l'imprimante :

Model=xerox/ph3115.ppd.gz

Si le pilote d'imprimante universel n'est pas compatible avec l'imprimante cliente, le chemin de fichier ppd du pilote d'imprimante natif peut être configuré. La valeur de ppdpath est le chemin d'accès absolu du fichier du pilote d'imprimante natif.

Par exemple, il existe un pilote ppd sous /home/tester/NATIVE_PRINTER_DRIVER.ppd.

ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd

Il existe trois types de pilote d'imprimante universel fournis par Citrix (postscript, pcl5 et pcl6). Ils peuvent être configurés dans le type de pilote si aucun pilote d'imprimante natif n'est disponible.

Par exemple, si le pilote d'imprimante par défaut est de type PCL5 :

drivertype=pcl5

> ## Remarque
>
> Citrix Receiver pour Mac et Citrix Receiver pour Linux prennent uniquement en charge les imprimantes PostScript ; par conséquent, les pilotes d'imprimante universels PCL6 et PCL5 ne sont pas applicables. Dans cette situation, ppdpath ou le modèle de pilote d'imprimante natif doit être défini sur une imprimante non-Postscript.

CDM ne fonctionne pas

La fonctionnalité CDM comprend un processus démon (ctxcdmd) ; si la fonction CDM échoue, redémarrez la machine VDA Linux et vérifiez si le démon a démarré correctement :

Ps -lef | grep ctxcdmd

Le nom du fichier dans le lecteur mappé doit respecter les règles de nomination d'OS VDA et Receiver.

Problèmes connus

L'état CAPS VERR de Citrix Receiver pour Android peut être annulé lors de l'itinérance de session

L'état de CAPS VERR peut être perdu lors de l'itinérance d'une connexion existante à Citrix Receiver pour Android. La solution consiste à utiliser la touche MAJ sur le clavier étendu pour basculer entre les majuscules et les minuscules.

Les raccourcis ALT ne fonctionnent pas toujours lors d'une connexion à un VDA Linux à l'aide de Citrix Receiver pour Mac

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Receiver pour Mac envoie AltGr pour les touches Options/Alt droite et gauche par défaut. Il est possible de modifier ce comportement dans les paramètres Citrix Receiver, mais les résultats varient selon les applications.

Les bibliothèques X client récentes peuvent causer des problèmes de mappage du clavier sur SuSE Linux Enterprise Desktop 11

Les versions récentes des packages xorg-x11-libX11 sur SuSE Linux Enterprise Desktop 11 peuvent rencontrer des problèmes avec les changements de mappage du clavier, qui à leur tour peuvent entraîner des problèmes avec la fonctionnalité du clavier au sein d'une session HDX. Ce problème peut se produire lorsque la version installée des packages se trouve dans la plage 7.4-5.11.11.1 à 7.4-5.11.15.1.

La solution consiste à revenir à la version SP3 stock du package xorg-x11-libX11, ce qui permet le fonctionnement normal des changements de mappage du clavier. Par exemple :

rpm -i --force xorg-x11-libX11-7.4-5.9.1

rpm – i --force xorg-x11-libX11-32bit-7.4-5.9.1

rpm -e xorg-x11-libX11-7.4-5.11.15.1

rpm -e xorg-x11-libX11-32bit-7.4-5.11.15.1

Cette opération doit être effectuée avant qu'un utilisateur ouvre une session sur la machine ; si cette opération est effectuée lorsqu'une session est active, ces paramètres ne sont pas appliqués jusqu'à la prochaine ouverture de session.

En cas de mise à niveau à partir de SP3 stock, les packages xorg-x11-libX11 ci-dessus peuvent être verrouillés pour la version installée de manière à ce qu'ils ne soient pas modifiés lors de la mise à niveau. Avant de procéder à la mise à niveau, exécutez ce qui suit :

zypper al xorg-x11-libX11

zypper al xorg-x11-libX11-32bit

Des lancements de session lents peuvent se produire lors de l'utilisation de VDA Linux avec un Delivery Controller à partir de XenDesktop v7.1

Le lancement lent est causé par la présence de paramètres CGP dans le fichier ICA généré par le Delivery Controller v7.1. Lorsque ces paramètres sont présents, Citrix Receiver tente d'établir une connexion sur le port TCP 2598. Par défaut, les paramètres de pare-feu sur certaines distributions Linux, telles que SLED 11, sont configurés pour rejeter les paquets TCP SYN, ce qui entraîne une temporisation et par conséquent un lancement de session lent. La solution consiste à configurer le pare-feu sur le VDA Linux pour qu'il rejette TCP SYN sur le port 1494. Ce problème a été résolu dans les versions récentes des Delivery Controller.

Échec de l'enregistrement lorsque le VDA Linux est associé au domaine

Dans certaines circonstances, lorsqu'un VDA Linux est associé au domaine et qu'un nouveau jeu de clés Kerberos est généré, le broker ne parvient pas à établir un contexte de sécurité avec le VDA. Ce problème est souvent causé par le fait que le broker utilise un ticket de service VDA mis en cache obsolète basé sur le jeu de clés Kerberos précédent. Le VDA peut quand même se connecter au broker, mais le broker ne sera pas en mesure d'établir un contexte de sécurité pour le VDA. Le symptôme courant est l'échec de l'enregistrement du VDA.

Ce problème se résout de lui-même lorsque le ticket de service VDA expire et qu'il est renouvelé, mais les tickets de service

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

ont en général une durée de vie assez longue. Elle peut être de plusieurs heures.

La solution consiste à effacer le cache des tickets du broker. Vous pouvez simplement redémarrer le broker ou exécuter en tant qu'administrateur la commande suivante sur le broker à partir d'une invite de commande :

```
klist -li 0x3e4 purge
```

Cette opération supprime tous les tickets de service du cache LSA détenu par le service réseau principal sous lequel le service de broker Citrix s'exécute. Les tickets de service pour d'autres VDA et, potentiellement, d'autres services sont supprimés. Mais ce n'est pas un problème : ces tickets de service seront de nouveau acquis depuis le serveur KDC le cas échéant.

Icône d'écran de verrouillage manquante lors de l'utilisation de HDX 3D Pro avec GNOME

Lorsque les pilotes NVIDIA GRID sont actifs, Gnome Desktop Manager (GDM) n'est pas actif et la fonctionnalité d'écran de verrouillage GDM n'est pas disponible.

Audio Plug-n-Play non pris en charge

Il est recommandé que tout périphérique de capture audio soit connecté à la machine cliente avant de commencer à enregistrer l'audio dans la session ICA. Si un périphérique est connecté après que l'application d'enregistrement audio a démarré, l'application peut cesser de répondre. Si ce problème se produit, redémarrez l'application. Le même problème peut se produire si un périphérique de capture est déconnecté pendant l'enregistrement.

Distorsion audio

Windows 10 Receiver peut rencontrer une distorsion audio lors de l'enregistrement audio.

Le pilote CTXPS n'est pas compatible avec certaines imprimantes PLC

Si l'impression présente des anomalies, définissez le pilote d'imprimante sur le pilote d'imprimante natif fourni par le fabricant.

Impression lente avec les documents volumineux

Lorsque vous imprimez un document volumineux sur une imprimante cliente locale, le fichier est transféré sur une connexion serveur. Si la connexion est lente, ce transfert risque de durer longtemps.

Notifications d'imprimante et de travaux d'impression d'autres sessions

Le concept de session de Linux n'est pas le même que celui du système d'exploitation Windows. Par conséquent, tous les utilisateurs reçoivent les notifications de l'ensemble du système. L'administrateur peut désactiver ces notifications en modifiant le fichier de configuration CUPS, /etc/cups/cupsd.conf.

Recherchez le nom de stratégie configuré dans le fichier.

```
DefaultPolicy default
```

Si le nom de la stratégie est default, ajoutez les lignes suivantes dans le bloc XML de la stratégie par défaut.

```
# Job/subscription privacy...

JobPrivateAccess default

JobPrivateValues default
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

SubscriptionPrivateAccess default

SubscriptionPrivateValues default

... ...

Require user @OWNER

Order deny,allow

Order deny,allow

Glossaire

Broker : composant XenDesktop responsable de la négociation des sessions HDX sur les différents VDA dans un déploiement XenDesktop. Également appelé DDC ou contrôleur XenDesktop.

Agent broker : composant sur la machine VDA Linux qui fournit le bureau à mettre à disposition. L'agent broker communique avec le broker pour permettre la négociation de sessions. Il est composé de deux composants principaux, le service VDA et le service HDX.

Citrix Director : console d'assistance Citrix permettant le suivi et le contrôle des VDA XenDesktop.

Citrix Studio : console d'administration Citrix utilisée pour configurer XenDesktop.

DDC : XenDesktop Desktop Delivery Controller. Également appelé Broker ou Delivery Controller.

FQDN (Fully Qualified Domain Name) : nom de domaine complet

HDX (High Definition Experience) : protocole d'expérience utilisateur haute définition. Anciennement appelé protocole ICA Citrix.

Service HDX : service Linux (ctxhdx) qui transmet à distance le bureau Linux virtuel via le protocole HDX. Il communique avec le service VDA pour permettre la négociation de sessions.

RHEL : Red Hat Enterprise Linux. Distribution Linux commerciale fournie par Red Hat.

SLED : SUSE Linux Enterprise Desktop. Distribution Linux commerciale fournie par Novell.

SLES : SUSE Linux Enterprise Server. Distribution Linux commerciale fournie par Novell.

VDA : Virtual Delivery Agent.

Service VDA : service Linux (ctxvda) qui communique avec le broker pour permettre la négociation de sessions. Il communique également avec le service HDX pour la mise à disposition de session distante.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Installer des VDA SUSE Linux

Jul 07, 2016

Vous pouvez créer des bureaux virtuels Linux basés sur la distribution SUSE. Préparez les machines virtuelles Linux, installez-y le nouveau logiciel Linux Virtual Delivery Agent, configurez le Delivery Controller, puis utilisez Studio pour mettre les bureaux à la disposition des utilisateurs.

Pour plus de détails, veuillez consulter les informations contenues dans cet article.

> **Remarque**
>
> Nous avons vérifié que les commandes Shell Linux décrites dans cet article fonctionnaient avec le Shell GNU Bash.

Cet article comprend les sections suivantes :

- Configuration système requise
- Configurer des Delivery Controller
- Préparer les machines Linux pour l'installation de VDA
- Configurer un catalogue et un groupe de mise à disposition de machines Linux
- Installer le logiciel VDA Linux
- Exécuter le logiciel VDA
- Désinstaller le logiciel VDA Linux
- Résolution des problèmes
- Problèmes connus
- Glossaire

Configuration système requise

Les distributions Linux suivantes sont prises en charge par le produit Linux Virtual Desktop :

- SUSE Linux Enterprise :
  - Desktop 11 Service Pack 4
  - Desktop 12 Service Pack 1
  - Server 11 Service Pack 4
  - Server 12 Service Pack 1
- Red Hat Enterprise Linux
  - Workstation 6.7
  - Workstation 7.2
  - Server 6.7
  - Server 7.2
- CentOS Linux
  - CentOS 6.7
  - CentOS 7.2

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **Remarque**
>
> Dans tous les cas, l'architecture de processeur prise en charge est x86-64.

Les versions suivantes de XenDesktop sont prises en charge par le VDA Linux :

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7,9

Le processus de configuration pour les VDA Linux diffère légèrement des VDA Windows. Toutefois, toute batterie de Delivery Controller est capable de négocier les connexions aux bureaux Windows et Linux.

> **Remarque**
>
> Le VDA Linux n'est pas compatible avec la version XenDesktop 7.0 ou une version antérieure.

Les versions suivantes de Citrix Receiver sont prises en charge :

- Citrix Receiver pour Windows version 4.4 ou version ultérieure (correspond à la version v14.4 de wfica32.exe)
- Citrix Receiver pour Linux version 13.3 ou version ultérieure
- Citrix Receiver pour Mac OS X version 12.1 ou version ultérieure
- Citrix Receiver pour Android version 3.8 ou version ultérieure
- Citrix Receiver pour iOS version 6.1.4 ou version ultérieure
- Citrix Receiver pour Chrome/HTML5 version 2.0 (uniquement via Access Gateway)

Les hyperviseurs suivants sont pris en charge pour l'hébergement des VM invité de VDA Linux :

- XenServer
- VMware ESX et ESXi
- Microsoft Hyper-V

L'hébergement de bare metal est également pris en charge.

> **Conseil**
>
> Reportez-vous à la documentation du fabricant de l'hyperviseur pour obtenir la liste des plates-formes prises en charge.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Les produits ou packages d'intégration d'Active Directory suivants sont pris en charge par le VDA Linux :

- Samba Winbind
- Services d'authentification Quest v4.1 ou version ultérieure
- Centrify DirectControl

> **Conseil**
>
> Reportez-vous à la documentation du fabricant du package d'intégration d'Active Directory pour obtenir la liste des plates-formes prises en charge.

Configurer des Delivery Controller

XenDesktop 7.7 ou version ultérieure contient les modifications nécessaires à la prise en charge de Linux Virtual Desktop ; cependant, pour les versions précédentes, un correctif ou un script de mise à jour est requis. Leur installation et leur vérification sont décrites dans cette section.

Pour XenDesktop 7.6 SP2, appliquez le correctif Update 2 pour mettre à jour le broker pour Linux Virtual Desktop. Les correctifs Update 2 sont disponibles ici :

- CTX142438 : Correctif Update 2 - Pour Delivery Controller 7.6 (32 bits) – Anglais
- CTX142439 : Correctif Update 2 - Pour Delivery Controller 7.6 (64 bits) – Anglais

Pour les versions antérieures de XenDesktop, un script PowerShell nommé **Update-BrokerServiceConfig.ps1** est fourni ; il met à jour la configuration du service de broker. Il est disponible dans le package suivant :

- citrix-linuxvda-scripts-1.3.0.zip

Répétez les étapes suivantes sur *chaque* Delivery Controller de la batterie :

1. Copiez le script **Update-BrokerServiceConfig.ps1** sur la machine Delivery Controller.
2. Ouvrez une console Windows PowerShell dans le contexte de l'administrateur local.
3. Accédez au dossier contenant le script.
4. Exécutez le script :

```
.\Update-BrokerServiceConfig.ps1
```

> **Remarque**
>
> Par défaut, PowerShell est configuré pour empêcher l'exécution des scripts PowerShell. Si le script ne réussit pas à s'exécuter, il se peut que vous deviez modifier la stratégie d'exécution PowerShell avant d'essayer à nouveau :
>
> ```
> Set-ExecutionPolicy Unrestricted
> ```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Le script **Update-BrokerServiceConfig.ps1** met à jour le fichier de configuration du service Broker avec de nouveaux points de terminaison WCF requis par le VDA Linux et redémarre le service de broker. Le script détermine automatiquement l'emplacement du fichier de configuration du service de broker. Une copie de sauvegarde du fichier de configuration d'origine est créée dans le même répertoire avec l'extension **.prelinux**.

Ces modifications n'ont pas d'impact sur la négociation des VDA Windows configurés pour utiliser la même batterie de Delivery Controller. Cela permet d'utiliser une seule batterie pour gérer et négocier les sessions pour les VDA Windows et Linux en toute facilité.

Pour vous assurer que les modifications de configuration requises ont été appliquées à un Delivery Controller, vérifiez si la chaîne **EndpointLinux** apparaît bien cinq fois dans le fichier :

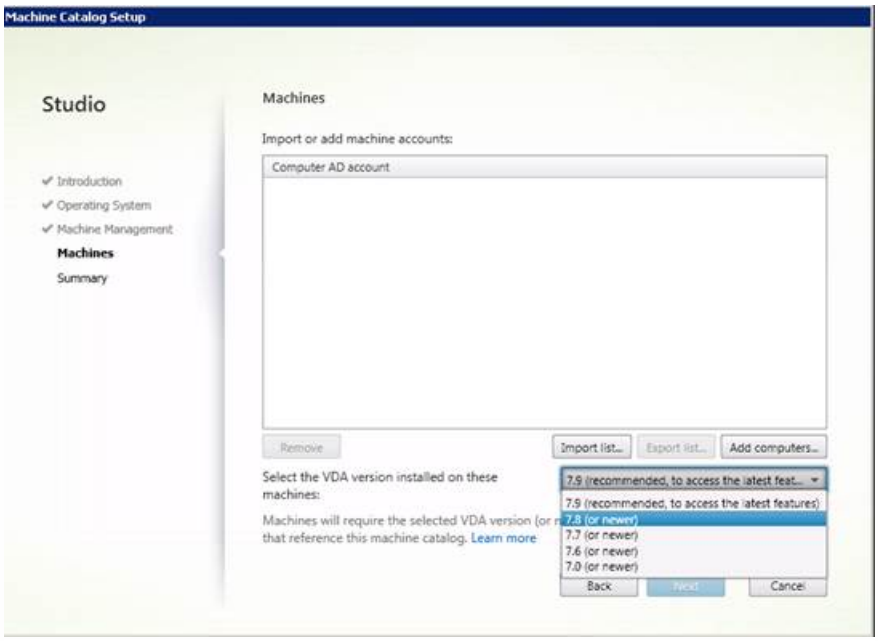
%PROGRAMFILES%\Citrix\Broker\Service\BrokerService.exe.config

À partir de l'invite de commande de Windows, connecté en tant qu'administrateur local :

```
cd "%PROGRAMFILES%"\Citrix\Broker\Service\

findstr EndpointLinux BrokerService.exe.config
```

Important

À partir de la version 1.3, l'agent broker du VDA Linux est défini sur XenApp/XenDesktop 7.8. Toutefois, lors de l'ajout d'un catalogue de machines à l'aide de l'écran **Création d'un catalogue de machines** de Studio, la valeur par défaut est automatiquement définie sur la version 7.9. Vous devez définir explicitement la version du VDA installée sur **7.8 (ou ultérieure)**. Référez-vous à l'image ci-dessous.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Préparer la machine Linux pour l'installation de VDA

L'outil SUSE Linux Enterprise YaST est utilisé pour configurer tous les aspects du système d'exploitation.

Pour démarrer l'outil YaST basé sur texte :

```
su -

yast
```

Vous pouvez également démarrer l'outil YaST basé sur interface utilisateur :

```
su -

yast2 &
```

Les sections suivantes fournissent des informations sur la configuration des paramètres et services réseau utilisés par le VDA Linux. La configuration du réseau doit être effectuée par le biais de l'outil YaST, et non via d'autres méthodes, telles que le Gestionnaire de réseau. Ces instructions sont basées sur l'utilisation de l'outil YaST avec interface utilisateur ; l'outil YaST basé sur texte peut être utilisé mais propose une autre méthode de navigation qui n'est pas abordée ici.

Configurer les paramètres hostname et DNS

1. Ouvrez YaST Network Settings (Paramètres réseau).
2. SLED 12 uniquement : Sur l'onglet **Global Options** (Options globales), définissez **Network Setup Method** (Méthode de configuration réseau) sur **Wicked Service** (Service Wicked).
3. Ouvrez l'onglet **Hostname/DNS**.
4. Désélectionnez **Change hostname via DHCP** (Changer le nom d'hôte via DHCP).
5. Sélectionnez **Assign Hostname to Loopback IP** (Attribuer le nom d'hôte à l'adresse IP de bouclage).
6. Modifiez les options suivantes pour refléter votre configuration réseau :

- Hostname (Nom d'hôte) : ajoutez le nom d'hôte DNS de la machine.
- Domain Name (Nom de domaine) : ajoutez le nom de domaine DNS de la machine.
- Name Server (Nom du serveur) : entrez l'adresse IP du serveur DNS. Il s'agit généralement de l'adresse IP du contrôleur de domaine AD.
- Domain Search list (Liste de recherche de domaine) : ajoutez le nom de domaine DNS.

> ### Remarque
>
> Le VDA Linux ne prend actuellement pas en charge la troncation du nom NetBIOS ; par conséquent, le nom de l'hôte ne doit pas comporter plus de 15 caractères.

> ### Conseil
>
> Utilisez uniquement les caractères a-z, 0-9 et tiret (-). Évitez le caractère de soulignement (_), les espaces et autres symboles. Ne

© 1999-2017 Citrix Systems, Inc. All rights reserved.

démarrez pas un nom d'hôte par un chiffre et ne le terminez pas par un tiret.

Désactiver DNS multidiffusion

Sur SLED uniquement, les paramètres par défaut activent DNS multidiffusion (mDNS), ce qui peut entraîner des résultats incohérents de résolution de nom. Par défaut, mDNS n'est pas activé sur SLES, aucune action n'est donc requise.

Pour désactiver mDNS, modifiez la ligne suivante dans /etc/nsswitch.conf :

```
hosts: files mdns_minimal [NOTFOUND=return] dns
```

de la façon suivante :

```
hosts: files dns
```

Vérifier le nom de l'hôte

Vérifiez que le nom d'hôte est correctement configuré :

```
hostname
```

Doit renvoyer uniquement le nom d'hôte de la machine et non pas son nom de domaine complet (FQDN).

Vérifiez que le nom de domaine complet est correctement configuré :

```
hostname -f
```

Doit renvoyer le nom de domaine complet de la machine.

Vérifier la résolution de nom et l'accessibilité du service

Vérifiez que vous pouvez résoudre le nom de domaine complet et effectuer un sondage ping sur le contrôleur de domaine et le Delivery Controller XenDesktop :

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
```

Si vous ne pouvez pas résoudre le nom de domaine complet ou effectuer un sondage ping sur l'une de ces machines, reprenez les étapes avant de continuer.

Il est très important de maintenir la synchronisation de l'horloge entre les VDA, les contrôleurs XenDesktop et les contrôleurs de domaine. L'hébergement du VDA Linux en tant que machine virtuelle peut entraîner des problèmes de décalage d'horloge. Pour cette raison, il est recommandé de synchroniser l'heure avec un service NTP à distance. Il peut être nécessaire d'apporter des modifications aux paramètres NTP par défaut :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Ouvrez YaST NTP Configuration et sélectionnez l'onglet **General Settings** (Paramètres généraux).
2. Dans la section Start NTP Daemon (Lancer le démon NTP), sélectionnez **Now and on Boot** (Maintenant et au démarrage).
3. Le cas échéant, sélectionnez l'élément **Undisciplined Local Clock (LOCAL)** et cliquez sur **Delete** (Supprimer).
4. Ajoutez une entrée pour un serveur NTP en cliquant sur **Add** (Ajouter).
5. Sélectionnez le type de serveur, **Server Type**, et cliquez sur **Next** (Suivant).
6. Entrez le nom DNS du serveur NTP dans le champ Address (Adresse). Ce service est généralement hébergé sur le contrôleur de domaine Active Directory.
7. Ne modifiez pas le champ Options.
8. Cliquez sur **Test** pour vérifier si le service NTP est accessible.
9. Cliquez sur **OK** dans une série de fenêtres pour enregistrer les modifications.

> ### Remarque
>
> Pour les installations SLES 12, si le démon NTP ne parvient pas à démarrer, cela peut être dû à un problème SUSE connu avec les stratégies AppArmor. Suivez la résolution ici pour des informations supplémentaires.

Le logiciel VDA Linux pour Suse Linux Enterprise fonctionne avec les packages suivants :

- PostgreSQL
  - SLED/SLES 11 : version 9.1 ou ultérieure
  - SLED/SLES 12 : version 9.3 ou ultérieure
- OpenJDK 1.7.0
- OpenMotif Runtime Environment 2.3.1 ou version ultérieure
- Cups
  - SLED/SLES 11 : version 1.3.7 ou ultérieure
  - SLED/SLES 12 : version 1.6.0 ou ultérieure
- Filtres Foomatic
  - SLED/SLES 11 : version 3.0.0 ou ultérieure
  - SLED/SLES 12 : version 1.0.0 ou ultérieure
- ImageMagick
  - SLED/SLES 11 : version 6.4.3.6 ou ultérieure
  - SLED/SLES 12 : version 6.8 ou ultérieure

Ajouter des référentiels

Certains packages requis ne sont pas disponibles dans tous les référentiels Suse Linux Enterprise :

- SLED 11 : PostgreSQL est disponible pour SLES 11 mais pas SLED 11.
- SLES 11 : OpenJDK et OpenMotif sont disponibles pour SLED 11 mais pas SLES 11.
- SLED 12 : PostgreSQL est disponible pour SLES 12 mais pas SLED 12. ImageMagick est disponible via le fichier ISO SDK SLE 12 ou le référentiel en ligne.
- SLES 12 : Il n'existe aucun problème ; tous les packages sont disponibles. ImageMagick est disponible via le fichier ISO SDK SLE 12 ou le référentiel en ligne.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour résoudre ce problème, l'approche recommandée consiste à obtenir les packages manquants depuis le support de l'autre édition de SLE. Autrement dit, sur SLED, installez les packages manquants depuis le support SLES et sur SLES, installez les packages manquants depuis le support SLED. L'approche décrite ci-dessous monte les fichiers de support ISO SLED et SLES et ajoute les référentiels.

SLED 11	sudo mkdir -p /mnt/sles sudo mount -t iso9660 \ path-to-iso/SLES-11-SP3-DVD-x86_64-GM-DVD1.iso /mnt/sles sudo zypper ar -f /mnt/sles sles
SLES 11	sudo mkdir -p /mnt/sled sudo mount -t iso9660 \ path-to-iso/SLED-11-SP3-DVD-x86_64-GM-DVD1.iso /mnt/sled sudo zypper ar -f /mnt/sled sled
SLED 12	sudo mkdir -p /mnt/sles sudo mount -t iso9660 \ path-to-iso/SLES-12-DVD-x86_64-GM-DVD1.iso /mnt/sles sudo zypper ar -f /mnt/sles sles
SLED/SLES 12	sudo mkdir -p /mnt/sdk sudo mount -t iso9660 \ path-to-iso/SLE-12-SDK-DVD-x86_64-GM-DVD1.iso /mnt/sdk sudo zypper ar -f /mnt/sdk sdk

Installer le client Kerberos

Installez le client Kerberos pour l'authentification mutuelle entre le VDA Linux et les contrôleurs XenDesktop :

```
sudo zypper install krb5-client
```

La configuration du client Kerberos dépend de l'approche d'intégration d'Active Directory utilisée, ce qui est expliqué plus loin.

Installer OpenJDK

VDA Linux dépendant de OpenJDK 1.7.0.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **Conseil**
>
> Pour éviter les problèmes, assurez-vous que vous avez installé uniquement la version 1.7.0 de OpenJDK. Supprimez toutes les autres versions de Java de votre système.

SLED	Sur SLED, Java Runtime Environment doit avoir été installé avec le système d'exploitation. Confirmez avec : sudo zypper info java-1_7_0-openjdk Mettez à jour vers la version la plus récente si l'état est signalé comme obsolète : sudo zypper update java-1_7_0-openjdk Vérifiez la version Java : java -version
SLES	Sur SLES, Java Runtime Environment doit être installé : sudo zypper install java-1_7_0-openjdk Vérifiez la version Java : java -version

Installer PostgreSQL

SLED/SLES 11	Installez les packages : sudo zypper install libecpg6 sudo zypper install postgresql?init sudo zypper install postgresql91 sudo zypper install postgresql91?server sudo zypper install postgresql?jdbc Certaines étapes de post-installation sont nécessaires pour initialiser le service de base de données et vous assurer que PostgreSQL est lancé au démarrage : sudo /sbin/insserv postgresql sudo /etc/init.d/postgresql restart
	Installez les packages :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SLED/SLES 12	sudo zypper install postgresql-init sudo zypper install postgresql93-server sudo zypper install postgresql-jdbc Certaines étapes de post-installation sont nécessaires pour initialiser le service de base de données et vous assurer que PostgreSQL est lancé au démarrage : sudo systemctl enable postgresql sudo systemctl restart postgresql Les fichiers de base de données résident sous /var/lib/pgsql/data.

Installer l'environnement OpenMotif

Le VDA Linux requiert le package motif ou openmotif, selon la distribution.

SLED/SLES 11	Installez le package : sudo zypper install openmotif-libs
SLED/SLES 12	Installez le package : sudo zypper install motif

Installer la prise en charge de l'impression

Le VDA Linux requiert les filtres cups et foomatic.

SLED/SLES 11	Installez les packages : sudo zypper install cups sudo zypper install foomatic-filters
SLED/SLES 12	Installez les packages : sudo zypper install cups sudo zypper install cups-filters-foomatic-rip

Installer ImageMagick

Installez le package ImageMagick :

sudo zypper install ImageMagick

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Supprimer les référentiels

Une fois les packages dépendants installés, les référentiels de l'autre édition configurés auparavant peuvent être supprimés et le support démonté :

SLED 11	Supprimez les packages suivants : sudo zypper rr sles sudo umount /mnt/sles sudo rmdir /mnt/sles
SLES 11	Supprimez les packages suivants : sudo zypper rr sled sudo umount /mnt/sled sudo rmdir /mnt/sled
SLED 12	Supprimez les packages suivants : sudo zypper rr sles sudo umount /mnt/sles sudo rmdir /mnt/sles
SLED/SLES 12	Supprimez les packages suivants : sudo zypper rr sdk sudo umount /mnt/sdk sudo rmdir /mnt/sdk

Certaines modifications sont requises pour l'exécution du VDA Linux en tant que machine virtuelle sur un hyperviseur pris en charge. Apportez les modifications suivantes en fonction de la plateforme d'hyperviseur utilisée. Aucune modification n'est requise si vous utilisez la machine Linux sur un matériel bare metal.

Corriger la synchronisation de l'heure sur Citrix XenServer

Si la fonctionnalité de synchronisation de l'heure de XenServer est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée car XenServer et NTP tenteront de gérer l'horloge du système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, l'horloge du système de chaque invité Linux doit être synchronisée avec NTP. Pour cela, la synchronisation de l'heure de l'hôte doit être désactivée. Aucune modification n'est requise en mode HVM.

Sur certaines distributions Linux, si vous utilisez un noyau Linux paravirtualisé avec XenServer Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de XenServer est présente et activée à partir de la VM Linux :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
su -

cat /proc/sys/xen/independent_wallclock
```

Cette commande renvoie une de ces valeurs :

- 0 - La fonctionnalité de synchronisation de l'heure est activée, et doit être désactivée.
- 1 - La fonctionnalité de synchronisation de l'heure est désactivée, et aucune action n'est requise.

Si le fichier /proc/sys/xen/indepent_wallclock n'est pas présent, les étapes suivantes ne sont pas requises.

Si cette option est activée, désactivez la fonctionnalité de synchronisation de l'heure en indiquant 1 dans le fichier :

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

Pour rendre cette modification permanente et persistante après le redémarrage, modifiez le fichier /etc/sysctl.conf en ajoutant la ligne suivante :

```
xen.independent_wallclock = 1
```

Pour vérifier ces modifications, redémarrez le système :

```
reboot
```

Après le redémarrage, vérifiez que cette configuration est correcte :

```
su -

cat /proc/sys/xen/independent_wallclock
```

Cette commande doit renvoyer la valeur 1.

Corriger la synchronisation de l'heure sur Microsoft Hyper-V

Les VM Linux sur lesquelles Hyper-V Integration Services est installé peuvent tirer parti de la fonctionnalité de synchronisation de l'heure Hyper-V pour utiliser l'heure du système d'exploitation hôte. Pour vous assurer que l'horloge du système est toujours précise, cette fonctionnalité doit être activée avec les services NTP.

Depuis le système d'exploitation de gestion :

1. Ouvrez la console du gestionnaire Hyper-V.
2. Pour les paramètres d'une VM Linux, sélectionnez **Integration Services**.
3. Assurez-vous que **Synchronisation date/heure** est sélectionné.

> ### Remarque
>
> Cette approche diffère de XenServer et VMware, pour lesquels la synchronisation de l'heure est désactivée pour éviter tout conflit avec NTP. La synchronisation de l'heure Hyper-V peut co-exister avec la synchronisation de l'heure NTP.

Corriger la synchronisation de l'heure sur ESX et ESXi

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si la fonctionnalité de synchronisation de l'heure de VMware est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée car l'hyperviseur et NTP tenteront de gérer l'horloge du système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, l'horloge du système de chaque invité Linux doit être synchronisée avec NTP. Pour cela, la synchronisation de l'heure de l'hôte doit être désactivée.

Si vous exécutez un noyau Linux paravirtualisé sur lequel VMware Tools est installé :

1. Ouvrez vSphere Client.
2. Modifiez les paramètres pour la VM Linux.
3. Dans la boîte de dialogue **Virtual Machine Properties** (Propriétés de la machine virtuelle), ouvrez l'onglet **Options**.
4. Sélectionnez VMware Tools.
5. Dans la zone **Advanced**, désélectionnez **Synchronize guest time with host** (Synchroniser l'heure de l'invité avec l'hôte).

Il existe un certain nombre de méthodes pour ajouter des machines Linux au domaine Active Directory qui sont prises en charge par XenDesktop pour Linux :

- Samba Winbind
- Service d'authentification Quest
- Centrify DirectControl

Suivez les instructions ci-dessous pour la méthode choisie.

Samba Winbind

Rejoindre un domaine Windows

Votre contrôleur de domaine doit être accessible et vous devez disposer d'un compte utilisateur Active Directory avec les autorisations nécessaires pour ajouter des machines au domaine.

1. Ouvrez YaST Windows Domain Membership.

2. Apportez les modifications suivantes :

- Définissez le domaine (Domain) ou le groupe de travail (Workgroup) sur le nom de votre domaine Active Directory ou l'adresse IP du contrôleur de domaine. Assurez-vous que le domaine est entré en majuscules.
- Sélectionnez Also Use SMB information for Linux Authentication (Utiliser aussi les informations SMB pour l'authentification Linux).
- Sélectionnez Create Home Directory on Login (Créer un répertoire de base à la connexion).
- Sélectionnez Single Sign-on for SSH (Authentification unique pour SSH).
- Assurez-vous que Offline Authentification (Authentification en mode déconnecté) n'est pas sélectionné. Cette option n'est pas compatible avec le VDA Linux.

3. Cliquez sur OK. Si vous êtes invité à installer des packages, cliquez sur Install.

4. Si un contrôleur de domaine est trouvé, vous êtes invité à joindre le domaine. Cliquez sur Yes.

5. Lorsque vous y êtes invité, entrez les informations d'identification d'un utilisateur de domaine avec les autorisations nécessaires pour ajouter des ordinateurs au domaine et cliquez sur OK.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. Un message indiquant si le processus a réussi s'affiche.

7. Si vous êtes invité à installer des packages samba et krb5, cliquez sur Install.

YaST peut avoir indiqué que ces modifications nécessiteront le redémarrage de certains services ou de la machine. Il est recommandé de redémarrer :

```
su -

reboot
```

SLED/SLES 12 uniquement : Corriger le nom de cache des informations d'identification

SLED/SLES 12 a modifié la spécification de nom du cache des informations d'identification Kerberos par défaut : FILE:/tmp/krb5cc_%{uid} est maintenant DIR:/run/user/%{uid}/krb5cc. Cette nouvelle méthode de mise en cache DIR n'est pas compatible avec le VDA Linux et doit être modifiée manuellement. En tant que root, modifiez /etc/krb5.conf en ajoutant le paramètre suivant dans la section [libdefaults] s'il n'est pas défini :

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

Vérifier l'appartenance au domaine

Le contrôleur XenDesktop requiert que toutes les machines VDA, Windows ou Linux, aient un objet ordinateur dans Active Directory.

Vérifiez que la machine est associée à un domaine à l'aide de la commande net ads de Samba :

```
sudo net ads testjoin
```

Vérifiez les informations supplémentaires de domaine et d'objet ordinateur avec :

```
sudo net ads info
```

Vérifier la configuration de Kerberos

Pour vérifier que Kerberos est correctement configuré pour être utilisé avec le VDA Linux, vérifiez que le fichier keytab système a été créé et contient des clés valides :

```
sudo klist –ke
```

Cette commande doit afficher la liste des clés disponibles pour les différentes combinaisons de noms principaux et de suites de chiffrement. Exécutez la commande kinit Kerberos pour authentifier la machine auprès du contrôleur de domaine à l'aide de ces clés :

```
sudo kinit -k MACHINE\$@REALM
```

Les noms de machine et de domaine doivent être spécifiés en majuscules, et le signe dollar ($) doit être placé dans une séquence d'échappement avec une barre oblique inverse (\) pour empêcher le remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom de domaine Kerberos ; assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

Vérifiez que le ticket TGT pour le compte de machine a été mis en cache à l'aide de :

```
sudo klist
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Examinez les détails du compte de machine à l'aide de :

```
sudo net ads status
```

Vérifier l'authentification utilisateur

Utilisez l'outil wbinfo pour vérifier que les utilisateurs de domaine peuvent s'authentifier auprès du domaine :

```
wbinfo --krb5auth=domain\\username%password
```

Le domaine spécifié ici est le nom de domaine Active Directory, et non le nom de domaine Kerberos. Pour le shell bash, la barre oblique inverse (\) doit être placée dans une séquence d'échappement avec une autre barre oblique inverse. Cette commande renvoie un message indiquant la réussite ou l'échec.

Pour vérifier que le module PAM Winbind est correctement configuré, ouvrez une session localement à l'aide d'un compte d'utilisateur de domaine qui ne s'est pas connecté à la machine précédemment.

```
ssh localhost -l domain\\username
```

```
id -u
```

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le uid renvoyé par la commande id -u :

```
ls /tmp/krb5cc_uid
```

Vérifiez que les tickets dans le cache d'identification de Kerberos de l'utilisateur sont valides et n'ont pas expiré :

```
klist
```

Quittez la session :

```
exit
```

Le même test peut être réalisé en ouvrant une session directement sur la console KDE ou Gnome.

Service d'authentification Quest

Configurer Quest sur le contrôleur de domaine

Cette procédure suppose que vous avez installé et configuré le logiciel Quest sur les contrôleurs de domaine Active Directory et disposez des droits Administrateur pour créer des objets ordinateur dans Active Directory.

Autoriser les utilisateurs de domaine à ouvrir une session sur des machines VDA Linux

Pour chaque utilisateur de domaine qui doit établir des sessions HDX sur une machine VDA Linux :

1. Dans la console de gestion Utilisateurs et ordinateurs Active Directory, ouvrez les propriétés de l'utilisateur Active Directory pour ce compte d'utilisateur.
2. Sélectionnez l'onglet Unix Account.
3. Sélectionnez la case Unix-enabled.
4. Définissez Primary GID Number sur l'ID d'un groupe d'utilisateurs de domaine.

> **Remarque**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> Ces instructions sont les mêmes que pour la configuration d'utilisateurs de domaine pour l'ouverture de session à l'aide de la console, RDP, SSH ou tout autre protocole de communication à distance.

Configurer Quest sur un VDA Linux

Configurer le démon VAS

Le renouvellement automatique des tickets Kerberos doit être activé et déconnecté ; l'authentification (ouverture de session en mode déconnecté) doit être désactivée :

```
sudo /opt/quest/bin/vastool configure vas vasd \
                auto-ticket-renew-interval 32400
sudo /opt/quest/bin/vastool configure vas vas_auth \
                allow-disconnected-auth false
```

Ces commandes définissent l'intervalle de renouvellement sur 9 heures (32400 secondes), ce qui est une heure de moins que la valeur par défaut de 10 heures pour la durée de vie de ticket. Définissez ce paramètre sur une valeur inférieure sur les systèmes avec une durée de vie de ticket Kerberos plus courte.

Configuration de PAM et de NSS

Quest requiert la configuration manuelle de PAM et NSS pour permettre la connexion d'utilisateur de domaine via HDX et d'autres services tels que su, ssh et RDP. Pour configurer PAM et NSS :

```
sudo /opt/quest/bin/vastool configure pam
sudo /opt/quest/bin/vastool configure nss
```

Rejoindre un domaine Windows

Associez la machine Linux au domaine Active Directory à l'aide de la commande vastool de Quest :

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

L'utilisateur est un utilisateur de domaine disposant des autorisations nécessaires pour associer des ordinateurs au domaine Active Directory. Le nom de domaine est le nom DNS du domaine ; par exemple, exemple.com.

Vérifier l'appartenance à un domaine

Le contrôleur XenDesktop requiert que toutes les machines VDA, Windows ou Linux, aient un objet ordinateur dans Active Directory. Pour vérifier qu'une machine Linux associée à Quest se trouve sur le domaine :

```
sudo /opt/quest/bin/vastool info domain
```

Si la machine est associée à un domaine, cette commande renvoie le nom de domaine. Si elle n'est pas associée, vous voyez le message d'erreur suivant :

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

default_realm not configured in vas.conf. Computer may not be joined to domain

Vérifier l'authentification utilisateur

Pour vérifier que Quest peut authentifier les utilisateurs de domaine à l'aide de PAM, ouvrez une session à l'aide d'un compte d'utilisateur de domaine qui ne s'est pas connecté à la machine précédemment.

```
ssh localhost -l domain\\username
```

```
id -u
```

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le uid renvoyé par la commande id -u :

```
ls /tmp/krb5cc_uid
```

Vérifiez que les tickets dans le cache d'identification de Kerberos de l'utilisateur sont valides et n'ont pas expiré :

```
/opt/quest/bin/vastool klist
```

Quittez la session :

```
exit
```

Le même test peut être réalisé en ouvrant une session directement sur la console KDE ou Gnome.

Centrify DirectControl

Rejoindre un domaine Windows

Avec le Centrify DirectControl Agent installé, associez la machine Linux au domaine Active Directory à l'aide de la commande **adjoin** Centrify :

```
su –
```

```
adjoin -w -V -u user domain-name
```

Le paramètre **user** est un utilisateur de domaine Active Directory disposant des autorisations nécessaires pour associer des ordinateurs au domaine Active Directory. Le paramètre de nom de domaine est le nom du domaine auquel associer la machine Linux.

Vérifier l'appartenance à un domaine

Le contrôleur XenDesktop requiert que toutes les machines VDA, Windows ou Linux, aient un objet ordinateur dans Active Directory. Pour vérifier qu'une machine Linux associée à Centrify se trouve sur le domaine :

```
su –
```

```
adinfo
```

Vérifiez que la valeur **Joined to domain** est valide et que **CentrifyDC mode** renvoie **connected**. Si le mode reste bloqué à l'état de démarrage, le client Centrify rencontre des problèmes de connexion au serveur ou d'authentification.

Des informations plus complètes sur le système et les diagnostics sont disponibles à l'aide de :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

adinfo --sysinfo all

adinfo –diag

Pour tester la connectivité avec les différents services Active Directory et Kerberos :

adinfo --test

Configurer un catalogue et un groupe de mise à disposition de machines Linux

Le processus de création de catalogues de machines et d'ajout de machines VDA Linux est très similaire à l'approche traditionnelle avec les VDA Windows. Reportez-vous à la documentation du produit Citrix pour obtenir une description complète de la méthode à utiliser pour effectuer ces tâches.

Pour la création de catalogues de machines contenant des machines VDA Linux, il existe quelques restrictions qui différencient ce processus de la création de catalogues de machines pour VDA Windows :

- Pour le système d'exploitation, sélectionnez :
  - Système d'exploitation de serveur Windows ou OS de serveur pour un modèle de mise à disposition de bureaux partagés hébergés.
  - Système d'exploitation de bureau Windows ou OS de bureau pour un modèle de mise à disposition de bureaux dédiés VDI.
- Assurez-vous que les machines sont définies avec alimentation non gérée.
- PVS et MCS n'étant pas pris en charge pour les VDA Linux, choisissez la méthode de déploiement **Autre service ou technologie** (images existantes).
- Ne combinez pas de machines VDA Linux et Windows dans le même catalogue de machines.

> ## Remarque
>
> Les versions antérieures de Citrix Studio ne prenaient pas en charge la notion de système d'exploitation Linux ; toutefois, la sélection de l'option Système d'exploitation de serveur Windows ou OS de serveur implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l'option Système d'exploitation de bureau Windows ou OS de bureau implique un modèle de mise à disposition d'un utilisateur XenDesktop unique par machine.

La documentation Citrix pour la création de catalogues de machines est référencée ci-dessous :

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7,9

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Les versions antérieures de XenDesktop ne sont pas prises en charge.

> **Conseil**
>
> Si une machine quitte et rejoint le domaine Active Directory, la machine devra être supprimée et ajoutée de nouveau au catalogue de machines.

Le processus de création d'un groupe de mise à disposition et d'ajout de catalogues de machines contenant des machines VDA Linux est presque identique aux machines VDA Windows. Reportez-vous à la documentation du produit Citrix en ligne pour obtenir une description complète de la méthode à utiliser pour effectuer ces tâches.

Lors de la création de groupes de mise à disposition qui contiennent des catalogues de machines VDA Linux, les restrictions suivantes s'appliquent :

- Pour le type de mise à disposition, sélectionnez Bureaux. Les machines VDA Linux ne prennent pas en charge la mise à disposition d'applications.
- Assurez-vous que les utilisateurs et les groupes AD que vous sélectionnez ont été correctement configurés pour l'ouverture de session sur les machines VDA Linux.
- N'autorisez pas l'ouverture de session d'utilisateurs non authentifiés (anonymes).
- Ne combinez pas le groupe de mise à disposition avec des catalogues de machines contenant des machines Windows.

La documentation Citrix pour la création de groupes de mise à disposition est référencée ci-dessous :

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7,9

Les versions antérieures de XenDesktop ne sont pas prises en charge.

Installer le logiciel VDA Linux

Si vous avez déjà installé une version de VDA Linux antérieure à la version 1.0, désinstallez-la avant d'installer la nouvelle version.

Arrêtez les services VDA Linux :

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx stop
```

Désinstallez le package :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

sudo rpm -e XenDesktopVDA

Important

La mise à niveau à partir de la Tech Preview vers les versions 1.0, 1.1, 1.2 ou 1.3 n'est pas prise en charge.

Remarque

À compter de la version 1.3, le chemin d'accès d'installation est différent. Dans les versions précédentes, les composants d'installation se trouvaient dans **/usr/local/** ; le nouvel emplacement est **/opt/Citrix/VDA/**.

Pour exécuter une commande, le chemin d'accès complet est nécessaire ; vous pouvez ajouter **/opt/Citrix/VDA/sbin** et /opt/Citrix/VDA/bin au chemin du système.

Installez le logiciel VDA Linux à l'aide du gestionnaire de package RPM :

Pour SuSE 11 :

sudo rpm -i XenDesktopVDA-1.3.0.312-1.x86_64.rpm

Pour SuSE 12 :

sudo rpm -i XenDesktopVDA-1.3.0.312-1.x86_64.rpm

Si vous avez déjà installé la version 1.1 du VDA Linux, mettez à niveau le logiciel VDA Linux à l'aide du gestionnaire de package RPM :

Pour SuSE 11 :

sudo rpm -U XenDesktopVDA-1.3.0.312-1.x86_64.rpm

Pour SuSE 12 :

sudo rpm -U XenDesktopVDA-1.3.0.312-1.x86_64.rpm

Important

Vous devez redémarrer la machine Linux VDA après la mise à niveau.

Après l'installation du package, vous devez configurer le VDA Linux en exécutant le script **ctxsetup.sh**. Si vous avez mis à niveau le package, vous devez exécuter le script ctxsetup.sh pour finaliser la mise à niveau. Avant d'apporter des

© 1999-2017 Citrix Systems, Inc. All rights reserved.

modifications, ce script va vérifier l'environnement et s'assurer que toutes les dépendances sont installées. Si nécessaire, ce script peut être réexécuté à tout moment pour modifier les paramètres.

Le script peut être exécuté manuellement avec invites ou automatiquement avec réponses pré-configurées. Consultez l'aide sur ce script avant de continuer :

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh –help
```

Configuration avec invites

Exécutez une configuration manuelle avec questions :

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Configuration automatique

Pour une installation automatique, les options requises par le script d'installation peuvent être fournies avec des variables d'environnement. Si toutes les variables requises sont présentes, le script n'invite pas l'utilisateur à entrer les informations, ce qui permet d'exécuter le processus d'installation à l'aide d'un script.

Les variables d'environnement prises en charge sont les suivantes :

- CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N - Le Virtual Delivery Agent prend en charge la spécification d'un nom de Delivery Controller à l'aide d'un enregistrement DNS CNAME. Il est généralement configuré sur N.
- CTX_XDL_DDC_LIST = list-ddc-fqdns – Le Virtual Delivery Agent requiert une liste séparée par des espaces de noms de domaines complets de Delivery Controller
- à utiliser pour s'enregistrer auprès d'un Delivery. Au moins un alias de nom de domaine complet (FQDN) ou CNAME doit être spécifié.
- CTX_XDL_VDA_PORT = port-number – Le Virtual Delivery Agent communique avec les Delivery Controller à l'aide d'un port TCP/IP. Il s'agit généralement du port 80.
- CTX_XDL_REGISTER_SERVICE = Y | N - Les services Linux Virtual Desktop prennent en charge le lancement lors du démarrage. Généralement configuré sur Y.
- CTX_XDL_ADD_FIREWALL_RULES = Y | N – Les services Linux Virtual Desktop requièrent que les connexions réseau entrantes soient autorisées via le pare-feu du système. Vous pouvez ouvrir automatiquement les ports requis (par défaut, les ports 80 et 1494) dans le pare-feu du système pour Linux Virtual Desktop. Généralement configuré sur Y.
- CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 – Le Virtual Delivery Agent requiert que les paramètres de configuration Kerberos s'authentifient auprès des Delivery Controller. La configuration de Kerberos est déterminée depuis l'outil d'intégration d'Active Directory installé et configuré sur le système. Spécifiez la méthode d'intégration d'Active Directory prise en charge à utiliser :
  - 1 - Samba Winbind
  - 2 - Service d'authentification Quest
  - 3 - Centrify DirectControl
- CTX_XDL_HDX_3D_PRO= Y | N – Linux Virtual Desktop prend en charge HDX 3D Pro, un ensemble de technologies d'accélération des graphiques conçues pour optimiser la virtualisation des applications riches en graphiques. HDX 3D Pro nécessite l'installation d'une carte graphique NVIDIA Grid compatible. Si HDX 3D Pro est sélectionné, le Virtual Delivery Agent doit être configuré pour le mode Bureaux VDI (session unique) – (c'est-à-dire, CTX_XDL_VDI_MODE=Y). Ceci n'est pas pris en charge avec SUSE. Assurez-vous que cette valeur est définie sur N.
- CTX_XDL_VDI_MODE= Y | N - Indiquer si la machine est configurée comme modèle de mise à disposition de bureaux dédiés (VDI) ou comme modèle de mise à disposition de bureaux partagés hébergés. Pour les environnements HDX 3D

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Pro, doit être défini sur Y. Il est généralement configuré sur N.

- CTX_XDL_SITE_NAME= dns-name – Le Virtual Delivery Agent découvre les serveurs LDAP à l'aide de DNS en interrogeant les enregistrements du service LDAP. Pour limiter les résultats de recherche DNS à un site local, un nom de site DNS peut être spécifié. Ce paramètre est généralement vide [none].
- CTX_XDL_LDAP_LIST= list-ldap-servers – Le Virtual Delivery Agent interroge par défaut le DNS pour découvrir les serveurs LDAP, mais si le DNS ne peut pas fournir les enregistrements du service LDAP, vous pouvez fournir une liste séparée par des espaces des noms de domaine complets (FQDN) LDAP avec le port LDAP (ex. ad1.masociété.com:389). Ce paramètre est généralement vide [none].
- CTX_XDL_SEARCH_BASE= search-base – Le Virtual Delivery Agent interroge par défaut LDAP à l'aide d'une base de recherche définie sur la racine du domaine Active Directory (ex. DC=masociété,DC=com), toutefois une base de recherche peut être spécifiée pour améliorer les performances (ex. OU=VDI,DC=masociété,DC=com). Ce paramètre est généralement vide [none].
- CTX_XDL_START_SERVICE = Y | N - Indiquer si les services VDA Linux sont lancés lorsque la configuration du VDA Linux est terminée. Généralement configuré sur Y.

> **Remarque**
>
> HDX 3D Pro n'est actuellement pas disponible sur SUSE.

Définissez la variable d'environnement et exécutez le script de configuration :

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Vous devez fournir l'option **-E** avec **sudo** pour transmettre les variables d'environnement au nouveau shell créé. Citrix vous recommande de créer un fichier de script shell à partir des commandes ci-dessus avec **#!/bin/bash** sur la première ligne.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Vous pouvez aussi spécifier tous les paramètres avec une seule commande :

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
    CTX_XDL_DDC_LIST=list-ddc-fqdns \
    CTX_XDL_VDA_PORT=port-number \
    CTX_XDL_REGISTER_SERVICE=Y|N \
    CTX_XDL_ADD_FIREWALL_RULES=Y|N \
    CTX_XDL_AD_INTEGRATION=1|2|3 \
    CTX_XDL_HDX_3D_PRO=Y|N \
    CTX_XDL_VDI_MODE=Y|N \
    CTX_XDL_SITE_NAME=dns-name \
    CTX_XDL_LDAP_LIST=list-ldap-servers \
    CTX_XDL_SEARCH_BASE=search-base \
    CTX_XDL_START_SERVICE=Y|N \
    /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Supprimer les modifications de configuration

Dans certains scénarios, il peut être nécessaire de supprimer les modifications de configuration effectuées par le script **ctxsetup.sh** sans désinstaller le package VDA Linux.

Consultez l'aide sur ce script avant de continuer :

```
sudo /usr/local/sbin/ctxcleanup.sh --help
```

Pour supprimer les modifications de configuration :

```
sudo /usr/local/sbin/ctxcleanup.sh
```

> ### Important
>
> Ce script supprimera toutes les données de configuration de la base de données et empêchera VDA Linux de fonctionner.

Journaux de configuration

Les scripts **ctxsetup.sh** et **ctxcleanup.sh** affichent les erreurs dans la console, avec des informations supplémentaires consignées dans un fichier journal de configuration :

```
/tmp/xdl.configure.log
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Redémarrez les services de VDA Linux pour que les modifications prennent effet.

Exécuter le logiciel VDA

Une fois que vous avez configuré le VDA Linux à l'aide du script ctxsetup.sh, utilisez les commandes suivantes pour contrôler le VDA Linux.

Pour démarrer les services VDA Linux :

sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start

Pour arrêter les services VDA Linux :

sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop

Pour redémarrer les services VDA Linux :

sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

sudo /sbin/service ctxvda start

Pour vérifier l'état de fonctionnement des services du VDA Linux :

sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status

Désinstaller le logiciel VDA Linux

Pour vérifier que le VDA Linux est installé et pour afficher la version du package installé :

rpm -q XenDesktopVDA

Pour afficher des informations plus détaillées :

rpm –qi XenDesktopVDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour désinstaller le package VDA Linux :

```
sudo rpm -e XenDesktopVDA
```

> **Remarque**
>
> La désinstallation du logiciel VDA Linux supprimera le PostgreSQL associé et d'autres données de configuration. Toutefois, le package PostgreSQL et les autres packages dépendants qui ont été installés avant l'installation du VDA Linux ne seront pas supprimés.

Cet article ne traite pas de la suppression des packages dépendants, y compris PostgreSQL.

Résolution des problèmes

Linux VDA v1.3 ajoute H264 et une valeur HardwareEncoding dans le chemin d'accès de registre HKLM\Software\Citrix\Ica\Session\\Graphics pour faciliter la résolution des problèmes graphiques rencontrés avec le VDA.

Exécutez la commande suivante pour publier le codage H.264 dans un Linux VDA avant le lancement d'une session :

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"AdvertiseH264" -d "0x00000001" --force
```

Lancez la session et vérifiez si la clé H264 est créée dans le chemin d'accès de registre. Si tel est le cas, le codage H.264 est utilisé.

```
/opt/Citrix/VDA/bin/ctxreg list -k
"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"
```

Le codage matériel 3D Pro est désactivé par défaut, utilisez la commande ci-dessous pour activer la fonction :

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"HardwareEncoding" -d "0x00000001" --force
```

Lancez la session et vérifiez la valeur de « HardwareEncoding » dans le chemin d'accès du Registre ; 0 signifie que le codage matériel n'est pas utilisé, 1 signifie qu'il est utilisé.

```
/opt/Citrix/VDA/bin/ctxreg list -k
"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Utilisez la commande ci-dessous pour interroger votre ID de session :

```
/opt/Citrix/VDA/bin/ctxqsession
```

Actuellement, Linux VDA ne permet pas aux utilisateurs de choisir l'environnement de bureau lors de l'ouverture de session ; pour contourner ce problème, l'utilisateur peut configurer un fichier (par exemple, .xsession) pour la distribution Linux afin de définir l'environnement de bureau par défaut pour chaque utilisateur. Reportez-vous aux documents accompagnant la distribution Linux pour plus d'informations.

Pour définir KDE comme environnement par défaut :

```
#! /usr/bin/env bash

exec startkde
```

Pour définir GNOME comme environnement de bureau par défaut :

```
#! /usr/bin/env bash

exec gnome-session
```

La plupart des problèmes proviennent d'une configuration incorrecte de la machine Linux, principalement des paramètres réseau, de la configuration du serveur de temps NTP ou de l'appartenance à un domaine Active Directory. Corriger la configuration de la machine Linux résout souvent les problèmes rencontrés avec le logiciel VDA.

L'agent broker et le service HDX consignent les entrées de journal dans syslog. L'équipe d'assistance de Citrix dispose d'un ensemble d'outils permettant un traçage supplémentaire lors d'un appel.

Journalisation du service HDX

Le service HDX est configuré pour consigner les entrées de journal dans syslog et aucune configuration supplémentaire n'est requise.

Journalisation de l'agent broker

L'agent broker (également appelé service ctxvda) écrit les données de journal dans syslog via des sockets réseau. Ce comportement n'est peut-être pas configuré initialement. Pour définir la journalisation de l'agent broker dans syslog, la configuration suivante est requise.

SLED/SLES 11

Modifiez le fichier /etc/syslog-ng/syslog-ng.conf en ajoutant la ligne suivante dans la section s_sys :

```
udp(ip(127.0.0.1) port(514));
```

Enregistrez et fermez le fichier syslog-ng.conf. Redémarrez le service syslog-ng pour appliquer la modification :

```
sudo service syslog-ng restart
```

SLED/SLES 12

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Ajoutez les lignes suivantes dans le fichier /etc/rsyslog.conf :

```
$ModLoad imudp

$UDPServerRun 514
```

Enregistrez et fermez le fichier rsyslog.conf. Redémarrez le service rsyslog pour appliquer la modification :

```
sudo service rsyslog restart
```

Vérifiez qu'aucun processus orphelin n'empêche les nouvelles sessions de démarrer :

```
sudo pkill -9 ctxhdx

sudo pkill -9 ctxgfx

sudo pkill -9 ctxlogin

sudo pkill -9 ctxvfb
```

Redémarrez les services VDA Linux et réessayez.

Vérifiez le propriétaire et les autorisations des fichiers et répertoires suivants :

- /var - Owner: root, Group: root, Permissions: 0755
- /var/xdl - Owner: ctxsrvr, Group: ctxadm, Permissions: 0755
- /var/xdl/.isacagent - Owner: root, Group: root, Permissions: 0666
- /var/xdl/.winsta - Owner: ctxsrvr, Group: ctxadm, Permissions: 0777
- /var/xdl/vda - Owner: root, Group: root, Permissions: 0755

Vérifiez que le volume sur la machine exécutant Citrix Receiver et le bureau Linux n'est pas désactivé ou réglé sur un niveau bas.

Vérifiez que l'audio est activé sur le VDA Linux. Utilisez l'outil ctxreg pour interroger la valeur de l'élément de configuration fDisableCam :

```
sudo ctxreg read -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam
```

Une valeur de 0x1 signifie que l'audio est désactivé. Pour l'activer, définissez fDisableCam sur 0x0 :

```
sudo ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam  -d 0x00000000
```

Si l'audio n'est toujours pas audible, vérifiez que le récepteur audio Citrix est chargé par pulseaudio. Ce module PulseAudio est chargé dans le démon pulseaudio au démarrage de la session. Utilisez l'outil pacmd pour vérifier si le récepteur audio Citrix est chargé :

```
pacmd list-sinks
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si le récepteur audio Citrix est chargé, le résultat doit être :

name:

driver:

Si le récepteur audio Citrix n'est pas chargé, arrêtez le processus ctxaudio et redémarrez-le.

Vérifiez que l'audio est activé sur le VDA Linux et que l'enregistrement audio est activé sur le client ICA. Si l'audio n'est toujours pas enregistré, vérifiez que la source audio Citrix est chargée par pulseaudio. Si l'enregistrement audio est activé sur le client ICA, ce module PulseAudio sera chargé dans le démon pulseaudio au démarrage de la session. Utilisez l'outil pacmd pour vérifier si la source audio Citrix est chargée :

pacmd list-sources

Si la source audio Citrix est chargée, le résultat doit être :

name:

driver:

Si la source audio Citrix n'est pas chargée, arrêtez le processus ctxaudio et redémarrez-le.

Il existe un certain nombre d'éléments à vérifier si l'impression ne fonctionne pas correctement. Le démon d'impression est un processus par session et doit être en cours d'exécution pour la durée de la session. Vérifiez que le démon d'impression est en cours d'exécution.

ps –ef | grep ctxlpmngt

Si le processus ctxlpmngt n'est pas exécuté, démarrez manuellement ctxlpmngt à partir d'une ligne de commande.

Si l'impression ne fonctionne toujours pas, l'élément suivant à vérifier est l'infrastructure CUPS. Le service ctxcups est pour la gestion d'imprimante et communique avec l'infrastructure Linux CUPS. Il s'agit d'un processus unique par machine qui peut être vérifié par :

service ctxcups status

Si le service n'est pas exécuté, démarrez-le manuellement :

service ctxcups start

Une impression illisible peut être causée par un pilote d'imprimante incompatible. Une configuration pilote par utilisateur est disponible et peut être configurée en modifiant le fichier de configuration ~/.CtxlpProfile.

[DEFAULT_PRINTER]

printername=

model=

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

ppdpath=

drivertype=

printername est un champ contenant le nom de l'imprimante par défaut actuelle du côté client. Il s'agit d'une valeur en lecture seule qui ne doit pas être modifiée.

Important

Les champs **ppdpath**, **model** et **drivertype** ne doivent pas être définis en même temps car un seul est appliqué pour l'imprimante mappée.

Si le pilote d'imprimante universel n'est pas compatible avec l'imprimante cliente, le modèle du pilote d'imprimante natif peut être configuré avec l'option model=. Le nom du modèle de l'imprimante peut être obtenu avec la commande lpinfo.

lpinfo –m

...

xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

...

Le modèle peut être défini pour correspondre à l'imprimante :

Model=xerox/ph3115.ppd.gz

Si le pilote d'imprimante universel n'est pas compatible avec l'imprimante cliente, le chemin de fichier ppd du pilote d'imprimante natif peut être configuré. La valeur de ppdpath est le chemin d'accès absolu du fichier du pilote d'imprimante natif.

Par exemple, il existe un pilote ppd sous /home/tester/NATIVE_PRINTER_DRIVER.ppd.

ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd

Il existe trois types de pilote d'imprimante universel fournis par Citrix (postscript, pcl5 et pcl6). Ils peuvent être configurés dans le type de pilote si aucun pilote d'imprimante natif n'est disponible.

Par exemple, si le pilote d'imprimante par défaut est de type PCL5 :

drivertype=pcl5

Remarque

Citrix Receiver pour Mac et Citrix Receiver pour Linux prennent uniquement en charge les imprimantes PostScript ; par conséquent, les pilotes d'imprimante universels PCL6 et PCL5 ne sont pas applicables. Dans cette situation, ppdpath ou le modèle de pilote d'imprimante natif doit être défini sur une imprimante non-Postscript.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

CDM ne fonctionne pas

La fonctionnalité CDM comprend un processus démon (ctxcdmd) ; si la fonction CDM échoue, redémarrez la machine VDA Linux et vérifiez si le démon a démarré correctement :

```
Ps -lef | grep ctxcdmd
```

Le nom du fichier dans le lecteur mappé doit respecter les règles d'affectation des noms d'OS VDA et Receiver.

Problèmes connus

L'état CAPS VERR de Citrix Receiver pour Android peut être annulé lors de l'itinérance de session

L'état de CAPS VERR peut être perdu lors de l'itinérance d'une connexion existante à Citrix Receiver pour Android. La solution consiste à utiliser la touche MAJ sur le clavier étendu pour basculer entre les majuscules et les minuscules.

Les raccourcis ALT ne fonctionnent pas toujours lors d'une connexion à un VDA Linux à l'aide de Citrix Receiver pour Mac

Citrix Receiver pour Mac envoie AltGr pour les touches Options/Alt droite et gauche par défaut. Il est possible de modifier ce comportement dans les paramètres Citrix Receiver, mais les résultats varient selon les applications.

Les bibliothèques X client récentes peuvent causer des problèmes de mappage du clavier sur SuSE Linux Enterprise Desktop 11

Les versions récentes des packages xorg-x11-libX11 sur SuSE Linux Enterprise Desktop 11 peuvent rencontrer des problèmes avec les changements de mappage du clavier, qui à leur tour peuvent entraîner des problèmes avec la fonctionnalité du clavier au sein d'une session HDX. Ce problème peut se produire lorsque la version installée des packages se trouve dans la plage 7.4-5.11.11.1 à 7.4-5.11.15.1.

La solution consiste à revenir à la version SP3 stock du package xorg-x11-libX11, ce qui permet le fonctionnement normal des changements de mappage du clavier. Par exemple :

```
rpm -i --force xorg-x11-libX11-7.4-5.9.1

rpm –i --force xorg-x11-libX11-32bit-7.4-5.9.1

rpm -e xorg-x11-libX11-7.4-5.11.15.1

rpm -e xorg-x11-libX11-32bit-7.4-5.11.15.1
```

Cette opération doit être effectuée avant qu'un utilisateur ouvre une session sur la machine ; si cette opération est effectuée lorsqu'une session est active, ces paramètres ne sont pas appliqués jusqu'à la prochaine ouverture de session.

En cas de mise à niveau à partir de SP3 stock, les packages xorg-x11-libX11 ci-dessus peuvent être verrouillés pour la version installée de manière à ce qu'ils ne soient pas modifiés lors de la mise à niveau. Avant de procéder à la mise à niveau, exécutez ce qui suit :

```
zypper al xorg-x11-libX11
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

zypper al xorg-x11-libX11-32bit

Des lancements de session lents peuvent se produire lors de l'utilisation de VDA Linux avec un Delivery Controller à partir de XenDesktop v7.1

Le lancement lent est causé par la présence de paramètres CGP dans le fichier ICA généré par le Delivery Controller v7.1. Lorsque ces paramètres sont présents, Citrix Receiver tente d'établir une connexion sur le port TCP 2598. Par défaut, les paramètres de pare-feu sur certaines distributions Linux, telles que SLED 11, sont configurés pour rejeter les paquets TCP SYN, ce qui entraîne une temporisation et par conséquent un lancement de session lent. La solution consiste à configurer le pare-feu sur le VDA Linux pour qu'il rejette TCP SYN sur le port 1494. Ce problème a été résolu dans les versions récentes des Delivery Controller.

Échec de l'enregistrement lorsque le VDA Linux est associé au domaine

Dans certaines circonstances, lorsqu'un VDA Linux est associé au domaine et qu'un nouveau jeu de clés Kerberos est généré, le broker ne parvient pas à établir un contexte de sécurité avec le VDA. Ce problème est souvent causé par le fait que le broker utilise un ticket de service VDA mis en cache obsolète basé sur le jeu de clés Kerberos précédent. Le VDA peut quand même se connecter au broker, mais le broker ne sera pas en mesure d'établir un contexte de sécurité pour le VDA. Le symptôme courant est l'échec de l'enregistrement du VDA.

Ce problème se résout de lui-même lorsque le ticket de service VDA expire et qu'il est renouvelé, mais les tickets de service ont en général une durée de vie assez longue. Ce processus peut prendre beaucoup de temps.

La solution consiste à effacer le cache des tickets du broker. Vous pouvez simplement redémarrer le broker ou exécuter en tant qu'administrateur la commande suivante sur le broker à partir d'une invite de commande :

klist -li 0x3e4 purge

Cette opération supprime tous les tickets de service du cache LSA détenu par le service réseau principal sous lequel le service de broker Citrix s'exécute. Les tickets de service pour d'autres VDA et, potentiellement, d'autres services sont supprimés. Mais ce n'est pas un problème : ces tickets de service seront de nouveau acquis depuis le serveur KDC le cas échéant.

Audio Plug-n-Play non pris en charge

Il est recommandé que tout périphérique de capture audio soit connecté à la machine cliente avant de commencer à enregistrer l'audio dans la session ICA. Si un périphérique est connecté après que l'application d'enregistrement audio a démarré, l'application peut cesser de répondre. Si ce problème se produit, redémarrez l'application. Le même problème peut se produire si un périphérique de capture est déconnecté pendant l'enregistrement.

Distorsion audio

Windows 10 Receiver peut rencontrer une distorsion audio lors de l'enregistrement audio.

Le pilote CTXPS n'est pas compatible avec certaines imprimantes PLC

Si l'impression présente des anomalies, définissez le pilote d'imprimante sur le pilote d'imprimante natif fourni par le fabricant.

Impression lente avec les documents volumineux

Lorsque vous imprimez un document volumineux sur une imprimante cliente locale, le fichier est transféré sur une connexion serveur. Si la connexion est lente, ce transfert risque de durer longtemps.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Notifications d'imprimante et de travaux d'impression d'autres sessions

Le concept de session de Linux n'est pas le même que celui du système d'exploitation Windows. Par conséquent, tous les utilisateurs reçoivent les notifications de l'ensemble du système. L'administrateur peut désactiver ces notifications en modifiant le fichier de configuration CUPS, /etc/cups/cupsd.conf.

Recherchez le nom de stratégie configuré dans le fichier.

```
DefaultPolicy default
```

Si le nom de la stratégie est default, ajoutez les lignes suivantes dans le bloc XML de la stratégie par défaut.

```
# Job/subscription privacy...

JobPrivateAccess default

JobPrivateValues default

SubscriptionPrivateAccess default

SubscriptionPrivateValues default

... ...

    Require user @OWNER

    Order deny,allow


    Order deny,allow
```

Glossaire

Broker : composant XenDesktop responsable de la négociation des sessions HDX sur les différents VDA dans un déploiement XenDesktop. Également appelé DDC ou contrôleur XenDesktop.

Agent broker : composant sur la machine VDA Linux qui fournit le bureau à mettre à disposition. L'agent broker communique avec le broker pour permettre la négociation de sessions. Il est composé de deux composants principaux, le service VDA et le service HDX.

Citrix Director : console d'assistance Citrix permettant le suivi et le contrôle des VDA XenDesktop.

Citrix Studio : console d'administration Citrix utilisée pour configurer XenDesktop.

DDC : XenDesktop Desktop Delivery Controller. Également appelé Broker ou Delivery Controller.

FQDN (Fully Qualified Domain Name) : nom de domaine complet

HDX (High Definition Experience) : protocole d'expérience utilisateur haute définition. Anciennement appelé protocole ICA Citrix.

Service HDX : service Linux (ctxhdx) qui transmet à distance le bureau Linux virtuel via le protocole HDX. Il communique avec

© 1999-2017 Citrix Systems, Inc. All rights reserved.

le service VDA pour permettre la négociation de sessions.

RHEL : Red Hat Enterprise Linux. Distribution Linux commerciale fournie par Red Hat.

SLED : SUSE Linux Enterprise Desktop. Distribution Linux commerciale fournie par Novell.

SLES : SUSE Linux Enterprise Server. Distribution Linux commerciale fournie par Novell.

VDA : Virtual Delivery Agent.

Service VDA : service Linux (ctxvda) qui communique avec le broker pour permettre la négociation de sessions. Il communique également avec le service HDX pour la mise à disposition de session distante.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Créer un site

Jul 07, 2016

Un *site* est le nom que vous donnez à un déploiement XenApp ou XenDesktop. Il comprend les Delivery Controller et autres composants principaux, les VDA, les connexions aux hôtes (le cas échéant), ainsi que les catalogues de machines et les groupes de mise à disposition que vous créez et gérez. Vous créez le site après avoir installé les composants et avant la création du premier catalogue de machines et groupe de mise à disposition.

Lorsque vous créez un site, vous êtes automatiquement inscrit au Programme d'amélioration de l'expérience utilisateur Citrix (CEIP). CEIP recueille des informations d'utilisation et des statistiques anonymes, puis les envoie à Citrix. Le premier package de données est envoyé à Citrix approximativement sept jours après la création du site. Vous pouvez changer votre participation à tout moment après la création du site en sélectionnant **Configuration** dans le panneau de navigation de Studio, puis l'onglet Assistance produit, et en suivant les instructions. Pour de plus amples informations sur le programme CEIP, consultez http://more.citrix.com/XD-CEIP.

L'utilisateur qui crée un site devient un administrateur complet ; pour de plus amples informations, consultez l'article Délégation de l'administration.

Consultez cet article avant de démarrer l'assistant de création de site ; il comprend les tâches à accomplir et les décisions à prendre en compte avant de créer le site.

Pour créer un site :

Ouvrez Studio, s'il n'est pas déjà ouvert. Vous êtes automatiquement dirigé vers l'action qui lance l'assistant de création de site. Les pages de l'assistant couvrent la configuration suivante :

Il existe deux types de site ; choisissez-en un :

- **Site de mise à disposition d'applications et de bureaux**. Si vous créez un site de mise à disposition d'applications et de bureaux, vous pouvez également choisir de créer un site de déploiement complet (recommandé) ou un site vide. Un site vide est uniquement partiellement configuré et il est généralement créé par des administrateurs expérimentés.
- **Site Remote PC Access**. Un site Remote PC Access autorise les utilisateurs désignés à accéder à distance à leurs ordinateurs de bureau via une connexion sécurisée.

Si vous créez maintenant un déploiement de mise à disposition d'applications et de bureaux, vous pouvez ajouter un déploiement Remote PC Access plus tard. Inversement, si vous créez un déploiement Remote PC Access maintenant, vous pouvez ajouter un déploiement complet ultérieurement.

Tapez un nom pour le site. Une fois le site créé, son nom apparaît en haut du panneau de navigation de Studio : **Citrix Studio** (*nom-site*).

La page **Bases de données** contient les sélections de configuration pour les bases de données du site, de contrôle et de journalisation de la configuration. Pour de plus amples informations sur les choix et les exigences de configuration de base de données, consultez l'article Bases de données.

Lorsque vous créez un site, si vous choisissez d'installer la base de données SQL Server Express en tant que base de données

© 1999-2017 Citrix Systems, Inc. All rights reserved.

du site (ce qui est le paramètre par défaut), la machine sera redémarrée après l'installation du logiciel de base de données Ce redémarrage ne se produit pas si vous choisissez de ne pas installer le logiciel SQL Server Express en tant que base de données du site.

Si vous n'utilisez pas l'installation par défaut de SQL Server Express Edition, assurez-vous que le logiciel SQL Server est installé sur les machines avant de créer un site ; l'article Configuration système requise répertorie les versions prises en charge.

Si vous souhaitez ajouter plusieurs Delivery Controller au site, et que vous avez déjà installé le logiciel du Controller sur d'autres serveurs, vous pouvez les ajouter au site à partir de cette page de l'assistant de création de site. Si vous souhaitez générer des scripts qui configureront les bases de données, ajoutez les Controller avant de générer les scripts.

Posez-vous la question de savoir si vous allez utiliser des licences existantes ou la licence d'évaluation gratuite de 30 jours qui vous permet d'ajouter des fichiers de licences ultérieurement. Vous pouvez aussi ajouter ou télécharger des fichiers de licences à partir de l'assistant de création de site. Pour de plus amples informations, consultez la documentation relative au système de licences.

Spécifiez l'adresse du serveur de licences au format *nom*[*port*]. Le nom doit être un nom de domaine complet (FQDN), NetBIOS ou une adresse IP ; un nom de domaine complet est recommandé. Si vous omettez le numéro de port, la valeur par défaut est 27000. Cliquez sur **Connect**. Vous ne pouvez pas passer à la page suivante de l'assistant tant qu'une connexion n'a pas été établie avec le serveur de licences.

Veuillez consulter la section Remote PC Access ci-dessous.

Si vous prévoyez d'utiliser des machines virtuelles sur un hôte (hyperviseur ou service de cloud) pour fournir des bureaux et des applications, vous pouvez éventuellement créer (configurer) la première connexion à votre hôte lorsque vous créez un site. Vous pouvez également spécifier des ressources réseau et de stockage pour cette connexion. Vous pouvez modifier cette connexion et les ressources plus tard, et créer des connexions supplémentaires.

Important : consultez l'article Connexions et ressources pour obtenir des informations sur la configuration des informations de connexion et des ressources dans l'assistant de création de site :

- Sources d'informations du type de connexion indique où trouver des informations sur chaque type de connexion prise en charge.
- Stockage hôte décrit les types de stockage et les méthodes de gestion du stockage.
- Gestion du stockage et Sélection du stockage décrivent comment configurer les informations de stockage lors de la création d'une connexion.

Si vous n'utilisez pas de VM sur un hyperviseur où un service de cloud pour fournir des applications et des bureaux (ou si vous allez utiliser Studio pour gérer les bureaux utilisateur hébergés sur des PC lames dédiés), sélectionnez le type de connexion **Aucun**.

Si vous configurez un site Remote PC Access et prévoyez d'utiliser la fonctionnalité Wake on LAN, sélectionnez le type d'hôte **Microsoft System Center Configuration Manager**.

Sur la page **Connexion**, spécifiez également si vous allez utiliser les outils Citrix (tels que Machine Creation Services) ou

© 1999-2017 Citrix Systems, Inc. All rights reserved.

d'autres outils pour créer des VM sur l'hôte.

Sur les pages **Stockage** et **Réseau**, configurez les informations requises en vous aidant des informations ci-dessus.

Rappel : l'article Connexion et ressources contient des instructions détaillées.

Vous pouvez sélectionner des fonctionnalités supplémentaires pour personnaliser votre site. Lorsque vous sélectionnez la case à cocher d'un élément qui requiert des informations, une boîte de dialogue de configuration s'affiche.

Intégration de AppDNA

Si vous prévoyez d'utiliser AppDisks et avez installé AppDNA, activez cette fonctionnalité pour permettre l'analyse des applications dans les Appdisks, vérifier les problèmes de compatibilité et prendre des mesures pour résoudre ces problèmes. Pour plus d'informations, veuillez consulter l'article AppDisks.

App-V Publishing

Sélectionnez cette fonctionnalité si vous prévoyez d'utiliser des applications à partir de packages Microsoft App-V qui sont situés sur des serveurs App-V. Lorsque vous sélectionnez cette case, vous êtes invité à fournir l'adresse URL du serveur de gestion Microsoft App-V et l'adresse URL et le numéro de port du serveur de publication d'App-V.

Si vous utilisez des applications depuis les packages App-V sur des emplacements de partage réseau uniquement, vous n'avez pas besoin d'activer cette fonctionnalité.

Vous pouvez également activer/désactiver et configurer cette fonctionnalité ultérieurement dans Studio. Pour plus d'informations, veuillez consulter l'article App-V.

Pour de plus amples informations sur les déploiements Remote PC Access, consultez l'article Remote PC Access.

Si vous utilisez la fonctionnalité Wake on LAN, suivez les étapes de configuration sur la console Microsoft System Center Configuration Manager avant de créer le site. Pour de plus amples informations, veuillez consulter l'article Microsoft System Center Configuration Manager.

Lorsque vous créez un site Remote PC Access :

- Si vous utilisez la fonctionnalité Wake on LAN, spécifiez l'adresse, les informations d'identification et les informations de connexion Microsoft System Center Configuration Manager sur la page **Gestion de l'alimentation**.
- Spécifiez les utilisateurs ou les groupes d'utilisateurs sur la page Utilisateurs ; aucune action par défaut n'ajoute automatiquement tous les utilisateurs. Vous pouvez également spécifier des comptes de machines (domaine et unité d'organisation (UO)) sur la page **Comptes de machines** de l'assistant.

  Pour ajouter des informations utilisateur, cliquez sur **Ajouter des utilisateurs**. Sélectionnez des utilisateurs et des groupes d'utilisateurs, puis cliquez sur **Ajouter des utilisateurs**.

  Pour ajouter des comptes de machines, cliquez sur **Ajouter des comptes de machines**. Sélectionnez les comptes de machines, puis cliquez sur **Ajouter des comptes de machines**. Cliquez sur **Ajouter des unités d'organisation**. Sélectionnez le domaine et les unités d'organisation et indiquez si les éléments des sous-dossiers doivent être inclus. Cliquez sur **Ajouter des unités d'organisation**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Remarque : lorsque vous créez un site Remote PC Access, un catalogue de machines appelé Remote PC User Machine Accounts est créé automatiquement ; il contient tous les comptes de machines que vous avez ajoutés dans l'assistant de création de site. Un groupe de mise à disposition appelé Remote PC User Desktops est créé automatiquement ; il contient tous les utilisateurs et les groupes d'utilisateurs que vous avez ajoutés.

La dernière page de l'assistant de création de site présente les informations que vous avez spécifiées. Utilisez le bouton **Précédent** si vous souhaitez modifier quoi que ce soit. Lorsque vous avez terminé, cliquez sur **Créer** ; la création de site commence.

Tester une configuration de site

Pour exécuter des tests après avoir créé le site, sélectionnez**Citrix Studio (Site** *nom site***)** dans la partie supérieure du panneau de navigation et cliquez sur **Tester le site** dans le panneau central. Vous pouvez afficher un rapport HTML des résultats de test du site.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Créer des catalogues de machines

Aug 22, 2016

Des collections de machines virtuelles ou physiques sont gérées comme une seule entité appelée *Catalogue de machines*. Toutes les machines d'un catalogue de machines ont le même type de système d'exploitation : serveur ou bureau. Un catalogue contenant des machines avec OS de serveur peut contenir des machines Windows ou Linux, mais pas les deux.

Studio vous guide dans le processus de création du premier catalogue de machines après la création du site. Après la création du premier catalogue de machines, Studio vous guide dans le processus de création de votre premier groupe de mise à disposition. Plus tard, vous pourrez modifier le catalogue que vous avez créé et créer des catalogues supplémentaires.

Généralités

Lorsque vous créez un catalogue de machines qui contient des VM, vous devez spécifier la manière dont les VM vont être provisionnées : vous pouvez utiliser les outils pris en charge par Studio, comme Machine Creation Services (MCS) ou Provisioning Services, ou vous pouvez utiliser vos propres outils pour fournir des machines. Si vos machines sont déjà fournies pour vous (et vous n'avez pas besoin d'utiliser d'images principales), vous devez quand même créer un ou plusieurs catalogues pour vos machines.

- Si vous utilisez Provisioning Services pour créer des machines, consultez la documentation Provisioning Services pour obtenir des instructions.
- Si vous choisissez MCS pour provisionner des VM, vous devez fournir une image principale (ou un instantané) comme guide pour créer des machines virtuelles identiques dans le catalogue. Avant de créer le catalogue, vous devez utiliser des outils sur votre hyperviseur ou service de cloud pour créer et configurer l'image principale : cela comprend l'installation d'un Virtual Delivery Agent (VDA) sur l'image. Ensuite, lorsque vous créez le catalogue de machines dans Studio, vous sélectionnez cette image (ou un instantané de cette image), spécifiez le nombre de machines virtuelles à créer dans le catalogue et configurez les informations supplémentaires.

Lorsque vous utilisez MCS ou PVS pour créer votre premier catalogue de machines, vous pouvez utiliser la connexion hôte que vous avez configurée lors de la création du site. Plus tard (après avoir créé votre premier catalogue de machines et groupe de mise à disposition), vous pouvez modifier les informations concernant cette connexion ou créer d'autres connexions.

Une fois que vous avez créé un catalogue de machines à l'aide de l'assistant, des tests sont exécutés automatiquement pour vous assurer qu'il est correctement configuré. Lorsque les tests sont terminés, vous pouvez afficher un rapport de test. Vous pouvez exécuter les tests à tout moment ultérieurement à partir de **Citrix Studio** *nom-site* dans le volet de navigation de Studio.

Conseil : si vous créez un catalogue directement à l'aide du SDK du PowerShell, plutôt que dans Studio, vous pouvez spécifier un modèle d'hyperviseur (VMTemplates), comme alternative à une image ou un instantané de l'image.

Si vous possédez des machines Windows XP ou Windows Vista, vous devez utiliser une version antérieure de VDA, et elles ne pourront pas utiliser les dernières fonctionnalités des produits. Si vous ne pouvez pas mettre à niveau ces machines vers une version de système d'exploitation Windows prise en charge, Citrix vous recommande de les conserver dans un catalogue de machines distinct.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Vous trouverez ci-après une brève présentation des actions MCS à exécuter après avoir fourni les informations dans l'assistant Créer un catalogue de machines.

- Si vous avez sélectionné une image principale (plutôt qu'un instantané) dans l'assistant, MCS crée un instantané.
- MCS crée une copie complète de l'instantané et la place sur chaque emplacement de stockage défini dans la connexion hôte.
- MCS ajoute les bureaux à Active Directory, qui crée des identités uniques.
- MCS crée le nombre de VM spécifiées dans l'assistant, avec deux disques pour chaque VM. Outre les deux disques par VM, une image principale est également stockée dans le même emplacement de stockage. Si vous avez défini plusieurs emplacements de stockage, chacun obtient les types de disque suivants :
  - La copie complète de l'instantané (mentionnée ci-dessus), qui est en lecture seule et partagée entre les VM qui viennent d'être créées.
  - Un disque d'identité 16 Mo unique qui attribue à chaque VM une identité unique. Chaque VM dispose d'un disque d'identité.
  - Un disque de différence unique pour stocker les écritures effectuées sur la VM. Ce disque est provisionné par allocation dynamique (si elle est prise en charge par le stockage hôte) et augmente la taille maximale de l'image principale, si nécessaire. Chaque VM dispose d'un disque de différence. Il s'agit du disque qui contient les modifications effectuées lors des sessions - il est permanent pour les bureaux dédiés ; pour les bureaux regroupés, il est supprimé et un nouveau est créé après chaque redémarrage.

Préparer une image principale sur l'hyperviseur ou le service de cloud

Conseil : pour de plus amples informations sur la création de connexions à des hyperviseurs et à des fournisseurs de cloud, consultez l'article Connexions et ressources.

L'image principale contient le système d'exploitation, les applications non virtualisées, le VDA, et d'autres logiciels.

À savoir :

- Une image principale peut également être appelée image clone, image principale, VM de base ou image de base. Les fournisseurs d'hôte et les fournisseurs de service cloud peuvent utiliser des termes différents.
- Lors de l'utilisation de Provisioning Services, vous pouvez utiliser une image principale ou un ordinateur physique comme machine cible principale. Provisioning Services utilise une terminologie différente de MCS pour faire référence aux images ; consultez la documentation pour plus de détails.
- Assurez-vous que l'hôte est doté de suffisamment de processeurs, de mémoire et de stockage pour prendre en charge le nombre de machines que vous envisagez de créer.
- Configurez la quantité d'espace disque nécessaire pour les bureaux et les applications, car cette valeur ne peut pas être modifiée ultérieurement ou dans le catalogue.
- Les catalogues de machines Remote PC Access ne requièrent pas d'images principales.
- Considérations liées à l'activation de Microsoft KMS lors de l'utilisation de MCS : si votre déploiement comprend un VDA 7.x avec XenServer 6.1 ou 6.2, vSphere ou hôte Microsoft System Center Virtual Machine Manager, vous n'avez pas à réarmer manuellement Microsoft Windows ou Microsoft Office. Si votre déploiement comprend un VDA 5.x avec un hôte XenServer 6.0.2, consultez l'article CTX128580.
- Installez et configurez le logiciel suivant sur l'image principale :
  - Intégration des outils pour votre hyperviseur (tels que les outils XenServer, Services d'intégration Hyper-V ou outils

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VMware). Si vous ignorez cette étape, vos applications et bureaux risquent de ne pas fonctionner correctement.

- Un VDA : Citrix recommande d'installer la version la plus récente pour autoriser l'accès aux dernières fonctionnalités. Si vous ne parvenez pas à installer un VDA sur l'image principale, la création du catalogue échoue.
- Outils tiers en fonction de vos besoins, tels que le logiciel antivirus ou les agents électroniques de distribution de logiciels. Configurez les services avec les paramètres appropriés pour vos utilisateurs et le type de machine (tels que la mise à jour des fonctionnalités).
- Les applications tierces qui ne sont pas virtualisées. Citrix recommande de virtualiser les applications, car cela réduit de manière significative les coûts en éliminant le besoin de mettre à jour l'image principale après l'ajout ou la reconfiguration d'une application. En outre, moins d'applications installées réduisent la taille des disques durs de l'image principale, ce qui économise les coûts de stockage.
- Les clients App-V avec les paramètres recommandés, si vous souhaitez publier des applications App-V. Le client App-V est disponible auprès de Microsoft.
- Lors de l'utilisation de MCS, et vous permet de localiser Microsoft Windows, installez les paramètres régionaux et les packs de langue. Lors du provisioning, lorsqu'un instantané est créé, les VM provisionnées utilisent les variables locales installées et les packs de langue.

Important : si vous utilisez Provisioning Services ou MCS, n'exécutez pas Sysprep sur les images principales.

Pour préparer une image principale :

1. À l'aide de l'outil de gestion de votre hyperviseur, créez une nouvelle image principale, puis installez le système d'exploitation, ainsi que tous les service packs et mises à jour. Spécifiez le nombre d'UC virtuelles (vous pouvez également spécifier cette valeur lorsque vous créez le catalogue de machines, mais uniquement à l'aide de PowerShell ; vous ne pouvez pas spécifier le nombre d'UC virtuelles dans l'interface utilisateur de Studio lors de la création d'un catalogue de machines). Assurez-vous de configurer la quantité d'espace disque nécessaire pour les bureaux et les applications, car cette valeur ne peut pas être modifiée ultérieurement ou dans le catalogue de machines.
2. Assurez-vous que le disque dur de votre ordinateur est connecté à l'emplacement de périphérique 0. La plupart des modèles d'image principale standard configurent cet emplacement par défaut, mais ce n'est peut-être pas le cas de certains modèles personnalisés.
3. Installez et configurez les logiciels répertoriés ci-dessus sur l'image principale :
4. Lors de l'utilisation de Provisioning Services, créez un fichier VHD pour le vDisk à partir de votre machine cible principale avant de joindre la machine cible principale à un domaine. Pour plus d'informations, veuillez consulter la documentation relative à Provisioning Services.
5. Joignez l'image principale au domaine dans lequel les applications et les bureaux seront membres, et assurez-vous que l'image principale est disponible sur l'hôte sur lequel les machines seront créées. Veuillez noter que l'association de l'image principale à un domaine n'est pas nécessaire si vous utilisez MCS : les machines provisionnées sont membres du domaine spécifié dans l'assistant Créer un catalogue de machines.
6. Citrix vous recommande de créer et de nommer un instantané de l'image principale afin qu'il puisse être identifié. Si vous spécifiez une image principale plutôt qu'un instantané lors de la création d'un catalogue de machines, Studio crée un instantané, mais vous ne pouvez pas le renommer.

Lorsque vous utilisez XenServer pour votre infrastructure d'hébergement, les machines compatibles GPU requièrent une image principale dédiée. Ces VM requièrent des lecteurs de carte vidéo qui prennent en charge les processeurs graphiques et qui doivent être configurés de manière à permettre à la VM de fonctionner avec des logiciels qui utilisent le processeur graphique pour les opérations.

1. Dans XenCenter, créez une VM avec un VGA, des réseaux et un processeur virtuel standard.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Mettez à jour la configuration de la VM pour activer l'utilisation du GPU (Passthough ou vGPU).
3. Installez un système d'exploitation pris en charge et activez RDP.
4. Installez XenServer Tools et les pilotes NVIDIA.
5. Désactiver la console Administrateur VNC (Virtual Network Computing) pour optimiser les performances, puis redémarrez la VM.
6. Vous êtes invité à utiliser le logiciel RDP (Connexion Bureau à distance). À l'aide de RDP, installez le VDA, puis redémarrez la machine virtuelle.
7. Si vous le souhaitez, vous pouvez créer un instantané de la VM en tant que modèle de la ligne de base pour d'autres images principales GPU.
8. À l'aide de RDP, installez des applications spécifiques au client qui sont configurées dans XenCenter et utilisent les capacités de processeur graphique.

Créer un catalogue de machines à l'aide de Studio

Avant de démarrer l'Assistant de création du catalogue de machines, consultez cette section pour en savoir plus sur le choix que vous effectuerez et les informations que vous devez fournir. Lorsque vous démarrez l'assistant, certaines des pages décrites ci-dessous peuvent ne pas s'afficher ou elles peuvent avoir des titres différents, en fonction de votre environnement et des choix que vous effectuez.

Important : si vous utilisez une image principale, assurez-vous que vous avez installé un VDA sur l'image avant de créer le catalogue de machines.

À partir de Studio :

- si vous avez créé un site, mais n'avez pas encore créé un catalogue de machines, Studio vous guidera au bon emplacement de départ pour créer un catalogue de machines.
- Si vous avez déjà créé un catalogue de machines et souhaitez en créer un autre, sélectionnez **Catalogues de machines** dans le volet de navigation Studio, puis sélectionnez **Créer un catalogue de machines** dans le volet Actions.

L'Assistant va vous guider au travers des éléments ci-dessous. Les pages de l'assistant qui s'affichent peuvent être différentes selon les sélections que vous effectuez.

Chaque catalogue contient des machines d'un seul type :

- **OS de serveur :** un catalogue avec OS de serveur fournit des bureaux et des applications qui peuvent être partagés par de multiples utilisateurs. Les machines peuvent exécuter des versions prises en charge des systèmes d'exploitation Windows ou Linux, mais le catalogue ne peut pas contenir les deux.
- **OS de bureau :** un catalogue avec OS de bureau fournit des bureaux et des applications qui sont affectés à différents utilisateurs.
- **Remote PC Access :** un catalogue Remote PC Access permet aux utilisateurs d'accéder à distance à leurs machines de bureau de bureau physique. Remote PC Access ne requiert pas de VPN pour fournir la sécurité.

La page **Gestion des machines** indique la manière dont les machines sont gérées et l'outil que vous utiliserez pour déployer les machines.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Indiquez si la gestion de l'alimentation des machines du catalogue sera effectuée au travers de Studio.

- Machines dont la gestion de l'alimentation est effectuée au travers de Studio ou provisionnées via un environnement de cloud, des VM ou des PC lames par exemple. Cette option est disponible uniquement si vous disposez d'une connexion à un hyperviseur ou un service de cloud déjà configuré.
- La gestion de l'alimentation des machines n'est pas effectuée au travers de Studio, les machines physiques par exemple.

Si vous avez indiqué que l'alimentation des machines est gérée au travers de Studio ou que les machines sont provisionnées via un environnement de cloud, choisissez l'outil que vous utiliserez pour déployer les machines.

- **Machine Creation Services (MCS)** : utilise une image principale pour créer et gérer les machines virtuelles. Les catalogues de machine dans les environnements de cloud utilisent MCS. MCS n'est pas disponible pour les machines physiques.
- **Provisioning Services** : vous permet de gérer des machines cibles en tant que collection de machines. Une image vDisk Provisioning Services créée à partir d'une machine cible principale permet de mettre à disposition des bureaux et des applications. Cette option n'est pas disponible pour les déploiements de cloud.
- **Autres** : un outil qui permet de gérer les machines se trouvant déjà dans le centre de données. Citrix vous recommande d'utiliser Microsoft System Center Configuration Manager ou une autre application tierce pour vous assurer que les machines du catalogue sont cohérentes.

La page **Expérience de bureau** (qui s'affiche uniquement lors de la création d'un catalogue de machines contenant des machines avec OS de bureau) détermine le type de bureaux qui seront créés. Les types diffèrent selon qu'ils sont attribués ou non à un utilisateur, et ce qui arrive aux modifications effectuées par l'utilisateur lorsque la machine redémarre.

Il existe trois types :

- **Regroupement aléatoire** : les bureaux sont affectés de façon aléatoire, les utilisateurs se connectent à un nouveau bureau (aléatoire) chaque fois qu'ils ouvrent une session. Lorsqu'un utilisateur ferme sa session, le bureau devient disponible pour un autre utilisateur. Lorsque le bureau est redémarré, les modifications effectuées sont supprimées.
- **Regroupement statique** : les bureaux sont affectés de façon permanente, les utilisateurs se connectent au même bureau (statique) chaque fois qu'ils ouvrent une session. Lorsqu'un utilisateur ferme sa session, le bureau reste disponible pour cet utilisateur uniquement. Lorsque le bureau est redémarré, les modifications effectuées sont supprimées.
- **Bureaux dédiés** : les bureaux sont attribués de façon permanente à un utilisateur. Lorsqu'un utilisateur ferme sa session, le bureau reste disponible pour cet utilisateur uniquement. Lorsque le bureau est redémarré, les modifications effectuées sont conservées. Vous pouvez enregistrer les modifications sur un disque de VM local ou sur une lettre de lecteur spécifiée sur un Personal vDisk distinct.

Sélectionnez la connexion à l'hyperviseur ou au service de cloud hôte, puis sélectionnez la machine virtuelle ou l'instantané créé(e) précédemment. Si vous créez le premier catalogue de machines, la seule connexion disponible est celle que vous avez configurée lors de la création du site.

Rappel :

- Si vous utilisez Provisioning Services ou MCS, n'exécutez pas Sysprep sur les images principales.
- Si vous spécifiez une image principale plutôt qu'un instantané, Studio crée un instantané, mais vous ne pouvez pas le renommer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour vous assurer que vous pouvez utiliser les dernières fonctionnalités des produits, assurez-vous que la dernière version de VDA est installée sur l'image principale. Ne modifiez pas la valeur par défaut de **Sélectionnez la version de VDA installée** sur la page de l'assistant.

Un message d'erreur s'affiche si vous sélectionnez un instantané ou une VM qui n'est pas compatible avec la technologie de gestion de machines que vous avez sélectionnée précédemment dans l'assistant.

Sélectionnez un ou plusieurs groupes de sécurité pour les machines virtuelles ; ils sont affichés uniquement si la zone de disponibilité prend en charge les groupes de sécurité.

Indiquez si les machines utiliseront le matériel partagé ou le matériel de compte dédié.

Le titre de cette page dépend de la méthode de déploiement que vous avez choisie sur la page **Gestion des machines**.

- Si vous avez choisi MCS, le titre de cette page est **Machines virtuelles**.
- Si vous avez choisi Provisioning Services, le titre de cette page est **Collection de périphériques**.
- Si vous avez choisi d'autres outils, le titre de cette page est **VM et utilisateurs**.

Sur cette page :

- Spécifiez le nombre de machines virtuelles à créer.
- Choisissez la quantité de mémoire (Mo) pour chaque machine.
- Si vous avez indiqué sur la page **Expérience de bureau** que les modifications apportées par l'utilisateur aux bureaux dédiés doivent être enregistrées sur un Personal vDisk distinct, spécifiez la taille de vDisk en gigaoctets et la lettre de lecteur.
- Si votre déploiement contient plusieurs zones, vous pouvez sélectionner une zone pour le catalogue.
- Si vous utilisez MCS pour déployer des machines et que vous créez des VM regroupées au hasard qui n'utilisent pas de Personal vDisks, vous pouvez configurer un cache à utiliser pour les données temporaires sur chaque machine. Pour plus de détails, consultez la section suivante.

Important : chaque machine virtuelle doit disposer d'un disque dur. Leur taille est définie dans l'image principale ; vous ne pouvez pas modifier la taille du disque dur dans le catalogue.

Configurer un cache pour les données temporaires

La mise en cache locale des données temporaires sur la VM est facultative. Vous pouvez activer le stockage des données temporaires sur le cache de la machine lorsque vous utilisez MCS pour gérer les machines regroupées (non dédiées) dans un catalogue. Si le catalogue utilise une connexion qui spécifie un stockage des données temporaires, vous pouvez activer et configurer les informations de mise en cache des données temporaires lorsque vous créez le catalogue.

Pour activer la mise en cache des données temporaires, le VDA de chaque machine dans le catalogue doit être à la version minimale 7.9.

Vous spécifiez si les données temporaires utilisent le stockage local ou partagé lorsque vous créez la connexion que le catalogue utilise ; pour de plus amples informations, veuillez consulter l'article Connexions et ressources. L'activation et la configuration du cache temporaire dans le catalogue contient deux cases à cocher : **Mémoire allouée au cache (Mo)** et **Taille du cache disque (Go)**. Les valeurs par défaut diffèrent selon le type de connexion. En général, les valeurs par défaut

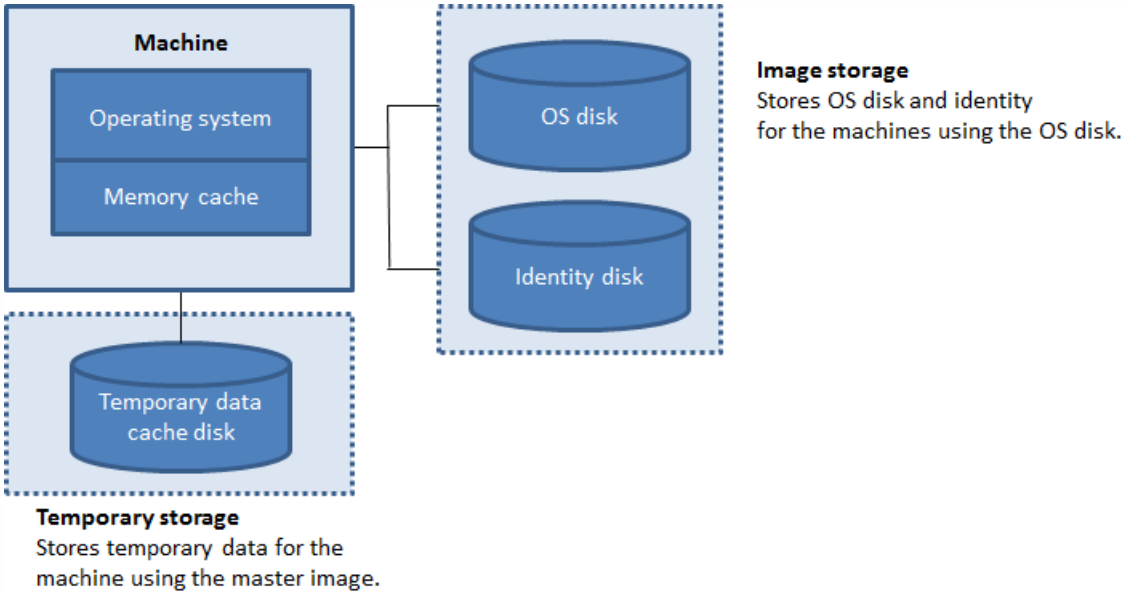
© 1999-2017 Citrix Systems, Inc. All rights reserved.

suffisent à la plupart des cas, cependant, tenez compte de l'espace nécessaire pour les :

- Fichiers de données temporaires créés par Windows, y compris le fichier de pages Windows.
- Données du profil utilisateur.
- Données ShareFile qui sont synchronisées sur les sessions des utilisateurs.
- Données qui peuvent être créées ou copiées par un utilisateur de session ou toute application que les utilisateurs peuvent installer dans la session.

Windows n'autorisera pas une session à utiliser une quantité de cache disque plus importante que la quantité d'espace disponible sur l'image principale originale à partir de laquelle les machines dans le catalogue de machines sont provisionnées. Par exemple, il n'existe aucun avantage à spécifier un disque de cache de 20 Go s'il existe uniquement 10 Go d'espace disponible sur l'image principale.

Si vous activez la case à cocher **Taille du cache disque**, les données temporaires sont initialement écrites dans la mémoire cache. Lorsque la mémoire cache atteint sa limite configurée (valeur **Mémoire allouée au cache**), les données les plus anciennes sont déplacées sur le disque de mise en cache des données temporaires.



La mémoire cache est prise en compte dans le calcul de la quantité totale de mémoire sur chaque machine ; par conséquent, si vous activez la case **Mémoire allouée au cache**, envisagez d'augmenter la quantité totale de mémoire sur chaque machine.

Si vous désactivez la case **Mémoire allouée au cache** et laissez la case **Taille du cache disque** activée, les données temporaires sont écrites directement sur le disque cache, ce qui utilise une quantité minimale de la mémoire cache.

La modification de la valeur par défaut **Taille du cache disque** peut affecter les performances. La taille doit correspondre aux besoins des utilisateurs et à la charge de travail placée sur la machine.

Important : si le cache disque vient à manquer d'espace, la session de l'utilisateur devient inutilisable.

Si vous désactivez la case **Taille du cache disque**, aucun disque cache n'est créé. Dans ce cas, spécifiez une valeur de **Mémoire allouée au cache** suffisante pour stocker toutes les données temporaires ; cela est uniquement possible si d'importantes quantités de RAM sont disponibles pour allocation à chaque machine virtuelle.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si vous désactivez ces deux cases à cocher, les données temporaires ne sont pas mises en cache ; elles sont écrites sur le disque de différence (situé dans l'espace de stockage du système d'exploitation) pour chaque machine virtuelle. (Il s'agit de l'action de provisioning dans les versions antérieures à la version 7.9).

La mise en cache ne doit pas être activée si vous avez l'intention d'utiliser ce catalogue pour créer des AppDisks.

Vous ne pouvez pas modifier les valeurs de cache dans un catalogue de machines après sa création.

Si vous prévoyez d'utiliser plusieurs cartes d'interface réseau, vous devez associer un réseau virtuel avec chaque carte. Par exemple, vous pouvez attribuer une carte pour accéder à un réseau sécurisé spécifique, et une autre carte pour accéder à un réseau plus courant. Vous pouvez également ajouter ou supprimer les cartes d'interface réseau à partir de cette page.

(Valide uniquement pour Catalogues Remote PC Access) Spécifiez les comptes de machines Active Directory ou des unités d'organisation (OU) à ajouter qui correspondent à des utilisateurs ou des groupes d'utilisateurs. N'utilisez pas de barre oblique (/) dans un nom d'unité d'organisation.

Vous pouvez choisir une connexion de gestion de l'alimentation configurée précédemment ou choisir de ne pas utiliser la gestion de l'alimentation. Si vous souhaitez utiliser la gestion de l'alimentation, mais une connexion adéquate n'a pas encore été configurée, vous pouvez créer cette connexion plus tard, puis modifiez le catalogue de machines pour mettre à jour les paramètres de gestion de l'alimentation.

Chaque machine du catalogue de machines a besoin d'un compte d'ordinateur Active Directory correspondant. Indiquez s'il faut créer de nouveaux comptes ou utiliser des comptes existants, ainsi que l'emplacement de ces comptes.

- Si vous créez de nouveaux comptes, vous devez disposer de l'accès à un compte d'administrateur de domaine pour le domaine dans lequel les machines se trouvent.

  Spécifiez le schéma d'affectation de nom du compte pour les machines qui seront créées, en utilisant des marques de hachage pour indiquer l'emplacement où les lettres ou chiffres séquentiels apparaîtront. N'utilisez pas de barre oblique (/) dans un nom d'unité d'organisation. Un nom ne peut pas commencer par un chiffre. Par exemple, un principe de dénomination de PC-Sales-##(0-9) sélectionnés dans les comptes d'ordinateur nommés PC-Sales-01, PC-Sales-02, PC-Sales-03, etc.

- Si vous utilisez des comptes existants, vous pouvez sélectionner les comptes ou cliquez sur Importer et spécifiez un fichier .csv contenant les noms de compte. Le contenu du fichier importé doit utiliser le format :

  [ADComputerAccount]
  ADcomputeraccountname.domain

  ...

  Assurez-vous qu'il existe suffisamment de comptes pour toutes les machines que vous ajoutez. Étant donné que Studio gère ces comptes, soit autorisez Studio à réinitialiser les mots de passe de tous les comptes soit spécifiez le mot de passe de compte, qui doit être le même pour tous les comptes.

Pour les catalogues contenant des machines physiques ou des machines existantes, sélectionnez ou importez des comptes

© 1999-2017 Citrix Systems, Inc. All rights reserved.

existants et attribuez chaque machine à un compte d'ordinateur Active Directory et à un compte d'utilisateur.

Pour les machines créées avec Provisioning Services, les comptes d'ordinateur pour les machines cibles sont gérés différemment ; consultez la documentation Provisioning Services.

Sur la page **Résumé** de l'assistant, vérifiez les paramètres que vous avez spécifiés. Entrez un nom et une description pour le catalogue ; les informations suivantes s'affichent dans Studio.

Une fois que vous avez vérifié les informations que vous avez spécifiées, cliquez sur **Terminer** pour lancer la création du catalogue.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Gérer les catalogues de machines

Jul 07, 2016

Dans cet article :

- Introduction
- Ajouter des machines à un catalogue de machines
- Supprimer des machines d'un catalogue de machines
- Modifier la description d'un catalogue de machines ou modifier les paramètres Remote PC Access
- Renommer un catalogue de machines
- Déplacer un catalogue de machines vers une autre zone
- Supprimer un catalogue de machines
- Gérer les comptes d'ordinateurs Active Directory dans un catalogue de machines
- Mettre un catalogue de machines à jour
- Mettre un catalogue de machines à niveau

Introduction

Vous pouvez ajouter ou supprimer des machines dans un catalogue de machines, renommer, modifier la description ou gérer les comptes d'ordinateurs Active Directory d'un catalogue.

La gestion des catalogues peut également consister à s'assurer que chaque machine dispose des mises à jour de système d'exploitation, des mises à jour des logiciels antivirus, des mises à niveau de système d'exploitation ou des modifications apportées à la configuration les plus récentes.

- Pour les catalogues de machines contenant des machines regroupées au hasard créées à l'aide de Machine Creation Services (MCS), vous pouvez gérer les machines en mettant à jour l'image principale utilisée dans le catalogue, puis en mettant à jour les machines. Cela vous permet de mettre à jour de manière efficace un grand nombre de machines utilisateur. Pour les machines créées par le biais de Provisioning services, les mises à jour des machines sont propagées via le vDisk. Pour plus d'informations, veuillez consulter la documentation relative à Provisioning Services.
- Pour les catalogues contenant des machines Remote PC Access et statiques, vous devez gérer les mises à jour des machines des utilisateurs en dehors de Studio, soit individuellement soit collectivement à l'aide d'outils de distribution de logiciels tiers.

Pour de plus amples informations sur la création et la gestion de connexions à des hyperviseurs hôtes et à des services de cloud, consultez l'article Connexions et ressources.

Ajouter des machines à un catalogue de machines

Avant de commencer :

- Assurez-vous que l'ordinateur hôte de virtualisation ((hyperviseur ou fournisseur de service cloud) dispose de suffisamment de processeurs, de mémoire et de stockage pour prendre en charge les machines supplémentaires.
- Vérifiez que vous disposez de suffisamment de comptes d'ordinateurs Active Directory inutilisés. Si vous utilisez des comptes existants, le nombre de machines que vous pouvez ajouter est limité par le nombre de comptes disponibles.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Si vous utilisez Studio pour créer des comptes d'ordinateurs Active Directory pour les machines supplémentaires, vous devez disposer des droits d'administrateur de domaine.

Pour ajouter des machines à un catalogue :

1. Sélectionnez les **catalogues de machines** dans le volet de navigation Studio.
2. Sélectionnez un catalogue de machines, puis sélectionnez **Ajouter des machines** dans le volet Actions.
3. Sélectionnez le nombre de machines virtuelles à ajouter.
4. S'il n'y a pas suffisamment de comptes Active Directory pour le nombre de machines virtuelles que vous ajoutez, sélectionnez le domaine et l'emplacement où les comptes seront créés. Spécifiez un schéma d'affectation de nom du compte, à l'aide des marques de hachage pour indiquer l'emplacement où les numéros séquentiels ou les lettres apparaîtront. N'utilisez pas de barre oblique (/) dans un nom d'unité d'organisation. Un nom ne peut pas commencer par un chiffre. Par exemple, un principe de dénomination de PC-Sales-##(0-9) sélectionnés dans les comptes d'ordinateur nommés PC-Sales-01, PC-Sales-02, PC-Sales-03, etc.
5. Si vous utilisez des comptes Active Directory existants, vous pouvez sélectionner les comptes ou cliquer sur **Importer** et spécifier un fichier .csv contenant les noms de compte. Assurez-vous qu'il existe suffisamment de comptes pour toutes les machines que vous ajoutez. Étant donné que Studio gère ces comptes, soit autorisez Studio à réinitialiser les mots de passe de tous les comptes soit spécifiez le mot de passe de compte (qui doit être le même pour tous les comptes).

Les machines sont créées en tant que processus en arrière-plan, qui peut être très long lors de la création d'un grand nombre de machines. La création de la machine se poursuit même si vous fermez Studio.

Supprimer des machines d'un catalogue de machines

Lorsque vous supprimez une machine d'un catalogue de machines, les utilisateurs ne peuvent plus y accéder ; donc, avant de supprimer une machine, assurez-vous que :

- Les données utilisateur sont sauvegardées ou ne sont plus nécessaires.
- Tous les utilisateurs sont déconnectés. L'activation du mode maintenance va empêcher les nouvelles connexions à une machine.
- Les machines sont hors tension.

Pour supprimer des machines d'un catalogue :

1. Sélectionnez **Catalogues de machines** dans le volet de navigation Studio.
2. Sélectionner un catalogue, puis sélectionnez **Afficher les machines** dans le volet Actions.
3. Sélectionnez une ou plusieurs machines, puis sélectionnez **Supprimer** dans le volet Actions.

Choisissez si vous souhaitez supprimer les machines en cours de suppression. Si vous choisissez de supprimer les machines, indiquez si les comptes Active Directory pour ces machines doivent être conservés, désactivés ou supprimés.

Modifier la description d'un catalogue de machines ou modifier les paramètres Remote PC Access

1. Sélectionnez les **catalogues de machines** dans le volet de navigation Studio.
2. Sélectionnez un catalogue, puis sélectionnez **Modifier le catalogue de machines** dans le volet Actions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. (Catalogues Remote PC Access uniquement) Sur la page **Gestion de l'alimentation**, vous pouvez modifier les paramètres de gestion de l'alimentation et sélectionner une connexion de gestion de l'alimentation. Sur la page **Unités d'organisation**, ajoutez ou supprimez des unités d'organisation Active Directory.
4. Sur la page **Description**, modifiez la description du catalogue.

Renommer un catalogue de machines

1. Sélectionnez les **catalogues de machines** dans le volet de navigation Studio.
2. Sélectionnez un catalogue, puis sélectionnez **Renommer le catalogue de machines** dans le volet Actions.
3. Entrez le nouveau nom.

Déplacer un catalogue de machines vers une autre zone

Si votre site contient plusieurs zones, vous pouvez déplacer un catalogue d'une zone vers une autre.

Avertissement : le déplacement d'un catalogue vers une zone autre que l'hyperviseur ou le service de cloud contenant les VM de ce catalogue peut affecter les performances.

1. Sélectionnez les **catalogues de machines** dans le volet de navigation Studio.
2. Sélectionnez un catalogue, puis sélectionnez **Déplacer** dans le volet Actions.
3. Sélectionnez la zone vers laquelle vous souhaitez déplacer le catalogue.

Supprimer un catalogue de machines

Avant de supprimer un catalogue de machines, assurez-vous que :

- Tous les utilisateurs ont fermé leur session et qu'aucune session déconnectée n'est en cours d'exécution.
- Le mode de maintenance est activé pour toutes les machines du catalogue, de sorte qu'il ne soit pas possible d'effectuer de nouvelles connexions.
- Toutes les machines des catalogues sont hors tension.
- Le catalogue n'est pas associé à un groupe de mise à disposition ; en d'autres termes, le groupe de mise à disposition ne contient pas les machines du catalogue.

Pour supprimer un catalogue de machines :

1. Sélectionnez les **catalogues de machines** dans le volet de navigation Studio.
2. Sélectionnez un catalogue, puis sélectionnez **Supprimer le catalogue de machines** dans le volet Actions.
3. Indiquez si les machines du catalogue doivent être supprimées. Si vous choisissez de supprimer les machines, indiquez si les comptes d'ordinateur Active Directory pour ces machines doivent être conservés, désactivés ou supprimés.

Gérer les comptes d'ordinateurs Active Directory dans

© 1999-2017 Citrix Systems, Inc. All rights reserved.

un catalogue de machines

Pour gérer les comptes Active Directory dans un catalogue de machines, vous pouvez :

- Libérer des comptes de machines non utilisés en supprimant les comptes d'ordinateurs Active Directory des catalogues de machines avec OS de bureau et avec OS de serveur. Ces comptes peuvent ensuite être utilisés pour d'autres machines.
- Ajoutez des comptes de façon à ce que lorsque plus de machines sont ajoutées au catalogue, les comptes d'ordinateurs soient déjà en place. N'utilisez pas de barre oblique (/) dans un nom d'unité d'organisation.

Pour gérer les comptes Active Directory :

1. Sélectionnez les **catalogues de machines** dans le volet de navigation Studio.
2. Sélectionnez un catalogue, puis sélectionnez **Gérer les comptes AD** dans le volet Actions.
3. Choisissez si vous souhaitez ajouter ou supprimer des comptes d'ordinateurs. Si vous ajoutez des comptes, indiquez la marche à suivre avec les mots de passe de compte : les réinitialiser ou entrer un mot de passe qui s'applique à tous les comptes. Vous pouvez réinitialiser les mots de passe si vous ne connaissez pas les mots de passe de compte actuels, vous devez avoir l'autorisation d'effectuer une réinitialisation du mot de passe. Si vous entrez un mot de passe, le mot de passe sera modifié sur les comptes lors de leur importation. Si vous supprimez un compte, indiquez si le compte dans Active Directory doit être conservé, désactivé ou supprimé.

Remarque : vous pouvez également indiquer si les comptes Active Directory doivent être conservés, désactivés ou supprimés lorsque vous supprimez les machines d'un catalogue ou supprimez un catalogue.

Mettre un catalogue de machines à jour

Citrix vous recommande de sauvegarder des copies ou des instantanés des images principales avant de mettre à jour les machines dans le catalogue. La base de données conserve un enregistrement historique des images principales utilisées avec chaque catalogue de machines. Vous pouvez restaurer un catalogue afin d'utiliser la version précédente de l'image principale si les utilisateurs rencontrent des problèmes avec les mises à jour que vous avez déployé sur leurs bureaux, ce qui permet de réduire les temps d'arrêt des utilisateurs. Ne supprimez, déplacez ou renommez pas les images principales ; sinon, vous ne pourrez pas restaurer un catalogue pour les utiliser.

Pour les catalogues qui utilisent Provisioning Services, vous devez publier un nouveau vDisk pour appliquer les modifications au catalogue. Pour de plus amples informations, consultez la documentation Provisioning Services.

Après qu'une machine a été mise à jour, elle redémarre automatiquement.

Conseil : pour de plus amples informations sur la gestion de connexions, consultez l'article Connexions et ressources.

Avant de mettre à jour le catalogue de machines, mettez à jour une image principale existante ou créez une nouvelle image sur votre hyperviseur hôte.

1. Sur votre hyperviseur ou fournisseur de services de cloud, prenez un instantané de la VM et donnez à l'instantané un nom significatif. Cet instantané peut être utilisé pour rétablir (restaurer) des machines dans le catalogue, si nécessaire.
2. Si nécessaire, démarrez l'image principale et ouvrez une session.
3. Installez les mises à jour ou apportez les modifications requises à l'image principale.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. Si l'image principale utilise un Personal vDisk, mettez à jour l'inventaire.
5. Consultez ces guides d'optimisation de système d'exploitation et appliquez les optimisations pour votre environnement : Guide d'optimisation de Windows 7 et Guide d'optimisation de bureau virtuel Windows 8/8.1.
6. Arrêtez la VM.
7. Prenez un instantané de la VM, puis donnez à l'instantané un nom significatif qui sera reconnu lorsque le catalogue sera mis à jour dans Studio. Bien que Studio puisse créer un instantané, Citrix vous recommande de créer un instantané à l'aide de la console de gestion de l'hyperviseur, puis de sélectionner cet instantané dans Studio. Cette méthode vous permet de choisir un nom et une description significatifs plutôt qu'un nom généré automatiquement. Pour les images principales GPU, vous pouvez modifier l'image principale uniquement par le biais de la console XenCenter de XenServer.

Pour préparer et distribuer la mise à jour à toutes les machines d'un catalogue :

1. Sélectionnez les **catalogues de machines** dans le volet de navigation Studio.
2. Sélectionnez un catalogue, puis sélectionnez **Mettre à jour les machines** dans le volet Actions.
3. Sur la page **Image principale**, sélectionnez l'hôte et l'image que vous souhaitez déployer.
4. Sur la page **Stratégie de déploiement**, indiquez lorsque les machines du catalogue de machines doivent être mises à jour avec la nouvelle image principale : lors de la prochaine fermeture de session ou immédiatement. Consultez la section ci-dessous pour plus de détails.
5. Vérifiez les informations dans la page **Résumé** et cliquez sur **Terminer**. Chaque machine redémarre automatiquement après sa mise à jour.

Conseil : si vous mettez à jour un catalogue directement à l'aide du SDK du PowerShell, plutôt que dans Studio, vous pouvez spécifier un modèle d'hyperviseur (VMTemplates), comme alternative à une image ou un instantané de l'image.

Stratégie de déploiement

La mise à jour de l'image lors de la prochaine fermeture de session est effectuée lorsque vous utilisez Citrix Connector pour System Center Configuration Manager.

Si vous choisissez de mettre à jour l'image immédiatement, configurez une heure de distribution et des notifications.

- **Heure de distribution :** vous pouvez choisir de mettre à jour toutes les machines en même temps, ou spécifier le délai nécessaire pour commencer la mise à jour de toutes les machines dans le catalogue. Un algorithme interne détermine le moment où chaque machine est mise à jour et redémarrée pendant cet intervalle.
- **Notification :** dans la liste déroulante de notification de gauche, indiquez si un message de notification doit s'afficher sur les machines avant qu'une mise à jour commence. Par défaut, aucun message ne s'affiche. Si vous choisissez d'afficher un message 15 minutes avant que la mise à jour commence, vous pouvez choisir (dans la liste déroulante de droite) de répéter le message toutes les cinq minutes après le premier message. Par défaut, le message n'est pas répété. Si vous choisissez de mettre à jour toutes les machines en même temps, le message de notification s'affiche sur chaque machine à l'heure appropriée avant que la mise à jour ne commence, calculée par un algorithme interne.

Après avoir déployé une image principale mise à jour/nouvelle, vous pouvez la restaurer. Cette opération peut être nécessaire si des problèmes se produisent avec les machines mises à jour. Lors de la restauration, les machines du catalogue reviennent à la dernière image fonctionnelle. Les nouvelles fonctionnalités qui nécessitent la nouvelle image ne seront plus disponibles. Comme avec le déploiement, restaurer une machine implique un redémarrage.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Sélectionnez **Catalogues de machines** dans le volet de navigation Studio.
2. Sélectionnez le catalogue, puis sélectionnez **Restaurer la mise à jour de la machine** dans le volet Actions.
3. Spécifiez quand appliquer la version antérieure de l'image principale aux machines, comme décrit ci-dessus pour l'opération de déploiement.

La restauration n'est appliquée qu'aux machines qui doivent être rétablies. Pour les machines qui n'ont pas été mises à jour avec l'image principale nouvelle ou mise à jour (par exemple, des machines avec des utilisateurs qui n'ont pas fermé leur session), les utilisateurs ne reçoivent pas de messages de notification et ne sont pas forcés de fermer la session.

Mettre à niveau un catalogue de machines ou rétablir une mise à niveau

Mettez à niveau le catalogue de machine après avoir mis à niveau les VDA sur les machines vers une version plus récente. Citrix recommande de mettre à niveau tous les VDA vers la version la plus récente de façon à ce qu'ils puissent tous accéder à toutes les fonctionnalités les plus récentes.

Avant de procéder à la mise à niveau d'un catalogue de machines :

- Si vous utilisez Provisioning Services, vous devez mettre à niveau la version du VDA dans la console Provisioning Services.
- Démarrez les machines mises à niveau afin qu'elles s'enregistrent auprès du Controller. Cela permet à Studio de déterminer si les machines du catalogue de machine doivent être mises à niveau.

Pour mettre à niveau un catalogue de machines :

1. Sélectionnez les **catalogues de machines** dans le volet de navigation Studio.
2. Sélectionnez le catalogue. L'onglet Détails dans le volet inférieur affiche les informations de version.
3. Sélectionnez **Mettre à niveau le catalogue**. Si Studio détecte que le catalogue de machines a besoin de procéder à la mise à niveau, il affiche un message. Suivez les invites. Si une ou plusieurs machines ne peut pas être mise à niveau, un message explique pourquoi. Citrix vous recommande de résoudre les problèmes de machine avant d'effectuer une mise à niveau du catalogue de machine pour vous assurer que toutes les machines fonctionnent correctement.

Une fois la mise à niveau du catalogue terminée, vous pouvez rétablir les machines vers leurs versions de VDA précédentes en sélectionnant le catalogue, puis en sélectionnant **Annuler** dans le volet Actions.

Remarque : si vous possédez des machines Windows XP ou Windows Vista, vous devez utiliser une version antérieure de VDA, et elles ne pourront pas utiliser les dernières fonctionnalités des produits. Si vous ne pouvez pas mettre à niveau ces machines vers un système d'exploitation Windows actuellement pris en charge, Citrix vous recommande de les conserver dans un catalogue distinct.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Créer des groupes de mise à disposition

Aug 22, 2016

Un groupe de mise à disposition est une collection de machines sélectionnées à partir d'un ou de plusieurs catalogues de machines. Le groupe de mise à disposition indique quels utilisateurs peuvent utiliser ces machines et les applications et/ou les bureaux à la disposition des utilisateurs.

La création d'un groupe de mise à disposition est la prochaine étape de la configuration de votre déploiement après la création d'un site et la création d'un catalogue de machines. Plus tard, vous pourrez modifier les paramètres initiaux dans le premier groupe de mise à disposition et créer d'autres groupes de mise à disposition. Il existe également des fonctionnalités et paramètres que vous pouvez configurer uniquement lors de la modification d'un groupe de mise à disposition, et non pas lors de sa création.

Pour Remote PC Access, lorsque vous créez un site, un groupe de mise à disposition appelé **Bureaux Remote PC Access** est automatiquement créé.

Pour créer un groupe de mise à disposition :

1. si vous avez créé un site et un catalogue de machines, mais n'avez pas encore créé un groupe de mise à disposition, Studio vous guidera au bon emplacement de départ pour créer un groupe de mise à disposition. Si vous avez déjà créé un groupe de mise à disposition et souhaitez en créer un autre, sélectionnez **Groupes de mise à disposition** dans le volet de navigation Studio, puis sélectionnez **Créer un groupe de mise à disposition** dans le volet Actions.
2. L'assistant Créer un groupe de mise à disposition démarre sur une page **Introduction**, que vous pouvez supprimer des futurs démarrages de cet assistant.
3. L'assistant vous guide ensuite au travers des pages décrites ci-dessous. Lorsque vous avez terminé chaque page, cliquez sur **Suivant** jusqu'à la page finale.

Sélectionnez un catalogue de machines et sélectionnez le nombre de machines que vous souhaitez utiliser dans ce catalogue.

À savoir :

- Au moins une machine doit rester non utilisée dans un catalogue de machines sélectionné.
- Un catalogue de machines peut être spécifié dans plus d'un groupe de mise à disposition ; cependant, une machine ne peut être utilisée que dans un seul groupe de mise à disposition.
- Un groupe de mise à disposition peut utiliser des machines de plus d'un catalogue, cependant ces catalogues doivent contenir les mêmes types de machines (OS de serveur, OS de bureau ou Remote PC Access). En d'autres termes, vous ne pouvez pas combiner des types de machines dans un groupe de mise à disposition. De même, si votre déploiement possède des catalogues de machines Windows et des catalogues de machines Linux, un groupe de mise à disposition peut contenir des machines d'un des types de système d'exploitation, mais pas les deux.
- Citrix vous recommande d'installer ou de mettre à niveau les machines avec la dernière version de VDA, et de mettre à niveau les catalogues de machines et les groupes de mise à disposition en fonction de vos besoins. Lors de la création d'un groupe de mise à disposition, si vous sélectionnez des machines sur lesquelles sont installées différentes versions de VDA, le groupe de mise à disposition sera compatible avec la version de VDA la plus ancienne (il s'agit du *niveau fonctionnel* du groupe). Par exemple, si l'une des machines que vous sélectionnez dispose d'un VDA version 7.1 et que d'autres machines ont la version actuelle, toutes les machines du groupe peuvent uniquement utiliser les fonctionnalités

© 1999-2017 Citrix Systems, Inc. All rights reserved.

qui étaient prises en charge dans le VDA 7.1. Cela signifie que certaines fonctionnalités qui nécessitent des versions de VDA ultérieures risquent de ne pas être disponibles dans ce groupe de mise à disposition. Par exemple, pour utiliser la fonctionnalité AppDisks, les VDA (et par conséquent le niveau fonctionnel du groupe) doivent être à la version 7.8 au minimum.

- Chaque machine dans un catalogue de machines Remote PC Access est automatiquement associée à un groupe de mise à disposition ; lorsque vous créez un site Remote PC Access, un catalogue nommé **Machines Remote PC Access** et un groupe de mise à disposition appelé **Bureaux Remote PC Access** sont créés automatiquement.

Cette page s'affiche uniquement si vous avez choisi un catalogue de machines contenant des machines avec OS de bureau statiques (attribuées). Choisissez **Applications** ou **Bureaux** sur la page Type de mise à disposition ; vous ne pouvez pas activer les deux.

Si vous avez sélectionné des machines à partir d'un catalogue d'OS de serveur ou OS de bureau aléatoires (regroupés), le type de mise à disposition est applications et bureaux par défaut : vous pouvez mettre à disposition des applications, des bureaux, ou les deux.

Pour ajouter un AppDisk, cliquez sur **Ajouter**. La boîte de dialogue Sélectionner des AppDisks dresse la liste des AppDisks disponibles dans la colonne de gauche. La colonne de droite dresse la liste des applications sur le AppDisk (la sélection de l'onglet **Applications** au-dessus de la colonne de droite dresse la liste des applications dans un format similaire à un menu Démarrer ; la sélection de l'onglet **Packages installés** dresse la liste des applications dans un format similaire à la liste Programmes et fonctionnalités.).

Sélectionnez une ou plusieurs cases.

Pour plus d'informations, veuillez consulter l'article AppDisks.

Spécifiez les utilisateurs et les groupes d'utilisateurs qui peuvent utiliser les applications et les bureaux dans le groupe de mise à disposition.

Où les listes d'utilisateurs sont spécifiées

Les listes d'utilisateurs Active Directory sont spécifiées lorsque vous créez ou modifiez les informations suivantes :

- La liste d'accès utilisateur d'un site, qui n'est pas configurée dans Studio. Par défaut, la règle de stratégie d'admissibilité d'application inclut tout le monde ; consultez les applets de commande du kit de développement PowerShell BrokerAppEntitlementPolicyRule pour plus de détails.
- Les groupes d'applications (s'ils ont été configurés).
- Les groupes de mise à disposition.
- Les applications.

La liste des utilisateurs qui peuvent accéder à une application via StoreFront est constituée à partir de l'intersection des listes utilisateur ci-dessus. Par exemple, pour configurer l'utilisation d'une application A pour un département particulier, sans pour autant limiter l'accès à d'autres groupes :

- Utilisez la règle de stratégie d'admissibilité d'application par défaut qui inclut tout le monde.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Configurez la liste des utilisateurs du groupe de mise à disposition pour autoriser tous les utilisateurs du siège social à utiliser toutes les applications spécifiées dans le groupe de mise à disposition.
- (Si des groupes d'applications sont configurés) Configurez la liste des utilisateurs du groupe d'applications pour permettre aux membres du département Administration et Finances d'accéder aux applications A à L.
- Configurez les propriétés de l'application A pour limiter sa visibilité uniquement au personnel des comptes clients du département Administration et Finances.

Utilisateurs authentifiés et non authentifiés

Il existe deux types d'utilisateurs : authentifiées et non authentifiés (les utilisateurs non authentifiés sont également appelés anonymes). Vous pouvez configurer un ou deux types dans un groupe de mise à disposition.

Authentifié

Pour accéder aux applications et aux bureaux, les utilisateurs et les membres du groupe que vous spécifiez par nom doivent présenter des informations d'identification comme une carte à puce ou un nom d'utilisateur et mot de passe à StoreFront ou Citrix Receiver. Pour les groupes de mise à disposition contenant des machines avec OS de bureau, vous pouvez importer les données utilisateur (une liste des utilisateurs) plus tard en modifiant le groupe de mise à disposition.

Non authentifié (anonyme)

Pour les groupes de mise à disposition contenant les machines avec OS de serveur, vous pouvez autoriser les utilisateurs à accéder à des applications et des bureaux sans présenter d'informations d'identification à StoreFront ou à Citrix Receiver. Par exemple, l'application peut nécessiter des informations d'identification, mais ce n'est pas le cas pour le portail et les outils d'accès Citrix. Un groupe d'utilisateurs anonymes est créé lorsque vous installez le premier Delivery Controller.

Pour accorder l'accès à des utilisateurs non authentifiés, chaque machine du groupe de mise à disposition doit posséder un VDA pour OS Windows Server (version minimum 7.6) installé. Lorsque des utilisateurs non authentifiés sont activés, vous devez disposer d'un magasin StoreFront non authentifié.

Des comptes d'utilisateurs non authentifiés sont créés sur demande lorsqu'une session est lancée et nommée AnonXYZ, dans lequel XYZ est une valeur unique à trois chiffres.

Les sessions utilisateur non authentifiées possèdent un délai d'inactivité par défaut de 10 minutes, et leurs sessions sont automatiquement fermées lorsque le client se déconnecte. La reconnexion, l'itinérance entre les clients et le contrôle de l'espace de travail ne sont pas pris en charge.

Le tableau suivant décrit les choix disponibles sur la page Utilisateurs :

Activer l'accès pour	Ajouter/affecter des utilisateurs et des groupes d'utilisateurs ?	Activer la case à cocher « Autoriser les utilisateurs non authentifiés » ?
Seuls les utilisateurs authentifiés	Oui	Non
Seuls les utilisateurs non authentifiés	Non	Oui

© 1999-2017 Citrix Systems, Inc. All rights reserved.

À la fois les utilisateurs authentifiées et non authentifiés	Oui	Oui

À savoir :

- vous ne pouvez pas ajouter d'applications aux groupes de mise à disposition Remote PC Access.
- Par défaut, les applications que vous ajoutez sont placées dans un dossier nommé Applications. Vous pouvez spécifier un dossier différent. Pour de plus amples informations, veuillez consulter l'article Gérer les applications.
- Vous pouvez modifier les propriétés d'une application lorsque vous l'ajoutez à un groupe de mise à disposition ou ultérieurement. Pour de plus amples informations, veuillez consulter l'article Gérer les applications.
- Si vous essayez d'ajouter une application et qu'une application avec le même nom existe déjà dans ce dossier, vous êtes invité à renommer l'application que vous ajoutez. Si vous refusez, l'application est ajoutée avec un suffixe qui la rend unique dans ce dossier d'application.
- Lorsque vous ajoutez une application à plusieurs groupes de mise à disposition, vous risquez de rencontrer un problème de visibilité si vous ne disposez pas d'autorisations suffisantes pour afficher l'application dans tous les groupes de mise à disposition. Dans ce cas, consultez un administrateur disposant des autorisations appropriées ou demandez une extension de vos autorisations à tous les groupes de mise à disposition auxquels l'application a été ajoutée.
- Si vous publiez deux applications du même nom vers les mêmes utilisateurs, modifiez la propriété Nom de l'application (pour l'utilisateur) dans Studio ; sinon, les utilisateurs verront des noms en double s'afficher dans Receiver.

Cliquez sur la liste déroulante **Ajouter** pour afficher les sources des applications.

- **À partir du menu Démarrer** : applications qui sont découvertes sur une machine créée à partir de l'image principale du catalogue sélectionné. Lorsque vous sélectionnez cette source, une nouvelle page s'ouvre avec une liste d'applications découvertes ; sélectionnez les applications que vous souhaitez ajouter, puis cliquez sur **OK**.
- **Manuellement définies** : applications qui se trouvent dans le site ou ailleurs dans votre réseau. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez taper le chemin d'accès de l'exécutable, le répertoire de travail, les arguments de la ligne de commande (facultatifs), et les noms affichés des administrateurs et des utilisateurs. Après avoir entré ces informations, cliquez sur **OK**.
- **Existantes** : applications déjà ajoutées au site, peut-être dans un autre groupe de mise à disposition. Lorsque vous sélectionnez cette source, une nouvelle page s'ouvre avec une liste d'applications découvertes ; sélectionnez les applications que vous souhaitez ajouter, puis cliquez sur **OK**.
- **App-V** : applications dans des packages App-V. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez sélectionner le serveur App-V ou la bibliothèque d'applications. Sélectionnez les applications que vous souhaitez ajouter à partir de l'écran des résultats et cliquez sur **OK**. Pour plus d'informations, veuillez consulter l'article App-V.

Si une source d'applications ou une application n'est pas disponible ou valide, elle n'est pas visible ou ne peut pas être sélectionnée. Par exemple, la source **existante** n'est pas disponible si aucune application n'a été ajoutée au site. Ou une application peut ne pas être compatible avec les types de session pris en charge sur des machines du catalogue sélectionné.

Le titre de cette page dépend du catalogue de machines que vous avez choisi dans l'assistant :

- Si vous avez choisi un catalogue de machines contenant des machines regroupées, cette page est appelée Bureaux.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Si vous avez choisi un catalogue de machines contenant des machines attribuées et spécifié « Bureaux » sur la page Type de mise à disposition, cette page est appelée Desktop User Assignments (Attributions utilisateur bureau).
- Si vous avez choisi un catalogue de machines contenant des machines attribuées et spécifié « Applications » sur la page Type de mise à disposition, cette page est appelée Application Machine User Assignments (Attributions utilisateur machine application).

Cliquez sur **Add**. Effectuez les opérations suivantes dans cette boîte de dialogue :

- Dans les champs Nom d'affichage et Description, tapez les informations à afficher dans Receiver.
- À l'aide des boutons radio, indiquez qui peut démarrer un bureau (pour les groupes avec machines regroupées) ou qui sera attribué à une machine lorsqu'ils démarrent le bureau (pour les groupes avec machines attribuées). Les utilisateurs peuvent être tout utilisateur pouvant accéder à ce groupe de mise à disposition, ou des utilisateurs et groupes d'utilisateurs spécifiques.
- Si le groupe contient des machines attribuées, spécifiez le nombre maximal de bureaux par utilisateur. Cette valeur doit être de 1 au minimum.
- Activez ou désactivez le bureau (pour les machines regroupées) ou la règle d'attribution de bureau (pour les machines attribuées). La désactivation d'un bureau arrête la mise à disposition de bureaux ; la désactivation d'une règle d'attribution de bureau arrête l'attribution automatique de bureaux aux utilisateurs.
- Lorsque vous avez terminé avec la boîte de dialogue, cliquez sur **OK**.

Entrez un nom pour le groupe de mise à disposition. Vous pouvez également entrer une description (facultatif), qui s'affichera dans Receiver et dans Studio.

Consultez les informations récapitulatives, puis cliquez sur **Terminer**. Si vous n'avez pas sélectionné d'applications ou spécifié de bureaux à mettre à disposition, vous êtes invité à indiquer si vous voulez continuer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Gérer les groupes de mise à disposition

Jul 07, 2016

Dans cet article :

- Introduction
- Modifier les paramètres utilisateur dans un groupe de mise à disposition
- Ajouter ou supprimer des utilisateurs dans un groupe de mise à disposition
- Modifier le type de mise à disposition d'un groupe de mise à disposition
- Modifier les adresses de StoreFront
- Mettre à niveau un groupe de mise à disposition ou rétablir une mise à niveau
- Gérer les groupes de mise à disposition Remote PC Access
- Arrêter et redémarrer les machines d'un groupe de mise à disposition
- Gérer l'alimentation des machines d'un groupe de mise à disposition
- Créer un programme de redémarrage pour les machines d'un groupe de mise à disposition
- Empêcher les utilisateurs de se connecter à une machine (mode de maintenance) dans un groupe de mise à disposition
- Modifier les attributions de machines des utilisateurs d'un groupe de mise à disposition
- Modifier le nombre maximal de machines par utilisateur dans un groupe de mise à disposition
- Gérer la charge des machines dans les groupes de mise à disposition
- Supprimer une machine d'un groupe de mise à disposition
- Restreindre l'accès aux machines dans un groupe de mise à disposition
- Mettre à jour une machine dans un groupe de mise à disposition
- Fermer ou déconnecter une session, ou envoyer un message aux utilisateurs d'un groupe de mise à disposition
- Configurer le pré-lancement de session et la persistance de session

Introduction

Cet article décrit les procédures permettant de gérer des groupes de mise à disposition. En plus de la modification des paramètres spécifiés lors de la création du groupe, vous pouvez configurer d'autres paramètres qui ne sont pas disponibles lorsque vous créez un groupe de mise à disposition.

Consultez l'article Applications pour de plus amples informations sur la gestion des applications dans les groupes de mise à disposition, notamment comment ajouter et supprimer des applications dans un groupe de mise à disposition, et modifier les propriétés d'application.

La gestion des groupes de mise à disposition nécessite les autorisations d'administration déléguée du rôle intégré d'administrateur de groupe de mise à disposition. Consultez l'article Administration déléguée pour plus de détails.

Modifier les paramètres utilisateur dans un groupe de mise à disposition

Le nom de cette page peut s'afficher comme **Paramètres utilisateur** ou **Paramètres de base**.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Paramètres utilisateur** (ou**Paramètres de base**), modifiez les paramètres dans le tableau suivant.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Paramètre	Description
Description	Le texte que StoreFront utilise et que les utilisateurs voient.
Activer le groupe de mise à disposition	Indique si le groupe de mise à disposition est activé ou non.
Bureaux par utilisateur	(Machines avec OS de bureau affectées uniquement) Le nombre maximal de bureaux partagés pouvant être actifs pour un utilisateur à la fois. Dans les déploiements affectés lors de la première utilisation, cette valeur spécifie le nombre de bureaux que les utilisateurs peuvent s'affecter à eux-mêmes.
Fuseau horaire	
Activer Secure ICA	Sécurise les communications vers et depuis les machines dans le groupe de mise à disposition à l'aide de SecureICA, qui crypte le protocole ICA (le niveau par défaut est de 128 bits ; le niveau peut être modifié à l'aide du SDK). Citrix vous recommande d'utiliser des méthodes de cryptage supplémentaires telles que le cryptage TLS lorsque d'un passage au travers de réseaux publics. SecureICA n'effectue pas non plus de contrôle d'intégrité des données.

Ajouter ou supprimer des utilisateurs dans un groupe de mise à disposition

Pour de plus amples informations sur les utilisateurs, consultez la section Utilisateurs dans l'article Créer un groupe de mise à disposition.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Utilisateurs**, pour ajouter des utilisateurs, cliquez sur **Ajouter**, puis spécifiez les utilisateurs que vous souhaitez ajouter. Pour supprimer des utilisateurs, sélectionnez un ou plusieurs utilisateurs, puis cliquez sur **Supprimer**. Vous pouvez également sélectionner/désactiver la case à cocher qui permet d'activer ou de désactiver l'accès par des utilisateurs non authentifiés.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour les groupes de mise à disposition contenant des machines avec OS de bureau physique, vous pouvez importer les informations de l'utilisateur à partir d'un fichier .csv après la création du groupe de mise à disposition. Vous pouvez également exporter des informations utilisateur vers un fichier .csv. Le fichier .csv peut contenir des données provenant d'une version antérieure du produit.

La première ligne du fichier .csv doit contenir les en-têtes de colonnes séparés par des virgules (dans n'importe quel ordre), ce qui peut inclure: ADComputerAccount, AssignedUser, VirtualMachine et HostId. Les lignes suivantes dans le fichier contiennent des données de valeurs séparées par des virgules. Les entrées ADComputerAccount peuvent être des noms communs, des adresses IP ou des noms uniques, le domaine et les paires de nom d'ordinateur.

Pour importer ou exporter des informations sur l'utilisateur :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe de mise à disposition, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Allocation de machine**, sélectionnez le bouton **Importer la liste** ou **Exporter la liste**, puis accédez à l'emplacement du fichier.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Modifier le type de mise à disposition d'un groupe de mise à disposition

Le type indique ce que le groupe de mise à disposition peut mettre à disposition : des applications, des bureaux, ou les deux.

Avant de changer un type **application uniquement** ou **bureaux et applications** en type **bureaux uniquement**, supprimez toutes les applications du groupe de mise à disposition.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Type de mise à disposition**, sélectionnez le type de mise à disposition requis.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Modifier les adresses de StoreFront

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **StoreFront**, sélectionnez ou ajoutez des adresses URL StoreFront qui seront utilisées par Citrix Receiver qui est installé sur chaque machine dans le groupe de mise à disposition.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Vous pouvez également spécifier l'adresse de serveur StoreFront en sélectionnant l'option **Configuration > StoreFront** dans le volet de navigation Studio.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mettre à niveau un groupe de mise à disposition ou rétablir une mise à niveau

Mettez à niveau un groupe de mise à disposition après avoir mis à niveau les VDA sur les machines et les catalogues de machines contenant les machines utilisées dans le groupe de mise à disposition.

Avant de commencer la mise à niveau du groupe de mise à disposition :

- Si vous utilisez Provisioning Services, vous devez mettre à niveau la version du VDA dans la console Provisioning Services.
- Démarrez les machines contenant le VDA mis à niveau afin qu'elles puissent s'enregistrer avec le Delivery Controller. Ce processus informe Studio de la nature des éléments nécessitant une mise à niveau dans le groupe de mise à disposition.
- Si vous devez continuer à utiliser des versions antérieures du VDA, il se peut que des fonctionnalités plus récentes ne soient pas disponibles. Pour de plus amples informations, consultez les articles sur la mise à niveau.

Pour mettre à niveau un groupe de mise à disposition :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe de mise à disposition, puis sélectionnez **Mettre à niveau le groupe de mise à disposition** dans le volet Actions. L'action **Mettre à niveau le groupe de mise à disposition** s'affiche uniquement si Studio détecte des VDA mis à niveau.

Avant de démarrer le processus de mise à niveau, Studio vous indique quelles machines, le cas échéant, ne peuvent pas être mises à niveau et pourquoi. Vous pouvez alors annuler la mise à niveau, résoudre les problèmes de la machine, puis démarrer la mise à niveau.

Une fois la mise à niveau terminée, vous pouvez rétablir les machines à leur état précédent en sélectionnant le groupe de mise à disposition, puis en sélectionnant **Annuler** dans le volet Actions.

Gérer les groupes de mise à disposition Remote PC Access

Si une machine dans un catalogue de machines Remote PC Access n'est pas affectée à un utilisateur, Studio attribue temporairement la machine à un groupe de mise à disposition associé à ce catalogue de machine. Cette affectation temporaire permet à la machine d'être affectée à un utilisateur ultérieurement.

L'association du groupe de mise à disposition avec le catalogue de machines a une valeur de priorité. La priorité détermine à quel groupe de mise à disposition cette machine est attribuée lorsque celui-ci s'enregistre auprès du système ou lorsqu'un utilisateur a besoin d'une machine : plus la valeur est basse, plus la priorité est élevée. Si un catalogue de machine Remote PC Access possède plusieurs affectations de groupe de mise à disposition, le logiciel sélectionne la correspondance avec la priorité la plus élevée. Vous pouvez définir cette valeur de priorité à l'aide du SDK du PowerShell.

Lors de leur création, les catalogues de machines Remote PC Access sont associés à un groupe de mise à disposition. Cela signifie que les comptes de machines ou unités d'organisation ajoutés au catalogue ultérieurement peuvent être ajoutés au groupe de mise à disposition. Cette association peut être désactivée ou activée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter ou supprimer une association de catalogue de machines Remote PC Access avec un groupe de mise à disposition :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe Remote PC Access.
3. Dans la section Détails, sélectionnez l'onglet **Catalogues de machines**, puis sélectionnez un catalogue Remote PC Access.
4. Pour ajouter ou restaurer une association, sélectionnez **Ajouter des bureaux**. Pour supprimer une association, sélectionnez **Supprimer l'association**.

Arrêter et redémarrer les machines d'un groupe de mise à disposition

Cette procédure n'est pas prise en charge par les machines Remote PC Access.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Afficher les machines** dans le volet Actions.
3. Sélectionnez la machine et sélectionnez l'une des options suivantes dans le volet Actions (il se peut que certaines options ne soient pas disponibles, en fonction de l'état des machines) :

- **Forcer l'arrêt**. Place la machine hors tension de manière forcée et actualise la liste des machines.
- **Redémarrer.** Requiert la fermeture du système d'exploitation de la machine, puis redémarrage de la machine. Si le système d'exploitation ne peut pas s'y conformer, la machine reste dans son état actuel.
- **Forcer le redémarrage.** Force l'arrêt du système d'exploitation, puis redémarre la machine.
- **Suspendre.** Met en pause la machine sans la fermer et actualise la liste de machines.
- **Arrêtez la machine.** Requiert la fermeture du système d'exploitation.

Pour les actions qui ne sont pas forcées, si la machine ne se ferme pas dans les 10 minutes, elle est mise hors tension. Si Windows tente d'installer des mises à jour durant la fermeture, il y a un risque que la machine soit mise hors tension avant la fin des mises à jour.

Citrix vous recommande d'empêcher les utilisateurs des machines avec OS de bureau de sélectionner **Arrêter** dans une session. Consultez la documentation des stratégies Microsoft pour plus de détails.

Vous pouvez également arrêter et redémarrer des machines sur une connexion ; consultez l'article Connexions et ressources.

Gérer l'alimentation des machines d'un groupe de mise à disposition

Vous pouvez gérer l'alimentation des machines avec OS de bureau virtuelles uniquement, pas celle des machines physiques (y compris les machines Remote PC Access). Les machines avec OS de bureau avec capacités GPU ne peuvent pas être suspendues et ainsi les opérations de mise hors tension échouent. Pour les machines avec OS de serveur, vous pouvez créer un programme de redémarrage, qui est également décrit dans cet article.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dans des groupes de mise à disposition contenant des machines regroupées, les machines avec OS de bureau virtuelles peuvent être dans l'un des états suivants :

- Allouées de manière aléatoire et en cours d'utilisation.
- Non allouées et non connectées.

Dans des groupes de mise à disposition contenant des machines statiques, les machines avec OS de bureau virtuelles peuvent être :

- allouées à titre permanent et en cours d'utilisation ;
- Allouées à titre permanent et non connectées (mais prêtes)
- Non allouées et non connectées

Lors d'une utilisation normale, les groupes de mise à disposition statiques contiennent toujours des machines allouées et non allouées à titre permanent. Initialement, aucune machine n'est allouée (sauf celles manuellement allouées lors de la création du groupe de mise à disposition). Lorsque les utilisateurs se connectent, les machines sont allouées à titre permanent. Vous pouvez gérer l'alimentation des machines non allouées complètement dans les groupes de mise à disposition, mais uniquement partiellement gérer les machines allouées à titre permanent.

Regroupements et tampons : pour les groupes de mise à disposition regroupés et les groupes de mise à disposition statiques avec des machines non allouées, un regroupement (dans ce cas) est un ensemble de machines non allouées ou allouées temporairement de machines qui sont conservées à l'état sous tension, prêtes pour la connexion des utilisateurs ; un utilisateur reçoit une machine immédiatement après l'ouverture de session. La taille du regroupement (le nombre de machines conservées sous tension) est configurable par heure de la journée. Pour les groupes de mise à disposition statiques, utilisez le kit de développement pour configurer le regroupement.

Un tampon en veille est un ensemble de machines non allouées qui sont activées lorsque le nombre de machines du regroupement tombe en dessous d'un seuil qui est un pourcentage de la taille du groupe de mise à disposition. Pour les grands groupes de mise à disposition, un certain nombre de machines peut être activé lors du dépassement du seuil. Aussi, planifiez attentivement les tailles de groupes de mise à disposition ou utiliser le kit de développement pour ajuster la taille de tampon par défaut.

Horloges d'état d'alimentation : vous pouvez utiliser les horloges d'état d'alimentation pour suspendre des machines une fois que les utilisateurs se sont déconnectés depuis un laps de temps spécifié. Par exemple, les machines seront suspendues automatiquement les machines en dehors des heures ouvrables si les utilisateurs se sont déconnectés depuis au moins 10 minutes. Les machines aléatoires ou les machines avec Personal vDisks sont automatiquement arrêtées lorsque les utilisateurs ferment leur session, à moins que vous n'ayez configuré la propriété de groupe de mise à disposition ShutdownDesktopsAfterUse dans le kit de développement.

Vous pouvez configurer des horloges pour les jours de la semaine et les week-ends et, pour les heures de pointe et les intervalles calmes.

Gestion partielle de l'alimentation des machines allouées à titre permanent : pour des machines allouées à titre permanent, vous pouvez définir des horloges d'état d'alimentation, mais pas des regroupements ou des mémoires tampons. Les machines sont activées au début de chaque période de pointe, puis désactivées au début des heures creuses, si bien que vous n'avez pas de contrôle précis (comme avec les machines non allouées) sur le nombre de machines qui deviennent disponibles pour compenser les machines qui sont utilisées.

Pour gérer la consommation des machines virtuelles avec OS de bureau :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Gestion de l'alimentation**, sélectionnez **Jours ouvrés** dans la liste déroulante Gestion de l'alimentation des machines. Par défaut, les jours de la semaine vont du lundi au vendredi.
4. Pour les groupes de mise à disposition aléatoires, dans **Machines à allumer**, cliquez sur **Modifier** et spécifiez la taille du regroupement durant les jours ouvrés. Ensuite, sélectionnez le nombre de machines à mettre sous tension.
5. Dans **Heures de pointe**, définissez les heures de pointe et les heures creuses de chaque jour.
6. Définissez les horloges d'état d'alimentation pour les heures de pointe et les heures creuses des jours de la semaine : Dans **Durant les heures de pointe > Après déconnexion**, indiquez le délai (en minutes) avant la suspension des machines déconnectées dans le groupe de mise à disposition, puis sélectionnez Suspendre. Dans **Durant les heures creuses > Après déconnexion**, indiquez le délai avant la suspension des machines déconnectées dans le groupe de mise à disposition, puis sélectionnez **Arrêter**. Cette horloge n'est pas disponible pour les groupes de mise à disposition avec des machines aléatoires.
7. Sélectionnez **Week-end** dans la liste déroulante Gérer l'alimentation des machines, puis configurez les heures de pointe et les horloges d'état d'alimentation pour les week-ends.
8. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Utilisez le SDK pour :

- arrêter, plutôt que suspendre, les machines en réponse aux horloges d'état d'alimentation ou si vous voulez que les horloges soient basées sur les fermetures de session et non sur les déconnexions.
- Modifiez les définitions par défaut des jours de la semaine et du week-end.

Créer un programme de redémarrage pour les machines d'un groupe de mise à disposition

Un programme de redémarrage spécifie quand redémarrer périodiquement toutes les machines d'un groupe de mise à disposition.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Programme de redémarrage**, si vous ne souhaitez pas redémarrer automatiquement les machines du groupe de mise à disposition, sélectionnez le bouton radio **Non** et passez à la dernière étape de cette procédure. Aucun programme de redémarrage ni aucune stratégie de déploiement ne sera configuré(e). Si un programme a été configuré précédemment, cette sélection l'annule.
4. Si vous souhaitez redémarrer automatiquement les machines du groupe de mise à disposition, sélectionnez le bouton radio **Oui**.
5. Pour la fréquence de **redémarrage**, choisissez **Quotidien** ou le jour de la semaine où le redémarrage doit s'effectuer.
6. Pour **Commencer le redémarrage à**, à l'aide d'une horloge 24 heures, spécifiez l'heure de la journée à laquelle commencer le redémarrage.
7. Pour **Durée du redémarrage**, indiquez si toutes les machines doivent démarrer en même temps, ou le temps total que devra prendre le lancement du redémarrage de toutes les machines dans le groupe de mise à disposition. Un algorithme interne détermine le moment où chaque machine est redémarrée pendant cet intervalle.
8. Dans la liste déroulante **Notification** de gauche, indiquez si un message de notification doit s'afficher sur les machines

© 1999-2017 Citrix Systems, Inc. All rights reserved.

concernées avant qu'un redémarrage commence. Par défaut, aucun message ne s'affiche. Si vous choisissez d'afficher un message 15 minutes avant que le redémarrage commence, vous pouvez choisir (dans la liste déroulante **Répéter la notification**) de répéter le message toutes les cinq minutes après le premier message. Par défaut, le message n'est pas répété.

9. Entrez le texte de notification dans la zone **Message de notification** ; il n'existe pas de texte par défaut. Si vous souhaitez que le message inclue le nombre de minutes avant le redémarrage, incluez la variable **%m%** (par exemple : Avertissement : votre ordinateur sera automatiquement redémarré dans %m% minutes.). Si vous sélectionnez un intervalle de répétition de notification et que votre message comprend le paramètre fictif %m%, la valeur diminue de cinq minutes dans chaque message. Si vous avez choisi de redémarrer toutes les machines en même temps, le message de notification s'affiche sur chaque machine du groupe de mise à disposition à l'heure appropriée avant que le redémarrage ne commence, calculée par l'algorithme interne.
10. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Vous ne pouvez pas réaliser de mise sous tension ou arrêt automatisé(e) dans Studio, un redémarrage uniquement.

Empêcher les utilisateurs de se connecter à une machine (mode de maintenance) dans un groupe de mise à disposition

Lorsque vous devez arrêter temporairement les nouvelles connexions aux machines, vous pouvez activer le mode de maintenance pour une ou toutes les machines dans un groupe de mise à disposition. Vous pouvez effectuer cette opération avant d'appliquer des correctifs ou à l'aide d'outils de gestion.

- Lorsqu'une machine avec OS de serveur se trouve en mode de maintenance, les utilisateurs peuvent se connecter à des sessions existantes mais ne peuvent pas démarrer de nouvelles sessions.
- Lorsqu'une machine avec OS de bureau (ou un ordinateur utilisant Remote PC Access) est en mode de maintenance, les utilisateurs ne peuvent pas se connecter ou se reconnecter. Les connexions courantes restent connectées jusqu'à ce qu'elles se déconnectent ou ferment leur session.

Pour activer ou désactiver le mode de maintenance :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe.
3. Pour activer le mode de maintenance pour toutes les machines dans le groupe de mise à disposition, sélectionnez **Activer le mode de maintenance** dans le volet Actions. Pour activer le mode de maintenance pour une machine, sélectionnez **Afficher les machines** dans le volet Actions. Sélectionnez une machine, puis sélectionnez **Activer le mode de maintenance** dans le volet Actions.
4. Pour désactiver le mode de maintenance pour une ou toutes les machines dans un groupe de mise à disposition, suivez les instructions précédentes, sélectionnez **Désactiver le mode de maintenance** dans le volet Actions.

Les paramètres Windows RDC (Remote Desktop Connection) affectent également le fait qu'une machine avec OS de serveur est en mode de maintenance. Le mode de maintenance est activé dans l'un des cas suivants :

- Le mode de maintenance est défini sur Activé, comme décrit ci-dessus.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- RDC est défini sur **Ne pas autoriser les connexions à cet ordinateur**.
- RDC n'est pas défini sur **Ne pas autoriser les connexions à cet ordinateur** et le paramètre de mode d'ouverture de session utilisateur de la configuration à distance d'hôte est **Autoriser les reconnexions mais refuser les nouvelles ouvertures de session** ou **Autoriser les reconnexions mais refuser les nouvelles ouvertures de session jusqu'au redémarrage du serveur**.

Vous pouvez également activer ou désactiver le mode de maintenance pour une connexion (ce qui affecte les machines qui utilisent cette connexion), ou pour un catalogue de machines (ce qui affecte les machines de ce catalogue).

Modifier les attributions de machines des utilisateurs d'un groupe de mise à disposition

Vous pouvez modifier les attributions des machines avec OS de bureau, des machines avec OS de serveur ou des machines créées au travers de Provisioning Services.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe.
3. Sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions. Sur la page **Bureaux** ou **Règles d'attribution de bureau** (une seule de ces pages sera disponible, en fonction du type de catalogue de machines que le groupe de mise à disposition utilise), spécifiez les nouveaux utilisateurs.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Modifier le nombre maximal de machines par utilisateur

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Règles d'attribution de bureau**, définissez le nombre maximal de bureaux par utilisateur.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Gérer la charge des machines dans les groupes de mise à disposition

Vous pouvez gérer la charge des machines avec OS de serveur uniquement.

La gestion de la charge mesure la charge du serveur et détermine le serveur à sélectionner dans les conditions actuelles d'environnement. Cette sélection est basée sur :

État du mode de maintenance du serveur : une machine avec OS de serveur est considérée pour l'équilibrage de charge uniquement lorsque le mode de maintenance est désactivé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Index de charge du serveur : détermine la probabilité qu'un serveur qui met à disposition des machines avec OS de serveur a de recevoir des connexions. L'index est une combinaison de calculateurs de charge : le nombre de sessions et les paramètres des mesures de performances tels que l'UC, le disque et l'utilisation de la mémoire. Vous devez spécifier des calculateurs de charge dans les paramètres de la stratégie de gestion de la charge.

Vous pouvez surveiller l'index de charge dans Director, la recherche Studio et le kit de développement.

Dans Studio, la colonne d'index de charge du serveur est masquée par défaut. Pour l'afficher, sélectionnez une machine, cliquez avec le bouton droit de la souris sur un en-tête de colonne, puis choisissez Sélectionner les colonnes. In the Machine category, select Load Index.

Dans le kit de développement, utilisez l'applet de commande Get-BrokerMachine. Pour de plus amples informations, consultez l'article CTX202150.

Un serveur d'index de charge de 10 000 indique que le serveur est complètement chargé. Si aucun des autres serveurs n'est disponible, il se peut que les utilisateurs reçoivent un message indiquant que le bureau ou l'application est actuellement indisponible lorsqu'ils lancent une session.

Paramètre de stratégie de tolérance d'ouvertures de session simultanées : le nombre maximal de demandes simultanées pour ouvrir une session sur le serveur. (Ce paramètre est équivalent à l'optimisation de la charge dans les versions antérieures à la version 7.5 de XenApp.)

Si le nombre de demandes d'ouvertures de session que tous les serveurs reçoivent est égal ou supérieur au paramètre Tolérance d'ouvertures de session simultanées, la prochaine demande d'ouverture de session est attribuée au serveur avec le nombre d'ouvertures de session en attente le plus faible. Si plusieurs serveurs répondent à ces critères, le serveur ayant l'index de charge le plus faible est sélectionné.

Supprimer une machine d'un groupe de mise à disposition

La suppression d'une machine la supprime d'un groupe de mise à disposition, mais ne la supprime pas dans le catalogue de machines que le groupe de mise à disposition utilise. Par conséquent, cette machine est disponible pour l'affectation à un autre groupe de mise à disposition.

Les machines doivent être arrêtés avant de pouvoir être supprimées. Pour empêcher temporairement les utilisateurs de se connecter à une machine pendant que vous la supprimez, placez-la en mode maintenance avant de l'arrêter.

Gardez à l'esprit que les machines peuvent contenir des données personnelles, soyez donc prudent avant d'allouer la machine à un autre utilisateur. Il se peut que vous souhaitiez créer une nouvelle image de la machine.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Afficher les machines** dans le volet Actions.
3. Vérifiez que la machine est arrêtée.
4. Sélectionnez **Supprimer du groupe de mise à disposition** dans le volet Actions.

Vous pouvez également supprimer une machine d'un groupe de mise à disposition au travers de la connexion utilisée par la machine. Pour de plus amples informations, veuillez consulter l'article Connexions et ressources.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Restreindre l'accès aux machines dans un groupe de mise à disposition

Toute modification que vous apportez pour restreindre l'accès aux machines dans un groupe de mise à disposition remplace les paramètres précédents, quelle que soit la méthode que vous utilisez. Vous pouvez :

Limiter l'accès des administrateurs à l'aide d'étendues d'administration déléguée. Vous pouvez créer et allouer une étendue qui permet aux administrateurs d'accéder à toutes les applications, et une autre qui ne leur donne accès qu'à certaines applications. Consultez l'article Administration déléguée pour plus de détails.

Limitez l'accès des utilisateurs via des expressions de stratégie SmartAccess qui filtrent les connexions utilisateur effectuées via NetScaler Gateway.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Dans la page **Stratégie d'accès**, sélectionnez **Connexions transitant par NetScaler Gateway**.
4. Pour choisir un sous-ensemble de ces connexions, sélectionnez **Connexions remplissant l'un des critères de filtre suivants**. Ensuite, définissez le site NetScaler Gateway, et ajoutez, modifiez ou supprimez les expressions de la stratégie SmartAccess pour les scénarios d'accès des utilisateurs autorisés. Pour plus d'informations, consultez la documentation relative à NetScaler Gateway.
5. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Limiter l'accès des utilisateurs via des filtres d'exclusion sur les stratégies d'accès que vous définissez dans le kit de développement. Des stratégies d'accès sont appliquées aux groupes de mise à disposition pour affiner les connexions. Par exemple, vous pouvez restreindre l'accès aux machines à un sous-ensemble d'utilisateurs, vous pouvez spécifier les machines utilisateur autorisées. Les filtres d'exclusion affinent davantage les stratégies d'accès. Vous pouvez, par exemple, refuser l'accès à un sous-ensemble d'utilisateurs ou de machines pour des raisons de sécurité. Par défaut, les filtres d'exclusion sont désactivés.

Par exemple, un laboratoire d'enseignement sur un sous-réseau du réseau d'entreprise, pour empêcher l'accès à ce laboratoire à un certain groupe de mise à disposition, quelle que soit la personne qui utilise les machines dans le laboratoire, utilisez la commande suivante : Set-BrokerAccessPolicy, -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True.

Vous pouvez également utiliser un astérisque (*) en tant que caractère générique afin de faire correspondre toutes les balises qui commencent par la même expression de stratégie. À titre d'exemple, si vous avez ajouté la balise VPDesktops_Direct à une machine et VPDesktops_Test à une autre machine, la définition de la balise dans le script Set-BrokerAccessPolicy sur VPDesktops_* applique le filtre aux deux machines.

Mettre à jour une machine dans un groupe de mise à disposition

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Afficher les machines** dans le volet Actions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Sélectionnez une machine, puis sélectionnez **Mettre à jour les machines** dans le volet Actions.

Pour sélectionner une autre image principale, sélectionnez **Image principale**, puis sélectionnez un instantané.

Pour appliquer les modifications et notifier les utilisateurs de la machine, sélectionnez **Envoyer une notification aux utilisateurs**. Ensuite, spécifiez : quand effectuer la mise à jour de l'image principale (maintenant ou lors du prochain redémarrage), l'horaire de distribution du redémarrage (le délai total imparti pour commencer la mise à jour de toutes les machines du groupe), et si les utilisateurs seront notifiés du redémarrage, ainsi que le message qu'ils recevront.

Fermer ou déconnecter une session, ou envoyer un message aux utilisateurs d'un groupe de mise à disposition

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Afficher les machines** dans le volet Actions.
3. Pour fermer la session d'un utilisateur, sélectionnez la session ou le bureau, puis sélectionnez **Fermer la session** dans le volet Actions. La session se ferme et la machine devient disponible auprès des autres utilisateurs, à moins qu'elle ne soit attribuée à un utilisateur spécifique.
4. Pour déconnecter une session, sélectionnez la session ou le bureau, puis sélectionnez **Déconnecter** dans le volet Actions. Les applications continuent à être exécutées et la machine reste attribuée à cet utilisateur. L'utilisateur peut se reconnecter à la même machine.
5. Pour envoyer un message aux utilisateurs, sélectionnez la session, la machine ou l'utilisateur, puis sélectionnez **Envoyer un message** dans le volet Actions. Entrez le message.

Vous pouvez configurer les horloges d'état d'alimentation pour les machines avec OS de bureau pour gérer automatiquement les sessions non utilisées. Consultez la section Gérer l'alimentation des machines pour plus de détails.

Configurer le pré-lancement de session et la persistance de session dans un groupe de mise à disposition

Ces fonctionnalités sont prises en charge sur les machines avec OS de serveur uniquement.

Les fonctionnalités de pré-lancement de session et de persistance de session aident les utilisateurs spécifiés à accéder aux applications rapidement, en démarrant des sessions avant qu'elles ne sont demandées (pré-lancement de session) et conserver les sessions d'applications actives après qu'un utilisateur ferme toutes les applications (persistance de session).

Par défaut, le pré-lancement de session et la persistance de session ne sont pas utilisées : une session démarre (se lance) lorsqu'un utilisateur démarre une application et reste active jusqu'à ce que la dernière application ouverte dans la session se ferme.

Notions importantes :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Le groupe de mise à disposition doit prendre en charge les applications, et les machines doivent être exécutées sur un VDA pour OS de serveur Windows, version minimale 7.6.
- Ces fonctionnalités sont uniquement prises en charge lors de l'utilisation de Citrix Receiver pour Windows, et requièrent également une configuration de Citrix Receiver supplémentaire. Pour obtenir des instructions, recherchez pré-lancement de session dans la documentation produit pour votre version de Citrix Receiver pour Windows.
- Veuillez noter que Citrix Receiver pour HTML5 n'est pas pris en charge.
- Lorsque vous utilisez le pré-lancement de session, si une machine utilisateur est placée en mode « suspendue » ou « veille prolongée », le pré-lancement ne fonctionne pas (quels que soient les paramètres de pré-lancement de session). Les utilisateurs peuvent verrouiller leurs machines/sessions, mais si un utilisateur ferme sa session sur Citrix Receiver, la session est fermée et le pré-lancement ne s'applique plus.
- Lorsque vous utilisez le pré-lancement de session, les machines clientes physiques ne peuvent pas utiliser les fonctions de gestion de l'alimentation en veille ou veille prolongée. Les utilisateurs de la machine cliente peuvent verrouiller leurs sessions, mais ne doivent pas les fermer.
- Les sessions pré-lancées et persistantes utilisent une licence, mais uniquement lorsque vous êtes connecté. Toute session pré-lancée et persistante non utilisée se déconnecte après 15 minutes par défaut. Cette valeur peut être configurée dans PowerShell (applet de commande New/Set-BrokerSessionPreLaunch).
- Une planification et un contrôle attentif des modèles d'activité de vos utilisateurs sont essentiels pour personnaliser ces fonctionnalités afin qu'elles se complètent l'une avec l'autre. Une configuration optimale équilibre les avantages d'une disponibilité d'application antérieure pour les utilisateurs par rapport au coût de licences en cours d'utilisation et de ressources allouées.
- Vous pouvez également configurer le pré-lancement de session pour une heure de la journée planifiée dans Citrix Receiver.

Il existe plusieurs façons de spécifier la durée pendant laquelle une session non utilisée reste active si l'utilisateur ne démarre pas une application : un délai configuré et des seuils de charge du serveur. Vous pouvez tous les configurer ; l'événement qui se produit en premier provoquera la fin de la session non utilisée.

- **Expiration du délai** : une expiration de délai configurée spécifie le nombre de minutes, heures ou jours pour lesquels une session pré-lancée inutilisée pré-lancés ou une session de persistance restent actives. Si vous configurez un délai d'expiration trop court, les sessions pré-lancées se termineront avant de permettre aux utilisateurs de bénéficier d'un accès aux applications plus rapide. Si vous configurez un délai d'expiration trop long, les connexions utilisateur entrantes peuvent être refusées car le serveur ne dispose pas de suffisamment de ressources.

  Vous ne pouvez pas désactiver cette expiration du délai depuis Studio, mais vous pouvez dans le kit de développement (applet de commandes New/Set-BrokerSessionPreLaunch). Si vous désactivez l'expiration du délai, elle n'apparaît pas dans l'affichage de Studio pour ce groupe de mise à disposition ou dans l'Assistant Modifier le groupe de mise à disposition.

- **Seuils** : les sessions pré-lancées se terminant automatiquement et les sessions de persistance basées sur la charge d'un serveur assure que les sessions restent ouverte le plus longtemps possible, en supposant que les ressources serveur sont disponibles. Les sessions pré-lancées et les sessions de persistance inutilisées ne provoqueront pas de refus de connexions, car elles seront arrêtées automatiquement lorsque les ressources sont nécessaires pour de nouvelles sessions utilisateur.

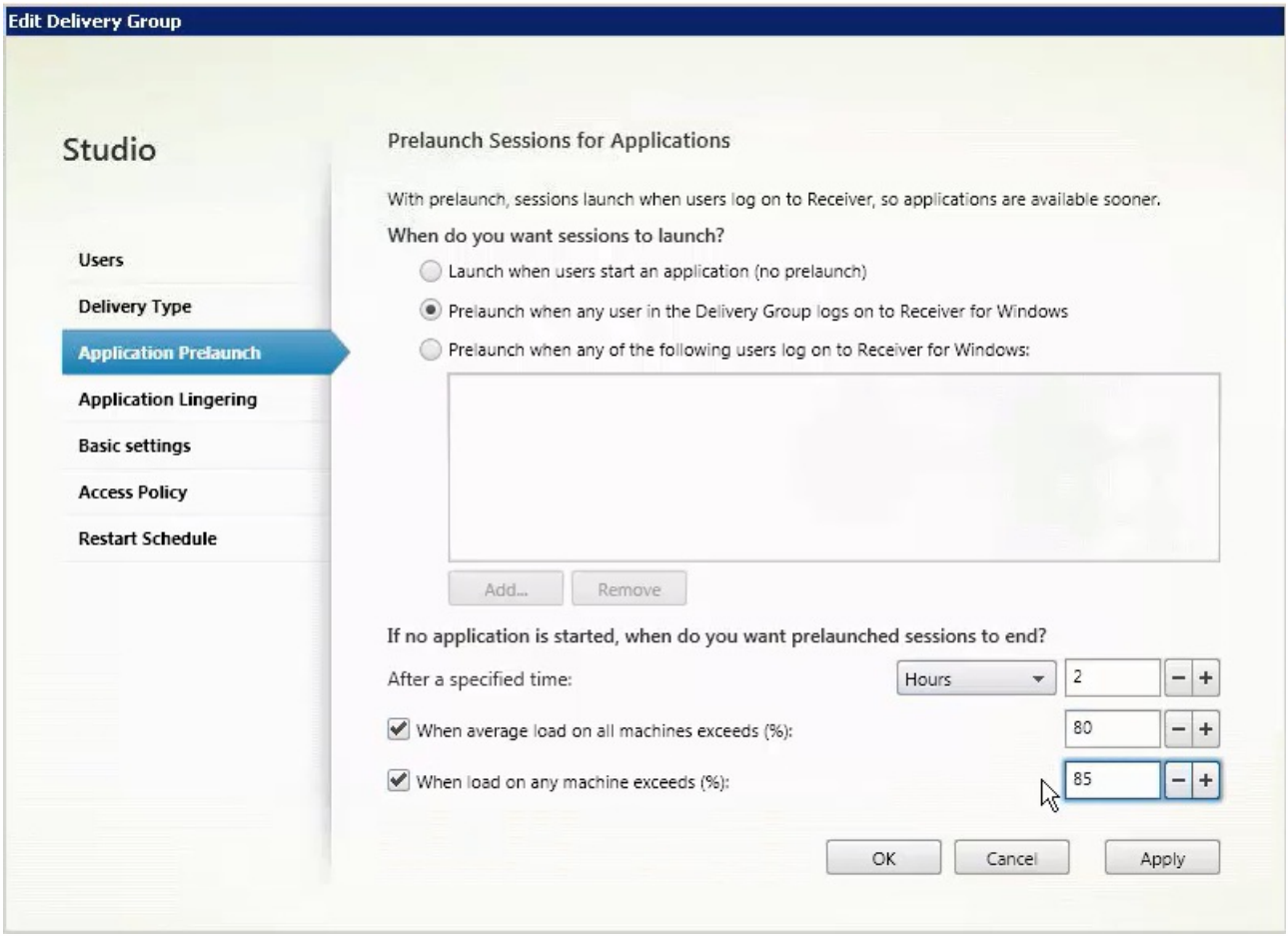
  Vous pouvez configurer deux seuils : la charge de pourcentage moyenne de tous les serveurs dans le groupe de mise à disposition et le pourcentage maximal de charge d'un serveur dans le groupe de mise à disposition. Lorsqu'un seuil est dépassé, les sessions qui se sont trouvées dans un état de pré-lancement ou de persistance pour la période la plus

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

longue est terminée, les sessions sont arrêtés une à une à toutes les minutes jusqu'à ce que la charge tombe en dessous du seuil. (Lorsque la valeur de seuil est dépassée, aucune nouvelle session de pré-lancement n'est démarrée

Les serveurs avec des VDA qui n'ont pas été inscrits avec le Controller et les serveurs en mode de maintenance sont considérés comme entièrement chargés. Un problème inattendu provoquera la fermeture automatique des sessions de pré-lancement et des sessions de persistance pour libérer de la capacité.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe de mise à disposition, puis cliquez sur **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Pré-démarrage d'application**, activez le pré-lancement de session, en choisissant le moment de démarrage des sessions :
   - Lorsqu'un utilisateur démarre une application. Il s'agit du paramètre par défaut ; le pré-lancement de session est désactivé.
   - Lorsqu'un utilisateur du groupe de mise à disposition ouvre une session sur Citrix Receiver pour Windows.
   - Lorsque tout le monde dans une liste d'utilisateurs et de groupes d'utilisateurs ouvre une session sur Citrix Receiver pour Windows. Veuillez également spécifier les utilisateurs ou les groupes d'utilisateurs si vous choisissez cette option.



4. Une session pré-lancée est remplacée par une session régulière lorsque l'utilisateur démarre une application. Si l'utilisateur ne démarre pas une application (la session pré-lancée n'est pas utilisée), les paramètres suivants affectent la durée pour

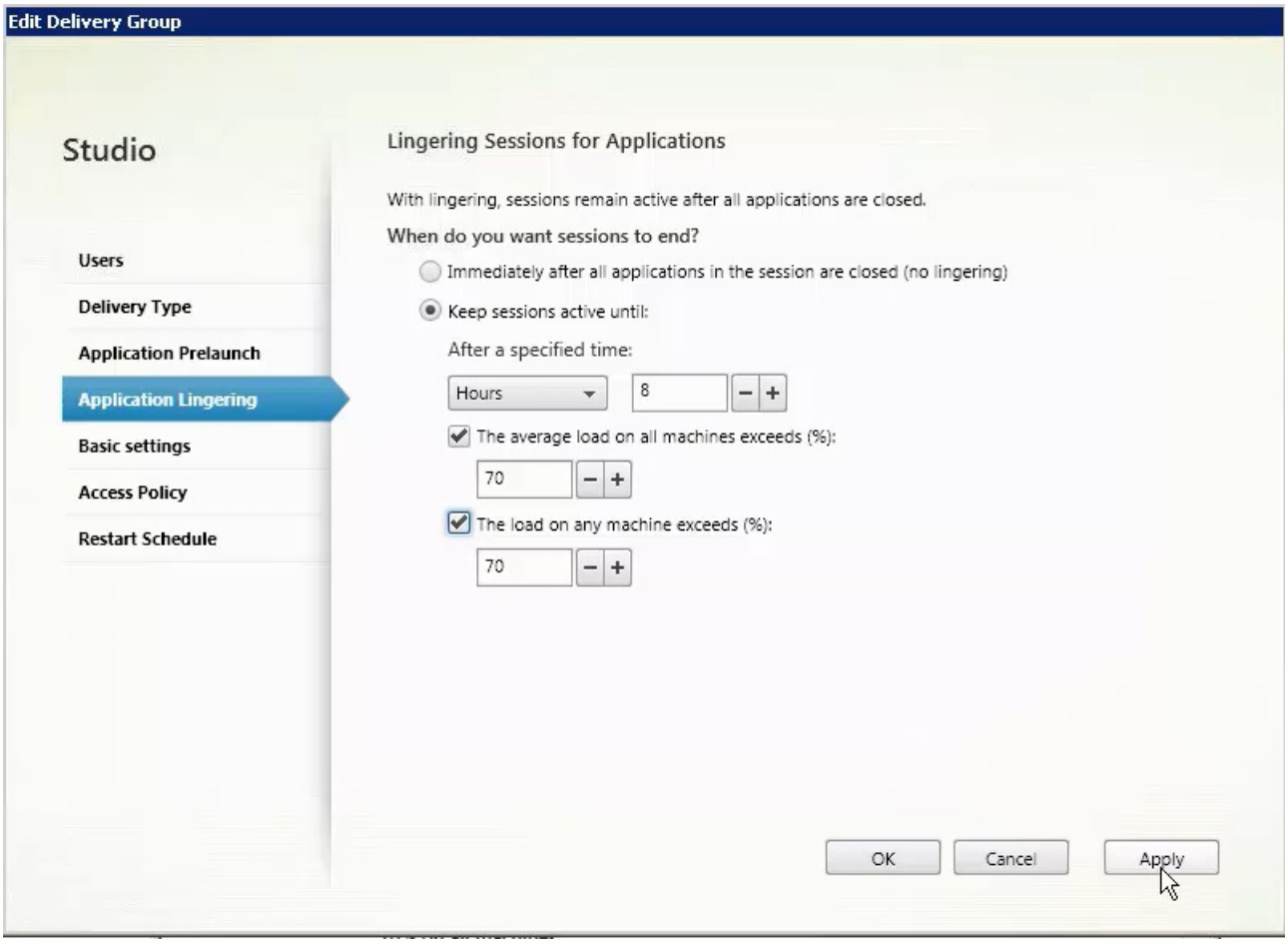
© 1999-2017 Citrix Systems, Inc. All rights reserved.

laquelle la session reste active.

- Lorsqu'un intervalle de temps spécifié expire. Vous pouvez modifier l'intervalle de temps (1-99 jours, 1-2 376 heures, heures ou 1-142 560 minutes).
- Lorsqu'une charge moyenne sur toutes les machines du groupe de mise à disposition dépasse un pourcentage spécifié (1-99%).
- Lorsque la charge de toute machine du groupe de mise à disposition dépasse un pourcentage spécifié (1-99%).

Récapitulatif : une session pré-lancée reste active jusqu'à ce que l'un des événements suivants se produise : un utilisateur lance une application, la durée spécifiée est écoulée, ou un seuil de charge spécifié est dépassé.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe de mise à disposition, puis cliquez sur **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Attente d'application**, activez la persistance de session en sélectionnant le bouton radio **Maintenir les sessions dans l'état actif jusqu'à**.



4. Plusieurs paramètres affectent la durée pendant laquelle une session persistante reste active si l'utilisateur ne démarre pas d'autre application.
   - Lorsqu'un intervalle de temps spécifié expire. Vous pouvez modifier l'intervalle de temps (1-99 jours, 1-2 376 heures, heures ou 1-142 560 minutes).
   - Lorsqu'une charge moyenne sur toutes les machines du groupe de mise à disposition dépasse un pourcentage spécifié (1-99%).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Lorsque la charge de toute machine du groupe de mise à disposition dépasse un pourcentage spécifié (1-99%).

Récapitulatif : une session de persistance reste active jusqu'à ce que l'un des événements suivants se produise : un utilisateur démarre une application, la durée spécifiée est écoulée, ou un seuil de charge spécifié est dépassé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Créer des groupes d’applications

Jul 07, 2016

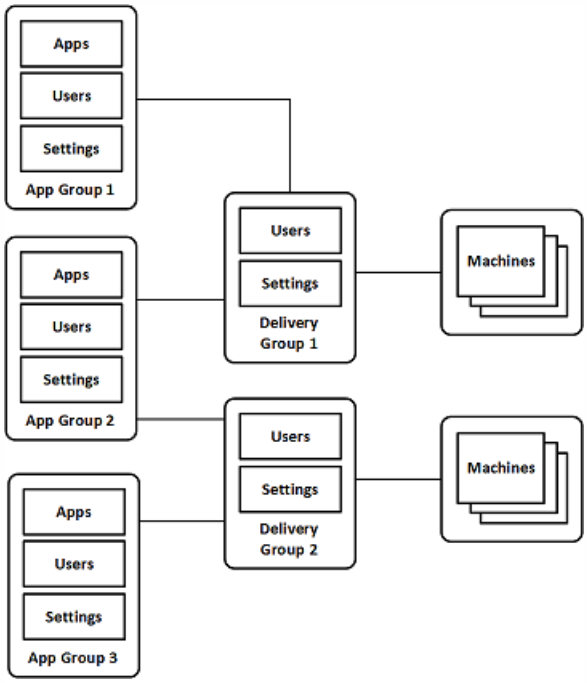
Introduction

Les groupes d'applications vous permettent de gérer des collections d'applications. Vous pouvez créer des groupes d’applications pour les applications partagées entre différents groupes de mise à disposition ou utilisées par un sous-ensemble d'utilisateurs dans des groupes de mise à disposition. Les groupes d'applications sont facultatifs ; ils offrent une alternative à l'ajout des mêmes applications sur plusieurs groupes de mise à disposition. Les groupes de mise à disposition peuvent être associés à plus d'un groupe d'applications, et un groupe d'applications peut être associée à plus d'un groupe de mise à disposition.

Comparativement à l’utilisation d’un plus grand nombre de groupes de mise à disposition, les groupes d'applications permettent de gérer les applications et de contrôler les ressources :

- Le regroupement logique d'applications et de leurs paramètres vous permet de gérer ces applications comme une unité unique. Par exemple, vous n’avez pas besoin d’ajouter (publier) la même application, une par une, à des groupes de mise à disposition individuels.
- Le partage de session entre des groupes d'applications peut économiser la consommation de ressources. Dans d'autres cas, la désactivation du partage de session entre les groupes d’applications peut s'avérer bénéfique.

Le graphique suivant illustre un déploiement XenApp ou XenDesktop qui comprend des groupes d'applications :



Dans cette configuration, les applications sont ajoutées à des groupes d’applications, et non à des groupes de mise à disposition. Les groupes de mise à disposition spécifient les machines qui seront utilisées. (Bien que cela ne soit pas affiché,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

les machines se trouvent dans des catalogues de machines).

Le groupe d'applications 1 est associé au groupe de mise à disposition 1. Les applications du groupe d'applications 1 sont accessibles par les utilisateurs spécifiés dans le groupe d'applications 1, à condition qu'ils figurent également dans la liste des utilisateurs du groupe de mise à disposition 1. Cette approche suit les recommandations selon lesquelles la liste d'utilisateurs d'un groupe d'applications doit être un sous-ensemble (une restriction) des listes d'utilisateurs des groupes de mise à disposition associés. Les paramètres du groupe d'applications 1 (tels que le partage de session d'application entre groupes d'applications, groupes de mise à disposition associés) s'appliquent aux applications et utilisateurs de ce groupe. Les paramètres du groupe de mise à disposition de 1 (tels que la prise en charge des utilisateurs anonymes) s'appliquent aux utilisateurs des groupes d'applications 1 et 2, car ces groupes d'applications ont été associés à ce groupe de mise à disposition.

Le groupe d'applications 2 est associé à deux groupes de mise à disposition : 1 et 2. Chacun de ces groupes de mise à disposition peut se voir attribuer une priorité dans le groupe d'applications 2, ce qui indique l'ordre dans lequel les groupes de mise à disposition vont être vérifiés lorsqu'une application est lancée. La charge des groupes de disposition ayant le même niveau de priorité est équilibrée. Les applications du groupe d'applications 2 sont accessibles par les utilisateurs spécifiés dans le groupe d'applications 2, à condition qu'ils figurent également dans les listes d'utilisateurs du groupe de mise à disposition 1 et du groupe de mise à disposition 2.

Conseils et considérations

Citrix vous recommande d'ajouter des applications à des groupes d'applications ou des groupes de mise à disposition, mais pas aux deux. Sinon, la complexité engendrée par le fait d'avoir des applications dans deux types de groupes peut rendre leur gestion plus difficile.

Par défaut, un groupe d'applications est activé. Lorsque vous créez un groupe d'applications, vous pouvez modifier le groupe pour modifier ce paramètre ; veuillez consulter l'article Gérer des groupes d'applications.

Par défaut, le partage de session d'application entre groupes d'applications est activé ; veuillez consulter la section Partage de session entre des groupes d'applications ci-dessous.

Citrix recommande de mettre à niveau vos groupes de mise à disposition vers la version actuelle. Cela requiert (1) de mettre à niveau les VDA sur les machines utilisées dans le groupe de mise à disposition, (2) de mettre à niveau les catalogues de machines contenant ces machines, puis (3) de mettre à niveau le groupe de mise à disposition. Pour de plus amples informations, consultez la section Gérer des groupes d'applications. Pour utiliser des groupes d'applications, vos composants principaux doivent être à la version minimale 7.9.

La création de groupes d'applications nécessite les autorisations d'administration déléguée du rôle intégré d'administrateur de groupe de mise à disposition. Consultez l'article Administration déléguée pour plus de détails.

Cet article introduit la notion « d'association » d'une application avec plus d'un groupe d'applications pour opérer une distinction avec l'ajout d'une nouvelle instance de cette application à partir d'une source disponible. De même, les groupes de mise à disposition sont associés à des groupes d'applications (et vice versa), plutôt que des ajouts ou des composants de l'un ou l'autre.

Partage de session entre des groupes d'applications

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Lorsque vous utilisez des groupes d'applications, vous pouvez autoriser ou interdire le partage de session d'application entre les groupes d'applications. (Ce comportement étend la fonctionnalité de partage de session standard disponible lors de l'utilisation de groupes de mise à disposition, comme décrit dans le premier exemple ci-dessous). Le partage de session d'application réduit les coûts associés au lancement de sessions d'application supplémentaires. Il permet également d'utiliser les fonctionnalités applicatives qui impliquent le Presse-papiers, telles que les opérations de copier-coller.

Exemple dans lequel l'activation du partage de session entre des groupes d'applications est utile :

> Un utilisateur du groupe A 1 démarre une session d'application en lançant Word, puis démarre Excel, alors que Word est toujours en cours d'exécution. Si le Controller trouve Excel sur le même serveur, la session est partagée. (Il s'agit de la fonctionnalité de partage de session de base utilisée dans les groupes de mise à disposition, si vous n'utilisez pas de groupes d'applications). Si Excel est introuvable sur le même serveur, et que le partage de session est activé pour le groupe d'applications 1, le Controller tente de partager la session si l'application est trouvée sur un autre serveur dans les groupes de mise à disposition associés avec le groupe d'applications 1, ou dans les groupes d'applications 2 et 3.

Exemple dans lequel la désactivation du partage de session entre des groupes d'applications est utile :

> Vous disposez d'applications qui ne fonctionnent pas correctement avec d'autres applications qui sont installées sur la même machine, telles que deux versions différentes de la même suite logicielle ou deux versions différentes du même navigateur Web. Vous ne souhaitez pas autoriser un utilisateur à lancer les deux versions dans la même session.
>
> Vous créez un groupe d'applications pour chaque version de la suite logicielle, et ajoutez les applications de chaque version de la suite logicielle au groupe d'applications correspondant. Si le partage de session entre les groupes est désactivé pour chacun de ces groupes d'application, un utilisateur spécifié dans ces groupes peuvent exécuter les applications de la même version dans la même session et peut toujours exécuter d'autres applications simultanément, mais pas dans la même session. Si l'utilisateur lance une des applications dont la version est différente (qui se trouvent dans un autre groupe d'applications), ou lance une application qui ne figure pas dans un groupe d'applications, cette application est lancée dans une nouvelle session.

IMPORTANT : cette fonctionnalité de partage de session entre groupes d'applications n'est pas une fonctionnalité de sécurité faisant appel à un sandbox. Elle n'est pas infaillible et elle ne peut pas empêcher les utilisateurs de lancer des applications dans leurs sessions via d'autres moyens (par exemple, au travers de l'Explorateur Windows).

Si une machine fonctionne à pleine capacité, le partage de session n'est pas autorisé.

Le partage de session d'application entre groupes d'applications doit être activé si vous souhaitez utiliser les fonctionnalités de pré-lancement de session et de persistance de session ; cependant, ces fonctionnalités doivent être activées et configurées dans chacun des groupes de mise à disposition associés au groupe d'applications ; vous ne pouvez pas les configurer dans les groupes d'applications.

Par défaut, le partage de session d'applications entre groupes d'applications est activé lorsque vous créez un groupe d'applications ; vous ne pouvez pas changer ce paramètre lors de la création du groupe. Lorsque vous créez un groupe d'applications, vous pouvez modifier le groupe pour modifier ce paramètre ; veuillez consulter l'article Gérer des groupes d'applications.

Créer un groupe d'applications

Pour créer un groupe d'applications :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Sélectionnez **Applications** dans le panneau de navigation de Studio, puis sélectionnez **Créer groupe d'applications** dans le volet Actions.
2. L'assistant Créer groupe d'applications démarre sur une page **Introduction**, que vous pouvez supprimer des futurs démarrages de cet assistant.
3. L'assistant vous guide ensuite au travers des pages décrites ci-dessous. Lorsque vous avez terminé chaque page, cliquez sur **Suivant** jusqu'à la page de synthèse.

Tous les groupes de mise à disposition sont répertoriés, avec le nombre de machines qu'ils contiennent.

- La liste **Groupes de mise à disposition compatibles** dresse la liste des groupes de mise à disposition que vous pouvez sélectionner. Les groupes de mise à disposition compatibles contiennent des machines avec OS de bureau ou de serveur aléatoires (non attribuées de façon permanente ou statique).
- La liste **Groupes de mise à disposition non compatibles** dresse la liste des groupes de mise à disposition que vous ne pouvez pas sélectionner. Chaque entrée explique pourquoi un groupe n'est pas compatible, par exemple parce qu'il contient machines attribuées de manière statique.

Un groupe d'applications peut être associé à des groupes de mise à disposition contenant des machines partagées (non privées) qui peuvent mettre à disposition des applications.

Vous pouvez également sélectionner des groupes de mise à disposition contenant des machines partagées qui mettent uniquement à disposition des bureaux, si (1) le groupe de mise à disposition contient des machines partagées et a été créé avec une version antérieure de XenDesktop 7.x, et (2) vous disposez de l'autorisation Modifier le groupe de mise à disposition. Le type de groupe de mise à disposition est automatiquement converti en « bureaux et applications » lorsque l'assistant Créer groupe d'applications est validé.

Bien que vous puissiez créer un groupe d'applications qui n'est associé à aucun groupe de mise à disposition – par exemple pour organiser les applications ou pour servir de stockage aux applications non utilisées – le groupe d'applications ne peut pas être utilisé pour mettre à disposition des applications tant qu'il ne spécifie pas au moins un groupe de mise à disposition. De plus, vous ne pouvez pas ajouter d'applications au groupe d'applications à partir de la source Depuis le menu Démarrer si aucun groupe de mise à disposition n'a été spécifié.

Les groupes de mise à disposition que vous sélectionnez spécifient les machines qui seront utilisées pour mettre à disposition des applications. Sélectionnez les cases à cocher en regard des groupes de mise à disposition que vous souhaitez associer au groupe d'applications.

Spécifiez quiconque peut utiliser les applications dans le groupe d'applications. Vous pouvez autoriser tous les utilisateurs et groupes d'utilisateurs dans les groupes de mise à disposition que vous avez sélectionnés sur la page précédente, ou sélectionner des utilisateurs et groupes d'utilisateurs spécifiques à partir de ces groupes de mise à disposition. Si vous limitez l'utilisation aux utilisateurs que vous spécifiez, seuls les utilisateurs spécifiés dans le groupe de mise à disposition et le groupe d'applications peuvent accéder aux applications dans ce groupe d'applications. Concrètement, la liste d'utilisateurs du groupe d'applications filtre les listes d'utilisateurs des groupes de mise à disposition.

La possibilité d'activer ou de désactiver l'utilisation d'applications par des utilisateurs non authentifiés est uniquement disponible dans les groupes de mise à disposition, et pas dans les groupes d'applications.

Où les listes d'utilisateurs sont spécifiées

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Les listes d'utilisateurs Active Directory sont spécifiées lorsque vous créez ou modifiez les informations suivantes :

- La liste d'accès utilisateur d'un site, qui n'est pas configurée dans Studio. Par défaut, la règle de stratégie d'admissibilité d'application inclut tout le monde ; consultez les applets de commande du kit de développement PowerShell BrokerAppEntitlementPolicyRule pour plus de détails.
- Liste d'utilisateurs du groupe d'applications.
- Liste d'utilisateurs du groupe de mise à disposition.
- Propriété de visibilité de l'application.

La liste des utilisateurs qui peuvent accéder à une application via StoreFront est constituée à partir de l'intersection des listes utilisateur ci-dessus. Par exemple, pour configurer l'utilisation d'une application A pour un département particulier, sans pour autant limiter l'accès à d'autres groupes :

- utiliser la règle de stratégie d'admissibilité d'application par défaut qui inclut tout le monde ;
- Configurez la liste des utilisateurs du groupe de mise à disposition pour autoriser les utilisateurs du siège social à utiliser toutes les applications spécifiées dans le groupe de mise à disposition.
- Configurez la liste des utilisateurs du groupe d'applications pour permettre aux membres du département Administration et Finances d'accéder aux applications A à L.
- Configurez les propriétés de l'application A pour limiter sa visibilité uniquement au personnel des comptes clients du département Administration et Finances.

À savoir :

- Par défaut, les applications que vous ajoutez sont placées dans un dossier nommé Applications. Vous pouvez spécifier un dossier différent. Si vous essayez d'ajouter une application et qu'une application avec le même nom existe déjà dans ce dossier, vous êtes invité à renommer l'application que vous ajoutez. Si vous acceptez le nom unique suggéré, l'application est ajoutée avec ce nouveau nom ; sinon, vous devez la renommer vous-même avant de pouvoir l'ajouter. Pour de plus amples informations, consultez la section Gérer les dossiers d'applications.
- Vous pouvez modifier les propriétés d'une application (paramètres) lorsque vous l'ajoutez ou ultérieurement. Voir la section Modifier les propriétés de l'application. Si vous publiez deux applications du même nom vers les mêmes utilisateurs, modifiez la propriété Nom de l'application (pour l'utilisateur) dans Studio ; sinon, les utilisateurs verront des noms en double s'afficher dans Citrix Receiver.
- Lorsque vous ajoutez une application à plusieurs groupes d'applications, vous risquez de rencontrer un problème de visibilité si vous ne disposez pas d'autorisations suffisantes pour afficher l'application dans tous ces groupes. Dans ce cas, consultez un administrateur disposant des autorisations appropriées ou demandez une extension de vos autorisations à tous les groupes auxquels l'application a été ajoutée.

Cliquez sur la liste déroulante **Ajouter** pour afficher les sources des applications.

Source	Description
À partir du menu Démarrer	Applications qui sont découvertes sur une machine dans les groupes de mise à disposition sélectionnés. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des applications découvertes. Sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**. Cette source ne peut pas être sélectionnée si vous avez (1) sélectionné des groupes

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	d'applications qui ne sont associés à aucun groupe de mise à disposition, (2) sélectionné des groupes d'applications avec des groupes de mise à disposition associés qui ne contiennent aucune machine, ou (3) sélectionné un groupe de mise à disposition ne contenant aucune machine.
Manuellement définies	Applications qui se trouvent dans le site ou ailleurs dans votre réseau. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez taper le chemin d'accès de l'exécutable, le répertoire de travail, les arguments de la ligne de commande (facultatifs), et les noms affichés des administrateurs et des utilisateurs. Après avoir entré ces informations, cliquez sur **OK**.
Machines existantes	Applications déjà ajoutées au site. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des applications découvertes. Sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**. Cette source ne peut pas être sélectionnée si le site ne dispose d'aucune application.
App-V	Applications dans des packages App-V. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez sélectionner le serveur App-V ou la bibliothèque d'applications. À partir de l'écran qui s'affiche, sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**. Pour plus d'informations, veuillez consulter l'article App-V. Cette source ne peut pas être sélectionnée (ou peut ne pas s'afficher) lorsque App-V n'est pas configuré pour le site.

Comme indiqué, certaines sources dans la liste déroulante **Ajouter** ne peuvent pas être sélectionnées s'il n'existe source valide de ce type. Les sources qui ne sont pas compatibles ne sont pas répertoriées (par exemple, vous ne pouvez pas ajouter de groupe d'applications à des groupes d'applications), par conséquent la source n'est pas répertoriée lorsque vous créez un groupe d'applications.

Cette page s'affiche uniquement si vous avez déjà créé une étendue. Par défaut, l'étendue **Tout** est sélectionnée. Pour plus d'informations, veuillez consulter l'article Administration déléguée.

Entrez un nom pour le groupe d'applications. Vous pouvez également entrer une description (facultatif).

Consultez les informations récapitulatives, puis cliquez sur **Terminer**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Gérer des groupes d'applications

Jul 07, 2016

Dans cet article :

- Introduction
- Activer ou désactiver un groupe d'applications
- Activer ou désactiver le partage de session d'application entre des groupes d'applications
- Renommer un groupe d'applications
- Ajouter, supprimer ou modifier la priorité d'associations de groupe de mise à disposition avec un groupe d'applications
- Ajouter ou supprimer des utilisateurs d'un groupe d'applications
- Modifier les étendues dans un groupe d'applications
- Supprimer un groupe d'applications

Introduction

Cet article décrit comment gérer les groupes d'applications que vous avez créés.

Consultez l'article Applications pour savoir comment gérer les applications de groupes d'applications ou de groupes de mise à disposition, notamment comment :

- Ajouter ou supprimer des applications d'un groupe d'applications
- Modifier les associations de groupe d'une application

La gestion des groupes d'applications nécessite les autorisations d'administration déléguée du rôle intégré d'administrateur de groupe de mise à disposition. Consultez l'article Administration déléguée pour plus de détails.

Activer ou désactiver un groupe d'applications

Lorsqu'un groupe d'applications est activé, il peut mettre à disposition les applications qui lui ont été ajoutées. La désactivation d'un groupe d'applications désactive chaque application dans ce groupe. Cependant, si ces applications sont également associées à d'autres groupes d'applications activés, elles peuvent être mises à disposition à partir de ces groupes. De même, si l'application a été expressément ajoutée à des groupes de mise à disposition associés au groupe d'applications (en plus d'être ajoutée au groupe d'applications), la désactivation du groupe d'applications n'affecte pas les applications dans ces groupes de mise à disposition.

Un groupe d'applications est activé lorsque vous le créez ; vous ne pouvez pas changer ce paramètre lors de la création du groupe.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Modifier groupe d'applications** dans le volet Actions.
3. Sur la page **Paramètres**, sélectionnez ou désélectionnez la case à cocher **Activer groupe d'applications**.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Activer ou désactiver le partage de session d'application entre des groupes d'applications

Le partage de session entre des groupes d'applications est activé lorsque vous créez un groupe d'applications ; vous ne pouvez pas changer ce paramètre lors de la création du groupe. Pour de plus amples informations sur le partage de session d'application, consultez la section Partage de session entre des groupes d'application.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Modifier groupe d'applications** dans le volet Actions.
3. Sur la page **Paramètres**, sélectionnez ou désélectionnez la case à cocher **Activer le partage de session d'application entre les groupes d'applications**.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Renommer un groupe d'applications

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Renommer groupe d'applications** dans le volet Actions.
3. Spécifiez le nouveau nom unique puis cliquez sur **OK**.

Ajouter, supprimer ou modifier la priorité d'associations de groupe de mise à disposition avec un groupe d'applications

Un groupe d'applications peut être associé à des groupes de mise à disposition contenant des machines partagées (non privées) qui peuvent mettre à disposition des applications.

Vous pouvez également sélectionner des groupes de mise à disposition contenant des machines partagées qui mettent uniquement à disposition des bureaux, si (1) le groupe de mise à disposition contient des machines partagées et a été créé avec une version antérieure de XenDesktop 7.x, et (2) vous disposez de l'autorisation Modifier le groupe de mise à disposition. Le type de groupe de mise à disposition est automatiquement converti en « bureaux et applications » lorsque la boîte de dialogue Modifier groupe d'applications est validée.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Modifier groupe d'applications** dans le volet Actions.
3. Sélectionnez la page **Groupes de mise à disposition**.
4. Pour ajouter des groupes de mise à disposition, cliquez sur **Ajouter**. Sélectionnez les cases à cocher des groupes de mise à disposition disponibles. (Les groupes de mise à disposition non compatibles ne peuvent pas être sélectionnés). Lorsque

© 1999-2017 Citrix Systems, Inc. All rights reserved.

vous avez terminé vos sélections, cliquez sur **OK**.

5. Pour supprimer des groupes de mise à disposition, sélectionnez les cases à cocher des groupes que vous souhaitez supprimer, puis cliquez sur **Supprimer**. Confirmez la suppression lorsque vous y êtes invité.
6. Pour modifier la priorité de groupes de mise à disposition, sélectionnez la case à cocher du groupe de mise à disposition et cliquez sur **Modifier la priorité**. Entrez la priorité (0 = priorité la plus élevée), puis cliquez sur **OK**.
7. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Ajouter ou supprimer des utilisateurs d'un groupe d'applications

Pour de plus amples informations sur les utilisateurs, consultez la section Utilisateurs dans l'article Créer des groupes de mise à disposition.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Modifier groupe d'applications** dans le volet Actions.
3. Sélectionnez la page **Utilisateurs**. Indiquez si vous souhaitez autoriser tous les utilisateurs dans les groupes de mise à disposition associés à utiliser les applications du groupe d'applications, ou uniquement des utilisateurs et groupes spécifiques. Pour ajouter des utilisateurs, cliquez sur **Ajouter**, puis spécifiez les utilisateurs que vous souhaitez ajouter. Pour supprimer des utilisateurs, sélectionnez un ou plusieurs utilisateurs, puis cliquez sur **Supprimer**.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Modifier les étendues dans un groupe d'applications

Vous pouvez modifier une étendue uniquement si vous avez créé une étendue (vous ne pouvez pas modifier l'étendue Tout). Pour plus d'informations, veuillez consulter l'article Administration déléguée.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Modifier groupe d'applications** dans le volet Actions.
3. Sélectionnez la page **Étendues**. Cochez ou décochez la case à cocher en regard d'une étendue.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Supprimer un groupe d'applications

Une application doit être associée à au moins un groupe de mise à disposition ou groupe d'applications. Si votre tentative de suppression d'un groupe d'applications a pour conséquence qu'une ou plusieurs applications n'appartiennent plus à un groupe, vous serez averti que la suppression de ce groupe supprimera également ces applications. Vous pouvez ensuite confirmer ou annuler la suppression.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

La suppression d'une application ne la supprime pas de sa source d'origine, mais si vous souhaitez de nouveau la rendre disponible, vous devez l'ajouter à nouveau.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Supprimer le groupe** dans le volet Actions.
3. Confirmez la suppression lorsque vous y êtes invité.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Remote PC Access

Jul 07, 2016

Remote PC Access permet à un utilisateur final d'ouvrir une session à distance pratiquement depuis n'importe quel emplacement sur le PC Windows physique au bureau.

> ## Important
>
> Dans XenApp et XenDesktop 7.9, utilisez uniquement la ligne de commande pour les déploiements Remote PC Access. Pour de plus amples informations, consultez les sections Installer à l'aide de la ligne de commande et Problèmes connus [#637741].

Virtual Delivery Agent (VDA) est installé sur le PC de bureau ; il s'enregistre auprès du Delivery Controller et permet de gérer la connexion HDX entre le PC et les machines clientes de l'utilisateur final. Remote PC Access prend en charge un modèle en libre-service, après avoir configuré la liste blanche des machines auxquelles les utilisateurs sont autorisés à accéder, les utilisateurs peuvent joindre leurs PC de bureau à un site d'eux-mêmes, sans l'intervention de l'administrateur. Le Citrix Receiver exécuté sur leur machine cliente permet d'accéder aux applications et données sur le PC de bureau à partir de la session de bureau Remote PC Access.

Il se peut qu'un utilisateur possède plusieurs bureaux, y compris plus d'un PC physique ou une combinaison de PC physiques et de bureaux virtuels.

Remarque : le mode Veille et Veille prolongée n'est pas pris en charge pour Remote PC Access. Remote PC Access est uniquement valide pour les licences XenDesktop ; les sessions consomment des licences de la même manière que d'autres sessions XenDesktop.

Considérations relatives à Active Directory

Avant de configurer le site de déploiement de Remote PC Access, configurez vos unités d'organisation (OU) et groupes de sécurité puis créez des comptes d'utilisateur. Utilisez ces comptes pour spécifier les utilisateurs pour les groupes de mise à disposition que vous utiliserez pour fournir Remote PC Access.

Si vous modifiez Active Directory après l'ajout d'une machine à un catalogue de machines, Remote PC Access ne réévalue pas cette affectation. Vous pouvez réaffecter manuellement une machine à un autre catalogue, si nécessaire.

Si vous déplacez ou supprimez des unités d'organisation, celles utilisées pour Remote PC Access peuvent devenir obsolètes. VDA risque de ne plus être associé avec le catalogue de machines ou le groupe de mise à disposition le plus approprié (le cas échéant).

Considérations de catalogue de machines et groupes de mise à disposition :

Une machine peut uniquement être attribuée à un catalogue de machines et un groupe de mise à disposition à la fois.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Vous pouvez placer les machines dans un ou plusieurs des catalogues de machines Remote PC Access.

Lors du choix des comptes de machines pour un catalogue de machines, sélectionnez la plus basse unité d'organisation (OU) applicable afin d'éviter des conflits potentiels avec des machines d'un autre catalogue de machines. Par exemple, dans le cas d'employés de banque, sélectionnez Guichets.

Vous pouvez affecter toutes les machines d'un catalogue de machines Remote PC Access via un ou plusieurs groupes de mise à disposition. Si vous disposez d'un groupe d'utilisateurs qui nécessite certains paramètres de stratégie et d'un autre groupe d'utilisateurs qui requiert des paramètres différents, l'attribution d'utilisateurs à différents groupes de mise à disposition vous permet de filtrer les stratégies HDX en fonction de chaque groupe de mise à disposition.

Si votre infrastructure informatique attribue une responsabilité pour traiter les utilisateurs en fonction de leur emplacement géographique, département, ou une autre catégorie, vous pouvez grouper les machines et les utilisateurs en conséquence afin de permettre l'administration déléguée. Assurez-vous que chaque administrateur dispose des permissions nécessaires pour les catalogues de machines et les groupes de mise à disposition correspondants.

Pour les utilisateurs équipés de PC de bureau exécutant Windows XP, créez un catalogue de machines et un groupe de mise à disposition distincts pour ces systèmes. Lors du choix des comptes de machine pour ce catalogue dans Studio, sélectionnez la case à cocher indiquant que certaines machines exécutent Windows XP.

Considérations de déploiement

Vous pouvez créer un déploiement Remote PC Access, puis ajouter des bureaux ou applications VDI (Virtual Desktop Infrastructure) traditionnelles ultérieurement. Vous pouvez également ajouter des bureaux Remote PC Access à un déploiement VDI existant.

Considérez l'activation de la fonction Assistance à distance de Windows lorsque vous installez le VDA sur le PC de bureau. Cette option permet aux équipes d'assistance utilisant Director d'afficher une session utilisateur et d'interagir avec elle via l'Assistance à distance Windows.

Déterminez la manière dont vous souhaitez déployer le VDA sur chaque PC de bureau. Citrix vous recommande d'utiliser la distribution électronique de logiciels telle que des scripts Active Directory et Microsoft System Center Configuration Manager. Le support d'installation contient des exemples de scripts Active Directory.

Consultez les considérations de sécurité pour les déploiements Remote PC Access.

Le démarrage sécurisé pour Remote PC Access est pris en charge sur Windows 10 et 8.1. Désactivez le démarrage sécurisé si vous prévoyez de déployer le poste de travail VDA sur un autre système d'exploitation.

Chaque PC de bureau doit être membre d'un domaine avec une connexion réseau câblée.

Windows 7 Aero est pris en charge sur le PC de bureau, mais n'est pas obligatoire.

Connectez le clavier et la souris directement sur l'ordinateur ou sur un ordinateur portable, mais pas sur le moniteur ou autres composants qui peuvent être éteints. Si vous devez connecter des périphériques d'entrée pour les composants tels que les moniteurs, ils ne doivent pas être éteints.

Si vous utilisez des cartes à puce, consultez la section Cartes à puce.

Remote PC Access peut être utilisé sur la plupart des ordinateurs portables. Pour améliorer l'accessibilité et offrir la meilleure

© 1999-2017 Citrix Systems, Inc. All rights reserved.

expérience de connexion possible, configurez les options d'économie d'énergie de l'ordinateur portable sur celles d'un PC de bureau. Par exemple :

- Désactivez la fonctionnalité Veille prolongée.
- Désactivez la fonctionnalité Veille.
- Définissez l'action de fermeture de l'écran sur Ne rien faire.
- Définissez l'action d'appuyer sur le bouton d'alimentation sur Arrêter.
- Désactivez les fonctionnalités d'économie d'énergie de la carte vidéo.
- Désactivez les fonctionnalités d'économie d'énergie de la carte d'interface réseau.
- Désactivez les technologies d'économie de la batterie.

Les éléments suivants ne sont pas pris en charge pour les machines Remote PC Access :

- Ancrage et retrait de l'ordinateur portable.
- Commutateurs KVM ou autres composants qui peuvent déconnecter une session.
- PC hybride, y compris PC et ordinateurs portables tout en un et NVIDIA Optimus.

Remote PC Access peut être utilisé sur la plupart des machines Surface Pro. XenDesktop 7.9 Citrix prend en charge Remote PC Access sur les machines Surface Pro avec Windows 8.1 ou 10. Pour améliorer l'accessibilité et offrir la meilleure expérience de connexion possible, configurez la machine Surface de manière similaire à un ordinateur portable ou de bureau. Par exemple :

- Désactiver la fonctionnalité de mise en veille ou veille prolongée
- Utiliser une connexion réseau filaire
- Toujours garder le clavier attaché lors de l'initiation ou de la reconnexion à une session
- Désactiver les technologies d'économie de la batterie

Installez Citrix Receiver sur chaque machine cliente qui accède au PC de bureau à distance.

Plusieurs utilisateurs avec l'accès distant au même PC de bureau voient la même icône dans Citrix Receiver. Lorsqu'un utilisateur ouvre une session à distance sur le PC, cette ressource est marquée comme non disponible pour d'autres utilisateurs.

Par défaut, une session d'utilisateur distant est automatiquement déconnectée lorsqu'un utilisateur local initie une session sur cette machine (en appuyant sur CTRL+ALT+Suppr). Pour éviter cette action automatique, ajoutez l'entrée de registre suivante sur le PC de bureau, puis redémarrez la machine.

> **Avertissement :** la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.
>
> HKLM\SOFTWARE\Citrix\PortICA\RemotePC "SasNotification"=dword:00000001
>
> Pour personnaliser le comportement de cette fonctionnalité sous HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\Remote PC
>
> RpcaMode (dword) :
>
> 1 = L'utilisateur distant aura toujours priorité s'il ne répond pas à l'interface utilisateur de messagerie dans le délai imparti.
>
> 2 = L'utilisateur local aura toujours priorité. Si ce paramètre n'est pas spécifié, l'utilisateur distant aura toujours priorité par défaut.
>
> RpcaTimeout (dword) :
>
> Nombre de secondes accordées à l'utilisateur avant que le type de mode à appliquer soit déterminé. Si ce paramètre n'est pas spécifié, la valeur par défaut est 30 secondes. La valeur minimale doit être 30 secondes. L'utilisateur doit redémarrer la machine pour que ces modifications soient

© 1999-2017 Citrix Systems, Inc. All rights reserved.

appliquées.

Lorsque l'utilisateur souhaite forcer l'accès à la console : l'utilisateur local peut appuyer sur Ctr+Alt+Suppr à deux reprises à intervalle de 10 secondes pour obtenir le contrôle local d'une session distante et forcer une déconnexion.

Une fois le Registre modifié et la machine redémarrée, si un utilisateur local appuie sur CTRL+ALT+Suppr pour ouvrir une session sur ce PC lorsqu'il est en cours d'utilisation par un utilisateur distant, cet utilisateur reçoit une invite lui demandant s'il souhaite ou non autoriser ou refuser la connexion de l'utilisateur local. L'action d'autorisation de la connexion déconnectera la session de l'utilisateur distant.

Remote PC Access et mode HDX 3D Pro

Pour Remote PC Access, le VDA est généralement configuré à l'aide de l'option VDA standard. Lorsque Remote PC Access est configuré avec HDX 3D Pro, l'occultation de moniteur est prise en charge avec Intel Iris Pro Graphics et Intel HD Graphics 5300 et supérieur (Processeurs Intel Core 5ème Génération et Processeurs Intel Core i5 6ème Génération), et NVIDIA Quadro et NVIDIA GRID

Pour de plus amples informations, consultez les sections Préparer l'installation et Accélération GPU pour OS de bureau Windows.

Wake on LAN

Remote PC Access prend en charge Wake on LAN, qui donne aux utilisateurs la possibilité d'activer des ordinateurs physiques à distance. Cette fonctionnalité permet aux utilisateurs de garder leur PC de bureau éteint lorsqu'il n'est pas en cours d'utilisation, et d'économiser de l'énergie. Il offre également un accès distant quand une machine a été éteinte par inadvertance, tel que lors d'événements météo.

La fonctionnalité Remote PC Access Wake on LAN est prise en charge sur les deux systèmes suivants :

- PC qui prennent en charge la technologie AMT (Intel Active Management)
- PC sur lesquels l'option Wake on LAN est activée dans le BIOS

Vous devez configurer Microsoft System Center Configuration Manager (ConfigMgr) 2012 pour utiliser la fonctionnalité Wake on LAN. ConfigMgr fournit un accès pour invoquer les commandes de mise sous tension AMT pour le PC, ainsi qu'une prise en charge du proxy de mise en éveil et des paquets magiques. Ensuite, lorsque vous utilisez Studio pour créer un déploiement Remote PC Access (ou lorsque vous ajoutez une autre connexion de gestion de l'alimentation à utiliser pour Remote PC Access), vous activez la gestion de l'alimentation et spécifiez des informations d'accès ConfigMgr.

Autres tâches :

- L'utilisation des opérations de mise sous tension AMT sont préférées pour des questions de sécurité et de fiabilité ; toutefois, la prise en charge est également fournie pour deux méthodes non AMT : ConfigMgr Wake Proxy et les paquets magiques bruts.
- Sur les machines compatibles AMT uniquement, la fonctionnalité Wake on LAN prend également en charge les actions Forcer l'arrêt et Forcer le redémarrage dans Studio et Director. En outre, une action de redémarrage est disponible dans StoreFront et Receiver.

Pour de plus amples informations, consultez Configuration Manager et Remote PC Access Wake on LAN.

Pour de plus amples informations sur le SDK Wake on LAN d'évaluation, qui vous permet, à vous ou à une solution Wake on LAN tierce, de créer un connecteur sans l'utilisation de System Center 2012 R2, consultez la section CTX202272. Le SDK Wake on LAN de cette version est disponible à des fins d'évaluation uniquement, et non à des fins d'utilisation dans un

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

environnement de production.

Séquence de configuration et considérations

Avant de créer le site Remote PC Access :

Si vous prévoyez d'utiliser la fonctionnalité de gestion de l'alimentation Remote PC Access (également appelée Remote PC Access Wake on LAN), effectuez les tâches de configuration sur les PC et sur Microsoft System Center Configuration Manager (ConfigMgr) 2012 avant de créer le déploiement Remote PC Access dans Studio. Consultez la section Configuration Manager et Remote PC Access Wake on LAN pour de plus amples informations.

Dans l'Assistant de création de site :

- Sélectionnez le type de site Remote PC Access.
- Sur la page Gestion de l'alimentation, vous pouvez activer ou désactiver la gestion de l'alimentation pour les machines dans le catalogue de machines Remote PC Access par défaut. Si vous activez la gestion de l'alimentation, spécifiez les informations de connexion ConfigMgr.
- Sur les pages Utilisateurs et Comptes de machines, spécifiez les utilisateurs et les comptes de machines.

La création d'un site Remote PC Access crée un catalogue de machines appelé Machines Remote PC Access et un groupe de mise à disposition par défaut appelé Bureaux Remote PC Access.

Si vous créez un autre catalogue de machines pour une utilisation avec Remote PC Access :

- Sur la page Système d'exploitation, sélectionnez Remote PC Access, puis choisissez une connexion de gestion de l'alimentation. Vous pouvez également choisir de ne pas utiliser la gestion de l'alimentation. S'il n'existe aucune connexion de gestion de l'alimentation configurée, vous pouvez en ajouter une à la fin de l'Assistant de création de catalogue de machines (type de connexion = Microsoft Configuration Manager Wake on LAN), puis modifiez le catalogue de machines, en spécifiant cette nouvelle connexion.
- Sur la page Comptes de machines, vous pouvez sélectionner les comptes de machines ou les unités d'organisation (UO) affichés, ou ajouter des comptes de machines et des unités d'organisation.

Installez le VDA sur les PC de bureau utilisés pour un accès local et distant. En général, vous pouvez déployer le VDA automatiquement à l'aide de votre logiciel de gestion de pack ; cependant, pour les déploiements d'évaluation ou de petite taille, vous pouvez installer le VDA manuellement sur chaque PC de bureau.

Lors de l'installation du VDA à partir de la ligne de commande, incluez l'option **/remotepc**. Cela empêche l'installation des composants suivants sur un OS de bureau (poste de travail) :

- Composant App V : Citrix Personalization for App-V - VDA
- Composant Upm : Citrix User Profile Manager
- Composant UpmVdaPlugin : Citrix User Profile Manager WMI Plugin
- Composant Mps : Machine Identity Service
- Composant VDisk : Personal vDisk

Durant une mise à niveau, si l'un des composants ci-dessus est installé, il sera détecté et mis à niveau par le programme d'installation.

Une fois le VDA installé, le prochain utilisateur de domaine qui ouvre une session de console (localement ou via RDP) sur le

© 1999-2017 Citrix Systems, Inc. All rights reserved.

PC de bureau est automatiquement affecté au bureau Remote PC Access. Si des utilisateurs de domaine supplémentaires se connectent à une session de console, ils sont également ajoutés à la liste des utilisateurs de bureau, en fonction des restrictions que vous avez configurés.

Pour utiliser des connexions RDP en dehors de votre environnement XenApp ou XenDesktop, vous devez ajouter des utilisateurs ou des groupes au groupe d'utilisateurs de l'accès direct.

Demandez aux utilisateurs de télécharger et d'installer Citrix Receiver sur chaque machine cliente qu'ils utiliseront pour accéder à distance au PC de bureau. Citrix Receiver est disponible depuis http://www.citrix.com où depuis le système de distribution d'application des appareils mobiles pris en charge.

Configurer les paramètres de connexion avancés

Vous pouvez modifier une connexion de gestion de l'alimentation pour configurer les paramètres avancés. Vous pouvez activer :

- le proxy de mise en éveil mis à disposition par ConfigMgr ;
- les paquets Wake on LAN (magiques). Si vous activez les paquets Wake on LAN, vous pouvez sélectionner une méthode de transmission Wake on LAN : émissions ou monodiffusions dirigées par des sous-réseaux.

Le PC utilise des commandes de mise sous tension AMT (si prises en charge), ainsi que tout paramètre avancé activé. Si le PC n'utilise pas de commandes de mise sous tension AMT, il utilise les paramètres avancés.

Résolution des problèmes

Delivery Controller inscrit les informations de diagnostic suivantes sur Remote PC Access dans le Journal d'événements d'application Windows. Les messages d'informations ne sont pas optimisés. Les messages d'erreur sont optimisés en éliminant les messages en double.

- 3300 (informations) : machine ajoutée au catalogue
- 3301 (informations) : machine ajoutée au groupe de mise à disposition
- 3302 (informations) : machine attribuée à l'utilisateur
- 3303 (erreur) : exception

Lorsque la gestion de l'alimentation est activée pour Remote PC Access, il se peut que des diffusions dirigées par des sous-réseaux ne parviennent pas à démarrer des machines qui sont situées sur un sous-réseau différent du Controller. Si vous avez besoin de la gestion de l'alimentation sur les sous-réseaux utilisant des diffusions dirigées par des sous-réseaux et AMT n'est pas disponible, essayez la méthode du proxy de mise en éveil ou de monodiffusion (assurez-vous que ces paramètres sont activés dans les propriétés avancées de la connexion de gestion de l'alimentation).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

App-V

Jul 07, 2016

Utilisation de App-V avec XenApp et XenDesktop

La Virtualisation d'application Microsoft (App-V) vous permet de déployer, mettre à jour et prendre en charge des applications en tant que services. Les utilisateurs accèdent aux applications sans les installer sur leur propre machine. App-V et Microsoft User State Virtualization (USV) fournissent l'accès aux applications et aux données, quel que soit l'emplacement et la connexion à Internet.

Le tableau suivant répertorie les versions prises en charge.

App-V	Versions XenDesktop et XenApp	
	Delivery Controller	VDA
5.0 et 5.0 SP1	XenDesktop 7 jusqu'à la version actuelle XenApp 7.5 jusqu'à la version actuelle	7.0 jusqu'à la version actuelle
5.0 SP2	XenDesktop 7 jusqu'à la version actuelle XenApp 7.5 jusqu'à la version actuelle	7.1 jusqu'à la version actuelle
5.0 SP3 et 5.1	XenDesktop 7.6 jusqu'à la version actuelle XenApp 7.6 jusqu'à la version actuelle	7.6 300 jusqu'à la version actuelle

Le client App-V ne prend pas en charge l'accès en mode déconnecté aux applications. La prise en charge de l'intégration App-V comprend l'utilisation de partages SMB pour les applications ; le protocole HTTP n'est pas pris en charge.

Si vous n'êtes pas un utilisateur expérimenté de App-V, veuillez consulter la documentation Microsoft. Voici un récapitulatif des composants App-V mentionnés dans cet article :

- **Serveur d'administration**. Fournit une console centralisée de gestion de l'infrastructure App-V et met à disposition des applications virtuelles pour le client de bureau App-V ainsi qu'un client aux services Bureau à distance. Le serveur d'administration App-V authentifie, requiert et fournit la sécurité, les mesures, la surveillance et la collecte des données requis par l'administrateur. Le serveur utilise Active Directory et ses outils de soutien pour gérer les utilisateurs et les applications.
- **Serveur de publication**. Fournit des clients App-V avec des applications pour certains utilisateurs, et héberge le pack

© 1999-2017 Citrix Systems, Inc. All rights reserved.

d'application virtuelle en vue du streaming. Il récupère les packs depuis le serveur d'administration.

- **Client**. Récupère des applications virtuelles, publie les applications sur le client et configure et gère automatiquement les environnements virtuels au moment de l'exécution sur les machines Windows. Vous installez le client App-V sur le VDA où il stocke les paramètres d'application virtuelle spécifiques à l'utilisateur, tels que le registre et les modifications apportées aux fichiers dans chaque profil utilisateur.

Les applications sont disponibles en toute transparence sans pré-configuration ou modifications apportées aux paramètres du système d'exploitation. Vous pouvez lancer les applications App-V à partir de machines avec OS de serveur et les groupes de mise à disposition avec OS de bureau :

- Via Citrix Receiver
- Depuis le menu Démarrer
- Via le client App-V et Citrix Receiver
- Simultanément par de multiples utilisateurs sur plusieurs machines
- Via Citrix StoreFront

Les propriétés de l'application App-V modifiées sont implémentées lorsque l'application est démarrée. Par exemple, pour les applications avec un nom d'affichage ou une icône personnalisée modifié(e), la modification s'affiche lorsque les utilisateurs démarrent l'application.

Vous pouvez utiliser des packages App-V créés avec App-V Sequencer puis placés sur des serveurs App-V ou des partages réseau.

- **Serveurs App-V** : l'utilisation d'applications depuis des packages situés sur des serveurs App-V requiert une communication constante entre Studio et les serveurs App-V pour la découverte, la configuration et le téléchargement vers les VDA. Cela entraîne des frais de matériel, d'infrastructure et d'administration. Studio et les serveurs App-V doivent rester synchronisés, particulièrement pour les permissions utilisateur.

  Cette méthode de gestion est appelée *double administration* car l'accès aux packages et aux applications App-V requiert à la fois Studio et les consoles du serveur App-V. Cette méthode fonctionne mieux dans des déploiements App-V et Citrix étroitement liés.

- **Partage réseau** : avec les packages placés sur un partage réseau, Studio ne dépend plus de l'infrastructure serveur App-V et base de données, ce qui diminue les frais (vous devez quand même installer le client Microsoft App-V sur chaque VDA.).

  Cette méthode de gestion est appelée *administration unique* car l'utilisation des packages et des applications App-V requiert uniquement la console Studio. Vous accédez au partage réseau et vous ajoutez un ou plusieurs packages App-V à partir de cet emplacement de la bibliothèque d'applications au niveau du site.

  La bibliothèque d'applications est un terme Citrix désignant un référentiel de mise en cache qui stocke des informations sur les packages App-V. La bibliothèque d'applications stocke également des informations sur les autres technologies de mise à disposition d'applications Citrix.

Vous pouvez utiliser une ou les deux méthodes de gestion simultanément. En d'autres termes, lorsque vous ajoutez des applications aux groupes de mise à disposition, les applications peuvent provenir de packages App-V situés sur des serveurs App-V et/ou sur un partage réseau.

Lorsque vous sélectionnez **Configuration > App-V Publishing** dans le panneau de navigation de Studio, l'écran affiche les

© 1999-2017 Citrix Systems, Inc. All rights reserved.

noms et les sources des packages App-V. La colonne Source indique si les packages sont situés sur le serveur App-V ou mis en cache dans la bibliothèque d'applications. Lorsque vous sélectionnez un package, le panneau Détails répertorie les applications contenues dans le package.

Installation

Le tableau suivant décrit la séquence de tâches de configuration permettant d'utiliser App-V dans XenApp et XenDesktop.

Méthode de gestion		Tâche
Administration unique	Double administration	
X	X	Déployer App-V
X	X	Création de packages et placement
	X	Configurer des adresses de serveurs App-V dans Studio
X	X	Installer le logiciel sur des machines VDA
X		Ajouter des packages App-V à la bibliothèque d'applications
X	X	Ajouter des applications App-V aux groupes de mise à disposition

Pour obtenir des instructions sur le déploiement de App-V, consultez http://technet.microsoft.com/en-us/virtualization/hh710199.

Si vous le souhaitez, vous pouvez modifier les paramètres de serveur de publication App-V. Citrix vous recommande d'utiliser les applets de commande du SDK sur le Controller ; consultez la documentation du SDK pour plus de détails.

- Pour afficher les paramètres de serveur de publication, entrez **Get-CtxAppvServerSetting -AppVPublishingServer** <*pubServer*>.
- Pour vous assurer que les applications App-V démarrent correctement, entrez **Set-CtxAppvServerSetting –UserRefreshonLogon 0**.

Si vous avez préalablement utilisé des paramètres d'objet de stratégie de groupe pour gérer les paramètres du serveur de publication, ces paramètres remplacent les paramètres d'intégration App-V, y compris les paramètres de l'applet de commande. Cela peut entraîner l'échec de lancement de l'application App-V. Citrix vous recommande de supprimer tous les paramètres de stratégie d'objet de stratégie de groupe, puis d'utiliser le kit de développement pour configurer ces paramètres.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Quelle que soit la méthode de gestion, créez les packages d'applications à l'aide de App-V Sequencer. Reportez-vous à la documentation Microsoft pour plus d'informations.

- Dans le cas d'une administration unique, assurez-vous que les packages sont disponibles sur un emplacement réseau partagé UNC ou SMB. Assurez-vous que l'administrateur Studio qui ajoute des applications aux groupes de mise à disposition possède au moins un accès en lecture à cet emplacement.
- En cas de double administration, publiez les packages sur le serveur de gestion App-V.

Que les packages se trouvent sur le serveur App-V ou sur un partage réseau, assurez-vous qu'ils possèdent les autorisations de sécurité appropriées pour permettre à l'administrateur Studio d'y accéder.

Cette procédure est valide uniquement pour la méthode de gestion « double administration ».

Spécifiez les adresses des serveurs de gestion et de publication App-V pour la double administration pendant ou après la création du site. Vous pouvez effectuer cette opération pendant ou après la création du site.

Lors de la création du site :

Sur la page **App-V** de l'assistant, entrez l'adresse URL du serveur de gestion Microsoft App-V et l'adresse URL et le numéro de port du serveur de publication App-V. Testez la connexion avant de continuer avec l'assistant. Si le test échoue, veuillez consulter la section Dépannage ci-dessous.

Après la création du site :

1. Sélectionnez **Configuration > App-V Publishing** dans le panneau de navigation de Studio.
2. Si vous n'avez pas spécifié d'adresse de serveur App-V précédemment, sélectionnez **Ajouter Microsoft Server** dans le panneau Actions.
3. Pour modifier des adresses de serveur App-V précédemment, sélectionnez **Modifier Microsoft Server** dans le panneau Actions.
4. Entrez l'URL du serveur de gestion Microsoft App-V ainsi que l'URL et le numéro de port du serveur de publication App-V.
5. Testez la connexion à ces serveurs avant de fermer la boîte de dialogue. Si le test échoue, veuillez consulter la section Dépannage ci-dessous.

Plus tard, si vous souhaitez supprimer tous les liens vers les serveurs de gestion et de publication App-V et empêcher Studio de découvrir des packages App-V à partir de ces serveurs, sélectionnez **Supprimer Microsoft Server** dans le panneau Actions. Cette action est autorisée uniquement si aucune des applications des packages situés sur ces serveurs n'est actuellement publiée dans des groupes de mise à disposition. Si c'est le cas, vous devez supprimer ces applications des groupes de mise à disposition avant de pouvoir supprimer les serveurs App-V.

Les machines contenant des VDA doivent disposer de deux ensembles de logiciels pour prendre en charge App-V : un ensemble fourni par Microsoft et l'autre par Citrix.

Client Microsoft App-V

Ce logiciel récupère des applications virtuelles, publie les applications sur le client et configure et gère automatiquement les environnements virtuels au moment de l'exécution sur les machines Windows. Le client App-V stocke les paramètres d'application virtuelle spécifiques à l'utilisateur, tels que le registre et les modifications apportées

© 1999-2017 Citrix Systems, Inc. All rights reserved.

aux fichiers dans chaque profil utilisateur.

Le client App-V est disponible auprès de Microsoft. Installez un client sur chaque machine contenant un VDA, ou sur l'image principale qui est utilisée dans un catalogue de machines pour créer des VM.

Conseil : après avoir installé le client App-V, avec des autorisations d'administrateur, exécutez l'applet de commande PowerShell **Get-AppvClientConfiguration** et assurez-vous que EnablePackageScripts est défini sur 1. Si elle n'est pas définie sur 1, exécutez l'applet de commande **Set-AppvClientConfiguration -EnablePackageScripts $true**.

Composants Citrix App-V

Le logiciel Citrix App-V est installé et activé par défaut lorsque vous installez un VDA ; ce processus crée également un compte possédant des autorisations d'administrateur local pour accéder aux composants de publication App-V.

Vous pouvez définir cette action par défaut lors de l'installation du VDA. Dans l'interface graphique, désélectionnez la case **Installer les composants de publication App-V** sur la page **Fonctionnalités**. Dans l'interface de ligne de commande, incluez l'option **/no_appv**.

Si vous désactivez la fonctionnalité des composants Citrix App-V lors de l'installation de VDA, mais souhaitez utiliser les applications App-V ultérieurement : dans la liste Programmes et fonctionnalités de la machine Windows, cliquez avec le bouton droit sur l'entrée **Citrix Virtual Delivery Agent**, puis sélectionnez **Modifier**. Un assistant démarre. Dans l'assistant, activez l'option qui installe et active les composants de publication App-V.

Cette procédure est valide uniquement pour la méthode de gestion « administration unique ».

Vous devez disposer d'au moins un accès en lecture pour le partage réseau contenant les packages App-V.

1. Sélectionnez **Configuration > App-V Publishing** dans le panneau de navigation de Studio.
2. Sélectionnez **Ajouter des packages** dans le volet Actions.
3. Recherchez le partage contenant les packages App-V et sélectionnez un ou plusieurs packages.
4. Cliquez sur **Add**.

La procédure suivante se concentre sur l'ajout d'applications App-V à des groupes de mise à disposition. Pour des informations complètes sur la création d'un groupe de mise à disposition, consultez l'article Créer des groupes de mise à disposition.

Étape 1 : choisissez si vous souhaitez créer un nouveau groupe de mise à disposition ou ajouter des applications App-V à un groupe de mise à disposition existant :

Pour créer un groupe de mise à disposition contenant des applications App-V :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez **Créer un groupe de mise à disposition** dans le volet Actions.
3. Sur les pages successives de l'assistant, spécifiez un catalogue de machines et des utilisateurs.

Pour ajouter des applications App-V à des groupes de mise à disposition existants :

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez **Ajouter des applications** dans le volet Actions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Sélectionnez un ou plusieurs groupes de mise à disposition dans lesquels les applications App-V seront ajoutées.

Étape 2 : sur la page **Applications** de l'assistant, cliquez sur la liste déroulante **Ajouter** pour afficher les sources d'applications. Sélectionnez **App-V**.

Étape 3 : Sur la page **Ajouter des applications App-V**, choisissez la source App-V : le serveur App-V ou la bibliothèque d'applications. L'écran suivant inclut les noms des applications ainsi que le nom de leur package et les versions de package. Cochez les cases en regard des applications que vous souhaitez ajouter. Cliquez ensuite sur **OK**.

Étape 4 : terminez l'assistant.

À savoir :

- Si vous modifiez les propriétés d'une application App-V lorsque vous l'ajoutez à un groupe de mise à disposition, les modifications sont apportées lorsque l'application est démarrée. Par exemple, si vous modifiez le nom d'affichage ou l'icône d'une application lorsque vous l'ajoutez au groupe, la modification est visible lorsque l'utilisateur démarre l'application.
- Si vous modifiez ultérieurement un groupe de mise à disposition contenant des applications App-V, les performances des applications App-V ne changent pas si vous modifiez le type de groupe de mise à disposition de « bureaux et applications » vers « applications uniquement ».

Supprimer des packages App-V de la bibliothèque d'applications

La suppression d'un package App-V de la bibliothèque d'applications le supprime de l'affichage du nœud App-V Publishing dans Studio ; toutefois, elle ne supprime pas ses applications des groupes de mise à disposition et ces applications peuvent encore être lancées. Le package reste dans son emplacement réseau physique (cette opération diffère de la suppression d'une application App-V d'un groupe de mise à disposition).

1. Sélectionnez **Configuration > App-V Publishing** dans le panneau de navigation de Studio.
2. Sélectionnez un ou plusieurs packages à supprimer.
3. Cliquez sur **Supprimer le package** dans le volet Actions.

Dépannage

Les problèmes qui peuvent se produire uniquement lors de l'utilisation du mode « double administration » sont indiqués par la mention (DOUBLE).

(DOUBLE) L'opération de test de la connexion a renvoyé une erreur lorsque vous spécifiez des adresses de serveur App-V dans Studio.

- Le serveur App-V est-il sous tension ? Envoyez une commande Ping ou vérifiez le Gestionnaire des services IIS ; chaque serveur App-V doit être dans un état démarré et en cours d'exécution.
- PowerShell à distance est-elle activée sur le serveur App-V ? Si ce n'est pas le cas, consultez l'article http://technet.microsoft.com/en-us/magazine/ff700227.aspx.
- L'administrateur Studio est-il également un administrateur de serveur App-V ?

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Le partage de fichiers est-il activé sur le serveur App-V ? Entrez **\\<*nom de domaine complet serveur App-V*>** dans l'Explorateur Windows ou avec la commande Exécuter.
- Le serveur App-V possède-t-il les mêmes autorisations de partage de fichiers que l'administrateur App-V ? Sur le serveur App-V, ajoutez une entrée pour \\<*Nom complet de serveurs App-V*> dans Noms et mots de passe utilisateur enregistrés, en spécifiant les informations d'identification de l'utilisateur qui dispose de privilèges d'administrateur sur le serveur App-V. Pour plus d'informations, consultez la section http://support.microsoft.com/kb/306541/fr.
- Le serveur App-V est-il dans Active Directory ?

  Si les machines Studio et le serveur App-V se trouvent dans différents domaines Active Directory qui ne disposent pas d'une relation d'approbation, à partir de la console PowerShell sur les machines Studio, exécutez **winrm s winrm/Config/client '@(TrustedHosts="**<*Nom complet du serveur App-V*>**")'**.

  Si TrustedHosts est géré par l'objet de stratégie de groupe, le message d'erreur suivant s'affiche : « Le paramètre de configuration TrustedHosts ne peut pas être modifié car il est contrôlé par des stratégies. La stratégie doit être définie sur « Non configuré » pour changer le paramètre de configuration. » Dans ce cas, ajoutez une entrée pour le nom de serveur App-V à la stratégie TrustedHosts dans l'objet de stratégie de groupe (Modèles d'administration > Composants Windows > Gestion à distance de Windows (WinRM) > Client WinRM).

(DOUBLE) La découverte échoue lors de l'ajout d'une application App-V à un groupe de mise à disposition.

- L'administrateur Studio est-il également un administrateur du serveur d'administration App-V ?
- Le serveur d'administration App-V est-il en cours d'exécution ? Envoyez une commande Ping ou vérifiez le Gestionnaire des services IIS ; chaque serveur App-V doit être dans un état démarré et en cours d'exécution.
- PowerShell à distance est-elle activée sur les deux serveurs App-V ? Si ce n'est pas le cas, consultez l'article http://technet.microsoft.com/en-us/magazine/ff700227.aspx.
- Les packages possèdent-ils des autorisations de sécurité appropriées pour que l'administrateur Studio ait accès ?

Les applications App-V ne démarrent pas.

- (DOUBLE) Le serveur de publication est-il en cours d'exécution ?
- (DOUBLE) Les packages App-V possèdent-ils les autorisations de sécurité nécessaires pour que les utilisateurs aient accès ?
- (DOUBLE) Sur le VDA, assurez-vous que Temp pointe vers l'emplacement correct et qu'il existe suffisamment d'espace disponible dans le répertoire Temp.
- (DOUBLE) Sur le serveur de publication App-V, exécutez **Get-AppvPublishingServer *** pour afficher la liste des serveurs de publication.
- (DOUBLE) Sur le serveur de publication App-V, vérifiez si UserRefreshonLogon est défini sur False. Si ce n'est pas le cas, le premier démarrage de l'application App-V échoue généralement.
- (DOUBLE) Sur le serveur de publication App-V, en tant qu'administrateur, exécutez **Set-AppvPublishingServer** et définissez UserRefreshonLogon sur False.
- Une version prise en charge du client App-V est-elle installée sur la machine qui contient le VDA ? Le paramètre « enable package scripts » est-il activé pour le VDA ?
- Sur la machine contenant le client App-V et le VDA, à l'aide de l'Éditeur du Registre (regedit), accédez à la clé HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppV. Vérifiez que la clé AppVServers possède la valeur suivante format : AppVManagementServer+metadata;PublishingServer (par exemple: http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082).
- Sur la machine contenant le client App-V et le VDA, assurez-vous que CtxAppVCOMAdmin dispose des privilèges d'administrateur. Ceci est généralement créé lors de l'installation du VDA et ajouté au groupe Administrateurs locaux sur

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

la machine du VDA. Toutefois, en fonction de la stratégie Active Directory, cet utilisateur risque de perdre l'association d'administration. Exécutez compmgmt.msc et recherchez Utilisateurs et Groupes locaux Utilisateurs. Si CtxAppVCOMAdmin n'est pas un administrateur, ajustez la stratégie de groupe afin que ce compte d'utilisateur conserve son association d'administration.

- Sur la machine ou l'image principale contenant le client App-V et le VDA, vérifiez que le paramètre ExecutionPolicy du PowerShell est défini sur RemoteSigned. Le client App-V fourni par Microsoft n'est pas signé et ce paramètre permet au PowerShell d'exécuter des scripts et applets de commande locaux non signés. Utilisez l'une des méthodes suivantes pour définir ExecutionPolicy : (1) En tant qu'administrateur, entrez l'applet de commande : **Set-ExecutionPolicy RemoteSigned** ou (2) Dans les paramètres de stratégie de groupe, accédez à Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows PowerShell > Activer l'exécution des scripts.

Si ces étapes ne résolvent pas les problèmes, l'administrateur doit activer et examiner les journaux.

Les journaux liés à la configuration App-V se trouvent à l'emplacement suivant : C:\CtxAppvLogs. Les journaux de lancement de l'application se trouvent à l'emplacement suivant : %LOCALAPPDATA%\Citrix\CtxAppvLogs. LOCALAPPDATA résout le dossier local pour l'utilisateur connecté. Veillez à vérifier dans le dossier local de l'utilisateur pour lequel le lancement de l'application a échoué.

Pour activer les journaux Studio et VDA utilisés pour App-V, vous devez disposer des privilèges d'administrateur. Vous aurez également besoin d'un éditeur de texte tel que le Bloc-notes.

Pour activer les journaux Studio :

1. Créez le dossier C:\CtxAppvLogs.
2. Accédez à C:\ProgramFiles\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1. Ouvrez CtxAppvCommon.dll.config dans un éditeur de texte et retirez les marques de commentaire de la ligne suivante :
3. Redémarrez le service Broker pour démarrer la journalisation.

Pour activer les journaux VDA :

1. Créez le dossier C:\CtxAppvLogs.
2. Accédez à C:\ProgramFiles\Citrix\ Virtual Desktop Agent. Ouvrez CtxAppvCommon.dll.config dans un éditeur de texte et retirez les marques de commentaire de la ligne suivante :
3. Supprimez les marques de commentaire de la ligne suivante et définissez la valeur de champ sur 1 :
4. Redémarrez la machine pour démarrer la journalisation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

AppDisks

Aug 22, 2016

Généralités

La gestion des applications et des images sur lesquelles elles sont installées peut être une tâche difficile. La fonctionnalité Citrix AppDisks apporte une solution. La fonctionnalité AppDisks sépare les applications et les groupes d'applications du système d'exploitation, ce qui vous permet de les gérer indépendamment.

Vous pouvez créer différents AppDisks contenant des applications conçues pour des groupes d'utilisateurs, puis assembler les AppDisks sur une image principale de votre choix. Regrouper et gérer les applications de cette manière vous offre un meilleur contrôle des applications et réduit le nombre d'images principales à gérer. Cela simplifie les tâches administratives et vous permet de répondre plus rapidement aux besoins de l'utilisateur. Vous pouvez mettre les applications à disposition dans des AppDisks par le biais de groupes de mise à disposition.

Si votre déploiement comprend également Citrix AppDNA, vous pouvez y intégrer la fonctionnalité AppDisks ; AppDNA permet à XenApp et à XenDesktop d'effectuer une analyse automatique des applications par AppDisk. L'utilisation d'AppDNA permet de profiter pleinement de la fonctionnalité AppDisks. Sans AppDNA, la compatibilité applicative n'est pas testée ou communiquée.

La fonctionnalité AppDisks diffère des autres technologies de provisioning d'applications par deux aspects : l'isolation et la gestion des modifications.

- Microsoft App-V permet aux applications incompatibles de co-exister en les isolant. La fonctionnalité AppDisks n'isole pas les applications. Elle sépare les applications (ainsi que les fichiers et les clés de registre associés) du système d'exploitation. Pour le système d'exploitation et l'utilisateur, l'aspect et le fonctionnement des AppDisks sont les mêmes que s'ils étaient installés directement sur une image principale.
- La gestion des modifications (la mise à jour des images principales et le test de compatibilité des mises à jour avec les applications installées) peut représenter une dépense importante. Les rapports AppDNA vous aident à identifier les problèmes et suggèrent des solutions. Par exemple, AppDNA peut identifier les applications qui ont des dépendances communes telles que .NET, ce qui vous permet de les installer sur une seule image de base commune. AppDNA peut également identifier les applications qui se chargent tôt dans la séquence de démarrage du système d'exploitation, vous permettant de vous assurer qu'elles se comportent comme prévu.

À savoir :

- La séparation des applications et du système d'exploitation, ou tout autre aspect de la fonctionnalité AppDisks, n'est pas visible pour l'utilisateur. Les applications se comportent comme si elles étaient installées sur l'image. Les AppDisks contenant des applications complexes peuvent entraîner un léger délai de démarrage du bureau.
- Vous pouvez utiliser les AppDisks avec des bureaux partagés hébergés.
- Vous pouvez partager les AppDisks sur différentes images principales et plates-formes de système d'exploitation (par application) ; toutefois, cela ne fonctionnera pas pour toutes les applications. Si vous disposez d'applications avec un script d'installation pour OS de bureau qui les empêche de fonctionner sur un OS de serveur, Citrix vous recommande de créer un package distinct des applications pour les deux systèmes d'exploitation.
- Dans de nombreux cas, les AppDisks fonctionnent sur différents systèmes d'exploitation. Par exemple, vous pouvez ajouter un AppDisk qui a été créé sur une VM Windows 7 à un groupe de mise à disposition contenant des machines

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Windows 2008 R2, tant que les deux systèmes d'exploitation ont le même nombre de bits (32 bits ou 64 bits) et prennent en charge l'application. Cependant, Citrix vous recommande de ne pas ajouter un AppDisk créé sur une version ultérieure du système d'exploitation (telle que Windows 10) à un groupe de mise à disposition contenant des machines exécutant une version antérieure du système d'exploitation (telle que Windows 7), car il risque de ne pas fonctionner correctement.

- Si vous avez besoin de limiter l'accès à des applications d'un AppDisk à un sous-ensemble d'utilisateurs d'un groupe de mise à disposition, Citrix vous recommande d'utiliser la stratégie de groupe pour masquer les applications d'un AppDisk pour certains utilisateurs. Le fichier exécutable de cette application reste disponible, mais ne sera pas exécuté pour ces utilisateurs.

Vue d'ensemble du déploiement

La liste suivante résume les étapes de déploiement des AppDisks. Vous trouverez plus de détails dans cet article.

1. À partir de la console de gestion de l'hyperviseur, installez un Virtual Delivery Agent (VDA) sur une VM.
2. Créez un AppDisk, ce qui inclut des étapes dans la console de gestion de l'hyperviseur et dans Studio.
3. À partir de la console de gestion de l'hyperviseur, installez les applications sur le AppDisk.
4. Scellez le AppDisk (à partir de la console de gestion de l'hyperviseur ou dans Studio). La possibilité de sceller permet à XenApp et à XenDesktop d'enregistrer les applications du AppDisk et les fichiers associés dans une bibliothèque d'applications (AppLibrary).
5. Dans Studio, créez ou modifiez un groupe de mise à disposition et sélectionnez les AppDisks à inclure ; cela s'appelle *attribuer les AppDisks* (même si vous utilisez l'action **Gérer les AppDisks** dans Studio). Lorsque des machines virtuelles du groupe de mise à disposition démarrent, XenApp et XenDesktop coordonnent avec AppLibrary, Machine Creation Services (MCS) ou Provisioning Services (PVS), et le Delivery Controller pour distribuer les AppDisks sélectionnés.

Configuration requise

L'utilisation de AppDisks présente des exigences en plus de celles répertoriées dans l'article Configuration système requise.

La fonctionnalité AppDisks est uniquement prise en charge dans les déploiements contenant (au minimum) les versions du Delivery Controller et de Studio fournies dans le téléchargement de XenApp et XenDesktop 7.8, y compris les composants requis que le programme d'installation déploie automatiquement (tels que .NET 4.5.2).

Les AppDisks peuvent être créés sur les versions de système d'exploitation Windows prises en charge pour les VDA. Les machines sélectionnées pour les groupes de mise à disposition qui utiliseront AppDisks doivent disposer de VDA version 7.8 au minimum.

> Citrix vous recommande d'installer ou de mettre à niveau les machines avec la dernière version de VDA (et de mettre à niveau les catalogues de machines et les groupes de mise à disposition en fonction de vos besoins). Lors de la création d'un groupe de mise à disposition, si vous sélectionnez des machines sur lesquelles sont installées différentes versions de VDA, le groupe de mise à disposition sera compatible avec la version de VDA la plus ancienne (Il s'agit du *niveau fonctionnel* du groupe). Pour plus d'informations sur le niveau fonctionnel, consultez l'article Créer des groupes de mise à disposition.

Pour provisionner des machines virtuelles qui seront utilisées pour créer des AppDisks, vous pouvez utiliser les éléments suivants :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- MCS fourni avec Controller 7.8 (minimum) ou la version PVS fournie sur la page de téléchargement avec votre version de XenApp et XenDesktop.
- Les versions de XenServer prises en charge (veuillez consulter l'article Configuration requise) ou VMware version 5.1 au minimum. (Les AppDisks ne peuvent pas être utilisés avec d'autres types d'hyperviseur et de service de cloud hôte pris en charge par XenApp et XenDesktop).

La création d'AppDisks n'est pas prise en charge avec les machines de catalogues MCS qui utilisent la mise en cache des données temporaires.

Les catalogues Remote PC Access ne prennent pas en charge les AppDisks.

Le service de cliché instantané des volumes Windows doit être activé sur la machine virtuelle sur laquelle vous créez un AppDisk. Ce service est activé par défaut.

Les groupes de mise à disposition utilisés avec les AppDisks peuvent contenir des machines regroupées au hasard dans des catalogues de machines avec OS de serveur ou OS de bureau. Vous ne pouvez pas utiliser les AppDisks avec des machines d'autres types de catalogue, tels que les catalogues de machines statiques regroupées ou dédiées (attribuées).

Les machines sur lesquelles Studio est installé doivent disposer de .NET Framework 3.5 (en plus d'autres versions .NET).

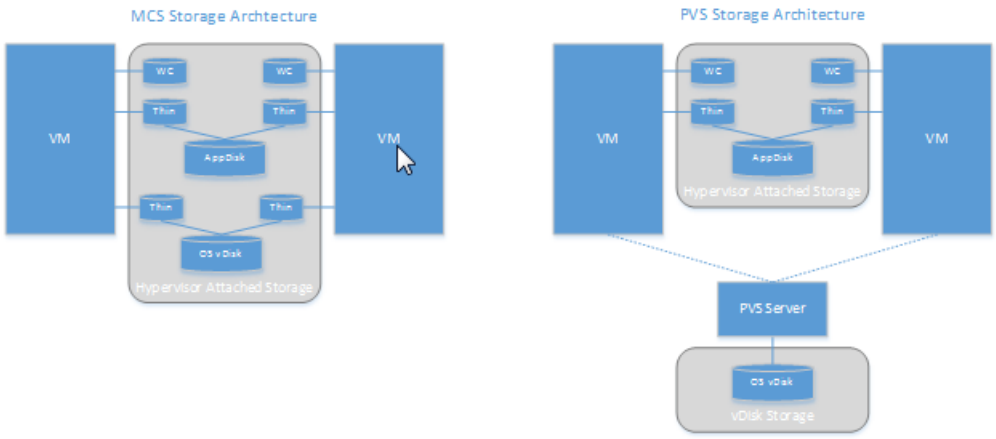
Les AppDisks peuvent affecter le stockage. Pour de plus amples informations, veuillez consulter la section Considérations sur le stockage et les performances.

Si vous utilisez AppDNA :

- Consultez la documentation de AppDNA et AppDisk FAQ.
- Le logiciel AppDNA doit être installé sur un autre serveur depuis un Controller. Utilisez la version AppDNA fournie avec cette version de XenApp et de XenDesktop. Pour les autres exigences de AppDNA, consultez sa documentation.
- Sur le serveur AppDNA, assurez-vous qu'il existe une exception de pare-feu pour le port par défaut 8199.
- Ne désactivez pas de connexion AppDNA lors de la création d'un AppDisk.
- Lorsque vous créez le site XenApp ou XenDesktop, vous pouvez activer l'analyse de compatibilité avec AppDNA sur la page **Fonctionnalités supplémentaires** de l'assistant de création de site. Vous pouvez également activer/désactiver cette fonctionnalité en sélectionnant l'option **Configuration > AppDNA** dans le volet de navigation Studio.

La séparation des applications et du système d'exploitation à l'aide de deux disques, et le stockage de ces disques dans différentes zones peuvent affecter votre stratégie de stockage. Le graphique suivant illustre les architectures de stockage MCS et PVS. « WC » indique le cache en écriture et « Thin » indique le disque léger utilisé pour stocker les différences entre le AppDisk d'une VM et les disques virtuels du système d'exploitation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Dans les environnements MCS :

Vous pouvez continuer à équilibrer la taille des AppDisks et des disques virtuels (vDisks) du système d'exploitation en suivant les recommandations de votre entreprise en termes de taille. Si les AppDisks sont partagés par plusieurs groupes de mise à disposition, la capacité de stockage générale peut être réduite.

Les vDisks du système d'exploitation et les AppDisks sont situés dans les mêmes zones de stockage, vous devez donc planifier attentivement vos besoins en termes de capacité de stockage pour éviter tout effet négatif sur la capacité lorsque vous déployez les AppDisks. Les AppDisks entraînent une surcharge, donc assurez-vous que votre stockage prend en charge cette surcharge et les applications.

Il n'y a aucun effet net sur IOPS car les vDisks du système d'exploitation et les AppDisks sont situés dans la même zone de stockage. Il n'existe pas de considérations à prendre en compte pour le cache en écriture lorsque vous utilisez MCS.

Dans les environnements PVS :

Vous devez prévoir une capacité et des IOPS plus importantes car les applications se déplacent du stockage sur AppDisk vers le stockage lié à l'hyperviseur.

Avec PVS, les vDisks du système d'exploitation et les AppDisks utilisent des zones de stockage différentes. La capacité de stockage des vDisks du système d'exploitation est réduite, mais le stockage lié à l'hyperviseur augmente. Par conséquent, vous devez configurer la taille de vos environnements PVS pour la prise en charge de ces modifications.

Les AppDisks dans le stockage lié à l'hyperviseur requièrent plus d'IOPS alors que les vDisks du système d'exploitation en requièrent moins.

Cache en écriture : PVS utilise un fichier VHDX dynamique sur un lecteur au format NTFS ; lorsque les blocs sont consignés dans le cache en écriture, le fichier VHDX est étendu de manière dynamique. Lorsque les AppDisks sont connectés à leur machine virtuelle associée, ils sont fusionnés avec les vDisks du système d'exploitation pour fournir une vue unifiée du système de fichiers. Cette fusion entraîne généralement l'écriture de données supplémentaires sur les caches en écriture, ce qui augmente la taille du fichier du cache en écriture. Vous devez prendre en compte cet aspect lors de la planification de la capacité.

Dans les environnements MCS et PVS, pensez à réduire la taille des vDisks du système d'exploitation pour tirer parti des AppDisks que vous créez. Sinon, planifiez un stockage plus important.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Lorsque plusieurs utilisateurs d'un site allument leurs ordinateurs simultanément (par exemple, en début de journée), les multiples requêtes de démarrage exercent une pression sur l'hyperviseur, ce qui peut affecter les performances. Pour PVS, les applications ne se trouvent pas sur le vDisk du système d'exploitation, donc le serveur PVS reçoit moins de requêtes. La charge étant plus légère sur chaque machine cible, le serveur PVS peut transmettre vers un plus grand nombre de cibles. Cependant, une plus grande densité cible-serveur peut avoir un effet négatif sur les performances « boot storm ».

Créer un AppDisk

Il existe deux façons de créer un AppDisk, d'installer les applications et de le sceller. Les deux méthodes comprennent des étapes dans la console de gestion de l'hyperviseur et dans Studio. Les méthodes se distinguent par l'emplacement où se déroulent la plupart des étapes.

Quelle que soit la méthode que vous utilisez :

- Prévoyez 30 minutes pour la création du AppDisk.
- Si vous utilisez AppDNA, suivez les instructions de la section Configuration requise ci-dessus. Ne désactivez pas de connexion AppDNA lors de la création d'un AppDisk.
- Lorsque vous ajoutez des applications à un AppDisk, pensez à installer les applications pour tous les utilisateurs. Réarmez les applications qui utilisent l'activation de Key Management Server (KMS). Pour de plus amples informations, consultez la documentation de l'application.
- Les fichiers, dossiers ou entrées de registre créés dans des emplacements spécifiques à l'utilisateur lors de la création du AppDisk ne sont pas conservés. Par ailleurs, certaines applications exécutent un assistant de première utilisation pour créer les données de l'utilisateur au cours de l'installation. Utilisez une solution de gestion de profils pour conserver ces données et empêcher l'affichage de l'assistant chaque fois que le AppDisk démarre.
- Si vous utilisez AppDNA, son analyse démarre automatiquement après la fin du processus de création. Pendant cet intervalle, l'état du AppDisk dans Studio est « Analyse ».

Les AppDisks sur des machines de catalogues de machines créés par Provisioning Services nécessitent une configuration supplémentaire durant la création du AppDisk. À partir de la console Provisioning Services :

1. Créez une nouvelle version du vDisk associé à la collection de machines qui contient la VM.
2. Placez la VM en mode de maintenance.
3. Lors de la création du AppDisk, sélectionnez la version de maintenance sur l'écran de démarrage chaque fois que la VM redémarre.
4. Après avoir scellé le AppDisk, placez la VM en production et supprimez la version vDisk que vous avez créée.

Cette procédure comporte trois tâches : créer le AppDisk, créer des applications sur le AppDisk, puis sceller le AppDisk.

Créer un AppDisk :

1. Sélectionnez **AppDisks** dans le panneau de navigation de Studio, puis sélectionnez **Créer un AppDisk** dans le volet Actions.
2. Consultez les informations sur la page **Introduction** de l'assistant, puis cliquez sur **Suivant**.
3. Sur la page **Créer un AppDisk**, sélectionnez le bouton radio **Créer un nouveau AppDisk**. Sélectionnez l'une des tailles de disque prédéfinies (petite, moyenne, grande) ou spécifiez une taille de disque en Go ; la taille minimale est de 3 Go. La

© 1999-2017 Citrix Systems, Inc. All rights reserved.

taille du disque doit être suffisante pour contenir les applications que vous ajoutez. Cliquez sur **Suivant**.

4. Sur la page **Machine de préparation**, sélectionnez un catalogue de machines regroupées au hasard à utiliser en tant qu'image principale sur laquelle le AppDisk sera créé. Remarque : l'écran dresse la liste de tous les catalogues de machines du site, séparés par type ; seuls les catalogues contenant au moins une machine disponible peuvent être sélectionnés. Si vous choisissez un catalogue qui ne contient pas de VM regroupées au hasard, la création de AppDisk échoue. Lorsque vous avez sélectionné une VM à partir d'un catalogue de machines regroupées au hasard, cliquez sur **Suivant**.
5. Sur la page **Résumé**, entrez un nom et une description pour le AppDisk. Vérifiez les informations que vous avez spécifiées sur les pages précédentes de l'assistant. Cliquez sur **Terminer**.

Rappel : si vous utilisez PVS, suivez les instructions dans la section Considérations sur PVS ci-dessus.

Lorsque l'assistant se ferme, l'écran Studio pour le nouveau AppDisk indique « Création ». Une fois que le AppDisk est créé, l'écran affiche « Prêt à installer les applications ».

Installer les applications sur le AppDisk :

À partir de la console de gestion de l'hyperviseur, installez les applications sur le AppDisk. (**Conseil :** si vous avez oublié le nom de la VM, sélectionnez **AppDisks** dans le panneau de navigation de Studio, puis sélectionnez **Installer des applications** dans le panneau Actions pour afficher son nom). Consultez la documentation de l'hyperviseur pour obtenir des informations sur l'installation des applications (**Rappel :** vous devez installer des applications sur le AppDisk à partir de la console de gestion de l'hyperviseur. N'utilisez pas la tâche Installer des applications du panneau Actions de Studio.).

Sceller le AppDisk :

1. Sélectionnez **AppDisks** dans le volet de navigation Studio.
2. Sélectionnez le AppDisk que vous avez créé, puis sélectionnez **Sceller AppDisk** dans le volet Actions.

Après avoir créé le AppDisk, installez-y des applications, puis scellez-le et attribuez-le à un groupe de mise à disposition.

Dans cette procédure, vous effectuez la création du AppDisk et la préparation des tâches à partir de la console de gestion de l'hyperviseur, puis vous importez le AppDisk dans Studio.

Préparer, installer les applications et sceller un AppDisk sur l'hyperviseur :

1. À partir de la console de gestion de l'hyperviseur, créez une VM et installez un VDA.
2. Arrêtez la machine et prenez un instantané.
3. Créez une nouvelle machine à partir de l'instantané, puis ajoutez-lui un nouveau disque. Ce disque (qui deviendra le AppDisk) doit être de taille suffisante pour stocker toutes les applications que vous installerez dessus.
4. Démarrez la machine, puis sélectionnez **Démarrer > Préparer AppDisk**. Si le raccourci du menu Démarrer n'est pas disponible sur l'hyperviseur, ouvrez une invite de commandes à C:\Program Files\Citrix Personal vDisk\bin et tapez : **CtxPvD.Exe –s LayerCreationBegin**. La machine redémarre et prépare le disque. Un second redémarrage se produit après quelques minutes lorsque la préparation est terminée.
5. Installez les applications que vous souhaitez mettre à la disposition des utilisateurs.
6. Cliquez deux fois sur le raccourci **Packager AppDisk** sur le bureau de la machine. La machine redémarre et le processus commence. Lorsque la boîte de dialogue se ferme, arrêtez la VM.

Utiliser Studio pour importer le AppDisk vous avez créé sur l'hyperviseur :

1. Sélectionnez **AppDisks** dans le panneau de navigation de Studio, puis sélectionnez **Créer un AppDisk** dans le volet Actions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Sur la page **Introduction**, consultez les informations et cliquez sur **Suivant**.
3. Sur la page **Créer un AppDisk**, sélectionnez le bouton radio **Importer un AppDisk existant**. Sélectionnez la ressource (réseau et stockage) dans laquelle le AppDisk que vous avez créé réside sur l'hyperviseur. Cliquez sur **Next**.
4. Sur la page **Machine de préparation**, accédez à la machine, sélectionnez le disque, puis cliquez sur **Suivant**.
5. Sur la page **Résumé**, entrez un nom et une description pour le AppDisk. Vérifiez les informations que vous avez spécifiées sur les pages précédentes de l'assistant. Cliquez sur **Terminer**. Studio importe le AppDisk.

Une fois que vous avez importé le AppDisk dans Studio, attribuez-le à un groupe de mise à disposition.

Attribuer un AppDisk à un groupe de mise à disposition

Vous pouvez attribuer un ou plusieurs AppDisks à un groupe de mise à disposition lorsque vous créez le groupe de mise à disposition ou ultérieurement. Les informations AppDisks que vous fournissez sont quasiment les mêmes.

Si vous ajoutez des AppDisks à un groupe de mise à disposition que vous créez, utilisez les instructions suivantes pour la page **AppDisks** de l'assistant Créer un groupe de mise à disposition (Pour de plus amples informations sur les autres pages de cet assistant, consultez l'article Créer des groupes de mise à disposition.).

Pour ajouter (ou supprimer) des AppDisks dans un groupe de mise à disposition existant :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe de mise à disposition, puis sélectionnez **Gérer les AppDisks** dans le volet Actions. Veuillez consulter les instructions suivantes pour la page **AppDisks**.
3. Lorsque vous modifiez la configuration du AppDisk dans un groupe de mise à disposition, un redémarrage des machines du groupe est requis. Sur la page **Stratégie de déploiement**, suivez les instructions de la section Créer un programme de redémarrage.

Page AppDisks :

La page **AppDisks** (dans l'assistant Créer un groupe de mise à disposition ou dans le flux Gérer les AppDisks) répertorie les AppDisks déjà déployés pour le groupe de mise à disposition et leur priorité (si vous créez le groupe de mise à disposition, la liste est vide.) Pour de plus amples informations, consultez la section Priorité AppDisk.

1. Cliquez sur **Add**. La boîte de dialogue Sélectionner des AppDisks dresse la liste de tous les AppDisks dans la colonne de gauche. Les cases des AppDisks qui sont déjà attribués à ce groupe de mise à disposition sont activées et ils ne peuvent pas être sélectionnés.
2. Sélectionnez les cases à cocher des AppDisks disponibles dans la colonne de gauche. La colonne de droite dresse la liste des applications sur le AppDisk (la sélection de l'onglet **Applications** au-dessus de la colonne de droite dresse la liste des applications dans un format similaire à un menu Démarrer ; la sélection de l'onglet **Packages installés** dresse la liste des applications dans un format similaire à la liste Programmes et fonctionnalités.).
3. Après avoir sélectionné un ou plusieurs AppDisks disponibles, cliquez sur **OK**.
4. Cliquez sur **Suivant** sur la page AppDisks.

Lorsque plusieurs AppDisks sont attribués à un groupe de mise à disposition, la page **AppDisks** (dans les écrans Créer un groupe de mise à disposition, Modifier le groupe de mise à disposition et Gérer les AppDisks) dresse la liste des AppDisks par

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ordre de priorité décroissante. Les entrées en haut de la liste ont la priorité plus élevée. La priorité indique l'ordre dans lequel les AppDisks sont traités.

Vous pouvez utiliser les flèches haut et bas en regard de la liste pour modifier la priorité AppDisk. Si AppDNA est intégré avec votre déploiement AppDisk, il analyse automatiquement les applications et définit la priorité lorsque les AppDisks sont attribués au groupe de mise à disposition. Plus tard, si vous ajoutez ou supprimez des AppDisks du groupe, vous pouvez cliquer sur **Ordre automatique** pour demander à AppDNA d'analyser la liste actuelle des AppDisks et de déterminer les priorités. L'analyse (et le changement de priorité, si nécessaire) peut prendre plusieurs minutes.

Gestion de AppDisks

Une fois que vous avez créé et attribué des AppDisks à des groupes de mise à disposition, vous pouvez modifier les propriétés des AppDisks via le nœud AppDisks dans le panneau de navigation de Studio. Les modifications apportées aux applications dans un AppDisk doivent être effectuées à partir de la console de gestion de l'hyperviseur.

Important : vous pouvez utiliser le service Windows Update pour mettre à jour les applications (telles que la suite Microsoft Office) sur un AppDisk. Toutefois, n'utilisez pas le service Windows Update pour appliquer les mises à jour du système d'exploitation à un AppDisk. Appliquez les mises à jour du système d'exploitation à l'image principale, et non pas au AppDisk ; sinon, le AppDisk ne s'initialise pas correctement.

- Lors de l'application de correctifs et d'autres mises à jour à des applications dans un AppDisk, appliquez uniquement ceux dont a besoin l'application. N'appliquez pas les mises à jour pour d'autres applications.
- Lors de l'installation des mises à jour Windows, vous devez d'abord désélectionner toutes les entrées, puis sélectionner le sous-ensemble requis par les applications sur les AppDisks que vous mettez à jour.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Local App Access et redirection d'adresse URL

Jul 07, 2016

Dans cet article :

- Introduction
- Configuration requise, considérations et limitations à prendre en compte
- Interaction avec Windows
- Configurer Local App Access et la redirection d'adresse URL

Introduction

Local App Access s'intègre en toute transparence avec les applications Windows installées localement dans un environnement de bureau hébergé sans passer d'un ordinateur à l'autre. Avec Local App Access, vous pouvez :

- Accédez aux applications installées localement sur un ordinateur portable, un PC ou tout autre périphérique physique directement à partir de votre bureau virtuel.
- Fournir une solution de mise à disposition d'applications flexible. Si les utilisateurs possèdent des applications locales que vous ne pouvez pas virtualiser ou qui ne sont pas gérées par le département informatique, ces applications se comporteront toujours comme si elles étaient installées sur un bureau virtuel.
- Éliminez la latence double-hop lorsque les applications sont hébergées séparément du bureau virtuel en plaçant le raccourci vers l'application publiée sur la machine Windows de l'utilisateur.
- Utiliser des applications telles que :
  - Logiciels de conférence vidéo tels que GoToMeeting.
  - Applications de niche ou spécialisées qui ne sont pas encore virtualisées.
  - Les applications et périphériques qui transfèrent des quantités très importantes de données depuis une machine utilisateur vers un serveur et à nouveau vers la machine utilisateur, comme les graveurs de DVD et les tuners TV.

Dans XenApp et XenDesktop, les sessions de bureau hébergées utilisent la redirection d'URL pour lancer les applications Local Access App. La redirection d'URL met l'application à disposition sous plusieurs adresses URL. Elle lance un navigateur local (en fonction de la liste noire d'adresses URL de votre navigateur) en cliquant sur des liens intégrés dans un navigateur dans une session de bureau. Si vous accédez à une URL qui n'est pas présente dans la liste noire, l'adresse URL est ouverte dans la session de bureau.

La redirection d'adresse URL ne fonctionne que pour les sessions de bureau, pas les sessions d'application. La seule fonctionnalité de redirection que vous pouvez utiliser pour des sessions d'application est la redirection de contenu hôte vers client, qui est un type de FTA serveur. Cette FTA redirige certains protocoles vers le client, tels que http, https, rtsp ou mms. Par exemple, si vous voulez ouvrir uniquement des liens avec http, les liens s'ouvrent directement avec l'application cliente. Il n'y a aucune liste noire ou blanche d'adresses URL de prise en charge.

Lorsque Local App Access est activé pour les bureaux hébergés, les adresses URL qui sont affichées pour les utilisateurs en tant que liens depuis des applications exécutées localement, depuis les applications hébergées par l'utilisateur ou en tant que raccourcis sur le bureau sont redirigées de l'une des manières suivantes :

- À partir de l'ordinateur de l'utilisateur vers le bureau hébergé
- À partir du serveur XenApp vers l'ordinateur de l'utilisateur
- Restitué dans l'environnement dans lequel ils sont lancés (et non pas redirigés)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour spécifier le chemin d'accès de redirection du contenu de sites Web spécifiques, configurez la liste blanche et la liste noire d'adresses URL sur Virtual Delivery Agent. Ces listes contiennent des clés de Registre de chaînes multiples qui spécifient les paramètres de stratégie de redirection d'URL ; pour de plus amples informations, consultez la section Paramètres de stratégie Local App Access.

Les adresses URL peuvent être restituées sur le VDA avec les exceptions suivantes :

- Informations géographiques et relatives aux paramètres régionaux : sites Web qui requièrent des informations sur les paramètres régionaux, telles que msn.com ou news.google.com (ouvre une page spécifique au pays en fonction de l'emplacement géographique). À titre d'exemple, si le VDA est provisionné à partir d'un centre de données situé au Royaume-Uni et que le client se connecte depuis l'Inde, l'utilisateur s'attend à voir in.msn.com mais voit uk.msn.com.
- Contenu multimédia : les sites Web contenant du contenu multimédia riche, lorsqu'ils sont restitués sur la machine cliente, offrent aux utilisateurs une expérience native et permettent d'économiser la bande passante même dans les réseaux à latence élevée. Bien qu'il existe une fonctionnalité de redirection Flash, ceci effectue un complément en redirigeant les sites avec d'autres types multimédia comme Silverlight. Ceci est dans un environnement ultra sécurisé. En effet, les URL qui sont approuvées par l'administrateur sont exécutées sur la machine cliente tandis que le reste des URL sont redirigées vers le VDA.

En plus de la redirection d'URL, vous pouvez également utiliser la redirection d'association de types de fichier (FTA). L'association de types de fichier lance des applications locales lorsqu'un fichier est détecté dans la session. Si l'application locale est lancée, elle doit avoir accès au fichier pour l'ouvrir. Par conséquent, vous pouvez uniquement ouvrir des fichiers qui résident sur des partages réseau ou sur des lecteurs clients (avec CDM) à l'aide d'applications locales. Par exemple, lors de l'ouverture d'un fichier PDF, si un lecteur PDF est une application locale, le fichier s'ouvre à l'aide de ce lecteur PDF. Étant donné que l'application locale peut accéder au fichier directement, il n'y a pas de transfert réseau du fichier via ICA pour ouvrir ce dernier.

Configuration requise, considérations et limitations à prendre en compte

Local App Access est pris en charge sur les systèmes d'exploitation compatibles avec les VDA pour OS de serveur Windows et les VDA pour OS de bureau Windows, et requiert Citrix Receiver pour Windows version 4.1 (minimum). Les navigateurs Web pris en charge sont les suivants :

- Internet Explorer 11. Vous pouvez utiliser Internet Explorer versions 8, 9 ou 10, mais Microsoft prend en charge la version 11 (et Citrix vous recommande d'utiliser cette version).
- Firefox 3.5 à 21.0
- Chrome 10

Vérifiez les informations et les limitations suivantes lors de l'utilisation de Local App Access et de la redirection d'adresse URL.

- Local App Access est uniquement conçu pour les bureaux virtuels en mode plein écran couvrant tous les moniteurs comme suit :
  - L'expérience utilisateur pourrait prêter à confusion si Local App Access est utilisé avec un bureau virtuel qui s'exécute en mode fenêtre ou ne couvre pas tous les moniteurs.
  - Pour les utilisateurs équipés de plusieurs moniteurs, si un moniteur est agrandi, il devient le bureau par défaut pour toutes les applications lancées dans cette session, même si les applications suivantes sont lancées généralement sur l'autre moniteur.
  - Cette fonctionnalité prend en charge un VDA ; il n'y a pas d'intégration avec plusieurs VDA simultanés.
- Certaines applications peuvent se comporter de manière inattendue et affecter les utilisateurs :
  - Les utilisateurs risquent d'être déroutés par les lettres de lecteur, telles que C: local plutôt que le lecteur C: du bureau virtuel.
  - Les imprimantes disponibles dans le bureau virtuel ne sont pas disponibles pour les applications locales.
  - Les applications qui nécessitent des autorisations élevées ne peuvent pas être lancées en tant qu'applications hébergées sur le client.
  - Aucun traitement spécial pour les applications à instance unique (telles que le Lecteur Windows Media).
  - Les applications locales s'affichent avec le thème Windows de la machine locale.
  - Les applications en plein écran ne sont pas prises en charge. Cela inclut les applications qui s'ouvrent en plein écran, telles que des diaporamas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

PowerPoint, ou les visionneuses de photos couvrant la totalité du bureau.
- Local App Access copie les propriétés de l'application locale (telles que les raccourcis sur le bureau et le menu Démarrer du client) sur le VDA ; cependant, il ne copie pas les autres propriétés, telles que les touches de raccourci et les attributs en lecture seule.
- Les applications qui permettent de personnaliser la manière dont est géré le chevauchement des fenêtres peuvent avoir des résultats imprévisibles. Par exemple, certaines fenêtres peuvent être masquées.
- Les raccourcis ne sont pas pris en charge, y compris Ordinateur, Corbeille, Panneau de configuration, les raccourcis du lecteur réseau et les raccourcis de dossiers.
- Les types de fichiers et fichiers suivants ne sont pas pris en charge : types de fichiers personnalisés, fichiers sans programmes associés, fichiers zippés et fichiers masqués.
- Le regroupement de la barre des tâches n'est pas pris en charge pour les applications mixtes 32 bits et 64 bits hébergées sur le client ou le VDA, telles que le regroupement d'applications locales 32 bits avec des applications VDA 64 bits.
- Les applications ne peuvent pas être lancées à l'aide de COM. Par exemple, si vous cliquez sur un document Office incorporé à une application Office, le lancement du processus ne peut pas être détecté et l'intégration de l'application locale échoue.

- La redirection d'URL prend uniquement en charge les adresses URL explicites (c'est-à-dire, celles qui apparaissant dans la barre d'adresse du navigateur ou celles détectées à l'aide de la barre de navigation du navigateur, selon le navigateur spécifique).
- La redirection d'adresses URL fonctionne uniquement avec les sessions de bureau, et non pas avec les sessions d'application.
- Le dossier du bureau local dans une session VDA n'autorise pas les utilisateurs à créer de nouveaux fichiers.
- Plusieurs instances d'une application exécutée localement se comportent conformément aux paramètres de barre des tâches établis pour le bureau virtuel. Les raccourcis vers des applications exécutées localement ne sont pas regroupés avec les instances en cours d'exécution de ces applications. Ils sont également non groupés avec les instances en cours d'exécution des applications hébergées ou les raccourcis épinglés pour les applications hébergées. Les utilisateurs ne peuvent fermer les fenêtres des applications exécutées localement qu'à partir de la barre des tâches. Bien que les utilisateurs puissent épingler les fenêtres d'applications locales à la barre des tâches et au menu Démarrer, les applications risquent de ne pas fonctionner de manière cohérente lors de l'utilisation de ces raccourcis.

Interaction avec Windows

L'interaction de Local App Access avec Windows comprend les comportements suivants.

- Comportement des raccourcis de Windows 8 et Windows Server 2012
  - Les applications Windows Store installées sur le client ne sont pas énumérées comme faisant partie des raccourcis Local App Access.
  - Les fichiers image et vidéo sont généralement ouverts par défaut à l'aide des applications du Windows Store. Toutefois, Local App Access énumère les applications du Windows Store et ouvre les raccourcis avec les applications du bureau.
- Programmes locaux
  - Pour Windows 7, le dossier est disponible dans le menu Démarrer.
  - Pour Windows 8, Programmes locaux est disponible uniquement lorsque l'utilisateur choisit **Toutes les applications** comme catégorie dans l'écran de démarrage. Les sous-dossiers ne sont pas tous affichés dans Programmes locaux.
- Fonctionnalités graphiques Windows 8 pour les applications
  - Les applications de bureau sont limitées à la zone de bureau et sont couvertes par l'écran d'accueil et les applications de style Windows 8.
  - Les applications Local App Access ne se comportent pas comme des applications de bureau en mode multi-écrans. En mode multi-écrans, l'écran d'accueil et le bureau s'affichent sur des moniteurs différents.
- Windows 8 et la redirection d'URL Local App Access
  - Étant donné que Windows 8 n'a aucun module complémentaire Internet Explorer activé, utilisez Internet Explorer sur le bureau pour activer la redirection d'adresse URL.
  - Dans Windows Server 2012, Internet Explorer désactive les modules complémentaires par défaut. Pour implémenter la redirection d'adresse URL, désactivez la configuration renforcée d'Internet Explorer. Réinitialisez ensuite les options d'Internet Explorer et redémarrez pour vous assurer que les modules complémentaires sont activés pour les utilisateurs standards.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurer Local App Access et la redirection d'adresse URL

Pour utiliser Local App Access et la redirection d'adresse URL à l'aide de Citrix Receiver :

- Installez Citrix Receiver sur la machine cliente locale. Vous pouvez activer les fonctionnalités lors de l'installation de Citrix Receiver ou vous pouvez activer le modèle Local App Access à l'aide de l'éditeur de stratégie de groupe.
- Définissez le paramètre de stratégie **Autoriser Local App Access** sur **Activé**. Vous pouvez également configurer les paramètres de stratégie de la liste blanche et la liste noire d'adresses URL pour la redirection d'adresses URL. Pour de plus amples informations, consultez la section Paramètres de stratégie Local App Access.

Pour activer Local App Access et la redirection d'adresse URL pour toutes les applications locales :

1. Définissez le paramètre de stratégie **Autoriser Local App Access** sur **Activé**. Lorsque ce paramètre est activé, le VDA permet au client de décider si les raccourcis publiés par l'administrateur ou les raccourcis Local App Access sont activés dans la session. (Lorsque ce paramètre est désactivé, les applications publiées par l'administrateur et les raccourcis Local App Access ne fonctionnent pas pour le VDA.) Ce paramètre de stratégie s'applique à la totalité de la machine, ainsi que la stratégie de redirection d'URL.
2. Activez Local App Access et la redirection d'adresses URL lors de l'installation de Citrix Receiver pour tous les utilisateurs d'une machine. Cette action enregistre également les modules complémentaires du navigateur requis pour la redirection d'adresses URL. À partir de l'invite de commandes, exécutez la commande appropriée pour installer Receiver avec l'option suivante :

   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

1. Exécutez **gpedit.msc**.
2. Sélectionnez **Configuration ordinateur**. Cliquez avec le bouton droit de la souris sur **Modèles d'administration** et sélectionnez **Ajout/suppression de modèles > Ajouter**.
3. Ajoutez le modèle icaclient.adm se trouvant dans le dossier de Citrix Receiver Configuration (généralement dans c:\Program Files (x86)\Citrix\Online Plugin\Configuration). (Une fois le modèle icaclient.adm ajouté à la configuration de l'ordinateur, il est également disponible dans la configuration de l'utilisateur.)
4. Développez **Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Receiver > Expérience utilisateur**.
5. Sélectionnez les **paramètres Local App Access**.
6. Sélectionnez **Activé** puis sélectionnez **Autoriser la redirection d'URL**. Pour la redirection d'adresse URL, enregistrez les modules complémentaires de navigateur à l'aide de la ligne de commande, comme décrit ci-dessous.

Pour fournir l'accès aux applications publiées uniquement :

1. Sur le serveur sur lequel le Delivery Controller est installé, exécutez **regedit.exe**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Naviguez jusqu'à HKLM\Software\Wow6432Node\Citrix\DesktopStudio.
2. Ajoutez l'entrée ClientHostedAppsEnabled de REG_DWORD avec une valeur de 1. (Une valeur 0 désactive Local App Access).

2. Redémarrez le serveur Delivery Controller, puis redémarrez Studio.
3. Publiez les applications Local App Access.
   1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio, puis sélectionnez l'onglet Applications.
   2. Sélectionnez **Créer Local Access Application** dans le volet Actions.
   3. Sélectionnez le groupe de mise à disposition de bureaux.
   4. Entrez le chemin d'accès complet de l'exécutable de l'application sur la machine locale de l'utilisateur.
   5. Indiquez si le raccourci vers l'application locale sur le bureau virtuel sera visible dans le menu Démarrer, sur le bureau ou les deux.
   6. Acceptez les valeurs par défaut sur la page Nom, puis vérifiez les paramètres.
4. Activez Local App Access et la redirection d'adresses URL lors de l'installation de Citrix Receiver pour tous les utilisateurs d'une machine. Cette action enregistre également les modules complémentaires du navigateur requis pour la redirection d'adresses URL. À partir de l'invite de commandes, exécutez la commande pour installer Citrix Receiver avec l'option suivante :
   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
5. Définissez le paramètre de stratégie **Autoriser Local App Access** sur **Activé**. Lorsque ce paramètre est activé, le VDA permet au client de décider si les raccourcis publiés par l'administrateur ou les raccourcis Local App Access sont activés dans la session. (Lorsque ce paramètre est désactivé, les applications publiées par l'administrateur et les raccourcis Local App Access ne fonctionnent pas pour le VDA.)

Remarque : les modules complémentaires du navigateur requis pour la redirection d'adresse URL ne sont pas enregistrés automatiquement lorsque vous installez Citrix Receiver à partir de la ligne de commande avec l'option /ALLOW_CLIENTHOSTEDAPPSURL=1.

Vous pouvez utiliser les commandes suivantes pour enregistrer et annuler l'enregistrement d'un ou de tous les modules complémentaires :

- Pour enregistrer les composants sur une machine cliente : <*dossier-installation-client*>\redirector.exe /reg<*navigateur*>.
- Pour annuler l'enregistrement des composants sur une machine cliente : <*dossier-installation-client*>\redirector.exe /unreg<*navigateur*>.
- Pour enregistrer les composants sur un VDA :<*dossier-VDAinstallation*> \VDARedirector.exe /reg<*navigateur*>
- Pour annuler l'enregistrement des composants sur un VDA :<*dossier-VDAinstallation*> \VDARedirector.exe /unreg<*navigateur*>

où <*navigateur*> est IE, FF, Chrome ou tous.

Par exemple, la commande suivante enregistre les composants Internet Explorer sur une machine exécutant Citrix Receiver.

```
C:\Program Files\Citrix\ICA Client\redirector.exe/regIE
```

La commande suivante enregistre tous les composants d'un VDA avec OS Windows Server.

```
C:\Program Files (x86)\Citrix\System32\VDARedirector.exe /regAll
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Par défaut, Internet Explorer redirige l'adresse URL entrée. Si l'adresse URL ne figure pas dans la liste noire mais est redirigée vers une autre adresse URL par le navigateur ou un site Web, l'adresse URL finale n'est pas redirigée, même si elle est présente dans la liste noire.

  Pour que la redirection d'adresse URL fonctionne correctement, activez le module complémentaire lorsque vous y êtes invité par le navigateur. Si les modules complémentaires utilisant les options Internet ou les modules complémentaires dans l'invite de commande sont désactivés, la redirection d'adresse URL ne fonctionne pas correctement.

- Les modules complémentaires Firefox redirigent toujours les adresses URL.

  Lorsqu'un module complémentaire est installé, Firefox vous invite à autoriser/empêcher l'installation du module complémentaire dans un nouvel onglet. Vous devez autoriser le module complémentaire pour que la fonctionnalité fonctionne.

- Le module complémentaire Chrome redirige toujours l'adresse URL finale qui est ouverte et non pas les adresses URL saisies.

  Les extensions ont été installées en externe. Si vous désactivez l'extension, la fonctionnalité de redirection d'adresse URL ne fonctionne pas dans Chrome. Si la redirection d'adresse URL est requise en mode Incognito, autorisez l'exécution de l'extension dans ce mode dans la page de paramètres du navigateur.

1. Sur le bureau hébergé, exécutez **gpedit.msc**.
2. Accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session State. Pour un système 64 bits, accédez à HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies\Session State.
3. Ajoutez l'entrée Terminate de REG_DWORD avec l'une des valeurs suivantes :
   - 1 : les applications locales continuent de s'exécuter lorsqu'un utilisateur ferme sa session ou se déconnecte de l'ordinateur virtuel. Lors de la reconnexion, les applications locales sont réintégrées si elles sont disponibles dans l'environnement local.
   - 3 : les applications locales se ferment lorsqu'un utilisateur ferme sa session ou se déconnecte de l'ordinateur virtuel.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenApp Secure Browser

Jul 07, 2016

Étant donné que les applications sont portées vers le Web, les utilisateurs doivent avoir recours à plusieurs fournisseurs et versions de navigateur pour assurer la compatibilité avec les applications Web. Si l'application est une application hébergée en interne, les organisations sont souvent obligées d'installer et de configurer des solutions VPN complexes pour fournir un accès aux utilisateurs distants. Les solutions VPN standard requièrent un agent côté client qui doit être maintenu sur de nombreux systèmes d'exploitation.

Grâce à XenApp Secure Browser, les utilisateurs bénéficient d'une expérience transparente avec les applications Web hébergées ; l'application Web hébergée s'affiche simplement dans le navigateur local de l'utilisateur. Par exemple, le navigateur par défaut d'un utilisateur est Mozilla Firefox, mais l'application est uniquement compatible avec Microsoft Internet Explorer. XenApp Secure Browser affiche l'application compatible avec Internet Explorer en tant qu'onglet du navigateur Firefox.

Déploiement de XenApp Secure Browser

Citrix vous recommande de tirer parti du plan Lifecycle Management pour XenApp Secure Browser pour en faciliter le déploiement. Dans le cadre du lancement de XenApp version 7.9, tous les clients XenApp et XenDesktop existants avec des plans Software Maintenance (SWM) ou Subscription Advantage (SA) actifs ont accès à l'édition Deploy de Citrix Lifecycle Management.

XenApp Secure Browser comprend des scripts permettant d'automatiser les tâches suivantes :

- Installer XenApp, y compris le serveur de licences Citrix et StoreFront
- Créer un site de mise à disposition XenApp
- Joindre les machines provisionnées à votre domaine

Pour utiliser le plan Citrix Lifecycle Management :

1. Dans la page d'accueil Workspace Cloud, accédez à Services; cliquez sur Request Trial for Lifecycle Management. Lorsque vous effectuez une demande de version d'évaluation, vous recevez un e-mail vous informant que le service d'évaluation est disponible. Cet e-mail est généralement envoyé au bout de 5-10 minutes.
2. Cliquez sur Manage (Gérer) dans l'e-mail que vous avez reçu lorsque vous avez effectué la demande pour afficher la page Lifecycle Management Overview.
3. Téléchargez l'ISO Citrix XenApp Secure Browser Edition 7.9 depuis le site de téléchargement Citrix.

Prenez en compte les points suivants après le téléchargement de l'ISO Secure Browser Edition 7.9 :

- Commencez à utiliser XenApp Secure Browser en suivant les instructions fournies dans XenApp Secure Installation with a Citrix Lifecycle Management Blueprint.
- Après avoir effectué l'installation, optimisez votre environnement pour la mise à disposition d'applications Web à l'aide de la procédure de configuration spécifiée dans le Guide de déploiement de XenApp Secure Browser.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour installer manuellement XenApp Secure Browser version 7.9 :

1. Téléchargez l'ISO Citrix XenApp Secure Browser Edition 7.9 depuis le site de téléchargement Citrix.
2. Suivez les instructions d'installation des composants de XenApp.
3. Configurez le mode de licence et l'édition de Secure Browser après l'installation, en effectuant les étapes supplémentaires suivantes :

    a. Sur le Delivery Controller, démarrez une session PowerShell en cliquant sur l'icône bleue sur la barre des tâches, ou en accédant au menu Démarrer > Tous les programmes > Accessoires > Windows PowerShell > Windows PowerShell.

    Remarque : sur les systèmes 64 bits, cela démarre la version 64 bits. Les versions 32 bits et 64 bits sont prises en charge toutes les deux.

    b. Tapez Asnp Citrix* et appuyez sur Entrée pour charger les modules PowerShell spécifiques à Citrix.

    Remarque : « Asnp » représente Add-PSSnapin.

    c. Vérifiez les paramètres de site et le mode de licence en exécutant l'applet de commande Get-ConfigSite.

    d. Définissez le mode de licence sur l'édition XenApp Secure Browser en exécutant Set-ConfigSite -ProductCode XDT -ProductEdition BAS.

    e. Vérifiez que le mode de licence et l'édition de XenApp Secure Browser sont correctement définis en exécutant l'applet de commande Get-BrokerSite.

> ## Remarque
>
> Après avoir effectué l'installation, optimisez votre environnement pour la mise à disposition d'applications Web à l'aide de la procédure de configuration spécifiée dans le Guide de déploiement de XenApp Secure Browser.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Server VDI

Aug 22, 2016

Utilisez la fonctionnalité Server VDI (Virtual Desktop Infrastructure) pour mettre à disposition un bureau depuis un système d'exploitation serveur vers un utilisateur unique.

- Les administrateurs d'entreprise peuvent mettre à disposition des systèmes d'exploitation serveur en tant que bureaux VDI, ce qui peut être utile pour les utilisateurs tels que les ingénieurs et les concepteurs.
- Les fournisseurs de service peuvent offrir des bureaux depuis le cloud ; ces bureaux sont conformes avec Microsoft Services Provider License Agreement (SPLA).

Vous pouvez utiliser le paramètre de stratégie Expérience de bureau améliorée Citrix pour faire prendre au système d'exploitation serveur l'apparence d'un système d'exploitation Windows 7.

Les fonctionnalités suivantes ne peuvent pas être utilisées avec Server VDI :

- Personal vDisks
- Applications hébergées
- Local App Access
- Connexions de bureau directes (sans broker)
- Remote PC Access

Server VDI est pris en charge par les systèmes d'exploitation sur le même serveur que le VDA pour système d'exploitation Windows Server.

1. Préparez le serveur Windows pour l'installation : assurez-vous que les services de rôle des services Bureau à distance ne sont pas installés et que les utilisateurs sont restreints à une session unique :
   - Utilisez le Gestionnaire de serveur Windows pour vous assurer que les services de rôle des services Bureau à distance ne sont pas installés. Supprimez-les si précédemment installés.
   - Assurez-vous que la propriété « Restreindre chaque utilisateur à une seule session » est activée.
     - Sur Windows Server 2008 R2, accédez à cette propriété via Outils d'administration > Services Bureau à distance > Configuration d'hôte de session Bureau à distance. Dans la section Modifier les paramètres > Général, le paramètre Restreindre chaque utilisateur à une seule session devrait indiquer Oui.
     - Sur Windows Server 2012, modifiez le Registre et définissez le paramètre de Terminal Server. Dans la clé de registre HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer définissez la valeur DWORD fSingleSessionPerUser sur 1.
2. Pour Windows Server 2008 R2, installez Microsoft .NET Framework 3.5 SP1 sur le serveur avant d'installer le VDA.
3. Utilisez l'interface de ligne de commande pour installer un VDA sur un serveur pris en charge ou sur une image principale de serveur, en spécifiant les options /quiet et /servervdi : Par défaut, le programme d'installation bloque le VDA avec OS Windows Desktop sur un système d'exploitation serveur ; l'utilisation de la ligne de commande remplace ce comportement.
   XenDesktopVdaSetup.exe /quiet /servervdi

   Vous pouvez spécifier le Delivery Controller ou les Controller lors de l'installation du VDA à l'aide de la ligne de commande, avec l'option **/controllers**.

   Utilisez l'option **/enable_hdx_ports** pour ouvrir des ports dans le pare-feu, sauf si le pare-feu doit être configuré manuellement.

   Ajoutez l'option **/masterimage** si vous installez le VDA sur une image, et que vous allez utiliser MCS pour créer des VM

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de serveur depuis cette image.

Ajoutez l'option **/enable_hdx_3d_pro** pour configurer le VDA en mode HDX 3D Pro.

N'incluez pas les options des fonctionnalités qui ne sont pas prises en charge avec Server VDI, telles que /baseimage ou /xa_server_location.

4. Créer un catalogue de machines pour Server VDI.
   1. Sur la page Système d'exploitation, sélectionnez **Système d'exploitation de bureau**.
   2. Sur la page Résumé, spécifiez un nom de catalogue de machines et une description pour les administrateurs qui l'identifient clairement en tant que Server VDI ; ce sera le seul indicateur dans Studio que le catalogue prend Server VDI en charge.

   Lors de l'utilisation de la fonction de recherche dans Studio, le catalogue Server VDI que vous avez créé s'affichera sur la page de l'onglet Machines avec OS de bureau, même si le VDA a été installé sur un serveur.

5. Créez un groupe de mise à disposition et attribuez le catalogue Server VDI que vous avez créé à l'étape précédente.

Si vous n'avez pas spécifié les Delivery Controller lors de l'installation du VDA, spécifiez-les après à l'aide du paramètre de stratégie Citrix, Active Directory, ou en modifiant les valeurs de registre de la machine VDA.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Personal vDisk

Jul 07, 2016

La fonctionnalité Personal vDisk permet de gérer une image unique de bureaux regroupés et streamés tout en autorisant les utilisateurs à installer des applications et à modifier leurs paramètres de bureau. Contrairement aux déploiements VDI (infrastructure de bureau virtuel) traditionnels impliquant des bureaux regroupés, dans lesquels les utilisateurs perdent les personnalisations qu'ils ont apportées et leurs applications personnelles lorsque l'administrateur modifie l'image principale, les déploiements utilisant des Personal vDisk conservent ces changements. Cela signifie que les administrateurs peuvent facilement gérer de manière centralisée leurs images principales tout en offrant aux utilisateurs une expérience de bureau personnalisée.

Personal vDisk offre cette séparation en redirigeant toutes les modifications apportées à la VM de l'utilisateur vers un disque distinct (le personal vDisk) connecté à la VM de l'utilisateur. Le contenu du Personal vDisk est fusionné au moment de l'exécution avec le contenu de l'image principale afin d'offrir une expérience unifiée. Ainsi, les utilisateurs peuvent toujours accéder aux applications approvisionnées par leur administrateur dans l'image principale.

Les Personal vDisk possèdent deux parties, qui utilisent différentes lettres de lecteur et sont de même taille par défaut :

- Profil utilisateur : contient les données utilisateur, les documents, et le profil de l'utilisateur. Par défaut, cette partie utilise le lecteur P: mais vous pouvez choisir une lettre de lecteur différente lorsque vous créez un catalogue de machines avec des machines qui utilisent des Personal vDisks. Le lecteur utilisé dépend également du paramètre EnableUserProfileRedirection.
- Fichier du disque dur virtuel (.vhd) : ce fichier contient tous les autres éléments, par exemple les applications installées dans C:\Program Files. Cette dernière n'est pas affichée dans Windows Explorer et ne nécessite pas de lettre de lecteur depuis la version 5.6.7.

Les Personal vDisk prennent en charge le provisioning d'applications au niveau du département, ainsi que les applications téléchargées et installées par les utilisateurs, y compris celles nécessitant des pilotes (mis à part les pilotes de phase 1), les bases de données et le logiciel de gestion de machine. Si une modification effectuée par un utilisateur entre en conflit avec une modification effectuée par un administrateur, un Personal vDisk offre une manière simple et automatique de concilier les modifications.

De plus, les applications administrées localement (telles que celles approvisionnées et gérées par les départements informatiques locaux) peuvent également être approvisionnées dans l'environnement de l'utilisateur. L'utilisateur n'observe aucune différence en termes de facilité d'utilisation ; Personal vDisk s'assure que toutes les modifications apportées et toutes les applications installées sont stockées sur le disque virtuel. Lorsqu'une application figurant sur un disque virtuel personnel est identique à une application figurant sur une image principale, la copie figurant sur le Personal vDisk est supprimée pour gagner de l'espace sans pour autant que l'utilisateur perde l'accès à l'application.

Les Personal vDisks sont stockés sur l'hyperviseur mais ils n'ont pas besoin d'être dans le même emplacement que d'autres disques attachés à ce bureau virtuel. Cela permet de réduire les coûts de stockage du Personal vDisk.

Au cours de la création d'un site, lorsque vous créez une connexion, vous définissez des emplacements de stockage pour les disques utilisés par les machines virtuelles. Vous pouvez séparer les Personal vDisks des disques utilisés par le système d'exploitation. Chaque machine virtuelle doit avoir accès à un emplacement de stockage pour les deux disques. Si le stockage local est utilisé pour les deux disques, ils doivent être accessibles à partir du même hyperviseur. Pour vous assurer que la configuration requise est présente, Studio offre uniquement des emplacements de stockage compatibles. Plus tard, vous pouvez également ajouter des Personal vDisks et du stockage sur les hôtes existants (mais pas les catalogues de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

machines) dans Configuration > Hébergement dans Studio.

Sauvegardez régulièrement les Personal vDisks à l'aide de la méthode de votre choix. Les vDisks sont des volumes standards dans un niveau de stockage hyperviseur, vous pouvez donc les sauvegarder comme tout autre volume.

Les améliorations suivantes sont comprises dans cette version :

- Cette version de Personal vDisk contient des améliorations au niveau des performances qui réduisent la durée requise pour appliquer la mise à jour d'une image à un catalogue Personal vDisk.

Les problèmes connus suivants ont été résolus dans cette version :

- La tentative de mise à niveau sur place d'une machine virtuelle de base depuis Microsoft Office 2010 vers Microsoft Office 2013 entraînait l'affichage d'une fenêtre de reconfiguration suivi d'un message d'erreur ; « Erreur 25004. La clé de produit que vous avez entrée ne peut pas être utilisée sur cet ordinateur. Dans le passé, il était recommandé de désinstaller Office 2010 sur la machine virtuelle de base avant d'installer Office 2013. Il n'est plus désormais nécessaire de désinstaller Office 2010 lors de l'exécution d'une mise à niveau sur place de la machine virtuelle de base (#391225).
- Durant le processus de mise à jour de l'image, si une version supérieure de Microsoft .Net était installée sur le Personal vDisk de l'utilisateur, elle était remplacée par une version inférieure provenant de l'image de base. Cela entraînait des problèmes pour les utilisateurs exécutant certaines applications installées sur leur Personal vDisk qui nécessitaient la version supérieure, telles que Visual Studio (#439009).
- Un disque doté d'une image Provisioning Services sur laquelle un Personal vDisk a été installé et activé ne peut pas être utilisé pour créer un catalogue de machines ne possédant pas de Personal vDisk. Cette restriction a été supprimée (#485189).

Nouveautés dans la version 7.6 :

- Gestion et notification des erreurs améliorées dans Personal vDisk. Dans Studio, lorsque vous afficher les machines PvD dans un catalogue, un onglet « PvD » fournit un statut de contrôle lors des mises à jour de l'image, ainsi que l'heure de fin et de progression estimée. Des affichages améliorés de l'état sont également fournis.
- Un outil de contrôle de la mise à jour de l'image Personal vDisk est disponible pour les versions antérieures sur le support ISO (ISO\Support\Tools\Scripts\PvdTool). Des capacités de contrôle sont prises en charge pour les versions précédentes, toutefois les capacités de reporting ne seront pas aussi robustes comparées à celles de la version actuelle.
- Le mode de test Provisioning Services vous permet de redémarrer les machines avec une image mise à jour d'un catalogue de test. Après avoir vérifié la stabilité, vous pouvez promouvoir la version de test de Personal vDisk en production.
- Une nouvelle fonctionnalité vous permet de calculer l'écart entre deux inventaires lors d'un inventaire, au lieu de le calculer pour chaque bureau PvD. De nouvelles commandes sont fournies pour l'exportation et l'importation d'un inventaire précédent pour les catalogues MCS. (Les vDisks principaux de Provisioning Services disposent déjà de l'inventaire précédent.)

Problèmes connus de la version 7.1.3 résolus dans la version 7.6 :

- L'interruption de la mise à niveau d'une installation de Personal vDisk pouvait endommager une installation Personal vDisk existante. [#424878]
- Un bureau virtuel pouvait cesser de répondre si le Personal vDisk était exécuté pendant une longue période et qu'une fuite de mémoire non paginée se produisait. [#473170]

Nouveaux problèmes connus dans la version 7.6 :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- La présence de produits anti-virus peut affecter la durée nécessaire pour exécuter l'inventaire ou effectuer une mise à jour. Les performances peuvent être améliorées si vous ajoutez CtxPvD.exe et CtxPvDSvc.exe à la liste d'exclusion PROCESS de votre produit anti-virus. Ces fichiers sont situés dans C:\Program Files\Citrix\personal vDisk\bin. [#326735]
- Les liens directs entre fichiers hérités de l'image principale ne sont pas conservés dans les catalogues Personal vDisk. [#368678]
- Après la mise à niveau de Microsoft Office 2010 vers 2013 sur l'image principale Personal vDisk, Office ne parviennent pas à démarrer sur des machines virtuelles, car la clé de produit Office licences KMS a été supprimée lors de la mise à niveau. Pour contourner le problème, désinstallez Office 2010 et réinstallez Office 2013 sur l'image principale. [#391225]
- Les catalogues Personal vDisk ne prennent pas en charge les contrôleurs VMware Paravirtual SCSI (PVSCSI). Pour éviter ce problème, utilisez le contrôleur par défaut. [#394039]
- Pour les bureaux virtuels créés avec Personal vDisk 5.6.0 et qui sont mis à niveau vers la version 7, les utilisateurs ayant ouvert une session sur la machine virtuelle (VM) principale précédemment risquent de ne pas pouvoir localiser leurs fichiers dans leur VM regroupée. Ce problème se produit car un nouveau profil utilisateur est créé lorsqu'ils se connectent à leurs VM regroupées. Il n'existe pas de solution pour ce problème. [#392459]
- Les Personal vDisks exécutant Windows 7 ne peuvent pas utiliser la fonctionnalité Sauvegarde et restauration lorsque la fonction de protection système de Windows est activée. Si la protection du système est désactivée, le profil utilisateur est sauvegardé, mais le fichier userdata.v2.vhd ne l'est pas. Citrix vous recommande de désactiver la protection du système et d'utiliser la fonctionnalité de sauvegarde et restauration pour sauvegarder le profil de l'utilisateur. [#360582]
- Lorsque vous créez un fichier VHD sur la VM de base à l'aide de l'outil de gestion du disque, vous risquez de ne pas être en mesure de monter le VHD. Pour contourner le problème, copiez le VHD sur le volume PvD. [#355576]
- Les raccourcis Office 2010 restent disponibles sur les bureaux virtuels après suppression de ce logiciel. Pour contourner ce problème, supprimez les raccourcis. [#402889]
- Lors de l'utilisation de Microsoft Hyper-V, vous ne pouvez pas créer un catalogue de machines avec des Personal vDisks lorsque les machines sont stockées localement et les vDisks sont stockés sur les volumes partagés de cluster (CSVs) ; la création de catalogue échoue avec une erreur. Pour contourner ce problème, utilisez une autre configuration de stockage pour les vDisks. [#423969]
- Lorsque vous ouvrez une session pour la première fois sur un bureau virtuel créé à partir d'un catalogue Provisioning Services, le bureau vous invite à redémarrer si le Personal vDisk a été réinitialisé (à l'aide de la commande ctxpvd.exe -s reset). Pour contourner ce problème, redémarrez le bureau lorsque vous y êtes invité. Ceci est une réinitialisation unique qui n'est pas nécessaire lorsque vous ouvrez une session à nouveau. [#340186]
- Si vous installez .NET 4.5 sur un Personal vDisk et la mise à jour d'image installe ou modifie .NET 4.0, les applications qui dépendent de .NET 4.5 échouent. Pour contourner ce problème, distribuez .NET 4.5 à partir de l'image de base en tant qu'image mise à jour.
- Consultez également la section
  — Problèmes connus
  de la documentation relative à la version XenApp et XenDesktop 7.6.

Problèmes connus de la version 7.1.1 résolus dans la version 7.1.3 :

- Les mises à niveau directes depuis Personal vDisk 5.6.0 vers Personal vDisk 7.x pouvaient entraîner l'échec de Personal vDisk. [#432992]
- Les utilisateurs ne pouvaient se connecter que de façon intermittence à des bureaux virtuels avec des Personal vDisks. [#437203]
- Si une opération de mise à jour d'image Personal vDisk était interrompue alors que Personal vDisk 5.6.5 ou version supérieure était mis à niveau vers Personal vDisk 7.0 ou version supérieure, les opérations de mise à jour ultérieures pouvaient échouer. [#436145]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problèmes connus de la version 7.1 résolus dans la version 7.1.1 :

- La mise à niveau de Symantec Endpoint Protection 12.1.3 via une mise à jour d'image provoque le signalement par symhelp.exe de définitions antivirus endommagées. [#423429]
- Personal vDisk peut entraîner le redémarrage des bureaux regroupés lorsque le Gestionnaire de contrôle des services (services.exe) se bloque. [#0365351]

Nouveaux problèmes connus dans la version 7.1.1 : aucun

Nouveautés dans la version 7.1 :

- Vous pouvez maintenant utiliser Personal vDisk avec des bureaux exécutant Windows 8.1, et la journalisation des événements a été améliorée.
- Copy-on-Write (CoW) n'est plus pris en charge. Lors de la mise à niveau de la version 7.0 vers la version 7.1 de Personal vDisk, toutes les modifications apportées aux données gérées par CoW sont perdues. Cette fonctionnalité était disponible à des fins d'évaluation dans XenDesktop 7 et était désactivée par défaut ; vous n'êtes pas affecté si elle n'était pas activée.

Problèmes connus de la version 7.0.1 résolus dans la version 7.1 :

- Si la valeur de la clé de Registre Personal vDisk EnableProfileRedirection est définie sur 1 ou ON, et plus tard, lors de la mise à jour de l'image, vous la changez en 0 ou OFF, l'ensemble de l'espace Personal vDisk peut se voir allouer aux applications installées par l'utilisateur, ne laissant plus d'espace pour les profils utilisateur, qui restent sur le vDisk. Si la redirection de profil est désactivée pour un catalogue et que vous l'activez durant la mise à jour d'une image, il est possible que les utilisateurs ne puissent pas ouvrir de session sur leur bureau virtuel. [#381921]
- Le service Bureau ne journalise pas l'erreur appropriée dans l'Observateur d'événements lorsque la mise à jour d'un inventaire Personal vDisk échoue. [#383331]
- Lors de la mise à niveau vers Personal vDisk 7.x, les règles modifiées ne sont pas préservées. Ce problème a été résolu pour les mises à niveau de la version 7.0 vers la version 7.1. Lors de la mise à niveau de la version 5.6.5 vers la version 7.1, vous devez d'abord enregistrer le fichier de règles et ensuite appliquer de nouveau les règles après la mise à niveau. [#388664]
- Les Personal vDisks exécutant Windows 8 ne peuvent pas installer d'applications à partir de Windows Store. Un message d'erreur s'affiche indiquant « Impossible de terminer votre achat » s'affiche. L'activation du service Windows Update ne résout pas ce problème, ce qui a été résolu. Toutefois, les applications installées par l'utilisateur doivent être réinstallées après redémarrage du système. [#361513]
- Certains liens symboliques sont absents des bureaux groupés Windows 7 avec Personal vDisks. Par conséquent, les applications qui stockent les icônes dans C:\Utilisateurs\Tous les utilisateurs n'affichent pas ces icônes dans le menu Démarrer. [#418710]
- Un Personal vDisk ne démarre si la taille du journal USN est dépassée en raison d'un grand nombre de modifications apportées au système après la mise à jour d'un inventaire. [#369846]
- Un Personal vDisk ne démarre pas avec un code d'état 0x20 et un code d'erreur 0x20000028. [#393627]
- Symantec Endpoint Protection 12.1.3 affiche le message « Proactive Threat Protection is malfunctioning » et l'état de la mise à jour en cours de ce composant n'est pas disponible. [#390204]

Nouveaux problèmes connus dans la version 7.1 : consultez la section
— Problèmes connus
de la documentation pour la version XenDesktop 7.1.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nouveautés dans la version 7.0.1 : Personal vDisk est désormais plus robuste aux modifications de l'environnement. Les bureaux virtuels équipés de Personal vDisks s'enregistrent maintenant auprès du Delivery Controller même si les mises à jour de l'image échouent, et les arrêts non sécurisés du système ne placent plus les vDisks dans un état désactivé permanent. Par ailleurs, l'utilisation de fichiers de règles vous permet maintenant d'exclure des fichiers et dossiers des vDisks lors d'un déploiement.

Problèmes connus de la version 5.6.13 résolus dans la version 7.0.1 :

- Les modifications apportées à l'appartenance à un groupe par les utilisateurs d'un bureau virtuel regroupé peuvent être perdues après la mise à jour d'une image. [#286227]
- Les mises à jour d'images peuvent échouer et invoquer un espace disque insuffisant même si le Personal vDisk dispose de suffisamment d'espace. [#325125]
- Certaines applications ne s'installent pas sur les bureaux virtuels équipés d'un Personal vDisk, et un message indiquant qu'un redémarrage est requis s'affiche. Ceci est dû à une opération de changement de nom en attente. [#351520]
- Les liens symboliques créés dans l'image principale ne fonctionnent pas sur les bureaux virtuels équipés de Personal vDisks. [#352585]
- Dans les environnements qui utilisent Citrix Profile Management et Personal vDisk, les applications qui examinent les profils utilisateur sur un volume système peuvent ne pas fonctionner correctement si la redirection de profil est activée. [#353661]
- Le processus de mise à jour de l'inventaire échoue sur les images principales lorsque la taille de l'inventaire est supérieure à 2 Go. [#359768]
- Les mises à jour d'images échouent avec le code d'erreur 112 et les Personal vDisks sont corrompus même s'ils disposent de suffisamment d'espace pour accommoder la mise à jour. [#363003]
- Le script de redimensionnement échoue pour les catalogues comptant plus de 250 bureaux. [#363365]
- Les modifications apportées par les utilisateurs à une variable d'environnement sont perdues lorsqu'une image est mise à jour. [#372295]
- Les utilisateurs locaux créés sur un bureau virtuel équipé d'un Personal vDisk sont perdus lorsqu'une image est mise à jour. [#377964]
- Un Personal vDisk peut ne pas démarrer si la taille du journal USN est dépassée en raison d'un grand nombre de modifications apportées au système après la mise à jour d'un inventaire. Pour éviter ce problème, augmentez la taille du journal USN jusqu'à un minimum de 32 Mo dans l'image principale et effectuez une mise à jour d'image. [#369846]
- Un problème qui empêche le bon fonctionnement des actions effectuées dans la ruche de registre AppSense Environment Manager lorsque AppSense est utilisé en mode Replace a été détecté avec Personal vDisk. Citrix et AppSense travaillent ensemble à la résolution du problème, qui est lié au comportement de l'API RegRestoreKey lors de l'installation de Personal vDisk.[#0353936]

- Lorsqu'une application installée sur un Personal vDisk (PvD) est liée à une autre application de la même version installée sur l'image principale, l'application sur le PvD peut s'arrêter de fonctionner après une mise à jour d'image. Ceci se produit si vous désinstallez l'application à partir de l'image principale ou si vous effectuez une mise à niveau vers une version plus récente, car cette action supprime les fichiers nécessaires à l'application sur le PvD à partir de l'image principale. Pour éviter ce problème, gardez l'application contenant les fichiers nécessaires à l'application sur le PvD sur l'image principale. Par exemple, l'image principale contient Office 2007 et un utilisateur installe Visio 2007 sur le PvD ; les applications Office et Visio fonctionnent correctement. Plus tard, l'administrateur remplace Office 2007 avec Office 2010 sur l'image principale, puis met à jour toutes les machines affectées par l'image mise à jour. Visio 2007 ne fonctionne plus. Pour éviter ce problème, gardez Office 2007 dans l'image principale. [#320915]

- Lors du déploiement de McAfee Virus Scan Enterprise (VSE), utilisez la version 8.8 correctif 4 ou version ultérieure sur une

© 1999-2017 Citrix Systems, Inc. All rights reserved.

image principale si vous utilisez Personal vDisk. [#303472]

- Si un raccourci créé vers un fichier dans l'image principale cesse de fonctionner (car le raccourci cible est renommé au sein de PvD), recréez le raccourci. [#367602]
- N'utilisez pas de liens absolus/directs dans une image principale. [#368678]
- La fonctionnalité de sauvegarde et de restauration de Windows 7 n'est pas prise en charge sur le Personal vDisk. [#360582]
- Après qu'une mise à jour de l'image principale ait été appliquée, l'utilisateur local et la console de groupe sont inaccessibles ou affichent des données incohérentes. Pour résoudre le problème, réinitialisez les comptes d'utilisateur sur la VM, ce qui nécessite la réinitialisation de la ruche de sécurité. Ce problème est résolu dans la version 7.1.2 (et fonctionne pour les machines virtuelles créées dans les versions ultérieures), mais le correctif ne fonctionne pas pour les machines virtuelles qui ont été créées avec une version antérieure puis mises à niveau. [#488044]
- Lors de l'utilisation d'une VM regroupée sur un environnement d'hyperviseur ESX, les utilisateurs voient une invite de redémarrage si le type de contrôleur SCSI sélectionné est de type « VMware Paravirtual ». Pour résoudre ce problème, utilisez un type de contrôleur LSI SCSI. [#394039]
- Après une réinitialisation de PvD sur un bureau créé à l'aide de Provisioning Services, il se peut que les utilisateurs reçoivent une invite de redémarrage après l'ouverture de session sur la VM. Pour contourner le problème, redémarrez le bureau. [#340186]
- Les utilisateurs de bureaux Windows 8.1 peuvent ne pas être en mesure d'ouvrir une session sur leurs PvD. Un administrateur peut voir le message « PvD was disabled due to unsafe shutdown » et le journal PvDActivation peut contenir le message « Failed to load reg hive [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]. ». Ceci se produit lorsque la VM de l'utilisateur n'est pas arrêtée correctement. Pour contourner le problème, réinitialisez le Personal vDisk. [#474071]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Installation et mise à niveau

Jul 07, 2016

Personal vDisk 7.x est pris en charge pour XenDesktop 5.6 jusqu'à la version actuelle. La documentation « Configuration requise » pour chaque version de XenDesktop dresse la liste des systèmes d'exploitation pris en charge par Virtual Delivery Agents (VDA), et les versions prises en charge des hôtes (ressources de virtualisation) et Provisioning Services. Pour de plus amples informations sur les tâches Provisioning Services, consultez la documentation Provisioning Services.

PvD est installé automatiquement lorsque vous installez ou mettez à niveau un VDA pour OS de bureau sur une machine. Si vous mettez à jour le logiciel PvD après l'installation du VDA, utilisez le fichier MSI PvD fourni sur le support d'installation de XenApp ou XenDesktop.

Activation du PvD :

- Si vous utilisez Machine Creation Services (MCS), PvD est automatiquement activé lorsque vous créez un catalogue de machines avec des machines avec OS de bureau qui utiliseront un Personal vDisk.
- Si vous utilisez Provisioning Services (PVS), PvD est automatiquement activé lorsque vous exécutez l'inventaire pendant le processus de création d'image (de base) principale, ou lors de la mise à jour automatique de l'inventaire pour vous.

L'installation de VDA offre des options pour activer PvD (en sélectionnant la case à cocher « Personal vDisk » dans l'interface graphique ou en spécifiant l'option /baseimage dans l'interface de ligne de commande). Toutefois, l'oubli de cette action lors de l'installation du VDA (par défaut) vous permet toujours d'utiliser la même image pour créer des bureaux PvD et non-PvD, car PvD est activé lors du processus de création de catalogue.

Vous ajoutez des Personal vDisks à des hôtes lorsque vous configurez un site. Vous pouvez choisir d'utiliser le même stockage sur l'hôte pour les VM et Personal vDisks, ou vous pouvez utiliser un stockage différent pour les Personal vDisks.

Plus tard, vous pouvez également ajouter des Personal vDisks et leur stockage à des hôtes existants (connexions), mais pas des catalogues de machines.

1. Sélectionnez Configuration > Hébergement dans le volet de navigation de Studio.
2. Sélectionnez Ajouter un stockage Personal vDisk dans le volet Actions et spécifiez l'emplacement de stockage.

La manière la plus facile de mettre à niveau Personal vDisk à partir d'une version antérieure à la version 7.x est simplement de mettre à niveau les VDA de votre système d'exploitation de bureau vers la version fournie avec la dernière version de XenDesktop. Exécutez ensuite l'inventaire PvD.

Vous pouvez également mettre uniquement à niveau PvD à l'aide du fichier MSI de PvD à partir d'ici.

Vous pouvez utiliser l'une des deux manières suivantes pour supprimer le logiciel PvD :

- Désinstaller le VDA ; cette option supprime également le logiciel PvD.
- Si vous avez mis PvD à jour à l'aide du fichier MSI PvD, vous pouvez effectuer la désinstallation à partir de la liste des programmes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si vous désinstallez PvD et que vous réinstallez la même version ou une version plus récente, sauvegardez la clé de registre HKLM\Software\Citrix\personal vDisk\config, qui contient les paramètres de configuration d'environnement susceptibles d'avoir été modifiés. Ensuite, après l'installation de PvD, réinitialisez les valeurs de registre qui peuvent avoir été modifiés en les comparant avec la version sauvegardée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurer et gérer

Jul 07, 2016

Cette rubrique décrit les éléments à prendre en compte lors de la configuration et de la gestion d'un environnement de Personal vDisk (PvD). Il couvre également des instructions et des descriptions de tâche conseillées.

Pour les procédures qui incluent l'utilisation du registre Windows :
Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

Les facteurs suivants affectent la taille du volume Personal vDisk principal :

- **Taille des applications que les utilisateurs installeront sur leurs PvD.**
  À chaque redémarrage, PvD détermine l'espace disponible restant dans la zone applicative (UserData.v2.vhd). Si cet espace tombe en dessous de 10 %, la zone applicative est étendue de façon à utiliser tout espace non utilisé dans la zone dédiée aux profils (par défaut, l'espace disponible sur le lecteur P:). L'espace ajouté à la zone applicative équivaut à 50 % de l'espace disponible combiné restant dans la zone applicative et la zone des profils.

  À titre d'exemple, si la zone applicative sur un PvD de 10 Go, qui est par défaut de 5 Go, atteint 4,7 Go et que la zone des profils dispose de 3 Go disponibles, l'espace ajouté à la zone applicative est calculé comme suit :

  Espace accru = (5.0 - 4.7)/2 + 3.0/2 = 1.65 Go

  L'espace ajouté à la zone applicative est approximatif car une provision est constituée pour le stockage des journaux et les surcharges potentielles. Le calcul et le dimensionnement possible sont effectués à chaque redémarrage.

- **Taille des profils utilisateur (si aucune solution de gestion des profils distincte n'est utilisée).**
  En plus de l'espace requis pour les applications, assurez-vous qu'il y ait suffisamment d'espace disponible sur les Personal vDisks pour stocker les profils utilisateur. Incluez tous les dossiers spéciaux non redirigés (tels que Mes documents et Ma musique) lors du calcul de l'espace requis. La taille des profils existants est disponible dans le Panneau de configuration (sysdm.cpl).

  Certaines solutions de redirection de profil stockent les fichiers stub (fichiers sentinel) à la place des données de profil réelles. Ces solutions de gestion des profils peuvent sembler ne stocker aucune donnée initialement, mais elles consomment en fait une entrée du répertoire du fichier dans le système de fichiers par fichier stub (environ 4 Ko par fichier). Si vous utilisez une telle solution, évaluez la taille en fonction des données de profil réelles et non des fichiers stub.

  Les applications de partage des fichiers d'entreprise (telles que ShareFile et Dropbox) peuvent synchroniser ou télécharger des données sur les zones de profil des utilisateurs sur les Personal vDisks. Si vous utilisez de telles applications, incluez suffisamment d'espace dans votre estimation de taille pour ces données.

- **Quantité de mémoire consommée par le VHD modèle contenant l'inventaire PvD.**
  Le VHD modèle contient les données d'inventaire PvD (fichiers sentinelles correspondant au contenu de l'image principale). La zone applicative PvD est créée depuis ce VHD. Étant donné que chaque fichier ou dossier sentinel contient une entrée de répertoire de fichier dans le système de fichiers, le contenu du VHD modèle consomme l'espace applicatif PvD avant même que des applications ne soient installées par les utilisateurs. Vous pouvez déterminer la taille du VHD

© 1999-2017 Citrix Systems, Inc. All rights reserved.

modèle en consultant l'image principale après la réalisation d'un inventaire. Vous pouvez également utiliser l'équation suivante pour effectuer un calcul approximatif :

Taille du modèle VHD = (nombre de fichiers sur l'image de base) x 4 Ko

Déterminez le nombre de fichiers et de dossiers en cliquant avec le bouton droit de la souris sur le lecteur C: sur l'image de VM de base et en sélectionnant Properties. À titre d'exemple, une image contenant 250 000 fichiers équivaut à un VHD modèle d'environ 1 024 000 000 octets (un peu moins d'1 Go). Cet espace ne pourra pas être utilisé pour l'installation d'applications dans la zone applicative PvD.

- **Quantité de mémoire utilisée par les opérations de mise à jour de l'image PvD**
  Durant les opérations de mise à jour de l'image PvD, un espace suffisant doit être disponible à la racine du PvD (par défaut, P:) afin de fusionner les modifications apportées aux deux versions de l'image et les modifications apportées par l'utilisateur à son PvD. En général, PvD se réserve quelques centaines de Mo à cette fin, mais les données supplémentaires écrites sur le lecteur P: peuvent consommer cet espace réservé et laisser un espace insuffisant pour mener à bien la mise à jour de l'image. Le script de statistiques du pool PvD (situé sur le support d'installation XenDesktop dans le dossier Support/Tools/Scripts) ou de la mise à jour de l'image PvD dans l'outil d'analyse (dans le dossier Support/Tools/Scripts/PvdTool) peut vous aider à identifier les disques PvD d'un catalogue en cours de mise à jour et qui sont presque plein.

  La présence de produits anti-virus peut affecter la durée nécessaire pour exécuter l'inventaire ou effectuer une mise à jour. Les performances peuvent s'améliorer si vous ajoutez CtxPvD.exe et CtxPvDSvc.exe à la liste d'exclusion de votre produit anti-virus. Ces fichiers sont situés dans C:\Program Files\Citrix\personal vDisk\bin. L'exclusion de ces exécutables de l'analyse du logiciel antivirus peut décupler les performances liées à l'inventaire et à la mise à jour d'image jusqu'à un facteur de 10.

- **La quantité de mémoire utilisée pour la croissance non anticipée (installation d'applications imprévue, etc).**
  Surestimez la taille totale (une quantité fixe ou un pourcentage de la taille du vDisk) afin de tenir compte de l'installation d'applications imprévues effectuées par l'utilisateur lors du déploiement.

Vous pouvez régler manuellement l'algorithme de redimensionnement automatique qui détermine la taille du VHD relative au lecteur P:, en définissant la taille initiale du VHD. Ceci peut être utile si, par exemple, vous savez que vos utilisateurs vont installer un certain nombre d'applications qui sont trop importantes pour contenir sur le VHD même après son redimensionnement par l'algorithme. Dans ce cas, vous pouvez augmenter la taille initiale de l'espace des applications pour accommoder les applications installées par l'utilisateur.

Il est préférable de régler la taille initiale du VHD sur une image principale. Éventuellement, vous pouvez régler la taille du VHD sur un bureau virtuel lorsqu'un utilisateur ne dispose pas de suffisamment d'espace pour installer une application. Cependant, vous devez répéter cette opération sur chaque bureau virtuel affecté ; vous ne pouvez pas régler la taille initiale du VHD dans un catalogue déjà créé.

assurez-vous que le VHD est assez important pour stocker des fichiers de définition antivirus, qui sont généralement importants.

Recherchez et définissez les clés de registre suivantes dans HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\personal vDisk\Config. (Ne modifiez pas d'autres paramètres de cette clé de Registre). Tous les paramètres doivent être spécifiés sur l'image principale (sauf pour MinimumVHDSizeInMB, qui peut être modifié sur un ordinateur individuel) ; les paramètres spécifiés sur l'image principale sont appliqués lors de la mise à jour d'image suivante.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- MinimumVHDSizeMB
  Spécifie la taille minimale (en mégaoctets) de la partie applicative (C:) du Personal vDisk. La nouvelle taille doit être supérieure à la taille existante mais inférieure à la taille du disque moins PvDReservedSpaceMB.

  L'augmentation de cette valeur alloue l'espace disponible de la partie réservée aux profils sur le vDisk à C:. Ce paramètre est ignoré si une valeur inférieure à la taille actuelle du lecteur C: est utilisée, ou si EnableDynamicResizeOfAppContainer est défini sur 0.

  Valeur par défaut = 2048

- EnableDynamicResizeOfAppContainer
  Active ou désactive l'algorithme de redimensionnement dynamique.
  - Lorsque cette option est définie sur 1, l'espace de l'application (C:) est redimensionné automatiquement lorsque l'espace libre sur C: est inférieur à 10%. Les valeurs autorisées sont 1 et 0. Un redémarrage est requis pour que le redimensionnement soit pris en compte.
  - Lorsque cette option est définie sur 0, la taille du VHD est déterminée en fonction de la méthode utilisée dans les versions antérieures à la version 7.x de XenDesktop

  Valeur par défaut = 1

- EnableUserProfileRedirection
  Active ou désactive la redirection du profil de l'utilisateur vers le vDisk.
  - Lorsque cette option est définie sur 1, PvD redirige les profils des utilisateurs sur le lecteur Personal vDisk (P: par défaut). Les profils sont généralement redirigés vers P:\Utilisateurs, ce qui correspond à un profil Windows standard. Cette redirection préserve les profils dans le cas où le bureau PvD doit être réinitialisé.
  - Lorsqu'elle est définie sur 0, tout l'espace disponible sur le vDisk moins PvDReservedSpaceMB est alloué à C:, la partie applicative du vDisk, et le lecteur du vDisk (P:) est masqué dans l'Explorateur Windows. Citrix vous recommande de désactiver la redirection en définissant la valeur sur 0, lorsque vous utilisez Citrix Profile Management ou une autre solution de gestion des profils itinérants.
    Ce paramètre permet de conserver les profils dans C:\Users plutôt que les rediriger vers le vDisk, et permet à la solution de profils itinérants de gérer les profils.

    Cette valeur assure que tout l'espace présent sur P: est attribué aux applications.

    Ceci suppose que cette valeur est définie sur 0, et qu'une solution de gestion des profils est en place. Si vous ne disposez pas d'une solution de gestion des profils itinérants, la désactivation de la redirection des profils n'est pas recommandée car les opérations de réinitialisation de PvD ultérieures entrainent la suppression des profils.

  Ne modifiez pas ce paramètre lorsque l'image est mise à jour car il ne modifie pas l'emplacement des profils existants mais il allouera tout l'espace disponible sur le Personal vDisk à C: et masquera le PvD.

  Configurez cette valeur avant de déployer un catalogue. Vous ne pouvez pas le modifier une fois que le catalogue est déployé.

  Important : à compter de XenDesktop 7.1, les modifications apportées à cette valeur ne sont pas appliquées lorsque vous effectuez une mise à jour d'image. Définissez la valeur de la clé lorsque vous créez tout d'abord le catalogue depuis lequel les profils proviennent. Vous ne pouvez pas modifier le comportement de redirection ultérieurement.
  Valeur par défaut = 1

- PercentOfPvDForApps
  Définit la répartition entre la partie applicative (C:) et la partie réservée aux profils du vDisk. Cette valeur est utilisée lors de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

la création de nouvelles VM et durant les mises à jour d'images si EnableDynamicResizeOfAppContainer est défini sur 0.

La modification de PercentOfPvDForApps fait la différence uniquement lorsque le paramètre EnableDynamicResizeOfAppContainer est défini sur 0. Par défaut, le paramètre EnableDynamicResizeOfAppContainer est défini sur 1 (activé), ce qui signifie que AppContainer (que vous voyez en tant que lecteur C) est développé uniquement lorsqu'il est presque plein (c'est-à-dire, dynamique) lorsque moins de 10% d'espace libre est restant.

L'augmentation de PercentOfPvDForApps augmente uniquement l'espace maximum pour lequel la partie Apps est autorisée à augmenter. Cet espace n'est pas provisionné pour vous immédiatement. Vous devez également configurer l'allocation fractionnée dans l'image principale, où elle sera appliquée lors de la prochaine mise à jour d'image.

Si vous avez déjà généré un catalogue de machines avec EnableDynamicResizeOfAppContainer défini sur 1, changez alors ce paramètre sur 0 dans l'image principale pour la mise à jour suivante, puis configurez une division d'allocation appropriée. La taille de division requise sera honorée tant qu'elle est plus importante que la taille allouée actuelle pour le lecteur C.

Si vous souhaitez conserver un contrôle total sur la division de l'espace, cette valeur devrait être définie sur 0. Ceci permet un contrôle total sur la taille du lecteur C, et ne compte pas sur la consommation de l'espace disque par l'utilisateur en dessous du seuil pour augmenter le lecteur.

Valeur par défaut = 50% (alloue une quantité d'espace égale pour les deux parties)

- **PvDReservedSpaceMB**
  Définit la taille de l'espace réservé (en méga-octets) sur le vDisk pour le stockage de journaux Personal vDisk et d'autres données.

  Si votre déploiement comprend XenApp 6.5 (ou une version antérieure) et utilise la fonctionnalité de streaming d'application, augmentant cette valeur par la taille du cache Rade.

  Valeur par défaut = 512

- **PvDResetUserGroup**
  Valide uniquement pour XenDesktop 5.6 : autorise le groupe d'utilisateurs spécifié à réinitialiser un Personal vDisk. Les versions ultérieures de XenDesktop utilisent l'administration déléguée pour cette opération.

Autres paramètres :

- **Service Windows Update** : assurez-vous que les mises à jour Windows sont définies sur Ne jamais rechercher des mises à jour et que le service Windows Update est désactivé dans l'image principale. Dans l'éventualité où le service Windows Update doit être exécuté sur le PvD, la définition de celui-ci sur Ne jamais rechercher des mises à jour vous aider à empêcher l'installation des mises à jour sur les machines associées.
  Windows 8 Store a besoin de ce service en cours d'exécution pour installer toute application moderne.
- **Mises à jour Windows** : elles comprennent les mises à jour d'Internet Explorer et doivent être appliquées à l'image principale.
- **Mises à jour nécessitant un redémarrage** : les mises à jour Windows appliquées à l'image principale peuvent nécessiter plusieurs redémarrages pour être entièrement installées ; cela dépend du type de correctifs délivrés dans ces mises à jour. Veillez à redémarrer correctement l'image principale afin de terminer l'installation des mises à jour Windows appliquées à cette dernière avant de dresser l'inventaire PvD.
- **Mises à jour applicatives** : mettez à jour les applications installées sur l'image principale pour économiser l'espace sur les vDisk des utilisateurs. Cela permet aussi d'éviter d'avoir à mettre à jour les applications sur chaque vDisk de l'utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Certains logiciels peuvent entrer en conflit avec la façon dont le PvD établit l'environnement de l'utilisateur, vous devez l'installer sur l'image principale (plutôt que sur la machine utilisateur) pour éviter ces conflits. En outre, bien que certains d'autres logiciels puissent ne pas entrer en conflit avec le bon fonctionnement du PvD, Citrix vous recommande d'installer le logiciel sur l'image principale.

Applications qui doivent être installées sur l'image principale :
- Agents et clients (par exemple, l'agent System Center Configuration Manager, le client App-V, Citrix Receiver)
- applications qui installent ou modifient des pilotes de démarrage précoce ;
- applications qui installent des logiciels d'impression ou de scanner ou des pilotes ;
- applications qui modifient la pile réseau Windows ;
- outils de VM tels que VMware Tools et XenServer Tools.

Applications qui devraient être installées sur l'image principale :
- Applications qui sont distribuées à un grand nombre d'utilisateurs. Dans les deux cas, désactivez la mise à jour des applications avant le déploiement :
  - Applications d'entreprise qui utilisent des licences en volume, par exemple Microsoft Office, Microsoft SQL Server
  - Applications communes, par exemple Adobe Reader, Firefox et Chrome
- Applications volumineuses telles que SQL Server, Visual Studio et infrastructures applicatives telles que .NET

Les recommandations et restrictions suivantes s'appliquent aux applications installées par les utilisateurs sur les machines disposant de Personal vDisks. Certaines ne peuvent pas être appliquées si les utilisateurs disposent de privilèges administratifs :
- Les utilisateurs ne devraient pas désinstaller une application à partir de l'image principale et réinstaller la même application sur leur Personal vDisk.
- Soyez prudent lors de la mise à jour ou de la désinstallation d'applications sur l'image principale. Après avoir installé la version d'une application sur l'image, un utilisateur peut installer un module d'extension (un plug-in par exemple) qui requiert cette version. Si une telle dépendance existe, la mise à jour ou la désinstallation de l'application sur l'image pourrait entraîner un dysfonctionnement de ce module complémentaire. Par exemple, avec Microsoft Office 2010 installé sur une image principale, un utilisateur installe Visio 2010 sur son Personal vDisk. Une mise à niveau ultérieure d'Office sur l'image principale peut rendre le logiciel Visio installé localement inutilisable.
- Les logiciels dotés de licences liées au matériel (via un dongle ou matériel basé sur signature) ne sont pas pris en charge.

Lors de l'utilisation de Provisioning Services avec PvD :
- Le compte Soap Service doit être ajouté au nœud Administrateur de Studio et doit disposer du rôle d'administrateur de la machine ou d'un rôle supérieur. Cela garantit que les bureaux PvD sont placés en mode de préparation lorsque le vDisk Provisioning Services (PVS) passe en mode de production.
- La fonctionnalité de gestion des versions de Provisioning Services doit être utilisée pour mettre à jour Personal vDisk. Lorsque la version est promue au rôle de production, le Soap Service place les bureaux PvD en mode de préparation.
- La taille du Personal vDisk doit toujours être supérieure au disque de cache en écriture de Provisioning Services (dans le cas contraire, Provisioning Services peut, par erreur, sélectionner Personal vDisk pour utilisation en tant que cache en écriture).
- Une fois que vous avez créé un groupe de mise à disposition, vous pouvez contrôler le Personal vDisk à l'aide de l'outil PvD Image Update Monitoring Tool ou des Scripts resize et poolstats (personal-vdisk-poolstats.ps1).

Taille du disque de cache en écriture créée correctement. En mode de fonctionnement normal, PvD capture la plupart des écritures des utilisateurs (modifications) et les redirige vers le Personal vDisk. Cela implique que vous pouvez réduire la taille du disque de cache en écriture Provisioning Services. Toutefois, lorsque PvD n'est pas actif (comme lors des opérations de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

mise à jour de l'image), un disque de cache en écriture Provisioning Services de petite taille peut se remplir rapidement, ce qui entraîne des blocages de la machine.

Citrix vous recommande de créer la taille des disques de cache en écriture Provisioning Services, conformément aux meilleures pratiques de Provisioning Services et ajouter une quantité d'espace égale à deux fois la taille du modèle VHD sur l'image principale (afin de répondre aux exigences de fusion). Il est très improbable qu'une opération de fusion utilise tout cet espace, mais cela est possible.

Lors de l'utilisation de Provisioning Services pour déployer un catalogue de machines PvD :

- Suivez les instructions de la documentation Provisioning Services.
- Vous pouvez modifier les paramètres de limitation de l'action d'alimentation en modifiant la connexion dans Studio, voir ci-dessous.
- Si vous mettez à jour le vDisk Provisioning Services, après l'installation ou la mise à jour des applications et d'autres logiciels et le redémarrage du vDisk, exécutez l'inventaire PvD, puis arrêtez la VM. Ensuite, effectuez la promotion de la nouvelle version en Production. Les bureaux PvD dans le catalogue devraient automatiquement entrer en mode de préparation. Si ce n'est pas le cas, vérifiez que le compte Soap Service possède des privilèges d'administrateur de machines ou plus élevés sur le Controller.

La fonctionnalité du mode de test de Provisioning Services vous permet de créer un catalogue de machines de test à l'aide d'une image principale mise à jour. Si des tests confirment la viabilité du catalogue de test, vous pouvez le promouvoir en production.

Lors de l'utilisation de Machine Creation Services (MCS) pour déployer un catalogue de machines PvD :

- Suivez les instructions de la documentation XenDesktop.
- Exécutez un inventaire PvD après la création de l'image principale et arrêter la VM (PvD ne fonctionnera pas correctement si vous n'éteignez pas la VM). Prenez ensuite un instantané de l'image principale.
- Dans l'assistant Créer un catalogue de machines, spécifiez la taille du Personal vDisk et la lettre de lecteur.
- Une fois que vous avez créé un groupe de mise à disposition, vous pouvez contrôler le Personal vDisk à l'aide de l'outil PvD Image Update Monitoring Tool ou des Scripts resize et poolstats (personal-vdisk-poolstats.ps1).
- Vous pouvez modifier les paramètres de limitation de l'action d'alimentation en modifiant la connexion dans Studio, voir ci-dessous.
- Si vous mettez à jour l'image principale, exécutez l'inventaire PvD après la mise à jour des applications et d'autres logiciels sur l'image, puis arrêter la VM. Prenez ensuite un instantané de l'image principale.
- Utilisez l'outil de contrôle de mise à jour de l'image PvD (PvD Image Update Monitoring Tool) ou le script personal-vdisk-poolstats.ps1 afin de valider qu'il y a suffisamment d'espace sur chaque VM PvD qui utilisera l'image principale mise à jour.
- Lorsque vous mettez à jour le catalogue de machines, les bureaux PvD entrent en mode de préparation lorsqu'ils traitent individuellement les modifications apportées à la nouvelle image principale. Les bureaux sont mis à jour en fonction de la stratégie de déploiement spécifiée lors de la mise à jour de machine.
- Utilisez l'outil de contrôle de mise à jour de l'image PvD ou le script personal-vdisk-poolstats.ps1 afin de contrôler le PvD en mode de préparation.

Utilisez les fichiers de règles pour exclure des fichiers et dossiers des vDisks. Vous pouvez les utiliser lorsque les Personal vDisks sont en déploiement. Les fichiers de règles sont appelés custom_*_rules.template.txt et sont situés dans le dossier \config. Les commentaires dans chaque fichier fournissent une documentation supplémentaire.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Lorsque vous activez le PvD et après toute mise à jour de l'image principale après l'installation, il est important d'actualiser l'inventaire du disque (appelé « exécuter l'inventaire ») et de créer une nouvelle capture instantanée.

Étant donné que ce sont les administrateurs qui gèrent les images principales et non les utilisateurs, si vous installez une application qui place des fichiers binaires dans le profil utilisateur de l'administrateur, les utilisateurs de bureaux virtuels partagés ne peuvent pas accéder à l'application (y compris les bureaux basés sur des catalogues de machines regroupés et regroupés avec des catalogues de machines PvD). Les utilisateurs doivent installer eux-mêmes de telles applications.

Il est recommandé de prendre un instantané de l'image après chaque étape de cette procédure.

1. Mettez à jour l'image principale en installant des applications ou des mises à jour du système d'exploitation et en procédant à la configuration du système sur la machine.
   Pour ce qui est des images principales basées sur Windows XP que vous prévoyez de déployer avec des disques virtuels personnels, vérifiez qu'aucune boîte de dialogue n'est ouverte (par exemple, des messages confirmant l'installation de logiciels ou vous invitant à utiliser des pilotes non signés). L'ouverture de boîtes de dialogue sur les images principales dans cet environnement empêche le VDA de s'enregistrer auprès de Delivery Controller. Vous pouvez désactiver les invites de pilotes non signés à l'aide du Panneau de configuration. Par exemple, accédez à Système > Matériel > Signature des pilotes et sélectionnez l'option permettant d'ignorer les avertissements.
2. Arrêtez la machine. Sur les machines Windows 7, cliquez sur Annuler lorsque Citrix Personal vDisk bloque la fermeture.
3. Dans la boîte de dialogue Citrix Personal vDisk, cliquez sur Mettre l'inventaire à jour. Cette opération peut prendre plusieurs minutes.
   Important : si vous interrompez la fermeture (ne serait-ce que pour apporter une mise à jour mineure à l'image), l'inventaire de Personal vDisk ne correspond plus à l'image principale. Cela provoque l'arrêt de la fonctionnalité Personal vDisk. Si vous interrompez la fermeture, vous devez redémarrer la machine, l'arrêter, et lorsque vous y êtes invité, cliquer de nouveau sur Mettre l'inventaire à jour.
4. Lorsque l'opération d'inventaire arrête la machine, prenez un instantané de l'image principale.

Vous pouvez exporter un inventaire vers un partage réseau, puis importer cet inventaire vers une image principale. Pour de plus amples informations, consultez la section Exporter et importer un inventaire PvD.

Citrix Broker Service contrôle l'état de l'alimentation des machines qui fournissent des bureaux et des applications. Le Broker Service peut contrôler plusieurs hyperviseurs via un Delivery Controller. La négociation des actions d'alimentation contrôlent l'interaction entre un Controller et l'hyperviseur. Pour éviter de surcharger l'hyperviseur, les actions de modification de l'état de l'alimentation d'une machine se voient attribuer une priorité et sont envoyées à l'hyperviseur à l'aide d'un mécanisme de limitation. Les paramètres suivants affectent la limitation. Vous pouvez spécifier ces valeurs en modifiant une connexion (onglet Avancé) dans Studio.

Pour configurer les valeurs de limitation de la connexion :

1. Sélectionnez Configuration > Hébergement dans le volet de navigation de Studio.
2. Sélectionnez la connexion, puis sélectionnez Modifier la connexion dans le volet Actions.
3. Vous pouvez modifier les valeurs suivantes :
   - **Actions simultanées (tous types)** : nombre maximal d'actions d'alimentation en cours simultanées autorisées. Ce paramètre est spécifié en tant que valeur absolue et en tant que pourcentage de la connexion à l'hyperviseur. La plus faible de ces deux valeurs est utilisée.
     Valeur par défaut = 100 absolue, 20%

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Mises à jour de l'inventaire de Personal vDisk simultanées** : nombre maximal d'actions d'alimentation Personal vDisk simultanées autorisées. Ce paramètre est spécifié en tant que valeur absolue et en tant que pourcentage de la connexion. La plus faible de ces deux valeurs est utilisée.
  Valeur par défaut = 50 absolue, 25%

  Pour calculer la valeur absolue : déterminez les valeurs totales IOPS (TIOPS) prises en charge par le stockage de l'utilisateur final (ceci doit être spécifié par le fabricant ou calculé). L'utilisation de 350 IOPS par machine virtuelle (IOPS/VM), détermine le nombre de machines virtuelles qui devraient être actives à tout moment donné sur le stockage. Calculez cette valeur en divisant le total des IOPS par IOPS/VM.

  Par exemple, si le stockage utilisateur est 14000 IPS, le nombre de VM actives est 14000 IOPS/350 IOPS/VM=40.

- **Nouvelles actions maximales par minute** : le nombre maximal de nouvelles actions d'alimentation qui peuvent être envoyées à l'hyperviseur par minute. Spécifié en tant que valeur absolue.
  Valeur par défaut = 10

Pour vous aider à identifier les valeurs optimales pour les paramètres suivants dans votre déploiement :

1. À l'aide des valeurs par défaut, mesurez le temps de réponse total pour une mise à jour d'image d'un catalogue de test. Il s'agit de la différence entre le début de la mise à jour d'une image (T1) et le moment où le VDA de la dernière machine du catalogue s'enregistre auprès du Controller (T2). Temps de réponse total = T2 - T1.
2. Mesurez les opérations E/S par seconde (IOPS) du stockage de l'hyperviseur lors de la mise à jour d'image. Ces données peuvent servir de référentiel pour l'optimisation. (Les valeurs par défaut peuvent être le meilleur paramètre ; il se peut également que le système comporte trop d'IOPS, ce qui nécessite de diminuer les valeurs des paramètres).
3. Modifiez la valeur « Opérations de mises à jour de l'inventaire de Personal vDisk » comme décrit ci-dessous (conserver tous les autres paramètres inchangés).
   1. Augmentez la valeur de 10 et mesurez le temps de réponse total après chaque modification. Continuez à augmenter la valeur de 10 et testez le résultat, jusqu'à détérioration ou aucun changement du temps de réponse total.
   2. Si l'étape précédente n'a entraîné aucune amélioration en augmentant la valeur, réduisez la valeur par incréments de 10 et mesurez le temps de réponse total après chaque diminution. Répétez ce processus jusqu'à ce que le temps de réponse total reste inchangé ou ne s'améliore pas davantage. Il est probable que cela soit la valeur de l'action d'alimentation PvD optimale.
4. Après l'obtention de la valeur du paramètre de l'action d'alimentation PvD, modifiez les actions simultanées (tous types) et les valeurs des nouvelles actions maximales par minute, une à la fois. Suivez la procédure décrite ci-dessus (en augmentant ou diminuant par incréments) pour tester des valeurs différentes.

System Center Configuration Manager (Configuration Manager) 2012 ne requiert aucune configuration spéciale et peut être installé de la même façon que toute autre image principale de l'application. Les informations suivantes s'appliquent uniquement à System Center Configuration Manager 2007. Les versions de Configuration Manager antérieures à Configuration Manager 2007 ne sont pas prises en charge.

Effectuez les opérations suivantes pour utiliser le logiciel agent de Configuration Manager 2007 dans un environnement PvD.

1. Installez l'agent du client sur l'image principale.
   1. Installez le client Configuration Manager sur l'image principale.
   2. Arrêtez le service ccmexec (Agent SMS) et désactivez-le.
   3. Supprimez les certificats SMS ou les certificats clients du magasin de certificats de l'ordinateur local comme suit :
      - Mode mixte : Certificats (ordinateur local)\SMS\Certificats

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Mode natif
  - Certificats (ordinateur local)\Personal\Certificates
  - Supprimez le certificat client émis par votre autorité de certification (généralement une infrastructure interne à clé publique)

4. Supprimez ou renommez C:\Windows\smscfg.ini.

2. Supprimez les informations qui identifient de façon unique le client.
   1. (Facultatif) Supprimez ou déplacez les fichiers journaux de C:\Windows\System32\CCM\Logs.
   2. Installez Virtual Delivery Agent (s'il n'est pas déjà installé) et exécutez l'inventaire PvD.
   3. Arrêtez l'image principale, prenez un instantané et créez un catalogue de VM à l'aide de cet instantané.
3. Validez Personal vDisk et démarrez les services. Effectuez ces étapes une seule fois, sur chaque bureau PvD, après qu'ils aient été démarrés pour la première fois. Pour ce faire, vous pouvez utiliser un objet de stratégie de groupe du domaine, par exemple.
   - Confirmez que PvD est actif en vérifiant la présence de la clé de registre HKLM\Software\Citrix\personal vDisk\config\virtual.
   - Définissez le service ccmexec (Agent SMS) sur Automatique et démarrez le service. Le client de Configuration Manager contacte le serveur Configuration Manager et récupère les nouveaux certificats et GUID uniques.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Outils

Jul 07, 2016

Vous pouvez utiliser les outils et utilitaires suivants pour configurer, personnaliser et surveiller les opérations de PvD.

Les fichiers de règles personnalisés fournis avec PvD vous permettent de modifier le comportement par défaut des mises à jour de l'image PvD des manières suivantes :

- Visibilité des fichiers sur PvD
- Comment les modifications apportées aux fichiers sont fusionnées
- Fichiers accessibles en écriture

Pour obtenir des instructions détaillées sur les fichiers de règles personnalisés et la fonctionnalité CoW, reportez-vous aux commentaires figurant dans les fichiers qui se trouvent dans C:\ProgramData\Citrix\personal vDisk\Config sur la machine sur laquelle PvD est installé. Les fichiers appelés « custom_* » décrivent les règles et comment les activer.

Deux scripts sont fournis pour surveiller et gérer la taille des PvD ; ils se trouvent dans le dossier Support\Tools\Scripts sur le support d'installation XenDesktop. Vous pouvez également utiliser l'outil de contrôle de mise à jour de l'image PvD, qui se trouve dans le dossier Support\Tools\Scripts\PvdTool, consultez la section http://blogs.citrix.com/2014/06/02/introducing-the-pvd-image-update-monitoring-tool/ pour plus de détails.

Utilisez resize-personalvdisk-pool.ps1 pour augmenter la taille des PvD dans tous les bureaux d'un catalogue. Les composants logiciels enfichables ou modules suivants pour votre hyperviseur doivent être installés sur la machine exécutant Studio :

- XenServer requiert XenServerPSSnapin
- vCenter requiert vSphere PowerCli
- System Center Virtual Machine Manager requiert la console VMM

Utilisez personal-vdisk-poolstats.ps1 pour vérifier l'état des mises à jour de l'image et pour vérifier l'espace réservé aux applications et aux profils utilisateur dans un groupe de PvD. Exécutez ce script avant de mettre à jour une image pour détecter si des bureaux sont à court d'espace, ce qui évite les défaillances durant la mise à jour. Ce script requiert l'activation du pare-feu Windows Management Instrumentation (WMI-In) sur les bureaux PvD. Vous pouvez l'activer sur l'image principale ou via un objet de stratégie de groupe.

Si la mise à jour d'une image échoue, l'entrée dans la colonne Update indique la raison.

Si un bureau devient endommagé ou altéré (en installant une application défectueuse ou autre), vous pouvez restaurer la zone applicative du PvD à un état par défaut (vide). La réinitialisation laisse les données du profil utilisateur intactes.

Pour réinitialiser la zone applicative du PvD, utilisez l'une des méthodes suivantes :

- Ouvrez une session sur le bureau de l'utilisateur en tant qu'administrateur. Lancez une invite de commandes et exécutez la commande C:\Program Files\Citrix\Personal vDisk\bin\CtxPvD.exe -s Reset.
- Accédez au bureau de l'utilisateur dans Citrix Director. Cliquez sur Réinitialiser Personal vDisk puis cliquez sur OK.

Le processus de mise à jour de l'image fait partie intégrante de la distribution de nouvelles images vers des bureaux PvD ; il comprend l'ajustement du Personal vDisk existant pour fonctionner avec la nouvelle image de base. Pour les déploiements qui utilisent Machine Creation Services (MCS), vous pouvez exporter un inventaire à partir d'une VM active sur un partage réseau, puis l'importer dans une image principale. Un différentiel est calculé à l'aide de cet inventaire dans l'image principale. Bien que l'utilisation de la fonctionnalité d'exportation/importation de l'inventaire ne soit pas obligatoire, elle peut améliorer les performances du processus général de mise à jour de l'image.

Pour utiliser la fonctionnalité d'exportation/importation de l'inventaire, vous devez être un administrateur. Si nécessaire, authentifiez-vous sur le partage de fichier utilisé pour l'importation/exportation avec « net use ». Le contexte utilisateur doit être en mesure d'accéder aux partages de fichiers utilisés pour l'importation/exportation.

- Pour exporter un inventaire, exécutez la commande d'exportation en tant qu'administrateur sur une machine qui contient un VDA avec PvD activé (version minimum 7.6) :
  Ctxpvdsvc.exe exportinventory “<chemin-vers-emplacement-exportation>”

  Le logiciel détecte l'emplacement de l'inventaire actuel et exporte l'inventaire vers un dossier nommé « ExportedPvdInventory » à l'emplacement spécifié. Voici un extrait de la sortie de la commande :
  C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe exportinventory \\share location\ExportedInventory Current inventory source location C:\CitrixPvD\Settings\Inventory\VER-LAS ... Exportin
- Pour importer un inventaire exporté précédemment, exécutez la commande d'importation en tant qu'administrateur sur l'image principale :

Pour importer

Exécuter la commande d'importation en tant qu'administrateur sur l'image principale.

Ctxpvdsvc.exe importinventory “<chemin-vers-inventaire-exporté>”

Le <chemin d'accès de l'inventaire exporté> doit être le chemin d'accès complet à l'inventaire des fichiers, qui est généralement <emplacement réseau\ExportedPvdInventory>.

L'inventaire est obtenu à partir de l'emplacement d'importation (où il a été préalablement exporté à l'aide de l'option exportinventory), puis importe l'inventaire vers le magasin d'inventaire sur l'image principale. Voici une l'extrait de la sortie de la commande :
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe importinventory \\share location\ExportedInventory\ExportedPvdInventory Importing inventory \\share location\ExportedInventory\ExportedPv
Une fois l'exportation terminée, le partage réseau devrait inclure les noms de fichiers suivants. Après l'importation, l'inventaire magasin sur l'image principale doit inclure les mêmes noms de fichier.

- Components.DAT
- règles_fichiers
- règles_dossiers
- règles_clé_registre
- RINGTHREE.DAT
- S-1-5-18.DAT
- SAM.DAT
- SECURITY.DAT
- SNAPSHOT.DAT

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- SOFTWARE.DAT
- SYSTEM.CurrentControlSet.DAT
- VDCATALOG.DAT
- vDiskJournalData

Important : les scripts ne déplacent pas les PvD vers le nouvel emplacement de stockage. Vous devez réaliser cette opération d'une autre façon.
Deux des scripts PowerShell fournis sur le support d'installation du produit (dans le dossier Support\Tools\Scripts) vous permettent de sauvegarder et restaurer des Personal vDisks. Utilisez les scripts de sauvegarde et de restauration pour migrer les PvD existants et les associations utilisateur d'un catalogue vers un autre. Cela peut être utile si vous modifiez votre stockage PvD. Le script de sauvegarde crée un fichier.xml avec les métadonnées d'un catalogue existant. Les métadonnées contiennent l'emplacement actuel des PvD sur le stockage, et les associations utilisateur avec les PvD. Le script de restauration utilise le fichier .xml pour associer les PvD à un nouveau catalogue et leur attribuer les utilisateurs appropriés.
- migration-backup.ps1 capture le mappage entre chaque utilisateur et leur Personal vDisk dans un catalogue de machines et stocke celles-ci dans un fichier .xml.
- migration-restore.ps1 utilise le fichier .xml pour recréer un bureau utilisateur dans un catalogue de machines.

Avant la sauvegarde et la restauration, notez les points suivants :
- Les scripts fonctionnent avec l'API de l'hyperviseur afin que le composant logiciel enfichable PowerShell de l'hyperviseur soit installé sur le Controller où les scripts sont exécutés.
- Exécutez les scripts à partir d'un emplacement qui a accès au Controller où le catalogue de machine a été créé.
- Les scripts sont pris en charge sur les plates-formes d'hyperviseur suivants : Citrix XenServer, Microsoft Hyper-V et VMware ESX

Sauvegarder un catalogue de machines

Effectuez une sauvegarde quand une modification est effectuée sur un catalogue de machines. Vous pouvez effectuer une sauvegarde lorsque les machines du catalogue sont actives.

Utilisez migration-backup.ps1 pour sauvegarder un catalogue de machines contenant des Personal vDisks. Le script requiert le nom du catalogue de machine et les informations de connexion de l'hyperviseur. Il itère ensuite au sein de toutes les machines affectées aux utilisateurs dans le catalogue de machine et, pour chaque machine, stocke le mappage entre le stockage Personal vDisk et l'utilisateur affecté. Ces informations se trouvent dans un fichier .xml, qui possède la structure suivante :

- PvDMigration.hypervisor.Type prend en charge VMware ESX, Citrix XenServer et Microsoft Hyper-V.
- PvDMigration.PVD stocke des informations à l'emplacement où le Personal vDisk est stocké et l'utilisateur est associé.
- PvDMigration.PVD.DiskId est l'identificateur unique du vDisk sur l'hyperviseur sur lequel la sauvegarde a été effectuée.
- PvDMigration.PVD.DiskName est le nom du fichier .vhd ou .vmdk.
- PvDMigration.PVD.SRName est le nom du fournisseur de stockage sur lequel la sauvegarde a été effectuée.
- PvDMigration.PVD.SRID est l'identificateur unique du fournisseur de stockage sur l'hyperviseur sur lequel la sauvegarde a été effectuée.
- PvDMigration.PVD.UserName est le nom de l'utilisateur associé à ce vDisk.
- PvDMigration.PVD.UserSid est le SID de l'utilisateur associé à ce vDisk.
- PvDMigration.PVD.State indique l'état de ce vDisk. Ceci peut être « sauvegardé » ou « traité ». Elle est « sauvegardée » après la sauvegarde initiale ; l'état change en « traité » après utilisation du fichier .xml pour la restauration de la sauvegarde.

Restaurer un catalogue de machines

Avant la restauration, notez les points suivants :
- Vous ne pouvez pas restaurer un catalogue de machines partageant la même image principale en tant que catalogue de machines sauvegardé.
- Vous devez créer une nouvelle image principale par la mise à jour de l'inventaire de l'image principale depuis laquelle le catalogue de machines sauvegardé a été créé.

Utilisez migration-restore.ps1 pour restaurer tout catalogue de machines contenant des Personal vDisks. Le script effectue les entrées suivantes :
- Le fichier .xml créé pendant le processus de sauvegarde.
- Le nom du catalogue de machines à restaurer.
- Le nom de l'emplacement où les Personal vDisks non connectés sont stockés. Ceci est répertorié dans le fichier .xml.
- Informations de connexion de l'hyperviseur

Le script migration-restore.ps1 recherche toute machine non affectée dans le catalogue de machines et lui affecte des utilisateurs. Il connecte également les Personal vDisks des utilisateurs vers les machines.

Exemple de scénario 1 : restaurer un catalogue de machines et ses Personal vDisks à l'aide de nouveaux noms de machines

Dans ce scénario, l'intégralité d'un catalogue de machines et les Personal vDisks connectés aux machines de celui-ci sont restaurés. Les machines se voient attribuer de nouveaux noms. Ce scénario peut se produire lorsque votre hyperviseur ou un hôte de stockage a échoué, ou lors de la migration des utilisateurs vers une nouvelle infrastructure.
1. Exécutez migration-backup.ps1 pour capturer le mappage utilisateur sur Personal vDisk dans le fichier .xml.
2. À l'aide d'une solution de sauvegarde, déplacez ou capturez les Personal vDisks depuis le catalogue de machines d'origine sur un disque :
   - VMware ESX ou Microsoft Hyper-V : les Personal vDisks sont situés sur le stockage spécifié par le Controller, dans un dossier contenant le nom de la machine à laquelle le vDisk est connecté.
   - Citrix XenServer : les Personal vDisks sont situés dans la racine de l'espace de stockage spécifié par le Controller. Le nom de chaque vDisk est un GUID.
3. Restaurez les Personal vDisks à partir du catalogue de machines d'origine à l'aide d'une solution de sauvegarde de stockage :
   - ESX ou Hyper-V : recherchez les vDisks dans un nouveau dossier de la nouvelle ressource de stockage. Sinon, laissez les vDisks dans le chemin d'accès d'origine de la nouvelle ressource de stockage.
   - XenServer : recherchez les vDisks dans la racine de la nouvelle ressource de stockage.
4. Créez un vDisk Provisioning Services ou un instantané Machine Creation Services depuis l'image principale que vous avez utilisée pour créer le catalogue de machines en échec.
5. Exécutez Mettre l'inventaire à jour depuis le menu Démarrer sur le vDisk ou l'instantané.
6. Recréez le catalogue de machines dans Studio à l'aide d'une autre convention d'appellation comme le catalogue de machines en échec (d'origine). Ceci génère un catalogue de nouvelles machines, chacun avec un nouveau Personal vDisk, que la base de données du site reconnaît.
7. Vérifiez que le catalogue de machines recréé est attribué au groupe de mise à disposition approprié.
8. Vérifiez que le groupe de mise à disposition est en mode de maintenance et que les machines qui s'y trouvent sont arrêtées.
9. Modifiez le fichier .xml généré par le script de sauvegarde :
   - ESX ou Hyper-V : si vous avez restauré les vDisks dans un nouveau dossier sur la nouvelle ressource de stockage à l'étape 3, pour chaque section PVD du fichier, remplacez le nom du dossier dans DiskName par l'emplacement des vDisks restaurés. Si vous avez restauré les vDisks à leur chemin d'origine sur le nouveau stockage, ignorez cette étape.
   - XenServer : évitez cette étape.
10. Sur le Controller, exécutez migration-restore.ps1, en spécifiant le nom du fichier .xml et l'emplacement dans lequel les vDisks sauvegardés sont stockés.

Exemple de scénario 2 : restaurez un catalogue de machines et ses Personal vDisks en réutilisant les noms de machines existantes

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dans ce scénario, l'intégralité d'un catalogue de machines et les Personal vDisks connectés aux machines de celui-ci sont restaurés. Les noms de machines (en échec) sont réutilisés. Ce scénario peut se produire lorsque votre hyperviseur ou un hôte de stockage a échoué.

1. Exécutez migration-backup.ps1 pour capturer le mappage user-to-Personal-vDisk.
2. À l'aide d'une solution de sauvegarde, déplacez ou capturez les Personal vDisks depuis le catalogue de machines d'origine sur un disque :
   - ESX ou Hyper-V : les Personal vDisks sont situés sur le stockage spécifié par le Controller, dans un dossier contenant le nom de la machine à laquelle le vDisk est connecté.
   - XenServer : les Personal vDisks sont situés dans la racine de l'espace de stockage spécifié par le Controller. Le nom de chaque vDisk est un GUID.
3. Restaurez les Personal vDisks à partir du catalogue de machines d'origine à l'aide d'une solution de sauvegarde de stockage :
   - ESX ou Hyper-V : recherchez les vDisks dans un nouveau dossier de la nouvelle ressource de stockage.
   - XenServer : recherchez les vDisks dans la racine de la nouvelle ressource de stockage.
4. Créez un vDisk Provisioning Services ou un instantané Machine Creation Services depuis l'image principale que vous avez utilisée pour créer le catalogue de machines en échec.
5. Exécutez Mettre l'inventaire à jour depuis le menu Démarrer sur le vDisk ou l'instantané.
6. Recréez le catalogue de machines dans Studio en utilisant la même convention d'appellation que le catalogue de machines en échec. Ceci génère un catalogue de nouvelles machines, chacun avec un nouveau Personal vDisk, que la base de données du site reconnaît.
7. Vérifiez que le catalogue de machines recréé est attribué au groupe de mise à disposition approprié.
8. Vérifiez que le groupe de bureaux est en mode de maintenance et que les machines qui s'y trouvent sont arrêtées.
9. Modifiez le fichier .xml généré par le script de sauvegarde :
   - ESX ou Hyper-V : pour chaque section PVD du fichier, remplacez le nom du dossier dans DiskName avec l'emplacement de la restauration des vDisks.
   - XenServer : évitez cette étape.
10. Exécutez le script migration-restore.ps1 sur le Controller avec le fichier .xml modifié en tant qu'entrée. Le script connecte les vDisks sans les déplacer.
11. Vérifiez que les données des utilisateurs ont été correctement restaurées.

Exemple de scénario 3 : restaurez un sous-ensemble de Personal vDisks dans un catalogue de machines

Dans ce scénario, certains des Personal vDisks d'un catalogue de machines ont échoué et sont restaurés. Les machines virtuelles dans le catalogue n'ont pas échoué.

1. Exécutez migration-backup.ps1 pour capturer le mappage utilisateur sur Personal vDisk dans le fichier .xml.
2. Le fichier .xml possède une section PVD pour chaque utilisateur dans le catalogue de machines. Pour les utilisateurs dont les Personal vDisks n'ont pas besoin de restauration, supprimez les utilisateurs et leurs sections associées du fichier.
3. Restaurez les Personal vDisks à partir du catalogue de machines d'origine à l'aide d'une solution de sauvegarde, comme décrit dans l'un des autres scénarios :
   - Pour utiliser de nouveaux noms de machine, suivez l'exemple de scénario 1.
   - Pour préserver les noms de machine, suivez l'exemple de scénario 2.
4. Assurez-vous de disposer de suffisamment de machines attribuées dans le catalogue. Ajoutez des machines si nécessaire. Vous avez besoin d'une nouvelle machine pour chaque utilisateur dont vous voulez restaurer le vDisk.
5. Vérifiez que le groupe de bureaux est en mode de maintenance et que les machines qui s'y trouvent sont arrêtées.
6. Sur le Controller, exécutez migration-restore.ps1 avec le fichier .xml modifié en tant qu'entrée.
7. Vérifiez que les données des utilisateurs ont été correctement restaurées.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Affichages, messages et résolution des problèmes

Jul 07, 2016

Dans Studio, lorsque vous choisissez une machine PvD dans un catalogue de machines, l'onglet « PvD »offre un statut de surveillance lors des mises à jour de l'image, ainsi que l'heure de fin et de progression estimée. Les affichages possibles de l'état lors de la mise à jour d'une image sont : Prêt, Préparation, En attente, En échec et Demandée.

Une mise à jour d'image peut échouer pour d'autres raisons par manque d'espace ou un bureau ne trouve pas le PvD suffisamment rapidement. Lorsque Studio indique qu'une mise à jour d'image a échoué, un code d'erreur est fourni avec un texte descriptif pour faciliter la résolution des problèmes. Utilisez l'outil de contrôle de mise à jour d'image Personal vDisk ou le script personal-vdisk-poolstats.ps1 afin de contrôler la progression de la mise à jour de l'image et obtenir les codes d'erreur associés à l'échec.

Si une mise à jour d'image échoue, les fichiers journaux suivants peuvent fournir davantage d'informations sur la résolution de ce problème :

- Journal du service PvD : C:\ProgramData\Citrix\personal vDisk\Logs\PvDSvc.log.txt
- Journal d'activation PvD : P:\PVDLOGS\PvDActivation.log.txt

Le contenu le plus récent se trouve à la fin du fichier journal.

Les erreurs suivantes sont valides pour la version 7.6 de PvD et version ultérieure :

- **Une erreur interne s'est produite. Vérifiez les journaux Personal vDisk pour plus de détails. Code d'erreur %d (%s)**
  Ceci est un passe-partout pour les erreurs n'appartenant à aucune catégorie, et il ne possède ainsi pas de valeur numérique. Toutes les erreurs inattendues se sont produites lors de la création de l'inventaire ou de la mise à jour de Personal vDisk sont indiquées par ce code d'erreur.
  - Collectez les journaux et contactez l'assistance Citrix.
  - Si cette erreur se produit lors de la mise à jour du catalogue, restaurez le catalogue vers la version précédente de l'image principale.
- **Il existe des erreurs de syntaxe dans les fichiers de règle. Consultez les journaux pour plus de détails.**
  Code d'erreur 2. Le fichier de règle contient des erreurs de syntaxe. Les fichiers journaux Personal vDisk contiennent le nom du fichier de règles et le numéro de ligne sur laquelle l'erreur de syntaxe a été détectée. Corrigez l'erreur de syntaxe dans le fichier de règle, puis recommencez l'opération.
- **L'inventaire stocké dans le Personal vDisk correspondant à la version précédente de l'image principale est endommagé ou illisible.**
  Code d'erreur 3. Le dernier inventaire est stocké dans « UserData.V2.vhd » dans « \ProgramData\CitrixPvD\Settings\Inventory\VER-LAST ». Restaurez l'inventaire correspondant à la dernière version de l'image principale en important le dossier « VER-LAST » à partir d'une machine PvD en cours d'exécution connue associée à la version précédente de l'image principale.
- **L'inventaire stocké dans le Personal vDisk correspondant à la version précédente de l'image principale est une version supérieure.**
  Code d'erreur 4. Ceci est dû à une incompatibilité de version de de Personal vDisk entre la dernière image principale et l'image principale courante. Réessayez d'effectuer la mise à jour du catalogue après l'installation de la dernière version de Personal vDisk dans l'image principale.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Un dépassement de capacité du journal des modifications de a été détecté.**
  Code d'erreur 5. Un dépassement de capacité du journal USN a été causé par un nombre important de modifications apportées à l'image principale lors de la création de l'inventaire. Si ce problème persiste après plusieurs tentatives, utilisez procmon pour déterminer si un logiciel tiers tente de créer ou de supprimer un grand nombre de fichiers pendant la création de l'inventaire.

- **Personal vDisk n'a pas pu détecter un disque connecté au système pour le stockage des données de l'utilisateur.**
  Code d'erreur 6. Vérifiez, tout d'abord, que le disque PvD est connecté à la VM au travers de la console de l'hyperviseur. Cette erreur se produit généralement à cause d'un logiciel de « prévention des fuites de données » empêchant l'accès au disque PvD. Si le disque PvD est connecté à la VM, essayez d'ajouter une exception pour « disque connecté » dans la configuration du logiciel de « prévention des fuites de données ».

- **Le système n'a pas été redémarré après l'installation. Effectuez le redémarrage pour appliquer les modifications.**
  Code d'erreur 7. Redémarrez le bureau et recommencez l'opération.

- **Installation altérée. Essayez de réinstaller Personal vDisk.**
  Code d'erreur 8. Installez Personal vDisk et réessayez.

- **L'inventaire Personal vDisk n'est pas à jour. Mettez à jour l'inventaire de l'image principale, puis réessayez.**
  Code d'erreur 9. L'inventaire Personal vDisk n'a pas été mis à jour dans l'image principale avant fermeture du bureau. Redémarrez l'image principale et arrêter le bureau au moyen de l'option « Mettre Personal vDisk à jour », puis créez un nouvel instantané ; utilisez cet instantané pour mettre le catalogue à jour.

- **Une erreur interne s'est produite lors du démarrage du Personal vDisk. Vérifiez les journaux Personal vDisk pour plus de détails.**
  Code d'erreur 10. Cela peut être causé par le pilote de PvD qui ne peut pas démarrer une session de virtualisation en raison d'une erreur interne ou d'une altération de Personal vDisk. Essayez de redémarrer le bureau via le Controller. Si le problème persiste, collectez les journaux et contactez l'assistance Citrix.

- **Le délai de Personal vDisk a expiré lors de la recherche d'un disque de stockage pour les paramètres de personnalisation des utilisateurs.**
  Code d'erreur 11. Cette erreur se produit lorsque le pilote PvD ne parvient pas à détecter le disque PvD dans les 30 secondes suivant le redémarrage. Ceci est généralement dû à un contrôleur SCSI non pris en charge ou une latence de stockage. Si ce problème se produit avec tous les bureaux du catalogue, modifiez le type de contrôleur SCSI associé à la « VM modèle »/« VM principale pour un type pris en charge par la technologie Personal vDisk. Si ce problème se produit uniquement avec certains bureaux du catalogue, il peut être dû à des pics de latence de stockage dus à un nombre important de bureaux démarrant en même temps. Essayez de limiter le paramètre des actions d'alimentation actives maximales associées à la connexion hôte.

- **Le Personal vDisk a été désactivé car un arrêt du système non sécurisé a été détecté. Redémarrez la machine.**
  Code d'erreur 12. Cela peut être dû au fait que le bureau n'est pas parvenu à terminer le processus de redémarrage avec PvD activé. Essayez de redémarrer le bureau. Si le problème persiste, observez le démarrage du bureau via la console de l'hyperviseur et vérifiez si le bureau est bloqué. Si un bureau se bloque lors du démarrage, restaurez le PvD à partir d'une sauvegarde (si vous en possédez une) ou réinitialisez le PvD.

- **La lettre de lecteur spécifiée pour le montage du Personal vDisk n'est pas disponible.**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Code d'erreur 13. Cela peut être dû au fait que le PvD n'est pas parvenu à monter le disque PvD lors du montage spécifié par l'administrateur. Le montage du disque PvD échouera si la lettre de lecteur est déjà utilisée par d'autres matériels. Sélectionnez une lettre différente comme point de montage pour le Personal vDisk.

- **Les pilotes en mode noyau de Personal vDisk n'ont pas réussi à s'installer.**
  Code d'erreur 14. Personal vDisk installe des pilotes lors de la première mise à jour de l'inventaire après l'installation. Certains produits anti-virus empêchent l'installation de ce pilote en dehors du contexte d'un programme d'installation. Désactivez temporairement l'analyse antivirus en temps réel ou ajoutez des exceptions dans l'antivirus pour les pilotes PvD lors de la première création d'inventaire.

- **Impossible de créer un instantané du volume système. Vérifiez que le service de cliché instantané des volumes est activé.**
  Code d'erreur 15. Cela peut se produire si le service de cliché instantané des volumes est désactivé. Activez le service de cliché instantané des volumes et réessayez d'effectuer un inventaire.

- **L'activation du journal des modifications a échoué. Réessayez après une attente de quelques minutes.**
  Code d'erreur 16. Personal vDisk utilise le journal des modifications pour le suivi des modifications apportées à l'image principale. Au cours de la mise à jour d'un inventaire, si le PvD détecte que le journal des modifications est désactivé, il tente de l'activer, cette erreur se produit lorsque cette tentative échoue. Patientez quelques minutes, puis réessayez.

- **Il n'y a pas suffisamment d'espace disponible sur le volume système.**
  Code d'erreur 17. Il n'y a pas suffisamment d'espace disponible sur le lecteur C du bureau pour l'opération de mise à jour de l'image. Développez le volume système ou supprimez des fichiers non utilisés pour libérer de l'espace dans le volume système. La mise à jour d'image doit commencer après le redémarrage suivant.

- **Il n'y a pas suffisamment d'espace disponible dans le stockage Personal vDisk. Développez le stockage Personal vDisk pour fournir plus d'espace.**
  Code d'erreur 18. Il n'y a pas suffisamment d'espace disponible sur le lecteur Personal vDisk lors de la réalisation d'une opération de mise à jour de l'image. Développez le stockage Personal vDisk ou supprimez des fichiers non utilisés pour libérer de l'espace dans le stockage Personal vDisk. La mise à jour d'image devrait redémarrer après le redémarrage suivant.

- **Le stockage Personal vDisk est trop engagé. Développez le stockage Personal vDisk pour fournir plus d'espace.**
  Code d'erreur 19. Il n'y a pas suffisamment d'espace disponible sur le lecteur Personal vDisk pour accueillir complètement un « UserData.V2.vhd » provisionné. Développez le stockage Personal vDisk ou supprimez des fichiers non utilisés pour libérer de l'espace dans le stockage Personal vDisk.

- **Registre système endommagé.**
  Code d'erreur 20. Le Registre système est altéré, endommagé, manquant ou illisible. Réinitialisez le Personal vDisk ou effectuez sa restauration à partir d'une sauvegarde antérieure.

- **Une erreur interne s'est produite lors de la réinitialisation de Personal vDisk. Vérifiez les journaux Personal vDisk pour plus de détails.**
  Code d'erreur 21. Ceci est un passe-partout pour toutes les erreurs rencontrées lors de la réinitialisation d'un Personal vDisk. Collectez les journaux et contactez l'assistance Citrix.

- **Échec de réinitialisation de Personal vDisk, car il n'y a pas suffisamment d'espace disponible dans le stockage Personal vDisk.**
  Code d'erreur 22. Il n'y a pas suffisamment d'espace disponible sur le lecteur Personal vDisk lors de la réalisation d'une opération de réinitialisation. Développez le stockage Personal vDisk ou supprimez des fichiers non utilisés pour libérer de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

l'espace dans le stockage Personal vDisk.

Les erreurs suivantes sont valides pour les versions PvD 7.x antérieures à 7.6 :

- **Échec de démarrage. Personal vDisk n'a pas pu détecter de disque de stockage pour les paramètres de personnalisation des utilisateurs.**
  Le logiciel PvD n'a pas réussi à trouver le Personal vDisk (par défaut le lecteur P:) ou n'a pas pu le monter en tant que point de montage sélectionné par l'administrateur lors de la création du catalogue.
  - Cherchez l'entrée suivante dans le journal du service PvD : « PvD 1 status --> 18:183 ».
  - Si vous utilisez une version de PvD antérieure à la version 5.6.12, la mise à niveau vers la dernière version résout ce problème.
  - Si vous utilisez la version 5.6.12 ou supérieure, utilisez l'outil de gestion du disque (diskmgmt.msc) pour déterminer si le lecteur P: est présent en tant que volume non monté. S'il est présent, exécutez chkdsk sur le volume pour déterminer s'il est endommagé, et essayez de le réparer à l'aide de chkdsk.
- **Échec de démarrage. Échec de démarrage de Citrix Personal vDisk. Pour obtenir de l'aide... Code d'état : 7, code d'erreur : 0x70**
  Le code d'état 7 implique qu'une erreur s'est produite lors de la tentative de mise à jour du PvD. Le code d'erreur peut être l'un des suivants :

Code d'erreur	Description
0x20000001	Impossible d'enregistrer le package de différentiel, probablement à cause d'un espace insuffisant dans le VHD.
0x20000004	Impossible d'obtenir les privilèges requis pour la mise à jour du PvD.
0x20000006	Impossible de charger la ruche depuis l'image PvD où l'inventaire PvD, probablement en raison d'une image ou d'un inventaire PvD endommagé.
0x20000007	Impossible de charger l'inventaire du système de fichiers, probablement en raison d'une image ou d'un inventaire PvD altéré.
0x20000009	Impossible d'ouvrir le fichier contenant l'inventaire du système de fichiers, probablement en raison d'une image ou d'un inventaire PvD altéré.
0x2000000B	Impossible d'enregistrer le package de différentiel, probablement à cause d'un espace insuffisant dans le VHD.
0x20000010	Impossible de charger le package de différentiel.
0x20000011	Fichiers de règles manquants.
0x20000021	Inventaire PvD endommagé.
0x20000027	Le catalogue « MojoControl.dat » est altéré.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Code d'erreur	Description
0x2000002B	Inventaire PvD endommagé ou manquant.
0x2000002F	Impossible d'enregistrer le fichier MOF installé par l'utilisateur sur la mise à jour de l'image, mettez à niveau vers 5.6.12 pour résoudre le problème.
0x20000032	Consultez le fichier PvDactivation.log.txt pour rechercher la dernière entrée de journal avec un code d'erreur Win32.
0x20	Impossible de monter le conteneur d'application pour une mise à jour d'image, mettez à niveau vers 5.6.12 pour résoudre le problème.
0x70	Espace insuffisant sur le disque.

- **Échec de démarrage. Citrix Personal vDisk n'est pas parvenu à démarrer [ou Personal vDisk a rencontré une erreur interne]. Pour obtenir de l'aide... Code d'état : 20, code d'erreur : 0x20000028**
  Les Personal vDisk ont été détecté mais aucune session PvD n'a pu être créée.

  Collectez les journaux et vérifiez SysVol-IvmSupervisor.log pour des échecs de création de session :
  1. Recherchez l'entrée suivante dans le journal : « IvmpNativeSessionCreate: failed to create native session, status XXXXX ».
  2. Si l'état est 0xc00002cf, vous pouvez résoudre le problème en ajoutant une nouvelle version de l'image principale au catalogue. Le code d'état implique une saturation du journal USN en raison d'un grand nombre de changements apportés après la mise à jour d'un inventaire.
  3. Redémarrez le bureau virtuel affecté. Si le problème persiste, contactez le support technique Citrix.
- **Échec de démarrage. Citrix Personal vDisk a été désactivé car un arrêt du système non sécurisé a été détecté. Pour réessayer, sélectionnez Réessayez. Si le problème persiste, contactez votre administrateur système.**
  La VM groupée ne peut pas terminer son démarrage avec le PvD activé. Déterminez tout d'abord la raison pour laquelle le démarrage ne peut pas être effectué. Les raisons possibles peuvent être l'apparition d'un écran bleu car :
  - Un produit anti-virus incompatible est présent sur l'image principale, par exemple des versions anciennes de Trend Micro.
  - L'utilisateur a installé un logiciel incompatible avec PvD. Cela est fort peu probable, mais vous pouvez le vérifier en ajoutant une nouvelle machine au catalogue et voir si elle redémarre correctement.
  - L'image PvD est endommagée. Cela a été rencontré dans la version 5.6.5.

  Pour vérifier que la VM affiche un écran bleu ou qu'elle redémarre prématurément :
  - Ouvrez une session sur la machine via la console de l'hyperviseur.
  - Cliquez sur Try Again et attendez que la machine s'arrête.
  - Démarrez la machine via Studio.
  - Utilisez la console de l'hyperviseur pour observer la console de machine lorsqu'elle démarre.

  Autres résolutions de problèmes :
  - Collectez l'image mémoire de la machine affichant l'écran bleu et envoyez-la à l'assistance technique de Citrix pour une analyse plus approfondie.
  - Vérifiez les erreurs dans les journaux d'événements associés au PvD :
    1. Montez UserData.V2.vhd à partir de la racine du lecteur P: à l'aide de DiskMgmt.msc en cliquant sur Action > Attach VHD.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Lancez Eventvwr.msc.
3. Ouvrez le journal d'événements système (Windows\System32\winevt\logs\system.evtx) depuis UserData.V2.vhd en cliquant sur Action > Open saved logs.
4. Ouvrez le journal d'événements d'applications (Windows\System32\winevt\logs\application.evtx) depuis UserData.V2.vhd en cliquant sur Action > Open saved logs.

- **Le Personal vDisk ne peut pas démarrer. Le Personal vDisk n'a pas pu démarrer car l'inventaire n'a pas été mis à jour. Mettez l'inventaire à jour dans l'image principale, puis réessayez. Code d'état : 15, code d'erreur : 0x0**
  L'administrateur a sélectionné un instantané incorrect lors de la création ou de la mise à jour du catalogue PvD (en d'autres termes, l'image principale n'a pas été arrêtée à l'aide de l'option Update Personal vDisk lors de la création de l'instantané).

Si Personal vDisk n'est pas activé, vous pouvez afficher les événements suivants dans l'Observateur d'événements de Windows. Sélectionnez le nœud Applications dans le panneau de gauche ; la Source des événements dans le panneau de droite est Citrix Personal vDisk. Si Personal vDisk est activé, aucun de ces événements n'est affiché.

Un ID d'événement de 1 signifie un message d'information et un ID de 2 signifie une erreur. Les événements ne peuvent pas tous être utilisés dans chaque version de Personal vDisk.

ID d'événement	Description
1	État de Personal vDisk : inventaire de mise à jour démarré.
1	État de Personal vDisk : inventaire de mise à jour terminé. GUID : %s.
1	État de Personal vDisk : mise à jour de l'image démarrée.
1	État de Personal vDisk : mise à jour de l'image terminée.
1	Réinitialisation en cours.
1	OK.
2	État de Personal vDisk : échec de l'inventaire de mise à jour avec : %s.
2	État de Personal vDisk : échec de mise à jour de l'image avec : %s.
2	État de Personal vDisk : échec de mise à jour de l'image avec erreur interne.
2	État de Personal vDisk : échec de l'inventaire de mise à jour avec : erreur interne.
2	Personal vDisk a été désactivé suite à un arrêt incorrect.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ID d'événement	Description
2	Échec de la mise à jour de l'image. Code d'erreur %d.
2	Personal vDisk a rencontré une erreur interne. Code d'état [%d] Code d'erreur [0x%X].
2	Échec de réinitialisation de Personal vDisk.
2	Détection du disque utilisé pour stocker les paramètres de personnalisation utilisateur impossible.
2	Espace disponible sur le disque de stockage insuffisant pour créer un conteneur Personal vDisk.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Supprimer des composants

Jul 07, 2016

Pour supprimer des composants, Citrix vous recommande d'utiliser la fonctionnalité Windows destinée à supprimer ou modifier des programmes. Vous pouvez également supprimer des composants à l'aide de la ligne de commande, ou d'un script sur le support d'installation.

Lorsque vous supprimez des composants, les composants pré-requis ne sont pas supprimés, et les paramètres du pare-feu ne sont pas modifiés. Lorsque vous supprimez un Controller, le logiciel SQL Server et les bases de données ne sont pas supprimés.

Avant de supprimer un Controller, supprimez-le du site. Avant de supprimer Studio ou Director, Citrix recommande de les fermer.

Si vous avez mis à niveau un Controller à partir d'un déploiement antérieur contenant l'Interface Web, vous devez supprimer le composant Interface Web séparément ; vous ne pouvez pas utiliser le programme d'installation pour supprimer l'Interface Web.

À partir de la fonctionnalité Windows pour la suppression ou la modification de programmes :

- Pour supprimer un Controller, Studio, Director, le serveur de licences ou StoreFront, sélectionnez Citrix XenApp ou Citrix XenDesktop , puis cliquez avec le bouton droit de la souris et sélectionnez Désinstaller. Le programme d'installation démarre, et vous permet de sélectionner les composants à supprimer.
  Sinon, vous pouvez supprimer StoreFront en cliquant avec le bouton droit de la souris sur Citrix StoreFront et en sélectionnant Désinstaller.
- Pour supprimer un VDA, sélectionnez Citrix Virtual Delivery Agent , puis cliquez avec le bouton droit de la souris et sélectionnez Désinstaller. Le programme d'installation démarre et vous permet de sélectionner les composants à supprimer.
- Pour supprimer le Serveur d'impression universelle, sélectionnez Serveur d'impression universelle Citrix, puis cliquez avec le bouton droit de la souris et sélectionnez Désinstaller.

À partir du répertoire d'installation \x64\XenDesktop sur le support d'installation, exécutez la commande XenDesktopServerSetup.exe.

- Pour supprimer un ou plusieurs composants principaux, utilisez les options /remove et /components.
- Pour supprimer tous les composants, utilisez l'option /removeall.

Pour plus d'informations sur les commandes et les paramètres, consultez la section Installer à l'aide de la ligne de commande.

Par exemple, les commandes suivantes suppriment Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio
```

À partir du répertoire d'installation \x64\XenDesktop sur le support d'installation, exécutez la commande XenDesktopVdaSetup.exe.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Pour supprimer un ou plusieurs composants principaux, utilisez les options /remove et /components.
- Pour supprimer tous les composants, utilisez l'option /removeall.

Pour plus d'informations sur les commandes et les paramètres, consultez la section Installer à l'aide de la ligne de commande.

Par exemple, la commande suivante supprime le VDA et Receiver.
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
Pour supprimer des VDA à l'aide d'un script dans Active Directory, consultez la section Installer ou supprimer des Virtual Delivery Agents à l'aide de scripts.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mettre à niveau et migrer

Jul 07, 2016

Mise à niveau des déploiements de modifications vers les dernières versions des composants sans définir de nouvelles machines ou sites ; cela s'appelle une mise à niveau sur place. Vous pouvez effectuer la mise à niveau :

- Depuis la version XenDesktop 5 (ou version ultérieure) à la version actuelle de XenDesktop
- Depuis la version XenApp 7.5 à la version XenApp actuelle

Vous pouvez également mettre à niveau un serveur de tâches XenApp 6.5 vers un VDA actuel pour système d'exploitation Windows Server. Ceci est une activité supplémentaire à la migration de XenApp 6.5.

Pour la mise à niveau d'une batterie XenDesktop 5 (ou version ultérieure) ou un site XenApp 7.5 :

1. Exécutez le programme d'installation sur les machines sur lesquelles les composants principaux et les VDA sont installés. Le logiciel détermine si une mise à niveau est disponible et installe la nouvelle version.
2. Utilisez Studio nouvellement mis à niveau pour mettre à niveau la base de données et le site.

Pour plus d'informations, veuillez consulter la section Mettre un déploiement à niveau.

Pour plus d'informations sur l'installation des corrections pour le Controller, consultez l'article du centre de connaissances CTX201988.

Pour mettre à niveau un serveur de tâches XenApp 6.5 vers un VDA actuel :

1. Exécutez le programme d'installation du produit sur un serveur de tâches XenApp 6.5. Le logiciel supprime le serveur de la batterie XenApp 6.5, supprime le logiciel XenApp 6.5 et installe un VDA actuel pour système d'exploitation Windows Server.
2. Après la mise à niveau du serveur, ajoutez-le aux catalogues de machines et groupes de mise à disposition dans le site actuel.

Pour de plus amples informations, consultez la section Mettre à niveau une tâche XenApp 6.5 vers un VDA pour OS Windows Server.

La migration déplace les données depuis déploiement antérieur vers la version la plus récente. Vous pouvez migrer un déploiement XenApp 6.5 ou un déploiement XenDesk 4. La migration comprend l'installation de composants actuels et la création d'un nouveau site, l'exportation de données à partir de l'ancienne batterie, puis l'importation des données vers le nouveau site.

Pour effectuer la migration de XenApp 6.5 :

1. Installez les composants de base et créez un nouveau site XenApp.
2. Dans le Controller XenApp 6.5, utilisez les applets de commande PowerShell pour l'exportation des données de stratégie et/ou de batterie vers les fichiers XML. Vous pouvez modifier le contenu de fichier XML pour personnaliser les informations que vous allez importer.
3. Dans le nouveau site, utilisez les applets de commande PowerShell et les fichiers XML pour importer les données de stratégie et/ou d'application vers le nouveau site.
4. Effectuez les tâches de post-migration dans le nouveau site.

Pour de plus amples informations, veuillez consulter la section Migrer XenApp 6.x.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour migrer depuis XenDesktop 4 :

1. Installez les composants de base et créez un nouveau site XenDesktop.
2. À partir de la batterie XenDesktop 4, utilisez l'outil de commande d'exportation pour l'exportation de données de batterie vers un fichier XML. Vous pouvez modifier le contenu de fichier XML pour personnaliser les informations que vous allez importer.
3. À partir du nouveau site, utilisez l'outil de commande d'importation et le fichier XML pour importer les données de la batterie vers le nouveau site.
4. Effectuez les tâches de post-migration dans le nouveau site.

Pour de plus amples informations, veuillez consulter la section Migrer XenDesktop 4.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mettre un déploiement à niveau

Aug 22, 2016

Dans cet article :

- Introduction
- Quelles versions des composants du produit peuvent être mises à niveau ?
- Configuration requise, limitations et préparation
- Considérations d'environnement mixte
- VDA sur les machines exécutant Windows XP ou Windows Vista
- VDA sur les machines exécutant Windows 8.x et Windows 7
- Prise en charge de VDA mixte
- Séquence de mise à niveau

Introduction

Vous pouvez mettre à niveau certains déploiements vers des versions plus récentes sans devoir d'abord configurer les nouvelles machines ou sites ; cela s'appelle une mise à niveau sur place. Vous pouvez effectuer la mise à niveau :

- Depuis la version XenDesktop 5 (ou version ultérieure) à la dernière version de XenDesktop (courante)
- Depuis XenApp version 7.5 (ou version ultérieure) à la dernière version de XenApp (courante)

Vous pouvez également utiliser le programme d'installation de la version XenApp actuelle pour mettre à niveau un serveur de tâches XenApp 6.5 vers une version actuelle de VDA pour système d'exploitation Windows Server. Ceci est une activité supplémentaire à la migration de XenApp 6.5 ; consultez la section Mettre à niveau une tâche XenApp 6.5 vers un VDA pour OS Windows Server.

Pour démarrer une mise à niveau, vous devez exécuter le programme d'installation à partir de la nouvelle version pour mettre à niveau la version précédemment installée des composants principaux (Delivery Controller, Citrix Studio, Citrix Director, le serveur de licences Citrix) et les VDA. Le programme d'installation détermine quels composants exigent une mise à niveau, puis démarre la mise à niveau dès que vous le désirez. Après la mise à niveau des composants, vous devez utiliser la version de Studio nouvellement mise à niveau pour mettre à niveau la base de données du site et le site.

Dans ce contenu, le mot produit fait référence à XenApp 7.x ou XenDesktop 7.x, sauf spécification contraire.

Quelles versions des composants du produit peuvent être mises à niveau ?

À l'aide du programme d'installation du produit et de Studio, vous pouvez effectuer la mise à niveau de :

- Delivery Controller 5 ou version ultérieure
- VDA 5.0 SP1 ou version ultérieure
  - Contrairement aux versions antérieures de VDA, vous devez utiliser le programme d'installation du produit pour mettre à niveau les VDA ; vous ne pouvez pas utiliser de MSI.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Si le programme d'installation détecte Receiver pour Windows (Receiver.exe) sur la machine, il est mis à niveau vers la version de Receiver incluse sur le support d'installation du produit.
- VDA 5.0 SP1 à VDA 7.8 : si le programme d'installation détecte Receiver pour Windows Enterprise (CitrixReceiverEnterprise.exe) sur la machine, il est mis à niveau vers Receiver pour Windows Enterprise 3.4.

- Director 1 ou version ultérieure
- Base de données : cela permet de mettre à niveau le schéma et migre les données pour la base de données du site (ainsi que les bases de données de journalisation de la configuration et de surveillance, si vous effectuez une mise à niveau à partir d'une version antérieure à la version 7.x)
- Personal vDisk

Utilisation de l'aide de la fonctionnalité/documentation du produit, mettez à niveau les éléments suivants si nécessaire :

- Provisioning Services (pour XenApp 7.x et XenDesktop 7.x, Citrix vous recommande d'utiliser la dernière version ; la version minimale prise en charge est Provisioning Services 7.0).
  - Mettez à niveau le serveur Provisioning Services à l'aide de la mise à niveau continue du serveur, et les clients à l'aide des versions vDisk.
  - Provisioning Services 7.x ne prend pas en charge la création de nouveaux bureaux avec XenDesktop 5. Ainsi, bien que les bureaux existants continuent de fonctionner, vous ne pouvez pas utiliser Provisioning Services 7.x pour créer de nouveaux bureaux tant que vous n'avez pas effectué la mise à niveau de XenDesktop. Par conséquent, si vous envisagez d'utiliser un environnement mixte de sites XenDesktop 5.6 et 7.x, ne mettez pas à niveau Provisioning Services vers la version 7.
- Microsoft System Center Virtual Machine Manager SCVMM Le produit actuel prend en charge SCVMM 2012 et SCVMM 2012 SP1 ; XenDesktop 5.x prend en charge les versions antérieures. Utilisez la séquence de mise à niveau suivante afin d'éviter l'interruption :
  1. Si vous possédez des Controller exécutant des versions antérieures à XenDesktop 5.6 FP1, mettez à niveau vers XenDesktop 5.6 FP1 (consultez la documentation XenDesktop pour cette version).
  2. Mettez à niveau le serveur SCVMM vers SCVMM 2012 ; consultez la documentation Microsoft pour obtenir des instructions.
  3. Mettez à niveau les composants XenDesktop vers la version actuelle.
  4. Si vous le souhaitez, vous pouvez mettre à niveau le serveur SCVMM vers SCVMM 2012 SP1.
- StoreFront.

Configuration requise, limitations et préparation

- Vous devez utiliser l'interface graphique du produit ou l'interface de ligne de commande du programme d'installation du produit pour la mise à niveau des composants principaux et VDA ; vous ne pouvez pas importer ou faire migrer des données à partir d'une version antérieure.
- Si vous installez ou mettez à niveau les composants vers la nouvelle version, mais ne choisissez pas de mettre à niveau d'autres composants (sur différentes machines) qui nécessitent une mise à niveau, Studio vous le rappelera. Par exemple, si une mise à niveau comprend les nouvelles versions de Controller et de Studio, et que vous effectuez une mise à niveau uniquement du Controller (mais que vous n'exécutez pas le programme d'installation sur la machine sur laquelle Studio est installé), Studio ne pourra pas vous permettre de continuer à gérer le site avant que vous mettiez Studio à niveau.
- Avant de mettre à niveau le serveur de licences Citrix, assurez-vous que votre abonnement à Subscription Advantage est toujours valide pour la nouvelle version du produit. Si vous mettez à niveau depuis une version antérieure à la version 7.x du produit, la date doit être au moins 2016.0518.
- Vous ne pouvez pas mettre à niveau XenDesktop Express Edition. Obtenez et installez une licence pour une édition

© 1999-2017 Citrix Systems, Inc. All rights reserved.

actuellement prise en charge, puis effectuez une mise à niveau.

- Avant de procéder à toute activité de mise à niveau, sauvegardez la base de données, comme indiqué dans l'article CTX135207, afin de pouvoir la restaurer en cas de problème après la mise à niveau de la base de données.
- Si vous le souhaitez, vous pouvez sauvegarder les modèles et mettre à niveau les hyperviseurs, le cas échéant.
- Assurez-vous que le site est fonctionnel et stable avant de démarrer une mise à niveau. Si un site présente des problèmes, la mise à niveau ne résoudra pas ces problèmes, et peut laisser le site dans un état difficile à réparer.
- Avant de démarrer une mise à niveau, fermez tous les programmes qui pourraient entraîner des verrouillages de fichier, y compris les consoles d'administration et les sessions PowerShell. (Le redémarrage de la machine assure que tout verrouillage de fichier est annulé et qu'aucune mise à jour Windows n'est en attente.)
- Si vous devez continuer à exécuter des sites de version antérieure et des sites de version actuelle, consultez la section Considérations d'environnement mixte.
- Si des VDA sont déjà installés sur les machines Windows XP ou Windows Vista, consultez la section VDA sur les machines exécutant Windows XP ou Windows Vista.
- Si vous ne prévoyez pas de mettre à niveau tous les VDA vers la version la plus récente, consultez la section Prise en charge de VDA mixte.
- Si votre déploiement comprend l'Interface Web, Citrix recommande d'utiliser StoreFront.
- En plus d'être un utilisateur du domaine, vous devez être un administrateur local sur les machines sur lesquelles vous mettez à niveau les composants du produit.
- Vérifiez la séquence de mise à niveau ci-dessous afin de pouvoir planifier et réduire tout problème potentiel.

Vous ne pouvez pas mettre à niveau :

- Depuis une version antérieure ou version Technology Preview
- Depuis une version de XenApp antérieure à la version 7.5 (à l'exception du logiciel de remplacement XenApp 6.5 sur un serveur avec un VDA courant pour OS de serveur ; voir Migrer XenApp 6.x)
- Depuis une version de XenDesktop antérieure à la version 5.6 ; voir Migrer XenDesktop 4
- Depuis XenApp à XenDesktop, ou depuis XenDesktop à XenApp

Recommandation : avant et lors de la mise à niveau, vérifiez l'intégrité du site. Exécutez **Tester le site** aux points de contrôle suivants :

- Avant de procéder à des copies de sauvegarde.
- Après la mise à niveau de chaque Controller.
- Après que les VDA et les autres composants sont mis à niveau.
- Après la mise à niveau du site à partir de Studio.

Considérations d'environnement mixte

Lorsque votre environnement contient des sites/batteries dont les versions de produits diffèrent (environnement mixte), Citrix recommande d'utiliser StoreFront pour regrouper les applications et les bureaux provenant de versions de produits différentes (par exemple, si vous disposez d'un site XenDesktop 7.1 et d'un site XenDesktop 7.5). Pour plus de détails, consultez la documentation StoreFront.

- Dans un environnement mixte, continuez à utiliser les versions de Studio et de Director pour chaque version, mais assurez-vous que les différentes versions sont installées sur des machines distinctes.
- Si vous voulez exécuter des sites XenDesktop 5.6 et 7.x simultanément et utiliser Provisioning Services pour les deux, déployez un nouveau Provisioning Services à utiliser avec le site 7.x, ou mettez à niveau Provisioning Services et soyez

© 1999-2017 Citrix Systems, Inc. All rights reserved.

incapable de provisionner de nouvelles charges de travail dans le site XenDesktop 5.6.

Citrix vous recommande de mettre à niveau tous les composants dans chaque site. Bien que vous puissiez utiliser des versions antérieures de certains composants, certaines fonctionnalités de la version la plus récente risquent de ne pas être disponibles. Par exemple, bien que vous puissiez utiliser les VDA actuels dans les déploiements contenant des versions antérieures de Controller, les nouvelles fonctionnalités de la version actuelle peuvent ne pas être disponibles. Des problèmes d'enregistrement de VDA peuvent aussi se produire lors de l'utilisation de versions antérieures. Voir Considérations de VDA mixte ci-dessous.

- Les sites ayant des Controller à la version 5.x et des VDA à la version 7.x ne devraient rester dans cet état que temporairement. Dans l'idéal, vous devez effectuer la mise à niveau de tous les composants dès que possible.
- Ne mettez pas à niveau une version autonome de Studio tant que vous n'êtes pas prêt à utiliser la nouvelle version.

VDA sur les machines exécutant Windows XP ou Windows Vista

Vous ne pouvez pas mettre à niveau les VDA installés sur les machines exécutant Windows XP ou Windows Vista vers une version 7.x. Vous devez utiliser le VDA 5.6 FP1 avec certaines corrections à chaud ; voir l'article CTX140941 pour obtenir des instructions. Bien que les VDA de versions antérieures s'exécutent dans un site 7.x, ils ne peuvent utiliser la plupart de ses fonctionnalités, notamment :

- Les fonctionnalités mentionnés dans Studio qui nécessitent une nouvelle version du VDA.
- Configuration des applications App-V dans Studio.
- Configuration des adresses Receiver StoreFront dans Studio.
- Prise en charge automatique des licences KMS Microsoft Windows lors de l'utilisation de Machine Creation Services (MCS). Veuillez consulter l'article CTX128580.
- Informations de Director :
  - Temps d'ouverture de session et événements de fin d'ouverture de session qui ont un impact sur la durée d'ouverture de session dans les vues Tableau de bord, Tendances et Détails de l'utilisateur.
  - La répartition des détails de la durée d'ouverture de session pour la connexion HDX et la durée d'authentification, ainsi que les détails de la durée de chargement du profil, la charge GPO, le script d'ouverture de session et l'établissement de la session interactive.
  - Plusieurs catégories de machine et taux d'échec de connexion.
  - Gestionnaire d'activités dans les vues Assistance et Détails de l'utilisateur.

Citrix vous recommande de réimager les machines Windows XP et Windows Vista vers une version de système d'exploitation pris en charge, puis d'installer la dernière version du VDA.

VDA sur les machines exécutant Windows 8.x et Windows 7

Pour mettre à niveau les VDA installés sur les machines exécutant Windows 8.x ou Windows 7 vers Windows 10, Citrix vous recommande de réimager les machines Windows 7 et Windows 8.x vers Windows 10, puis d'installer le VDA pour Windows 10. Si réimager n'est pas une option, désinstallez le VDA avant de mettre à niveau le système d'exploitation, sinon, le VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

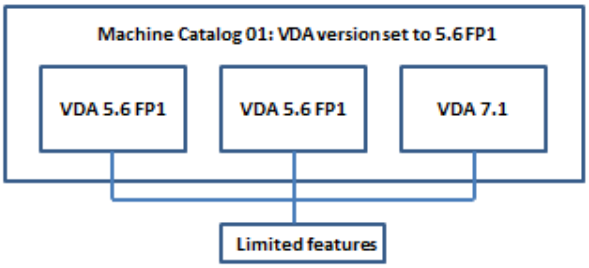
sera dans un état non pris en charge.

Prise en charge de VDA mixte

Lorsque vous mettez à niveau le produit vers une version ultérieure, Citrix vous recommande de mettre à niveau tous les composants principaux et les VDA, vous pouvez accéder à toutes ses nouvelles fonctionnalités dans votre édition. Par exemple, pour utiliser le pré-lancement de session, la persistance de session, et les fonctionnalités des utilisateurs non authentifiés dans la version 7.6, les VDA doivent posséder la version 7.6 au minimum installée.

Dans certains environnements, vous risquez de ne pas pouvoir mettre à niveau tous les VDA vers la version la plus récente. Dans ce scénario, lorsque vous créez un catalogue de machines, vous pouvez spécifier la version du VDA installée sur les machines. Par défaut, ce paramètre spécifie la dernière version du VDA recommandée, vous devez tenir compte de la modification de ce paramètre uniquement si le catalogue de machines contient des machines avec des versions antérieures du VDA. Cependant, si des versions VDA sont mixées dans un catalogue de machines, cela peut avoir des effets indésirables

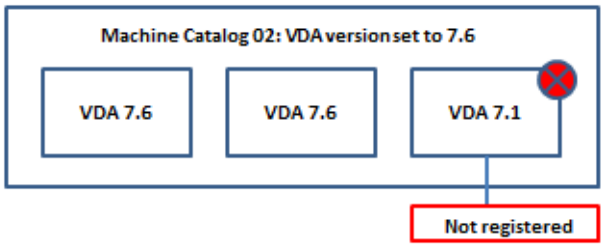
Comme indiqué ci-dessus, si votre déploiement comprend des systèmes Windows XP et Windows Vista, vous devez utiliser une version antérieure du VDA, et le catalogue de machines contenant ces machines doit spécifier de la version VDA 5.6 FP1. Le VDA s'enregistre avec succès avec le Controller, mais ces machines ne pourront pas utiliser la plupart des nouvelles fonctionnalités des versions 7.x (y compris StoreFront). Cela s'applique également aux machines que vous ajoutez à ce catalogue qui possèdent des VDA version 7.x. Le graphique suivant illustre ceci.



Dans le cas ci-dessus, si vous devez continuer à utiliser des VDA de version plus ancienne, placez-les dans un catalogue de machines par eux-mêmes.

Si un catalogue de machine est créé avec le paramètre de valeur par défaut de VDA recommandée, et toutes les machines du catalogue possèdent une version antérieure de VDA installée, ces machines ne pourront pas s'enregistrer auprès du Controller et ne fonctionneront pas.

Imaginons, par exemple, que la dernière version du VDA est 7.6. Vous créez un catalogue de machines à l'aide du paramètre par défaut du VDA : « 7.6 (recommandé pour accéder aux dernières fonctionnalités) ». Vous ajoutez trois machines à ce catalogue : deux avec VDA 7.6 et une avec VDA 7.1.

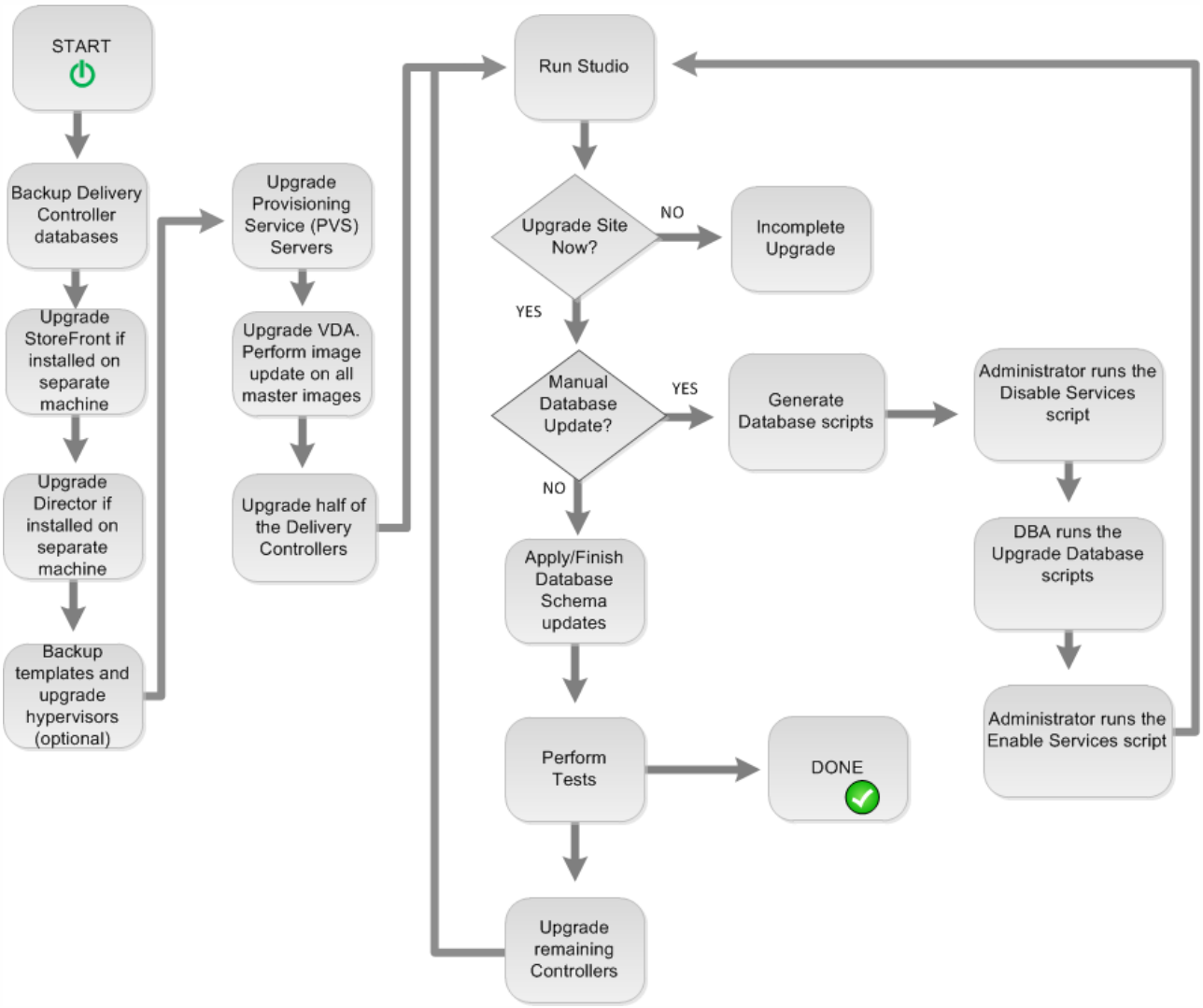


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dans cet exemple, la machine comportant la version VDA 7.1 ne pourra pas s'enregistrer avec le Controller. Si vous ne pouvez pas mettre à niveau ce VDA, vous pouvez créer un nouveau catalogue de machines configuré avec un paramètre VDA de « version 7.0 ou ultérieure » et ajouter cette machine. Bien que cette machine ne puisse pas utiliser les nouvelles fonctionnalités de la version 7.6, elle sera en mesure de s'enregistrer avec le Controller.

Séquence de mise à niveau

La séquence de mise à niveau est illustrée ci-dessous ; les descriptions suivent. Si les composants sont installés sur des machines différentes, vous exécutez le programme d'installation sur chacune de ces machines.



Pour exécuter l'interface graphique du programme d'installation du produit, ouvrez une session sur la machine, puis insérez le support ou montez le lecteur ISO pour la nouvelle version. Cliquez deux fois sur **Sélection automatique**. Pour utiliser l'interface de ligne de commande, consultez la section Installer à l'aide de la ligne de commande.

1. Si plus d'un composant principal est installé sur le même serveur (par exemple, le Controller, Studio et le serveur de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

licences) et plusieurs de ces composants possèdent de nouvelles versions disponibles, ils seront mis à niveau lorsque vous exécutez le programme d'installation sur le serveur. Si les composants principaux sont installés sur des machines autres que le Delivery Controller, exécutez le programme d'installation sur chacune de ces machines (dans l'ordre de préférence: Serveur de licences, StoreFront, et Director).

2. Mettez à niveau les serveurs et les clients Provisioning Services, à l'aide des instructions de la documentation Provisioning Services.
3. Exécutez le programme d'installation du produit sur des machines contenant les VDA. Bien qu'il soit possible de mettre à niveau les VDA avant ou après la mise à niveau des Controller, Citrix vous recommande de le faire avant, car elle permet de faire rapidement activer les nouvelles fonctionnalités après la mise à niveau.
   Lors de la mise à niveau des VDA à partir d'une version antérieure (version 7.x) qui sont installés sur des machines physiques (y compris à Remote PC Access), qui utilisent l'interface de ligne de commande avec le paramètre: /EXCLUDE "Personal vDisk","Machine Identity Service". Par exemple :

   C:\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /EXCLUDE "Personal vDisk","Machine Identity Service"

4. Exécutez le programme d'installation du produit sur la moitié des Controller. (Cette opération mettra également à niveau les autres composants principaux installés sur ces serveurs). Par exemple, si votre site comporte quatre Controller, exécutez le programme d'installation sur deux d'entre eux.
   - Le fait de laisser la moitié des Controller actifs permet aux utilisateurs d'accéder au site. Les VDA peuvent s'enregistrer auprès des Controller restants. Il peut aussi arriver que le site dispose d'une capacité réduite car moins de Controller sont disponibles. La mise à niveau entraîne une brève interruption dans l'établissement de nouvelles connexions client au cours des dernières étapes de mise à niveau de la base de données. Le Controller mis à niveau ne peut pas traiter les demandes tant que l'intégralité du site n'a pas été mise à niveau.
   - Si votre site comporte un seul Controller, le site est inutilisable lors de la mise à niveau.
5. Si Studio est installé sur une autre machine que l'un des Controller vous avez mis à niveau à l'étape précédente, exécutez le programme d'installation sur la machine sur laquelle Studio est installé.
6. Depuis la version de Studio nouvellement mise à niveau, mettez à niveau la base de données du site. Pour de plus amples informations, consultez la section Mettez à niveau la base de données et le site.
7. Depuis la version de Studio nouvellement mise à niveau, sélectionnez **Citrix Studio** *nom-site* dans le volet de navigation. Sélectionnez l'onglet **Tâches courantes**. Sélectionnez **Mettre à niveau les Delivery Controller restants**.
8. Après avoir effectué la mise à niveau et confirmé l'achèvement, fermez puis rouvrez Studio.
9. Dans la section Configuration du site de la page Tâches courantes, sélectionnez **Procéder à l'enregistrement**. L'inscription des Controller les rend disponibles pour le site.
10. Lorsque vous sélectionnez **Terminer** lorsque la mise à niveau est terminée, vous vous voyez offrir l'opportunité de vous inscrire dans le Programme d'amélioration du produit (CEIP) Citrix, qui collecte des informations anonymes relatives à votre déploiement. Ces informations sont utilisées pour améliorer la qualité, la fiabilité et les performances nos produits.
11. Après la mise à niveau des composants, de la base de données et du site, utilisez Studio pour :
    - Testez le site nouvellement mis à niveau. À partir de Studio, sélectionnez **Citrix Studio** *nom du site* dans le volet de navigation. Sélectionnez l'onglet **Tâches courantes**, puis sélectionnez **Tester le site**. Ces tests ont été exécutés automatiquement après que vous ayez mis à niveau la base de données, mais vous pouvez les exécuter à tout moment.
    - Mettre à jour toutes les images principales qui utilisent le VDA mis à niveau.
    - Mettez à niveau les catalogues de machines et les groupes de mise à disposition.

Après mise à niveau des composants principaux et des VDA, utilisez la version nouvellement mise à niveau de Studio pour initier une mise à niveau automatique ou manuelle de la base de données et du site.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Pour une mise à niveau automatique de la base de données, les autorisations de l'utilisateur de Studio doivent inclure la possibilité de mettre à jour le schéma de base de données SQL Server (par exemple, le rôle de base de données db_securityadmin ou db_owner). Pour de plus amples informations, veuillez consulter l'article Bases de données.
- Si l'utilisateur Studio ne possède pas ces autorisations, l'initiation de la mise à niveau manuelle d'une base de données générera des scripts. L'utilisateur Studio exécute certains de ces scripts depuis Studio ; l'administrateur de la base de données exécute d'autres scripts à l'aide d'un outil tel que SQL Server Management Studio. Si les scripts SQL sont exécutés manuellement, ils doivent être exécutés à l'aide de l'utilitaire SQLCMD ou de SQL Management Studio en mode SQLCMD. Si ce n'est pas le cas, des erreurs peuvent se produire.

Important : Citrix recommande vivement de sauvegarder la base de données avant de procéder à la mise à niveau, comme décrit dans l'article CTX135207.
Lors d'une mise à niveau de base de données, les services du produit sont désactivés. Pendant ce temps, les Controller ne peuvent pas initier de nouvelles connexions pour le site, ainsi effectuez une planification prudente.

Une fois la mise à niveau de la base de données terminée, et les services du produit activés, Studio teste l'environnement et la configuration, puis génère un rapport HTML. Si des problèmes sont identifiés, vous pouvez restaurer la sauvegarde de la base de données. Après avoir résolu les problèmes, vous pouvez effectuer la mise à niveau de la base de données à nouveau.

Mettre à niveau la base de données et le site automatiquement - Lancez le logiciel Studio nouvellement mis à niveau. Lorsque vous choisissez de démarrer la mise à niveau du site automatiquement et confirmer que vous êtes prêt, la mise à niveau de la base de données et du site se poursuit.

Mettre à niveau la base de données et le site manuellement - Ce processus inclut la génération et l'exécution de scripts.

1. Lancez le logiciel Studio nouvellement mis à niveau. Après avoir choisi d'effectuer la mise à niveau manuelle du site, l'Assistant vérifie la compatibilité du serveur de licences et des demandes de confirmation. Après confirmation que vous avez sauvegardé la base de données, l'Assistant génère et affiche les scripts et une liste des étapes de mise à niveau.
2. Exécutez les scripts dans l'ordre indiqué :

Script	Description
DisableServices.ps1	Script PowerShell à exécuter par l'utilisateur de Studio sur un Controller pour désactiver les services du produit.
UpgradeSiteDatabase.sql	Script SQL à exécuter par l'administrateur de la base de données sur le serveur qui contient la base de données du site, à l'aide d'un outil tel que SQL Server Management Studio.
UpgradeMonitorDatabase.sql	Script SQL à exécuter par l'administrateur de la base de données sur le serveur qui contient la base de données de surveillance, à l'aide d'un outil tel que SQL Server Management Studio.
UpgradeLoggingDatabase.sql	Script SQL à exécuter par l'administrateur de la base de données sur le serveur qui contient la base de données de journalisation de la configuration, à l'aide d'un outil tel que SQL Server Management Studio. Exécutez ce script uniquement si cette base de données change (par exemple, après l'application d'un correctif logiciel).
EnableServices.ps1	Script PowerShell à exécuter par l'utilisateur de Studio sur un Controller pour activer les services du produit.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Une fois que vous avez terminé la liste des tâches affichées, sélectionnez **Terminer la mise à niveau et revenir aux Tâches courantes**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mettre à niveau une tâche XenApp 6.5 vers un nouveau VDA

Jul 07, 2016

Lorsque vous exécutez le programme d'installation du produit actuel sur un serveur de tâches XenApp 6.5 :

- Supprime le serveur de la batterie XenApp 6.5 (cette tâche appelle automatiquement le programme d'installation XenApp 6.5 de l'interface de ligne de commande)
- Supprime le logiciel XenApp 6.5
- Installe un nouveau VDA (XenApp 7.6 ou version ultérieure) pour système d'exploitation Windows Server

Lorsque vous utilisez le programme d'installation de l'interface graphique, vous serez guidé au travers du même assistant que vous avez utilisé lors de l'installation des VDA pour OS Windows Server dans votre nouveau site XenApp. De même, l'interface de ligne de commande utilise les mêmes commandes et paramètres que vous utilisez pour installer d'autres VDA.

REMARQUE : bien qu'il soit possible de mettre à niveau un serveur de tâches XenApp 6.5, l'installation du logiciel VDA actuel sur une nouvelle machine fournit une meilleure sécurité.

Vous vous êtes probablement déjà familiarisés avec le programme d'installation lors de l'installation des composants principaux et VDA XenApp. Lancez le programme d'installation (Installer à l'aide de l'interface graphique) ou entrez la commande (Installer à l'aide de la ligne de commande) sur le serveur de tâches XenApp 6.5.

À savoir :

- Cette mise à jour n'est pas valide sur des serveurs XenApp 6.5 configurés en mode Hôte de session uniquement (également appelés serveurs en mode de session uniquement ou serveurs de tâches).
- La désinstallation de XenApp 6.5 nécessite plusieurs redémarrages du serveur. Lors de l'utilisation de l'interface de ligne de commande, vous pouvez utiliser l'option /NOREBOOT pour empêcher cette action automatique ; toutefois, vous devez redémarrer le serveur pour la désinstallation et les installations suivantes pour continuer.
- Si une erreur se produit lors du processus de désinstallation de XenApp, consultez le journal des erreurs de désinstallation dont il est fait référence dans le message d'erreur. Les fichiers journaux désinstallés résident dans le dossier « %TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\. »
- Une fois la mise à niveau terminée, vérifiez les paramètres et les entrées de registre IMA, ainsi que les paramètres système et registres HDX. Certains paramètres peuvent ne plus s'appliquer ou ne pas fonctionner de la même manière.
- Après avoir effectué la mise à niveau des serveurs de tâches XenApp 6.5, depuis Studio dans le nouveau site XenApp, créez des catalogues de machines (ou modifier des catalogues existants) pour les tâches mise à niveau.
- Si vous avez migré les paramètres de stratégie et d'application à partir d'un serveur Controller XenApp 6.5 (voir Migrer XenApp 6.x), assignez les groupes de mise à disposition contenant les applications publiées migrées pour le catalogue de machine qui héberge ces applications dans XenApp 6.5.

Symptômes : la suppression du logiciel XenApp 6.5 échoue. Le journal de désinstallation contient le message : « Erreur 25703. Une erreur s'est produite lors du branchement de XML dans Internet Information Server. Le programme d'installation ne peut pas copier des fichiers dans votre répertoire des scripts IIS. Vérifiez que votre installation d'IIS est correcte.

- Cause : le problème se produit sur les systèmes sur lesquels (1) pendant la phase initiale de l'installation de XenApp 6.5, vous avez indiqué que le service XML Citrix (CtxHttp.exe) ne peut pas partager un port avec IIS, et (2) .NET Framework 3.5.1 est installé.
- Résolution :
  1. Supprimez le rôle de Serveur Web (IIS) à l'aide de l'Assistant Supprimer des rôles sur le serveur Windows. (Vous pouvez réinstaller le rôle Serveur Web (IIS) plus tard).
  2. Redémarrez le serveur.
  3. À l'aide de l'option Ajout/Suppression de programmes, désinstallez les éléments suivants :
     1. Citrix XenApp 6.5
     2. Microsoft Visual C++ 2005 Redistributable Package (x64), version 8.0.56336
  4. Redémarrez le serveur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. Exécutez le programme d'installation de XenApp pour installer le VDA pour système d'exploitation Windows Server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Migrer XenApp 6.x

Jul 07, 2016

Important : consultez la totalité de cet article avant de commencer une migration.

L'outil de migration XenApp 6.x (l'outil de migration) est une collection de scripts PowerShell contenant des applets de commande qui migrent une stratégie et des données de batterie XenApp 6.x (6.0 ou 6.5). Sur le serveur de Controller XenApp 6.x, vous pouvez exécuter des applets de commande d'exportation qui collectent ces données dans des fichiers XML. Ensuite, depuis le Controller XenApp 7.6, exécutez les applets de commande d'importation qui créent des objets à l'aide des données collectées au cours de l'exportation.

Une présentation vidéo de l'outil de migration est disponible ici.

La séquence suivante résume le processus de migration ; des détails sont fournis plus tard.

1. Sur un Controller XenApp 6.0 ou 6.5 :
    1. Importez les modules d'exportation PowerShell.
    2. Exécuter les applets de commande d'exportation pour exporter des stratégies et/ou des données de batterie vers les fichiers XML.
2. Copiez les fichiers XML (et le dossier d'icônes si vous choisissez de ne pas les incorporer dans les fichiers XML lors de l'exportation) dans le Controller XenApp 7.6.
3. Sur XenApp 7.6 Controller :
    1. Importez les modules d'importation du PowerShell.
    2. Exécutez les applets de commande d'importation pour importer la stratégie et/ou les données de la batterie de serveurs (applications), à l'aide des fichiers XML en entrée.
4. Terminez les étapes de post-migration.

Avant d'exécuter la migration, vous pouvez exporter vos paramètres XenApp 6.5, puis effectuer une importation de l'aperçu sur le site XenApp 7.6. L'aperçu identifie des points d'échec possibles pour vous permettre de résoudre les problèmes avant de procéder à l'importation elle-même. Par exemple, un aperçu peut détecter qu'une application du même nom existe déjà dans le nouveau site XenApp 7.6. Vous pouvez également utiliser les fichiers journaux générés à partir de l'aperçu en tant que guide de migration.

Sauf spécification contraire, le terme 6.x fait référence à XenApp 6.0 ou 6.5.

Cette version de décembre 2014 (version 20141125) contient les mises à jour suivantes :

- Si vous rencontrez des problèmes lors de l'utilisation de l'outil de migration sur une batterie XenApp 6.x, signalez-les au forum d'assistancehttp://discussions.citrix.com/forum/1411-xenapp-7x/, afin que Citrix puisse les examiner et potentiellement améliorer l'outil.
- Nouveau conditionnement : le fichier XAMigration.zip contient désormais deux packs distincts et indépendants : ReadIMA.zip et ImportFMA.zip. Pour effectuer l'exportation depuis un serveur XenApp 6.x, vous avez uniquement besoin de ReadIMA.zip. Pour effectuer l'importation vers un serveur XenApp 7.6, vous avez uniquement besoin d'ImportFMA.zip.
- L'applet de commande Export-XAFarm prend en charge un nouveau paramètre (EmbedIconData) qui élimine le besoin de copier les données d'icône pour séparer des fichiers.
- L'applet de commande d'Import-XAFarm prend en charge trois nouveaux paramètres :
    - MatchServer : importez des applications depuis des serveurs dont les noms correspondent à une expression
    - NotMatchServer : importez des applications depuis des serveurs dont les noms ne correspondent pas à une expression
    - IncludeDisabledApps : importez des applications désactivées
- Les pré-démarrées ne sont pas importées.
- L'applet de commande Export-Policy fonctionne sur XenDesktop 7.x.

L'outil de migration est disponible depuis le site de téléchargement Citrix sous XenApp 7.6. Le fichier XAMigration.zip contient deux packs séparés et indépendants :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ReadIMA.zip : contient les fichiers utilisés pour exporter des données depuis votre batterie XenApp 6.x, plus les modules partagés.

Module ou fichier	Description
ExportPolicy.psm1	Module de script PowerShell pour l'exportation de stratégies XenApp 6.x vers un fichier XML.
ExportXAFarm.psm1	Module de script PowerShell pour l'exportation de paramètres de batterie XenApp 6.x vers un fichier XML.
ExportPolicy.psd1	Fichier manifeste PowerShell pour module de script ExportPolicy.psm1.
ExportXAFarm.psd1	Fichier manifeste PowerShell pour module de script ExportXAFarm.psm1.
LogUtilities.psm1	Module de script PowerShell partagé qui contient des fonctions de journalisation.
XmlUtilities.psd1	Fichier manifeste PowerShell pour module de script XmlUtilities.psm1.
XmlUtilities.psm1	Module de script PowerShell partagé qui contient les fonctions XML.

- ImportFMA.zip : contient les fichiers utilisés pour importer des données vers votre batterie XenApp 7.6, plus les modules partagés.

Module ou fichier	Description
ImportPolicy.psm1	Module de script PowerShell pour l'importation de stratégies vers XenApp 7.6
ImportXAFarm.psm1	Module de script PowerShell pour l'importation des applications vers XenApp 7.6.
ImportPolicy.psd1	Fichier manifeste PowerShell pour module de script ImportPolicy.psm1.
ImportXAFarm.psd1	Fichier manifeste PowerShell pour module de script ImportXAFarm.psm1.
PolicyData.xsd	Schéma XML pour les données de stratégie.
XAFarmData.xsd	Schéma XML pour les données de batterie XenApp.
LogUtilities.psm1	Module de script PowerShell partagé qui contient des fonctions de journalisation.
XmlUtilities.psd1	Fichier manifeste PowerShell pour module de script XmlUtilities.psm1.
XmlUtilities.psm1	Module de script PowerShell partagé qui contient les fonctions XML.

- Les paramètres de stratégie ne sont pas tous importés ; veuillez consulter la section Paramètres de stratégie non importés. Les paramètres qui ne sont pas pris en charge sont ignorés et affichés dans le fichier journal.
- Bien que tous les détails d'application soient collectés dans le fichier XML de sortie lors de l'opération d'exportation, seules les applications installées sur le serveur sont importées dans le site XenApp 7.6. Les bureaux, le contenu et la plupart des applications publiés livrés en streaming ne sont pas pris en charge (voir les paramètres de l'applet de commande Import-XAFarm dans Étapes détaillées : importer les données pour les exceptions).
- Les serveurs d'applications ne sont pas importés.
- La plupart des propriétés d'application ne sont pas importées en raison des différences entre les technologies XenApp 6.x Independent Management Architecture (IMA) et XenApp 7.6 FlexCast Management Architecture (FMA) ; voir Mappage des propriétés d'application.
- Un groupe de mise à disposition est créé lors de l'importation. Voir Utilisation avancée pour plus de détails sur l'utilisation des paramètres pour filtrer les éléments importés.
- Seuls les paramètres de stratégie Citrix créés avec la console de gestion AppCenter sont importés, les paramètres de stratégie Citrix créés avec les Objets de stratégie de groupe (GPO) ne sont pas importés.
- Les scripts de migration sont uniquement conçus pour les migrations de XenApp 6.x à XenApp 7.6.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Les dossiers imbriqués contenant plus de cinq niveaux ne sont pas pris en charge par Studio et ne seront pas importés. Si votre structure de dossier d'applications contient plus de cinq niveaux, réduisez le nombre de dossiers imbriqués avant l'importation.

Les fichiers XML créés par les scripts d'exportation peuvent contenir des informations confidentielles sur votre environnement et votre organisation, telles que des noms d'utilisateurs, des noms de serveur et autres données de batteries, d'applications et de configuration de stratégies XenApp. Stockez et gérez ces fichiers dans des environnements sécurisés.

Lisez attentivement les fichiers XML avant de les utiliser comme entrée pour l'importation des stratégies et des applications pour vous assurer qu'ils ne contiennent pas de modifications non autorisées.

Les affectations des objets de stratégie (anciennement connus sous le nom de filtres de stratégie) contrôlent la manière dont les stratégies sont appliquées. Après avoir importé les stratégies, vérifiez l'affectation des objets de chaque stratégie pour vous assurer qu'il n'existe aucune faille de sécurité résultant de l'importation. Les différents groupes d'utilisateurs, d'adresses IP ou de noms de client peuvent être appliqués à la stratégie après l'importation. Les paramètres autoriser/refuser peuvent avoir différentes significations après l'importation.

Les scripts fournissent une journalisation complète qui effectue le suivi de toutes les exécutions de l'applet de commande, des messages d'information, des résultats d'exécution de l'applet de commande, des avertissements et des erreurs.

- L'utilisation de la plupart des applets de commande PowerShell Citrix est journalisée. Toutes les applets de commande PowerShell des scripts d'importation qui créent de nouveaux objets de site sont journalisées.
- La progression de l'exécution du script est journalisée, y compris les objets en cours de traitement.
- Les actions principales qui affectent l'état du flux sont journalisées, y compris les flux effectués à partir de la ligne de commande.
- Tous les messages imprimés dans la console sont journalisés, y compris les avertissements et les erreurs.
- Chaque ligne est horodatée à la milliseconde près.

Citrix vous recommande de spécifier un fichier journal lorsque vous exécutez chacune des applets de commande d'importation et d'exportation.

Si vous ne spécifiez pas un nom de fichier journal, celui-ci est stocké dans le dossier de base de l'utilisateur actuel (spécifié dans la variable $HOME de PowerShell) si ce dossier existe ; sinon, il est placé dans le dossier d'exécution du script courant. Le nom de journal par défaut est « XFarmAAAAMMJJHHmmSS-xxxxxx » où les six derniers chiffres constituent un nombre aléatoire.

Par défaut, toutes les informations de progression sont affichées. Pour supprimer l'affichage, spécifiez le paramètre NoDetails dans l'applet de commande d'exportation et d'importation.

En général, un script arrête l'exécution lorsqu'une erreur est détectée, et vous pouvez réexécuter l'applet de commande après la suppression des conditions d'erreurs.

Les conditions qui ne sont pas considérées comme des erreurs sont journalisées ; la plupart sont considérées comme des avertissements et l'exécution du script continue. Par exemple, des types d'applications non pris en charge sont considérés comme des avertissements et ne sont pas importés. Les applications qui existent déjà dans le site XenApp 7.6 ne sont pas importées. Les paramètres de stratégie qui sont déconseillés dans XenApp 7.6 ne sont pas importés.

La migration des scripts utilise la plupart des applets de commande PowerShell, et toutes les erreurs possibles peuvent ne pas être journalisées. Pour de plus amples informations sur la journalisation, utilisez les fonctionnalités de journalisation du PowerShell. Par exemple, les transcriptions du PowerShell journalisent tout ce qui est imprimé à l'écran. Pour plus d'informations, consultez l'aide des applets de commande Start-Transcript et Stop-Transcript.

Important : n'oubliez pas de consulter la totalité de cet article avant de commencer une migration.
Vous devez connaître les concepts de base sur la stratégie d'exécution, les modules, les applets de commande et les scripts PowerShell. Bien que des connaissances complètes liées aux scripts ne soient pas requises, vous devez comprendre les applets de commande que vous exécutez. Utilisez l'applet de commande Get-Help pour afficher l'aide de chaque applet de commande de migration avant de l'exécuter. Par exemple :
Get-Help -full Import-XAFarm
Spécifiez un fichier journal sur la ligne de commande et vérifiez toujours le fichier journal après l'exécution d'une applet de commande. Si un script échoue, vérifiez et corrigez les erreurs dans le fichier journal, puis réexécutez l'applet de commande.

À savoir :

- Pour optimiser la mise à disposition d'applications pendant l'exécution de deux déploiements (la batterie XenApp 6.x et le nouveau site XenApp 7.6), vous pouvez regrouper les deux déploiements dans StoreFront ou l'Interface Web. Consultez la documentation eDocs pour votre version de StoreFront ou de l'Interface Web (Gérer > Créer un magasin).
- Les données de l'icône d'application sont gérées de deux manières différentes :
  - si vous spécifiez le paramètre EmbedIconData dans l'applet de commande Export-XAFarm, les données de l'icône d'application exportées sont incorporées dans le fichier XML de sortie.
  - Si vous ne spécifiez pas le paramètre EmbedIconData dans l'applet de commande Export-XAFarm, les données de l'icône d'application exportées sont

© 1999-2017 Citrix Systems, Inc. All rights reserved.

stockées dans un dossier nommé en ajoutant la chaîne « -icons » au nom de base du fichier XML de sortie. Par exemple, si le paramètre XmlOutputFile est « FarmData.xml », le dossier « FarmData-icons » est alors créé pour stocker les icônes de l'application.
Les fichiers de données des icônes dans ce dossier sont des fichiers .txt qui sont nommés à l'aide du nom de navigateur de l'application publiée (bien que les fichiers soient des fichiers .txt, les données stockées sont des données d'icône binaires codées, qui peuvent être lues par le script d'importation pour recréer l'icône de l'application). Lors de l'opération d'importation, si le dossier d'icône ne se trouve pas dans le même emplacement que le fichier XML d'importation, des icônes génériques sont utilisées pour chaque application importée.

- Les noms des modules de script, des fichiers manifestes, des modules partagés et des applets de commande sont similaires. Utilisez la saisie semi-automatique avec précaution afin d'éviter des erreurs. Par exemple, Export-XAFarm est une applet de commande. ExportXAFarm.psd1 et ExportXAFarm.psm1 sont des fichiers qui ne peuvent pas être exécutés.
- Dans les sections détaillées ci-dessous, la plupart des valeurs de paramètre de <chaîne> affichent les guillemets. Ceux-ci sont facultatifs pour les chaînes à mot unique.

Pour exporter depuis le serveur XenApp 6.x :

- L'exportation doit être exécutée sur un serveur XenApp 6.x configuré avec le mode de serveur Controller et hôte de session (plus couramment appelé Controller).
- Pour exécuter les applets de commande d'exportation, vous devez être un administrateur XenApp avec la permission de lecture des objets. Vous devez également disposer de suffisamment de permissions Windows pour exécuter des scripts PowerShell ; les procédures détaillées ci-dessous contiennent les instructions.
- Vérifiez que la batterie XenApp 6.x se trouve dans un état d'intégrité normal avant de procéder à l'exportation. Sauvegardez la base de données de la batterie. Vérifiez l'intégrité de la batterie à l'aide de l'outil Citrix IMA Helper (CTX133983) : à partir de l'onglet du magasin de données IMA, exécutez une vérification de base (puis utilisez l'option DSCheck pour résoudre les entrées non valides). La résolution des problèmes avant d'effectuer la migration vous aide à empêcher les échecs d'exportation. Par exemple, si un serveur n'a pas été correctement supprimé de la batterie, il se peut que ses données soient conservées dans la base de données, ce qui peut entraîner l'échec des applets de commande dans le script d'exportation (par exemple, Get-XAServer -ZoneName). Si les applets de commande échouent, le script échoue.
- Vous pouvez exécuter les applets de commande d'exportation sur une batterie de serveurs en direct qui possède des connexions utilisateur actives ; les scripts d'exportation ne lisent que la configuration statique de la batterie et les données de stratégie.

Pour effectuer l'importation vers le serveur XenApp 7.6 :

- Vous pouvez importer des données vers les déploiements XenApp 7.6 (et sur les versions ultérieures prises en charge). Vous devez installer un Controller XenApp 7.6 et Studio, puis créer un site avant d'importer les données que vous avez exportées depuis la batterie XenApp 6.x. Bien que les VDA ne soient pas nécessaires pour importer des paramètres, Ils autorisent les types de fichiers d'application à être mis à disposition.
- Pour exécuter les applets de commande d'importation XenApp, vous devez être un administrateur XenApp avec autorisation de lecture et de création des objets. Un administrateur complet possède ces autorisations. Vous devez également disposer de suffisamment de permissions Windows pour exécuter des scripts PowerShell ; les procédures détaillées ci-dessous contiennent les instructions.
- Aucune autre connexion utilisateur ne doit être active lors d'une importation. Les scripts d'importation créent beaucoup de nouveaux objets et des dysfonctionnements peuvent se produire si les autres utilisateurs modifient la configuration en même temps.

N'oubliez pas que vous pouvez exporter des données, puis utiliser le paramètre -Preview avec les applets de commande d'importation pour voir ce qui se passe réellement durant une importation, mais sans importer quoi que ce soit. Les journaux indiquent exactement ce qui se passe durant une importation réelle ; si des erreurs se produisent, vous pouvez les résoudre avant de démarrer une importation réelle.

Une vidéo de la marche à suivre pour l'exportation est disponible ici.

Effectuez les étapes suivantes pour l'exportation de données à partir d'un Controller XenApp 6.x vers des fichiers XML.

1. Téléchargez le pack de l'outil de migration XAMigration.zip à partir du site de téléchargement de Citrix. Par commodité, placez-le dans un partage de fichiers réseau pouvant être accédé par la batterie XenApp 6.x et le site XenApp 7.6. Décompressez le fichier XAMigration.zip dans le partage de fichiers du réseau. Deux fichiers zip devraient être présents : ReadIMA.zip et ImportFMA.zip.
2. Ouvrez une session sur le Controller XenApp 6.x en tant qu'administrateur XenApp avec au moins une autorisation en lecture seule et une autorisation Windows pour exécuter des scripts PowerShell.
3. Copiez ReadIMA.zip depuis le partage de fichiers du réseau vers un ControllerXenApp 6.x. Décompressez et extrayez ReadIMA.zip sur le Controller dans un dossier (par exemple : C:\XAMigration).
4. Ouvrez une console PowerShell et définissez le répertoire courant à l'emplacement du script. Par exemple :
   cd C:\XAMigration
5. Vérifiez la stratégie d'exécution de script en exécutant Get-ExecutionPolicy.
6. Définissez la stratégie d'exécution de script sur RemoteSigned au minimum pour autoriser les scripts à être exécutés. Par exemple :
   Set-ExecutionPolicy RemoteSigned
7. Importez les fichiers de définition des modules ExportPolicy.psd1 et ExportXAFarm.psd1 :
   Import-Module .\ExportPolicy.psd1

   Import-Module .\ExportXAFarm.psd1

© 1999-2017 Citrix Systems, Inc. All rights reserved.

À savoir :

- Si vous souhaitez uniquement exporter des données de stratégie, vous ne pouvez importer que le fichier de définition du module ExportPolicy.psd1. De même, si vous souhaitez uniquement exporter des données de la batterie, importez uniquement ExportXAFarm.psd1.
- L'importation des fichiers de définition de module ajoute également les composants enfichables PowerShell requis.
- N'importez pas les fichiers de script .psm1.

8. Pour exporter des données de stratégie, exécutez l'applet de commande Export-Policy.

Paramètre	Description
-XmlOutputFile "<chaîne>.xml"	Nom de fichier de sortie XML ; ce fichier contient les données exportées. Doit posséder une extension .xml. Le fichier ne doit pas exister, mais si un chemin d'accès est spécifié, le chemin parent doit exister. Valeur par défaut : Aucun ; ce paramètre est requis.
-LogFile « <chaîne> »	Nom du fichier journal. Une extension est facultative. Le fichier est créé s'il n'existe pas. Si le fichier existe et que le paramètre NoClobber est également spécifié, une erreur est générée ; sinon, le contenu du fichier est remplacé. Valeur par défaut : consultez la section Journalisation et gestion des erreurs
-NoLog	Ne pas générer de sortie de journal. Ceci remplace le paramètre LogFile, s'il est également spécifié. Valeur par défaut : false; une sortie de journal est générée
-NoClobber	Ne pas remplacer un fichier journal spécifié dans le paramètre LogFile. Si le fichier journal n'existe pas, ce paramètre n'a aucun effet. Valeur par défaut : false ; un fichier journal existant est remplacé
-NoDetails	Ne pas envoyer de rapports détaillés sur l'exécution du script à la console. Valeur par défaut : false ; des rapports détaillés sont envoyés à la console
-SuppressLogo	N'imprimez pas le message « Version de l'outil de migration XenApp 6.x vers XenApp/XenDesktop 7.6 #aaaaMMjj-hhmm# » sur la console. Ce message, qui identifie la version du script, peut être utile lors de la résolution des problèmes ; par conséquent, Citrix vous recommande d'omettre ce paramètre. Valeur par défaut : false ; le message est imprimé sur la console

Exemple : l'applet de commande suivante exporte des informations de stratégie pour le fichier XML appelé MyPolicies.xml. L'opération est journalisée dans le fichier appelé MyPolicies.log.

```
Export-Policy -XmlOutputFile ".\MyPolicies.XML"  -LogFile ".\MyPolicies.Log"
```

9. Pour exporter des données de la batterie, exécutez l'applet de commande Export-XAFarm, en spécifiant un fichier journal et un fichier XML.

Paramètre	Description
-XmlOutputFile "<chaîne>.xml"	Nom de fichier de sortie XML ; ce fichier contient les données exportées. Doit posséder une extension .xml. Le fichier ne doit pas exister, mais si un chemin d'accès est spécifié, le chemin parent doit exister. Valeur par défaut : Aucun ; ce paramètre est requis.
-LogFile « <chaîne> »	Nom du fichier journal. Une extension est facultative. Le fichier est créé s'il n'existe pas. Si le fichier existe et que le paramètre NoClobber est également spécifié, une erreur est générée ; sinon, le contenu du fichier est remplacé. Valeur par défaut : consultez la section Journalisation et gestion des erreurs
-NoLog	Ne pas générer de sortie de journal. Ceci remplace le paramètre LogFile, s'il est également spécifié. Valeur par défaut : false; une sortie de journal est générée
-NoClobber	Ne pas remplacer un fichier journal spécifié dans le paramètre LogFile. Si le fichier journal n'existe pas, ce paramètre n'a aucun effet. Valeur par défaut : false ; un fichier journal existant est remplacé

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètre	Description
-NoDetails	Ne pas envoyer de rapports détaillés sur l'exécution du script à la console. Valeur par défaut : false ; des rapports détaillés sont envoyés à la console
-SuppressLogo	N'imprimez pas le message « Version de l'outil de migration XenApp 6.x vers XenApp/XenDesktop 7.6 #aaaaMMjj-hhmm# » sur la console. Ce message, qui identifie la version du script, peut être utile lors de la résolution des problèmes ; par conséquent, Citrix vous recommande d'omettre ce paramètre. Valeur par défaut : false ; le message est imprimé sur la console
-IgnoreAdmins	Ne pas exporter les informations de l'administrateur. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : false ; les informations administrateur sont exportées
-IgnoreApps	Ne pas exporter les informations d'application. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : false ; les informations de l'application sont exportées
-IgnoreServers	Ne pas exporter les informations du serveur. Valeur par défaut : false ; les informations du serveur sont exportées
-IgnoreZones	Ne pas exporter les informations de zone. Valeur par défaut : false ; les informations de zone sont exportées.
-IgnoreOthers	Ne pas exporter les informations telles que la journalisation de la configuration, les calculateurs de charge, les stratégies d'équilibrage de charge, les pilotes d'imprimante et les groupes de tâches. Valeur par défaut : false ; d'autres informations sont exportées Remarque : l'objectif du commutateur -IgnoreOthers est de vous autoriser à continuer l'exportation en cas d'erreur qui pourrait affecter les données actuellement utilisées dans le processus d'exportation ou d'importation.
-AppLimit <entier>	Nombre d'applications à exporter. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : toutes les applications sont exportées
-EmbedIconData	Incorporez les données de l'icône d'application dans le même fichier XML que les autres objets. Valeur par défaut : les icônes sont stockées séparément. Consultez la section Configuration requise, préparation et meilleures pratiques pour de plus amples informations
-SkipApps <entier>	Nombre d'applications à ignorer. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : aucune application n'est ignorée

Exemple : l'applet de commande suivante exporte les informations sur la batterie vers le fichier XML nommé MyFarm.xml. L'opération est journalisée sur le fichier MyFarm.log. Un dossier nommé « MyFarm-icons » est créé pour stocker les fichiers de données de l'icône de l'application ; ce dossier se trouve au même emplacement que MyFarm.XML.

```
Export-XAFarm -XmlOutputFile ".\MyFarm.XML" -LogFile ".\MyFarm.Log"
```

Une fois les scripts d'exportation terminés, les fichiers XML spécifiés sur la ligne de commande contiennent la stratégie et les données de la batterie XenApp. Les fichiers de l'icône de l'application contiennent des fichiers de données d'icône, et le fichier journal indique ce qui s'est passé lors de l'exportation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Une vidéo de la marche à suivre pour l'importation est disponible ici.

N'oubliez pas que vous pouvez exécuter une importation d'aperçu (en émettant l'applet de commande Import-Policy ou Import-XAFarm avec le paramètre Preview) et consultez les fichiers journaux avant d'effectuer une importation.

Effectuez les étapes suivantes pour importer des données vers un site XenApp 7.6, en utilisant les fichiers XML générés lors de l'exportation.

1. Ouvrez une session sur le Controller XenApp 7.6 en tant qu'administrateur possédant des permissions en lecture et écriture et des permissions Windows pour exécuter des scripts PowerShell.
2. Si vous n'avez pas décompressé le pack de l'outil de migration XAMigration sur le partage de fichiers réseau, faites-le maintenant. Copiez ImportFMA.zip depuis le partage de fichiers du réseau vers un Controller XenApp 7.6. Décompressez et extrayez ImportFMA.zip sur le contrôleur dans un dossier (par exemple : C:\XAMigration).
3. Copiez les fichiers XML (les fichiers de sortie générés lors de l'exportation) depuis le Controller XenApp 6.x vers le même emplacement sur le Controller XenApp 7.6 sur lequel vous avez extrait les fichiers ImportFMA.zip.
   Si vous choisissez de ne pas incorporer les données de l'icône d'application dans le fichier de sortie XML lorsque vous exécutez l'applet de commande Export-XAFarm, assurez-vous de copier le dossier et les fichiers de données d'icône sur le même emplacement sur le Controller XenApp 7.6 que le fichier XML de sortie contenant les données de l'application et les fichiers ImportFMA.zip extraits.
4. Ouvrez une console PowerShell et définissez le répertoire courant à l'emplacement du script.
   cd C:\XAMigration
5. Vérifiez la stratégie d'exécution de script en exécutant Get-ExecutionPolicy.
6. Définissez la stratégie d'exécution de script sur RemoteSigned au minimum pour autoriser les scripts à être exécutés. Par exemple :
   Set-ExecutionPolicy RemoteSigned
7. Importez les fichiers de définition de module PowerShell ImportPolicy.psd1 et ImportXAFarm.psd1 :
   Import-Module .\ImportPolicy.psd1

   Import-Module .\ImportXAFarm.psd1

   À savoir :
   - Si vous souhaitez uniquement importer des données de stratégie, vous ne pouvez importer que le module et les fichiers de définition de module ImportPolicy.psd1. De même, si vous souhaitez uniquement importer des données de batterie, importez uniquement ImportXAFarm.psd1.
   - L'importation des fichiers de définition de module ajoute également les composants enfichables PowerShell requis.
   - N'importez pas les fichiers de script .psm1.
8. Pour importer des données de stratégie, exécutez l'applet de commande Import-Policy, en spécifiant le fichier XML contenant les données de stratégie exportées.

Paramètre	Description
-XmlInputFile "<chaîne>.xml"	Nom du fichier d'entrée XML ; ce fichier contient des données collectées à partir de l'exécution de l'applet de commande Export-Policy. Doit posséder une extension .xml. Valeur par défaut : Aucun ; ce paramètre est requis.
-XsdFile « <chaîne> »	Nom du fichier XSD. Les scripts d'importation utilisent ce fichier pour valider la syntaxe du fichier d'entrée XML. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : PolicyData.XSD
-LogFile « <chaîne> »	Nom du fichier journal. Si vous avez copié les fichiers journaux d'exportation vers ce serveur, vous pouvez utiliser un autre nom de fichier journal avec l'applet de commande d'importation. Valeur par défaut : consultez la section Journalisation et gestion des erreurs
-NoLog	Ne pas générer de sortie de journal. Ce paramètre remplace le paramètre LogFile, si celui-ci est également spécifié. Valeur par défaut : false; une sortie de journal est générée
-NoClobber	Ne pas remplacer un fichier journal spécifié dans le paramètre LogFile. Si le fichier journal n'existe pas, ce paramètre n'a aucun effet. Valeur par défaut : false ; un fichier journal existant est remplacé
-NoDetails	Ne pas envoyer de rapports détaillés sur l'exécution du script à la console.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètre	Description
	Valeur par défaut : false ; des rapports détaillés sont envoyés à la console
-SuppressLogo	N'imprimez pas le message « Version de l'outil de migration XenApp 6.x vers XenApp/XenDesktop 7.6 #aaaaMMjj-hhmm# » sur la console. Ce message, qui identifie la version du script, peut être utile lors de la résolution des problèmes ; par conséquent, Citrix vous recommande d'omettre ce paramètre. Valeur par défaut : false ; le message est imprimé sur la console
-Preview	Effectuez un aperçu de l'importation : lisez des données à partir du fichier d'entrée XML, mais n'importez pas d'objets dans le site. Le fichier journal et la console indiquent ce qui s'est passé lors de l'importation de l'aperçu. Un aperçu illustre auprès des administrateurs ce qui doit se passer durant une importation réelle. Valeur par défaut : false ; une importation réelle se produit

Exemple : l'applet de commande suivante importe des données de stratégie à partir du fichier XML nommé MyPolicies.xml. L'opération est journalisée dans le fichier appelé MyPolicies.log.

```
Import-Policy -XmlInputFile ".\MyPolicies.XML"  -LogFile ".\MyPolicies.Log"
```

9. Pour importer des applications, exécutez l'applet de commande Import-XAFarm, en spécifiant un fichier journal et le fichier XML contenant les données de la batterie exportées.

Paramètre	Description
-XmlInputFile "<chaîne>.xml"	Nom du fichier d'entrée XML ; ce fichier contient des données collectées à partir de l'exécution de l'applet de commande Export-XAFarm. Doit posséder une extension .xml. Valeur par défaut : Aucun ; ce paramètre est requis.
-XsdFile « <chaîne> »	Nom du fichier XSD. Les scripts d'importation utilisent ce fichier pour valider la syntaxe du fichier d'entrée XML. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : XAFarmData.XSD
-LogFile « <chaîne> »	Nom du fichier journal. Si vous avez copié les fichiers journaux d'exportation vers ce serveur, vous pouvez utiliser un autre nom de fichier journal avec l'applet de commande d'importation. Valeur par défaut : consultez la section Journalisation et gestion des erreurs
-NoLog	Ne pas générer de sortie de journal. Ce paramètre remplace le paramètre LogFile, si celui-ci est également spécifié. Valeur par défaut : false; une sortie de journal est générée
-NoClobber	Ne pas remplacer un fichier journal spécifié dans le paramètre LogFile. Si le fichier journal n'existe pas, ce paramètre n'a aucun effet. Valeur par défaut : false ; un fichier journal existant est remplacé
-NoDetails	Ne pas envoyer de rapports détaillés sur l'exécution du script à la console. Valeur par défaut : false ; des rapports détaillés sont envoyés à la console
-SuppressLogo	N'imprimez pas le message « Version de l'outil de migration XenApp 6.x vers XenApp/XenDesktop 7.6 #aaaaMMjj-hhmm# » sur la console. Ce message, qui identifie la version du script, peut être utile lors de la résolution des problèmes ; par conséquent, Citrix vous recommande d'omettre ce paramètre. Valeur par défaut : false ; le message est imprimé sur la console
-Preview	Effectuez un aperçu de l'importation : lisez des données à partir du fichier d'entrée XML, mais n'importez pas d'objets dans le site. Le fichier journal et la console indiquent ce qui s'est passé lors de l'importation de l'aperçu. Un aperçu illustre auprès des administrateurs ce qui doit se passer durant une importation réelle.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètre	Description
	Valeur par défaut : false ; une importation réelle se produit
-DeliveryGroupName « <chaîne> »	Nom du groupe de mise à disposition pour toutes les applications importées. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : « <nom-batterie-xenapp> -DeliveryGroup »
-MatchFolder « <chaîne> »	Importer uniquement les applications dans des dossiers portant des noms qui correspondent à la chaîne. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : aucune correspondance ne se produit
-NotMatchFolder « <chaîne> »	Importer uniquement ces applications dans des dossiers portant des noms qui ne correspondent pas à celui de la chaîne. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : aucune correspondance ne se produit
-MatchServer « <chaîne> »	Importez uniquement ces applications depuis les serveurs dont les noms correspondent à la chaîne. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation.
-NotMatchServer « <chaîne> »	Importez uniquement ces applications depuis les serveurs dont les noms ne correspondent pas à la chaîne. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : aucune correspondance ne se produit
-MatchWorkerGroup « <chaîne> »	Importer uniquement les applications publiées vers des groupes de tâches avec des noms qui correspondent à la chaîne. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : aucune correspondance ne se produit
-NotMatchWorkerGroup « <chaîne> »	Importer uniquement les applications publiées vers des groupes de tâches avec des noms qui ne correspondent pas à la chaîne. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : aucune correspondance ne se produit
-MatchAccount « <chaîne> »	Importer uniquement les applications publiées vers les comptes d'utilisateur avec des noms qui correspondent à la chaîne. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : aucune correspondance ne se produit
-NotMatchAccount « <chaîne> »	Importer uniquement les applications publiées vers des comptes d'utilisateur avec des noms qui ne correspondent pas à la chaîne. Consultez la section Utilisation avancée pour de plus amples informations sur son utilisation. Valeur par défaut : aucune correspondance ne se produit
-IncludeStreamedApps	Importer des applications de type « StreamedToClientOrServerInstalled ». (Aucune autre des applications streamées n'est importée.) Valeur par défaut : les applications livrées en streaming ne sont pas importées
-IncludeDisabledApps	Importez des applications qui ont été marquées comme désactivées. Valeur par défaut : les applications désactivées ne sont pas importées

Exemple : l'applet de commande suivante importe des applications à partir du fichier XML appelé MyFarm.xml. L'opération est journalisée dans le fichier appelé MyFarm.log.

```
Import-XAFarm -XmlInputFile ".\MyFarm.XML"  -LogFile ".\MyFarm.Log"
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

10. Une fois l'importation terminée, effectuez les tâches de post-migration.

Après l'importation réussie des stratégies XenApp 6.x et des paramètres de batterie dans un site XenApp 7.6, utilisez les instructions suivantes pour vous assurer que les données ont été importées correctement.

- **Stratégies et paramètres de stratégie**
  L'importation des stratégies est fondamentalement une opération de copie, à l'exception des paramètres et des stratégies obsolètes qui ne sont pas importés. La vérification post-migration implique essentiellement la comparaison des deux côtés.

  1. Le fichier journal répertorie toutes les stratégies et tous les paramètres importés et ignorés. Tout d'abord, consultez le fichier journal et identifiez les paramètres et les stratégies qui n'ont pas été importés.
  2. Comparez les stratégies XenApp 6.x avec les stratégies importées dans XenApp 7.6. Les valeurs des paramètres doivent rester les mêmes (à l'exception des paramètres de stratégie obsolètes, comme indiqué dans l'étape suivante).
     - Si vous disposez d'un petit nombre de stratégies, vous pouvez réaliser une comparaison visuelle côte à côte des stratégies affichées dans l'AppCenter de XenApp 6.5 et des stratégies affichées dans Studio de XenApp 7.6.
     - Si vous disposez d'un nombre important de stratégies, une comparaison visuelle peut ne pas être possible. Dans de tels cas, utilisez l'applet de commande d'exportation de la stratégie (Export-Policy) pour exporter les stratégies XenApp 7.6 vers un fichier XML différent, puis utilisez un outil de comparaison de texte (comme windiff) pour comparer les données de ce fichier aux données du fichier XML utilisé lors de l'exportation de la stratégie à partir de XenApp 6.5.
  3. Utilisez les informations dans la section Paramètres de stratégie non importés pour déterminer ce qui peut avoir changé lors de l'importation. Si une stratégie XenApp 6.x contient uniquement des paramètres obsolètes, comme une stratégie totale, elle n'est pas importée. Par exemple, si une stratégie XenApp 6.x ne contient que des paramètres de test HMR, cette stratégie est totalement ignorée, car il n'existe pas de paramètre équivalent pris en charge dans XenApp 7.6.
     Certains paramètres de stratégie XenApp 6.x ne sont plus pris en charge, mais les fonctionnalités équivalentes sont implémentées dans XenApp 7.6. Par exemple, dans XenApp 7.6, vous pouvez configurer un programme de redémarrage pour les machines avec OS de serveur en modifiant un groupe de mise à disposition ; cette fonctionnalité a été précédemment implémentée au travers des paramètres de stratégie.
  4. Vérifiez et confirmez la manière dont les filtres sont appliqués à votre site XenApp 7.6 par rapport à leur utilisation dans XenApp 6.x ; des différences significatives entre la batterie XenApp 6.x et le site XenApp 7.6 pourraient changer l'effet des filtres.

- **Filtres**
  Examinez attentivement les filtres pour chaque stratégie. Des modifications peuvent être nécessaires pour assurer qu'ils fonctionnent toujours dans XenApp 7.6 comme initialement prévu dans XenApp 6.x.

Filtre	Notions importantes
Type d'accès	Le contrôle d'accès doit contenir les mêmes valeurs que les filtres XenApp 6.x originaux et devrait fonctionner sans nécessiter de modifications.
Citrix CloudBridge	Une valeur booléenne simple ; devrait fonctionner sans nécessiter de modifications.
Adresse IP de machine cliente	Affiche les plages d'adresses IP des clients ; chaque plage est soit autorisée soit refusée. Le script d'importation préserve les valeurs, mais elles peuvent nécessiter des modifications si d'autres clients se connectent aux machines de VDA XenApp 7.6.
Nom du client	Identique au filtre d'adresse IP client, le script d'importation préserve les valeurs, mais elles peuvent nécessiter des modifications si d'autres clients se connectent aux machines de VDA XenApp 7.6.
Unité d'organisation	Les valeurs peuvent être conservées, selon que les unités d'organisation peuvent être résolues ou non au moment où elles sont importées. Consultez ce filtre étroitement, particulièrement si les machines XenApp 6.x et XenApp 7.6 résident dans des domaines différents. Si vous ne configurez pas les valeurs de filtre correctement, il se peut que la stratégie soit appliquée à un ensemble d'unités d'organisation incorrect. Les unités d'organisation sont uniquement représentées par des noms, il existe donc un risque qu'un nom d'unité d'organisation soit résolu à une unité d'organisation contenant différents membres de l'unité d'organisation dans le domaine XenApp 6.5. Même si certaines valeurs du filtre de l'unité d'organisation sont conservées, vérifiez les valeurs attentivement.
Utilisateur ou groupe	Les valeurs peuvent être conservées, selon que les comptes peuvent être résolus ou non au moment où ils sont importés. Similaire à des unités d'organisation, les comptes sont résolus en utilisant uniquement les noms, ainsi, si le site XenApp 7.6 dispose d'un domaine avec les mêmes noms de domaine et d'utilisateur, mais qu'ils sont en fait deux domaines et utilisateurs différents, les

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Filtre	comptes résolus peuvent être différents des utilisateurs de domaine XenApp 6.x. Si vous ne consultez et modifiez pas correctement Notions importantes les valeurs de filtre, des applications de stratégies incorrectes peuvent se produire.
Groupe de tâches	Les groupes de tâches ne sont pas pris en charge dans XenApp 7.6. Utilisez le groupe de mise à disposition, le type de groupe de mise à disposition et les filtres de balises, qui sont pris en charge dans XenApp 7.6 (et non pas dans XenApp 6.x). • Groupe de mise à disposition : autorise l'application des stratégies en fonction des groupes de mise à disposition. Chaque entrée de filtre spécifie un groupe de mise à disposition et peut être autorisé ou refusé. • Type de groupe de mise à disposition : autorise l'application des stratégies sur les types de groupes de mise à disposition. Chaque filtre spécifie un type de groupe de mise à disposition qui peut être autorisé ou refusé. • Balise : spécifie l'application de stratégie basée sur les balises créées pour les machines du VDA. Chaque balise peut être autorisée ou refusée.

Pour récapituler, les filtres qui impliquent les modifications de l'utilisateur de domaine requièrent le plus d'attention si la batterie XenApp 6.x et le site XenApp 7.6 se trouvent dans des domaines différents. Étant donné que le script d'importation utilise uniquement des chaînes de noms de domaine et d'utilisateur pour résoudre les utilisateurs dans le nouveau domaine, certains comptes peuvent être résolus et d'autres non. Bien qu'il n'existe qu'un risque infime que des domaines et utilisateurs différents aient le même nom, vous devriez vérifier ces filtres attentivement pour vous assurer qu'ils contiennent des valeurs correctes.

- **Applications**
  Les scripts d'importation d'application n'importent pas simplement des applications ; ils créent également des objets, tels que des groupes de mise à disposition. Si l'importation de l'application implique plusieurs itérations, les hiérarchies de dossier d'application originales peuvent changer de manière significative.
  1. Tout d'abord, consultez les fichiers journaux de migration qui contiennent des informations sur les applications qui ont été importées, les applications qui ont été ignorées et les applets de commande qui ont été utilisées pour créer les applications.
  2. Pour chaque application :
     - Vérifiez visuellement pour vous assurer que les propriétés de base ont été conservées lors de l'importation. Utilisez les informations de la section Mappage des propriétés d'application pour déterminer les propriétés qui ont été importées sans être modifiées, qui n'ont pas été importées ou qui ont été initialisées à l'aide des données d'applications XenApp 6.x.
     - Vérifiez la liste des utilisateurs. Le script d'importation importe automatiquement la liste explicite des utilisateurs dans la liste de visibilité de limite de l'application dans XenApp 7.6. Vérifiez pour vous assurer que la liste reste la même.
  3. Les serveurs d'applications ne sont pas importés. Cela signifie qu'aucune des applications importées n'est accessible à cet instant. Les groupes de mise à disposition qui contiennent ces applications doivent se voir attribuer les catalogues de machines qui contiennent les machines qui possèdent les images exécutables des applications publiées. Pour chaque application :
     - Assurez-vous que le nom de l'exécutable et le répertoire de travail pointent vers un exécutable qui existe sur les machines attribuées au groupe de mise à disposition (via les catalogues de machines).
     - Vérifiez un paramètre de ligne de commande (qui peut être quoi que ce soit, tel qu'un nom de fichier, une variable d'environnement ou un nom d'exécutable). Vérifiez que le paramètre est valide pour toutes les machines des catalogues de machines attribués au groupe de mise à disposition.
- **Fichiers journaux**
  Les fichiers journaux sont les ressources de référence les plus importantes pour une importation et une exportation. C'est pourquoi les fichiers journaux existants ne sont pas remplacés par défaut, et les noms de fichier journal par défaut sont uniques.

  Comme indiqué dans la section « Journalisation et gestion des erreurs », si vous choisissez d'utiliser la couverture de journalisation supplémentaire avec les applets de commande PowerShell Start-Transcript et Stop-Transcript (qui enregistrent tout ce que vous tapez et imprimez dans la console), cette sortie ainsi que le fichier journal, fournit une référence complète de l'activité d'importation et d'exportation.

  À l'aide des horodatages des fichiers journaux, vous pouvez effectuer un diagnostic de certains problèmes. Par exemple, si une exportation ou une importation a été exécutée pour une très longue durée, vous pouvez déterminer si une connexion de base de données défaillante ou la résolution des comptes utilisateur a pris plus de temps.

  Les commandes enregistrées dans les fichiers journaux vous indiquent également la manière dont certains objets sont lus ou créés. Par exemple, pour créer un groupe de mise à disposition, plusieurs commandes sont exécutées non seulement pour créer l'objet de groupe de mise à disposition, mais également d'autres objets, tels que les règles de stratégie d'accès qui permettent l'attribution d'objets d'application au groupe de mise à disposition.

  Le fichier journal peut également être utilisé pour diagnostiquer une exportation ou une importation en échec. En général, les dernières lignes du fichier journal indiquent ce qui a causé l'échec, le message d'erreur d'échec est également enregistré dans le fichier journal. Ensemble avec le fichier XML, le fichier journal peut être utilisé pour déterminer l'objet impliqué dans l'échec.

Après avoir vérifié et effectué le test de la migration, vous pouvez :

1. Effectuez la mise à niveau de vos serveurs de tâches XenApp 6.5 vers des Virtual Delivery Agents (VDA) actuels en exécutant le programme d'installation 7.6 sur le serveur, qui supprime le logiciel XenApp 6.5 puis installe automatiquement un VDA courant. Consultez la section Mettre à niveau une tâche XenApp 6.5 vers un VDA pour OS Windows Server pour des instructions.
   Pour les serveurs de tâches XenApp 6.0, vous devez désinstaller manuellement le logiciel XenApp 6.0 du serveur. Vous pouvez alors utiliser le programme

© 1999-2017 Citrix Systems, Inc. All rights reserved.

d'installation 7.6 pour installer le VDA courant. Vous ne pouvez pas utiliser le programme d'installation 7.6 pour supprimer automatiquement le logiciel XenApp 6.0.

2. Dans Studio, dans le nouveau site XenApp, créez des catalogues de machines (ou modifiez des catalogues existants) pour les tâches mises à niveau.
3. Ajouter les machines mises à niveau du catalogue de machines aux groupes de mise à disposition contenant les applications installées sur ces VDA pour système d'exploitation Windows Server.

Par défaut, l'applet de commande Export-Policy exporte toutes les données de stratégie dans un fichier XML. De même, Export-XAFarm exporte les données de la batterie dans un fichier XML. Vous pouvez utiliser des paramètres de ligne de commande pour contrôler de manière plus avancée quels éléments sont exportés et importés.

- **Exporter les applications partiellement** : si vous possédez un grand nombre d'applications et souhaitez contrôler combien sont exportées dans le fichier XML, utilisez les paramètres suivants :
  - AppLimit : spécifie le nombre d'applications à exporter.
  - SkipApps : spécifie le nombre d'applications à ignorer avant d'exporter les applications suivantes.

  Vous pouvez utiliser ces deux paramètres pour exporter de grandes quantités d'applications par segments gérables. Par exemple, la première fois que vous exécutez Export-XAFarm, vous souhaitez exporter uniquement les 200 premières applications, vous spécifiez ainsi cette valeur dans le paramètre AppLimit.
  Export-XAFarm -XmlOutputFile "Apps1-200.xml" -AppLimit "200"
  La prochaine fois que vous exécutez Export-XAFarm, vous souhaitez exporter les 100 applications suivantes, et vous utilisez le paramètre SkipApps pour ignorer les applications que vous avez déjà exporté (les 200 premières), et le paramètre AppLimit pour exporter les 100 applications suivantes.
  Export-XAFarm -XmlOutputFile "Apps201-300.xml" -AppLimit "100" -SkipApps "200"
- **Ne pas exporter certains objets** : certains objets peuvent être ignorés et n'ont donc pas besoin d'être exportés, plus particulièrement les objets qui ne sont pas importés ; voir Paramètres de stratégie non importés et Mappage des propriétés d'application. Utilisez les paramètres suivants pour empêcher l'exportation des objets inutiles :
  - IgnoreAdmins : ne pas exporter les objets de l'administrateur
  - IgnoreServers : ne pas exporter les objets du serveur
  - IgnoreZones : ne pas exporter les objets de zone
  - IgnoreOthers : ne pas exporter la journalisation de la configuration, le calculateur de charge, la stratégie d'équilibrage de charge, le pilote d'imprimante et les objets des groupes de tâches
  - IgnoreApps : ne pas exporter les applications ; cela vous permet d'exporter d'autres données dans un fichier de sortie XML, puis d'exécuter l'exportation à nouveau pour exporter des applications vers un fichier de sortie XML différent.

  Vous pouvez également utiliser ces paramètres pour résoudre les problèmes qui pourraient provoquer l'échec de l'exportation. Par exemple, si vous possédez un serveur erroné dans une zone, il se peut que la zone d'exportation échoue ; si vous incluez le paramètre IgnoreZones, l'exportation continue avec d'autres objets.

- **Noms de groupe de mise à disposition** : si vous ne souhaitez pas placer toutes vos applications dans un seul groupe de mise à disposition (par exemple, car elles sont accédées par différents utilisateurs et publiées sur différents serveurs), vous pouvez exécuter Import-XAFarm plusieurs fois, en spécifiant différentes applications et un groupe de mise à disposition différent à chaque fois. Bien que vous puissiez utiliser les applets de commande PowerShell pour déplacer les applications d'un groupe de mise à disposition à un autre après la migration, l'importation de manière sélective vers des groupes de mise à disposition uniques peut réduire ou éliminer l'effort de déplacement des applications ultérieurement.
  1. Utilisez l'applet de commande Import-XAFarm avec le paramètre DeliveryGroupName. Le script crée le groupe de mise à disposition spécifié s'il n'existe pas.
  2. Utilisez les paramètres suivants dans les expressions régulières pour filtrer les applications devant être importées dans le groupe de mise à disposition, en fonction du dossier, du groupe de tâches, du compte utilisateur et/ou des noms de serveurs. Il est recommandé d'entourer l'expression régulière de guillemets simples ou doubles. Pour de plus amples informations sur les expressions régulières, consultez la section http://msdn.microsoft.com/fr-fr/library/hs600312(v=vs.110).aspx.
     - MatchWorkerGroup et NotMatchWorkerGroup : par exemple, pour les applications publiées vers des groupes de tâches, l'applet de commande suivante importe des applications dans le groupe de tâches appelé « applications de productivité » vers un groupe de mise à disposition XenApp 7.6 du même nom :
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log –MatchWorkerGroup 'Productivity Apps' –DeliveryGroupName 'Productivity Apps'
     - MatchFolder et NotMatchFolder : par exemple, pour les applications organisées dans des dossiers d'application, l'applet de commande suivante importe des applications dans le dossier nommé « applications de productivité » dans un groupe de mise à disposition XenApp 7.6 du même nom.
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log –MatchFolder 'Productivity Apps' –DeliveryGroupName 'Productivity Apps'
       Par exemple, l'applet de commande suivante importe des applications dans tout dossier dont le nom contient « MS Office Apps » dans le groupe de mise à disposition par défaut.
       Import-XAFarm -XmlInputFile .\THeFarmApps.XML -MatchFolder ".*/MS Office Apps/.*"
     - MatchAccount et NotMatchAccount : par exemple, pour les applications publiées vers des utilisateurs ou des groupes d'utilisateurs Active Directory, l'applet de commande suivante importe des applications publiées vers le groupe d'utilisateurs nommé « groupe Finance » vers un groupe de mise à disposition XenApp 7.6 appelé « Finance ».
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log –MatchAccount 'DOMAIN\\Finance Group' –DeliveryGroupName 'Finance'
     - MatchServer et NotMatchServer : par exemple, pour les applications organisées sur des serveurs, l'applet de commande suivante importe les

© 1999-2017 Citrix Systems, Inc. All rights reserved.

applications associées au serveur qui n'est pas nommé « Courant » dans un groupe de mise à disposition XenApp appelé « Ancienne génération ».
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log -NotMatchServer 'Current' -DeliveryGroupName 'Legacy'

- **Personnalisation** : les programmeurs PowerShell peuvent créer leurs propres outils. Par exemple, vous pouvez utiliser le script d'exportation en tant qu'outil d'inventaire pour le suivi des modifications dans une batterie XenApp 6.x. Vous pouvez également modifier les fichiers XSD (ou créer vos propres fichiers XSD) pour stocker des données supplémentaires ou des données dans des formats différents dans les fichiers XML. Vous pouvez spécifier un fichier XSD non défaut avec chacune des applets de commande d'importation.
  Remarque : bien que vous puissiez modifier les fichiers de script pour répondre à des besoins de migration spécifiques ou avancés, la prise en charge est limitée aux scripts dans leur état non modifié. Le support technique Citrix vous recommande de rétablir les scripts non modifiés pour déterminer le comportement attendu et fournir de l'assistance, le cas échéant.

- Si vous utilisez PowerShell version 2.0 et que vous avez ajouté le composant logiciel enfichable du fournisseur PowerShell de stratégie de groupe Citrix ou le composant logiciel enfichable de l'outil Citrix Common Commands à l'aide de l'applet de commande Add-PSSnapIn, vous pouvez voir le message d'erreur « La référence d'objet n'est pas définie à une instance d'un objet » lorsque vous exécutez les applets de commande d'importation ou d'exportation. Cette erreur n'affecte pas l'exécution du script et peut être ignorée.
- Évitez d'ajouter ou de supprimer le composant logiciel enfichable du fournisseur PowerShell de stratégie de groupe Citrix dans la même session de console dans laquelle les modules de script d'importation et d'exportation sont utilisés, car ces modules de script ajoutent automatiquement le composant logiciel enfichable. Si vous ajoutez ou supprimez le composant logiciel enfichable séparément, il se peut que vous aperceviez les erreurs suivantes :
  - « Un lecteur nommé 'LocalGpo' existe déjà ». Cette erreur s'affiche lorsque le composant logiciel enfichable est ajouté deux fois ; le composant tente de monter le lecteur LocalGpo lorsqu'il est chargé, puis signale l'erreur.
  - « Impossible de trouver un paramètre correspondant au nom 'Controller' ». Cette erreur s'affiche lorsque le composant logiciel enfichable n'a pas été ajouté, mais le script tente de monter le lecteur. Le script ne sait pas que le composant logiciel enfichable a été supprimé. Fermez la console et démarrez une nouvelle session. Dans la nouvelle session, importez les modules de script ; n'ajoutez pas ou ne supprimez pas le composant logiciel enfichable séparément.
- Lors de l'importation des modules, si vous cliquez avec le bouton droit sur un fichier .psd1 et sélectionnez Ouvrir ou Ouvrir avec PowerShell, la fenêtre de la console PowerShell va s'ouvrir et se fermer rapidement jusqu'à ce que vous arrêtiez le processus. Pour éviter cette erreur, saisissez le nom de module du script PowerShell directement dans la fenêtre de la console PowerShell (par exemple, Import-Module.\ExportPolicy.psd1).
- Si vous recevez une erreur de permission lors de l'exécution d'une importation ou exportation, assurez-vous que vous êtes un administrateur XenApp avec permission de lecture des objets (pour l'exportation) ou de lecture et de création des objets (pour l'importation). Vous devez également disposer de suffisamment de permissions Windows pour exécuter des scripts PowerShell.
- Si une exportation échoue, vérifiez que la batterie XenApp 6.x se trouve dans un état d'intégrité normal en exécutant les outils DSMAINT et DSCHECK sur le serveur Controller XenApp 6.x.
- Si vous exécutez un aperçu de l'importation, puis ultérieurement exécutez les applets de commande d'importation pour une migration, mais découvrez que rien n'a été importé, vérifiez que vous avez supprimé le paramètre Preview des applets de commande d'importation.

Les paramètres de stratégie ordinateur et utilisateur suivants ne sont pas importés, car ils ne sont plus pris en charge. Veuillez noter que les stratégies non filtrées ne sont jamais importées. Les fonctionnalités et composants qui prennent en charge ces paramètres ont été remplacés par de nouvelles technologies/nouveaux composants ou elles ne s'appliquent plus à cause de modifications apportées à l'architecture et à la plate-forme.

Paramètres de stratégie Ordinateur non importés

- Type d'accès des connexions
- Niveau du serveur de gestion UC
- Résolution d'adresse DNS
- Nom de batterie
- Mise en cache d'icône complète
- Contrôle de l'intégrité, Tests de contrôle de l'intégrité
- Nom d'hôte du serveur de licences, port du serveur de licences
- Limiter les sessions utilisateur, Limite sur les sessions administrateur
- Nom du calculateur de charge
- Journalisation des événements des limites d'ouverture de session.
- Pourcentage maximal de serveurs possédant un contrôle de l'ouverture de session
- Optimisation de la mémoire, Liste d'exclusion d'applications pour l'optimisation de mémoire, Intervalle d'optimisation de la mémoire, Programme d'optimisation de mémoire : jour du mois, Programme d'optimisation de mémoire : jour de la semaine, Programme d'optimisation de mémoire : heure
- Approbation de client d'applications en mode déconnecté, Journalisation des événements des applications en mode déconnecté, Période de validité de la licence d'applications en mode déconnecté, Utilisateurs d'applications en mode déconnecté
- Demander le mot de passe
- Avertissement de redémarrage personnalisé, Texte d'avertissement de redémarrage personnalisé, Horaire de désactivation des ouvertures de session pour le redémarrage, Fréquence de programmation du redémarrage, Intervalle de randomisation du programme de redémarrage, Date de début de la programmation du redémarrage, Horaire de programmation du redémarrage, Intervalle d'avertissement de redémarrage, Horaire de début de l'avertissement de redémarrage,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Avertissement du redémarrage auprès des utilisateurs, Redémarrages programmés

- Observation *
- Requêtes d'approbation XML (configurées dans StoreFront)
- Filtrage d'adaptateur d'adresse IP virtuelle, Liste de programmes de compatibilité d'adresse IP virtuelle, Compatibilité d'adresse IP virtuelle améliorée, Liste de programmes d'adresses de l'adaptateur de filtre d'adresse IP virtuelle
- Nom de charge de travail
- Édition de produit XenApp, Modèle de produit XenApp
- Port du service XML

* Remplacé(s) par l'Assistance à distance Windows

Paramètres de stratégie Utilisateur non importés

- Connecter automatiquement les ports COM du client, Connecter automatiquement les ports LPT du client
- Redirection de port COM client, Redirection de port LPT client
- Noms des imprimantes clientes
- Limite d'ouvertures de session simultanées
- Entrée depuis des connexions observées *
- Intervalle d'horloge de déconnexion de persistance, Intervalle d'horloge de fin de persistance
- Journaliser les tentatives d'observation *
- Notifier l'utilisateur de connexions observées en attente *
- Intervalle d'horloge de déconnexion de pré-lancement, Intervalle d'horloge de fin de pré-lancement
- Importance de session
- Single Sign-On, Magasin central Single Sign-On
- Utilisateurs qui peuvent observer d'autres utilisateurs, Utilisateurs qui ne peuvent pas observer d'autres utilisateurs *

* Remplacé(s) par l'Assistance à distance Windows

Les types d'application suivants ne sont pas importés.

- Bureaux de serveur
- Contenu
- Applications livrées en streaming (App-V est la nouvelle méthode utilisée pour les applications livrées en streaming)

Le script d'importation des données de la batterie importe uniquement des applications. Les propriétés d'application suivantes sont importées sans modification.

Propriété IMA	Propriété FMA
AddToClientDesktop	ShortcutAddedToDesktop
AddToClientStartMenu	ShortcutAddedToStartMenu
ClientFolder	ClientFolder
CommandLineExecutable	CommandLineExecutable
CpuPriorityLevel	CpuPriorityLevel
Description	Description
DisplayName	PublishedName
Activé	Activé
StartMenuFolder	StartMenuFolder
WaitOnPrinterCreation	WaitForPrinterCreation

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Propriété IMA	Propriété FMA
WorkingDirectory	WorkingDirectory
FolderPath	AdminFolderName

Remarque : IMA et FMA possèdent des restrictions différentes sur la longueur du nom de dossier. Dans IMA, la limite du nom de dossier est de 256 caractères ; la limite FMA est de 64 caractères. Lors de l'importation, les applications possédant un chemin d'accès contenant un nom de dossier de plus de 64 caractères sont ignorées. La limite s'applique uniquement au nom du dossier dans le chemin d'accès au dossier ; le chemin d'accès entier vers le dossier peut être plus long que les limites notées. Pour éviter que des applications soient ignorées lors de l'importation, Citrix vous recommande de vérifier la longueur du nom de dossier d'application et de la raccourcir, si nécessaire, avant l'exportation.

Les propriétés d'applications suivantes sont initialisées ou non initialisées par défaut, ou définies sur des valeurs fournies dans les données XenApp 6.x :

Propriété FMA	Valeur
Nom	Initialisé pour le nom de chemin complet, qui contient les propriétés IMA FolderPath et DisplayName, mais sans la chaîne de préfixe « Applications\ »
ApplicationType	HostedOnDesktop
CommandLineArguments	Initialisé à l'aide des arguments de ligne de commande XenApp 6.x
IconFromClient	Non initialisée ; la valeur par défaut est false.
IconUid	Initialisé à un objet d'icône créé à l'aide de données d'icônes XenApp 6.x
SecureCmdLineArgumentsEnabled	Non initialisée ; la valeur par défaut est true.
UserFilterEnabled	Non initialisée ; la valeur par défaut est false.
UUID	En lecture seule, affecté par le Controller
Visible	Non initialisée ; la valeur par défaut est true.

Les propriétés d'application suivantes sont partiellement migrées :

Propriété IMA	Commentaires
Types de fichiers	Seuls les types de fichiers qui existent sur le nouveau site XenApp sont migrés. Les types de fichiers qui n'existent pas sur le nouveau site sont ignorés. Les types de fichiers sont importés uniquement après que les types de fichier du nouveau site aient été mis à jour.
IconData	Les nouveaux objets d'icône sont créés si les données d'icône ont été fournies pour les applications exportées.
Comptes	Les comptes d'utilisateur d'une application sont partagés entre la liste des utilisateurs du groupe de mise à disposition et l'application. Les utilisateurs explicites sont utilisés pour initialiser la liste des utilisateurs de l'application. En outre, le compte « Utilisateurs de domaine » pour le domaine des comptes utilisateur est ajouté à la liste des utilisateurs du groupe de mise à disposition.

Les propriétés de XenApp 6.x suivantes ne sont pas importées :

Propriété IMA	Commentaires
ApplicationType	Ignorée.
HideWhenDisabled	Ignorée.
AccessSessionConditions	Remplacée par les stratégies d'accès du groupe de mise à disposition.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Propriété IMA	Commentaires
AccessSessionConditionsEnabled	Remplacée par les stratégies d'accès du groupe de mise à disposition.
ConnectionsThroughAccessGatewayAllowed	Remplacée par les stratégies d'accès du groupe de mise à disposition.
OtherConnectionsAllowed	Remplacée par les stratégies d'accès du groupe de mise à disposition.
AlternateProfiles	FMA ne prend pas en charge les applications livrées en streaming.
OfflineAccessAllowed	FMA ne prend pas en charge les applications livrées en streaming.
ProfileLocation	FMA ne prend pas en charge les applications livrées en streaming.
ProfileProgramArguments	FMA ne prend pas en charge les applications livrées en streaming.
ProfileProgramName	FMA ne prend pas en charge les applications livrées en streaming.
RunAsLeastPrivilegedUser	FMA ne prend pas en charge les applications livrées en streaming.
AnonymousConnectionsAllowed	FMA utilise une technologie différente pour prendre en charge les connexions (anonymes) non authentifiées.
ApplicationId, SequenceNumber	Données uniques à IMA
AudioType	FMA ne prend pas en charge les options de connexion clientes avancées.
EncryptionLevel	SecureICA est activé/désactivé dans les groupes de mise à disposition.
EncryptionRequired	SecureICA est activé/désactivé dans les groupes de mise à disposition.
SslConnectionEnabled	FMA utilise une implémentation TLS différente.
ContentAddress	FMA ne prend pas en charge le contenu publié.
ColorDepth	FMA ne prend pas en charge les apparences de fenêtre avancées.
MaximizedOnStartup	FMA ne prend pas en charge les apparences de fenêtre avancées.
TitleBarHidden	FMA ne prend pas en charge les apparences de fenêtre avancées.
WindowsType	FMA ne prend pas en charge les apparences de fenêtre avancées.
InstanceLimit	FMA ne prend pas en charge les limites d'application.
MultipleInstancesPerUserAllowed	FMA ne prend pas en charge les limites d'application.
LoadBalancingApplicationCheckEnabled	FMA utilise une technologie différente pour prendre en charge l'équilibrage de charge.
PreLaunch	FMA utilise une technologie différente pour la prise en charge du pré-lancement de session.
CachingOption	FMA utilise une technologie différente pour la prise en charge du pré-lancement de session.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Propriété FMA	Commentaires
ServerName	FMA utilise une technologie différente.
WorkerGroupNames	FMA ne prend pas en charge les groupes de tâches.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Migrer XenDesktop 4

Jul 07, 2016

Vous pouvez transférer des données et des paramètres d'une batterie XenDesktop 4 vers un site XenDesktop 7.x à l'aide de l'outil de migration, qui est disponible dans le dossier Support > Tools > MigrationTool sur le support d'installation XenDesktop. L'outil comprend :

- L'outil d'exportation, XdExport, qui exporte des données de la batterie XenDesktop 4 vers un fichier XML (nom par défaut : XdSettings.xml). Le schéma du fichier XML réside dans le fichier XdFarm.xsd.
- L'outil d'importation, XdImport, qui importe des données en exécutant le script PowerShell Import-XdSettings.ps1.

Pour utiliser l'outil de migration, les deux déploiements doivent avoir la même version d'hyperviseur (par exemple, XenServer 6.2) et un environnement Active Directory.

Vous ne pouvez pas utiliser cet outil pour effectuer la migration de XenApp, et vous ne pouvez pas migrer XenDesktop 4 vers XenApp.

Conseil : vous pouvez effectuer la mise à niveau de XenDesktop 5 (ou version ultérieure) vers la version de XenDesktop actuelle ; consultez la rubrique Mettre un déploiement à niveau.

Toutes les données et tous les paramètres ne sont pas exportés. Les éléments de configuration suivants ne sont pas migrés car ils sont exportés mais non importés :

- Administrateurs
- Paramètres d'administration déléguée
- Dossiers de groupes de bureaux
- Configuration du système de licences
- Clés de registre

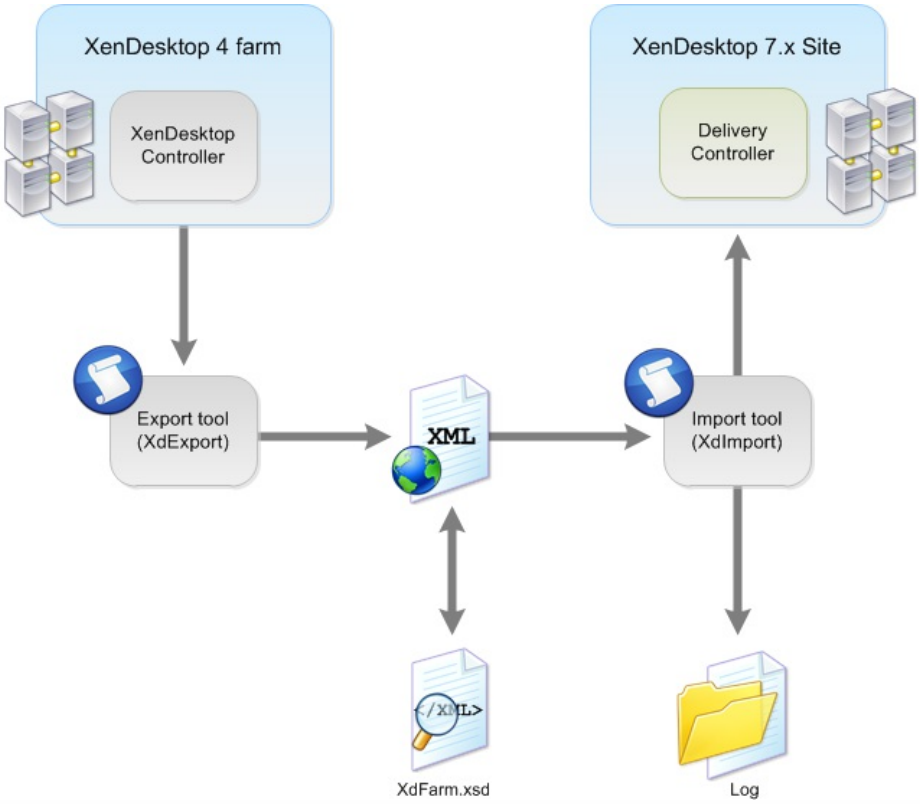
Ces cas d'utilisation ne sont pas directement pris en charge dans la migration :

- Fusion des paramètres de stratégies ou des paramètres du groupe de bureaux ou d'hébergement.
- Fusion de bureaux privés dans des groupes de mise à disposition aléatoires.
- Ajustement des paramètres de composants existants au travers des outils de migration.

Pour de plus amples informations, consultez la section Qu'est-ce qui est et qui n'est pas migré.

La figure suivante présente le processus de migration.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Le processus de migration suivant cette séquence :

1. Dans la console Studio sur le Controller XenDesktop 4, activez le mode maintenance pour toutes les machines à exporter.
2. Exportez les données et paramètres depuis votre batterie XenDesktop 4 vers un fichier XML à l'aide de l'outil d'exportation ; voir la section Exporter à partir d'une batterie XenDesktop 4.
3. Modifiez le fichier XML afin qu'il ne contienne que les données et paramètres à importer dans votre nouveau site XenDesktop ; voir la section Modification du fichier XML de l'outil de migration.
4. Importez les données et paramètres depuis le fichier XML vers votre nouveau site XenDesktop à l'aide de XdImport ; voir la section Importer les données de XenDesktop 4.
5. Pour apporter des modifications supplémentaires, répétez les étapes 3 et 4. Après avoir effectué les modifications, il se peut que vous vouliez importer des bureaux supplémentaires dans des groupes de mise à disposition existants. Pour ce faire, utilisez le paramètre Mergedesktops lors de l'importation.
6. Effectuez les tâches de post-migration ; voir la section Tâches d'après migration.

Effectuez les opérations suivantes avant de commencer la migration :

- Veillez à bien comprendre quelles données peuvent être exportées et importées, et de quelle manière cela s'applique à votre propre déploiement. Voir la section Qu'est-ce qui est et qui n'est pas migré.
- Citrix vous recommande de sauvegarder manuellement la base de données du site, de façon à ce que vous puissiez la restaurer en cas de problème.
- Installez les composants XenDesktop 7.x et créez un site, y compris la base de données.
- Pour faire migrer depuis XenDesktop 4, tous les VDA doivent se trouver au niveau de XenDesktop 5.x afin qu'ils soient compatibles avec à la fois les Controller XenDesktop 4 et XenDesktop 7.x. Une fois que l'infrastructure des Controller exécute complètement XenDesktop 7.x, les VDA Windows 7 peuvent être mis à niveau vers XenDesktop 7.x. Pour de plus amples informations, consultez la section Exemples de migration.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Exporter à partir d'une batterie XenDesktop 4

Jul 07, 2016

L'outil d'exportation XdExport extrait les données d'une batterie XenDesktop 4 unique et génère un fichier XML à partir des représentations des valeurs de données.

Le schéma du fichier XML réside dans le fichier nommé XdFarm.xsd, qui est inclus dans le téléchargement de l'outil de migration : XdExport.zip et XdImport.zip.

Exécutez XdExport sur un XenDesktop 4 Controller dans la batterie à partir de laquelle vous souhaitez exporter les données. Le kit de développement PowerShell XenDesktop 4 doit être installé sur cette machine. Vous devez posséder les permissions suivantes pour exporter les données :

- L'identité utilisateur d'au moins un administrateur Citrix en lecture seule de la batterie.
- L'accès en écriture au registre.

Bien que ce ne soit pas recommandé, vous pouvez exécuter l'outil pendant que XenDesktop Controller est en cours d'utilisation (par exemple, lorsque les utilisateurs sont connectés à VDA).

Citrix recommande ce qui suit :

- Le XenDesktop 4 Controller sur lequel vous exécutez l'outil doit être mis à jour avec les corrections publiques.
- N'apportez pas de modifications à la configuration du site alors que l'exportation est en cours d'exécution (par exemple, durant la suppression de groupes de bureaux).

1. Téléchargez XdExport.zip et extrayez les fichiers vers XenDesktop 4 Controller.
2. À l'invite de commande, exécutez XdExport.exe avec les paramètres facultatifs suivants :

Paramètre	Description
-Verbose	Génère des messages contenant des informations de progression détaillées.
-FilePath <chemin>	Indique l'emplacement du fichier XML vers lequel les données de la batterie sont exportées. Par défaut = .\XdSettings.xml
-Overwrite	Remplace les fichiers existants dans l'emplacement spécifié dans -FilePath. Si vous omettez ce paramètre et qu'un fichier de résultat existe déjà, l'outil s'arrête et affiche le message d'erreur suivant : Error: File already exists. Specify -Overwrite to allow the file to be overwritten. "
-? ou -help	Affiche du texte décrivant les paramètres et s'arrête sans exporter les données.

3. Si l'outil s'exécute correctement, le message Done s'affiche. Le fichier XDSettings.xml réside dans l'emplacement spécifié dans le paramètre FilePath. En cas d'échec de l'outil, un message d'erreur s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Modification du fichier XML de l'outil de migration

Jul 07, 2016

Avant d'importer des données sur un site XenDesktop 7.x, vérifiez et modifiez le contenu du fichier XML généré par l'outil d'exportation (XdExport), particulièrement si vous migrez en plusieurs étapes et importez certains utilisateurs, groupes de mise à disposition et stratégies avant d'autres.

Utilisez un éditeur de texte quelconque ou un éditeur XML spécifique tel que le Bloc-notes Microsoft XML Notepad pour afficher ou modifier le contenu du fichier.

Certains éléments du contenu XML doivent être présents pour que le fichier XML soit accepté par l'outil d'importation (XdImport).

Le schéma XML requis est défini dans le fichier XdFarm.xsd, fourni lors du téléchargement de l'outil de migration. Lors de l'utilisation de ce fichier :

- Un attribut minOccurs avec une valeur de 1 ou plus indique que des éléments spécifiques doivent être présents si l'élément parent est présent.
- Si le fichier XML fourni à l'outil d'importation n'est pas valide, l'outil s'arrête et un message d'erreur s'affiche, vous permettant de repérer à quel endroit du fichier se situe le problème.

Pour importer un sous-ensemble de bureaux et de groupes de mise à disposition, modifiez le contenu de l'élément DesktopGroups. L'élément DesktopGroups peut contenir plusieurs éléments DesktopGroup et chaque élément DesktopGroup inclut un élément Desktops qui peut à son tour contenir de nombreux éléments Desktop.

Vous ne devez pas supprimer l'élément DesktopGroups, mais vous pouvez supprimer tous les éléments DesktopGroup qu'il contient et le laisser vide. De même, dans chaque élément DesktopGroup, l'élément Desktops doit être présent, sans nécessairement contenir des éléments Desktop.

Supprimez les éléments Desktop ou DesktopGroup pour éviter l'importation de certaines machines ou de groupes de mise à disposition entiers. Par exemple, le fichier XML contient :

… … … … … … …

Dans cet exemple, vos modifications empêchent l'importation du Groupe1. Seule la Machine3 du Groupe2 sera importée :

… … …

Dans XenDesktop 4, les groupes de bureaux peuvent être organisés dans des dossiers, les groupes de bureaux du même nom peuvent apparaître dans des dossiers différents, et le nom du groupe de bureau interne est le nom qui s'affiche aux utilisateurs. Dans cette version, les groupes de mise à disposition ne peuvent pas être placés dans des dossiers, et chaque groupe de mise à disposition doivent posséder un nom interne unique et le nom qui s'affiche aux utilisateurs peut être différent du nom interne. Pour prendre en charge ces différences, vous devrez peut-être renommer les groupes de bureaux.

Par exemple, votre batterie XenDesktop 4 peut contenir deux groupes de bureaux différents qui apparaissent sous le nom « Mon bureau » pour deux utilisateurs différents et vous pouvez utiliser des dossiers de groupes de bureaux pour atteindre ce résultat. Si ces groupes de mise à disposition doivent rester distincts dans le site XenDesktop 7.x, vous devez modifier le nom des groupes de bureaux dans le fichier XML pour les rendre uniques.

Si un groupe de mise à disposition du site XenDesktop 7.x porte le même nom qu'un groupe de bureaux importé et si les

© 1999-2017 Citrix Systems, Inc. All rights reserved.

groupes de mise à disposition doivent rester séparés dans le site XenDesktop 7.x, vous devez modifier le nom du groupe de bureaux XenDesktop 4 dans le fichier XML afin qu'il reste unique dans le site. Si le groupe de bureaux à importer est réellement le même que le groupe de mise à disposition XenDesktop 7.x, et que les machines dans le fichier XML doivent être fusionnées avec le groupe de bureaux existant, vous ne devez pas renommer le groupe de bureaux ; au lieu de cela, spécifiez le paramètre -MergeDesktops dans l'outil d'importation. Par exemple, si le fichier XML contient :

… \Sales … \Finance

Supprimez les noms en double comme suit :

… \Sales … \Finance

Vous pouvez supprimer des stratégies du fichier XML et spécifier des noms uniques pour éviter leur duplication. La fusion de stratégies n'est pas prise en charge.

- Lorsque vous importez des données de stratégie, soit la totalité des stratégies est importée, soit, en cas de problème, aucune donnée n'est importée.
- L'importation d'un grand nombre de stratégies avec de nombreux paramètres peut prendre plusieurs heures.
- Si vous importez des stratégies par lots, leurs priorités d'origine peuvent être affectées. Lorsque vous importez des stratégies, elles conservent leurs priorités relatives, mais elles acquièrent une priorité supérieure à celle des stratégies déjà dans le site. Par exemple, si vous importez quatre stratégies avec des priorités de 1 à 4 en deux lots, vous devez importer en premier les stratégies de priorité 3 et 4, car une priorité supérieure sera automatiquement accordée au deuxième lot.

Pour importer un sous-ensemble de stratégies dans le site XenDesktop 7.x, modifiez le contenu de l'élément Policies. L'élément Policies peut contenir plusieurs éléments Policy. Vous ne devez pas supprimer l'élément Policies, mais vous pouvez supprimer tous les éléments Policy qu'il contient et le laisser vide. Supprimez tous les éléments Policy pour éviter l'importation de certaines stratégies de la batterie XenDesktop 4. Par exemple, si le fichier XML contient :

… …

Pour éviter par exemple que des stratégies XenDesktop 4 n'entrent en conflit avec des stratégies déjà configurées dans le site XenDesktop 7.x, modifiez le fichier pour supprimer les éléments individuels Policy, comme suit :

Vous pouvez également modifier le fichier de façon à importer la stratégie sous un autre nom, comme indiqué ci-après :

… …

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Importer les données de XenDesktop 4

Jul 07, 2016

L'outil d'importation, XdImport, lit les paramètres de XenDesktop 4 contenus dans le fichier XML généré par l'outil d'exportation, XdExport, et les applique à un site XenDesktop 7.x existant. L'outil d'importation utilise le script PowerShell Import-XdSettings.ps1.

Pour appliquer uniquement un sous-ensemble de données exportées, modifiez le fichier XML avant d'exécuter l'outil d'importation. Par exemple, vous pouvez supprimer des groupes de bureaux et des stratégies qui ne sont pas nécessaires dans votre déploiement XenDesktop 7.x. L'outil d'importation s'exécute correctement si vous laissez des éléments entiers vides. Par exemple, vous pouvez supprimer tous les groupes de bureaux sans engendrer de problèmes. L'outil valide toujours le fichier XML avant d'importer des données.

Exécutez XdImport sur n'importe quelle machine sur laquelle les SDK XenDesktop 7.x sont installés. Vous devez disposer de l'identité d'administrateur XenDesktop complet pour exécuter l'outil.

Avant d'importer, vérifiez que vous avez configuré un site XenDesktop 7.x, y compris sa base de données. Citrix vous recommande d'effectuer l'importation vers XenDesktop 7.x avant toute configuration d'un site général ou évaluation par les utilisateurs. Fusionnez les configurations uniquement lorsque le site n'est pas utilisé.

1. Créez un site XenDesktop 7.x.
2. Téléchargez XdImport.zip et extrayez les fichiers vers la machine sur laquelle vous allez utiliser l'outil.
3. Dans une session PowerShell, exécutez Import-XdSettings.ps1. avec les paramètres suivants :

Paramètre	Description
-HypervisorConnectionCredentials	(Obligatoire). Table de hachage PowerShell qui met en correspondance les adresses d'hyperviseurs avec les instances PSCredential nécessaires à la création de Entrez les informations d'identification de l'hyperviseur auquel la batterie XenDesktop 4 se connecte. Pour un hyperviseur unique, créez l'argument comme indiqué ci-après : $credential = Get-Credential $mappings = @{"http://" =$credential} .\Import-XdSettings.ps1 -FilePath. \XdSettings.xml -HypervisorConnectionCredentials $mappi L'adresse spécifiée dans la table de hachage doit correspondre exactement à l'adresse contenue dans le fichier XML. Par exemple, avec un hyperviseur XenServer et VMware, créez l'argument suivant : $Xencredential = Get-Credential $VMWcredential = Get-Credential $mappings = @{"http://" = $Xencredential;"http:///SDK" = $VMWcredential} .\Import-XdSetting
-FilePath <chemin>	La valeur de est requise. L'emplacement du fichier XML à partir duquel les données de la batterie doivent être importées.
-AdminAddress	Nom d'un Controller sur le site XenDesktop 7.x. Valeur par défaut = XA
-MergeDesktops	Ajoute les bureaux définis dans le fichier XML pour les groupes de mise à disposition dans le site XenDesktop 7.x qui ont le même nom que les groupes décrits d ajoutés. Si vous omettez ce paramètre, aucun contenu n'est ajouté aux groupes de bureaux existants dans le site XenDesktop 7.x.
-SkipMachinePolicy	Le script ne crée pas de stratégie machine contenant les paramètres de niveau du site. Si vous ne fournissez pas ce paramètre et s'il existe déjà une stratégie n
-WhatIf	Effectue une série de tests pour déterminer ce qui serait modifié ou ajouté au site XenDesktop 7.x. L'inclusion de ce paramètre envoie les informations au fichi
-LogFilePath <chemin>	Chemin complet du fichier journal. Le fichier journal contient une description de toutes les écritures effectuées au niveau du site XenDesktop 7.x. Par défaut =
-? ou -help	Affiche des informations sur les paramètres et quitte sans exporter les données.

Si le fichier XML contient des données de stratégie, soit toutes les stratégies sont importées, soit, en cas de problème, aucune donnée de stratégie n'est importée. L'importation d'un grand nombre de stratégies avec de nombreux paramètres peut prendre plusieurs heures.

Lorsque le script prend fin, le message Done apparaît. Une fois que vous avez importé les données à partir du fichier XML, vous pouvez soit exécuter d'autres opérations d'importation ou d'exportation soit, si toutes les données pertinentes ont été importées, effectuer les tâches post-migration.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Tâches d'après migration

Jul 07, 2016

Après l'importation des données à partir d'une batterie XenDesktop 4 vers un site XenDesktop 7.x, effectuez les tâches suivantes avant d'utiliser le nouveau site à des fins de production :

- Mettez à niveau les Virtual Delivery Agents (VDA). Bien que cela ne soit pas requis, Citrix vous recommande de mettre à niveau les VDA avant la mise à niveau des Controller, de Studio ou de Director.
  - Pour Windows Vista et Windows XP, mettez à niveau vers XenDesktop 5. 6 Feature Pack 1 Virtual Desktop Agent.
  - Pour Windows 7, mettez à niveau vers XenDesktop 7.x Virtual Delivery Agent.
- Créez les administrateurs nécessaires pour le site XenDesktop 7.x.
- Mettez à jour les machines utilisateur : Citrix vous recommande de mettre à niveau les machines utilisateur avec la dernière version de Citrix Receiver de façon à bénéficier des correctifs et du support relatif aux nouvelles fonctionnalités.
- Modifiez les bureaux importés pour utiliser la découverte du Controller de registre, et faites-les pointer vers les Controller XenDesktop 7.x en utilisant l'une des méthodes suivantes :
  - Modifiez manuellement le registre pour supprimer l'entrée de registre GUID de l'unité d'organisation (UO) obsolète et ajouter une entrée de registre ListOfDDCs.
  - Configurez une stratégie de machine pour distribuer la liste des Controller aux bureaux à l'aide de la stratégie Active Directory GPMC.msc. Vous ne pouvez pas utiliser Studio pour configurer ce paramètre.

  La découverte de Controller basée sur le registre est activée par défaut pour XenDesktop 7.x, mais la découverte basée sur Active Directory est néanmoins disponible.

- Si vous le souhaitez, vous pouvez mettre en œuvre les paramètres de clé de registre suivants décrits dans les meilleures pratiques pour l'enregistrement basé sur le registre dans XenDesktop dans l'article CTX133384 :
  - Heartbeatperiodms
  - Preparesessionconnectiontimeoutsec
  - Maxworkers
  - Disableactivesessionreconnect
  - Controllersgroupguid

  Si vous n'effectuez pas cette action, les paramètres par défaut XenDesktop 7.x pour ces clés sont utilisés.

- Désactivez le mode de maintenance pour les machines importées si elles se trouvaient dans ce mode dans XenDesktop 4 avant la génération du fichier XML.
- Vérifiez que les paramètres XenDesktop 7.x sont corrects, notamment si vous avez modifié le fichier XML PortICAConfig dans XenDesktop 4.
- Vérifiez tous les composants migrés pour vous assurer que la migration a réussi.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Exemples de migration

Jul 07, 2016

Dans cet exemple, une batterie XenDesktop 4 est en cours d'utilisation. La batterie XenDesktop 4 possède 50 groupes de bureaux, et chaque groupe contient une moyenne de 100 bureaux. Les bureaux XenDesktop 4 sont fournis par le biais de Provisioning Services (PVS), et les machines sont en cours d'exécution sur des hyperviseurs VMware ESX. Le logiciel VDA installé sur toutes les VM est le logiciel VDA XenDesktop 4.

Étapes de migration

1. Mettez à niveau tous les VDA XenDesktop 4 vers le logiciel VDA XenDesktop 5.6 Feature Pack 1. Ceci permet aux VDA de s'enregistrer avec le Controller XenDesktop 4 et XenDesktop 7 Delivery Controller.
2. Assurez-vous que tous les utilisateurs ferment leur session sur la batterie XenDesktop 4.
3. Assurez-vous que toutes les machines se trouvent en mode maintenance.
4. Exécutez l'outil d'exportation (XdExport) sur la batterie XenDesktop 4.
5. Installez des composants XenDesktop 7.
    1. Utilisez Studio pour créer un site de mode de production complet.
    2. Si Provisioning Services fait partie de votre déploiement, vous devez mettre à niveau le serveur et les agents Provisioning Services.
    3. Mettez à niveau le serveur de licences et les licences associées.
6. Décompressez l'outil d'importation (XdImport) dans un répertoire local sur XenDesktop 7 Controller.
7. Copiez le fichier XML (XdSettings.xml) généré à l'étape 4 par l'outil d'exportation sur le répertoire local.
8. À partir du volet de la console PowerShell du nœud racine de Studio sur le site XenDesktop 7, démarrez une session Powershell.
9. Exécutez l'outil d'importation (XdImport) en transmettant les informations d'identification des hyperviseurs associés, et le chemin d'accès au fichier XML.
10. Recréez manuellement les paramètres d'administrateur à partir du nœud Administrateur dans le volet de navigation Studio ; voir Délégation de l'administration pour plus de détails.
11. Modifiez les bureaux importés pour utiliser la découverte de Controller basée sur le registre, et faites-les pointer vers le nouveau Controller XenDesktop 7.
12. Pour les VDA exécutés sous Windows 7, Citrix vous recommande de mettre à niveau les VDA pour utiliser le VDA XenDesktop 7 pour OS de bureau Windows, ce qui permet d'accéder à toutes les nouvelles fonctionnalités.
    Après avoir effectué la mise à niveau des VDA vers XenDesktop 7 pour les machines d'un catalogue ou d'un groupe de mise à disposition, mettez à niveau le catalogue et les groupes de mise à disposition.
13. Désactivez le mode de maintenance pour les groupes de mise à disposition.
14. Configurez StoreFront pour fournir les bureaux anciennement fournis par le biais de l'interface Web. Pour plus d'informations, consultez la documentation StoreFront.

Dans cet exemple, la migration se produit dans un certain nombre d'étapes, chaque étape de la migration d'un sous-ensemble des bureaux restants. Une batterie XenDesktop 4 est en cours d'utilisation, et un site XenDesktop 7.1 a déjà été créé et est en cours d'utilisation. La batterie XenDesktop 4 possède 50 groupes de bureaux, et chaque groupe contient une moyenne de 100 bureaux. Les bureaux XenDesktop 4 sont fournis via Provisioning Services, et les machines sont en cours d'exécution sur des hyperviseurs Citrix XenServer. Le logiciel VDA installé sur toutes les VM est le logiciel VDA XenDesktop 4.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Étapes de migration

1. Exécutez l'outil d'exportation sur la batterie XenDesktop 4.
    1. Décompressez l'outil d'exportation (XdExport) sur l'une des machines Desktop Delivery Controller de la batterie.
    2. En tant qu'administrateur Citrix, exécutez l'outil d'exportation sans paramètres.
2. Copiez et modifiez le fichier XML résultant afin qu'il contienne uniquement les groupes et les bureaux que vous souhaitez migrer.
3. Dans la batterie XenDesktop 4, assurez-vous que tous les utilisateurs des bureaux à migrer ont fermé leur session et activer le mode de maintenance pour tous les bureaux qui doivent être migrés.
4. Décompressez l'outil d'importation (XdImport) dans un répertoire local sur le Delivery Controller XenDesktop 7.1.
5. Copiez le fichier XML modifié dans le répertoire local.
6. À partir du volet de la console PowerShell du nœud racine de Studio sur le site XenDesktop 7,1, démarrez une session Powershell.
7. Exécutez l'outil d'importation (XdImport) en transmettant les informations d'identification des hyperviseurs associés, et le chemin d'accès au fichier XML.
8. Recréez manuellement les paramètres d'administrateur à partir du nœud Administrateur dans le volet de navigation Studio ; voir Délégation de l'administration pour plus de détails.
9. Modifiez les bureaux importés pour utiliser la découverte de Controller basée sur le registre, et faites-les pointer vers le nouveau Controller XenDesktop 7,1.
10. Mettez tous les VDA à niveau vers le logiciel VDA approprié.
11. Après avoir effectué la mise à niveau des VDA vers XenDesktop 7 pour les machines d'un catalogue ou d'un groupe de mise à disposition, mettez à niveau le catalogue et les groupes de mise à disposition.
12. Désactivez le mode de maintenance pour les groupes de mise à disposition.
13. Configurez StoreFront pour fournir les bureaux anciennement fournis par le biais de l'interface Web. Pour plus d'informations, consultez la documentation StoreFront.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Qu'est-ce qui est et qui n'est pas migré

Jul 07, 2016

Bien qu'il ne soit pas exhaustif, ce tableau décrit ce qu'il advient des données les plus significatives lors de la migration vers cette version. Sauf spécification contraire, le type de données est importé.

Type de données	Remarques
Groupes de bureaux	Groupes de bureaux deviennent des groupes de mise à disposition dans cette version. Les icônes des groupes de bureaux ne sont pas exportées. SecureIcaRequired est défini sur True si DefaultEncryptionLevel dans XenDesktop 4 n'est pas Basic. Si un groupe de bureaux dans la batterie XenDesktop 4 a le même nom qu'un groupe de mise à disposition dans le site XenDesktop 7.x, vous pouvez ajouter des bureaux appartenant au groupe XenDesktop 4 vers un groupe de mise à disposition du même nom dans le site cible. Pour cela, spécifiez le paramètre MergeDesktops lorsque vous exécutez l'outil d'importation. Les paramètres du groupe de mise à disposition XenDesktop 7.x ne sont pas remplacés par les paramètres du groupe XenDesktop 4. Si ce paramètre n'est pas spécifié et si un groupe porte le même nom que celui défini dans le fichier XML, l'outil affiche une erreur et s'arrête sans importer les données.
Bureaux	Vous ne pouvez pas ajouter de bureaux privés à un groupe de mise à disposition aléatoire. Les bureaux aléatoires ne peuvent pas être ajoutée à un groupe de mise à disposition statique.
Machines	Les machines sont importées dans quatre catalogues de machines. Les catalogues de machines suivants sont automatiquement créés dans le site XenDesktop 7.x par l'outil d'importation : • Machines existantes aléatoires importées (pour les VM groupées) • Machines existantes statiques importées (pour les VM attribuées) • Machines physiques aléatoires importées (pour les PC ou blade) • Machines physiques statiques importées (pour les PC privés ou blade) Toute importation de machines ultérieure utilise les quatre mêmes catalogues de machine.
Pools de gestion de regroupement	Inclut les pools multi-regroupement et les paramètres de regroupement inactif, y compris la programmation. • PeakBuffersizePercent est défini sur 10 % par défaut. • OffPeakBufferSizePercent est défini sur 10 % par défaut. • Les jours non sélectionnés dans le paramètre Business days sur XenDesktop 4 sont importés dans le cadre du schéma Weekend dans cette version. • Les heures d'action HostingXD4 sont arrondies à la minute la plus proche. • Les heures de début sont arrondies à l'heure la plus proche. • Les heures de fin sont arrondies à l'heure la plus proche.
Paramètres de	Les paramètres de batterie suivants sont importés en tant que stratégie de machine :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Type de données	Remarques
batterie	• IcaKeepAlive • AutoClientReconnect • SessionReliability Le paramètre permettant d'activer le lecteur Flash n'est pas importé.
Stratégies	Certaines données de stratégies sont importées. Les filtres, les paramètres et les imprimantes sont importés en tant que stratégies utilisateur. Pour plus d'informations sur l'importation et l'exportation des stratégies utilisateur, veuillez consulter le second tableau fourni dans ce document. • De nouvelles règles de stratégies d'accès sont créées à partir des paramètres de groupes XenDesktop 4. • Lorsque des stratégies sont importées, leur priorité relative est maintenue. Cependant, elles sont toujours ajoutées avec une priorité supérieure à celle des stratégies déjà dans le site XenDesktop 7.x. • La fusion des stratégies n'est pas prise en charge. Il n'existe pas d'option pour importer des stratégies dans Active Directory. Celles-ci sont toujours stockées dans le site.
Attribution d'utilisateurs	
Paramètres d'hyperviseurs	Ce paramètre est obligatoire avec l'outil XdImport. Les adresses d'hyperviseur sont exportées, mais les informations d'identification requises pour y accéder ne le sont pas. Pour créer des connexions d'hyperviseur dans le site XenDesktop 7.x, vous devez extraire les adresses du fichier XML et créer une table de hachage Powershell qui les met en correspondance avec les instances d'informations d'identification adéquates. Vous spécifiez ensuite cette table dans le paramètre HypervisorConnectionCredentials de l'outil d'importation. Pour plus d'informations, veuillez consulter la section Importer les données de XenDesktop 4. Aucun paramètre de fusion ou de mise à jour des paramètres d'hyperviseur pour les groupes de bureaux et les connexions d'hyperviseur existants n'est pris en charge.
Administrateurs	(Non importé.) Aucune donnée d'administrateur, y compris sur les administrateurs délégués, n'est importée. Vous devez créer de nouveaux administrateurs pour votre site XenDesktop 7.x.
Configuration du système de licences	(Non importé.) Inclut des informations telles que le nom du serveur de licences et l'édition. Les fichiers de licences ne sont pas exportés.
Dossiers de groupes de bureaux	(Non importé.) Cette version ne gère pas les dossiers de groupes de bureaux. S'il existe des doublons des noms de groupes de bureaux (car des dossiers différents dans la batterie XenDesktop 4 contiennent des groupes avec le même nom), si vous ne modifiez pas les noms dans le fichier XML, l'outil d'importation s'arrête.
Clés de registre	(Non importé). Pour plus d'informations sur la mise en œuvre de clés de registre, veuillez consulter la

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Type de données	Remarques
	section Tâches d'après migration.

Le tableau suivant présente la manière dont les données de stratégie utilisateur sont exportées et importées.

Catégorie et paramètre XenDesktop 4	Fichier XML	Catégorie et paramètre XenDesktop 7.x
Bande passante\Effets visuels\Limites de session Canaux virtuels OEM	ClientOEMVCBandwidth	Non importé
Machines clientes\Ressources\Autre Désactiver les canaux virtuels OEM	DisableOEMVirtualChannels	Non importé
Espace de travail utilisateur\Fuseaux horaires Ne pas utiliser l'heure locale des clients	DoNotUseClientLocalTime	Non importé
Sécurité\Cryptage Cryptage SecureICA	ClientSecurityRequirement	Non importé
Bande passante\SpeedScreen Accélération de l'affichage des images à l'aide d'une compression avec perte	Paramètres LossyCompression	ICA\Affichage visuel\Images fixes Niveau de compression avec perte Valeur de seuil de compression avec perte Compression intensive ICA\Affichage visuel\Images en mouvement Niveau de compression progressif Valeur de seuil de compression progressif
Bande passante\Effets visuels Désactiver le papier peint du bureau	TurnOffWallpaper	ICA\IU de bureau Papier peint du bureau

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Catégorie et paramètre XenDesktop 4	Fichier XML	Catégorie et paramètre XenDesktop 7.x
Bande passante\Effets visuels	TurnOffMenuWindowAnimation	ICA\IU de bureau
Animation de menu		Animation de menu
Bande passante\Effets visuels Masquer le contenu des fenêtres pendant leur déplacement	DoNotShowWindowContentsWhileDragging	ICA\IU de bureau Afficher le contenu de la fenêtre lors d'un cliquer déplacer
Bande passante\Effets visuels\Limites de session Audio	ClientAudioBandwidth__AllowedBandWidth	ICA\Bande passante Limite de bande passante de redirection audio
Bande passante\Effets visuels\Limites de session Presse-papiers	ClientClipboardBandwidth__AllowedBandWidth	ICA\Bande passante Limite de bande passante de redirection du Presse-papiers
Bande passante\Effets visuels\Limites de session Ports COM	ClientComBandwidth__AllowedBandWidth	ICA\Bande passante Limite de bande passante pour la redirection du port COM Non importé dans XenDesktop 7.0 à 7.8
Bande passante\Effets visuels\Limites de session Lecteurs	ClientDriveBandwidth__AllowedBandWidth	ICA\Bande passante Limite de bande passante de redirection de fichier
Bande passante\Effets visuels\Limites de session Ports LPT	ClientLptBandwidth__AllowedBandWidth	ICA\Bande passante Limite de bande passante pour la redirection du port LPT Non importé dans XenDesktop 7.0 à 7.8
Bande passante\Effets visuels\Limites de session	OverallBandwidth__AllowedBandWidth	ICA\Bande passante

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Catégorie et paramètre XenDesktop 4	Fichier XML	Catégorie et paramètre XenDesktop 7.x
Globale pour session		Limite de bande passante globale de session
Bande passante\Effets visuels\Limites de session Imprimante	LimitPrinterBandWidth__AllowedBandWidth	ICA\Bande passante Limite de bande passante de redirection d'imprimante
Machines clientes\Ressources\Audio Micros	ClientAudioMicrophone__TurnOn	ICA\Audio Redirection du microphone client
Machines clientes\Ressources\Audio Qualité sonore	ClientAudioQuality__Quality	ICA\Audio Qualité audio
Machines clientes\Ressources\Audio Désactiver les haut-parleurs	DisableClientAudioMapping	ICA\Audio Redirection audio du client
Machines clientes\Ressources\Lecteurs Connexion	ConnectClientDriveAtLogon__TurnOn	ICA\Redirection de fichiers Connecter automatiquement les lecteurs
Machines clientes\Ressources\Lecteurs Désactiver les lecteurs de disquette	DisableClientDriveMapping__DisableFloppyDrive	ICA\Redirection de fichiers Lecteurs de disquette clients
Machines clientes\Ressources\Lecteurs Désactiver les disques durs	DisableClientDriveMapping__DisableHardDrive	ICA\Redirection de fichiers Lecteurs fixes clients
Machines clientes\Ressources\Lecteurs Désactiver les lecteurs de CD-ROM	DisableClientDriveMapping__DisableCdrom	ICA\Redirection de fichiers Lecteurs optiques clients
Machines clientes\Ressources\Lecteurs Désactiver les lecteurs distants	DisableClientDriveMapping__DisableRemote	ICA\Redirection de fichiers Lecteurs réseau clients
Machines clientes\Ressources\Lecteurs Désactiver les lecteurs USB	DisableClientDriveMapping__DisableUSB	ICA\Redirection de fichiers Lecteurs amovibles clients

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Catégorie et paramètre XenDesktop 4	Fichier XML	Catégorie et paramètre XenDesktop 7.x
Machines clientes\Ressources\Lecteurs\Optimiser Écritures asynchrones	CDMAsyncWrites	ICA\Redirection de fichiers Utiliser les écritures asynchrones
Machines clientes\Ressources\Autre Désactiver le mappage du Presse-papiers	DisableClientClipboardMapping	ICA Redirection de Presse-papiers client
Machines clientes\Ressources\Ports Désactiver les ports COM	DisableClientCOMPortMapping	ICA\Redirection de ports Redirection de port COM client Non importé dans XenDesktop 7.0 à 7.8
Machines clientes\Ressources\Ports Désactiver les ports LPT	DisableClientLPTPortMapping	ICA\Redirection de ports Redirection de port LPT client Non importé dans XenDesktop 7.0 à 7.8
Machines clientes\Ressources\USB USB	RemoteUSBDevices__DisableRemoteUSBDevices	ICA\Périphériques USB Redirection de périphérique USB client
Impression\Imprimantes clientes Création automatique	ConnectClientPrinterAtLogon__Flag	ICA\Impression\Imprimantes clientes Créer automatiquement les imprimantes clientes
Impression\Imprimantes clientes Imprimantes clientes d'ancienne génération	LegacyClientPrinters__TurnOn	ICA\Impression\Imprimantes clientes Noms des imprimantes clientes
Impression\Imprimantes clientes Rétention des propriétés d'imprimante	ModifiedPrinterProperties__WriteMethod	ICA\Impression\Imprimantes clientes Rétention des propriétés

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Catégorie et paramètre XenDesktop 4	Fichier XML	Catégorie et paramètre XenDesktop 7.x
Impression\Imprimantes clientes Routage des tâches d'impression	ClientPrintingForNetworkPrinter__TurnOn	d'imprimante ICA\Impression\Imprimantes clientes Connexions directes aux serveurs d'impression
Impression\Imprimantes clientes Désactiver le mappage des imprimantes clientes	DisableClientPrinterMapping	ICA\Impression Redirection d'imprimante cliente
Impression\Pilotes Installation automatique du pilote natif de l'imprimante	PrintDriverAutoInstall__TurnOn	ICA\Impression\Pilotes Installation automatique de pilotes d'imprimante fournis par défaut
Impression\Pilotes Pilote universel	ClientPrintDriverToUse	ICA\Impression\Pilotes Utilisation du pilote d'impression universelle
Impression\Imprimantes de session Imprimantes de session	NetworkPrinters	ICA\Impression Imprimantes de session
Impression\Imprimantes de session Choisir l'imprimante par défaut de la machine cliente	DefaultToMainClientPrinter__NetworkDefault DefaultToMainClientPrinter__TurnOn	ICA\Impression Imprimante par défaut

Tous les composants XenDesktop 4 ne sont pas pris en charge dans cette version. Les éléments suivants ne sont pas migrés :

- **Virtual Delivery Agent** : avant qu'un Delivery Controller XenDesktop 7.x puisse gérer des bureaux virtuels dans XenDesktop 4, vous devez mettre à niveau les VDA vers une version minimale de XenDesktop 5.x.
- **Controller** : vous devez déployer de nouveaux serveurs Controller. Vous ne pouvez pas mettre à niveau un Controller XenDesktop 4 vers un site XenDesktop 7.x. Les sites XenDesktop 7.x ne peuvent pas être associés à une batterie XenDesktop 4, et les Controller XenDesktop 4 ne peuvent pas être associés à un site XenDesktop 7.x. En outre, chaque version est différente de la configuration requise sur le serveur ; XenDesktop 4 nécessite Windows Server 2003 et XenDesktop 7.x requiert une version plus récente de Windows Server.
- **Interface Web** : Citrix recommande d'utiliser StoreFront avec XenDesktop 7.x. Consultez la documentation de StoreFront pour l'installation et les détails d'installation. Lorsque le programme d'installation XenDesktop détecte l'Interface Web, il installe StoreFront, mais ne supprime pas l'Interface Web.
- **Configuration de l'Unité d'organisation Active Directory (UO)** : le partage d'une unité d'organisation (UO) entre deux batteries ou deux sites, ou entre une batterie et un site n'est pas pris en charge. Si vous prévoyez de configurer le nouveau

© 1999-2017 Citrix Systems, Inc. All rights reserved.

site de façon à utiliser la découverte de contrôleurs Active Directory plutôt que la découverte de contrôleurs de registre par défaut, vous devez créer une nouvelle unité d'organisation pour prendre en charge cette fonctionnalité.

- **Fichier XML PortICAConfig** : si vous avez modifié les paramètres par défaut de ce fichier, vous devrez probablement les configurer en fonction du nouveau site via des objets de stratégie de groupe.
- **Paramètres de journalisation de la configuration fournis par le biais de XenDesktop 4 Service Pack 1**.
- **Données relatives à Provisioning Services**.
- **Applications** :
- **Liste de contrôleurs**.
- **NetScaler Gateway**.
- **Paramètres de limitation du journal des événements**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sécuriser

Jul 07, 2016

XenApp et XenDesktop offre une solution sécurisée de par sa conception qui vous permet de configurer votre environnement selon vos besoins en termes de sécurité.

Un problème de sécurité souvent rencontré en informatique concerne la perte ou le vol des données des travailleurs mobiles. En hébergeant les applications et les bureaux, XenApp et XenDesktop sépare les données sensibles et la propriété intellectuelle des machines de point de terminaison de manière sécurisée en conservant les données dans un centre de données. Lorsque des stratégies sont activées pour autoriser le transfert des données, toutes les données sont cryptées.

Les centres de données XenDesktop et XenApp facilitent également les réponses aux incidents avec un service de contrôle et de gestion centralisé. Director permet au département informatique de surveiller et d'analyser les données qui sont accédées sur le réseau et Studio permet au département informatique d'appliquer des correctifs logiciels et de remédier à la plupart des vulnérabilités dans le centre de données au lieu de résoudre les problèmes localement sur chaque machine utilisateur.

XenApp et XenDesktop simplifie également les audits et assure la conformité à la règlementation car les enquêteurs peuvent utiliser une piste d'audit centralisée pour déterminer les personnes qui ont accès aux applications et aux données. Director collecte des données d'historique concernant les mises à jour du système et l'utilisation des données utilisateur en accédant à la journalisation de la configuration et l'API OData.

L'administration déléguée vous permet de configurer des rôles administrateur pour contrôler l'accès à XenDesktop et XenApp à un niveau plus précis. Ceci permet une plus grande souplesse dans votre organisation pour fournir à certains administrateurs un accès complet aux tâches, opérations et étendues alors que d'autres administrateurs ont un accès limité.

XenApp et XenDesktop fournit un contrôle plus précis aux administrateurs sur les utilisateurs en appliquant des stratégies à différents niveaux du réseau (à partir du niveau local de l'unité d'organisation). Ce contrôle des stratégies détermine si un utilisateur, une machine ou des groupes d'utilisateurs et de périphériques peuvent se connecter, imprimer, copier/coller, ou mapper les lecteurs locaux, ce qui peut réduire les problèmes de sécurité causés par des travailleurs tiers intérimaires. Les administrateurs peuvent également utiliser la fonctionnalité Desktop Lock, les utilisateurs finaux peuvent alors uniquement utiliser le bureau virtuel tout en empêchant tout accès au système d'exploitation local de la machine utilisateur.

Les administrateurs peuvent améliorer la sécurité de XenApp ou XenDesktop en configurant le site pour utiliser le protocole de sécurité TLS (Transport Layer Security) du Controller ou entre utilisateurs finaux et Virtual Delivery Agents (VDA). Le protocole peut également être activé sur un site pour fournir l'authentification de serveur, le cryptage du flux de données et le contrôle de l'intégrité des messages pour une connexion TCP/IP.

XenApp et XenDesktop fournit également l'authentification multi-facteurs pour Windows ou une application spécifique. L'authentification multi-facteurs peut également être utilisée pour gérer toutes les ressources mises à disposition par XenApp et XenDesktop. Ces méthodes comprennent :

- Jetons
- Cartes à puce
- RADIUS
- Kerberos
- Biométrie

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenDesktop peut être intégré à plusieurs des solutions de sécurité tierces, allant de la gestion de l'identité à un logiciel antivirus. Une liste des produits pris en charge peut être obtenue à l'adresse http://www.citrix.com/ready.

Les versions Premium de XenApp et XenDesktop sont certifiées pour la norme des critères communs. Pour obtenir une liste de ces normes, accédez à http://www.commoncriteriaportal.org/cc/.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Considérations de sécurité et meilleures pratiques

Aug 22, 2016

Ce document décrit ce qui suit :

- Bonnes pratiques en matière de sécurité lors de l'utilisation de cette version, et les différences en termes de sécurité entre XenDesktop et un environnement informatique classique
- Gérer les comptes utilisateur
- Gérer les privilèges utilisateur
- Gérer les droits d'ouverture de session
- Configurer les droits des utilisateurs
- Configurer les paramètres du service
- Scénarios de déploiement et leurs implications en termes de sécurité.
- Considérations de sécurité Remote PC Access

Votre entreprise peut être tenue de satisfaire à certaines normes de sécurité pour remplir ses obligations réglementaires. Ce document ne traite pas de ce sujet, car ces normes de sécurité évoluent continuellement. Pour obtenir les informations les plus récentes sur les normes de sécurité et les produits Citrix, consultez http://www.citrix.com/security/.

Bonnes pratiques en matière de sécurité

Maintenez à jour toutes les machines de votre environnement avec des correctifs de sécurité. L'un des avantages est de pouvoir utiliser des clients légers comme terminaux, ce qui vous simplifie énormément la tâche.

Protégez toutes les machines de votre environnement avec un logiciel antivirus.

Envisagez d'utiliser un logiciel anti-malware spécifique à la plate-forme tel que la Trousse à outils EMET de Microsoft pour les machines Windows. Certaines autorités recommandent d'utiliser la dernière version de EMET prise en charge par Microsoft dans leurs environnements qui sont soumis à des réglementations strictes. D'après Microsoft, EMET peut ne pas être compatible avec certains logiciels, par conséquent il doit faire l'objet de tests rigoureux avec vos applications avant le déploiement dans un environnement de production. XenApp et XenDesktop ont été testés avec EMET 5.5 dans sa configuration par défaut. Pour le moment, nous ne recommandons pas d'utiliser EMET sur une machine sur laquelle est installé un Virtual Delivery Agent (VDA).

Protégez toutes les machines de votre environnement avec des pare-feu de périmètre, y compris aux limites des enclaves.

Si vous faites migrer un environnement classique vers cette version, il peut être nécessaire de repositionner un pare-feu de périmètre existant ou d'en ajouter de nouveaux. Supposons, par exemple, qu'un pare-feu de périmètre soit positionné entre un client classique et un serveur de base de données dans le centre de données. Avec cette version, ce pare-feu de périmètre doit être positionné de façon telle que le bureau virtuel et la machine utilisateur se trouvent d'un côté du pare-feu, et les serveurs de bases de données et les Delivery Controller du centre de données de l'autre côté. Envisagez par conséquent de créer une enclave dans votre centre de données qui contiendra les serveurs de bases de données et les Controller. Il peut également être recommandé de mettre en place une protection entre la machine utilisateur et le bureau virtuel.

Toutes les machines de votre environnement devraient être protégées par un pare-feu personnel. Lorsque vous installez des composants principaux et des VDA (Virtual Delivery Agents), vous pouvez choisir que les ports requis pour le composant de la

© 1999-2017 Citrix Systems, Inc. All rights reserved.

fonctionnalité de communication soient ouverts automatiquement si le service Pare-feu Windows est détecté (même si le pare-feu n'est pas activé). Vous pouvez également configurer ces ports des pare-feu manuellement. Si vous utilisez un autre pare-feu, vous devez configurer le pare-feu manuellement.

Remarque : les ports TCP 1494 et 2598 sont utilisés par les protocoles ICA et CGP. Ils sont donc susceptibles d'être ouverts afin que les utilisateurs se trouvant hors du centre de données puissent y accéder. Citrix vous recommande de ne pas utiliser ces ports à d'autres fins pour éviter tout risque d'attaque des interfaces d'administration. Les ports 1494 et 2598 sont officiellement enregistrés auprès de l'IANA (Internet Assigned Number Authority, voir http://www.iana.org/).

Toutes les communications réseau doivent être correctement sécurisées et cryptées pour répondre à votre stratégie de sécurité. Vous pouvez sécuriser toutes les communications entre vos ordinateurs Microsoft Windows avec IPSec ; reportez-vous à la documentation de votre système d'exploitation pour plus d'informations à ce sujet. De plus, les communications entre les machines utilisateurs et les bureaux sont sécurisées via Citrix SecureICA, configuré par défaut sur un cryptage 128 bits. Vous pouvez configurer SecureICA lorsque vous créez ou mettez à jour un groupe de mise à disposition.

Appliquez les recommandations Windows pour la gestion de comptes. Ne créez pas de compte sur un modèle ou une image avant sa duplication par Machine Creation Services ou Provisioning Services. Ne planifiez pas de tâches à l'aide de comptes de domaine privilégiés stockés. Ne créez pas manuellement de comptes de machines Active Directory partagés. Ces recommandations permettront d'éviter une attaque de machines par l'obtention des mots de passe de compte persistants locaux et leur utilisation pour se connecter à des images partagées MCS et PVS appartenant à d'autres utilisateurs.

Gérer les comptes utilisateur

Si l'option permettant d'installer des composants de publication App-V est sélectionnée lors de l'installation d'un Virtual Delivery Agent (VDA), ou si cette fonctionnalité est ajoutée ultérieurement, le compte administratif local CtxAppVCOMAdmin est ajouté au VDA. Si vous utilisez la fonctionnalité de publication App-V, ne modifiez pas ce compte. Si vous n'avez pas besoin d'utiliser la fonctionnalité de publication App-V, ne la sélectionnez pas lors de l'installation. Si vous décidez plus tard de ne pas utiliser la fonctionnalité de publication App-V, vous pouvez supprimer ou désactiver ce compte.

Gérer les privilèges utilisateur

Accordez aux utilisateurs uniquement les droits qui leur sont nécessaires. Les privilèges Microsoft Windows sont toujours appliqués aux bureaux de la manière habituelle : vous configurez les privilèges à l'aide de l'attribution des droits utilisateur et de l'appartenance aux groupes via la stratégie de groupe. L'un des avantages de cette version est qu'il est possible d'octroyer à un utilisateur des droits d'administration sur un bureau sans lui accorder le contrôle physique de l'ordinateur qui héberge ce bureau.

Veuillez noter ce qui suit lors de la planification des privilèges des bureaux :

- Par défaut, lorsque des utilisateurs non privilégiés se connectent à un bureau, ils voient le fuseau horaire du système exécutant le bureau au lieu de celui de leur propre machine utilisateur. Pour savoir comment autoriser les utilisateurs à voir leur heure locale lorsqu'ils utilisent des bureaux, veuillez consulter l'article Gérer les groupes de mise à disposition.
- Un utilisateur qui est administrateur d'un bureau dispose d'un contrôle total sur ce dernier. S'il s'agit d'un bureau regroupé et non d'un bureau dédié, tous les autres utilisateurs de ce bureau, y compris les utilisateurs futurs, doivent lui faire confiance. Tous les utilisateurs doivent être conscients que ce genre de situation peut représenter un risque potentiel permanent pour la sécurité de leurs données. Cette remarque ne s'applique pas aux bureaux dédiés, qui n'ont qu'un seul

© 1999-2017 Citrix Systems, Inc. All rights reserved.

utilisateur ; celui-ci ne doit être l'administrateur d'aucun autre bureau.
- Un utilisateur qui est administrateur d'un bureau peut généralement installer des logiciels sur ce bureau, y compris des logiciels potentiellement malveillants. Il a aussi la possibilité de surveiller ou de contrôler le trafic sur tout réseau connecté au bureau.

Gérer les droits d'ouverture de session

Accordez aux utilisateurs uniquement les droits d'ouverture de session qui leur sont nécessaires. À l'instar des privilèges Microsoft Windows, les droits d'ouverture de session sont toujours appliqués aux bureaux de la manière habituelle : vous configurez les droits d'ouverture de session à l'aide de l'attribution des droits utilisateur et de l'appartenance aux groupes via la stratégie de groupe.

Les droits d'ouverture de session Windows sont les suivants : ouverture de session locale, ouverture de session via les Services Bureau à distance, ouverture de session sur le réseau, ouverture de session en tant que traitement par lots et ouverture de session en tant que service.

Selon Microsoft, le droit d'ouverture de session « Autoriser l'ouverture de session par les services Bureau à distance » est accordé par défaut au groupe Utilisateurs du Bureau à distance (excepté sur les contrôleurs de domaine).

La stratégie de sécurité de votre organisation peut stipuler explicitement que ce groupe soit supprimé de ce droit d'ouverture de session. Considérez l'approche suivante :

- Le Virtual Delivery Agent (VDA) de l'OS de serveur utilise les Services Bureau à distance Microsoft. Vous pouvez configurer le groupe Utilisateurs du Bureau à distance en tant que groupe restreint, et contrôler l'appartenance au groupe via des stratégies de groupe Active Directory. Référez-vous à la documentation Microsoft pour plus d'informations.
- Pour les autres composants de XenApp et XenDesktop, y compris le VDA pour OS de bureau, le groupe Utilisateurs du Bureau à distance n'est pas requis. Étant donné que le groupe Utilisateurs du Bureau à distance ne nécessite pas le droit d'ouverture de session « Autoriser l'ouverture de session au travers des services Bureau à distance » pour ces composants, vous pouvez le supprimer. Autres tâches :
  - Si vous administrez ces ordinateurs via les Services Bureau à distance, assurez-vous que tous les administrateurs sont déjà membres du groupe Administrateurs.
  - Si vous n'administrez pas ces ordinateurs via les Services Bureau à distance, vous pouvez désactiver les Services Bureau à distance sur ces ordinateurs.

Bien qu'il soit possible d'ajouter des utilisateurs et des groupes au droit d'ouverture de session « Interdire l'ouverture de session par les services Bureau à distance », l'interdiction de droits d'ouverture de session n'est généralement pas recommandée. Référez-vous à la documentation Microsoft pour plus d'informations.

Configurer les droits des utilisateurs

L'installation de Delivery Controller crée les services Windows suivants :

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService Microsoft) : gère les comptes d'ordinateurs Active Directory pour les machines virtuelles.
- Citrix Analytics (NT SERVICE\CitrixAnalytics) : collecte des informations sur l'utilisation de la configuration du site, si cette

© 1999-2017 Citrix Systems, Inc. All rights reserved.

collecte a été approuvée par l'administrateur du site. Ces informations sont ensuite envoyées à Citrix pour aider à améliorer le produit.

- Citrix App Library (NT SERVICE\CitrixAppLibrary) : prend en charge la gestion et le provisioning d'AppDisks, l'intégration d'AppDNA et la gestion d'App-V.
- Citrix Broker Service (NT SERVICE\CitrixBrokerService) : sélectionne les applications ou bureaux virtuels qui sont disponibles pour les utilisateurs.
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging) : enregistre toutes les modifications de configuration et d'autres modifications apportées par les administrateurs du site.
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService) : référentiel à l'échelle du site pour la configuration partagée.
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin) : gère les autorisations accordées aux administrateurs.
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest) : gère les auto-tests des autres services Delivery Controller.
- Citrix Host Service (NT SERVICE\CitrixHostService) : stocke des informations sur les infrastructures d'hyperviseur utilisées dans un déploiement XenApp ou XenDesktop, et offre également des fonctionnalités utilisées par la console pour énumérer les ressources dans un pool d'hyperviseurs.
- Citrix Machine Creation Service (NT SERVICE\CitrixMachineCreationService) : orchestre la création de machines virtuelles de bureau.
- Citrix Monitor Service (NT SERVICE\CitrixMonitor) : collecte des métriques pour XenApp ou XenDesktop, stocke les données d'historique, et fournit une interface de requête pour la résolution des problèmes et les outils de reporting.
- Citrix Storefront Service (NT SERVICE\CitrixStorefront) : prend en charge la gestion de StoreFront. (Ne fait pas partie du composant StoreFront).
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService) : prend en charge les opérations d'administration privilégiée de StoreFront. (Ne fait pas partie du composant StoreFront).

L'installation de Delivery Controller crée également les services Windows suivants. Ces services sont également créés lorsqu'ils sont installés avec d'autres composants Citrix :

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc) : prend en charge la collecte d'informations de diagnostic destinées au support technique de Citrix.
- Service de télémétrie Citrix (NT SERVICE\CitrixTelemetryService) : collecte des informations de diagnostic à des fins d'analyse par Citrix, de façon à ce que les résultats de l'analyse et les recommandations puissent être consultés par les administrateurs pour diagnostiquer les problèmes avec le site.

L'installation de Delivery Controller crée également les services Windows suivants. Ils ne sont pas actualisés et sont donc désactivés. N'activez pas :

- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService)
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService)

À l'exception du service Citrix Storefront Privileged Administration Service, le droit d'ouverture de session Ouvrir une session en tant que service et les privilèges Ajuster les quotas de mémoire pour un processus, Générer des audits de sécurité et Remplacer un jeton de niveau processus sont accordés à ces services. Vous n'avez pas besoin de changer ces droits d'utilisateur. Ces privilèges ne sont pas utilisés par le Delivery Controller et sont automatiquement désactivés.

Configurer les paramètres du service

© 1999-2017 Citrix Systems, Inc. All rights reserved.

À l'exception du service Citrix StoreFront Privileged Administration Service et du Service de télémétrie Citrix, les services Windows Delivery Controller répertoriés ci-dessus dans la section Configurer les droits des utilisateurs sont configurés pour ouvrir une session sous l'identité NETWORK SERVICE. Ne modifiez pas ces paramètres de service.

Le service Citrix StoreFront Privileged Administration Service est configuré pour ouvrir une session sous l'identité Système local (NT AUTHORITY\SYSTEM). Ceci est requis pour les opérations de Delivery Controller et de StoreFront qui ne sont normalement pas disponibles pour les services (y compris la création de sites IIS Microsoft). Ne modifiez pas ses paramètres de service.

Le Service de télémétrie Citrix est configuré pour ouvrir une session sous sa propre identité spécifique au service.

Vous pouvez désactiver le Service de télémétrie Citrix. Outre ce service, et les services qui sont déjà désactivés, ne désactivez aucun des autres services Windows Delivery Controller.

Configurer les paramètres de registre

Il n'est plus nécessaire d'activer la création de noms de fichiers et de dossiers au format 8.3 sur le système de fichiers du VDA. La clé de registre **NtfsDisable8dot3NameCreation** peut être configurée pour désactiver la création de noms de fichiers et de dossiers au format 8.3. Vous pouvez également configurer ce comportement à l'aide de la commande **fsutil.exe behavior set disable8dot3**.

Implications en termes de sécurité du scénario de déploiement

Votre environnement utilisateur peut se composer soit de machines utilisateur non gérées par votre entreprise et totalement sous le contrôle de l'utilisateur, soit de machines utilisateur gérées et administrées par votre entreprise. Les considérations de sécurité pour ces deux environnements sont généralement différentes.

Machines utilisateur gérées

Les machines utilisateur gérées font l'objet d'un contrôle administratif ; elles sont soit sous votre propre contrôle, soit sous celui d'une autre organisation à laquelle vous faites confiance. Vous pouvez configurer et fournir directement aux utilisateurs les machines utilisateur ; vous pouvez également fournir des terminaux sur lesquels un seul bureau s'exécute en mode plein écran seulement. Suivez les bonnes pratiques générales en matière de sécurité décrites ci-dessous pour toutes les machines utilisateur gérées. Cette version présente l'avantage de n'exiger qu'un minimum de logiciels sur une machine utilisateur.

Une machine utilisateur gérée peut être configurée pour être utilisée en mode plein écran seulement ou en mode fenêtre.

- Mode plein écran uniquement : les utilisateurs ouvrent une session sur celle-ci à partir de l'écran d'ouverture de session Windows habituel. Les mêmes informations d'identification de l'utilisateur sont alors utilisées pour ouvrir automatiquement une session sur cette version.
- Les utilisateurs voient leur bureau dans une fenêtre : les utilisateurs doivent d'abord ouvrir une session sur la machine utilisateur, puis sur cette version via le site Web fourni avec le produit.

Machines utilisateur non gérées

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Les machines utilisateur qui ne sont pas gérées et administrées par une organisation de confiance ne peuvent pas être considérées comme des machines sous contrôle administratif. Vous pouvez, par exemple, autoriser les utilisateurs à se procurer et à configurer leurs propres machines, mais ceux-ci peuvent ne pas respecter les bonnes pratiques générales en matière de sécurité décrites ci-dessus. Cette version présente l'avantage de mettre, en toute sécurité, des bureaux à la disposition des machines utilisateur non gérées. Ces machines doivent tout de même disposer d'une protection antivirus de base capable d'arrêter les enregistreurs de frappes et les attaques similaires axées sur la saisie.

Considérations sur le stockage de données

Lorsque vous utilisez cette version, vous pouvez empêcher les utilisateurs de stocker des données sur les machines utilisateur qui sont sous leur contrôle physique. Toutefois, vous devez encore envisager les conséquences de l'enregistrement, par les utilisateurs, de données sur leurs bureaux. Enregistrer des données sur les bureaux n'est pas une bonne pratique ; celles-ci doivent être stockées sur des serveurs de fichiers, des serveurs de bases de données ou d'autres référentiels où elles feront l'objet d'une protection appropriée.

Votre environnement peut être composé de différents types de bureaux, tels que des bureaux regroupés ou dédiés. Les utilisateurs ne doivent jamais stocker de données sur des bureaux partagés, tels que les bureaux regroupés. S'ils stockent des données sur des bureaux dédiés, celles-ci doivent être supprimées si les bureaux sont ensuite mis à la disposition d'autres utilisateurs.

Environnements à versions mixtes

Les environnements à versions mixtes sont inévitables lors de certaines mises à niveau. Suivez les recommandations et réduisez la durée pendant laquelle les composants Citrix de versions différentes co-existent. Dans les environnements à versions mixtes, la stratégie de sécurité, par exemple, peut ne pas être appliquée de façon uniforme.

Remarque: ce comportement est caractéristique d'autres produits logiciels ; l'utilisation d'une version antérieure d'Active Directory n'applique que partiellement la stratégie de groupe avec les versions ultérieures de Windows.

Le scénario suivant décrit un problème de sécurité qui peut se produire dans un environnement Citrix à versions mixtes spécifique. Lorsque Citrix Receiver 1.7 est utilisé pour se connecter à un bureau virtuel exécutant le VDA dans XenApp et XenDesktop 7.6 Feature Pack 2, le paramètre de stratégie **Autoriser le transfert de fichiers entre les bureaux et le client** est activé dans le site, mais ne peut pas être désactivé par un Delivery Controller exécutant XenApp et XenDesktop 7.1. Il ne reconnaît pas le paramètre de stratégie, qui est disponible dans la version ultérieure du produit. Ce paramètre de stratégie permet aux utilisateurs de télécharger des fichiers sur leur bureau virtuel, ce qui cause le problème de sécurité. Pour contourner ce problème, mettez à niveau le Delivery Controller ou une instance autonome de Studio vers la version 7.6 Feature Pack 2, puis utilisez la stratégie de groupe pour désactiver le paramètre de stratégie. Vous pouvez également utiliser la stratégie locale sur tous les bureaux virtuels concernés.

Considérations de sécurité Remote PC Access

Remote PC Access implémente les fonctionnalités de sécurité suivantes :

- La carte à puce est prise en charge.
- Lorsqu'une session à distance se connecte, le moniteur du PC de bureau affiche un écran noir.
- Remote PC Access redirige toutes les entrées de claviers et de souris vers la session à distance, sauf la combinaison CTRL+ALT+SUPPR et les cartes à puce et les périphériques biométriques USB.
- SmoothRoaming est prise en charge uniquement pour un seul utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Lorsqu'un utilisateur a ouvert une session distante connectée à un PC de bureau, seul cet utilisateur peut reprendre l'accès local sur le PC de bureau. Pour reprendre l'accès local, l'utilisateur appuie sur Ctrl+Alt+Suppr sur le PC local et ouvre une session avec les mêmes informations d'identification utilisées par la session à distance. L'utilisateur peut également reprendre l'accès local en insérant une carte à puce ou en tirant parti de la biométrie, si votre système possède une intégration fournisseur des informations d'identification tierces appropriées. Ce comportement par défaut peut être substitué par l'activation de changement rapide d'utilisateur via des objets de stratégie de groupe (GPO) ou en modifiant le registre.

Remarque : Citrix recommande de ne pas attribuer de privilèges d'administrateur VDA aux utilisateurs de sessions.

Assignations automatiques

Par défaut, Remote PC Access prend en charge l'assignation automatique de plusieurs utilisateurs à un VDA. Dans XenDesktop 5.6 Feature Pack 1, les administrateurs peuvent modifier ce comportement en utilisant le script PowerShell RemotePCAccess.ps1. Cette version utilise une entrée du Registre pour autoriser ou interdire plusieurs affectations de PC distants automatiques, ce paramètre s'applique à l'intégralité du site.

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

Pour restreindre les affectations automatiques pour un utilisateur unique :

Sur chaque Controller du site, définissez la clé de registre suivante :

HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Nom : AllowMultipleRemotePCAssignments

Type : REG_DWORD

Données : 0 = Désactiver l'attribution de plusieurs utilisateurs, 1 = Activer l'affectation de plusieurs utilisateurs (valeur par défaut).

S'il existe une ou plusieurs affectations d'utilisateur, supprimez-les à l'aide des commandes du kit de développement afin que le VDA puisse ensuite être admissible pour une seule affectation automatique.

- Supprimez tous les utilisateurs affectés à partir du VDA : $machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine
- Supprimez le VDA du groupe de mise à disposition : $machine | Remove-BrokerMachine -DesktopGroup $desktopGroup

Redémarrez le PC de bureau physique.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Délégation de l'administration

Jul 07, 2016

Grâce à l'utilisation d'un contrôle basé sur des objets et des rôles, le modèle d'administration déléguée vous offre une souplesse permettant d'adapter les activités d'administration déléguée aux besoins de votre entreprise. L'administration déléguée prend en charge les déploiements de toutes les tailles et vous permet d'affiner la granularité des autorisations à mesure que votre déploiement gagne en complexité. L'administration déléguée utilise trois concepts : les administrateurs, les rôles et les étendues.

- **Administrateurs** : un administrateur représente une personne ou un groupe de personnes identifié par leur compte Active Directory. Chaque administrateur est associé à un ou plusieurs rôles et à des paires d'étendues.
- **Rôles** : un rôle représente une fonction de tâche à laquelle des permissions sont associées. Par exemple, le rôle Administrateur du groupe de mise à disposition possède des autorisations telles que « Créer un groupe de mise à disposition » et « Supprimer le bureau d'un groupe de mise à disposition ». Un administrateur peut avoir plusieurs rôles pour un même site, donc une personne peut être administrateur du groupe de mise à disposition et administrateur du catalogue de machines. Les rôles peuvent être intégrés ou personnalisés.

  Les rôles intégrés sont :

Rôle	Autorisations
Administrateur complet	Peut effectuer toutes les tâches et toutes les opérations. Un administrateur complet est toujours associé à l'étendue Tout.
Administrateur en lecture seule	Peut afficher tous les objets dans les étendues spécifiées ainsi que les informations générales, mais ne peut rien modifier. Par exemple, un administrateur en lecture seule avec l'étendue = Londres peut voir tous les objets globaux (tels que la journalisation de la configuration) et les objets associés à Londres (par exemple, les groupes de mise à disposition Londres). Toutefois, cet administrateur ne peut pas afficher d'objets dans l'étendue New York (en supposant que les étendues Londres et New York ne se chevauchent pas).
Administrateur du service d'assistance	Peut afficher des groupes de mise à disposition et gérer les sessions et les machines associées à ces groupes. Peut afficher le catalogue de machines et les informations d'hôte des groupes de mise à disposition en cours de surveillance et peut également effectuer des opérations de gestion de session et de gestion de l'alimentation de la machine pour les machines figurant dans ces groupes de mise à disposition.
Administrateur du catalogue de machines	Peut créer et de gérer des catalogues de machines et y provisionner des machines. Peut créer des catalogues de machines à partir de l'infrastructure de virtualisation, Provisioning Services et des machines physiques. Ce rôle peut gérer les images de base et installer le logiciel, mais ne peut pas assigner les applications ou bureaux aux utilisateurs.
Administrateur de groupe de mise à disposition	Peut mettre à disposition des applications, bureaux et machines ; peut également gérer les sessions associées. Il peut également gérer les configurations d'applications et de bureaux, telles que les stratégies et les paramètres de gestion de l'alimentation.
Administrateur d'hôte	Peut gérer les connexions hôtes et leurs paramètres de ressources associés. Impossible de mettre à disposition des machines, applications ou bureaux aux utilisateurs.

  Dans certaines éditions du produit, vous pouvez créer des rôles personnalisés correspondants aux besoins de votre organisation, et déléguer des autorisations avec plus de détails. Vous pouvez utiliser les rôles personnalisés pour allouer des autorisations à la précision d'une action ou d'une tâche dans la console.

- **Étendues** : une étendue représente une collection d'objets. Les étendues sont utilisées pour grouper les objets de manière pertinente pour votre organisation (par exemple, l'ensemble de groupes de mise à disposition utilisé par l'équipe des ventes). Les objets peuvent appartenir à plus d'une étendue ; par exemple, un objet peut être marqué comme appartenant à une ou plusieurs étendues. Il existe une étendue intégrée appelée « Tout » qui contient tous les objets. Le rôle d'administrateur complet est toujours associé à l'étendue Tout.

La société XYZ a décidé de gérer les applications et bureaux en fonction de leur département (Comptabilité, Ventes et Production) et de leur système d'exploitation de bureau (Windows 7 ou Windows 8). L'administrateur a créé cinq étendues, puis a attribué deux étendues à chaque groupe de mise à disposition : une pour le département où ils sont utilisés et une pour le système d'exploitation qu'ils utilisent.

Les administrateurs suivants ont été créés :

Administrateur	Rôles	Étendues
domaine/fred	Administrateur complet	Tous (le rôle Administrateur complet a toujours la portée Tout)
domaine/rob	Administrateur en lecture seule	Tous
domaine/heidi	Administrateur en lecture seule Administrateur du service d'assistance	Tous Ventes

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administrateur	Rôles	Étendues
domaine/warehouseadmin	Administrateur du service d'assistance	Distribution
domaine/peter	Administrateur de groupe de mise à disposition Administrateur du catalogue de machines	Win7

- Fred est un administrateur complet qui peut afficher, modifier et supprimer tous les objets dans le système.
- Rob peut afficher tous les objets dans le site mais ne peut pas les modifier ou les supprimer.
- Heidi peut afficher tous les objets et peut effectuer des tâches de support technique sur les groupes de mise à disposition dans l'étendue Ventes. Cela lui permet de gérer les sessions et les machines associées à ces groupes ; elle ne peut pas effectuer de modifications dans le groupe de mise à disposition, telles que l'ajout ou la suppression de machines.
- Toute personne qui est membre du groupe de sécurité Active Directory admindistribution peut afficher et effectuer des tâches d'assistance sur des machines dans l'étendue Distribution.
- Peter est un spécialiste Windows 7 et peut gérer tous les catalogues de machines Windows 7 et mettre à disposition des applications, bureaux et machines Windows 7, quelle que soit l'étendue du département auquel elles appartiennent. L'administrateur a envisagé de donner à Peter le rôle d'administrateur complet pour l'étendue Win7 ; elle en a décidé autrement, car un administrateur complet a également des droits complets sur tous les objets qui ne sont pas inclus dans l'étendue, tels que « Site » et « Administrateur ».

En général, le nombre d'administrateurs et la granularité de leurs autorisations dépendent de la taille et de la complexité du déploiement.

- Dans les déploiements de petite taille ou de preuve de concept, toutes les tâches sont effectuées par un ou plusieurs administrateurs ; il n'y a pas de délégation. Dans ce cas, créez chaque administrateur avec le rôle Administrateur complet intégré, qui a la portée Tout.
- Dans les déploiements plus importants avec plus d'ordinateurs, d'applications et de bureaux, une plus grande délégation est nécessaire. Plusieurs administrateurs ont peut-être des responsabilités fonctionnelles plus spécifiques (rôles). Par exemple, deux sont des administrateurs complets et les autres sont des administrateurs du service d'assistance. En outre, un administrateur peut ne gérer que certains groupes d'objets (étendues), tels que des catalogues de machines. Dans ce cas, créez de nouvelles étendues, ainsi que des administrateurs avec l'un des rôles intégrés et les étendues appropriées.
- Même les déploiements plus importants peuvent nécessiter plus (ou plus spécifiques) d'étendues, ainsi que des administrateurs différents dotés de rôles non conventionnels. Dans ce cas, modifiez ou créez des étendues supplémentaires, créez des rôles personnalisés et créez chaque administrateur avec un rôle personnalisé ou intégré, ainsi que des étendues existantes et nouvelles.

Pour garantir une souplesse et facilité de configuration, vous pouvez créer de nouvelles étendues lorsque vous créez un administrateur. Vous pouvez également spécifier des étendues lors de la création ou de la modification de catalogues de machines ou de connexions.

Lorsque vous créez un site en tant qu'administrateur local, votre compte d'utilisateur devient automatiquement un administrateur complet avec autorisations complètes sur tous les objets. Après la création d'un site, les administrateurs locaux n'ont pas de privilèges spéciaux.

Le rôle administrateur complet a toujours l'étendue Tout ; vous ne pouvez pas le modifier.

Par défaut, un administrateur est activé. La désactivation d'un administrateur peut être nécessaire si vous créez le nouvel administrateur maintenant, mais cette personne ne possèdera des droits d'administration que bien plus tard. Pour les administrateurs activés existants, il se peut que vous souhaitiez désactiver plusieurs d'entre eux pendant que vous réorganisez vos objets/étendues, puis les réactiver lorsque vous êtes prêt à utiliser la configuration mise à jour dans votre environnement de production. Vous ne pouvez pas désactiver un administrateur complet si cela a pour conséquence qu'il n'existe plus d'administrateur complet activé. La case à cocher activer/désactiver est disponible lors de la création, de la copie ou de la modification d'un administrateur.

Lorsque vous supprimez une paire rôle/étendue lors de la copie, la modification ou la suppression d'un administrateur, il supprime uniquement la relation entre le rôle et l'étendue de cet administrateur ; il ne peut pas supprimer le rôle ou l'étendue et n'affecte aucun autre administrateur qui est configuré avec cette paire rôle/étendue.

Pour gérer des administrateurs, cliquez sur Configuration > Administrateurs dans le panneau de navigation de Studio, puis cliquez sur l'onglet Administrateurs dans la partie supérieure du panneau central.

- Pour créer un administrateur, cliquez sur Créer un nouvel administrateur dans le volet Actions. Entrez le nom ou recherchez le nom du compte d'utilisateur, sélectionnez ou créez une étendue, et sélectionnez un rôle. Le nouvel administrateur est activé par défaut, vous pouvez le modifier.
- Pour copier un administrateur, sélectionnez l'administrateur dans le panneau du milieu, puis cliquez sur Copier l'administrateur dans le volet Actions. Entrez le nom ou recherchez le nom de compte de l'utilisateur. Vous pouvez sélectionner puis modifier les paires rôle/étendue et vous pouvez en ajouter de nouvelles. Le nouvel administrateur est activé par défaut, vous pouvez le modifier.
- Pour modifier un administrateur, sélectionnez l'administrateur dans le panneau du milieu, puis cliquez sur Modifier l'administrateur dans le volet Actions. Vous pouvez modifier ou supprimer les paires rôle/étendue et en ajouter de nouvelles.
- Pour supprimer un administrateur, sélectionnez l'administrateur dans le panneau du milieu, puis cliquez sur Supprimer l'administrateur dans le volet Actions. Vous ne pouvez pas supprimer un administrateur complet si cela a pour conséquence qu'il n'existe plus d'administrateur complet.

Les noms des rôles peuvent contenir jusqu'à 64 caractères Unicode ; ils ne peuvent contenir les caractères suivants : \ (barre oblique inverse), / (barre oblique), ; (point-virgule), : (deux-points), # (dièse) , (virgule), * (astérisque), ? (point d'interrogation), = (signe égal), < (flèche gauche), > (flèche droite), | (barre verticale), [ ] (crochet droit ou

© 1999-2017 Citrix Systems, Inc. All rights reserved.

gauche), ( ) (parenthèse droite ou gauche), " (guillemets) et ' (apostrophe). Les descriptions peuvent contenir jusqu'à 256 caractères unicode.

Vous ne pouvez pas modifier ou supprimer un rôle intégré. Vous ne pouvez pas supprimer un rôle personnalisé si un administrateur l'utilise.

Remarque : seules certaines éditions de produit prennent en charge les rôles personnalisés. Les éditions qui ne prennent pas en charge les rôles personnalisés n'ont aucune entrée dans le volet Actions.
Pour gérer les rôles, cliquez sur Configuration > Administrateurs dans le panneau de navigation de Studio, puis cliquez sur l'onglet Rôles en haut du panneau central.

- Pour afficher les détails d'un rôle, sélectionnez le rôle dans le volet central. La partie inférieure du panneau central répertorie les types d'objets et les autorisations associées pour le rôle. Cliquez sur l'onglet Administrateurs dans le volet inférieur pour afficher une liste des administrateurs détiennent actuellement ce rôle.
- Pour créer un rôle personnalisé, cliquez sur Créer un nouveau rôle dans le volet Actions. Entrez un nom et une description. Sélectionnez les types d'objets et les autorisations.
- Pour copier un rôle, sélectionnez le rôle dans le volet central, puis cliquez sur Copier un rôle dans le volet Actions. Modifiez le nom, la description, les types d'objet et les autorisations nécessaires.
- Pour modifier un rôle personnalisé, sélectionnez le rôle dans le volet central, puis cliquez sur Modifier un rôle dans le volet Actions. Modifiez le nom, la description, les types d'objet et les autorisations nécessaires.
- Pour supprimer un rôle personnalisé, sélectionnez le rôle dans le volet central, puis cliquez sur Supprimer un rôle dans le volet Actions. Lorsque vous y êtes invité, confirmez la suppression.

Lorsque vous créez un site, la seule étendue disponible est l'étendue 'Tout', qui ne peut pas être supprimée.

Vous pouvez créer des étendues à l'aide de la procédure ci-dessous. Vous pouvez également créer des étendues lorsque vous créez un administrateur ; chaque administrateur doit être associé à au moins une paire de un rôle/étendue. Lorsque vous créez ou modifiez des bureaux, des catalogues de machines, des applications ou des hôtes, vous pouvez les ajouter à une étendue existante ; si vous ne les ajoutez pas à une étendue, ils restent dans l'étendue 'Toute'.

La création d'un site ne peut faire être incluse à une étendue, ni les objets d'administration déléguée (étendues et rôles). Cependant, les objets ne pouvant pas être inclus à une étendue sont inclus dans l'étendue « Tout ». (Les administrateurs complets disposent toujours de l'étendue Toute.) Les machines, actions d'alimentation, bureaux et sessions ne sont pas directement inclus à une étendue ; des permissions sur ces objets peuvent être accordées aux administrateurs via les catalogues de machines ou groupes de mise à disposition associés.

Les noms d'étendue peuvent contenir jusqu'à 64 caractères Unicode ; ils ne peuvent contenir les caractères suivants : \ (barre oblique inverse), / (barre oblique), ; (point-virgule), : (deux-points), # (dièse) , (virgule), * (astérisque), ? (point d'interrogation), = (signe égal), < (flèche gauche), > (flèche droite), | (barre verticale), [ ] (crochet droit ou gauche), ( ) (parenthèse droite ou gauche), " (guillemets) et ' (apostrophe). Les descriptions peuvent contenir jusqu'à 256 caractères unicode.

Lorsque vous copiez ou modifier une étendue, n'oubliez pas que la suppression des objets dans l'étendue peut rendre ces objets inaccessibles à l'administrateur. Si l'étendue modifiée est associée à un ou plusieurs rôles, assurez-vous que les mises à jour que vous apportez à l'étendue ne rendent pas une paire rôle/étendue inutilisable.

Pour gérer des étendues, cliquez sur Configuration > Administrateurs dans le panneau de navigation de Studio, puis cliquez sur l'onglet Étendues dans la partie supérieure du panneau central.

- Pour créer une étendue, cliquez sur Créer une nouvelle étendue dans le volet Actions. Entrez un nom et une description. Pour inclure tous les objets d'un type particulier (par exemple, les groupes de mise à disposition), sélectionnez le type d'objet. Pour inclure des objets spécifiques, développez le type, puis sélectionnez les objets individuels (par exemple, les groupes de mise à disposition individuels utilisés par l'équipe des Ventes).
- Pour copier une étendue, sélectionnez l'étendue dans le volet central, puis cliquez sur Copier étendue dans le volet Actions. Entrez un nom et une description. Modifiez les types d'objets et les objets, si nécessaire.
- Pour modifier une étendue, sélectionnez l'étendue dans le volet central, puis cliquez sur Modifier l'étendue dans le volet Actions. Modifiez le nom, la description, les types d'objet et les objets, si nécessaire.
- Pour supprimer une étendue, sélectionnez l'étendue dans le volet central, puis cliquez sur Supprimer l'étendue dans le volet Actions. Lorsque vous y êtes invité, confirmez la suppression.

Vous pouvez créer deux types de rapports d'administration déléguée :

- Ce rapport HTML indique les paires rôle/étendue associées à un administrateur et dresse la liste des autorisations individuelles pour chaque type d'objet (par exemple, les groupes de mise à disposition et les catalogues de machines). Vous pouvez générer ce rapport à partir de Studio.
  Pour créer ce rapport, cliquez sur Configuration > Administrateurs dans le volet de navigation. Sélectionnez un administrateur dans le panneau du milieu, puis cliquez sur Créer un rapport dans le volet Actions.

  Vous pouvez également demander ce rapport lors de la création, de la copie ou de la modification d'un administrateur.

- Un rapport HTML ou CSV qui mappe tous les rôles personnalisés et intégrés à des autorisations. Vous pouvez générer ce rapport en exécutant le script PowerShell nommé OutputPermissionMapping.ps1.
  Pour exécuter ce script, vous devez être un administrateur complet, un administrateur en lecture seule ou un administrateur personnalisé avec autorisation de lecture des rôles. Le script se trouve dans : Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts\.

  Syntaxe :

  OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path <chaîne>] [-AdminAddress <chaîne>] [-Show] [<CommonParameters>]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètre	Description
-Help	Affiche l'aide du script.
-Csv	Spécifie le fichier CSV de sortie. Valeur par défaut = HTML
-Path <chaîne>	Où écrire la sortie. Valeur par défaut = stdout
-AdminAddress <chaîne>	Adresse IP ou nom d'hôte du Delivery Controller auquel se connecter. Valeur par défaut = XA
-Show	(Valide uniquement lorsque le paramètre -Path est également spécifié). Lorsque vous écrivez la sortie vers un fichier, ce paramètre entraîne l'ouverture de la sortie dans un programme approprié, tel qu'un navigateur Web.
	Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer et OutVariable. Pour plus d'informations, veuillez consulter la documentation Microsoft.

L'exemple suivant écrit une table HTML sur un fichier appelé Roles.html et ouvre la table dans un navigateur Web.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\ Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"  -Path Roles.html –Show
```

L'exemple suivant écrit une table CSV sur un fichier appelé Roles.csv. La table n'est pas affichée.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\ Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"  –CSV -Path Roles.csv
```

À partir d'une invite de commande Windows, l'exemple de commande précédente est :

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\ Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'  -CSV -Path Roles.csv"
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cartes à puce

Aug 22, 2016

Les cartes à puce et les technologies équivalentes sont prises en charge selon les indications décrites dans cet article. Pour utiliser des cartes à puce avec XenApp ou XenDesktop :

- Il est important de bien comprendre la stratégie de sécurité de votre organisation concernant l'utilisation des cartes à puce. Ces stratégies peuvent, par exemple, déterminer comment les cartes à puce sont délivrées et comment les utilisateurs doivent les protéger. Il peut être nécessaire de réévaluer certains aspects de ces stratégies dans un environnement XenApp ou XenDesktop.
- Déterminez les types de machine utilisateur, les systèmes d'exploitation et les applications publiées qui doivent être utilisés avec des cartes à puce.
- Familiarisez-vous avec la technologie de carte à puce ainsi que le matériel et les logiciels de votre fournisseur de carte à puce.
- Déterminez comment déployer des certificats numériques dans un environnement distribué.

Types de cartes à puce

Les cartes à puce d'entreprise et de consommateur ont les mêmes dimensions et connecteurs électriques et utilisent les mêmes lecteurs de carte à puce.

Les cartes à puce d'entreprise contiennent des certificats numériques. Ces cartes à puce prennent en charge l'ouverture de session Windows, et peuvent également être utilisées avec des applications pour la signature numérique et le cryptage de documents et d'e-mails. XenApp et XenDesktop prennent en charge ces utilisations.

Les cartes à puce pour consommateur ne contiennent pas de certificats numériques ; elles contiennent un secret partagé. Ces cartes à puce peuvent prendre en charge les paiements (par carte de crédit avec puce et signature ou avec puce et code PIN). Elles ne prennent pas en charge l'ouverture de session Windows ou les applications Windows standard. Des applications Windows spécialisées et une infrastructure logicielle adaptée (notamment, par exemple, une connexion à un réseau de carte de paiement) sont requises pour utiliser ces cartes à puce. Contactez votre conseiller Citrix pour de plus amples informations sur la prise en charge de ces applications spécialisées sur XenApp ou XenDesktop.

Pour les cartes à puce d'entreprise, il existe des équivalents compatibles qui peuvent être utilisés de manière similaire.

- Un jeton USB équivalent à une carte à puce se connecte directement à un port USB. Ces jetons USB sont généralement de la taille d'un lecteur flash USB, mais peuvent être aussi petits qu'une carte SIM utilisée dans un téléphone mobile. Ils se présentent comme une combinaison d'une carte à puce et d'un lecteur de carte à puce USB.
- Une carte à puce virtuelle utilisant un module de plateforme sécurisée (TPM) Windows se présente en tant que carte à puce. Ces cartes à puce virtuelles sont prises en charge par Windows 8 et Windows 10, à l'aide de Citrix Receiver 4.3 minimum.
  - Les versions de XenApp et XenDesktop antérieures à 7.6 FP3 ne prennent pas en charge les cartes à puce virtuelles.
  - Pour de plus amples informations sur les cartes à puce virtuelles, consultez la section Virtual Smart Card Overview.

    Remarque : le terme « carte à puce virtuelle » est également utilisé pour décrire un certificat numérique simplement stocké sur l'ordinateur de l'utilisateur. Ces certificats numériques ne sont pas réellement similaires aux cartes à puce.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

La prise en charge des cartes à puce de XenApp et XenDesktop repose sur les spécifications standard PC/SC (Personal Computer/Smart Card) de Microsoft. La configuration minimale requise exige que les cartes à puce et les lecteurs de carte à puce soient pris en charge par le système d'exploitation Windows sous-jacent et soient certifiés WHQL (laboratoires Microsoft de contrôle qualité du matériel conçu pour Windows). Consultez la documentation Microsoft pour plus d'informations sur la conformité PC/SC du matériel. D'autres types de machines utilisateur peuvent être conformes aux normes PS/SC. Pour plus d'informations, reportez-vous au programme Citrix Ready sur http://www.citrix.com/ready/.

En règle générale, un pilote de périphérique séparé est nécessaire pour la carte à puce ou équivalent de chaque fournisseur. Cependant, si des cartes à puce sont conformes à une norme telle que la norme NIST Personal Identity Verification (PIV), il est possible d'utiliser un seul pilote de périphérique pour une gamme de cartes à puce. Le pilote de périphérique doit être installé sur la machine utilisateur et le Virtual Delivery Agent (VDA). Le pilote de périphérique est souvent fourni dans le cadre du package de middleware de la carte à puce, disponible auprès d'un partenaire Citrix ; le package de middleware de carte à puce propose des fonctionnalités avancées. Le pilote de périphérique peut également être décrit comme fournisseur de service cryptographique (CSP), fournisseur de stockage de clés (KSP) ou minipilote.

Les combinaisons carte à puce et logiciel intermédiaire suivantes ont été testées par Citrix comme exemples représentatifs de leur type. Cependant, d'autres cartes à puce et middleware peuvent également être utilisés. Pour de plus amples informations sur les cartes à puce et middleware compatibles avec Citrix consultez http://www.citrix.com/ready.

Logiciels intermédiaires	Correspondance des cartes
ActivClient 7.0 (mode DoD activé)	Carte DoD CAC
ActivClient 7.0 en mode PIV	Carte NIST PIV
Mini-pilote Microsoft	Carte NIST PIV
Minipilote GemAlto pour carte .NET	GemAlto .NET v2+
Pilote natif Microsoft	Cartes à puce virtuelles (TPM)

Pour de plus amples informations sur l'utilisation de cartes à puce avec d'autres types de périphériques, consultez la documentation relative à Citrix Receiver pour ce périphérique. Pour plus d'informations sur l'utilisation de PIV avec XenDesktop, consultez la section Configuration de Citrix XenDesktop 7.6 et NetScaler Gateway 10.5 avec authentification par carte à puce PIV.

Pour de plus amples informations sur l'utilisation de cartes à puce avec d'autres types de périphériques, consultez la documentation relative à Citrix Receiver pour ce périphérique.

Les cartes à puce sont uniquement prises en charge pour l'accès à distance vers les postes de travail physiques exécutant Windows 10, Windows 8 ou Windows 7 ; les cartes à puce ne sont pas prises en charge par les postes de travail exécutant Windows XP.

Les cartes à puce suivantes ont été testées avec Remote PC Access :

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Logiciels intermédiaires	Correspondance des cartes
Minipilote Gemalto .NET	Gemalto .NET v2+
ActivIdentity ActivClient 6.2	NIST PIV
ActivIdentity ActivClient 6.2	CAC
Minipilote Microsoft	NIST PIV
Pilote natif Microsoft	Cartes à puce virtuelles

Types de lecteurs de carte à puce

Un lecteur de carte à puce peut être intégré à la machine utilisateur, ou être connecté séparément à la machine utilisateur (généralement via USB ou Bluetooth). Les lecteurs de carte avec contact qui sont conformes à la spécification USB CCID sont pris en charge. Ils contiennent une fente dans laquelle l'utilisateur insère la carte à puce. La norme ZKA (Zentraler Kredit Ausschuss ou Central Credit Committee) définit quatre catégories de lecteurs de carte avec contact.

- Les lecteurs de carte à puce de classe 1 sont les plus courants et sont généralement dotés d'une seule fente. Les lecteurs de carte à puce de classe 1 sont pris en charge, généralement avec un pilote de périphérique CCID standard fourni avec le système d'exploitation.
- Les lecteurs de carte à puce de classe 2 présentent également un pavé numérique sécurisé qui n'est pas accessible par la machine utilisateur. Les lecteurs de carte à puce de classe 2 peuvent être intégrés à un clavier avec un pavé numérique sécurisé. Pour les lecteurs de carte à puce de classe 2, contactez votre conseiller Citrix ; un pilote de périphérique spécifique au lecteur peut être nécessaire pour activer la fonctionnalité de pavé numérique sécurisé.
- Les lecteurs de carte à puce de classe 3 sont également dotés d'un affichage sécurisé. Les lecteurs de carte à puce de classe 3 ne sont pas pris en charge.
- Les lecteurs de carte à puce de classe 4 contiennent également un module de transaction sécurisé. Les lecteurs de carte à puce de classe 4 ne sont pas pris en charge.

Remarque : la classe du lecteur de carte à puce n'est pas liée à la classe du périphérique USB.

Les lecteurs de carte à puce doivent être installés avec un pilote de périphérique correspondant sur la machine utilisateur.

Expérience utilisateur

La prise en charge des cartes à puce est intégrée dans XenApp et XenDesktop, à l'aide d'un canal virtuel de carte à puce ICA/HDX spécifique qui est activé par défaut.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Important : n'utilisez pas la redirection USB générique pour les lecteurs de carte à puce. Elle est désactivée par défaut pour les lecteurs de carte à puce et n'est pas prise en charge si activée.

Plusieurs cartes à puce et plusieurs lecteurs peuvent être utilisés sur la même machine utilisateur, mais si une authentification pass-through est utilisée, une seule carte à puce doit être insérée lorsque l'utilisateur démarre un bureau virtuel ou une application. Lorsqu'une carte à puce est utilisée dans une application (par exemple pour des fonctions de signature numérique ou de cryptage), l'utilisateur peut être invité plusieurs fois à insérer une carte à puce ou à saisir un code PIN. Ceci peut se produire si plusieurs cartes à puce sont insérées en même temps.

- Si les utilisateurs sont invités à insérer une carte à puce alors que celle-ci se trouve déjà dans le lecteur, ils doivent sélectionner Annuler.
- Si les utilisateurs sont invités à entrer le code PIN, ils doivent le saisir à nouveau.

Si vous utilisez des applications hébergées s'exécutant sur Windows Server 2008 ou 2008 R2 et avec des cartes à puce exigeant Microsoft Base Smart Card Cryptographic Service Provider, vous constaterez peut-être que tous les autres utilisateurs qui utilisent une carte à puce dans le processus d'ouverture de session sont bloqués. Pour plus de détails et pour obtenir une correction pour ce problème, veuillez consulter l'article http://support.microsoft.com/kb/949538.

Vous pouvez réinitialiser les codes confidentiels à l'aide d'un système de gestion de carte ou d'un outil du fournisseur.

Avant de déployer les cartes à puce

- Vous devez vous procurer un pilote de périphérique pour le lecteur de carte à puce et l'installer sur la machine utilisateur. De nombreux lecteurs de carte à puce peuvent utiliser le pilote de périphérique CCID fourni par Microsoft.
- Vous devez vous procurer un pilote de périphérique et un logiciel de fournisseur de services de chiffrement (CSP) depuis votre fournisseur de carte à puce et les installer sur les machines utilisateur et les bureaux virtuels. Le pilote et le logiciel CSP doivent être compatibles avec XenApp et XenDesktop, consultez la documentation du fournisseur de compatibilité. Pour les bureaux virtuels utilisant des cartes à puce qui prennent en charge et utilisent le modèle minipilote, les minipilotes de carte à puce devraient se télécharger automatiquement, mais vous pouvez les obtenir à partir de http://catalog.update.microsoft.com ou auprès votre fournisseur. En outre, si des middlewares PKCS #11 sont requis, obtenez-les auprès de votre fournisseur de carte.
- **Important :** Citrix recommande d'installer et de tester les pilotes et le logiciel CSP sur un ordinateur physique avant d'installer le logiciel Citrix.
- Ajoutez l'adresse URL de Receiver pour Web à la liste Sites de confiance pour les utilisateurs qui travaillent avec des cartes à puce dans Internet Explorer avec Windows 10. Dans Windows 10, Internet Explorer n'est pas exécuté par défaut en mode protégé pour les sites de confiance.
- Assurez-vous que votre infrastructure de clé publique (PKI) est configurée correctement. Cela assure que le mappage de certificat vers le compte est correctement configuré pour l'environnement Active Directory et que la validation du certificat utilisateur peut être effectuée avec succès.
- Assurez-vous que votre déploiement répond à la configuration système requise des autres composants Citrix utilisé avec des cartes à puce, y compris Citrix Receiver et StoreFront.
- Vérifiez l'accès aux serveurs suivants de votre site :
  - Le contrôleur de domaine Active Directory pour le compte d'utilisateur associé à un certificat d'ouverture de session sur la carte à puce
  - Delivery Controller
  - Citrix StoreFront
  - Citrix NetScaler Gateway/Citrix Access Gateway 10.x

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- VDA
- (Facultatif pour Remote PC Access) : Microsoft Exchange Server

Activer l’authentification par carte à puce

Étape 1. Problème de cartes à puce pour les utilisateurs en fonction de votre stratégie d’émission de carte.

Étape 2. (Facultatif) Définissez des cartes à puce pour activer les utilisateurs pour Remote PC Access.

Étape 3. Installez et configurez le Delivery Controller et StoreFront (s'ils ne sont pas déjà installés pour l'utilisation des cartes à puce à distance).

Étape 4. Activez StoreFront pour l'utilisation des cartes à puce. Pour de plus amples informations, consultez la section Configurer l'authentification par carte à puce dans la documentation de StoreFront.

Étape 5. Activez NetScaler Gateway/Access Gateway pour utiliser la carte à puce. Pour de plus amples informations, consultez la section Configuration de l'authentification et de l'autorisation et Configuration de l'accès par carte à puce avec l'Interface Web dans la documentation NetScaler.

Étape 6. Activez VDAs pour l'utilisation des cartes à puce.

- Assurez-vous que le VDA possède les applications et les mises à jour requises.
- Installez les logiciels intermédiaires.
- Définissez l'utilisation d'une carte à puce à distance, l’activation de la communication des données de carte à puce entre Receiver sur une machine utilisateur et une session de bureau virtuel.

Étape 7. Activez les machines utilisateur (y compris les machines appartenant à un domaine ou non) pour utiliser la carte à puce. Consultez la section Configurer l'authentification par carte à puce dans la documentation de StoreFront pour plus de détails.

- Importez le certificat racine de l'autorité de certification et le certificat émis par l’autorité de certificat dans le magasin de clés de la machine.
- Installez le middleware de carte à puce de votre fournisseur.
- Installez et configurez Citrix Receiver pour Windows, en vous assurant d'importer le fichier icaclient.adm à l'aide de la console de gestion des stratégies de groupe et d'activer l'authentification par carte à puce.

Étape 8. Testez le déploiement. Assurez-vous que votre déploiement est correctement configuré en démarrant un bureau virtuel avec une carte à puce d'utilisateur test. Testez tous les mécanismes d'accès possibles (par exemple, accès au bureau via Internet Explorer et Citrix Receiver).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Déploiements de carte à puce

Jul 07, 2016

Les types de déploiements de carte à puce suivants sont pris en charge par cette version du produit et par les environnements mixtes contenant cette version. D'autres configurations peuvent fonctionner mais ne sont pas prises en charge.

Type	Connectivité StoreFront
Ordinateurs appartenant à un domaine local	Directement connectés
Accès à distance à partir d'ordinateurs appartenant à un domaine	Connectés au travers de NetScaler Gateway
Ordinateurs n'appartenant pas à un domaine	Directement connectés
Accès à distance depuis des ordinateurs n'appartenant pas à un domaine	Connectés au travers de NetScaler Gateway
Ordinateurs n'appartenant pas à un domaine et clients légers accédant au site Desktop Appliance	Connectés au travers des sites Desktop Appliance
Ordinateurs appartenant à un domaine et clients légers accédant à StoreFront au travers de l'adresse URL XenApp Services	Connectés via les adresses URL XenApp Services

Les types de déploiement sont définis par les caractéristiques de la machine utilisateur sur laquelle le lecteur de carte à puce est connecté :

- Indique si la machine appartient à un domaine ou n'appartient pas à un domaine.
- Comment le périphérique est-il connecté à StoreFront.
- Quel logiciel est utilisé pour afficher les applications et les bureaux virtuels.

En outre, les applications compatibles avec les cartes à puce, telles que Microsoft Word et Microsoft Excel, peuvent être utilisées dans ces déploiements. Ces applications permettent aux utilisateurs de signer numériquement ou de crypter des documents.

Lorsque cela est possible dans chacun de ces déploiements, Receiver prend en charge l'authentification bimodale en offrant à l'utilisateur le choix d'utilisation d'une carte à puce ou de saisie de leur nom d'utilisateur et mot de passe. Ceci est utile si la carte à puce ne peut pas être utilisé (par exemple, si l'utilisateur l'a laissé chez lui, ou que le certificat d'ouverture de session a expiré).

Étant donné que les utilisateurs de machines n'appartenant pas à un domaine ouvrent une session sur Receiver pour Windows directement, vous pouvez autoriser les utilisateurs à revenir à l'authentification explicite. Si vous configurez l'authentification bimodale, les utilisateurs sont initialement invités à ouvrir une session à l'aide de leurs cartes à puce et codes PIN mais ont la possibilité de sélectionner l'authentification explicite s'ils rencontrent des problèmes avec leurs cartes à puce.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si vous déployez NetScaler Gateway, les utilisateurs ouvrent une session sur leurs machines et sont invités par Receiver pour Windows à s'authentifier auprès de NetScaler Gateway. Cela s'applique aussi bien aux machines appartenant à un domaine qu'à celles n'appartenant pas à un domaine. Les utilisateurs peuvent ouvrir une session sur NetScaler Gateway à l'aide de leurs cartes à puce et codes PIN, ou avec des informations d'identification explicites. Cela vous permet de fournir aux utilisateurs une authentification bimodale pour l'ouverture de session NetScaler Gateway. Configurez l'authentification unique de NetScaler Gateway à StoreFront et déléguez la validation des informations d'identification à NetScaler Gateway pour les utilisateurs de cartes à puce de façon à ce que les utilisateurs soient authentifiés auprès de StoreFront de manière silencieuse.

Dans un environnement Citrix, les cartes à puce sont prises en charge dans une forêt unique. Les ouvertures de session par carte à puce entre les forêts nécessitent une approbation de forêt bidirectionnelle pour tous les comptes d'utilisateur. Les déploiements plus complexes de forêts multiples impliquant des cartes à puce (c'est-à-dire, où les approbations sont uniquement à sens unique ou de types différents) ne sont pas pris en charge.

Vous pouvez utiliser des cartes à puce dans un environnement Citrix qui comprend des bureaux distants. Cette fonctionnalité peut être installée localement (sur la machine utilisateur à laquelle la carte à puce est connectée) ou à distance (sur le bureau distant à laquelle la machine utilisateur se connecte).

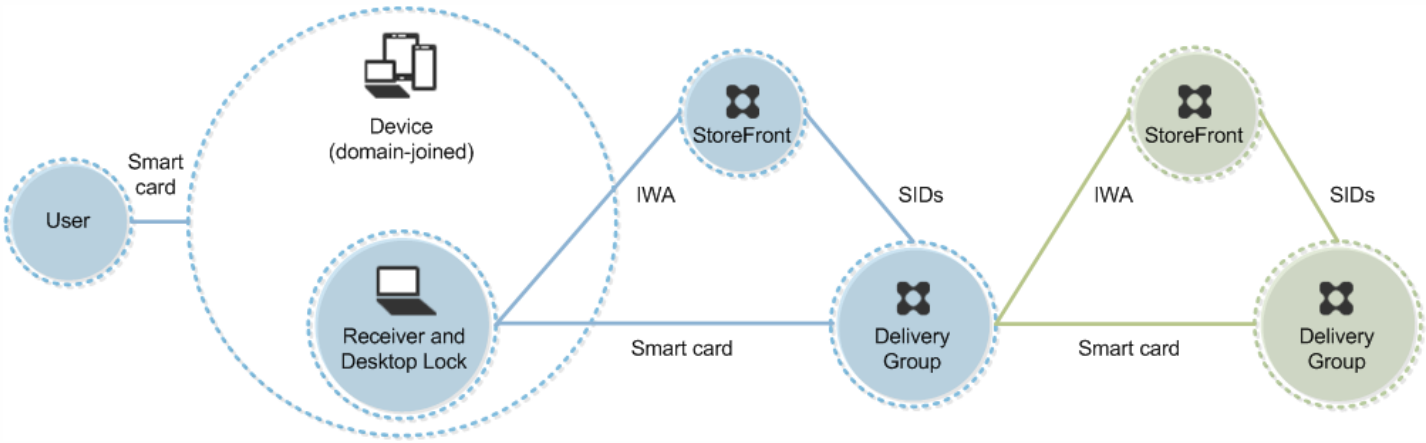
La stratégie définie pour le retrait de la carte à puce sur le produit détermine ce qui se passe lorsque vous retirez la carte à puce du lecteur au cours d'une session. Cette stratégie est configurée et gérée par le système d'exploitation Windows.

Paramètre de stratégie	Comportement du Bureau
Aucune action	Aucune action.
Verrouiller la station de travail	La session de bureau est déconnectée et le bureau virtuel est verrouillé.
Forcer la fermeture de session	L'utilisateur est obligé de fermer la session. Si la connexion réseau est interrompue et que ce paramètre est activé, la session peut être fermée et l'utilisateur peut perdre des données.
Déconnecter en cas de session Terminal Server	La session est déconnectée et le bureau virtuel est verrouillé.

Si la vérification de la révocation des certificats est activée et qu'un utilisateur insère une carte à puce avec un certificat non valide dans un lecteur de carte, l'utilisateur ne peut pas authentifier ou accéder au bureau ou à l'application associée à ce certificat. Par exemple, si le certificat non valide est utilisé pour le déchiffrement de messagerie, l'e-mail reste crypté. Si d'autres certificats sur la carte, tels que ceux utilisées pour l'authentification, sont toujours valides, ces fonctions restent actives.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

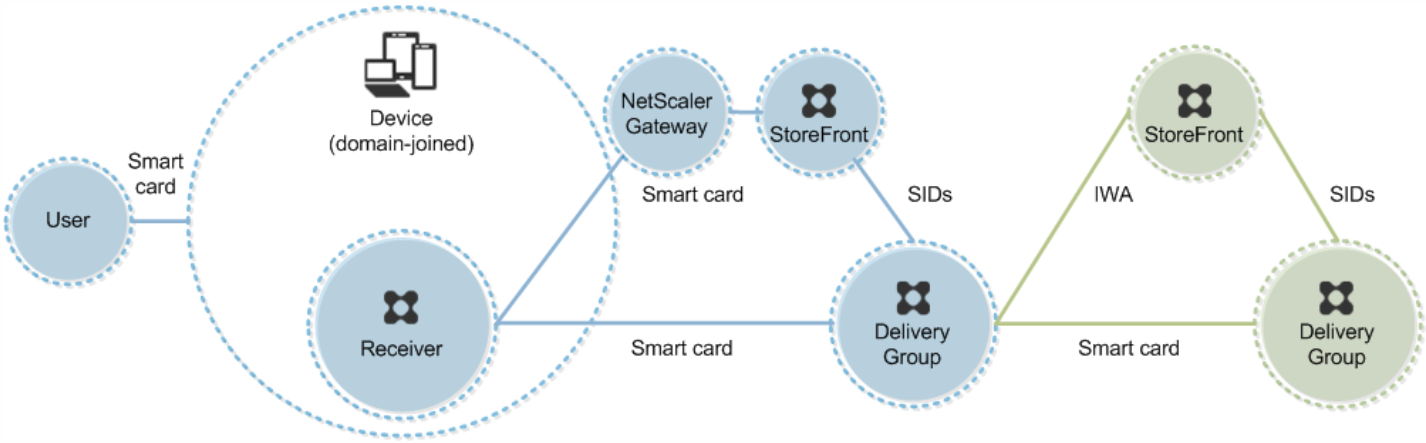
Ce déploiement implique des machines utilisateur appartenant à un domaine qui exécutent Desktop Viewer et se connectent directement à StoreFront.



Un utilisateur ouvre une session sur une machine à l'aide d'une carte à puce et du code confidentiel. Receiver authentifie l'utilisateur à un serveur StoreFront à l'aide de l'authentification Windows intégrée (IWA). StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à XenApp ou XenDesktop. Lorsque l'utilisateur démarre un bureau virtuel ou une application, l'utilisateur n'est pas invité à entrer un code confidentiel, car la fonctionnalité d'authentification unique est configurée sur Receiver.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

Ce déploiement implique des machines utilisateur appartenant à un domaine qui exécutent Desktop Viewer et se connectent à StoreFront via NetScaler Gateway/Access Gateway.



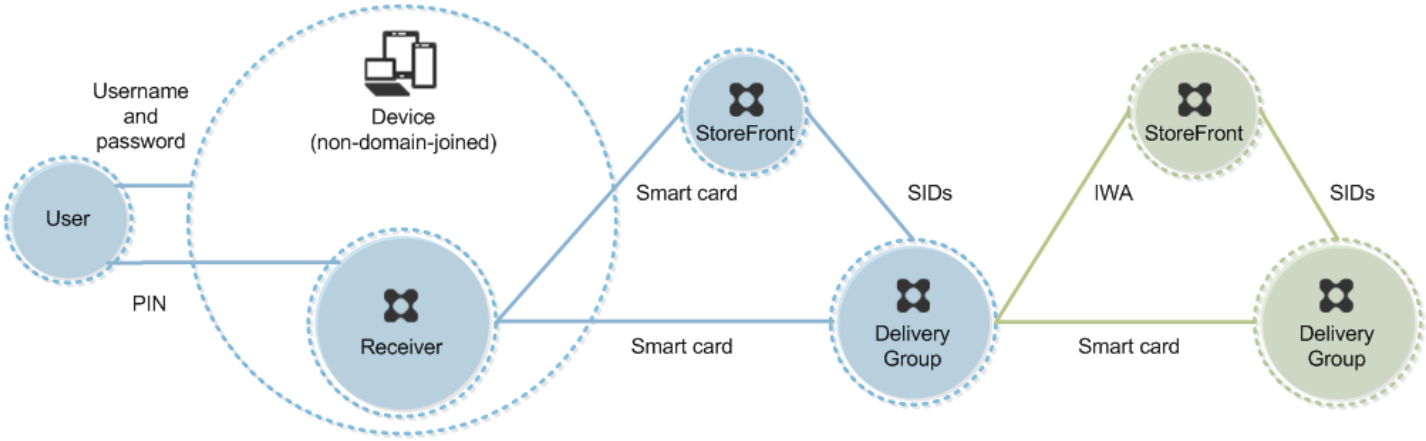
Un utilisateur ouvre une session sur une machine à l'aide d'une carte à puce et d'un code confidentiel, puis ouvre une session sur NetScaler Gateway/Access Gateway. Cette seconde ouverture de session peut être effectuée avec la carte à puce et un code confidentiel ou un nom d'utilisateur et un mot de passe car Receiver permet l'authentification bimodale dans ce déploiement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

L'utilisateur ouvre automatiquement une session sur StoreFront, qui transmet les identificateurs de sécurité (SID) de l'utilisateur à XenApp ou XenDesktop. Lorsque l'utilisateur démarre un bureau ou une application virtuel(le), l'utilisateur n'est pas invité à entrer à nouveau un code confidentiel, car la fonctionnalité d'authentification unique est configurée sur Receiver.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

Ce déploiement implique des machines utilisateur n'appartenant pas au domaine qui exécutent Desktop Viewer et se connectent directement à StoreFront.



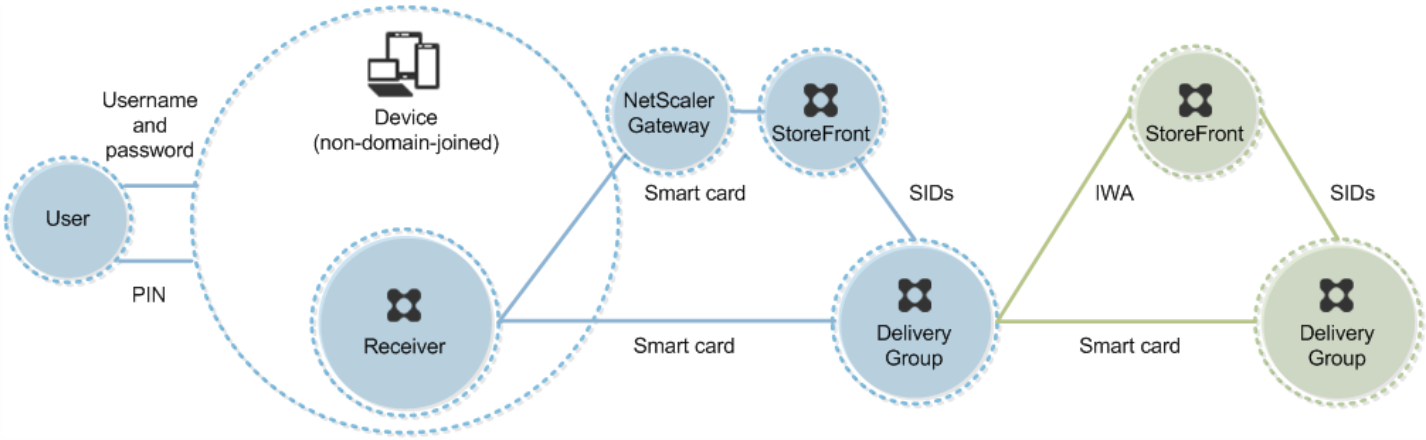
Un utilisateur ouvre une session sur une machine. En général, l'utilisateur entre un nom d'utilisateur et un mot de passe, mais puisque la machine n'appartient pas à un domaine, les informations d'identification de cette ouverture de session sont facultatives. Comme l'authentification bimodale est possible dans ce déploiement, Receiver invite l'utilisateur à entrer une carte à puce et un code confidentiel ou un nom d'utilisateur et un mot de passe. Receiver s'authentifie ensuite auprès de StoreFront.

StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à XenApp ou XenDesktop. Lorsque l'utilisateur démarre un bureau virtuel ou une application, l'utilisateur est invité à entrer un code confidentiel, car la fonctionnalité d'authentification unique n'est pas disponible dans ce déploiement.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

Ce déploiement implique des machines utilisateur n'appartenant pas au domaine qui exécutent Desktop Viewer et se connectent directement à StoreFront.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Un utilisateur ouvre une session sur une machine. En général, l'utilisateur entre un nom d'utilisateur et un mot de passe, mais puisque la machine n'appartient pas à un domaine, les informations d'identification de cette ouverture de session sont facultatives. Comme l'authentification bimodale est possible dans ce déploiement, Receiver invite l'utilisateur à entrer une carte à puce et un code confidentiel ou un nom d'utilisateur et un mot de passe. Receiver s'authentifie ensuite auprès de StoreFront.

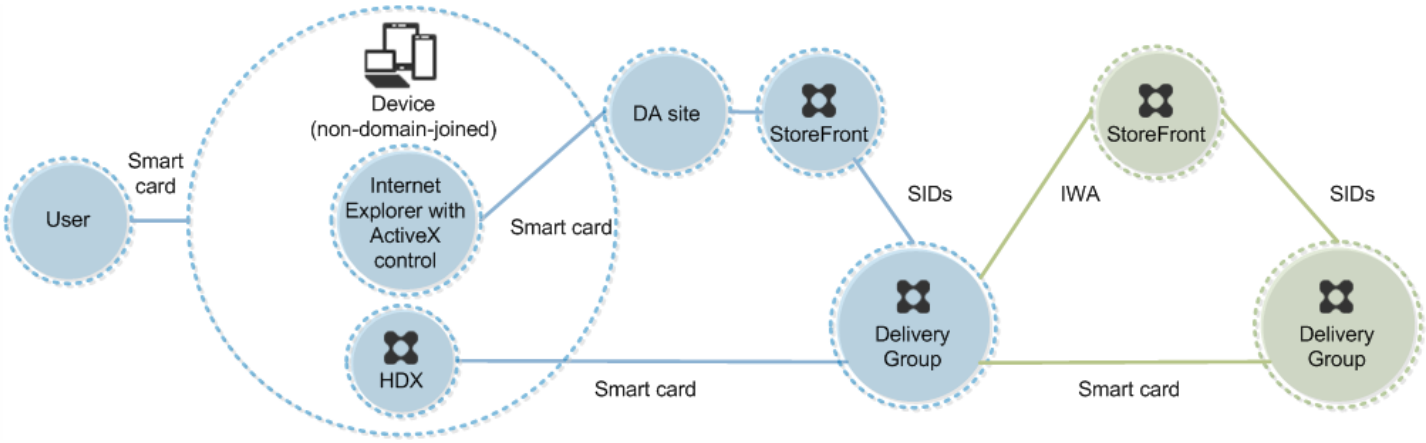
StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à XenApp ou XenDesktop. Lorsque l'utilisateur démarre un bureau virtuel ou une application, l'utilisateur est invité à entrer un code confidentiel, car la fonctionnalité d'authentification unique n'est pas disponible dans ce déploiement.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

Ce déploiement implique des machines utilisateur n'appartenant pas au domaine pouvant exécuter Desktop Lock et se connecter à StoreFront via des sites Desktop Appliance.

Desktop Lock est un composant distinct fourni avec XenApp, XenDesktop et VDI-in-a-Box. Il constitue une alternative à Desktop Viewer et il est conçu principalement pour les ordinateurs Windows réaffectés et les clients légers Windows. Desktop Lock remplace le shell Windows et le Gestionnaire des tâches dans ces machines utilisateur, ce qui empêche les utilisateurs d'accéder à des machines sous-jacentes. Grâce à Desktop Lock, les utilisateurs peuvent accéder aux bureaux Windows Server Machine et aux bureaux Windows Desktop Machine. l'installation de Desktop Lock est facultative.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

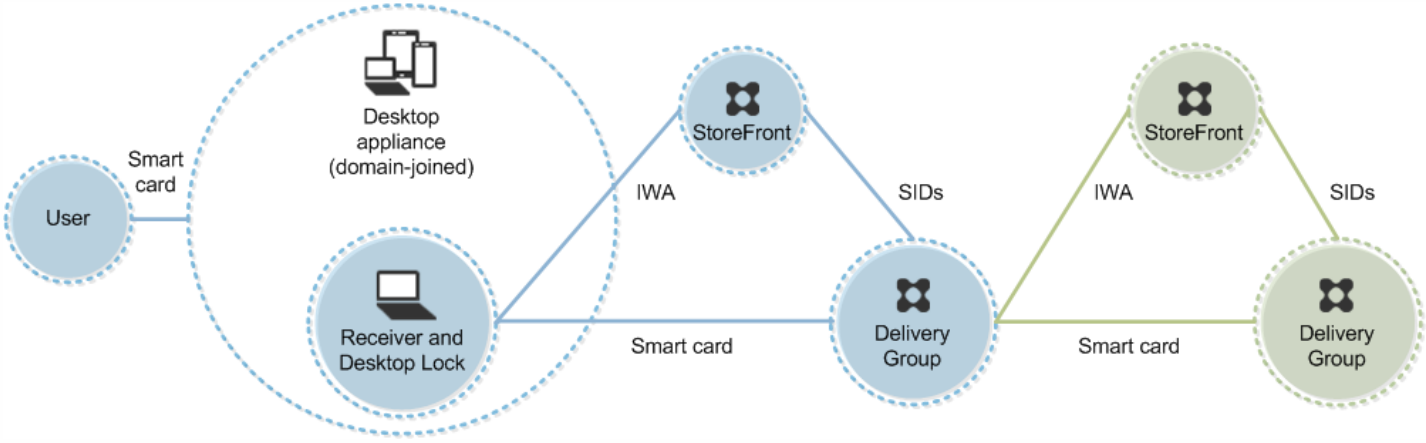


Un utilisateur ouvre une session sur une machine avec une carte à puce. Si Desktop Lock est en cours d'exécution sur la machine, celle-ci est configurée pour démarrer un site Desktop Appliance au travers d'Internet Explorer exécuté en mode Kiosque. Un contrôle ActiveX présent sur le site invite l'utilisateur à entrer un code confidentiel, et l'envoie à StoreFront. StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à XenApp ou XenDesktop. Le premier bureau disponible de la liste alphabétique d'un groupe de bureaux attribué démarre.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

Ce déploiement implique des machines utilisateur appartenant à un domaine qui exécutent Desktop Lock et se connectent à StoreFront via les adresses URL XenApp Services.

Desktop Lock est un composant distinct fourni avec XenApp, XenDesktop et VDI-in-a-Box. Il constitue une alternative à Desktop Viewer et il est conçu principalement pour les ordinateurs Windows réaffectés et les clients légers Windows. Desktop Lock remplace le shell Windows et le Gestionnaire des tâches dans ces machines utilisateur, ce qui empêche les utilisateurs d'accéder à des machines sous-jacentes. Grâce à Desktop Lock, les utilisateurs peuvent accéder aux bureaux Windows Server Machine et aux bureaux Windows Desktop Machine. l'installation de Desktop Lock est facultative.



Un utilisateur ouvre une session sur une machine à l'aide d'une carte à puce et du code confidentiel. Si Desktop Lock est en

© 1999-2017 Citrix Systems, Inc. All rights reserved.

cours d'exécution sur la machine, il authentifie l'utilisateur à un serveur StoreFront à l'aide de l'authentification Windows intégrée (IWA). StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à XenApp ou XenDesktop. Lorsque l'utilisateur démarre un bureau virtuel, l'utilisateur n'est pas invité à entrer un code confidentiel, car la fonctionnalité d'authentification unique est configurée sur Receiver.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Authentification unique et single sign-on avec des cartes à puce

Jul 07, 2016

L'authentification unique avec des cartes à puce sur les bureaux virtuels est prise en charge sur les machines utilisateur exécutant Windows 10, Windows 8 et Windows 7 SP1, éditions Enterprise et Professional.

L'authentification unique avec des cartes à puce sur les applications hébergées est prise en charge sur les serveurs exécutant Windows Server 2008 et Windows Server 2012.

Pour utiliser l'authentification unique avec des applications hébergées sur des cartes à puce, vous devez activer l'utilisation de Kerberos lorsque vous configurez Authentification unique avec carte à puce comme méthode d'authentification pour le site.

Remarque : la disponibilité de l'authentification unique avec des cartes à puce dépend de nombreux facteurs, notamment, mais pas exclusivement :

- les stratégies de sécurité de votre organisation concernant l'authentification unique.
- Type et configuration de logiciels intermédiaires.
- Types de lecteur de carte à puce.
- Stratégie de mise en cache du code confidentiel de logiciels intermédiaires.

L'authentification unique avec des cartes à puce est configurée sur Citrix StoreFront. Consultez la section *— Configurer le service d'authentification* dans la documentation de StoreFront pour plus de détails.

Citrix Single Sign-On est une fonctionnalité qui implémente l'authentification unique lors du lancement de bureaux virtuels et d'applications. Vous pouvez utiliser cette fonctionnalité dans des déploiements de carte à puce, appartenant à un domaine, direct-to-StoreFront et appartenant à un domaine, NetScaler-to-StoreFront pour réduire le nombre de fois où les utilisateurs entrent leur code confidentiel. Pour utiliser l'authentification unique dans ces types de déploiement, modifiez les paramètres suivants dans le fichier default.ica, qui se trouve sur le serveur StoreFront :

- Déploiements de carte à puce appartenant à un domaine, directement vers StoreFront : définissez DisableCtrlAltDel sur Off
- Déploiements de carte à puce appartenant à un domaine, NetScaler vers StoreFront : définissez UseLocalUserAndPassword sur On

Pour obtenir des instructions sur la configuration de ces paramètres, consultez la documentation de StoreFront ou NetScaler Gateway.

La disponibilité de la fonctionnalité d'authentification unique dépend de nombreux facteurs, notamment, mais pas exclusivement :

- Les stratégies de sécurité de votre organisation relatives à l'authentification unique.
- Type et configuration de logiciels intermédiaires.
- Types de lecteur de carte à puce.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Stratégie de mise en cache du code confidentiel de logiciels intermédiaires.

Remarque : lorsque l'utilisateur ouvre une session sur Virtual Delivery Agent (VDA) sur une machine lorsqu'un lecteur de carte à puce est connecté, une mosaïque Windows peut sembler représenter le mode d'authentification précédent réussi, tel qu'une carte à puce ou un mot de passe. Par conséquent, lorsque l'authentification unique est activée, la mosaïque d'authentification unique peut s'afficher. Pour ouvrir une session, l'utilisateur doit sélectionner Changer d'utilisateurs pour sélectionner une autre mosaïque car la mosaïque d'authentification unique ne fonctionne pas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Transport Layer Security (TLS)

Aug 22, 2016

La configuration d'un site XenApp ou XenDesktop pour utiliser le protocole TLS (Transport Layer Security) de sécurité inclut les procédures suivantes :

- Obtenir, installer et enregistrer un certificat de serveur sur tous les Delivery Controller, et configurer un port avec le certificat SSL. Pour de plus amples informations, consultez la rubrique Installer les certificats de serveur TLS sur des Controller.
  Si vous le souhaitez, vous pouvez modifier les ports que le Controller utilise pour écouter le trafic HTTP et HTTPS.

- Activez les connexions TLS entre les utilisateurs et Virtual Delivery Agents (VDA) en renseignant les tâches suivantes :
  - Configurez TLS sur les machines où le VDA est installé. (Par commodité, les références supplémentaires sur les machines sur lesquelles les VDA sont installés sont simplement appelées « VDA ») Vous pouvez utiliser un script PowerShell fourni par Citrix, ou le configurer manuellement. Pour de plus amples informations, consultez la section À propos des paramètres TLS sur les VDA. Pour de plus amples informations, consultez la section Configurer TLS sur un VDA à l'aide du script PowerShell et Configurer manuellement TLS sur un VDA.
  - Configurez SSL dans les groupes de mise à disposition contenant les VDA en exécutant un jeu de cmdlets PowerShell dans Studio. Pour de plus amples informations, consultez la section Configurer TLS sur les groupes de mise à disposition.

  Configuration requise et considérations :
  - L'activation des connexions TLS entre les utilisateurs et les VDA est valide uniquement pour les sites XenApp 7.6 et XenDesktop 7.6, ainsi que les versions ultérieures prises en charge.
  - Configurez TLS dans les groupes de mise à disposition et le VDA après l'installation de composants, créez un site, créez des catalogues de machines, et créez des groupes de mise à disposition.
  - Pour configurer TLS dans les groupes de mise à disposition, vous devez disposer de l'autorisation de modification des règles d'accès de Controller ; un administrateur complet possède ces permissions.
  - Pour configurer TLS sur les VDA, vous devez être un administrateur Windows sur la machine sur laquelle le VDA est installé.
  - Si vous prévoyez de configurer TLS sur les VDA qui ont été mis à niveau à partir de versions antérieures, désinstallez tous les relais SSL sur ces machines avant de les mettre à niveau.
  - Le script PowerShell permet de configurer TLS sur les VDA statiques ; il ne configure pas TLS sur les VDA regroupés qui sont provisionnés par Machine Creation Services ou Provisioning Services, où l'image de la machine cliente est réinitialisée à chaque redémarrage.

Pour les tâches qui incluent l'utilisation du registre Windows :
Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.
Pour plus d'informations sur l'activation de TLS pour la base de données du site, consultez la section CTX137556.

Pour HTTPS, Le service XML prend en charge les fonctionnalités TLS par le biais de certificats de serveur mais pas de certificats de client. Pour obtenir, installer et enregistrer un certificat sur un Controller, et pour configurer un port avec le certificat SSL :

- Si IIS est installé sur le Controller, suivez les instructions dans https://technet.microsoft.com/en-us/library/cc771438%28v=ws.10%29.aspx.
- Si IIS n'est pas installé sur le Controller, le certificat pourrait être configuré comme suit :
  1. Procurez-vous un certificat de serveur SSL et installez-le sur le Controller comme décrit dans l'article http://blogs.technet.com/b/pki/archive/2009/08/05/how-to-create-a-web-server-ssl-certificate-manually.aspx. Pour plus d'informations sur l'outil certreq, consultez l'article http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx.
     Si vous prévoyez d'utiliser le script PowerShell pour configurer TLS sur VDA, et sauf si vous prévoyez de spécifier l'empreinte numérique du certificat SSL, vérifiez que le certificat est présent dans la zone Ordinateur local > Personnel > Certificats du magasin de certificats. Si plusieurs certificats résident à cet emplacement, le premier détecté sera utilisé.
  2. Configurez un port avec le certificat ; consultez http://msdn.microsoft.com/fr-fr/library/ms733791%28v=vs.110%29.aspx.

Par défaut, le service XML du Controller écoute le trafic HTTP sur le port 80 et le trafic HTTPS sur le port 443. Bien que vous puissiez utiliser des ports différents de ceux par défaut, n'oubliez pas les risques de sécurité relatifs à l'exposition d'un Controller à des réseaux non approuvés. Le déploiement d'un serveur StoreFront autonome est préférable à la modification des valeurs par défaut.
Pour modifier la valeur par défaut des ports HTTP ou HTTPS utilisés par le Controller, exécutez la commande suivante à partir de Studio : BrokerService.exe -WIPORT <http-port> -WISSLPORT <https-port>

où <http-port> est le numéro de port pour le trafic HTTP et <https-port> le numéro de port pour le trafic HTTPS.

Remarque : après avoir modifié un port, il se peut que Studio affiche un message sur la compatibilité et la mise à niveau des licences. Pour résoudre le problème, ré-enregistrez les instances de service à l'aide de la séquence de l'applet de commande PowerShell suivante :
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS | Unregister-ConfigRegisteredServiceInstance Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" | Regist

Si vous souhaitez que le service XML ignore le trafic HTTP, définissez la valeur de registre suivante sur le Controller dans HKLM\Software\Citrix\DesktopServer\ et redémarrez le service Broker.

Pour ignorer le trafic HTTP, définissez XmlServicesEnableNonSsl sur 0.

Il existe une valeur de registre correspondant pour ignorer le trafic HTTPS : XmlServicesEnableSsl. Assurez-vous qu'elle n'est pas définie sur 0.

Lorsque vous configurez le protocole TLS sur les VDA, il modifie les autorisations sur le certificat SSL installé, offrant au service ICA un accès en lecture à la clé privée du certificat, et informant le service ICA des opérations suivantes :

- **Quel certificat utiliser dans le magasin de certificat à utiliser pour TLS**.
- **Quel numéro de port TCP utiliser pour les connexions TLS**.
  Le Pare-feu Windows (s'il est activé) doit être configuré pour autoriser les connexions entrantes sur ce port TCP. Cette configuration est effectuée pour vous si vous utilisez le script PowerShell.

- **Quelles sont les versions du protocole TLS à autoriser**.

> **Important**
>
> Citrix recommande aux clients de vérifier leur utilisation de SSLv3 et de prendre des mesures pour reconfigurer leurs déploiements pour supprimer la prise en charge de SSLv3, le cas échéant. Veuillez consulter l'article CTX200238.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Les versions prises en charge du protocole TLS suivent une hiérarchie (de la plus basse à la plus élevée) : SSL 3.0, TLS 1.0, TLS 1.1 et TLS 1.2. Vous devez spécifier la version minimale autorisée ; toutes les connexions de protocole utilisant cette version ou une version supérieure sont autorisées.

Par exemple, si vous spécifiez TLS 1.1 comme version minimale, les connexions de protocole TLS 1.1 et TLS 1.2 sont autorisées. Si vous spécifiez SSL 3.0 en tant que version minimale, les connexions pour toutes les versions prises en charge sont alors autorisées. Si vous spécifiez TLS 1.2 comme version minimale, seules les connexions TLS 1.2 sont autorisées.

- **Quels chiffrements TLS sont autorisés**.
  Une suite de chiffrement est une liste de chiffrements TLS courants. Lorsqu'un client se connecte et envoie une liste de chiffrements TLS pris en charge, le VDA fait correspondre le chiffrement d'un client avec l'un des chiffrements de sa suite de chiffrement configurée et accepte la connexion. Si le client envoie un chiffrement qui n'est pas dans la suite de chiffrement du VDA, le VDA rejette la connexion.

  Trois suites de chiffrement sont prises en charge : GOV(ernment), COM(mercial), et ALL. Les chiffrements des suites de chiffrement dépendent du mode FIPS Windows ; voir http://support2.microsoft.com/kb/811833/fr pour plus d'informations sur le mode FIPS Windows. Le tableau suivant répertorie les chiffrements de chaque suite de chiffrement prise en charge.

Suite de chiffrement TLS	GOV	COM	ALL	GOV	COM	ALL
Mode FIPS	Off	Off	Off	On	On	On
RSA_KEYX	x	x	x	x	x	x
RSA_SIGN	x	x	x	x	x	x
3DES	x		x	x		x
RC4		x	x			
MD5	x	x	x			
SHA	x	x	x	x	x	x
SHA_256	x	x	x	x	x	x
SHA_384	x	x	x	x	x	x
SHA_512	x	x	x	x	x	x
AES	x	x	x	x	x	x

Un groupe de mise à disposition ne peut pas avoir un mélange d'un VDA avec TLS configuré et d'autres VDA sans TLS configuré. Lorsque vous configurez le protocole TLS pour un groupe de mise à disposition, vous devez avoir déjà configuré TLS pour tous les VDA dans ce groupe de mise à disposition.

Le script Enable-VdaSSL.ps1 active ou désactive l'écouteur TLS sur un VDA. Ce script est disponible dans le dossier Support > Tools > SslSupport sur le support d'installation.

Lorsque vous activez le protocole TLS, le script désactive toutes les règles du Pare-feu Windows existantes pour le port TCP spécifié avant d'ajouter une règle qui permet au service ICA d'accepter des connexions entrantes sur le port TCP TLS uniquement. Cela désactive également les règles du Pare-feu Windows pour :

- Citrix ICA 1494 (valeur par défaut : 8008)
- Citrix CGP 2598 (valeur par défaut : 8008)
- Citrix WebSocket 8008 (valeur par défaut : 8008)

Le résultat est que les utilisateurs peuvent se connecter uniquement via TLS ; ils ne peuvent pas utiliser de données brutes ICA, CGP ou WebSocket pour se connecter.

Le script contient des descriptions de la syntaxe suivante, ainsi que d'autres exemples ; vous pouvez utiliser un outil tel que le Bloc-notes++ pour consulter ces informations.

Vous devez spécifier le paramètre –Enable ou –Disable ; tous les autres paramètres sont facultatifs.

Syntaxe

Enable-VdaSSL {-Enable | -Disable} [–SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"<suite>"] [-CertificateThumbPrint "<thumbprint>"]

Paramètre	**Description**
-Enable	Installe et active l'écouteur TLS sur le VDA. Soit ce paramètre ou le paramètre -Disable est requis.
-Disable	Désactive l'écouteur TLS sur le VDA. Soit ce paramètre ou le paramètre –Enable est requis. Si vous spécifiez ce paramètre, aucun autre paramètre n'est valide.
–SSLPort <port>	Port TLS. Valeur par défaut : 443
-SSLMinVersion “<version-ssl-min>”	Version minimale du protocole TLS, entourés de guillemets. Les valeurs valides sont : « SSL_3.0 », « TLS_1.0 », « TLS_1.1 » et « TLS_1.2 ». Valeur par défaut: « TLS_1.0 » **Important** : Citrix recommande aux clients de vérifier leur utilisation de SSLv3 et de prendre des mesures pour reconfigurer leurs déploiements pour supprimer la prise en charge de SSLv3, le cas échéant. Veuillez consulter l'article CTX200238.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètre	Description
-SSLCipherSuite « <suite> »	Suite de chiffrement TLS, entourés de guillemets. Les valeurs valides sont : « GOV », « COM » et « ALL ». Valeur par défaut : « ALL »
-CertificateThumbPrint « <empreinte> »	Empreinte numérique du certificat SSL dans le magasin de certificats, entourée de guillemets. Ce paramètre est généralement utilisé lorsque le magasin de certificats possède plusieurs certificats, le script utilise l'empreinte numérique pour sélectionner le certificat que vous voulez utiliser. Valeur par défaut : le premier certificat disponible détecté dans la zone Ordinateur local > Personnel > Certificats du magasin de certificats.

Exemples

Le script suivant installe et active la version de protocole TLS 1.2.
Enable-VdaSSL –Enable
Le script suivant installe et active l'écouteur TLS et spécifie le port TLS 400, la suite de chiffrement GOV et une valeur de protocole minimale TLS 1.2 SSL.
Enable-VdaSSL – Enable –SSLPort 400 'SSLMinVersion "TLS_1.2" –SSLCipherSuite "GOV"
Le script suivant désactive l'écouteur TLS sur le VDA.
Enable-VdaSSL –Disable

Lors de la configuration manuelle de TLS sur un VDA, vous offrez un accès en lecture générique à la clé privée du certificat TLS pour le service approprié sur chaque VDA : NT SERVICE\PorticaService pour un VDA pour OS Windows Desktop, ou NT SERVICE\TermService pour un VDA pour OS Windows Server. Sur la machine sur laquelle le VDA est installé :

1. Lancer la console MMC (Microsoft Management Console) : Démarrer > Exécuter > mmc.exe.
2. Ajouter le composant logiciel enfichable Certificats à la console MMC :
   1. Sélectionner Fichier > Ajouter/Supprimer un composant logiciel enfichable.
   2. Sélectionnez Certificats et cliquez sur Ajouter.
   3. Lorsque vous y êtes invité par « Ce composant logiciel enfichable gérera toujours les certificats pour : », choisissez « Le compte d'ordinateur », puis cliquez sur Suivant.
   4. Lorsque vous y êtes invité par « Sélectionnez l'ordinateur à gérer par ce composant logiciel enfichable », choisissez « Ordinateur local », puis cliquez sur Terminer.
3. Sous Certificats (Ordinateur local) > Personnel > Certificats, cliquez avec le bouton droit de la souris sur le certificat, puis sélectionnez Toutes les tâches > Gérer les clés privées.
4. L'Éditeur de liste de contrôle d'accès affiche « Autorisations pour les clés privées (NomConvivial) » où (NomConvivial) est le nom de votre certificat SSL. Ajoutez l'un des services suivants et accordez-lui un accès en lecture :
   - Pour un VDA pour OS Windows Desktop, « PORTICASERVICE »
   - Pour un VDA pour OS de serveur Windows, « TERMSERVICE »
5. Cliquez deux fois sur le certificat SSL installé. Dans la boîte de dialogue du certificat, sélectionnez l'onglet Détails, puis faites défiler vers le bas. Cliquez sur Empreinte numérique.
6. Exécutez la commande regedit et rendez-vous sur HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.
   1. Modifier la clé d'empreinte numérique SSL et copiez la valeur de l'empreinte numérique du certificat SSL dans cette valeur binaire. Vous pouvez ignorer sans risque les éléments inconnus dans la boîte de dialogue Modifier la valeur binaire (tels que '0000' et les caractères spéciaux).
   2. Modifier la clé SSLEnabled et modifiez la valeur DWORD sur 1. (Pour désactiver SSL ultérieurement, changez la valeur DWORD sur 0).
   3. Si vous souhaitez modifier les paramètres par défaut (facultatif), utilisez les informations suivantes dans le même chemin d'accès du Registre :
      - SSLPort DWORD : numéro de port SSL. Valeur par défaut : 443.
      - SSLMinVersion DWORD : 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2. Valeur par défaut : 2 (TLS 1.0).
      - SSLCipherSuite DWORD : 1 = GOV, 2 = COM, 3 = ALL. Valeur par défaut : 3 (ALL).
7. Assurez-vous que le port TCP TLS est ouvert dans le Pare-feu Windows s'il n'est pas la valeur par défaut (443). (Lors de la création de la règle de trafic entrant dans le Pare-feu Windows, assurez-vous que ses propriétés possèdent les entrées sélectionnées « Autoriser la connexion » et « Activé ».)
8. Assurez-vous qu'aucune autre application ou service (tel que IIS) utilisent le port TCP TLS.
9. Pour les VDA pour OS Windows Server, redémarrez la machine pour que les modifications prennent effet. (Il n'est pas nécessaire de redémarrer les machines contenant des VDA pour OS Windows Desktop).

Effectuez cette procédure pour chaque groupe de mise à disposition qui contient les VDA vous avez configurés pour les connexions TLS.

1. À partir de Studio, ouvrez la console PowerShell.
2. Exécutez asnp Citrix.* pour charger les applets de commande du produit Citrix.
3. Exécutez Get-BrokerAccessPolicyRule -DesktopGroupName '<delivery-group-name>' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true.
   où <groupe-mise-à-disposition> est le nom du groupe de mise à disposition contenant les VDA.
4. Exécutez Set-BrokerSite -DnsResolutionEnabled $true.

Si une erreur de connexion se produit, consultez le journal des événements système du VDA.

Lors de l'utilisation de Receiver pour Windows, si vous recevez une erreur de connexion (comme 1030) qui indique une erreur TLS, désactivez Desktop Viewer, puis essayez de vous reconnecter, bien que la connexion échoue toujours, une description du problème TLS sous-jacent peut être fournie (par exemple, vous avez spécifié un modèle incorrect lors de la demande d'un certificat auprès de l'autorité de certification).

Communications entre le Controller et le VDA

Les communications entre le Controller et le VDA sont sécurisées par la protection des messages de Windows Communication Framework (WCF). Une protection supplémentaire au niveau du transport à l'aide de TLS n'est pas requise. La configuration WCF utilise Kerberos pour l'authentification mutuelle entre le Controller et le VDA. Le cryptage utilise AES en mode CBC avec une clé 256 bits. L'intégrité des messages est assurée par SHA-1.

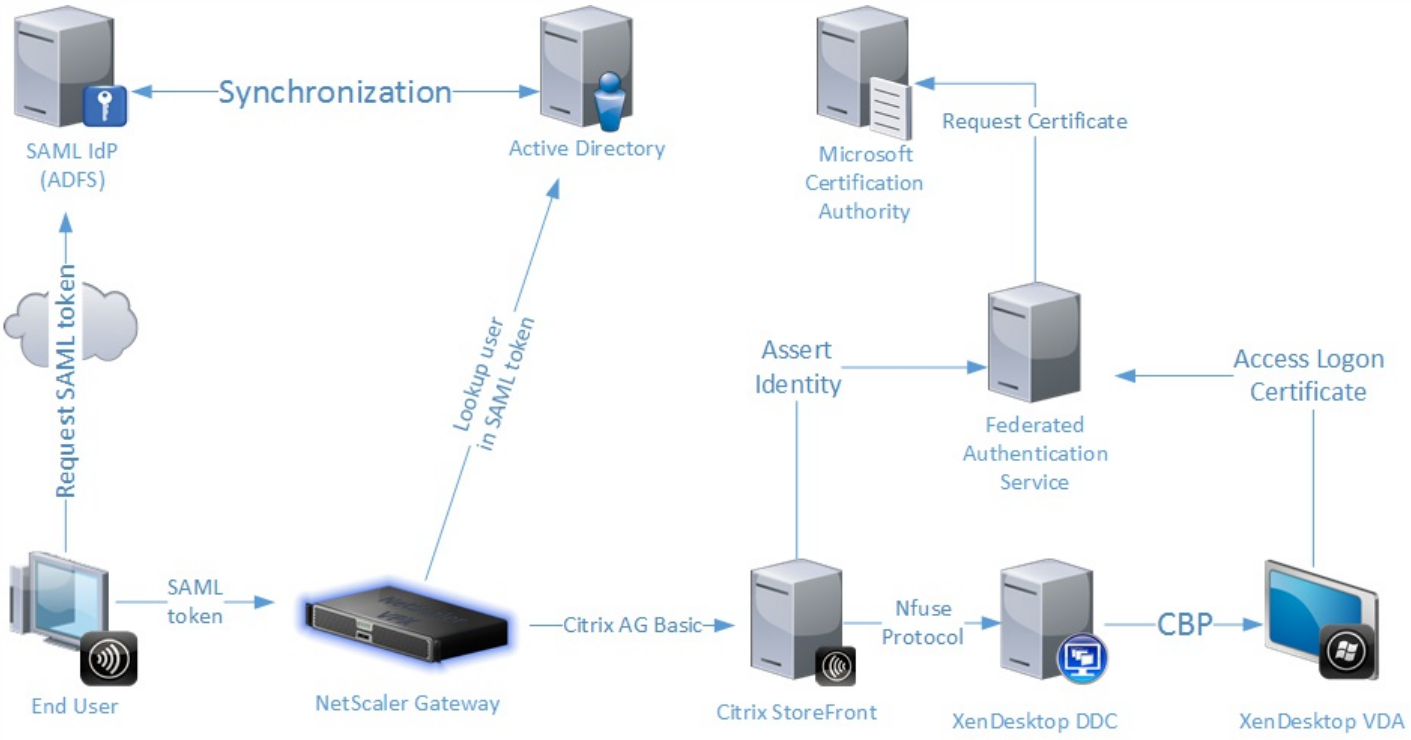
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Service d'authentification fédérée

Jul 13, 2016

Le Service d'authentification fédérée de Citrix est un composant doté de privilèges conçu pour s'intégrer avec les Services de certificats Active Directory. Il émet des certificats pour les utilisateurs de manière dynamique, ce qui leur permet de se connecter à un environnement Active Directory comme s'ils avaient une carte à puce. Cela permet à StoreFront d'utiliser un éventail plus large d'options d'authentification, telles que les assertions SAML (Security Assertion Markup Language). SAML est généralement utilisé comme une alternative aux comptes utilisateur Windows traditionnels sur Internet.

Le diagramme suivant illustre l'intégration du Service d'authentification fédérée avec une autorité de certification Microsoft, ainsi que la fourniture de services de support à StoreFront et aux VDA XenApp et XenDesktop.



Les serveurs StoreFront approuvés contactent le Service d'authentification fédérée (FAS) lorsque les utilisateurs demandent accès à l'environnement Citrix. Le FAS accorde un ticket qui permet à une seule session XenApp ou XenDesktop de s'authentifier avec un certificat pour cette session. Lorsqu'un VDA doit authentifier un utilisateur, il se connecte au FAS utilise le ticket. Seul le FAS a accès à la clé privée du certificat de l'utilisateur ; le VDA doit envoyer au FAS chaque opération de signature et de décryptage opération qu'il doit effectuer avec le certificat.

Configuration requise

Le service d'authentification fédérée est pris en charge sur les serveurs Windows (Windows Server 2008 R2 ou version supérieure).

- Citrix vous recommande d'installer le FAS sur un serveur qui ne contient pas d'autres composants Citrix.
- Le serveur Windows doit être sécurisé. Il aura accès à un certificat d'autorité d'inscription et à une clé privée qui lui

© 1999-2017 Citrix Systems, Inc. All rights reserved.

permettent d'émettre automatiquement des certificats pour les utilisateurs du domaine, et il aura accès à ces certificats utilisateur et clés privées.

Dans le site XenApp ou XenDesktop :

- Les Delivery Controller doivent être à la version minimale 7.9.
- Les VDA doivent être à la version minimale 7.9. Vérifiez que la configuration de la stratégie de groupe Service d'authentification fédérée a été correctement appliquée aux VDA avant de créer le catalogue de machines de la manière habituelle ; consultez la section Configurer une stratégie de groupe pour plus de détails.
- Le serveur StoreFront doit être à la version minimale 3.6 (il s'agit de la version fournie avec l'ISO XenApp et XenDesktop 7.9).

Lors de la planification de votre déploiement de ce service, veuillez consulter la section Considérations de sécurité.

Références :

- Services de certificats Active Directory

  https://technet.microsoft.com/fr-fr/library/hh831740.aspx

- Configuration de Windows pour l'ouverture de session par certificat

  http://support.citrix.com/article/CTX206156

Séquence d'installation et de configuration

1. Installer le service d'authentification fédérée
2. Activer le plug-in Service d'authentification fédérée sur les serveurs StoreFront
3. Configurer une stratégie de groupe
4. Utilisez la console d'administration Service d'authentification fédérée pour : (a) Déployer les modèles fournis, (b) Définir des autorités de certification, et (c) Autoriser le service d'authentification fédérée à utiliser votre autorité de certification
5. Configurer des règles d'utilisateur

Installer le service d'authentification fédérée

Pour des raisons de sécurité, Citrix recommande d'installer le FAS sur un serveur dédié qui est sécurisé de la même manière qu'un contrôleur de domaine ou une autorité de certification. Le FAS peut être installé à partir du bouton **Service d'authentification fédérée** sur l'écran de démarrage autorun lorsque l'ISO est inséré.

Les composants suivants vont être installés :

- Service d'authentification fédérée
- Applets de commande du composant logiciel enfichable PowerShell pour configurer à distance le Service d'authentification fédérée
- Console d'administration du Service d'authentification fédérée.
- Modèles de stratégie de groupe du Service d'authentification fédérée (CitrixFederatedAuthenticationService.admx/adml)
- Fichiers de modèle de certificat pour la configuration de l'autorité de certification
- Compteurs de performances et journaux d'événements

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Activer le plug-in Service d'authentification fédérée sur un magasin StoreFront

Pour activer l'intégration du Service d'authentification fédérée sur un magasin StoreFront, exécutez les applets de commande PowerShell suivantes sous un compte d'administrateur. Si vous disposez de plus d'un magasin, ou si le magasin a un autre nom, le texte du chemin d'accès ci-dessous peut différer.

```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName "FASClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "FASLogonDataProvider"
```

Pour arrêter d'utiliser le FAS, utilisez le script PowerShell suivant :

```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName "standardClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```

Configurer le Delivery Controller

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour utiliser le Service d'authentification fédérée, configurez le Delivery Controller XenApp ou XenDesktop de manière à approuver les serveurs StoreFront qui peuvent s'y connecter : exécutez l'applet de commande PowerShell **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true**.

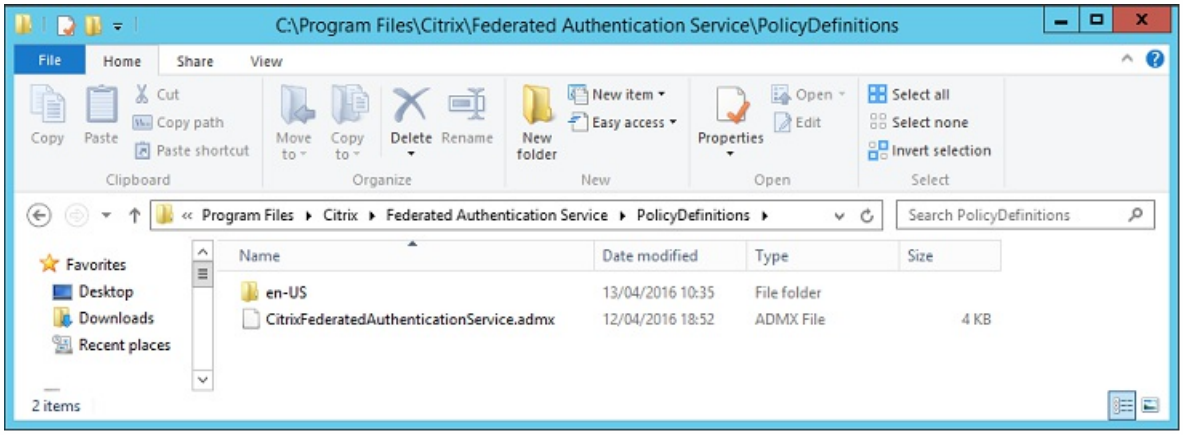
Configurer une stratégie de groupe

Après avoir installé le Service d'authentification fédérée, vous devez spécifier les adresses DNS complètes des serveurs FAS dans une stratégie de groupe à l'aide des modèles de stratégie de groupe fournis dans le cadre de l'installation.

Important : assurez-vous que les serveurs StoreFront qui demandent des tickets et les VDA utilisant des tickets disposent d'adresses DNS identiques, y compris l'attribution automatique de numéros appliquée aux serveurs par l'objet de stratégie de groupe.

À des fins de simplicité, les exemples suivants configurent une seule stratégie au niveau du domaine qui s'applique à toutes les machines ; cependant, cela n'est pas requis. Le FAS fonctionnera tant que les serveurs StoreFront, les VDA, et la machine exécutant la console d'administration FAS voient la même liste d'adresses DNS. Veuillez noter que l'objet de stratégie de groupe ajoute un numéro d'index pour chaque entrée, qui doit également correspondre si plusieurs objets sont utilisés.

Étape 1. Sur le serveur sur lequel vous avez installé le FAS, localisez le fichier C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx et le dossier en-US.

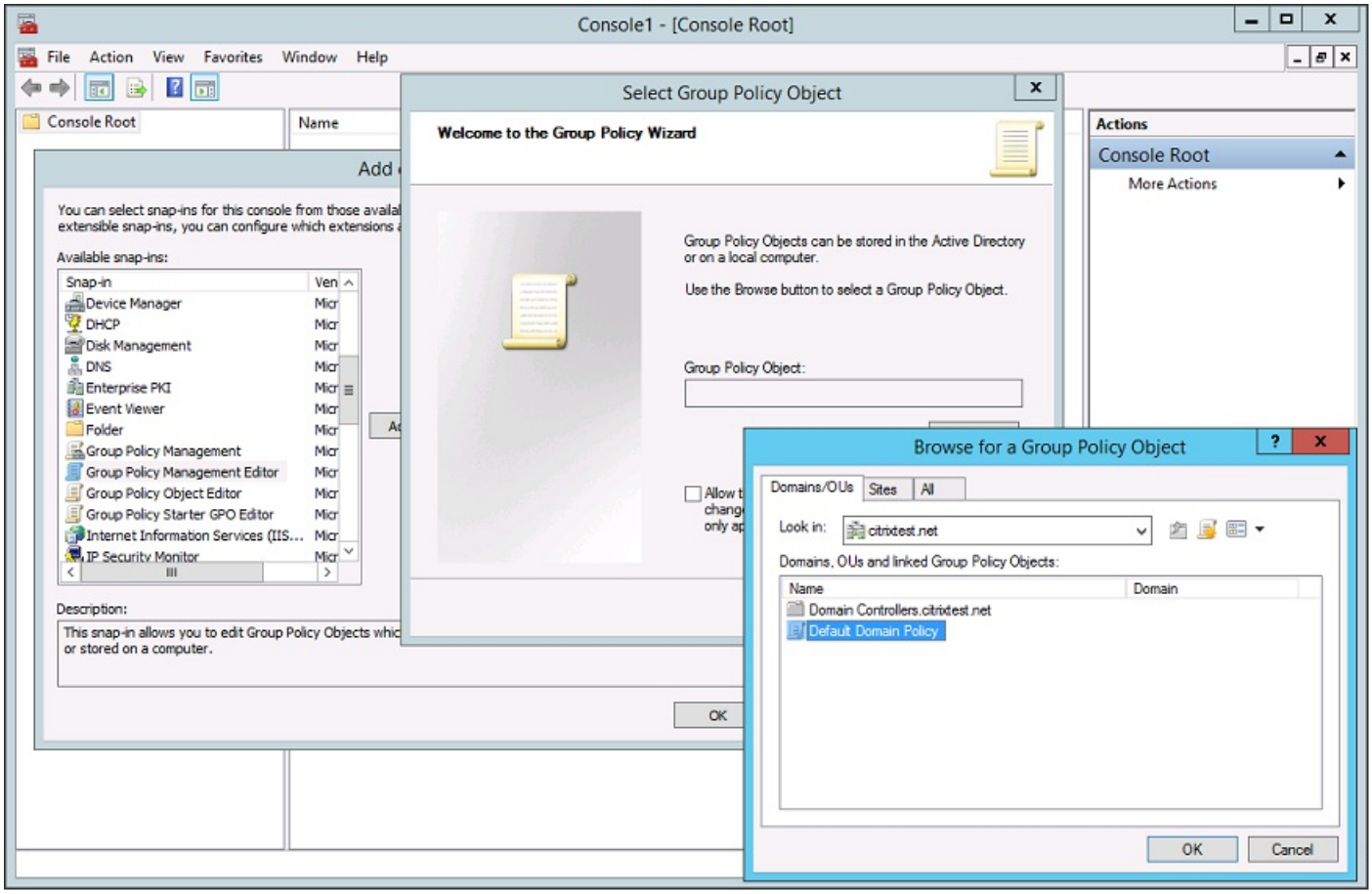


Étape 2. Copiez ces derniers sur votre contrôleur de domaine et placez-les dans C:\Windows\PolicyDefinitions et le sous-dossier en-US.

Étape 3. Exécutez la console Microsoft Management Console (mmc.exe à partir de la ligne de commande). À partir de la barre de menu, sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**. Ajoutez **Éditeur d'objets de stratégie de groupe**.

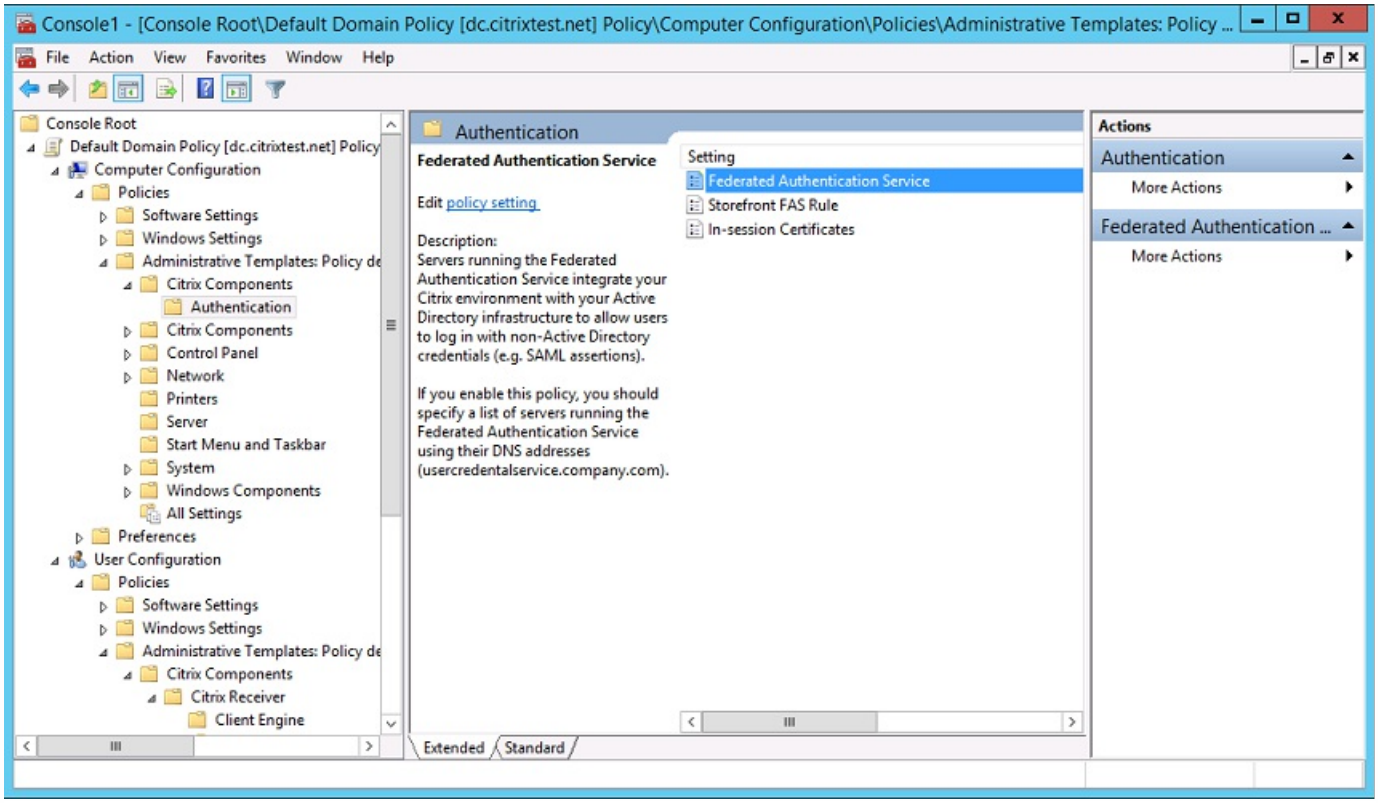
Lorsque vous y êtes invité par un objet de stratégie de groupe, sélectionnez **Parcourir**, puis sélectionnez la **stratégie de domaine par défaut**. Éventuellement, vous pouvez créer et sélectionner un objet de stratégie approprié pour votre environnement, à l'aide des outils de votre choix. La stratégie doit être appliquée à toutes les machines exécutant des logiciels Citrix affectés (VDA, serveurs StoreFront, outils d'administration).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

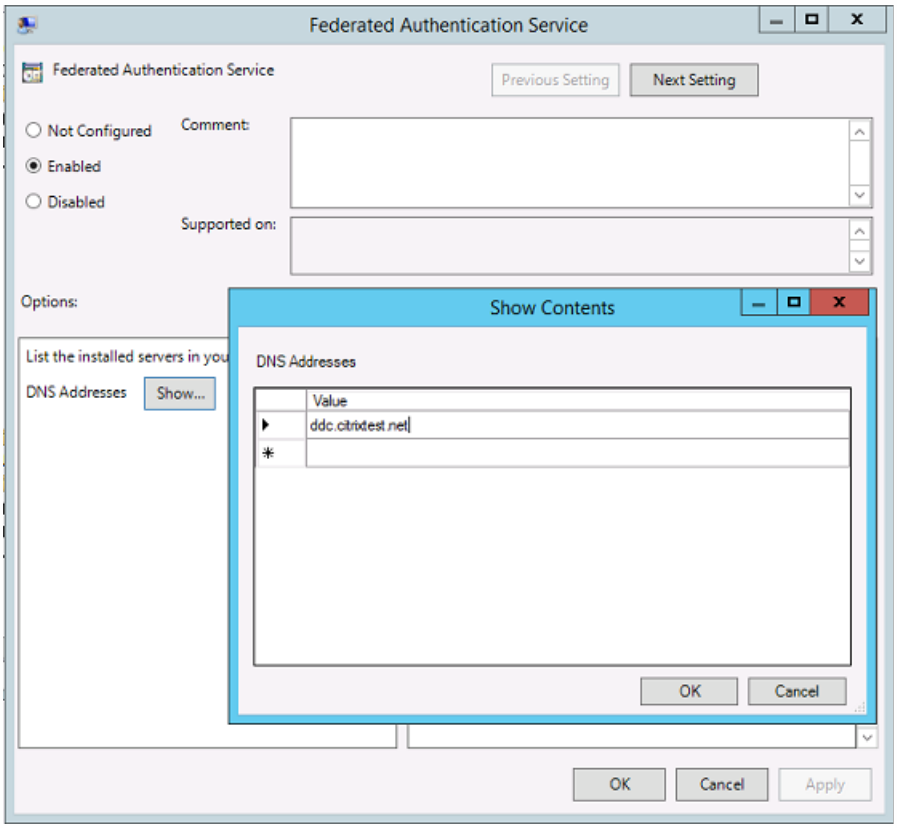


Étape 4. Accédez à la stratégie Service d'authentification fédérée située dans Configuration ordinateur/Stratégies/Modèles d'administration/Composants Citrix/Authentification.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Étape 5. Ouvrez la stratégie Service d'authentification fédérée et sélectionnez **Activé**. Cela vous permet de sélectionner le bouton **Afficher**, dans lequel vous pouvez configurer les adresses DNS de vos serveurs FAS.



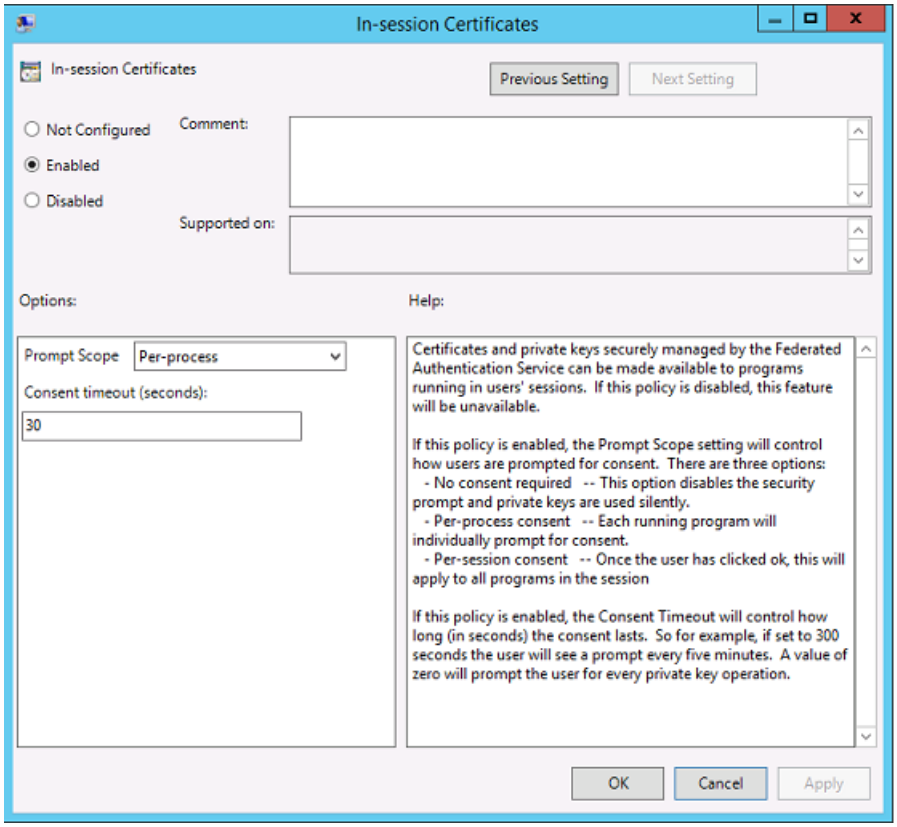
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Étape 6. Entrez les adresses DNS des serveurs hébergeant votre Service d'authentification fédérée.

Rappel : si vous entrez plusieurs adresses, l'ordre de la liste doit être cohérent entre les serveurs StoreFront et les VDA. Cela comprend des entrées vides ou non utilisées.

Étape 7. Cliquez sur **OK** pour quitter l'assistant de stratégie de groupe et appliquer les modifications à la stratégie de groupe. Vous devrez peut-être redémarrer les machines (ou exécuter **gpupdate/force** à partir de la ligne de commande) pour que les modifications prennent effet.

Le modèle de stratégie de groupe prend en charge la configuration du système pour les certificats dans la session. Ceci place les certificats dans le magasin de certificats personnel de l'utilisateur après l'ouverture de session afin que les applications puissent les utiliser. Par exemple, si vous exigez l'authentification TLS pour accéder aux serveurs Web dans la session VDA, le certificat peut être utilisé par Internet Explorer. Par défaut, les VDA n'autoriseront pas l'accès aux certificats après l'ouverture de session.



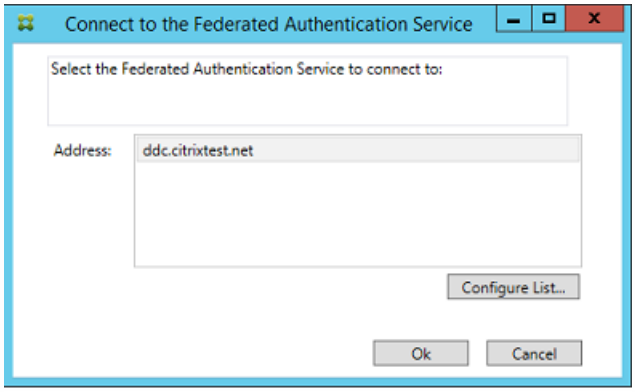
Utilisation de la console d'administration du Service d'authentification fédérée

Le console d'administration du Service d'authentification fédérée est installée dans le cadre du Service d'authentification fédérée. Une icône (Service d'authentification fédérée de Citrix) est placée dans le menu Démarrer.

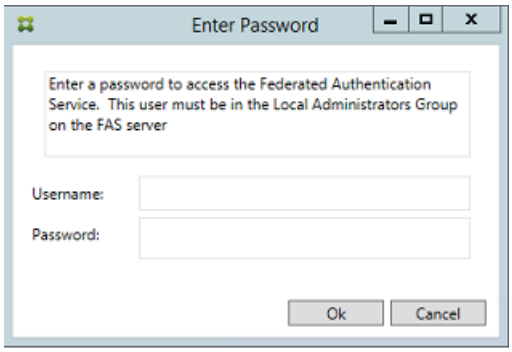
La console tente de localiser automatiquement les serveurs FAS dans votre environnement à l'aide de la configuration de la

© 1999-2017 Citrix Systems, Inc. All rights reserved.

stratégie de groupe. Si cela échoue, consultez la section Configurer une stratégie de groupe.

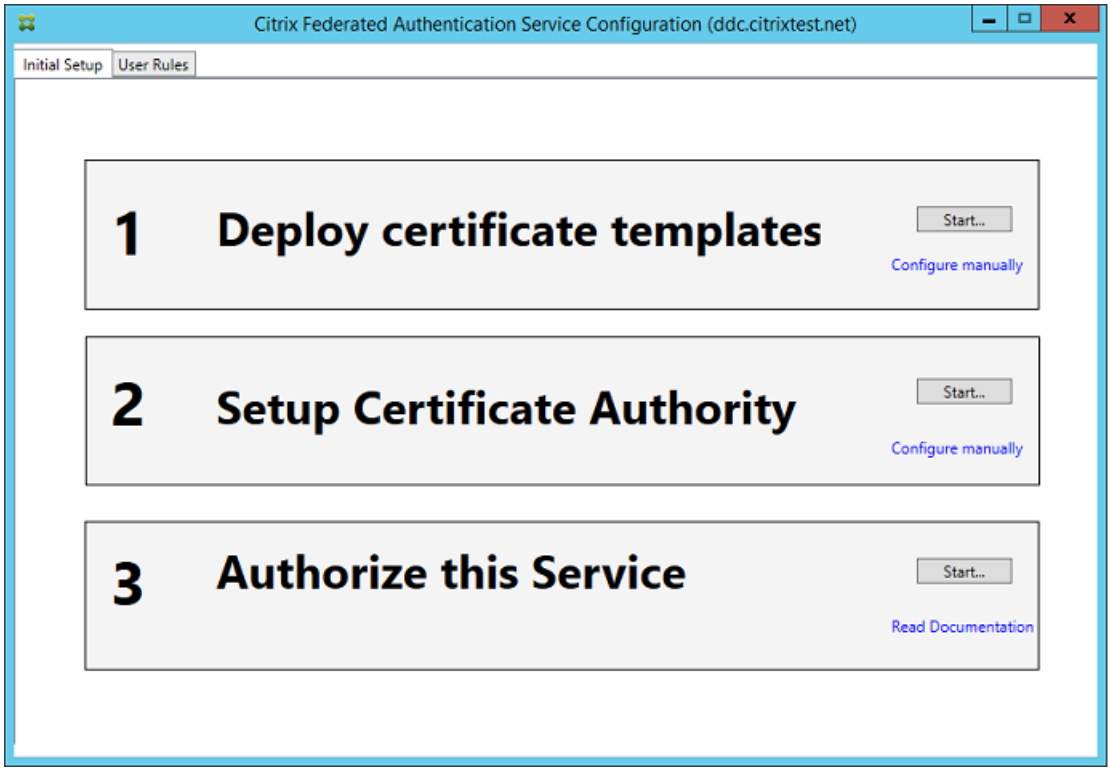


Si votre compte utilisateur n'est pas membre du groupe Administrateurs sur la machine exécutant le Service d'authentification fédérée, vous serez invité à entrer des informations d'identification.



La première fois que la console d'administration est utilisée, elle vous guide au travers d'un processus en trois étapes qui déploie les modèles de certificat, configure l'autorité de certification et autorise le Service d'authentification fédérée à utiliser l'autorité de certification. Certaines des étapes peuvent également être effectuées manuellement à l'aide des outils de configuration du système d'exploitation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

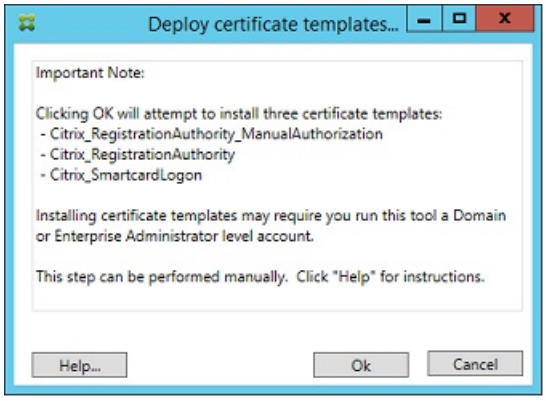


Déployer des modèles de certificat

Pour éviter des problèmes d'interopérabilité avec d'autres logiciels, le Service d'authentification fédérée offre trois modèles de certificats Citrix pour son propre usage.

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

Ces modèles doivent être enregistrés auprès d'Active Directory. Si la console ne peut pas les trouver, l'outil **Déployer des modèles de certificat** peut les installer. Cet outil doit être exécuté sous un compte disposant des autorisations nécessaires pour gérer votre forêt d'entreprise.



La configuration des modèles peut être trouvée dans les fichiers XML avec l'extension .certificatetemplate qui sont installés

© 1999-2017 Citrix Systems, Inc. All rights reserved.

avec le service d'authentification fédérée dans :

C:\Program Files\Citrix\Federated Authentication Service\CertificateTemplates

Si vous ne disposez pas des autorisations nécessaires pour installer ces fichiers modèles, donnez-les à votre administrateur Active Directory.

Pour installer manuellement les modèles, vous pouvez utiliser les commandes PowerShell suivantes :

```
$template = [System.IO.File]::ReadAllBytes("$Pwd\Citrix_SmartcardLogon.certificatetemplate")
 $CertEnrol = New-Object -ComObject X509Enrollment.CX509EnrollmentPolicyWebService
 $CertEnrol.InitializeImport($template)
 $comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)

$writabletemplate = New-Object -ComObject X509Enrollment.CX509CertificateTemplateADWritable
 $writabletemplate.Initialize($comtemplate)
 $writabletemplate.Commit(1, $NULL)
```

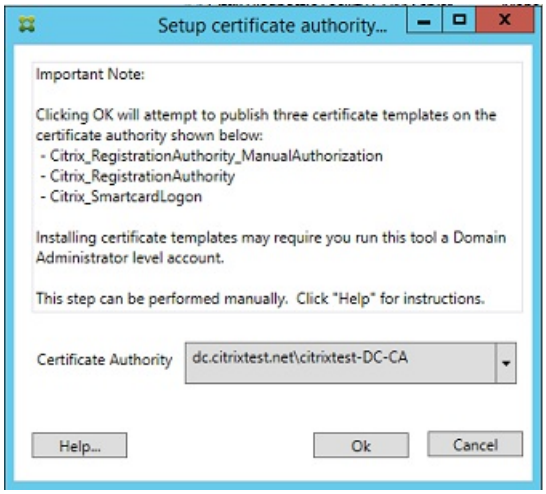
Configurer des services de certificats Active Directory

Après l'installation de modèles de certificats Citrix, ils doivent être publiés sur un ou plusieurs serveurs d'autorité de certification Microsoft. Reportez-vous à la documentation Microsoft sur la manière de déployer des services de certificats Active Directory.

Si les modèles ne sont pas publiés sur au moins un serveur, l'outil **Configurer une autorité de certification** permet de les publier. Vous devez exécuter cet outil en tant qu'utilisateur disposant d'autorisations suffisantes pour gérer l'autorité de certification.

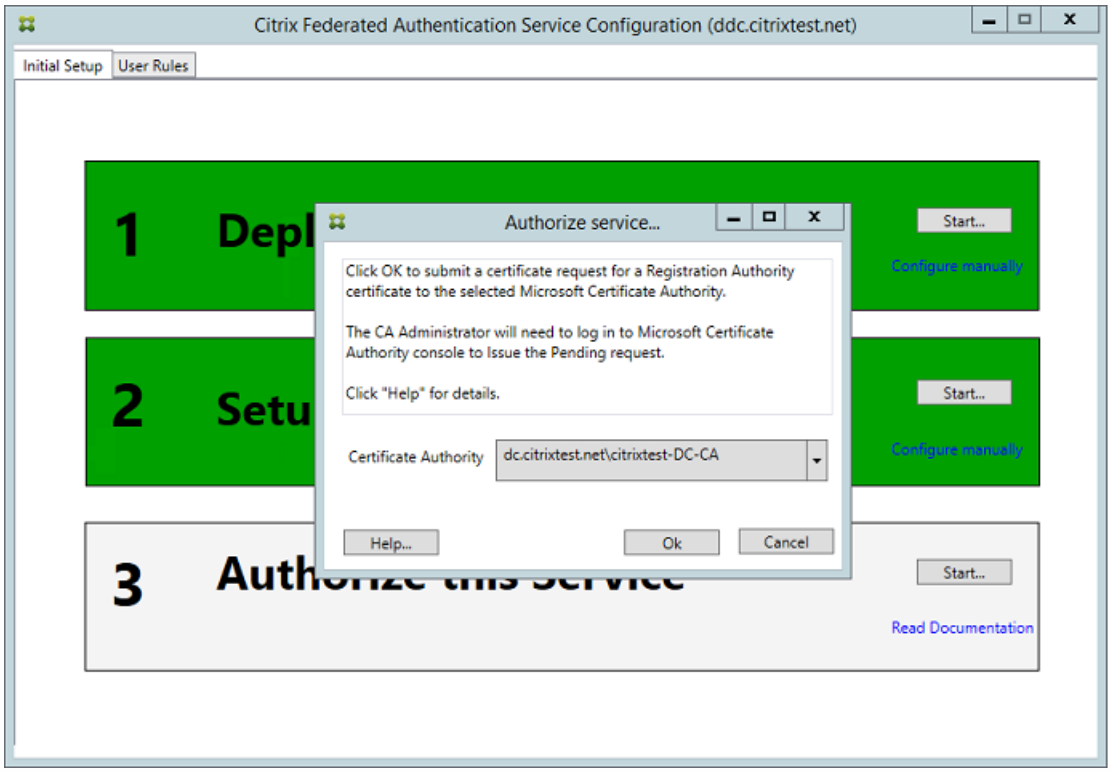
(Les modèles de certificats peuvent également être publiés à l'aide de la console Autorité de certification de Microsoft.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



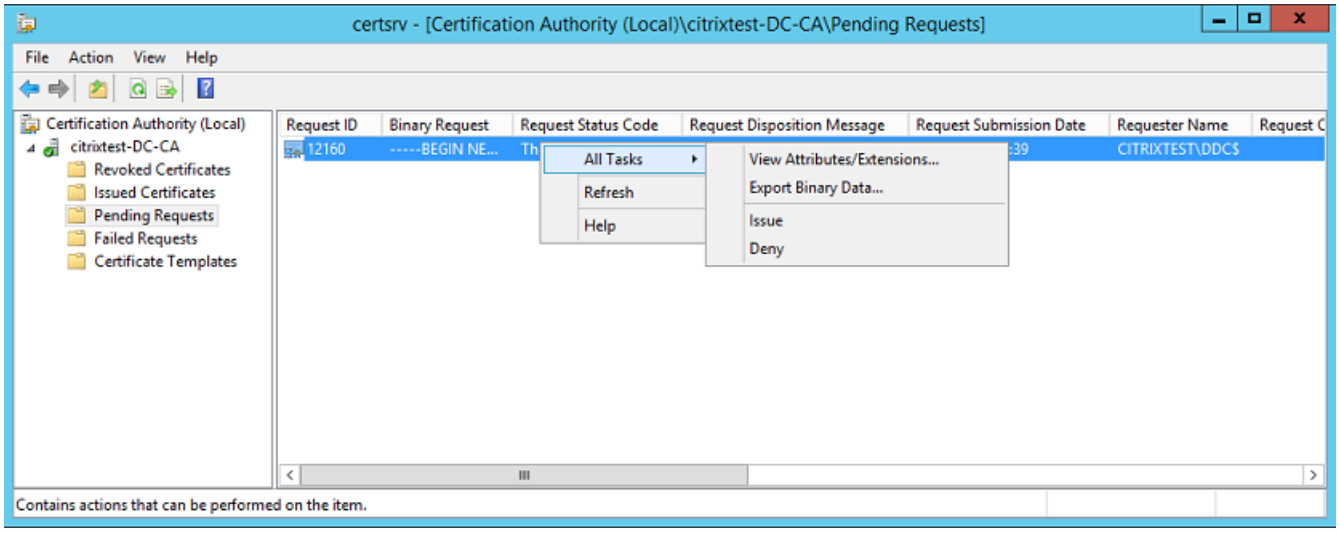
Autoriser le Service d'authentification fédérée

La dernière étape de configuration dans la console initie l'autorisation du Service d'authentification fédérée. La console d'administration utilise le modèle Citrix_RegistrationAuthority_ManualAuthorization pour générer une requête de certificat, puis l'envoie à l'une des autorités de certification qui publient ce modèle.

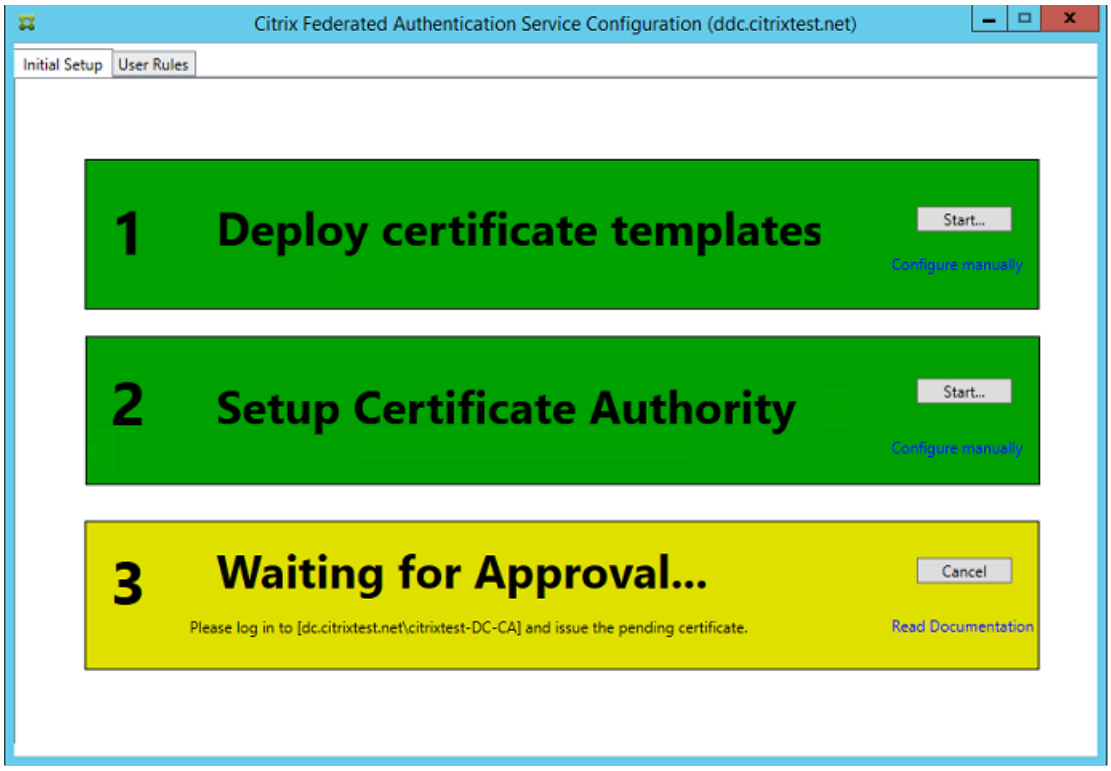


Une fois la requête envoyée, elle apparaît dans la liste **Demandes en attente** de la console Autorité de certification de Microsoft. L'administrateur de l'autorité de certification doit choisir d'**émettre** ou de **rejeter** la requête avant que la configuration du Service d'authentification fédérée puisse continuer. Veuillez noter que la demande d'autorisation s'affiche en tant que **Demande en attente** depuis le compte de la machine FAS.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Cliquez avec le bouton droit sur **Toutes les tâches**, puis sélectionnez **Émettre** ou **Rejeter** pour la demande de certificat. La console d'administration du Service d'authentification fédérée détecte automatiquement lorsque ce processus est terminé. Cette opération peut prendre plusieurs minutes.

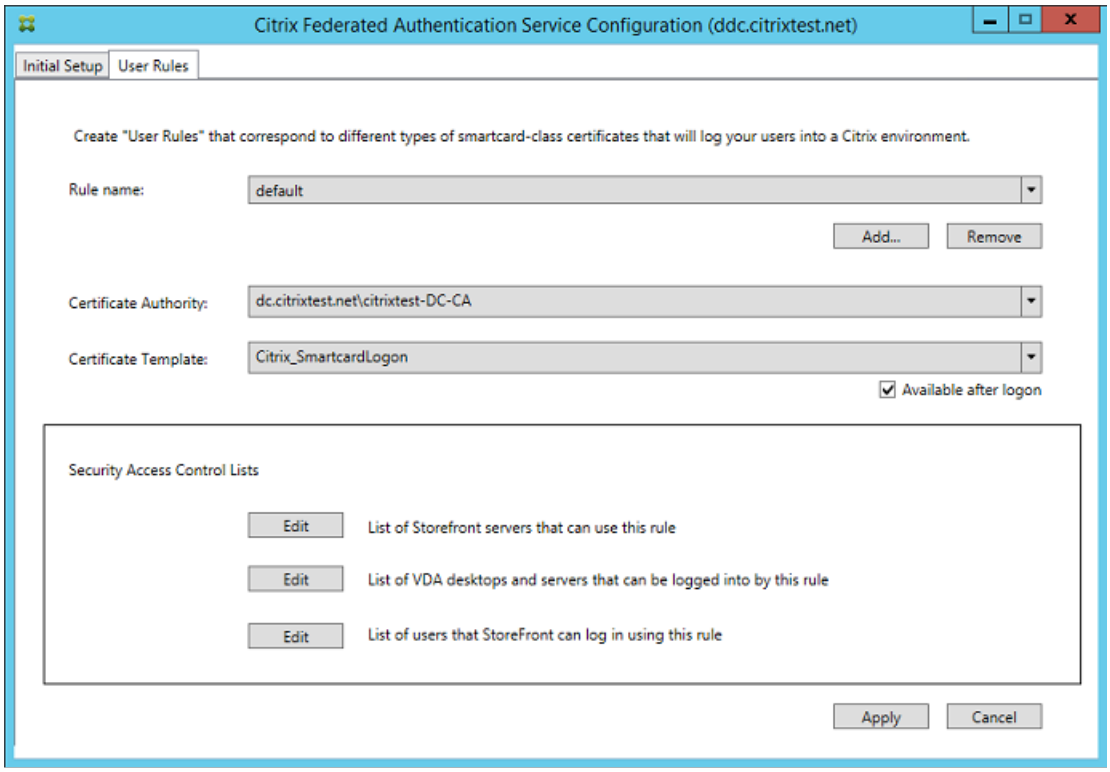


Configurer des règles d'utilisateur

Une règle d'utilisateur autorise l'émission de certificats pour l'ouverture de session sur des VDA et l'utilisation dans la session, conformément aux instructions de StoreFront. Chaque règle spécifie les serveurs StoreFront qui sont approuvés pour demander des certificats, les utilisateurs pour lesquels ils peuvent être demandés, et les VDA autorisés à les utiliser.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour terminer la configuration du Service d'authentification fédérée, l'administrateur doit définir la règle par défaut en basculant sur l'onglet User Rules de la console d'administration FAS, en sélectionnant une autorité de certification sur laquelle publier le modèle Citrix_SmartcardLogon et en modifiant la liste des serveurs StoreFront. La liste des VDA est par défaut Ordinateurs du domaine et la liste des utilisateurs est par défaut Utilisateurs du domaine ; ces informations peuvent être modifiées si les valeurs par défaut ne sont pas appropriées.



Champs :

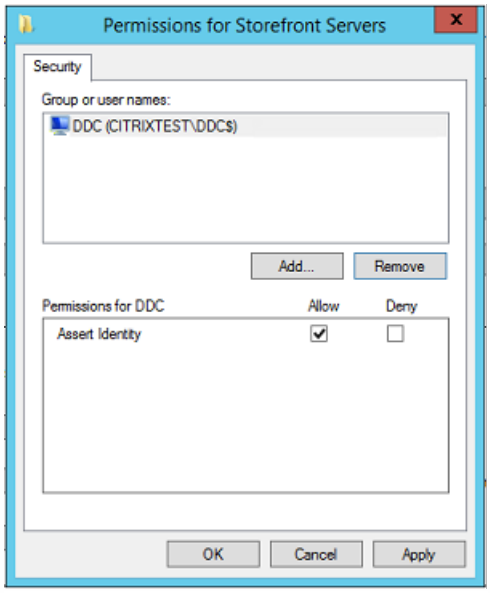
Certificate Authority et Certificate Template : le modèle de certificat et l'autorité de certification qui seront utilisés pour émettre des certificats utilisateur. Il doit s'agir du modèle Citrix_SmartcardLogon, ou d'une copie modifiée de ce dernier, sur l'une des autorités de certification sur laquelle le modèle est publié.

La console FAS prend en charge l'ajout de multiples autorités de certification à des fins de basculement et d'équilibrage de charge, à l'aide de commandes PowerShell. De même, des options de création de certificats plus avancées peuvent être configurées à l'aide de la ligne de commande et des fichiers de configuration. Consultez les sections PowerShell et Modules matériels de sécurité.

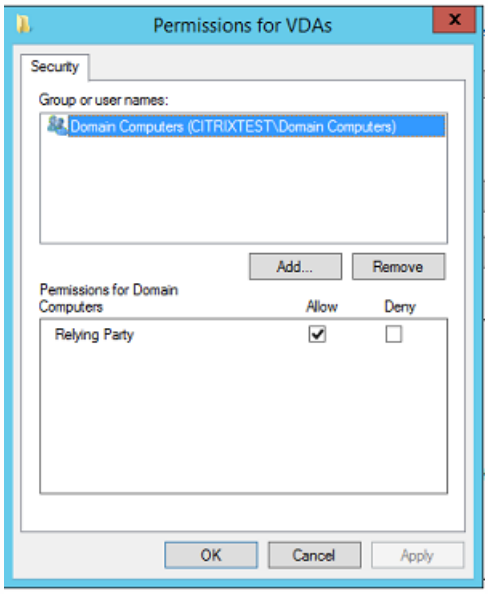
In-Session Certificats : la case à cocher **Available after logon** détermine si un certificat peut également être utilisé en tant que certificat dans la session. Si cette case n'est pas sélectionnée, le certificat sera utilisé uniquement pour l'ouverture de session ou la reconnexion, et l'utilisateur n'aura pas accès au certificat après l'authentification.

List of StoreFront servers that can use this rule : liste des serveurs StoreFront approuvés qui sont autorisés à demander des certificats pour l'ouverture de session ou la reconnexion des utilisateurs. Notez que ce paramètre est critique à la sécurité et doit être géré avec soin.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

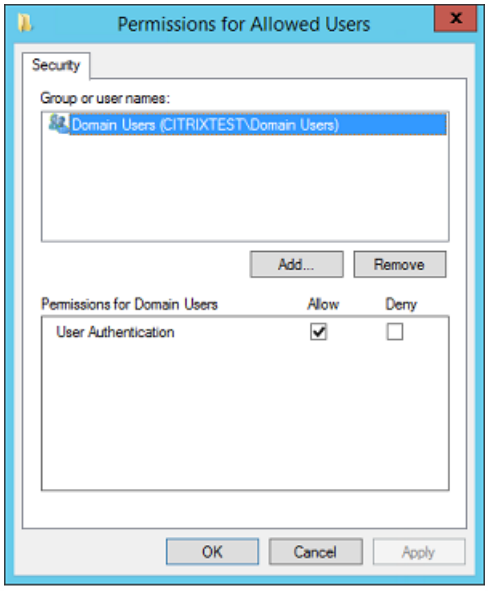


List of VDA desktops and servers that can be logged into by this rule: liste des machines VDA qui peuvent connecter les utilisateurs à l'aide du système FAS.



List of users that StoreFront can log in using this rule: liste des utilisateurs pour lesquels des certificats peuvent être émis par le Service d'authentification fédérée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Vous pouvez créer des règles supplémentaires pour référencer des autorités et des modèles de certificat différents, qui peuvent être configurés pour avoir des propriétés et des autorisations différentes. Ces règles peuvent être configurées pour être utilisées par différents serveurs StoreFront, qui devront être configurés pour demander la nouvelle règle par nom. Par défaut, StoreFront requiert les **valeurs par défaut** lors du contact du Service d'authentification fédérée. Cela peut être modifié à l'aide des options de configuration de la stratégie de groupe.

Pour créer un nouveau modèle de certificat, dupliquez le modèle Citrix_SmartcardLogon dans la console Autorité de certification de Microsoft, renommez-le (par exemple, Citrix_SmartcardLogon2) et modifiez-le si nécessaire. Créez une nouvelle règle d'utilisateur en cliquant sur **Add** afin de référencer le nouveau modèle de certificat.

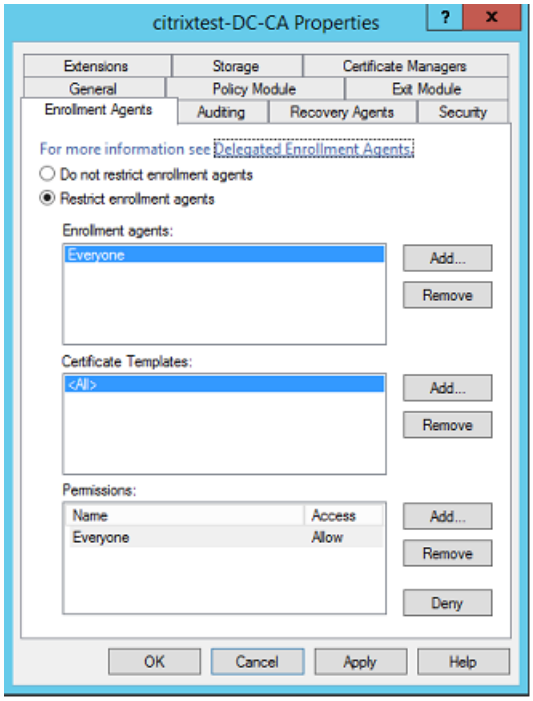
Considérations de sécurité

Le Service d'authentification fédérée dispose d'un certificat d'autorité d'inscription qui lui permet d'émettre des certificats de manière autonome de la part de vos utilisateurs de domaine. C'est la raison pour laquelle il est important de développer et d'appliquer une stratégie de sécurité pour protéger les serveurs FAS et limiter leurs autorisations.

Agents d'inscription délégués

L'autorité de certification Microsoft permet de contrôler les modèles que le serveur FAS peut utiliser, ainsi que de limiter les utilisateurs pour lesquels le serveur FAS peut émettre des certificats.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Citrix recommande fortement de configurer ces options de façon à ce que le Service d'authentification fédérée puisse uniquement émettre des certificats pour les utilisateurs visés. Par exemple, il est conseillé d'empêcher le Service d'authentification fédérée d'émettre des certificats aux utilisateurs d'un groupe d'utilisateurs protégés ou d'un groupe d'administration.

Configuration de la liste de contrôle d'accès

Comme indiqué dans la section Configurer des rôles utilisateur, vous devez configurer une liste de serveurs StoreFront autorisés à assumer des identités utilisateur sur le Service d'authentification fédérée lorsque des certificats sont émis. De même, vous pouvez restreindre les utilisateurs pour lesquels des certificats seront émis, et les machines VDA auprès desquelles ils peuvent s'authentifier. Cela vient s'ajouter à tout Active Directory standard ou toute fonctionnalité de sécurité d'autorité de certification que vous configurez.

Paramètres de pare-feu

Toutes les communications avec les serveurs FAS utilisent des connexions réseau Kerberos WCF authentifiées mutuellement sur le port 80.

Analyse du journal des événements

Le Service d'authentification fédérée et le VDA écrivent des informations dans le journal d'événements Windows. Ces informations peuvent être utilisées à des fins de contrôle et d'audit. La section Journaux d'événements dresse la liste des entrées de journal d'événements qui peuvent être générées.

Modules matériels de sécurité

Toutes les clés privées, y compris celles des certificats utilisateur émis par le Service d'authentification fédérée, sont stockées en tant que clés privées non exportables par le Compte de service réseau. Le Service d'authentification fédérée prend en charge l'utilisation d'un module matériel de sécurité cryptographique, si votre stratégie de sécurité l'exige.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Une configuration cryptographique de faible niveau est disponible dans le fichier FederatedAuthenticationService.exe.config. Ces paramètres s'appliquent lorsque les clés privées sont créées. Par conséquent, des paramètres différents peuvent être utilisés pour les clés privées d'autorité d'inscription (par exemple, 4 096 bits, Module de plateforme sécurisée protégé) et les certificats utilisateur d'exécution.

Paramètre	Description
ProviderLegacyCsp	Lorsque cette option est définie sur true, FAS utilisera l'API CryptoAPI (CAPI) de Microsoft. Sinon, FAS utilisera l'API Cryptography Next Generation (CNG) de Microsoft.
ProviderName	Nom du fournisseur CAPI ou CNG à utiliser.
ProviderType	Fait référence à la propriété Microsoft KeyContainerPermissionAccessEntry.ProviderType PROV_RSA_AES 24. Doit être toujours 24, sauf si vous utilisez un HSM avec CAPI et que le fournisseur HSM en décide autrement.
KeyProtection	Contrôle l'indicateur « Exportable » des clés privées. Permet également l'utilisation du stockage de clé TMP (Module de plateforme sécurisée), s'il est pris en charge par le matériel.
KeyLength	Longueur de clé des clés privées RSA. Les valeurs prises en charge sont 1024, 2048 et 4096 (valeur par défaut : 2048).

PowerShell SDK

Bien que la console d'administration Service d'authentification fédérée convienne aux déploiements simples, l'interface PowerShell offre des options plus avancées. Lorsque vous utilisez des options qui ne sont pas disponibles dans la console, Citrix recommande d'utiliser uniquement PowerShell pour la configuration.

La commande suivante ajoute les applets de commande PowerShell :

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

Utilisez **Get-Help** <*nom cmdlet*> pour afficher l'aide de l'applet de commande. Le tableau suivant dresse la liste de plusieurs commandes où * représente un verbe PowerShell standard (comme New, Get, Set, Remove).

Commandes	Généralités
*-FasServer	Dresse la liste des serveurs FAS et les reconfigure dans l'environnement actuel.
*-FasAuthorizationCertificate	Gère le certificat d'autorité d'inscription.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

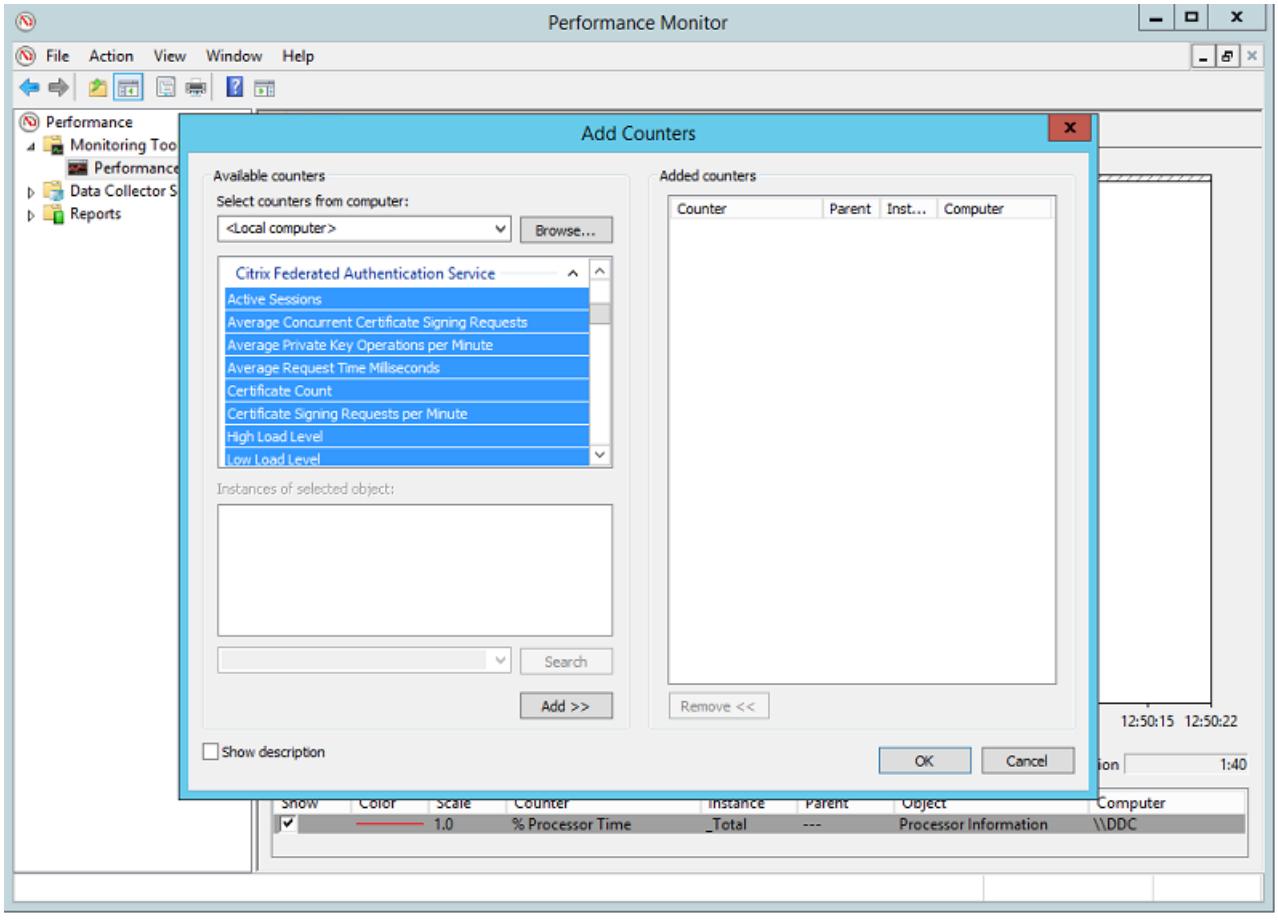
*-FasCertificateDefinition	Contrôle les paramètres que le FAS utilise pour générer des certificats.
*-FasRule	Gère les règles d'utilisateurs configurées sur le Service d'authentification fédérée.
*-FasUserCertificate	Dresse la liste et gère les certificats mis en cache par le Service d'authentification fédérée.

Des applets de commande PowerShell peuvent être utilisées à distance en spécifiant l'adresse d'un serveur FAS.

Vous pouvez également télécharger un fichier zip contenant tous les fichiers d'aide de l'applet de commande du SDK PowerShell du Service d'authentification fédérée ; consultez l'article SDK PowerShell.

Compteurs de performances

Le Service d'authentification fédérée inclut un jeu de compteurs de performances conçus pour surveiller la charge.



Le tableau suivant répertorie les compteurs disponibles. La plupart des compteurs sont des moyennes mobiles de cinq minutes.

Nom	Description

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Active Sessions	Nombre de connexions surveillées par le Service d'authentification fédérée.
Concurrent CSRs	Nombre de demandes de certificat traitées simultanément.
Private Key ops	Nombre d'opérations de clé privée effectuées par minute.
Request time	Durée requise pour générer et signer un certificat.
Certificate Count	Nombre de certificats mis en cache dans le Service d'authentification fédérée.
CSR per minute	Nombre de demandes CRS traitées par minute.
Low/Medium/High	Estimations de la charge que le Service d'authentification fédérée peut accepter en termes de « demandes CSR par minute ». Le dépassement du seuil « High Load » peut entraîner l'échec du lancement de sessions.

Journaux d'événements

Les tableaux suivants répertorient les entrées de journal d'événements générées par le Service d'authentification fédérée.

Événements d'administration

[Source de l'événement : Citrix.Authentication.FederatedAuthenticationService]

Ces événements sont consignés en réponse à une modification de la configuration du serveur Service d'authentification fédérée.

Codes de journal
[S001] ACCESS DENIED: User [{0}] is not a member of Administrators group
[S002] ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}]
[S003] Administrator [{0}] setting Maintenance Mode to [{1}]
[S004] Administrator [{0}] enrolling with CA [{1}] templates [{2} and {3}]
[S005] Administrator [{0}] de-authorizing CA [{1}]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[S006] Administrator [{0}] creating new Certificate Definition [{1}]
[S007] Administrator [{0}] updating Certificate Definition [{1}]
[S008] Administrator [{0}] deleting Certificate Definition [{1}]
[S009] Administrator [{0}] creating new Role [{1}]
[S010] Administrator [{0}] updating Role [{1}]
[S011] Administrator [{0}] deleting Role [{1}]
[S012] Administrator [{0}] creating certificate [upn: {0} sid: {1} role: {2}][Certificate Definition: {3}]
[S013] Administrator [{0}] deleting certificates [upn: {0} role: {1} Certificate Definition: {2}]

Codes de journal
[S401] Performing configuration upgrade -- [From version {0}][to version {1}]
[S402] ERROR: The Citrix Federated Authentication Service must be run as Network Service [currently running as: {0}]

Création d'assertions d'identité [Service d'authentification fédérée]

Ces événements sont journalisés au moment de l'exécution sur le serveur du Service d'authentification fédérée lorsqu'un serveur approuvé assume l'ouverture de session d'un utilisateur.

Codes de journal
[S101] Server [{0}] is not authorized to assert identities in role [{1}]
[S102] Server [{0}] failed to assert UPN [{1}] (Exception: {2}{3})
[S103] Server [{0}] requested UPN [{1}] SID {2}, but lookup returned SID {3}
[S104] Server [{0}] failed to assert UPN [{1}] (UPN not allowed by role [{2}])

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[S105] Server [{0}] issued identity assertion [upn: {0}, role {1}, Security Context: [{2}]
[S120] Issuing certificate to [upn: {0} role: {1} Security Context: [{2}]]
[S121] Issuing certificate to [upn: {0} role: {1}] on behalf of account {2}
[S122] Warning: Server is overloaded [upn: {0} role: {1}][Requests per minute {2}].

Agissant en tant que partie de confiance [Service d'authentification fédérée]

Ces événements sont journalisés au moment de l'exécution sur le serveur du Service d'authentification fédérée lorsqu'un VDA connecte un utilisateur.

Codes de journal
[S201] Relying party [{0}] does not have access to a password.
[S202] Relying party [{0}] does not have access to a certificate.
[S203] Relying party [{0}] does not have access to the Logon CSP
[S204] Relying party [{0}] accessing the Logon CSP [Operation: {1}]
[S205] Calling account [{0}] is not a relying party in role [{1}]
[S206] Calling account [{0}] is not a relying party
[S207] Relying party [{0}] asserting identity [upn: {1}] in role: [{2}]
[S208] Private Key operation failed [Operation: {0}][upn: {1} role: {2} certificateDefinition {3}][Error {4} {5}].

Serveur de certificat dans la session [Service d'authentification fédérée]

Ces événements sont journalisés sur le serveur du Service d'authentification fédérée lorsqu'un utilisateur utilise un certificat

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

dans la session.

Codes de journal
[S301] Access Denied: User [{0}] does not have access to a Virtual Smart Card
[S302] User [{0}] requested unknown Virtual Smart Card [thumbprint: {1}]
[S303] User [{0}] does not match Virtual Smart Card [upn: {1}]
[S304] User [{1}] running program [{2}] on computer [{3}] using Virtual Smart Card [upn: {4} role: {5}] for private key operation: [{6}]
[S305] Private Key operation failed [Operation: {0}][upn: {1} role: {2} containerName {3}][Error {4} {5}].

Ouverture de session [VDA]

[Source de l'événement : Citrix.Authentication.IdentityAssertion]

Ces événements sont journalisés sur le VDA durant la phase d'ouverture de session.

Codes de journal
[S101] Identity Assertion Logon failed. Unrecognised Federated Authentication Service [id: {0}]
[S102] Identity Assertion Logon failed. Could not lookup SID for {0} [Exception: {1}{2}]
[S103] Identity Assertion Logon failed. User {0} has SID {1}, expected SID {2}
[S104] Identity Assertion Logon failed. Failed to connect to Federated Authentication Service: {0} [Error: {1} {2}]
[S105] Identity Assertion Logon. Logging in [Username: {0}][Domain: {1}]
[S106] Identity Assertion Logon. Logging in [Certificate: {0}]
[S107] Identity Assertion Logon failed. [Exception: {1}{2}]
[S108] Identity Assertion Subsystem. ACCESS_DENIED [Caller: {0}]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Certificats dans la session [VDA]

Ces événements sont journalisés sur le VDA lorsqu'un utilisateur tente d'utiliser un certificat dans la session.

Codes de journal
[S201] Virtual Smart Card Authorized [User: {0}][PID: {1} Name:{2}][Certificate {3}]
[S202] Virtual Smart Card Subsystem. No smart cards available in session {0}
[S203] Virtual Smart Card Subsystem. Access Denied [caller: {0}, session {1}, expected: {2}]
[S204] Virtual Smart Card Subsystem. Smart card support disabled.

Demande de certificat et génération de codes [Service d'authentification fédérée]

[Source de l'événement : Citrix.TrustFabric]

Ces événements de bas niveau sont journalisés lorsque le serveur du Service d'authentification fédérée effectue des opérations cryptographiques au niveau du journal.

Codes de journal
[S0001]TrustArea::TrustArea: Installed certificate chain
[S0002]TrustArea::Join: Callback has authorized an untrusted certificate
[S0003]TrustArea::Join: Joining to a trusted server
[S0004]TrustArea::Maintain: Renewed certificate
[S0005]TrustArea::Maintain: Retrieved new certificate chain
[S0006]TrustArea::Export: Exporting private key
[S0007]TrustArea::Import: Importing Trust Area
[S0008]TrustArea::Leave: Leaving Trust Area

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[S0009]TrustArea::SecurityDescriptor: Setting Security Descriptor
[S0010]CertificateVerification: Installing new trusted certificate
[S0011]CertificateVerification: Uninstalling expired trusted certificate
[S0012]TrustFabricHttpClient: Attempting single sign-on to {0}
[S0013]TrustFabricHttpClient: Explicit credentials entered for {0}
[S0014]Pkcs10Request::Create: Created PKCS10 request
[S0015]Pkcs10Request::Renew: Created PKCS10 request
[S0016]PrivateKey::Create
[S0017]PrivateKey::Delete
[S0018]TrustArea::TrustArea: Waiting for Approval
[S0019]TrustArea::Join: Delayed Join
[S0020]TrustArea::Join: Delayed Join
[S0021]TrustArea::Maintain: Installed certificate chain

Codes de journal
[S0101]TrustAreaServer::Create root certificate
[S0102]TrustAreaServer::Subordinate: Join succeeded
[S0103]TrustAreaServer::PeerJoin: Join succeeded
[S0104]MicrosoftCertificateAuthority::GetCredentials: Authorized to use {0}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[S0104]MicrosoftCertificateAuthority::SubmitCertificateRequest Error {0}
[S0105]MicrosoftCertificateAuthority::SubmitCertificateRequest Issued cert {0}
[S0106]MicrosoftCertificateAuthority::PublishCRL: Published CRL
[S0107]MicrosoftCertificateAuthority::ReissueCertificate Error {0}
[S0108]MicrosoftCertificateAuthority::ReissueCertificate Issued Cert {0}
[S0109]MicrosoftCertificateAuthority::CompleteCertificateRequest - Still waiting for approval
[S0110]MicrosoftCertificateAuthority::CompleteCertificateRequest - Pending certificate refused
[S0111]MicrosoftCertificateAuthority::CompleteCertificateRequest Issued certificate
[S0112]MicrosoftCertificateAuthority::SubmitCertificateRequest - Waiting for approval
[S0120]NativeCertificateAuthority::SubmitCertificateRequest Issued cert {0}
[S0121]NativeCertificateAuthority::SubmitCertificateRequest Error
[S0122]NativeCertificateAuthority::RootCARollover New root certificate
[S0123]NativeCertificateAuthority::ReissueCertificate New certificate
[S0124]NativeCertificateAuthority::RevokeCertificate
[S0125]NativeCertificateAuthority::PublishCRL

Informations connexes

- Les déploiements FAS courants sont décrits dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée.
- Des informations pratiques sont disponibles dans l'article Configuration et gestion du Service d'authentification fédérée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Vue d'ensemble des architectures du Service d'authentification fédérée

Jul 13, 2016

Introduction

Le Service d'authentification fédérée (FAS) est un composant Citrix qui s'intègre avec votre autorité de certification (CA) Active Directory, qui permet aux utilisateurs d'être authentifiés dans un environnement Citrix. Ce document présente les différentes architectures d'authentification susceptibles d'être appropriées à votre déploiement.

Lorsqu'il est activé, le FAS délègue l'authentification utilisateur aux serveurs StoreFront approuvés. StoreFront est doté d'un ensemble complet d'options d'authentification articulées autour de technologies Web modernes. En outre, il peut être étendu facilement grâce au SDK StoreFront ou à des plug-ins IIS tiers. L'objectif de base est que toute technologie d'authentification qui peut authentifier un utilisateur sur un site Web peut maintenant être utilisée pour la connexion à un déploiement Citrix XenApp ou XenDesktop.

Ce document décrit certaines architectures de déploiement de haut niveau, par complexité croissante.

- Déploiement interne
- Déploiement NetScaler Gateway
- ADFS SAML
- Mappage de compte B2B
- Jonction à un domaine Azure AD (Azure AD Join) avec Windows 10

Des liens vers les articles FAS sont fournis. Pour toutes les architectures, l'article Service d'authentification fédérée est le document de référence principal pour la configuration du FAS.

Le FAS est autorisé à émettre des certificats de classe de carte à puce automatiquement à la place des utilisateurs Active Directory qui sont authentifiés par StoreFront. Il utilise des API similaires aux outils qui permettent aux administrateurs de provisionner des cartes à puce physiques.

Lorsqu'un utilisateur est connecté à un VDA Citrix XenApp ou XenDesktop, le certificat est attaché à la machine, et le domaine Windows interprète l'ouverture de session en tant qu'authentification par carte à puce standard.

Déploiement interne

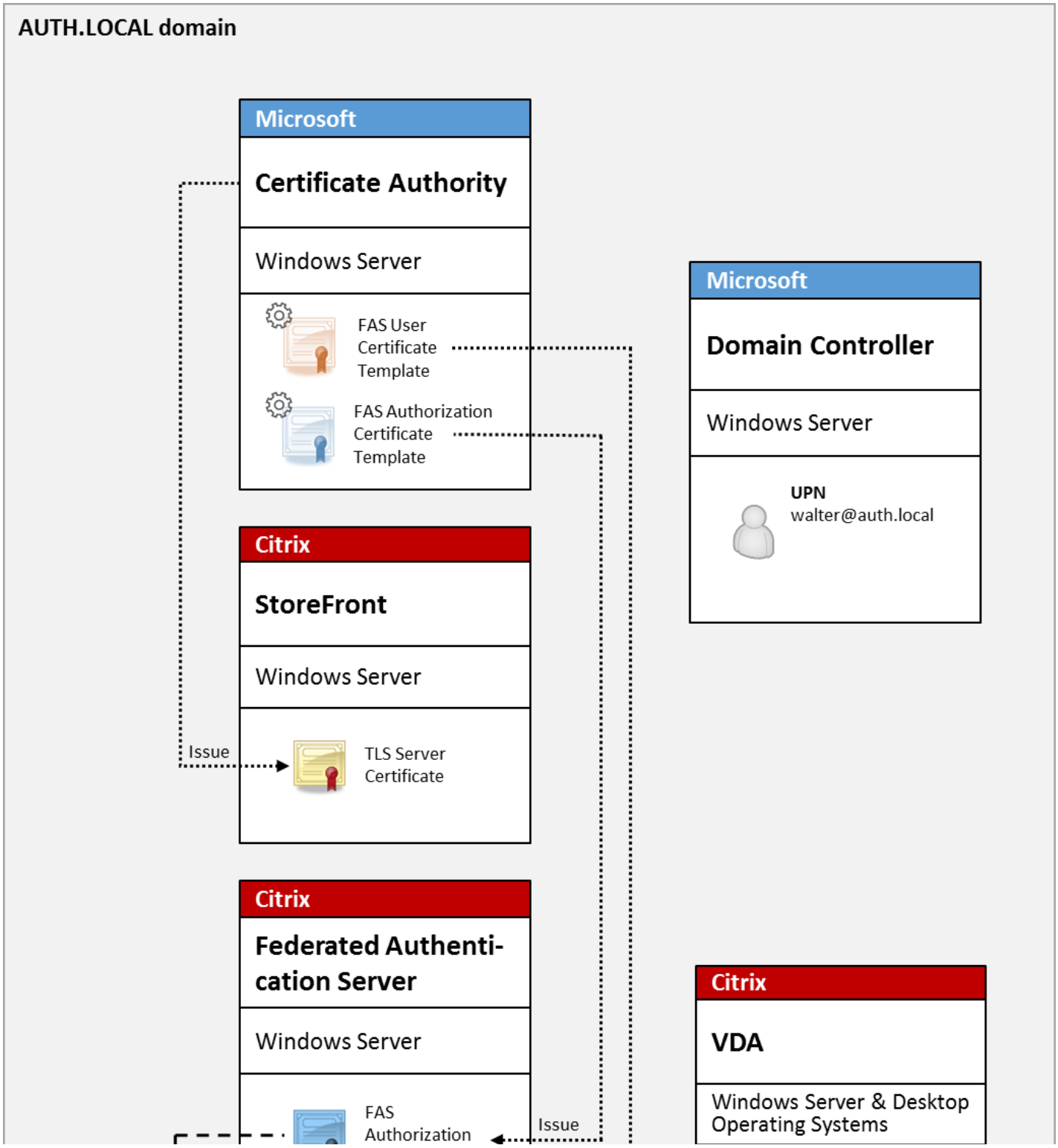
Le FAS permet aux utilisateurs de s'authentifier en toute sécurité auprès de StoreFront à l'aide de plusieurs options d'authentification (y compris l'authentification unique Kerberos) et de se connecter à une session Citrix HDX authentifiée.

Cela rend possible l'authentification Windows sans invite de saisie d'informations d'identification ou de codes PIN de carte à puce et sans l'utilisation de fonctionnalités de « gestion des mots de passe enregistrés » telles que le service Single Sign-On. Cela peut être utilisé pour remplacer les fonctionnalités d'ouverture de session de la délégation Kerberos contrainte disponibles dans les versions précédentes de XenApp.

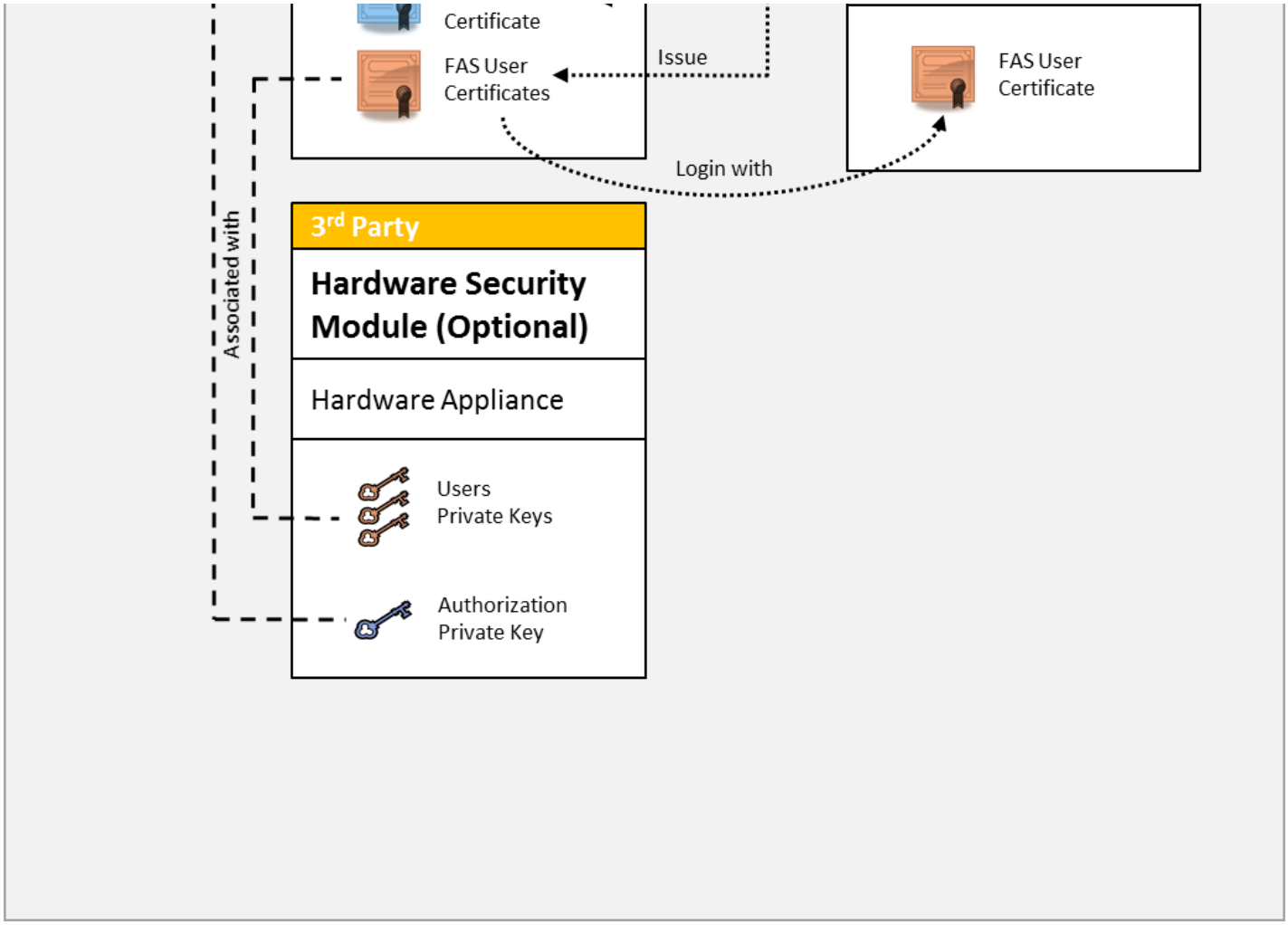
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Tous les utilisateurs ont accès aux certificats PKI dans leur session, qu'ils se soient connectés ou non aux machines de point de terminaison avec une carte à puce. Ceci permet une migration fluide vers des modèles d'authentification à deux facteurs, et ce, même à partir de périphériques tels que des smartphones et tablettes qui ne disposent pas d'un lecteur de carte à puce.

Ce déploiement ajoute un nouveau serveur exécutant le FAS, qui est autorisé à émettre des certificats de classe de carte à puce pour le compte d'utilisateurs. Ces certificats sont alors utilisés pour se connecter à des sessions utilisateur dans un environnement Citrix HDX comme si une ouverture de session par carte à puce était utilisée.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



L'environnement XenApp ou XenDesktop doit être configuré de la même manière que l'ouverture de session par carte à puce à, ce qui est décrit dans l'article CTX206156.

Dans un déploiement existant, cela implique généralement de s'assurer qu'une autorité de certification (CA) Microsoft appartenant au domaine soit disponible, et que des certificats de contrôleur de domaine ont été attribués aux contrôleurs de domaine. (Consultez la section « Émission de certificats de contrôleur de domaine » dans l'article CTX206156).

Informations connexes :

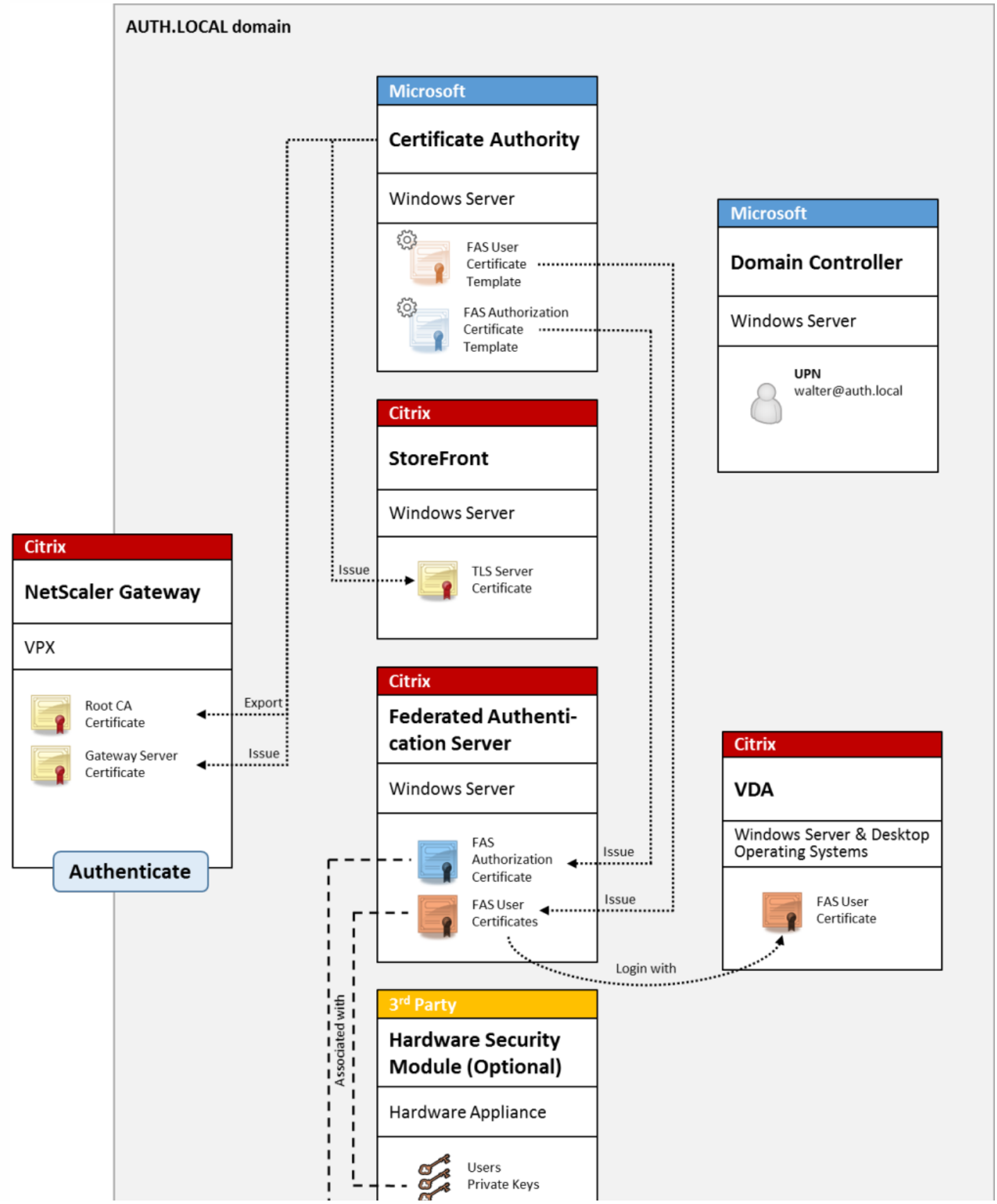
- Les clés peuvent être stockées dans un module de sécurité matériel (HSM) ou un module de plateforme sécurisée (TPM). Pour de plus amples informations, consultez l'article Protection des clés privées du Service d'authentification fédérée.
- L'article Service d'authentification fédérée décrit comment installer et configurer le FAS.

Déploiement NetScaler Gateway

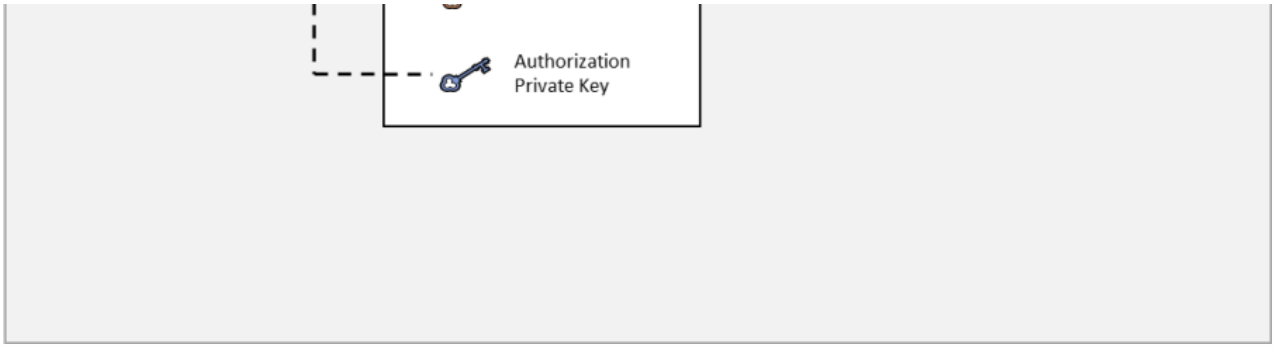
Le déploiement NetScaler est similaire au déploiement interne, mais ajoute Citrix NetScaler Gateway couplé avec StoreFront, et déplace le point principal d'authentification sur NetScaler. Citrix NetScaler comprend des options d''authentification et d'autorisation avancées qui peuvent être utilisées pour sécuriser l'accès à distance aux sites Web d'une entreprise.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ce déploiement peut être utilisé pour éviter l'affichage de plusieurs invites de saisie de code PIN qui se produisent lors de l'authentification auprès de NetScaler, puis de la connexion à une session utilisateur. Il permet également d'utiliser les technologies d'authentification NetScaler avancées sans nécessiter de mots de passe Active Directory ou de cartes à puce.



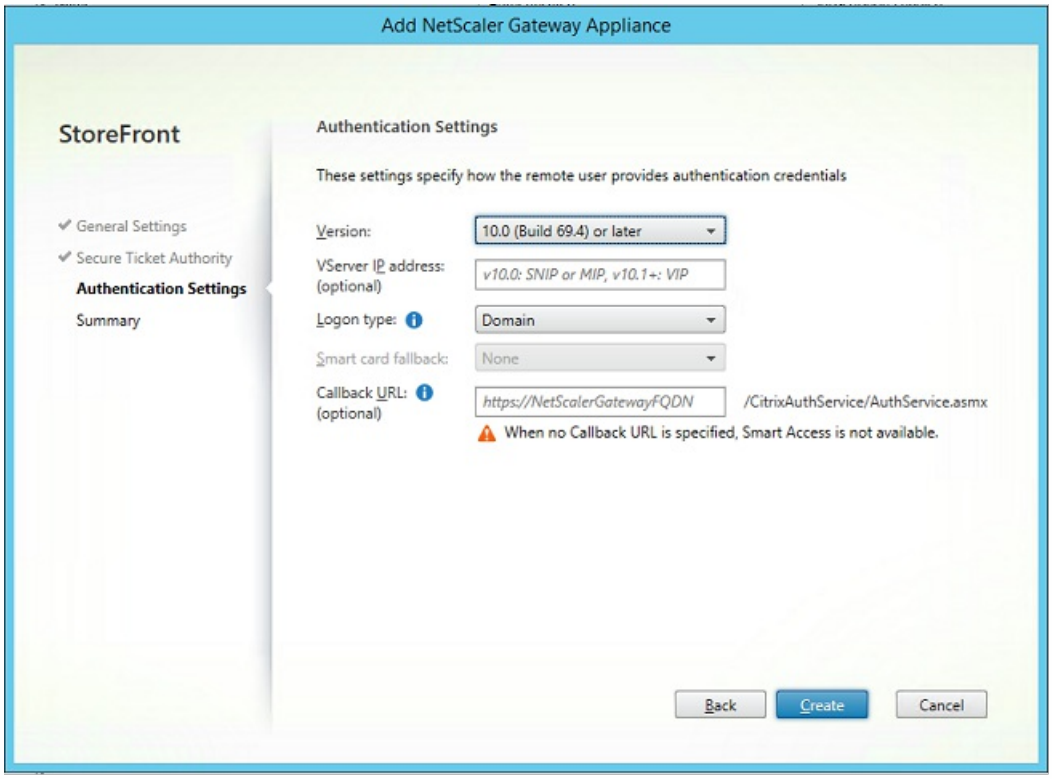
© 1999-2017 Citrix Systems, Inc. All rights reserved.



L'environnement XenApp ou XenDesktop doit être configuré de la même manière que l'ouverture de session par carte à puce à, ce qui est décrit dans l'article CTX206156.

Dans un déploiement existant, cela implique généralement de s'assurer qu'une autorité de certification (CA) Microsoft appartenant au domaine soit disponible, et que des certificats de contrôleur de domaine ont été attribués aux contrôleurs de domaine. (Consultez la section « Émission de certificats de contrôleur de domaine » dans l'article CTX206156).

Lors de la configuration de NetScaler Gateway en tant que système d'authentification principal, assurez-vous que toutes les connexions entre NetScaler et StoreFront sont sécurisées à l'aide du protocole TLS. En particulier, assurez-vous que l'URL de rappel est correctement configurée pour pointer vers le serveur NetScaler, car cela peut être utilisé pour authentifier le serveur NetScaler dans ce déploiement.



Informations connexes :

- Pour configurer NetScaler Gateway, consultez la section Comment configurer NetScaler Gateway 10.5 pour l'utiliser avec StoreFront 3.6 et XenDesktop 7.6.

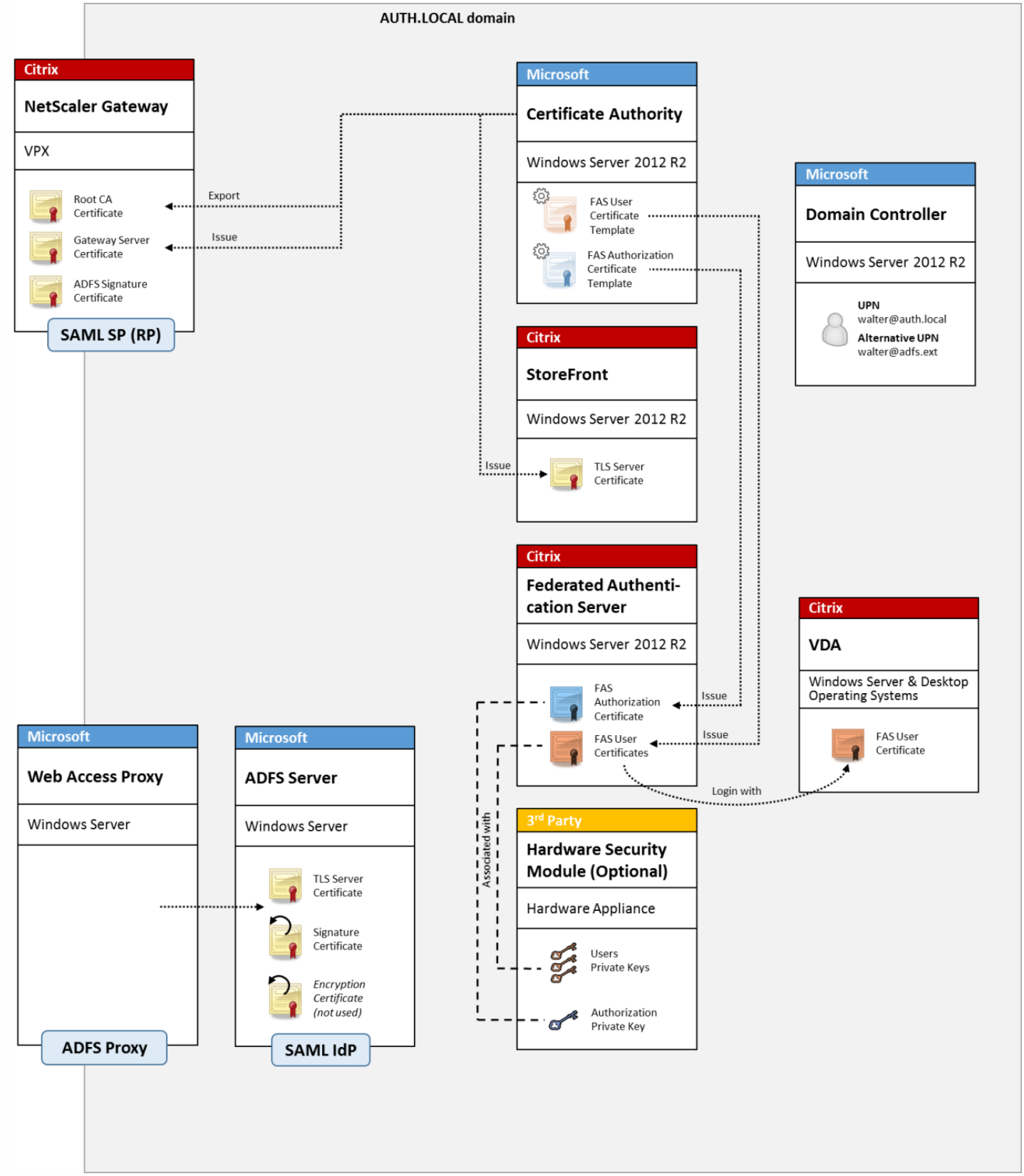
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- L'article Service d'authentification fédérée décrit comment installer et configurer le FAS.

Déploiement SAML ADFS

Une technologie d'authentification NetScaler clé permet l'intégration avec Microsoft ADFS, qui peut agir en tant que fournisseur d'identité SAML (IdP). Une assertion SAML est un bloc XML signé de manière cryptographique émis par un fournisseur d'identité approuvé qui autorise un utilisateur à ouvrir une session sur un ordinateur. Cela signifie que le serveur FAS permet maintenant de déléguer l'authentification d'un utilisateur au serveur Microsoft ADFS (ou d'autres fournisseurs d'identité SAML).

© 1999-2017 Citrix Systems, Inc. All rights reserved.



ADFS est généralement utilisé pour authentifier de manière sécurisée les utilisateurs auprès des ressources d'entreprise à distance via Internet ; par exemple, il est souvent utilisé pour l'intégration à Office 365.

Informations connexes :

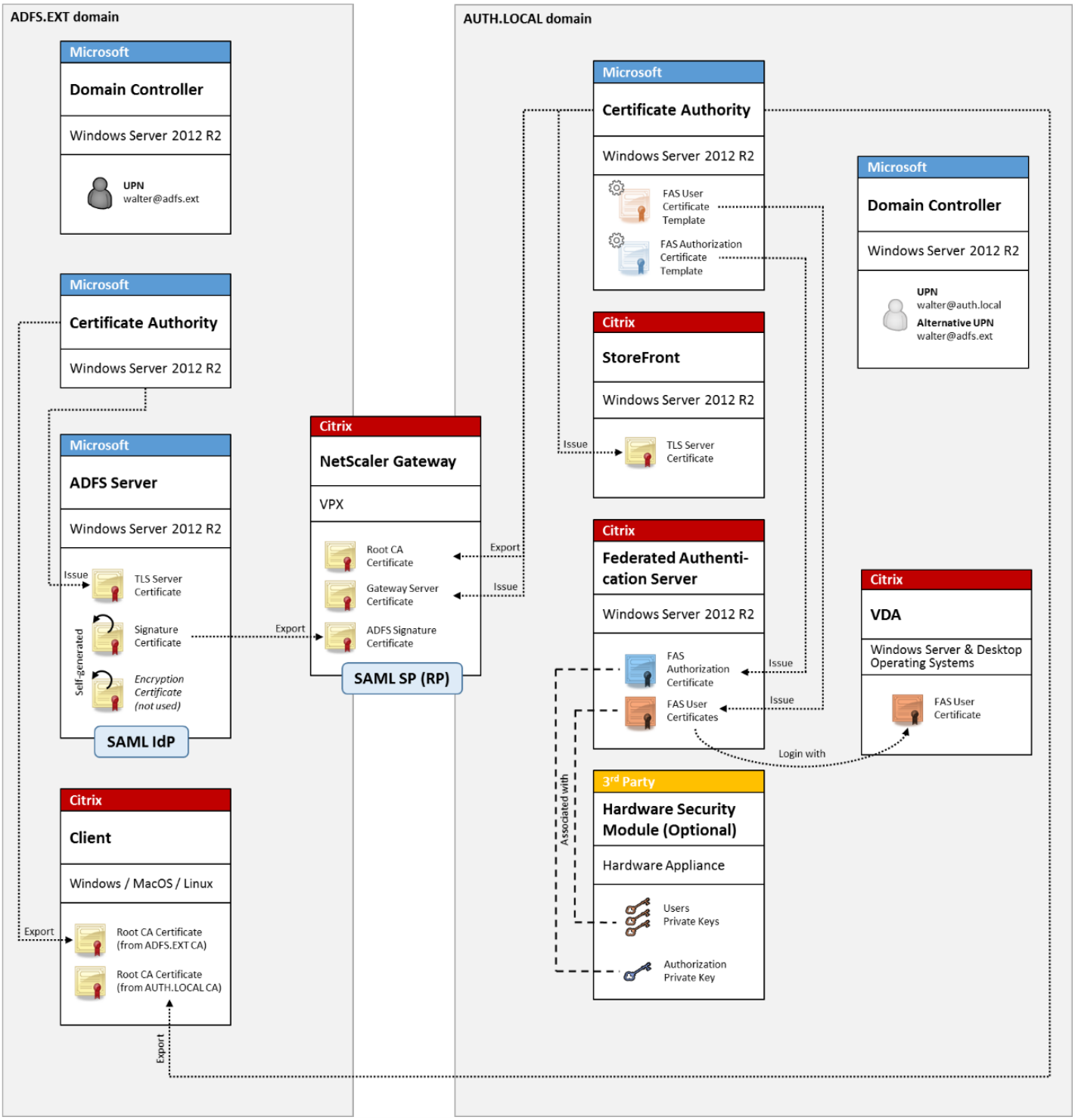
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- L'article Déploiement ADFS du Service d'authentification fédérée contient des détails.
- L'article Service d'authentification fédérée décrit comment installer et configurer le FAS.
- La section Déploiement NetScaler Gateway dans cet article contient des recommandations en matière de configuration.

Mappage de compte B2B

Si deux entreprises souhaitent utiliser réciproquement leurs systèmes informatiques, une option courante consiste à configurer un serveur Active Directory Federation Service (ADFS) avec une relation d'approbation. Cela permet aux utilisateurs d'une entreprise de s'authentifier en toute transparence auprès de l'environnement Active Directory (AD) d'une autre entreprise. Lors de l'ouverture de session, chaque utilisateur utilise ses propres informations d'identification d'ouverture de session d'entreprise ; ADFS mappe automatiquement ces dernières à un « compte fantôme » dans l'environnement Active Directory de l'entreprise homologue.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



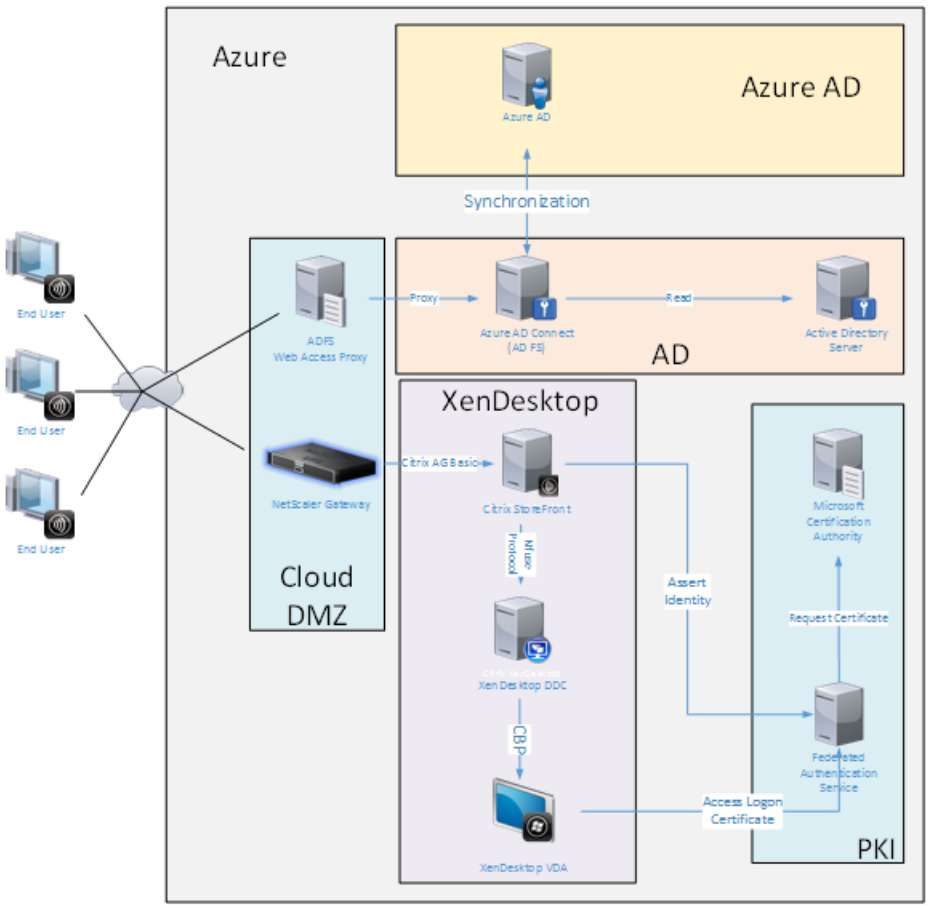
Informations connexes :

- L'article Service d'authentification fédérée décrit comment installer et configurer le FAS.

Jonction à un domaine Azure AD (Azure AD Join) avec Windows 10

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Windows 10 a introduit le concept de « Azure AD Join » (Jonction à un domaine Azure AD), qui est d'un point de vue conceptuel similaire à la jointure de domaine Windows traditionnelle mais ciblé pour les scénarios « via Internet ». Ce concept convient tout particulièrement aux ordinateurs portables et tablettes. Comme avec la jonction de domaine Windows traditionnelle, Azure AD est équipé de fonctionnalités permettant d'utiliser des modèles d'authentification unique pour la connexion aux sites Web et aux ressources de l'entreprise. Ces derniers sont tous « compatibles Internet », ils fonctionnent donc à partir de n'importe quel emplacement connecté à Internet, et pas seulement sur le réseau local du bureau.



Ce déploiement est un exemple dans lequel il n'existe pas de concept « d'utilisateurs de bureau ». Les ordinateurs portables sont inscrits et s'authentifient via Internet à l'aide des fonctionnalités de Azure AD.

Veuillez noter que l'infrastructure dans ce déploiement peut s'exécuter partout où une adresse IP est disponible : en interne, fournisseur hébergé, Azure ou un autre fournisseur de cloud. Le synchronisateur Azure AD Connect se connectera automatiquement à Azure AD. Le graphique utilise des VM Azure à des fins de simplicité.

Informations connexes :

- L'article Service d'authentification fédérée décrit comment installer et configurer le FAS.
- L'article Intégration d'Azure AD au Service d'authentification fédérée contient des détails.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Déploiement ADFS du Service d'authentification fédérée

Jul 13, 2016

Introduction

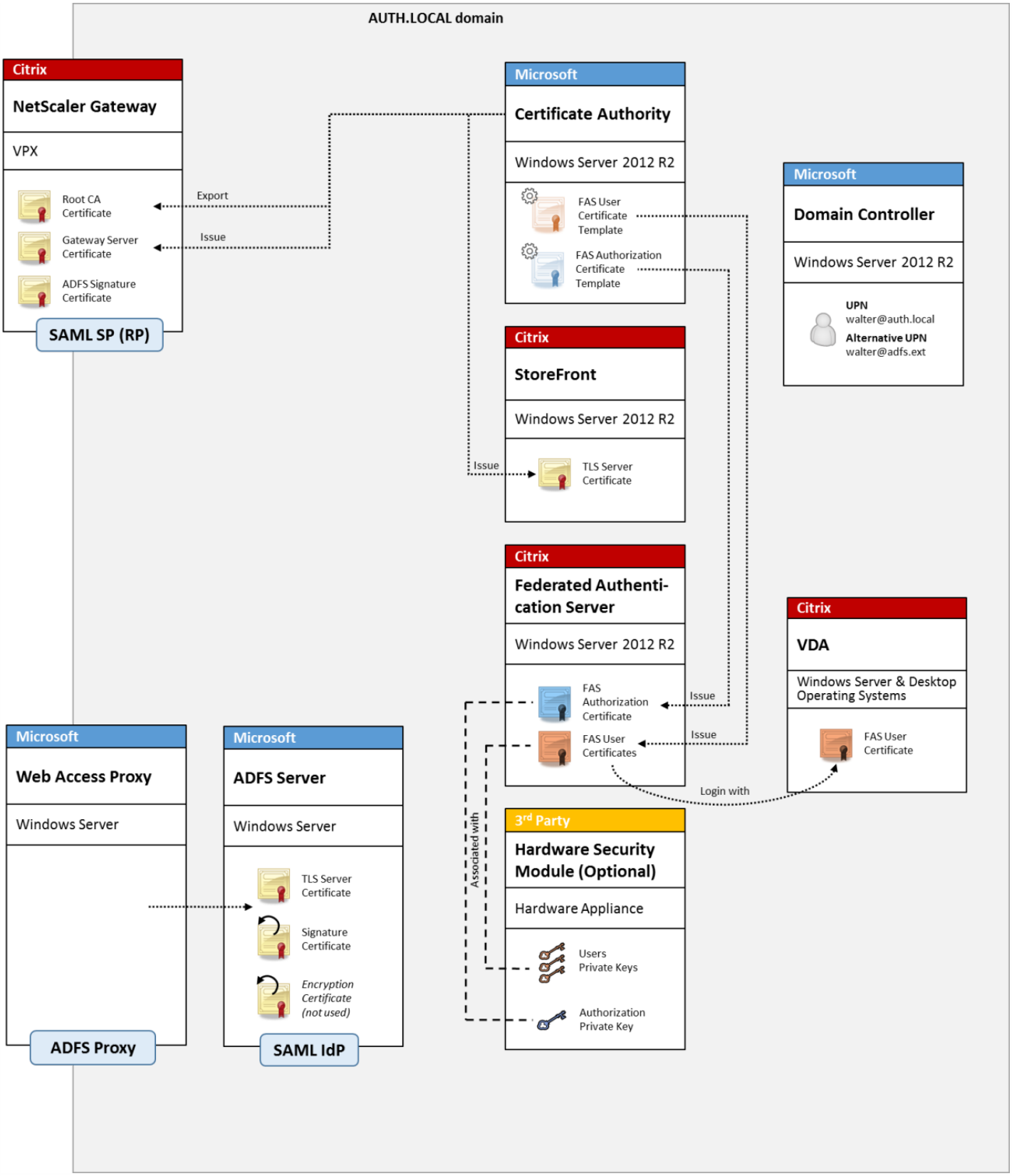
Ce document décrit comment intégrer un environnement Citrix avec Microsoft ADFS.

De nombreuses organisations utilisent ADFS pour gérer l'accès sécurisé aux sites Web qui requièrent un seul point d'authentification. Par exemple, une entreprise peut disposer de contenu et de téléchargements supplémentaires disponibles pour les employés ; ces emplacements doivent être protégés avec des informations d'identification d'ouverture de session Windows standard.

Le Service d'authentification fédérée (FAS) permet également d'intégrer Citrix NetScaler et Citrix StoreFront avec le système d'ouverture de session ADFS, ce qui réduit toute confusion potentielle pour le personnel de l'entreprise.

Ce déploiement intègre NetScaler en tant que partie de confiance pour Microsoft ADFS.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Présentation SAML

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SAML (Security Assertion Markup Language) est un système d'ouverture de session sur navigateur Web de « redirection vers une page d'ouverture de session ». La configuration comprend les éléments suivants :

URL de redirection [URL du service Single Sign-On]

Lorsque NetScaler découvre qu'un utilisateur a besoin d'être authentifié, il indique au navigateur Web de l'utilisateur d'utiliser un HTTP POST vers une page Web d'ouverture de session SAML sur le serveur ADFS. Il s'agit généralement d'une adresse https:// au format : https://adfs.mycompany.com/adfs/ls.

Cette page Web POST comprend d'autres informations, notamment « l'adresse de retour » à laquelle ADFS renverra l'utilisateur lorsque l'ouverture de session est terminée.

Identificateur [Nom de l'émetteur/EntityID]

EntityId est un identificateur unique que NetScaler inclut dans ses données POST à ADFS. Il renseigne ADFS sur le service auquel l'utilisateur tente de se connecter et applique différentes stratégies d'authentification le cas échéant. S'il est émis, le fichier XML d'authentification SAML pourra uniquement être utilisé pour ouvrir une session sur le service identifié par EntityId.

En règle générale, EntityID est l'adresse URL de la page d'ouverture de session du serveur NetScaler, mais une quelconque autre adresse peut être utilisée, à condition que NetScaler et ADFS l'acceptent : https://ns.mycompany.com/application/logonpage.

Adresse de retour [URL de réponse]

Si l'authentification réussit, ADFS indique au navigateur Web de l'utilisateur de publier un fichier ADFS d'authentification SAML sur l'une des URL de réponse qui sont configurées pour EntityId. Il s'agit généralement d'une adresse https:// sur le serveur NetScaler d'origine au format : https://ns.mycompany.com/cgi/samlauth

S'il existe plusieurs URL de réponse configurées, NetScaler peut en choisir une dans sa publication d'origine sur ADFS.

Certificat de signature [Certificat IDP]

ADFS signe de manière cryptographique les objets blob XML d'authentification SAML à l'aide de sa clé privée. Pour valider cette signature, NetScaler doit être configuré pour vérifier ces signatures à l'aide de la clé publique incluse dans un fichier de certificat. Le fichier de certificat sera généralement un fichier texte obtenu à partir du serveur ADFS.

URL d'authentification unique [URL de déconnexion unique]

ADFS et NetScaler prennent en charge un système de « déconnexion centrale ». Il s'agit d'une adresse URL que NetScaler interroge parfois pour vérifier que l'objet blob XML d'authentification SAML représente toujours une session actuellement connectée.

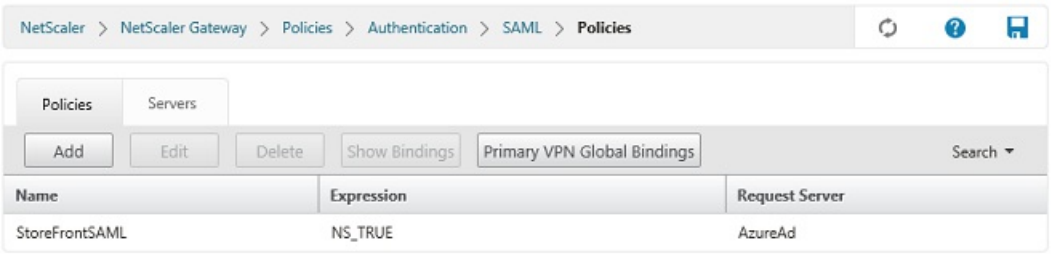
Cette fonctionnalité est facultative et n'a pas besoin d'être configurée. Il s'agit généralement d'une adresse https:// au format https://adfs.mycompany.com/adfs/logout. (Notez que cette dernière peut être la même que l'URL d'ouverture de session unique).

Configuration

La section Déploiement NetScaler Gateway de l'article Architectures du Service d'authentification fédérée explique

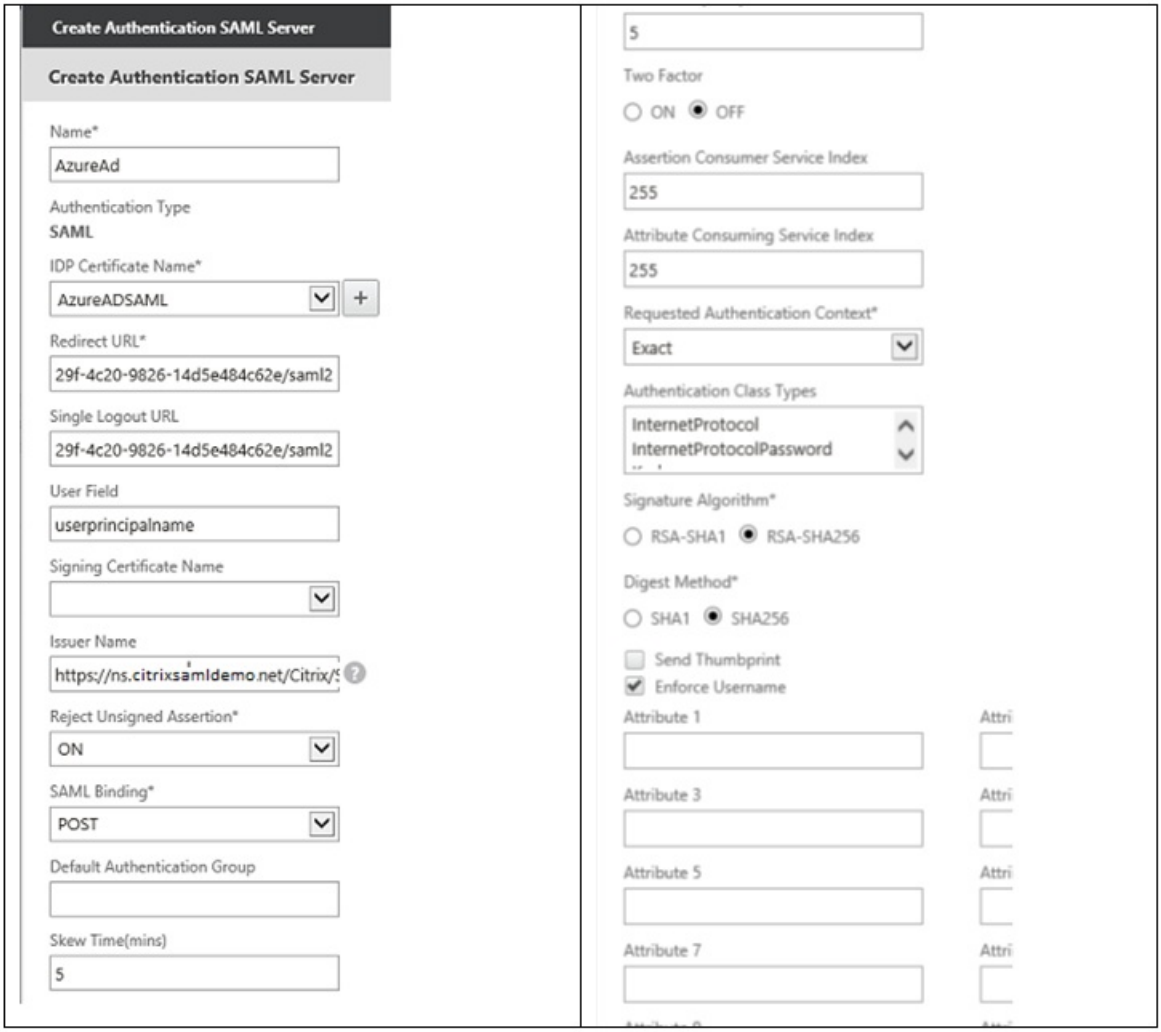
© 1999-2017 Citrix Systems, Inc. All rights reserved.

comment configurer NetScaler Gateway afin de gérer les options d'authentification LDAP standard, à l'aide de l'assistant d'installation de XenApp et XenDesktop NetScaler. Une fois la configuration terminée, vous pouvez créer une nouvelle stratégie d'authentification sur NetScaler qui autorise l'authentification SAML. Cela peut remplacer la stratégie LDAP par défaut utilisée par l'assistant d'installation de NetScaler.



Renseigner la stratégie SAML

Configurez le nouveau serveur IdP SAML à l'aide des informations obtenues précédemment dans la console de gestion ADFS. Lorsque cette stratégie est appliquée, NetScaler redirige l'utilisateur vers ADFS pour l'ouverture de session, et accepte les blocs XML d'authentification SAML signés.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Informations connexes

- L'article Service d'authentification fédérée est le document de référence principal pour obtenir des informations sur l'installation et la configuration du FAS.
- Les déploiements FAS courants sont décrits dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée.
- Des informations pratiques sont disponibles dans l'article Configuration et gestion du service d'authentification fédérée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Intégration d’Azure AD au Service d'authentification fédérée

Aug 22, 2016

Dans cet article :

- Introduction
- Architecture
- Créer une zone DNS
- Créer un service de cloud
- Créer des machines virtuelles Windows
- Configurer un DNS interne
- Configurer une adresse DNS externe
- Configurer des groupes de sécurité
- Créer un certificat ADFS
- Configurer Azure AD
- Activer Azure AD Join (Jonction à un domaine Azure AD)
- Installer XenApp ou XenDesktop
- Configurer une nouvelle application Azure AD pour l’authentification unique sur StoreFront
- Installer et configurer NetScaler Gateway
- Configurer l'adresse de StoreFront
- Activer la prise en charge de l'authentification SAML NetScaler
- Vérifier le système de bout en bout
- Annexe

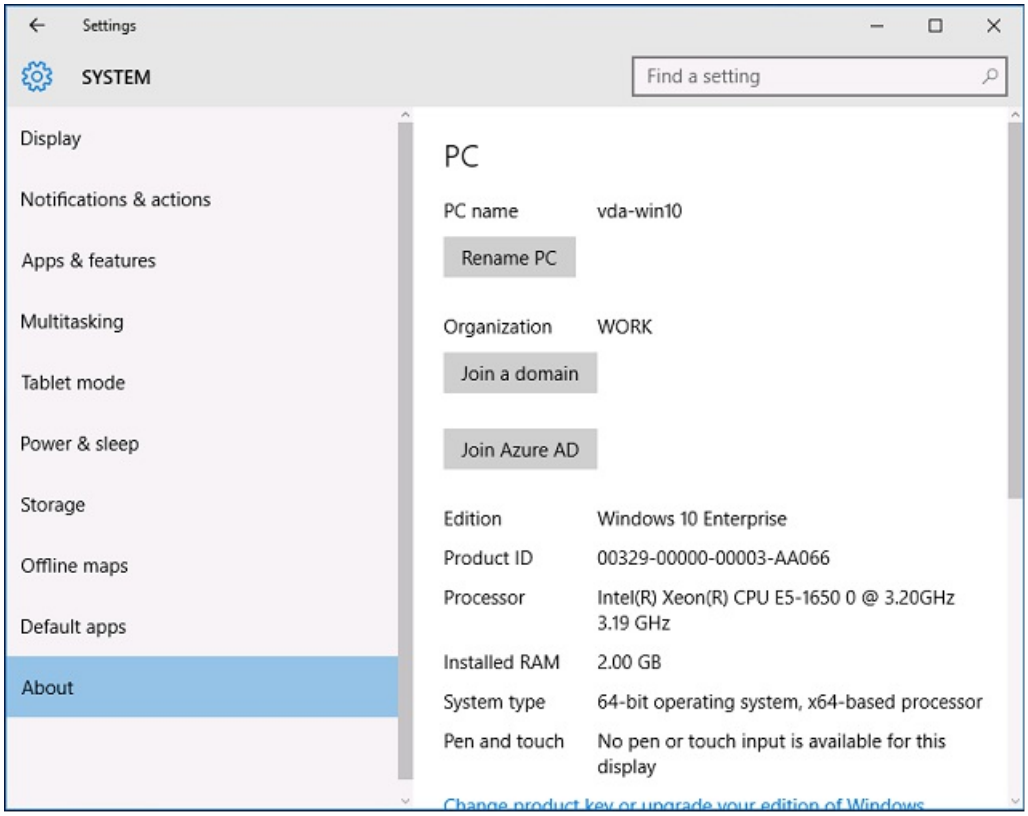
Introduction

Ce document décrit comment intégrer un environnement Citrix avec la fonctionnalité Azure AD de Windows 10.

Windows 10 a introduit Azure AD, qui est un nouveau modèle de jonction de domaine dans lequel les ordinateurs portables itinérants peuvent être joints à un domaine d'entreprise via Internet à des fins de gestion et d'authentification unique.

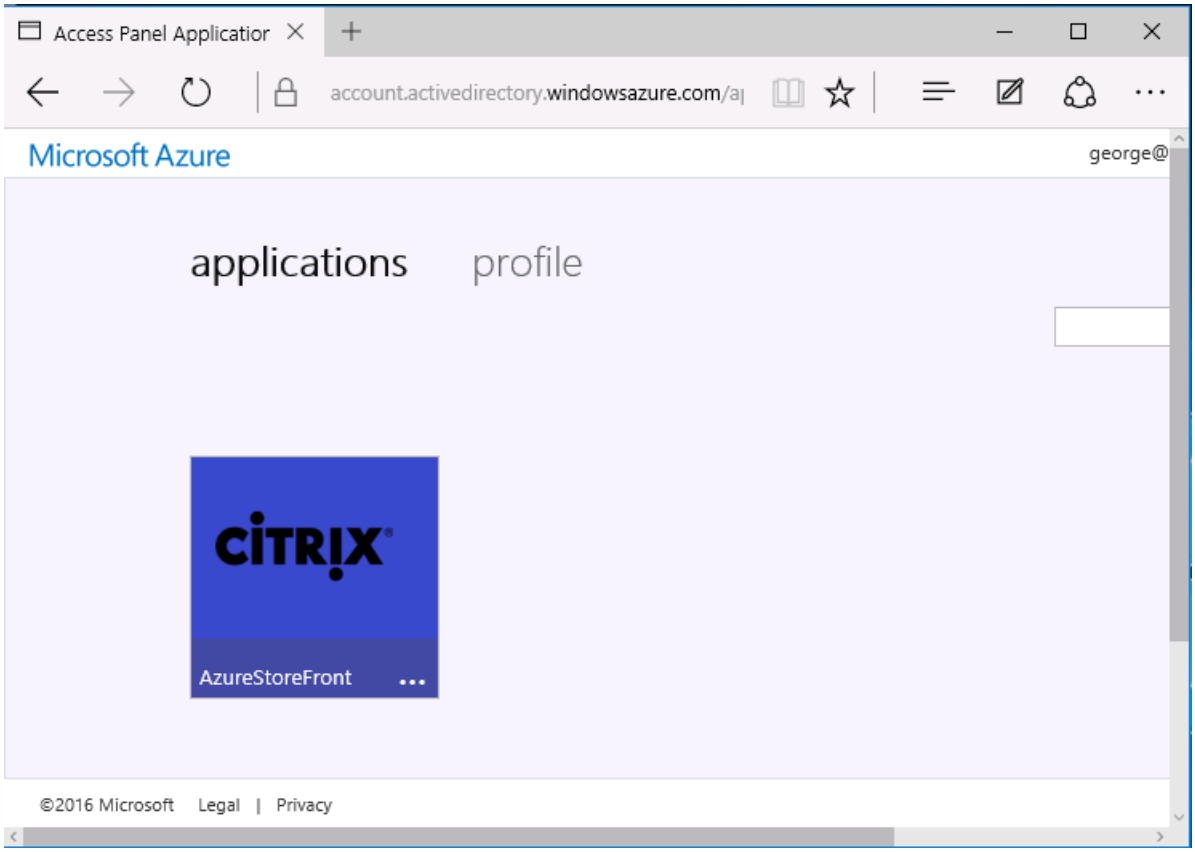
L'exemple de déploiement dans ce document décrit un système dans lequel l’informatique fournit aux nouveaux utilisateurs une adresse de messagerie d'entreprise et un code d'inscription pour leurs ordinateurs portables Windows 10 personnels. Les utilisateurs accèdent à ce code via Système > À propos de > Connecter à Azure AD dans le volet **Paramètres**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Une fois que l'ordinateur portable est inscrit, le navigateur Web Microsoft Edge se connecte automatiquement aux sites Web de l'entreprise et aux applications publiées Citrix via la page Web d'applications Azure SAAS, avec d'autres applications Azure telles que Microsoft Office 365.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

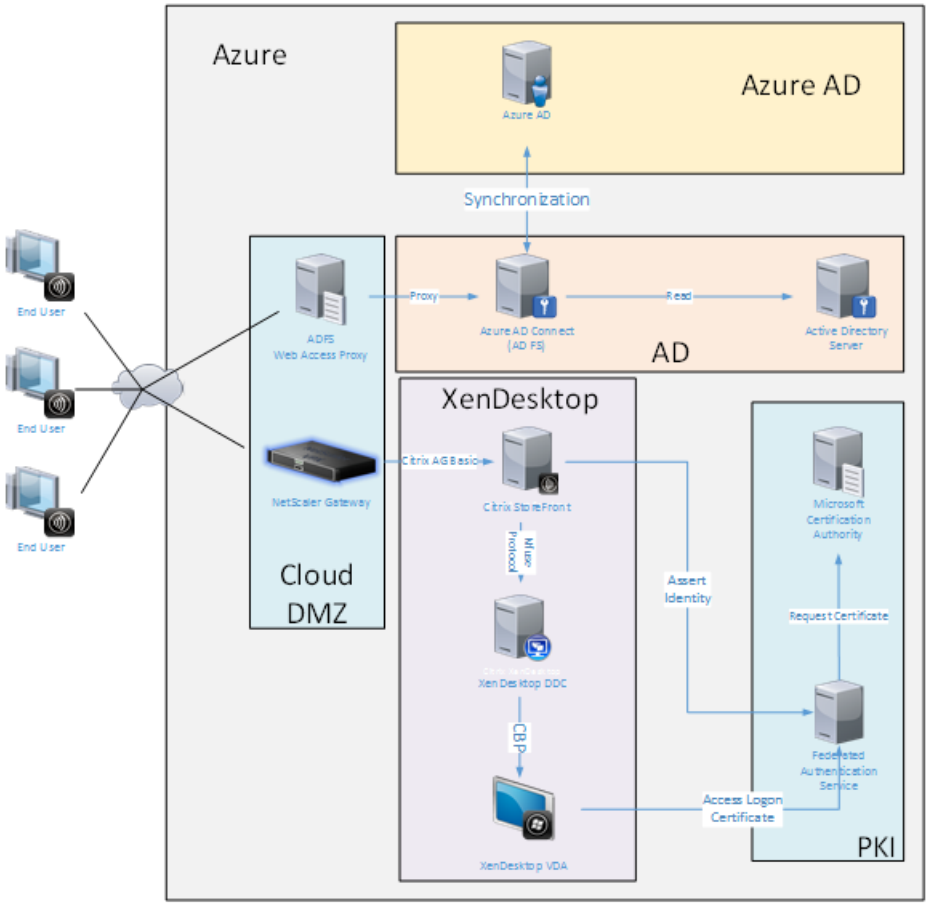


Architecture

Cette architecture réplique un réseau d'entreprise traditionnel dans Azure, tout en intégrant des technologies de cloud modernes telles que Azure AD et Office 365. Les utilisateurs sont considérés comme des travailleurs distants, et la notion d'intranet n'a pas lieu.

Le modèle peut être appliqué aux entreprises disposant déjà de systèmes locaux, car le service de synchronisation Azure AD Connect peut établir un lien à Azure via Internet.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Les connexions sécurisées et l'authentification unique, qui sont traditionnellement derrière un pare-feu sur le LAN et l'authentification NTLM/ Kerberos, sont remplacées dans cette architecture par des connexions TLS à Azure et SAML. Des nouveaux services sont créés à mesure que des applications Azure sont jointes à Azure AD. Les applications existantes qui nécessitent Active Directory (telles qu'une base de données SQL Server) peuvent être exécutées à l'aide d'une VM de serveur Active Directory standard dans la partie IAAS du Azure Cloud Service.

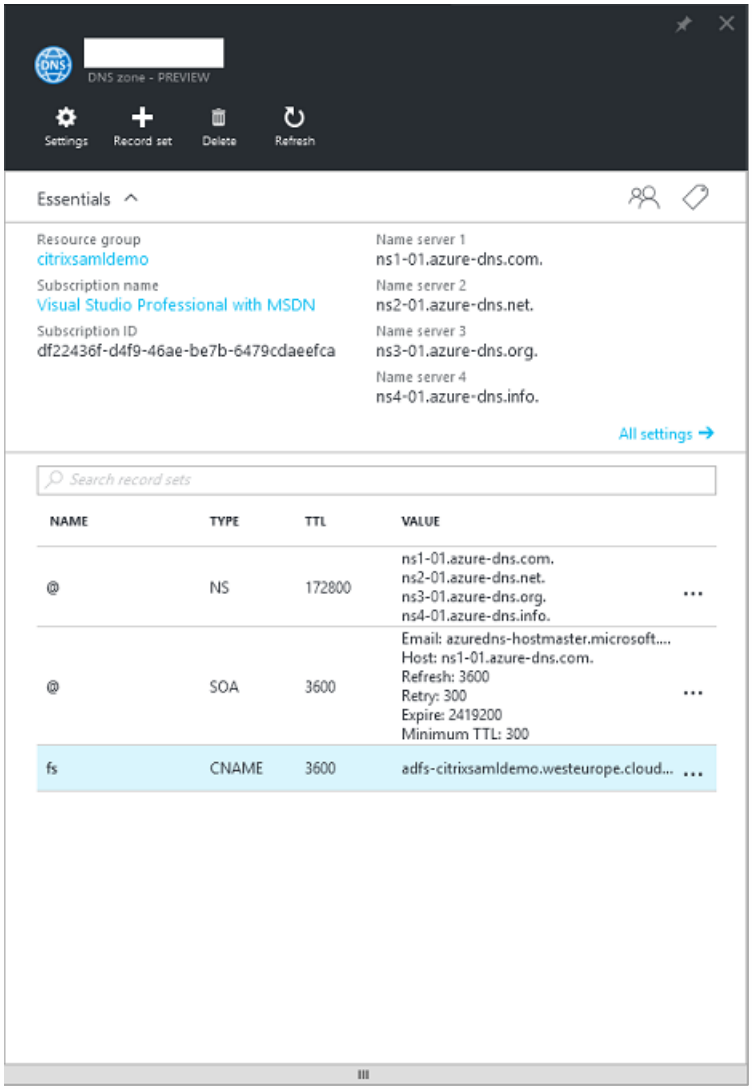
Lorsqu'un utilisateur lance une application traditionnelle, elle est accessible à l'aide des applications publiées XenApp et XenDesktop. Les différents types d'applications sont compilés via la page **Applications Azure** de l'utilisateur, à l'aide des fonctionnalités d'authentification unique de Microsoft Edge. Microsoft fournit également des applications Android et iOS qui peuvent énumérer et lancer des applications Azure.

Créer une zone DNS

Azure AD requiert que l'administrateur ait enregistré une adresse DNS publique et qu'il contrôle la zone de délégation pour le suffixe de nom de domaine. Pour ce faire, l'administrateur peut utiliser la fonctionnalité de zone DNS d'Azure.

Cet exemple utilise le nom de zone DNS « citrixsamldemo.net. »

© 1999-2017 Citrix Systems, Inc. All rights reserved.



La console affiche les noms des serveurs de noms DNS Azure. Ces derniers doivent être référencés dans les entrées NS du bureau d'enregistrement DNS pour la zone (par exemple, citrixsamldemo.net. NS n1-01.azure-dns.com)

Lors de l'ajout de références aux VM exécutées dans Azure, il est plus facile d'utiliser un pointeur CNAME vers l'enregistrement DNS géré par Azure pour la VM. Si l'adresse IP de la VM change, vous n'aurez pas besoin de mettre à jour manuellement le fichier de la zone DNS.

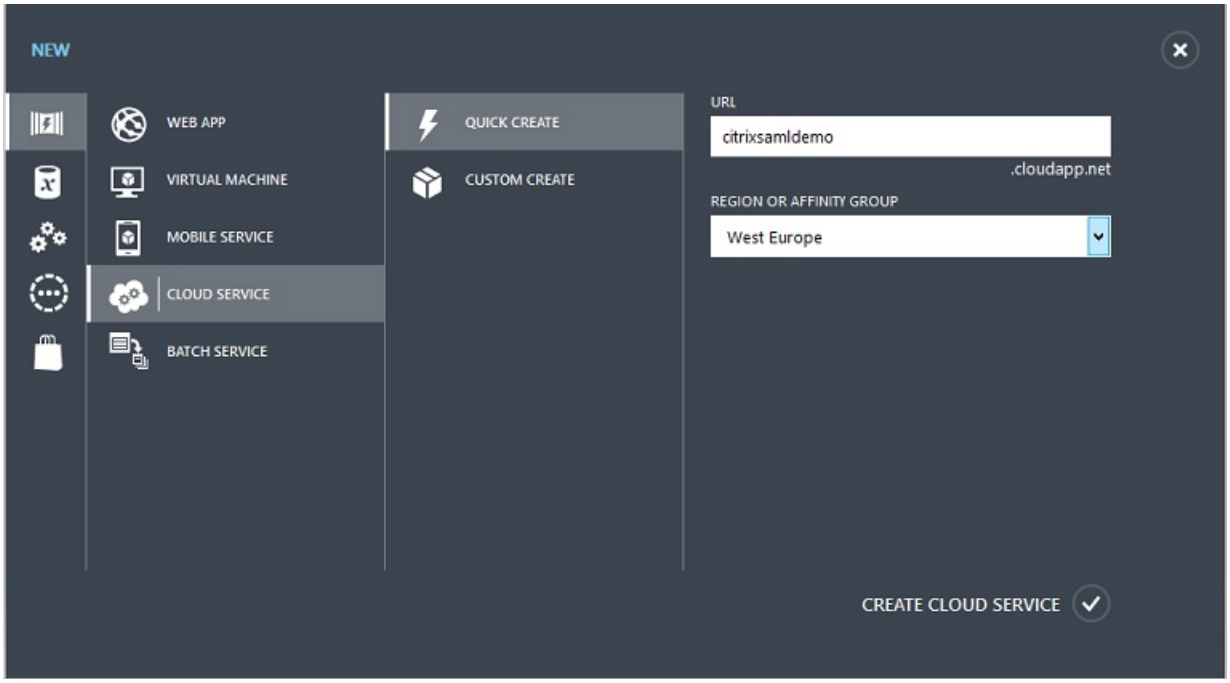
Les suffixes des adresses DNS internes et externes correspondront pour ce déploiement. Le domaine est citrixsamldemo.net, et utilise un split DNS (10.0.0.* en interne).

Ajoutez une entrée « fs.citrixsamldemo.net » qui fait référence au serveur proxy d'application Web (pointant vers wap-citrixsamldemo ... ci-dessus). Il s'agit du service de fédération pour cette zone.

Créer un service de cloud

Cet exemple configure un environnement Citrix comprenant un environnement Active Directory avec un serveur ADFS exécuté dans Azure. Un service de cloud appelé « citrixsamldemo » est créé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

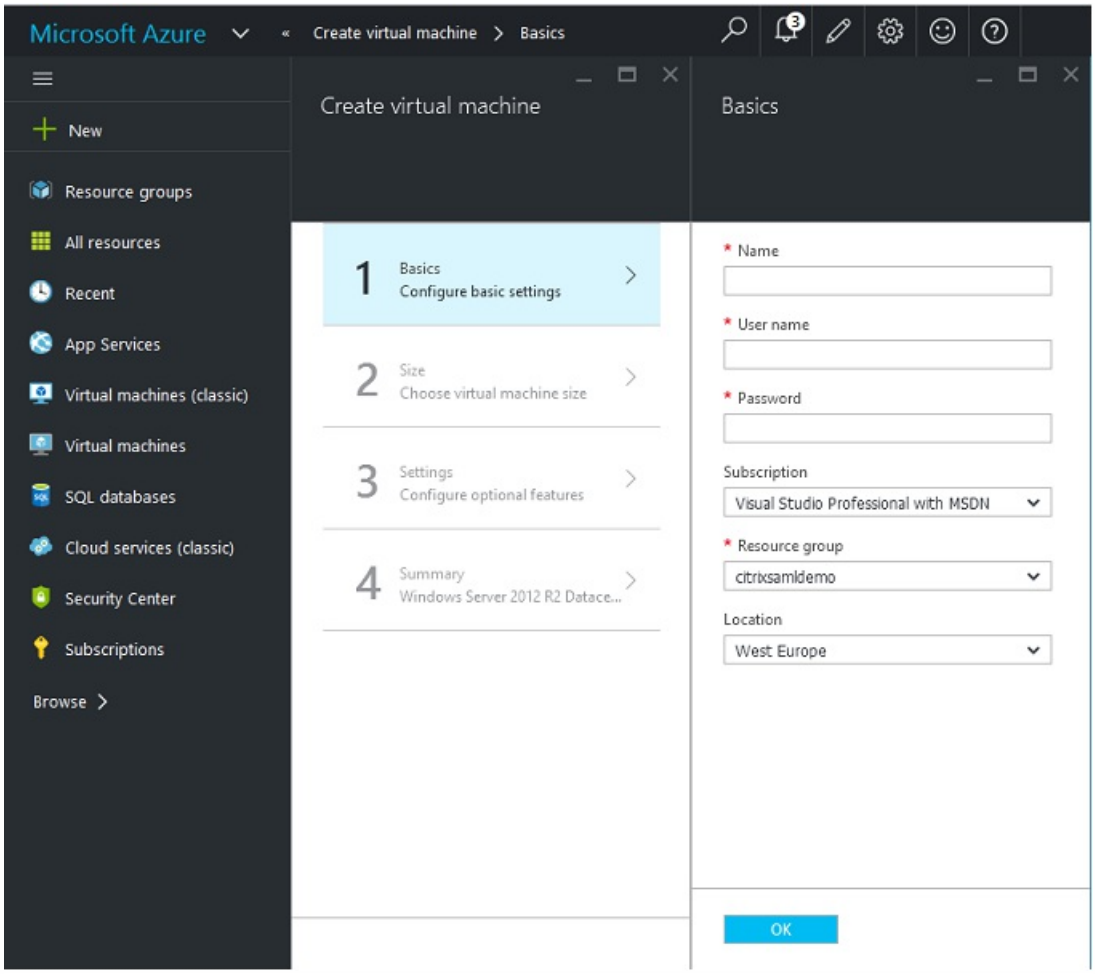


Créer des machines virtuelles Windows

Créez cinq VM Windows exécutées dans le service de cloud :

- Contrôleur de domaine (domaincontrol)
- Serveur ADFS Azure Connect (adfs)
- Proxy d'accès Web ADFS (proxy d'application Web, non joint à un domaine)
- Citrix XenDesktop Delivery Controller (ddc)
- Citrix XenDesktop Virtual Delivery Agent (vda)

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Contrôleur de domaine

- Ajoutez les rôles **Serveur DNS** et **Services de domaine Active Directory** pour créer un déploiement Active Directory standard (dans cet exemple, citrixsamldemo. net). Une fois la promotion de domaine terminée, ajoutez le rôle **Services de certification Active Directory**.
- Créez un compte d'utilisateur normal pour le test (par exemple, George@citrixsamldemo.net).
- Étant donné que ce serveur exécutera le DNS interne, tous les serveurs doivent faire référence à ce serveur pour la résolution DNS. Cette opération peut être effectuée au travers de la page des **paramètres Azure DNS**. (Pour de plus amples informations, consultez la section Annexe dans ce document).

Contrôleur ADFS et serveur proxy d'application Web

- Joignez le serveur ADFS au domaine citrixsamldemo. Le serveur proxy d'application Web doit rester dans un groupe de travail isolé, vous devez donc enregistrer une adresse DNS manuellement avec le DNS AD.
- Exécutez l'applet de commande **Enable-PSRemoting –Force** sur ces serveurs afin d'autoriser l'accès à distance PowerShell via les pare-feu depuis l'outil Azure AD Connect.

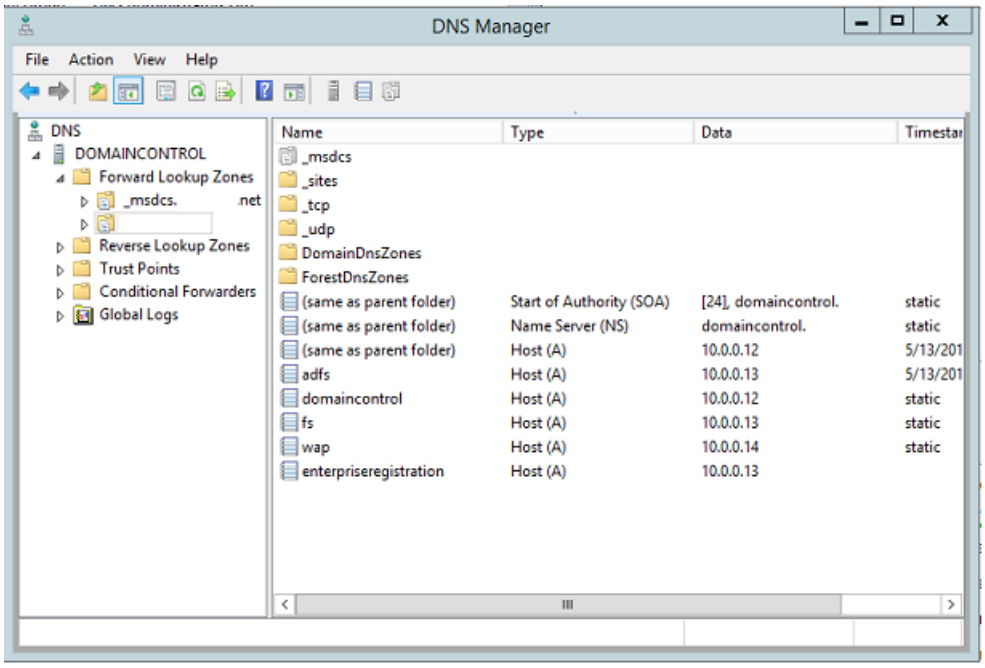
XenDesktop Delivery Controller et VDA

- Installez XenApp ou XenDesktop Delivery Controller et le VDA sur les deux autres serveurs Windows joints à citrixsamldemo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurer un DNS interne

Une fois le contrôleur de domaine installé, configurez le serveur DNS afin de gérer l'affichage interne de citrixsamldemo.net, et d'agir en tant que redirecteur vers un serveur DNS externe (par exemple : 8.8.8.8).

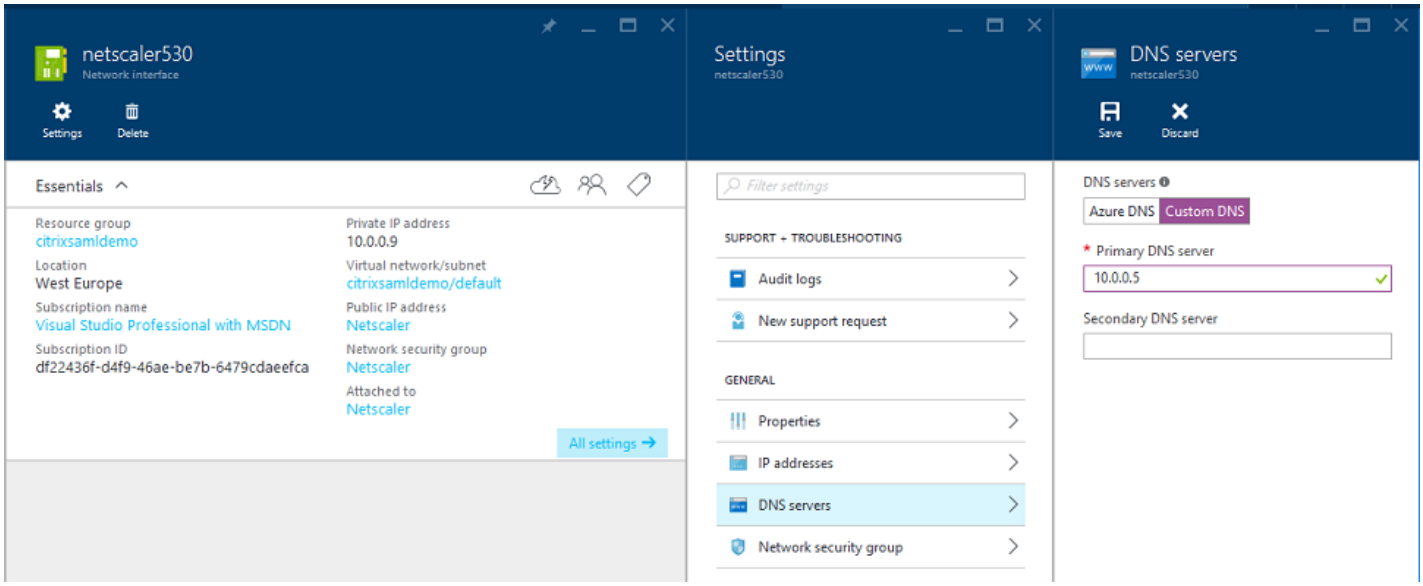


Ajoutez un enregistrement statique pour :

- wap.citrixsamldemo.net [la VM du proxy d'application Web ne sera pas jointe au domaine]
- fs.citrixsamldemo.net [adresse du serveur de fédération interne]
- enterpriseregistration.citrixsaml.net [identique à fs.citrixsamldemo.net]

Toutes les VM exécutées dans Azure doivent être configurées pour utiliser uniquement ce serveur DNS. Vous pouvez effectuer cette opération à l'aide de l'interface réseau.

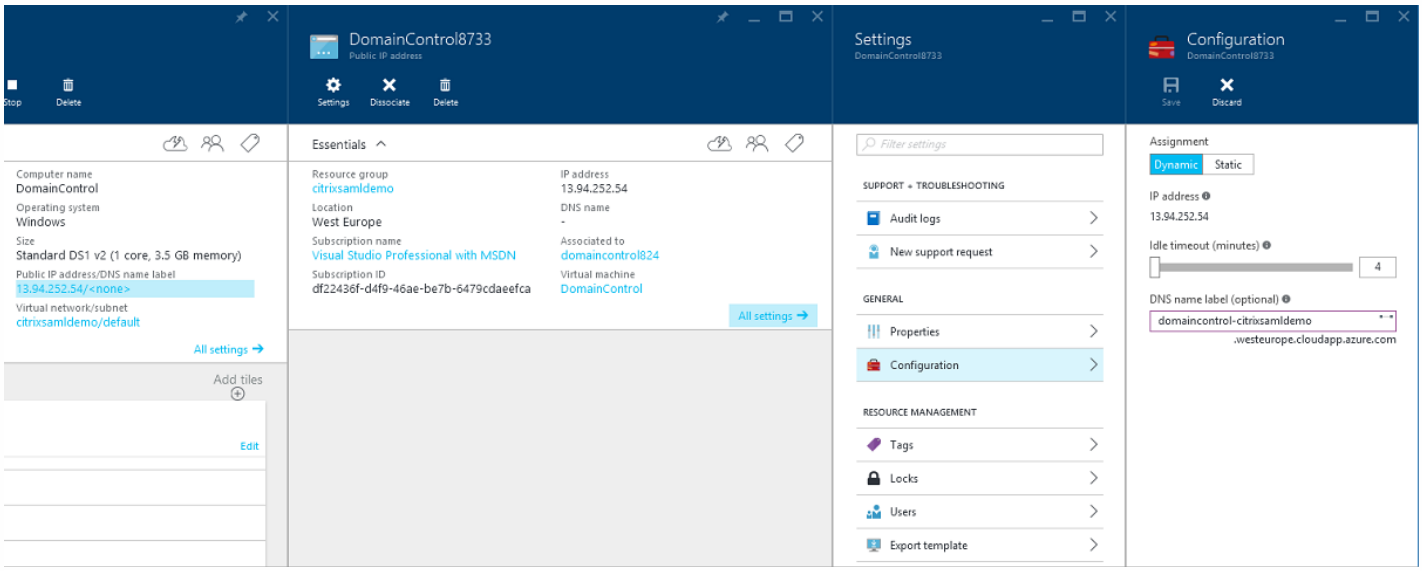
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Par défaut, l'adresse IP interne (10.0.0.9) est attribuée de manière dynamique. Vous pouvez utiliser le paramètre d'adresses IP pour attribuer l'adresse IP de manière permanente. Ceci doit être effectué pour le serveur proxy d'application Web et le contrôleur de domaine.

Configurer une adresse DNS externe

Lorsqu'une VM est en cours d'exécution, Azure gère son propre serveur de zone DNS qui pointe vers l'adresse IP publique attribuée à la VM. Il est utile d'activer cette fonctionnalité car Azure attribue par défaut des adresses IP au démarrage de chaque VM.



Cet exemple attribue l'adresse DNS domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com au contrôleur de domaine.

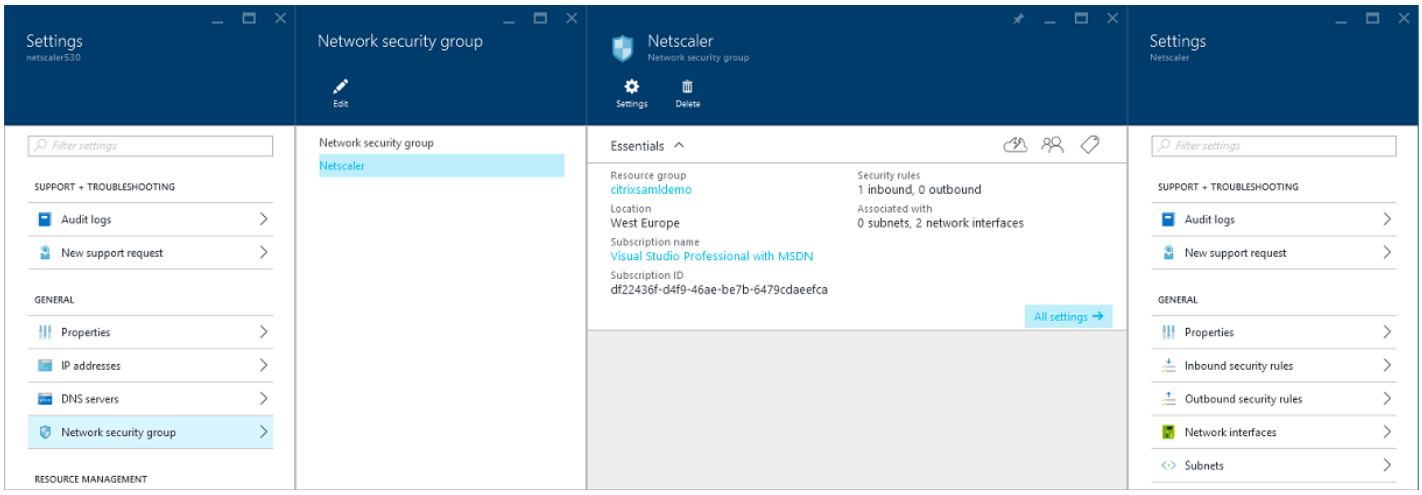
Notez que lorsque la configuration distante est terminée, seuls le proxy d'application Web et les VM NetScaler doivent

© 1999-2017 Citrix Systems, Inc. All rights reserved.

disposer d'adresses IP publiques. (Lors de la configuration, l'adresse IP publique est utilisée pour accéder à distance à l'environnement).

Configurer des groupes de sécurité

Le cloud Azure gère les règles de pare-feu pour l'accès TCP/UDP aux VM à partir d'Internet à l'aide de groupes de sécurité. Par défaut, toutes les VM autorisent l'accès RDP. Les serveurs NetScaler et proxy d'application Web doivent également autoriser TLS sur le port 443.



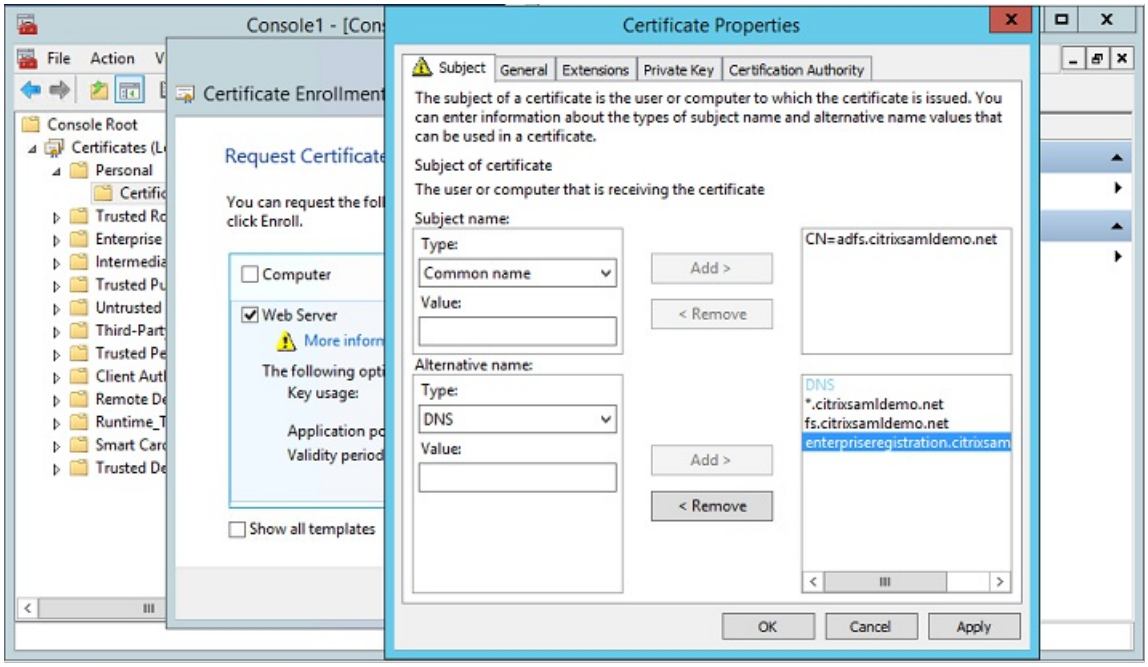
Créer un certificat d'ADFS

Activez le modèle de certificat **Serveur Web** sur l'autorité de certification Microsoft (CA). Ceci permet la création d'un certificat avec des adresses DNS personnalisées qui peuvent être exportées (y compris la clé privée) sur un fichier pfx. Vous devez installer ce certificat sur les serveurs ADFS et proxy d'applications Web, par conséquent le fichier pfx est l'option préférée.

Émettez un certificat de serveur Web avec les noms de sujets suivants :

- Commonname:
  - adfs.citrixsamldemo.net [nom d'ordinateur]
- SubjectAltname:
  - *.citrixsamldemo.net [nom de zone]
  - fs.citrixsamldemo. net [entrée dans le DNS]
  - enterpriseregistration.citrixsamldemo.net

© 1999-2017 Citrix Systems, Inc. All rights reserved.



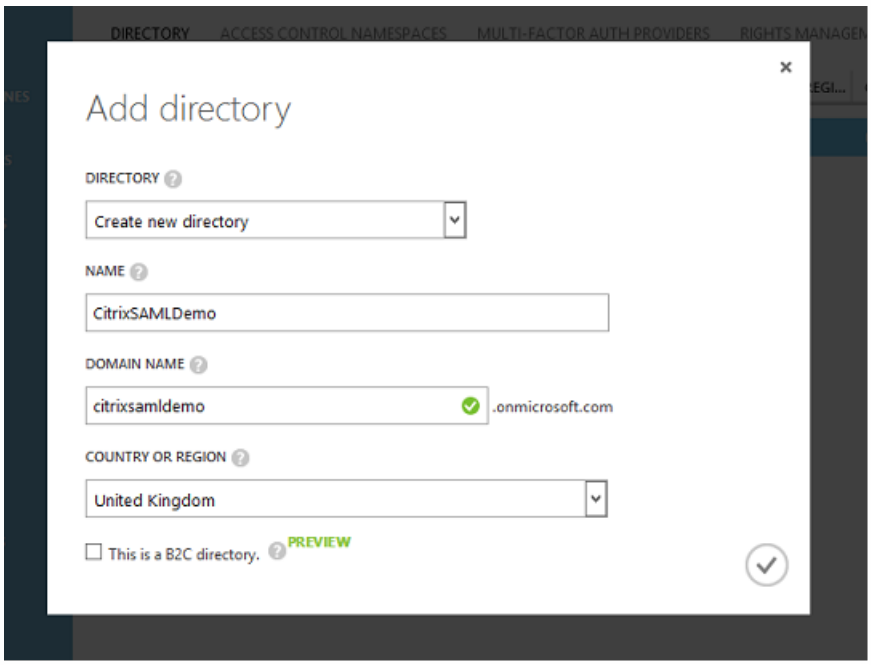
Exportez le certificat sur un fichier pfx, y compris une clé privée protégée par mot de passe.

Configurer Azure AD

Cette section décrit en détail la création d'une nouvelle instance Azure AD et la création d'identités utilisateur qui peuvent être utilisées pour joindre Windows 10 à Azure AD.

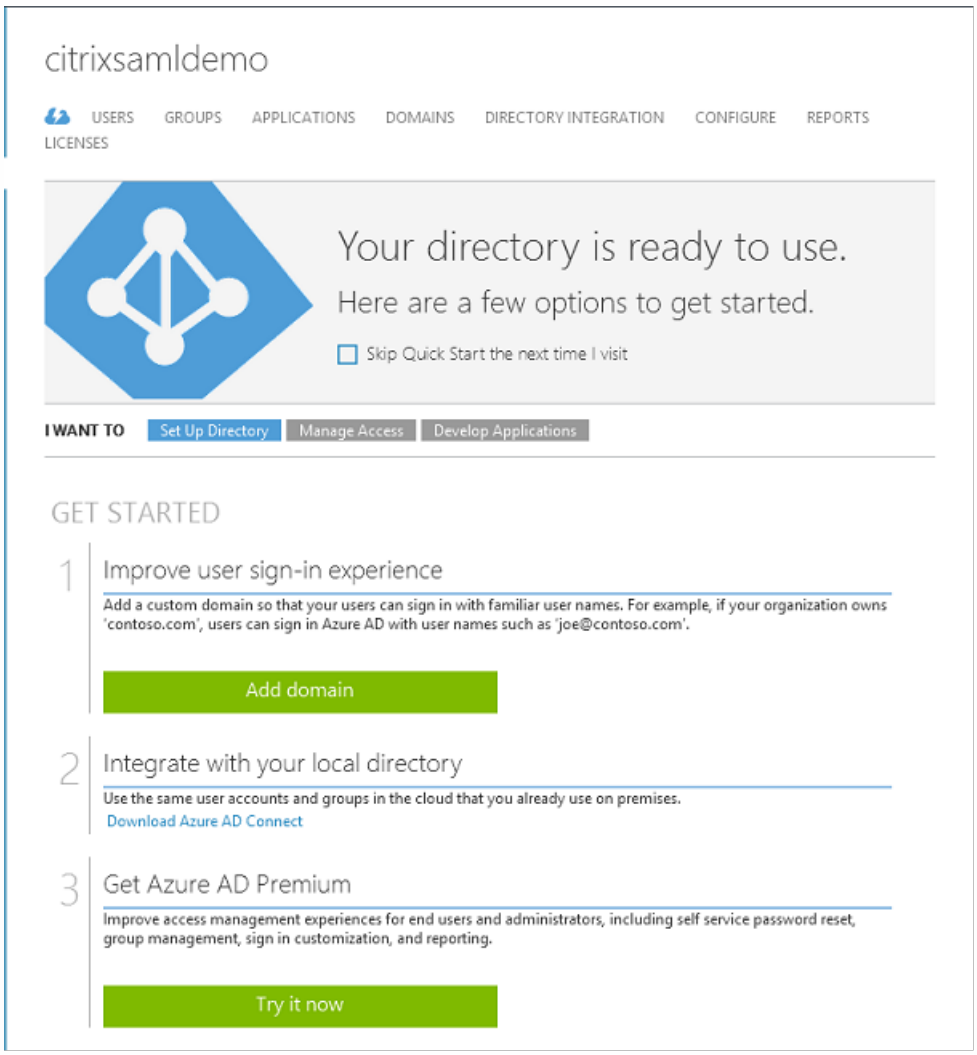
Créer un nouveau répertoire

Ouvrez une session sur le portail Azure et créez un nouveau répertoire.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

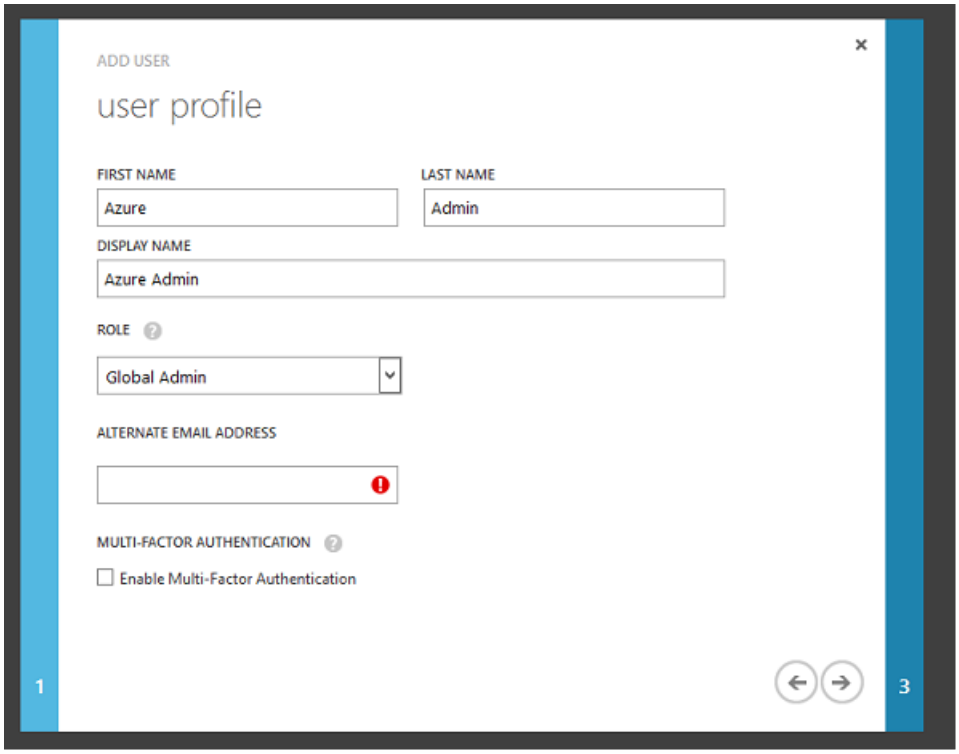
Une fois le répertoire créé, une page de résumé apparaît.



Créer un utilisateur administrateur global (AzureAdmin)

Créez un administrateur global dans Azure (dans cet exemple, AzureAdmin@citrixsamldemo.onmicrosoft.com) et ouvrez une session avec le nouveau compte pour définir un mot de passe.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Enregistrer votre domaine avec Azure AD

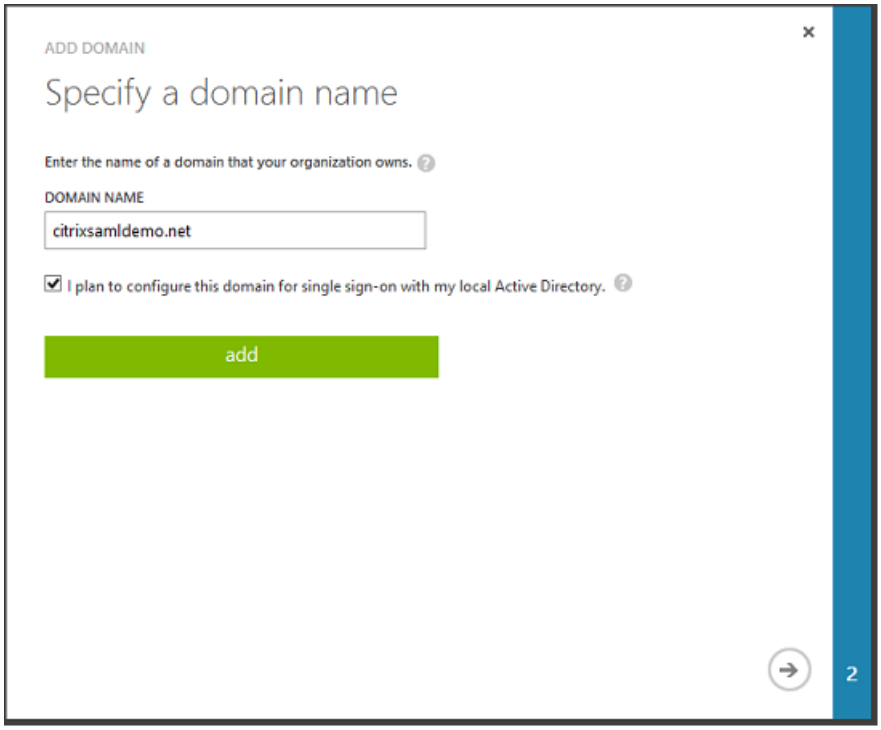
Par défaut, les utilisateurs sont identifiés avec une adresse e-mail au format : *<nom.utilisateur>@<société>.onmicrosoft.com*.

Bien que cela fonctionne sans configuration supplémentaire, une adresse e-mail au format standard est préférable, de préférence une qui correspond au compte de messagerie de l'utilisateur final : @.com

L'action **Ajouter un domaine** configure une redirection de votre domaine d'entreprise réel. Cet exemple utilise citrixsamldemo.net.

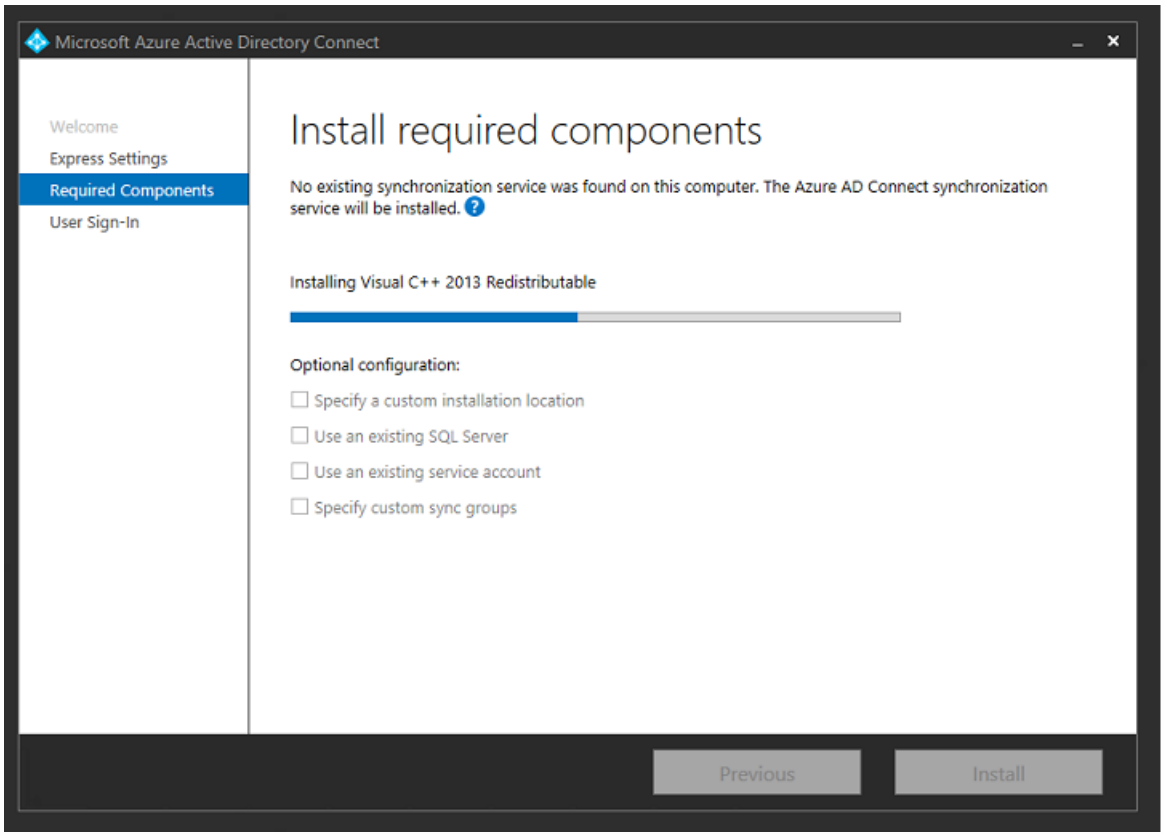
Si vous configurez ADFS pour l'authentification unique, activez la case à cocher.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



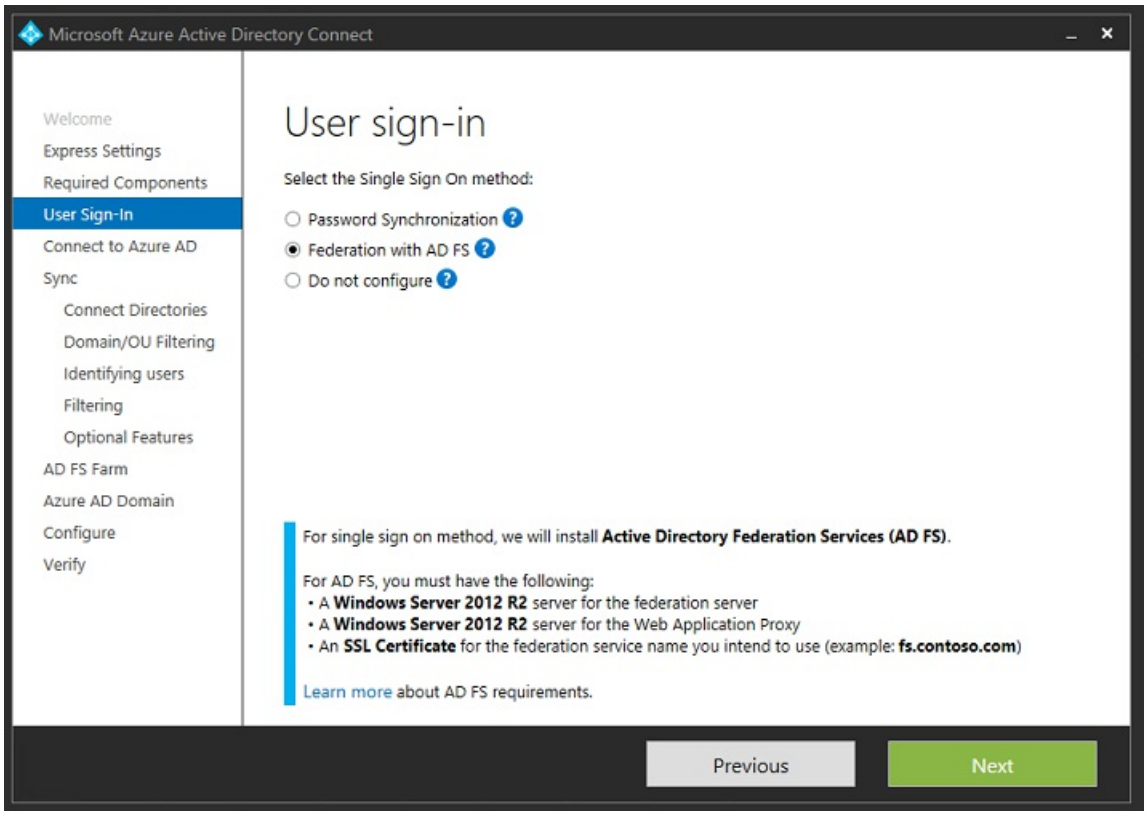
Installer Azure AD Connect

L'étape 2 de l'interface de configuration d'Azure AD redirige l'utilisateur vers la page de téléchargement Microsoft d'Azure AD Connect. Installez ce composant sur la VM ADFS. Utilisez **Installation personnalisée**, plutôt que **Configuration rapide** afin que les options ADFS soient disponibles.

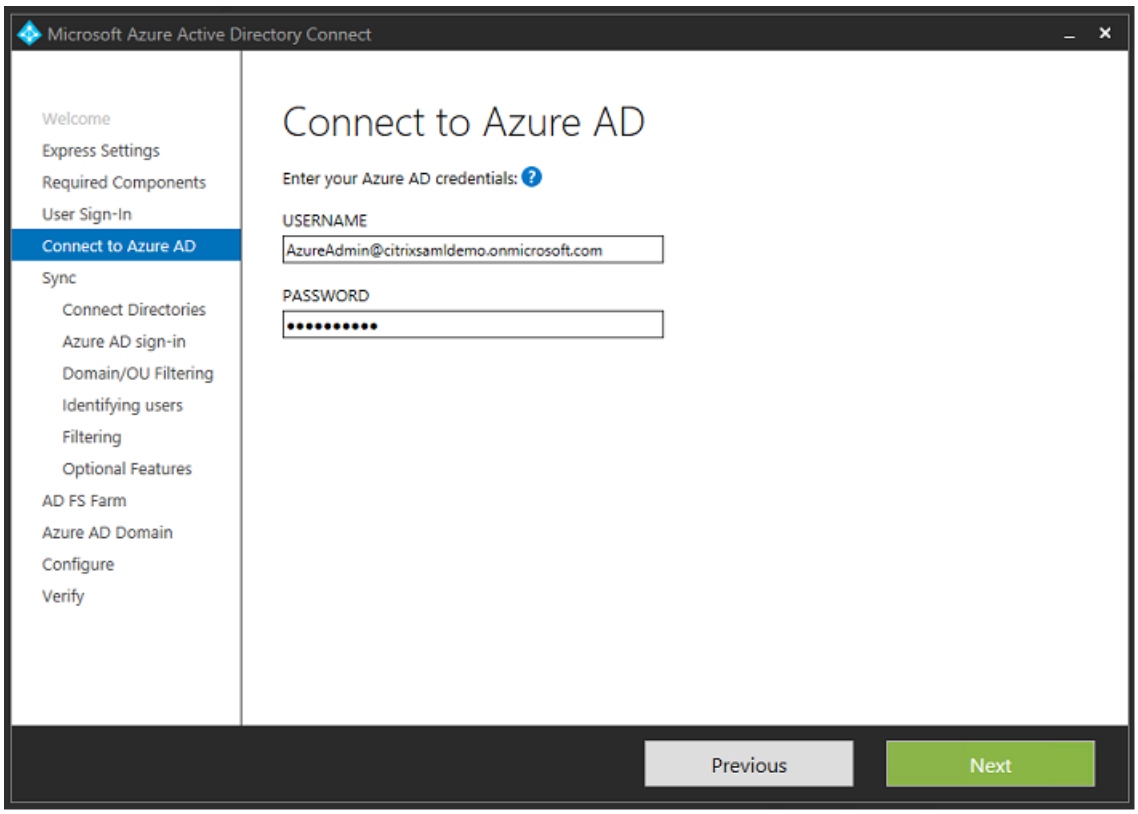


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Sélectionnez l'option d'authentification unique **Fédération avec AD FS**.

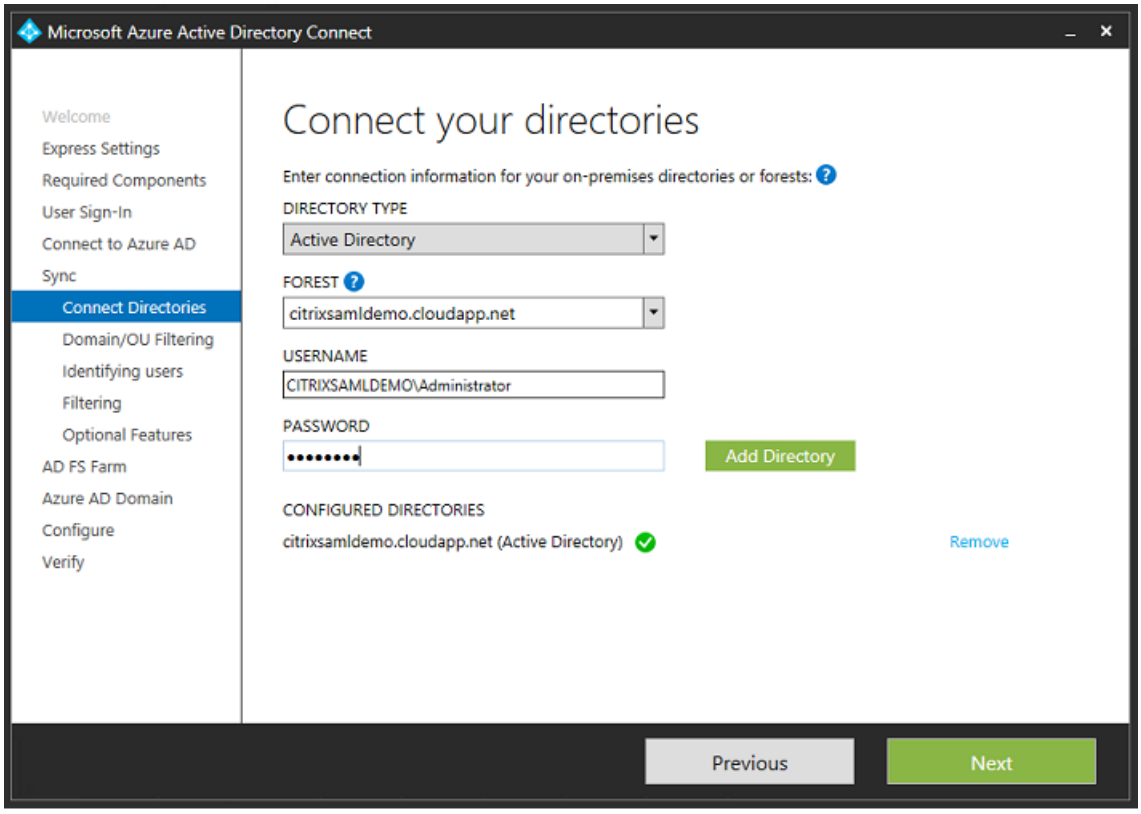


Connectez-vous à Azure avec le compte administrateur que vous avez créé précédemment.



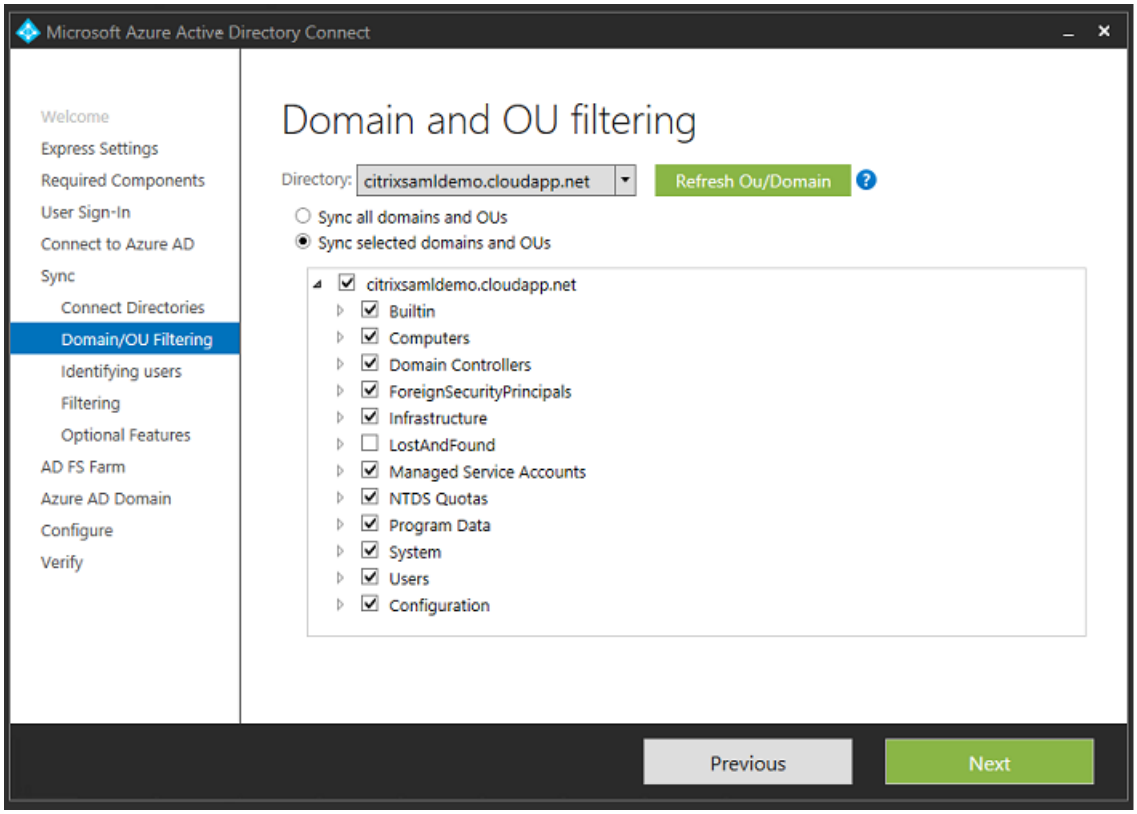
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sélectionnez la forêt AD interne.

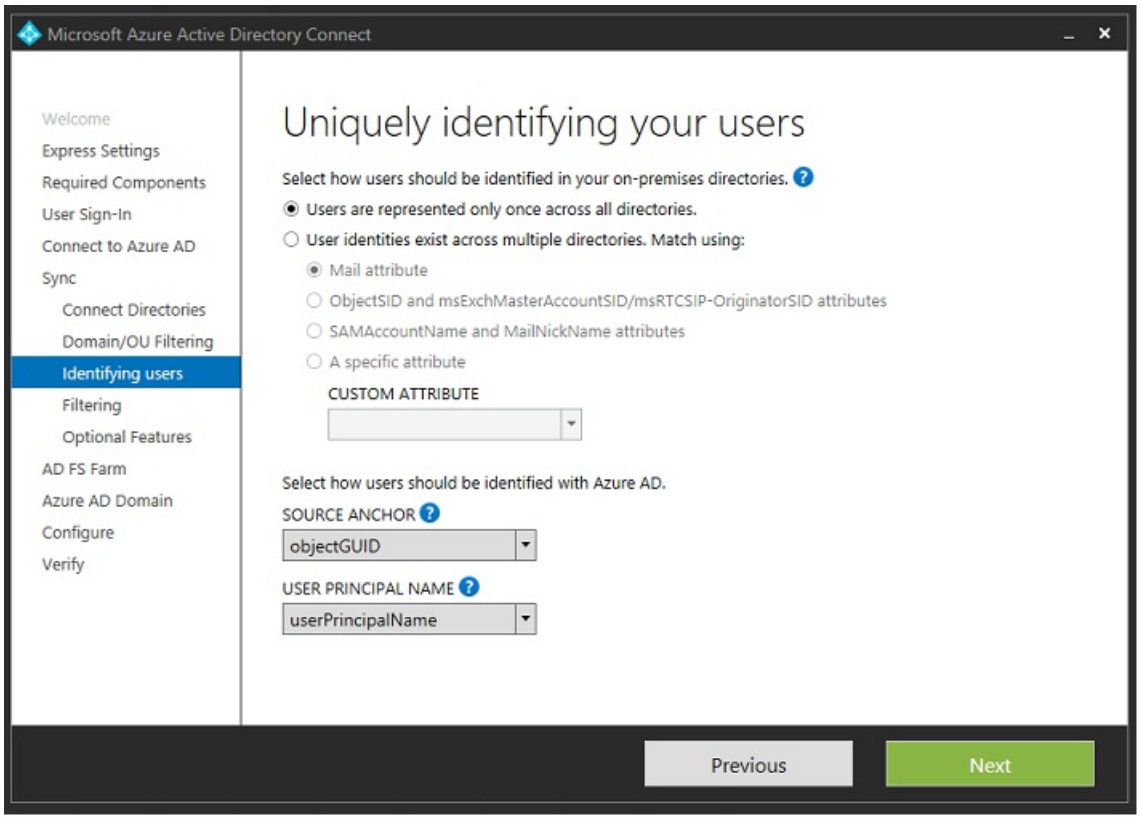


Synchronisez tous les anciens objets Active Directory avec Azure AD.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

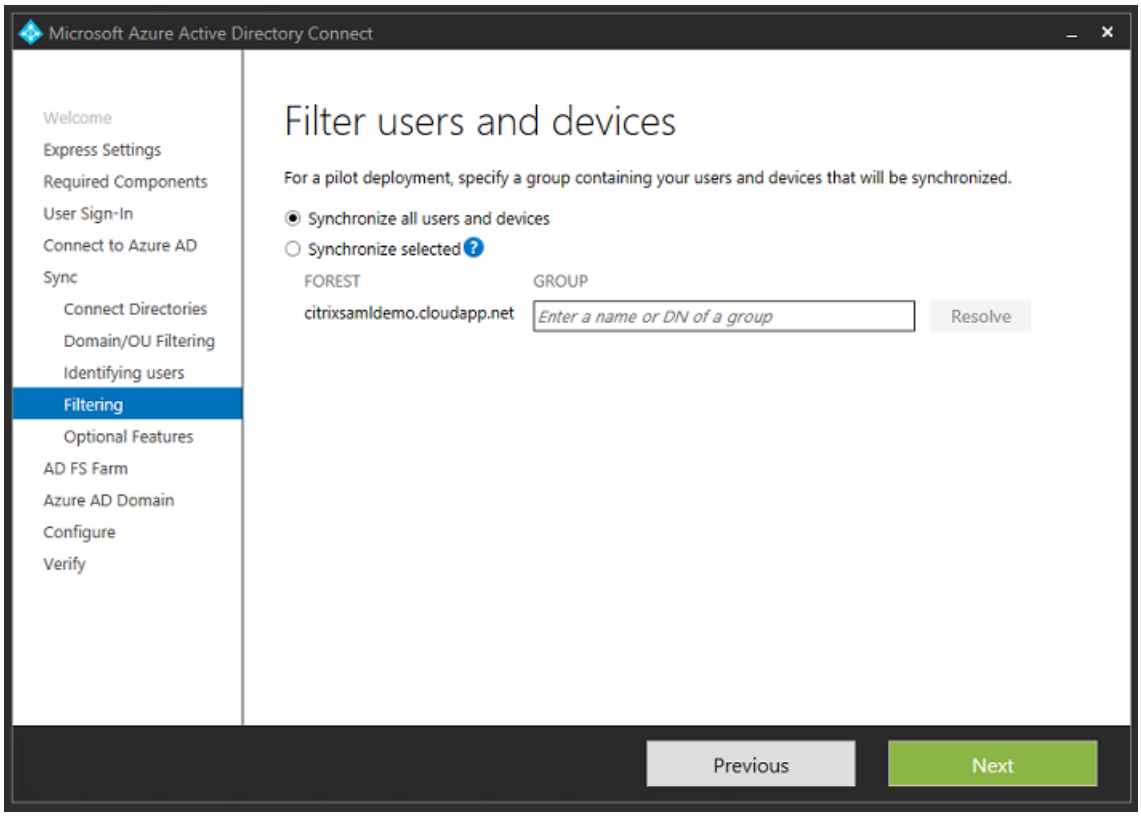


Si la structure de répertoire est simple, les noms d'utilisateur sont suffisamment uniques pour identifier un utilisateur qui ouvre une session.

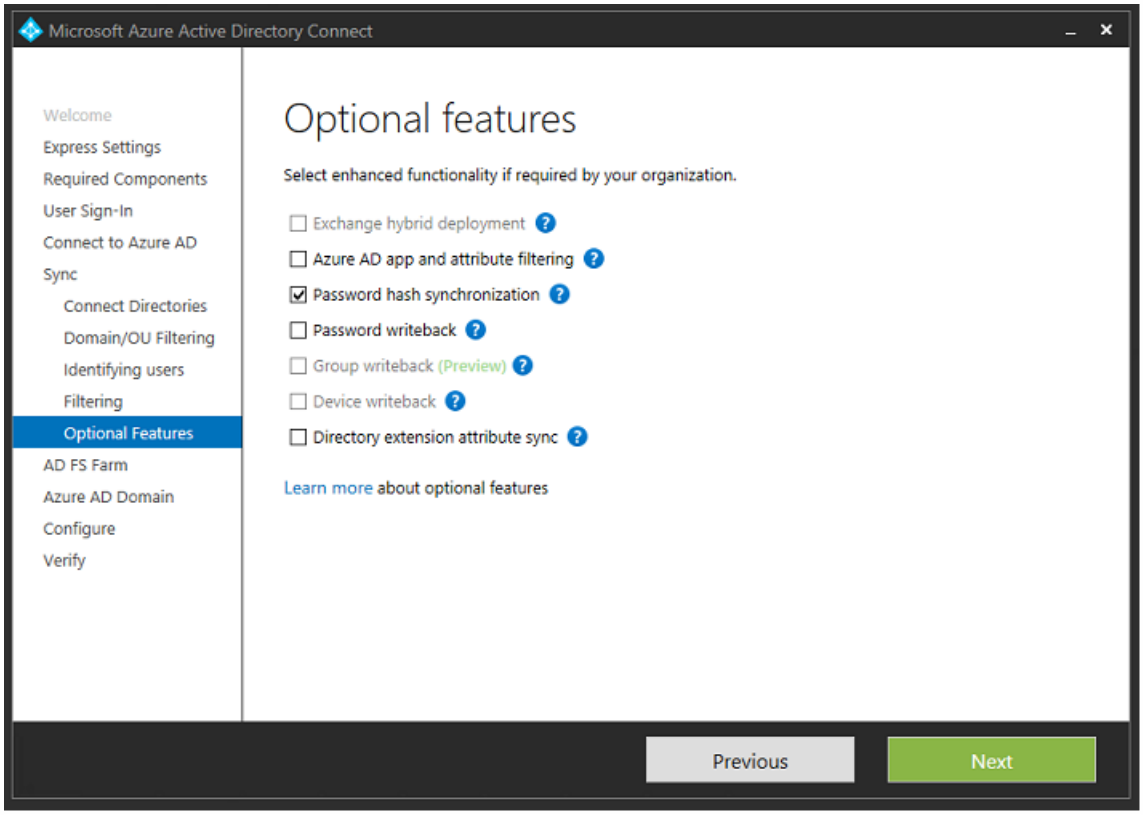


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Acceptez les options de filtrage par défaut, ou limitez les utilisateurs et machines à un ensemble de groupes particulier.

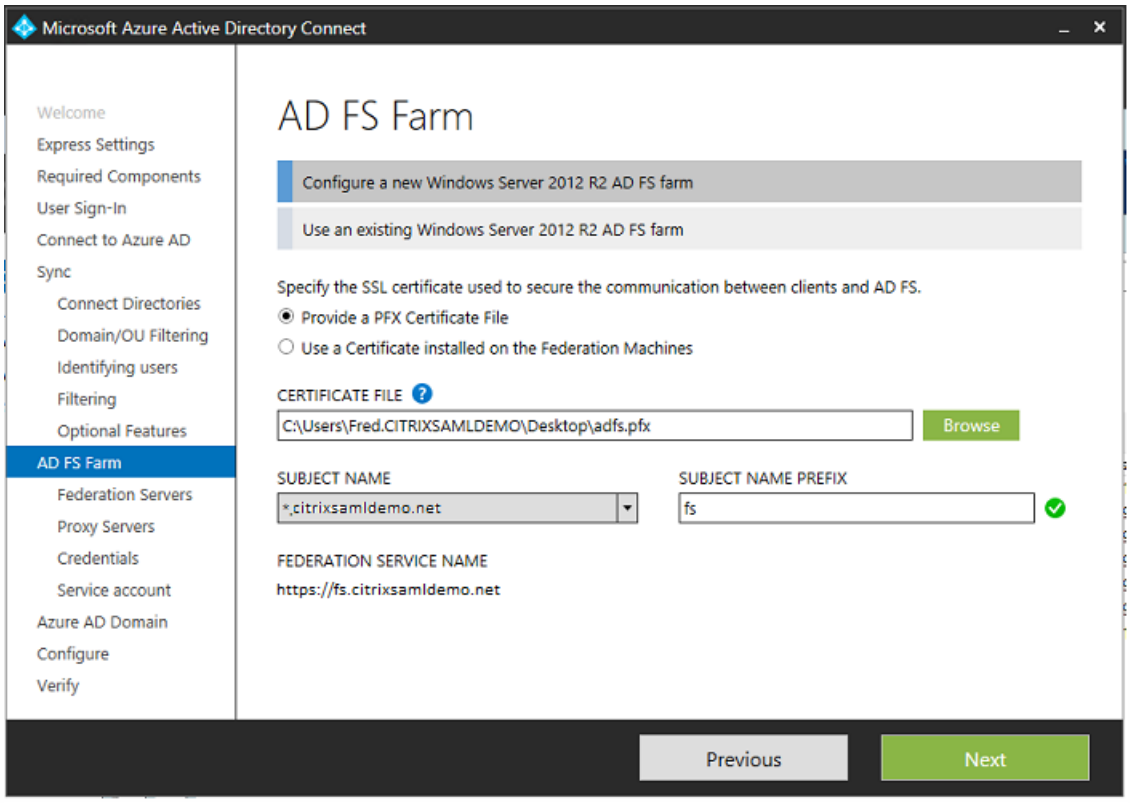


Si vous le souhaitez, vous pouvez synchroniser les mots de passe Azure AD avec Active Directory. Ceci n'est généralement pas nécessaire pour l'authentification ADFS.



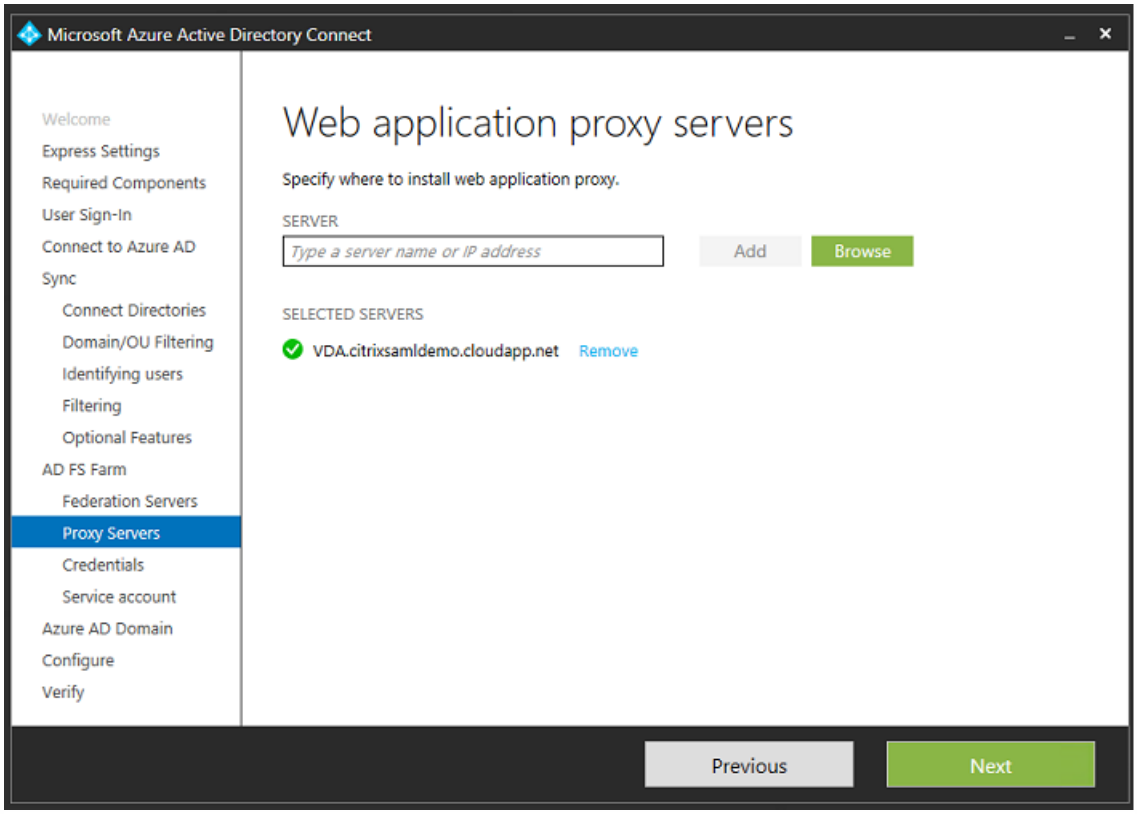
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sélectionnez le fichier .pfx de certificat à utiliser dans ADFS, en spécifiant fs.citrixsamldemo.net en tant que nom DNS.



Lorsque vous êtes invité à sélectionner un serveur proxy, entrez l'adresse du serveur wap.citrixsamldemo.net. Vous devrez peut-être exécuter l'applet de commande **Enable-PSRemoting –Force** en tant qu'administrateur sur le serveur proxy d'application Web, de façon à ce que Azure AD Connect puisse le configurer.

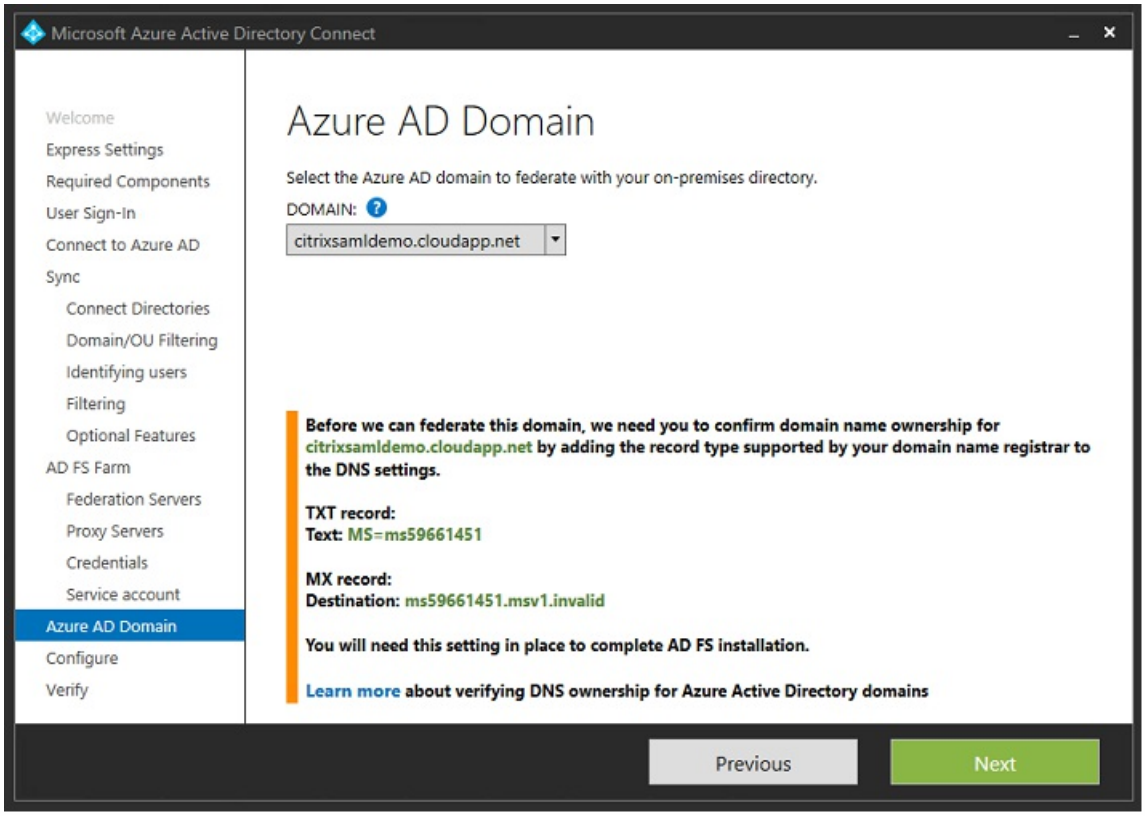
© 1999-2017 Citrix Systems, Inc. All rights reserved.



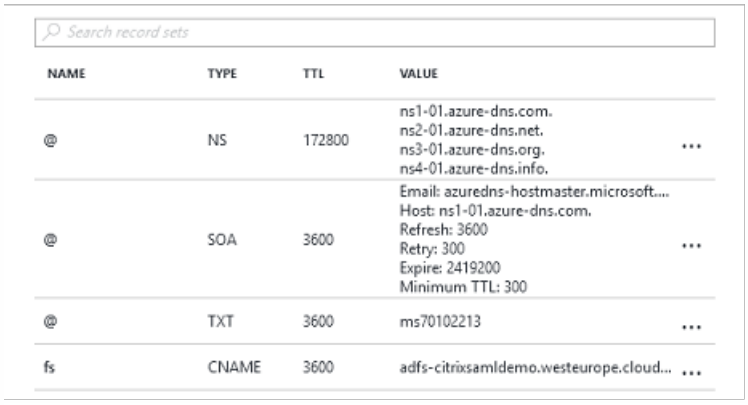
Remarque : si cette étape échoue en raison de problèmes de confiance avec PowerShell à distance, essayez de joindre le serveur proxy d'application Web au domaine.

Pour les étapes restantes de l'assistant, utilisez les mots de passe de l'administrateur et créez un compte de service pour ADFS. Azure AD Connect vous invitera alors à valider l'appartenance de la zone DNS.

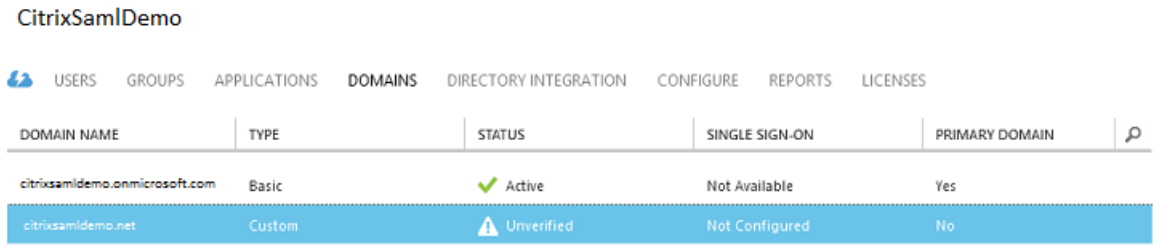
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Ajoutez les enregistrements TXT et MX aux enregistrements d'adresses DNS dans Azure.



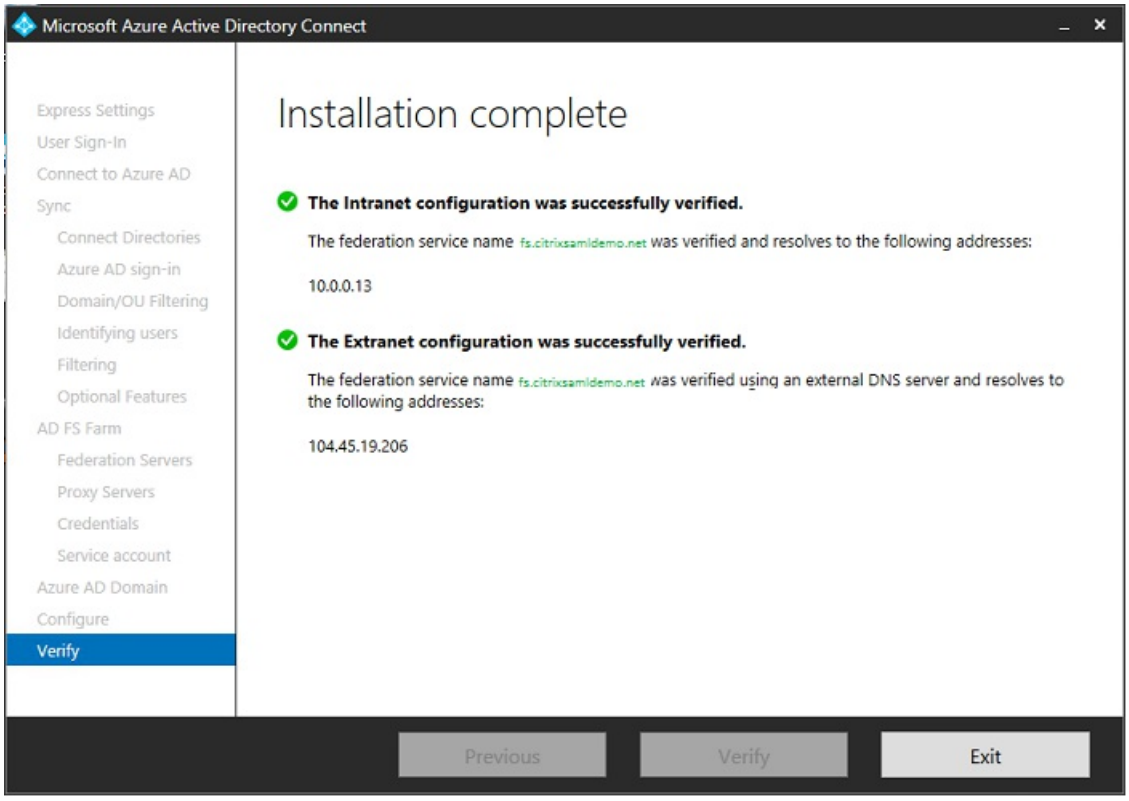
Cliquez sur **Vérifier** dans la console de gestion Azure.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Remarque : si cette étape échoue, vous pouvez vérifier le domaine avant d'exécuter Azure AD Connect.

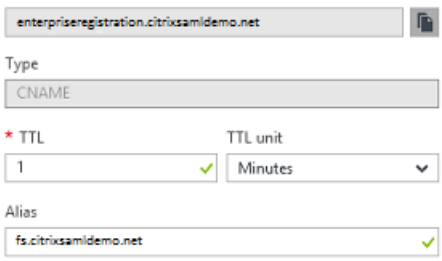
Lorsque l'installation est terminée, l'adresse externe fs.citrixsamldemo.net est contactée sur le port 443.



Activer Azure AD Join (Jonction à un domaine Azure AD)

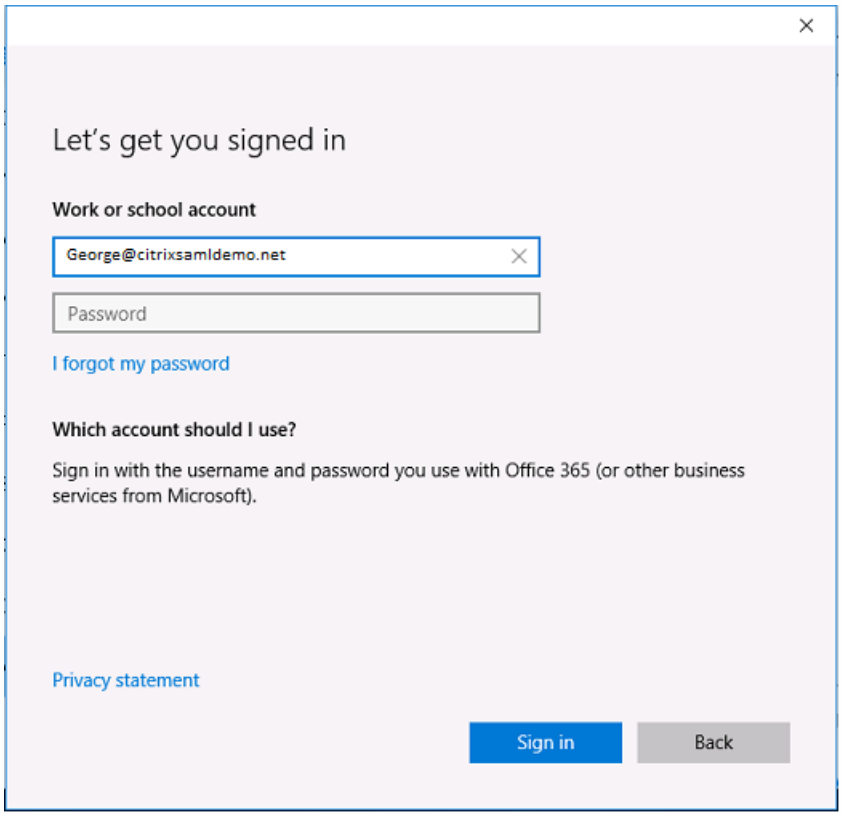
Lorsqu'un utilisateur entre une adresse e-mail afin que Windows 10 puisse réaliser la jonction Azure AD, le suffixe DNS est utilisé pour construire un enregistrement DNS CNAME qui doit pointer vers ADFS : enterpriseregistration..

Dans cet exemple, il s'agit de fs.citrixsamldemo.net.

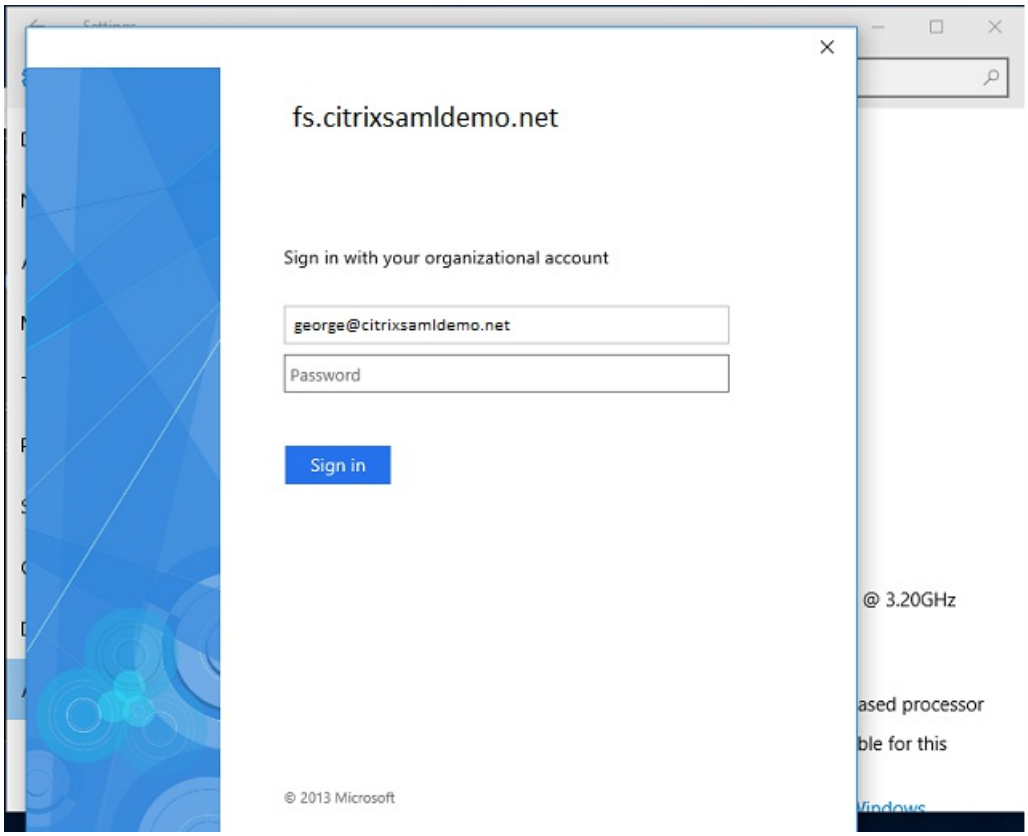


Si vous n'utilisez pas d'autorité de certification publique, assurez-vous que le certificat racine ADFS est installé sur l'ordinateur Windows 10 de façon à ce que Windows fasse confiance au serveur ADFS. Effectuez une jonction de domaine Azure AD à l'aide du compte utilisateur standard généré précédemment.

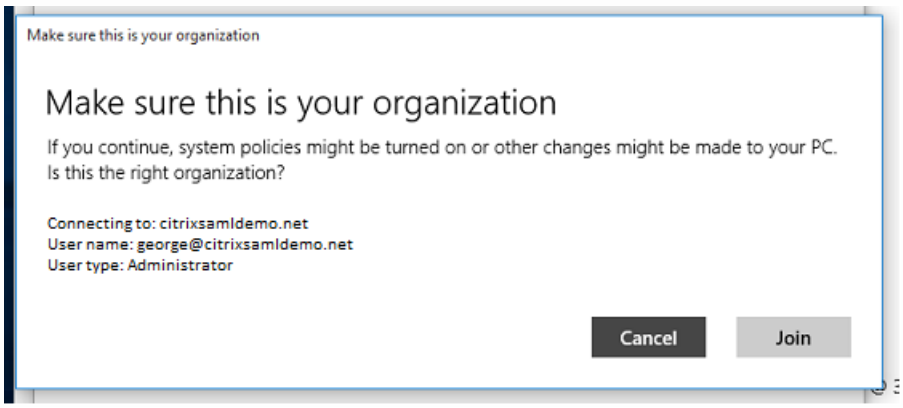
© 1999-2017 Citrix Systems, Inc. All rights reserved.

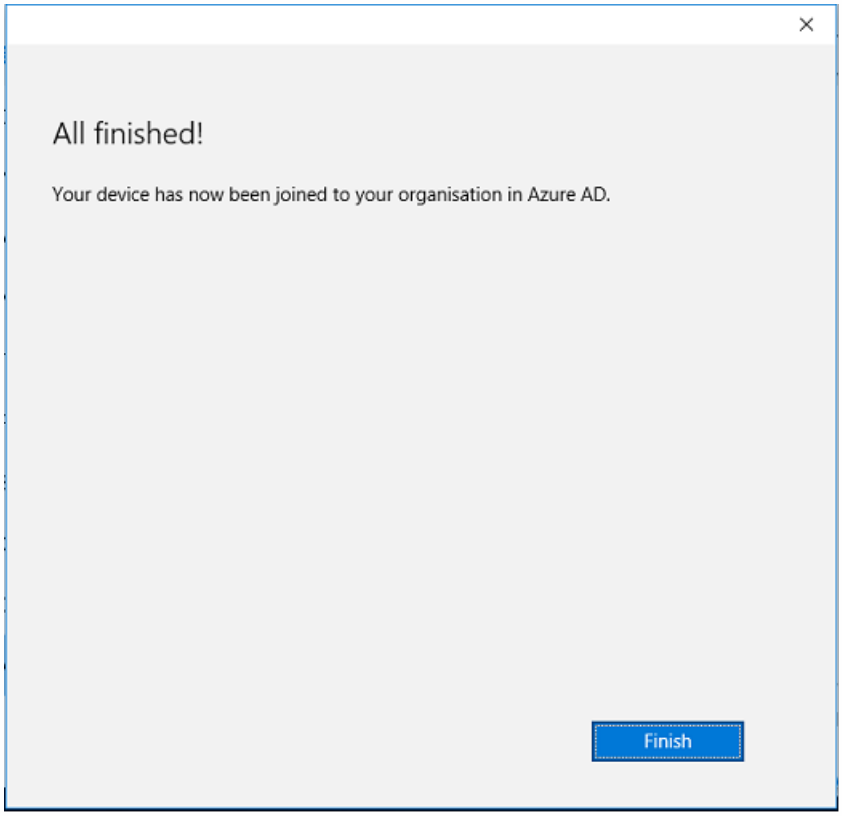


Veuillez noter que le nom UPN doit correspondre au nom UPN reconnu par le contrôleur de domaine ADFS.



 © 1999-2017 Citrix Systems, Inc. All rights reserved.





Vérifiez que la jonction Azure AD a réussi en redémarrant la machine et en ouvrant une session à l'aide de l'adresse e-mail de l'utilisateur. Une fois connecté, lancez Microsoft Edge et connectez-vous à http://myapps.microsoft.com. Le site Web doit utiliser l'authentification unique automatiquement.

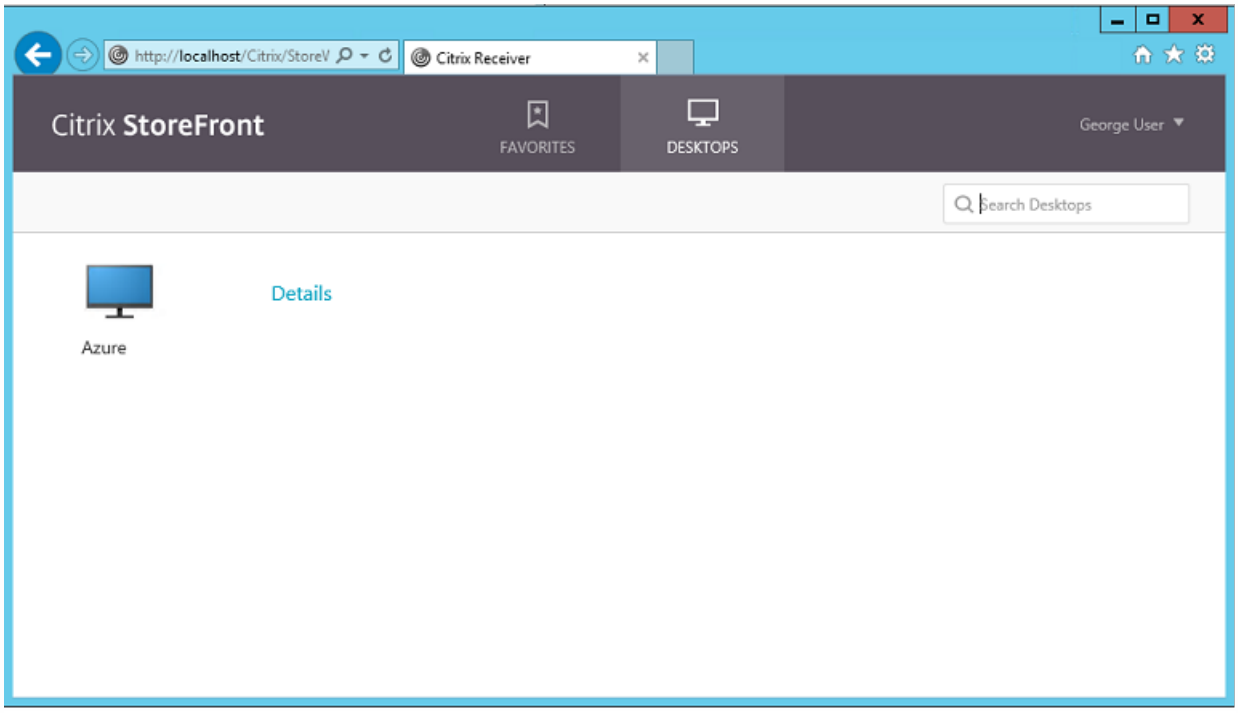
Installer XenApp ou XenDesktop

Vous pouvez installer le Delivery Controller et des machines virtuelles VDA dans Azure directement depuis l'ISO XenApp ou XenDesktop de la manière habituelle.

Dans cet exemple, StoreFront est installé sur le même serveur que le Delivery Controller. Le VDA est installé en tant que travailleur RDS Windows 2012 R2 autonome, sans intégration avec Machine Creation Services (mais cela peut être configuré). Vérifiez que l'utilisateur George@citrixsamldemo.net peut s'authentifier avec un mot de passe avant de

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

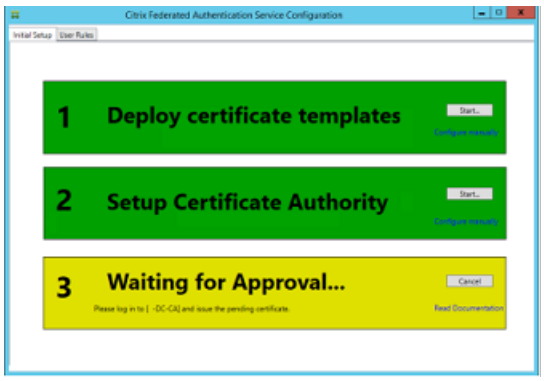
continuer.



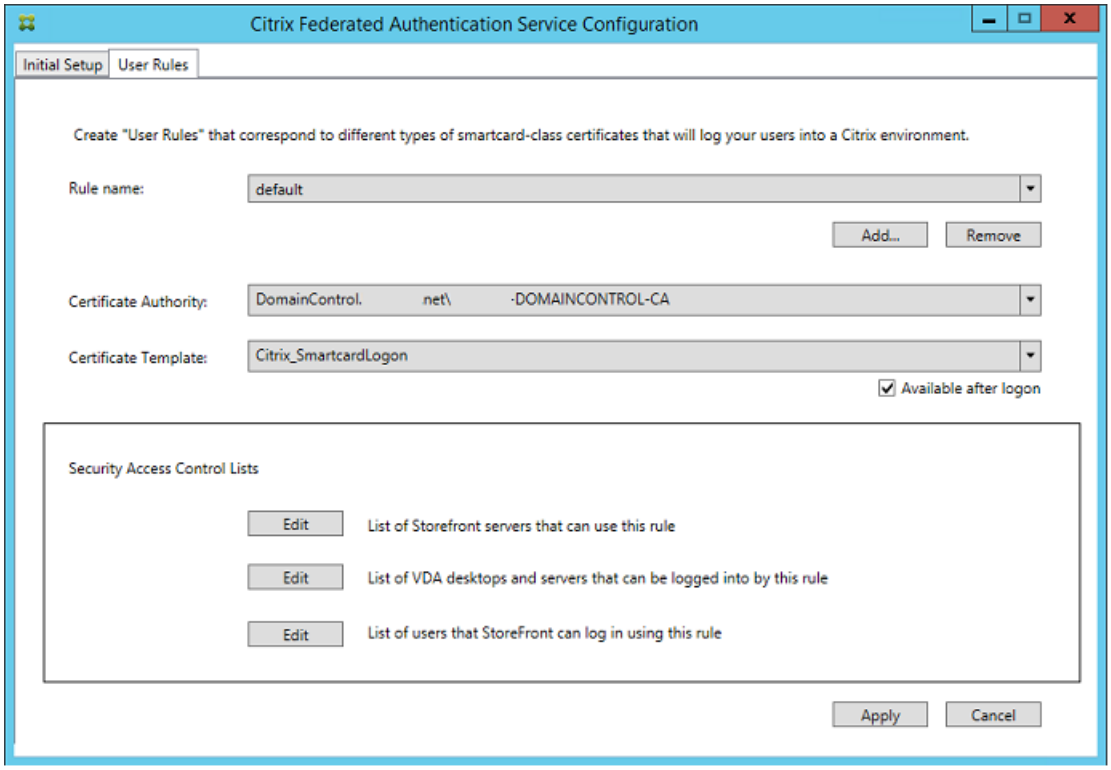
Exécutez l'applet de commande **Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** sur le Controller pour permettre à StoreFront de s'authentifier sans les informations d'identification de l'utilisateur.

Installer le service d'authentification fédérée

Installez le composant Service d'authentification fédérée (FAS) sur le serveur ADFS et configurez une règle pour faire en sorte que le Controller agisse en tant que StoreFront approuvé.

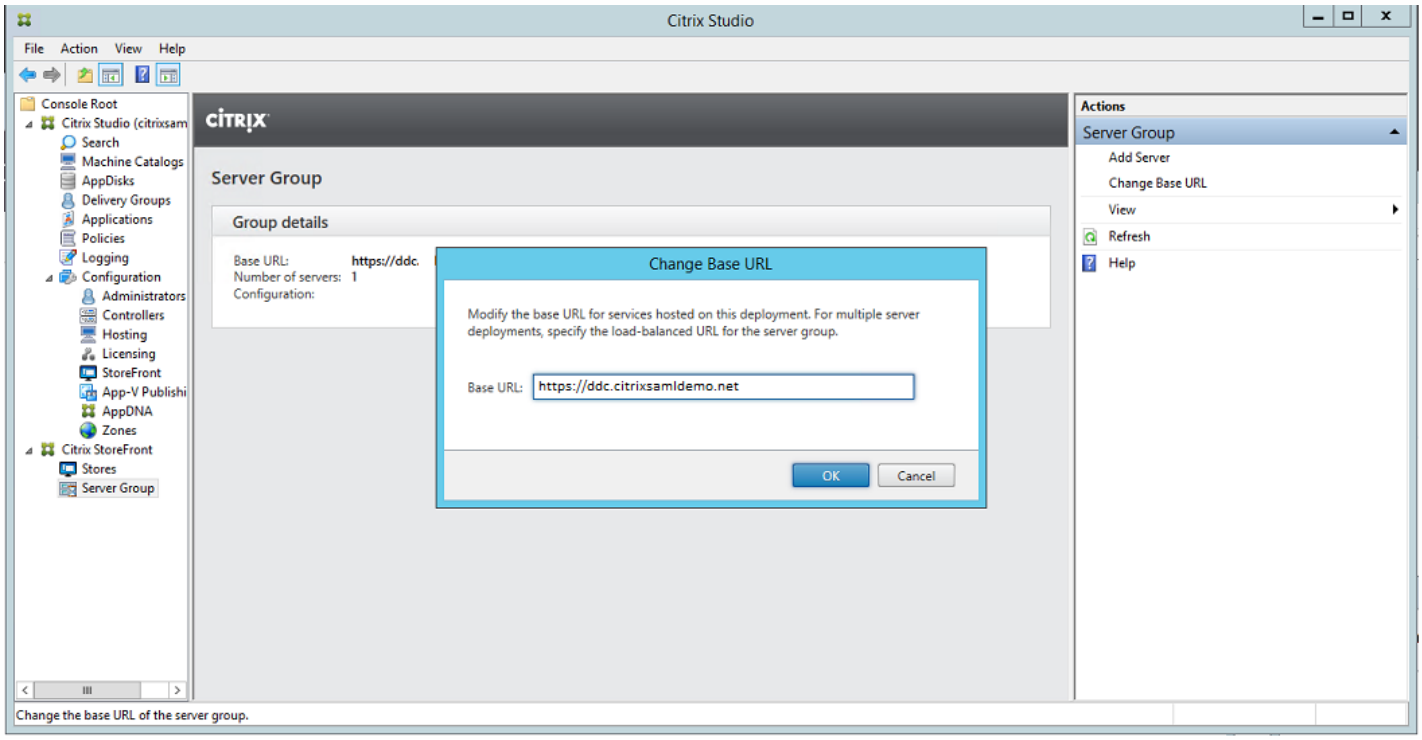


© 1999-2017 Citrix Systems, Inc. All rights reserved.



Configurer StoreFront

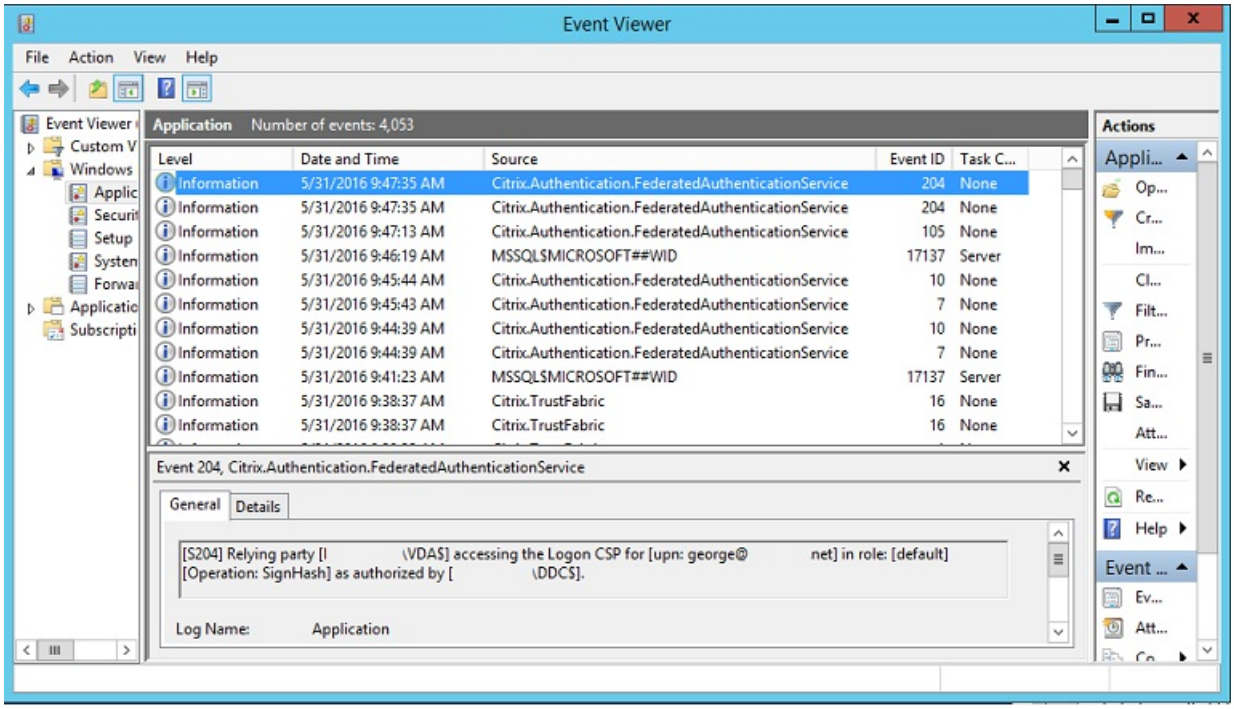
Demandez un certificat d'ordinateur pour le Delivery Controller, et configurez IIS et StoreFront pour utiliser HTTPS en définissant une liaison IIS pour le port 443 et en modifiant l'adresse de base de StoreFront sur https:.



Configurez StoreFront pour utiliser le serveur (FAS) (utilisez le script PowerShell dans l'article Service d'authentification

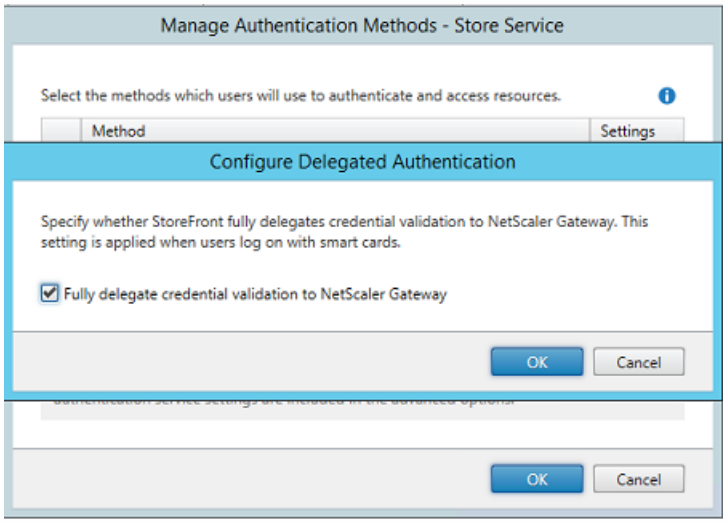
© 1999-2017 Citrix Systems, Inc. All rights reserved.

fédérée) et effectuez des tests en interne dans Azure, en vous assurant que l'ouverture de session utilise le FAS en vérifiant l'observateur d'événements sur le serveur FAS.



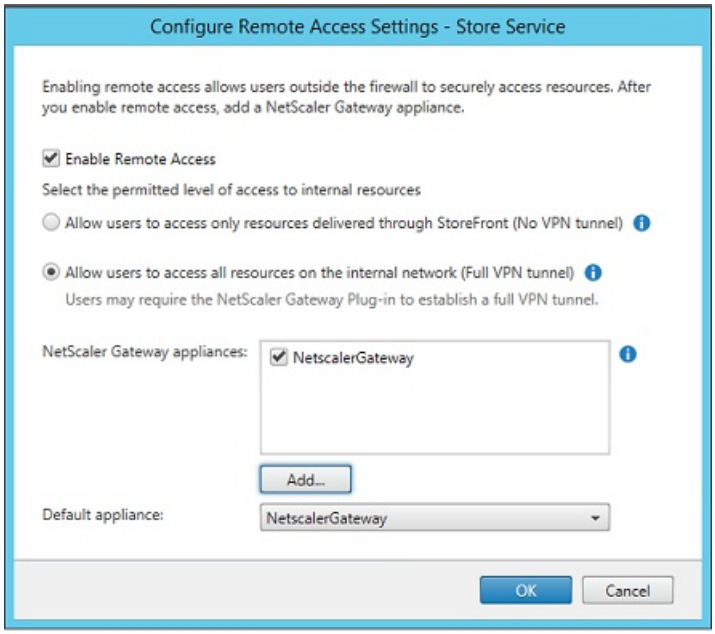
Configurer StoreFront pour utiliser NetScaler

À l'aide de l'interface **Gérer les méthodes d'authentification** de la console de gestion StoreFront, configurez StoreFront de manière à ce qu'il utilise NetScaler pour l'authentification.



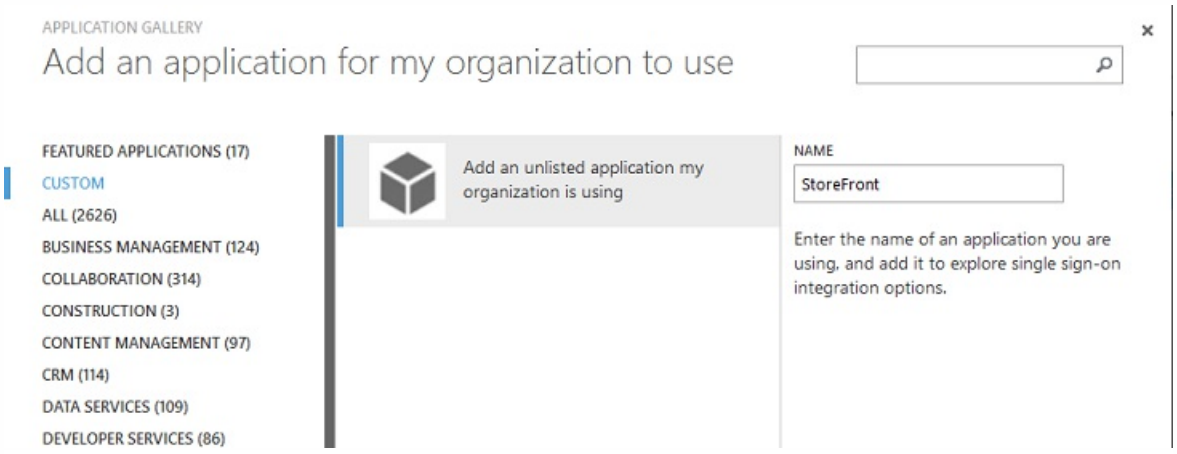
Pour intégrer les options d'authentification NetScaler, configurez une STA (Secure Ticket Authority) et configurez l'adresse NetScaler Gateway.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Configurer une nouvelle application Azure AD pour le Single Sign-On sur StoreFront

Cette section utilise les fonctionnalités d'authentification unique d'Azure AD SAML 2.0, qui requièrent un abonnement Azure Active Directory Premium. Dans l'outil de gestion Azure AD, sélectionnez **Nouvelle application** et **Ajouter une application à partir de la galerie**.



Sélectionnez **PERSONNALISER > Ajouter une application non répertoriée que mon organisation utilise** pour créer une nouvelle application personnalisée pour vos utilisateurs.

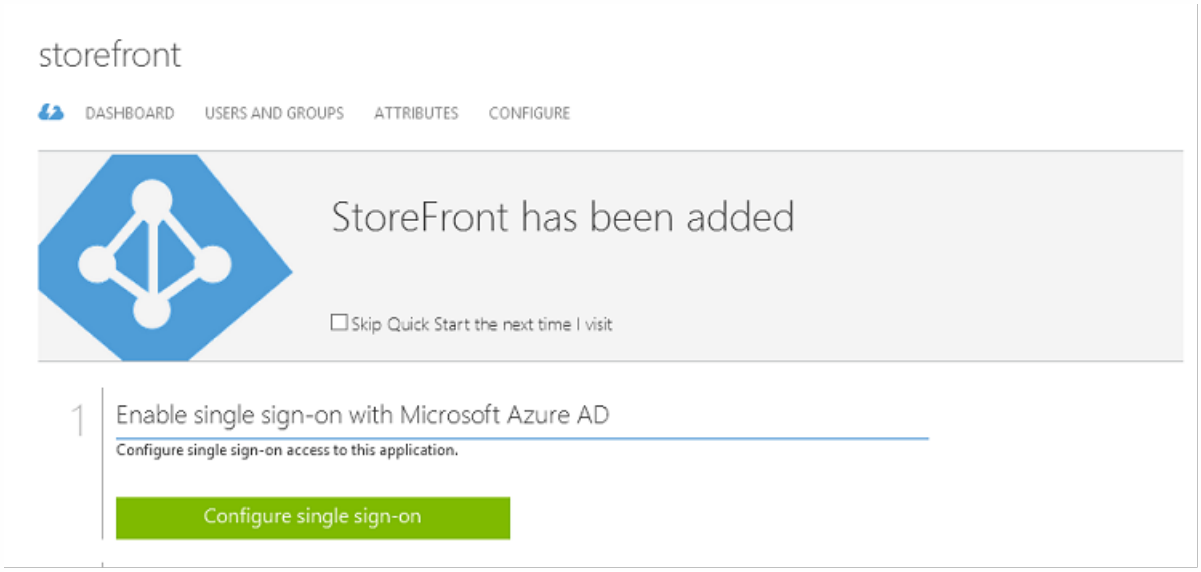
Configurer une icône

Créez une image de 215 x 215 pixels et chargez-la sur la page CONFIGURER pour l'utiliser comme icône pour l'application.

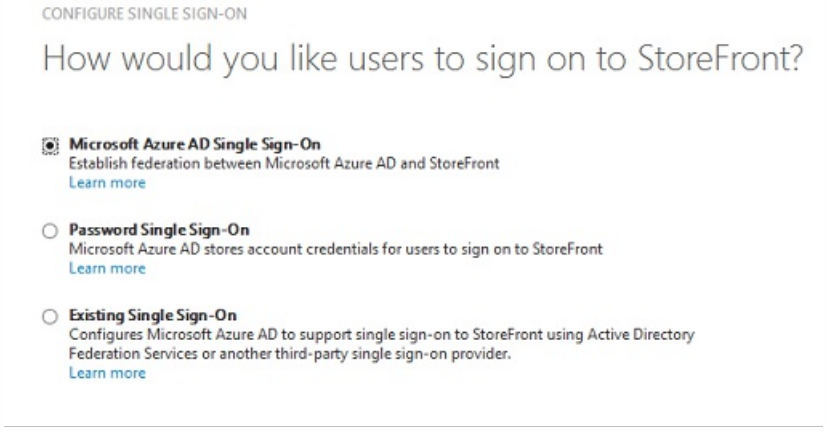
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurer l'authentification SAML

Retournez sur la page de tableau de bord de l'application et sélectionnez **Configurer l'authentification unique**.

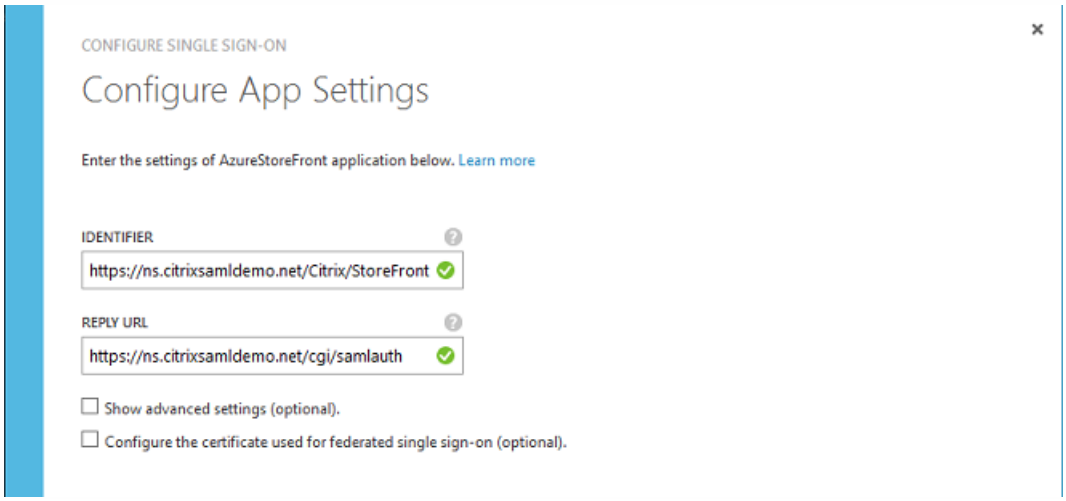


Ce déploiement utilise l'authentification SAML 2.0, qui correspond à **Authentification unique avec Microsoft Azure AD**.

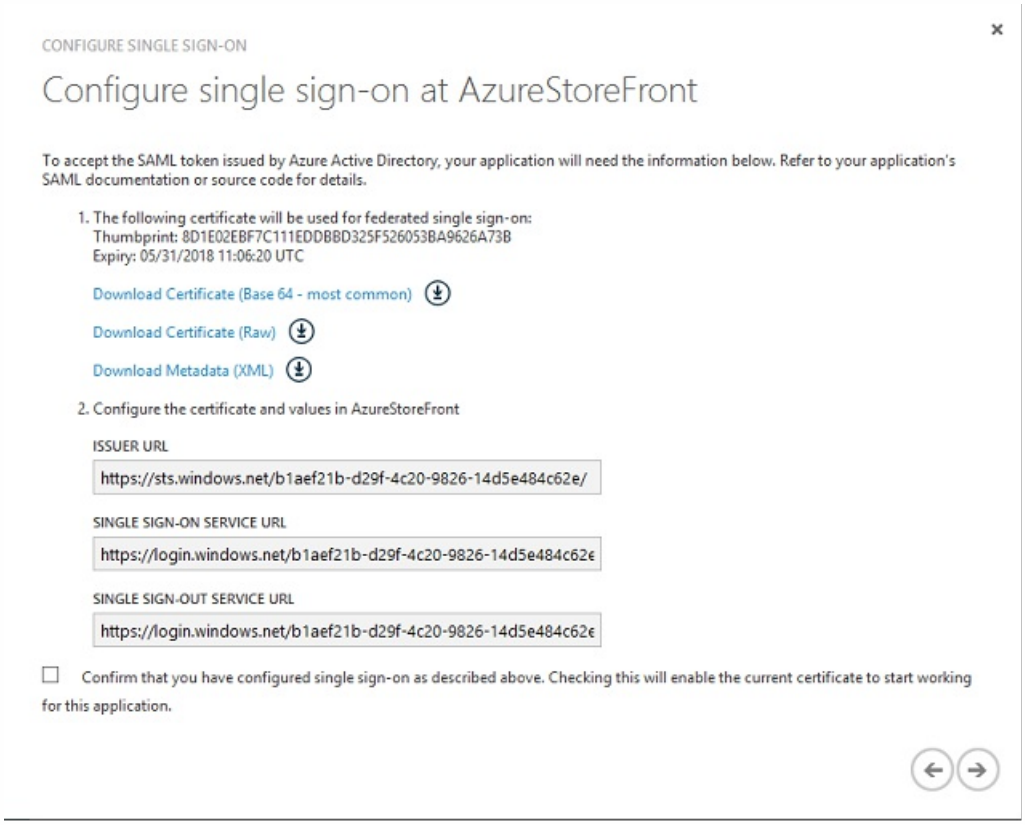


© 1999-2017 Citrix Systems, Inc. All rights reserved.

L'**identificateur** peut être une chaîne arbitraire (doit correspondre à la configuration fournie à NetScaler) ; dans cet exemple, l'**URL de réponse** est /cgi/samlauth sur le serveur NetScaler.



La page suivante contient des informations qui sont utilisées pour configurer NetScaler en tant que partie de confiance pour Azure AD.

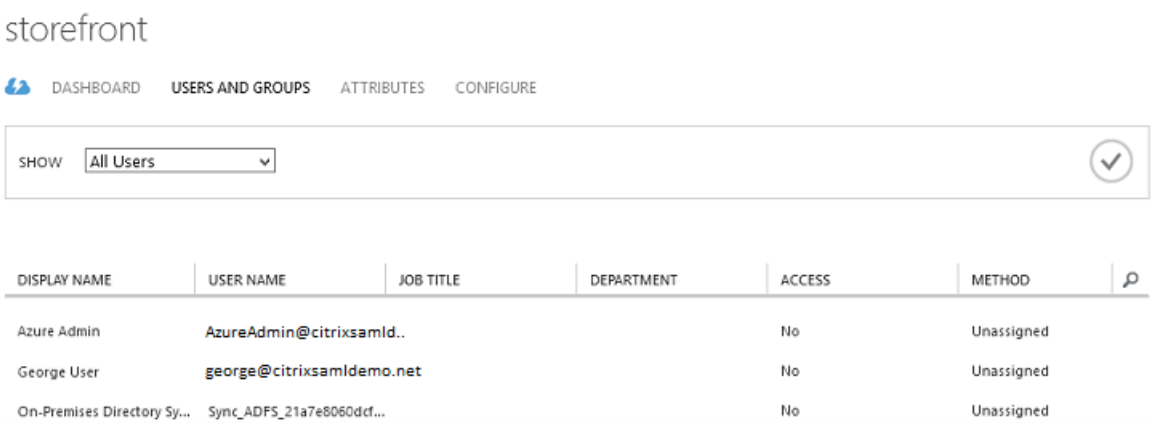


Téléchargez le certificat de signature approuvé base 64 et copiez les URL de connexion et de déconnexion. Collez ces dernières dans les écrans de configuration de NetScaler qui suivent.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

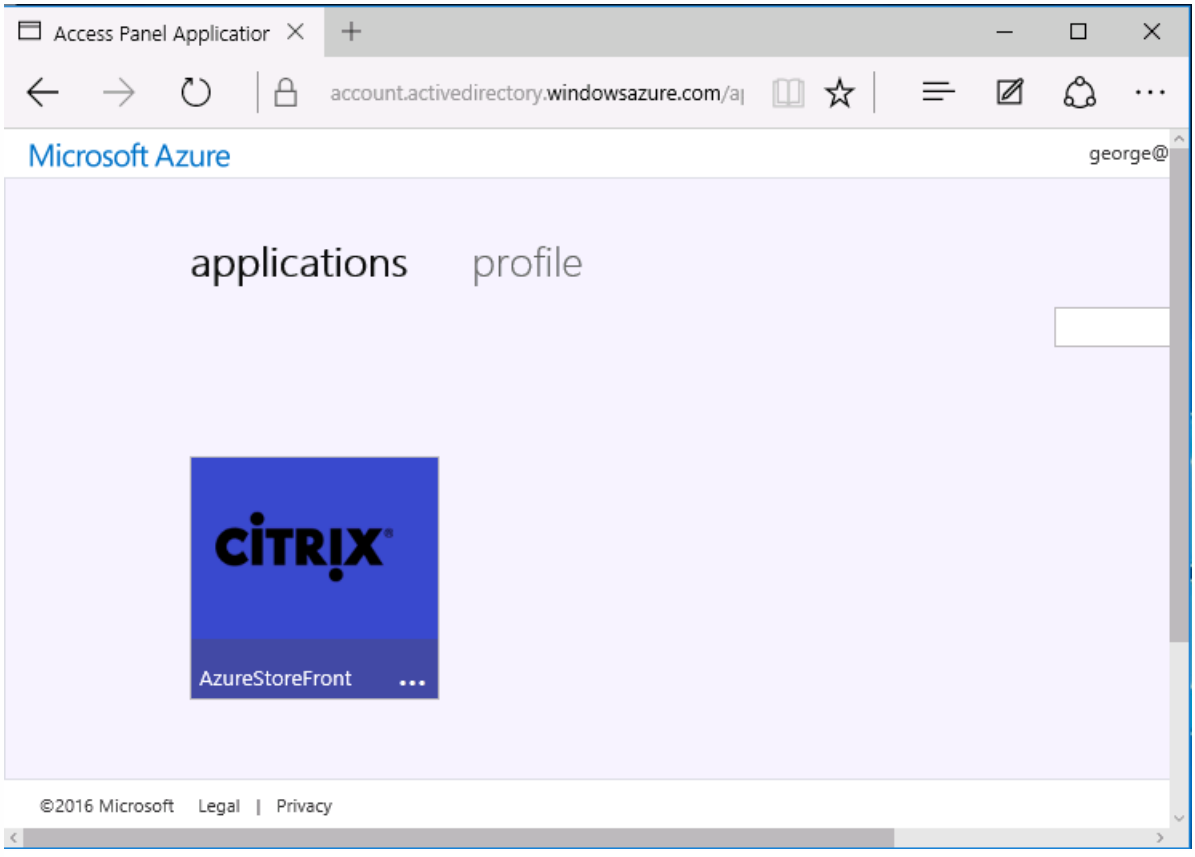
Attribuer l'application aux utilisateurs

La dernière étape consiste à activer l'application afin qu'elle apparaisse sur la page de contrôle “myapps.microsoft.com” des utilisateurs. Cette opération est réalisée sur la page UTILISATEURS ET GROUPES. Attribuez l'accès aux comptes d’utilisateurs de domaine synchronisés par Azure AD Connect. D'autres comptes peuvent également être utilisés, mais ils doivent être explicitement mappés car ils ne sont pas conformes au format @.



Page MyApps

Lorsque l'application a été configurée, elle s'affiche dans les listes d’applications Azure des utilisateurs lorsqu'ils visitent https://myapps.microsoft.com.

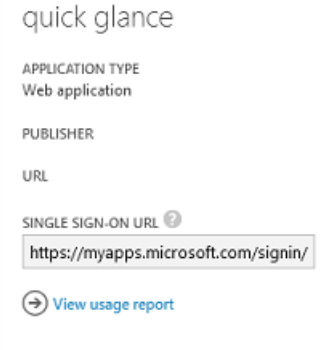


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Lorsqu'il est joint à Azure AD, Windows Azure 10 prend en charge l'authentification unique aux applications Azure pour l'utilisateur qui ouvre une session. Le fait de cliquer sur l'icône dirige le navigateur vers la page Web SAML cgi/samlauth qui a été configurée précédemment.

URL d'authentification unique

Retournez à l'application dans le tableau de bord Azure AD. Une adresse URL d'authentification unique est maintenant disponible pour l'application. Cette adresse URL est utilisée pour fournir des liens de navigateur Web ou pour créer des raccourcis du menu Démarrer qui dirigent les utilisateurs directement dans StoreFront.



Collez cette adresse URL dans un navigateur Web pour vous assurer que vous êtes redirigé par Azure AD sur la page Web NetScaler cgi/samlauth configurée précédemment. Ceci fonctionne uniquement pour les utilisateurs qui ont été attribués, et fournira l'authentification unique uniquement aux sessions Windows 10 jointes à Azure AD. (Les autres utilisateurs seront invités à entrer des informations d'identification Azure AD).

Installer et configurer NetScaler Gateway

Pour accéder à distance au déploiement, cet exemple utilise une VM distincte exécutant NetScaler. Cela peut être acheté sur le Azure Store. Cet exemple utilise la version « BYOL » (avec apport de sa propre licence) de NetScaler 11.0.

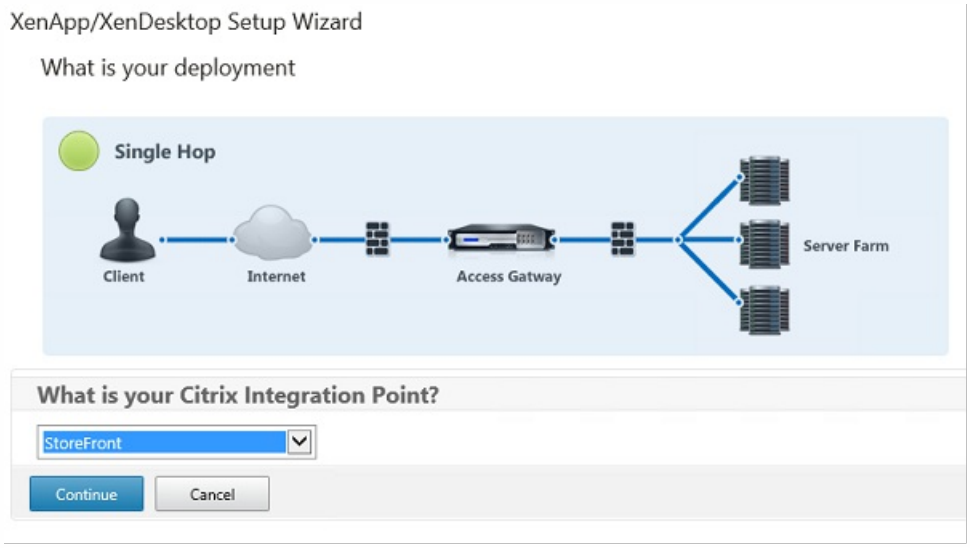
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ouvrez une session sur la VM NetScaler en pointant un navigateur Web sur l'adresse IP interne et en entrant les informations d'identification spécifiées lorsque l'utilisateur s'est authentifié. Notez que vous devez modifier le mot de passe de l'utilisateur nsroot dans la VM Azure AD.

Ajoutez des licences en sélectionnant **redémarrer** après l'ajout de chaque fichier de licences, puis pointez la résolution DNS vers le contrôleur de domaine Microsoft.

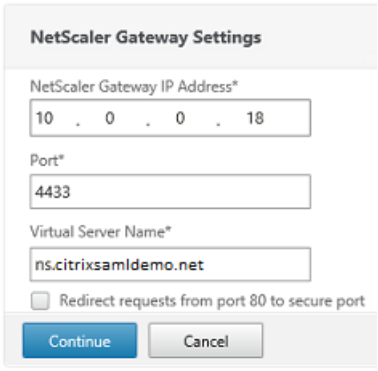
Exécuter l'assistant d'installation de XenApp et XenDesktop

Cet exemple démarre en configurant une intégration StoreFront simple sans SAML. Une fois que le déploiement est opérationnel, il ajoute une stratégie d'ouverture de session SAML.

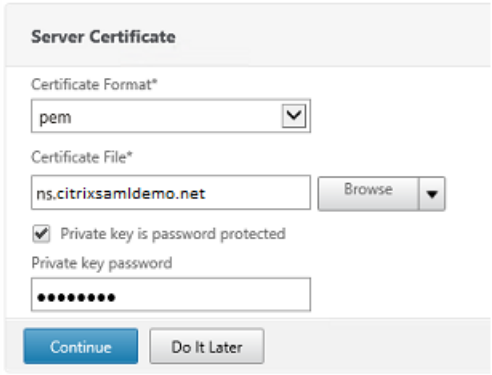


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sélectionnez les paramètres NetScaler StoreFront standard. À des fins d'utilisation dans Microsoft Azure, cet exemple configure le port 4433, plutôt que le port 443. Vous pouvez également transférer le port ou remapper le site Web d'administration de NetScaler.



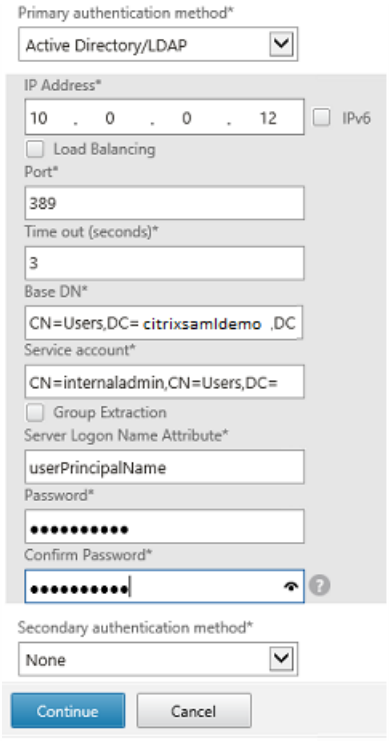
À des fins de simplicité, l'exemple charge un certificat de serveur existant et la clé privée stockée dans un fichier.



Configurer le contrôleur de domaine pour la gestion de comptes AD

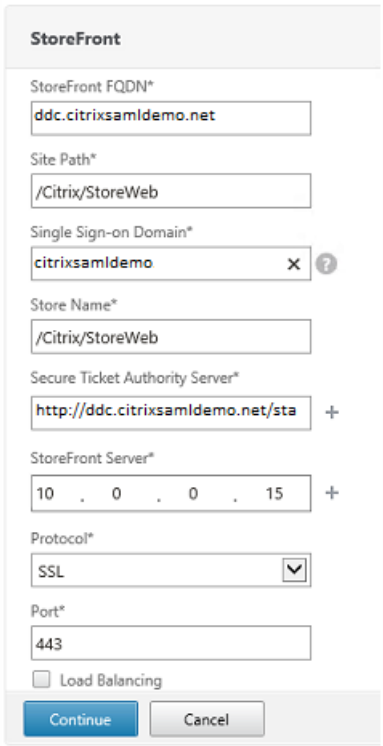
Le contrôleur de domaine sera utilisé pour la résolution de compte, il convient donc d'ajouter son adresse IP dans la méthode d'authentification principale. Notez les formats attendus dans chaque champ de la boîte de dialogue.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Configurer l'adresse de StoreFront

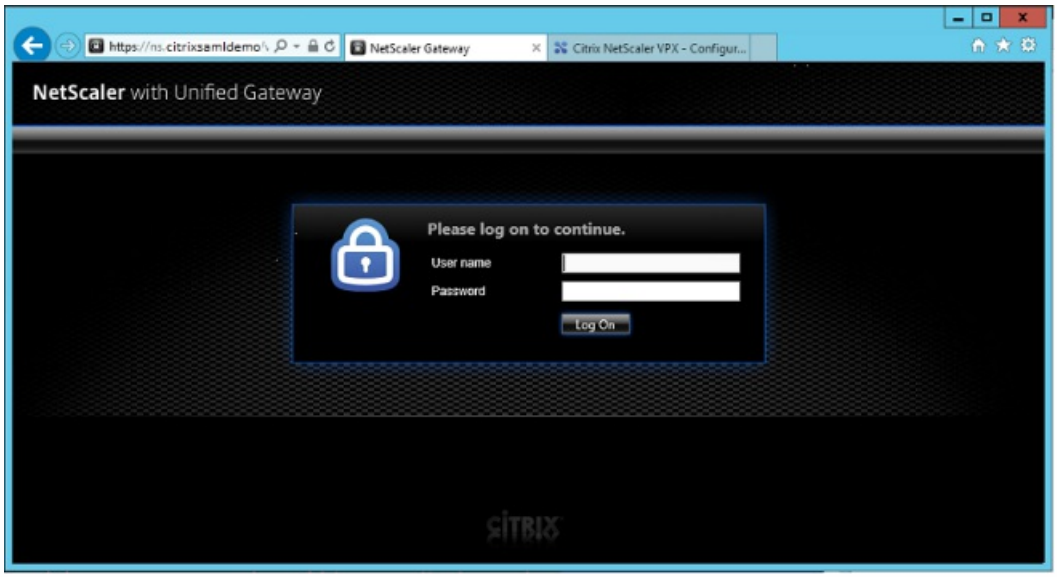
Dans cet exemple, StoreFront a été configuré avec HTTPS, vous devez donc sélectionner les options du protocole SSL.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

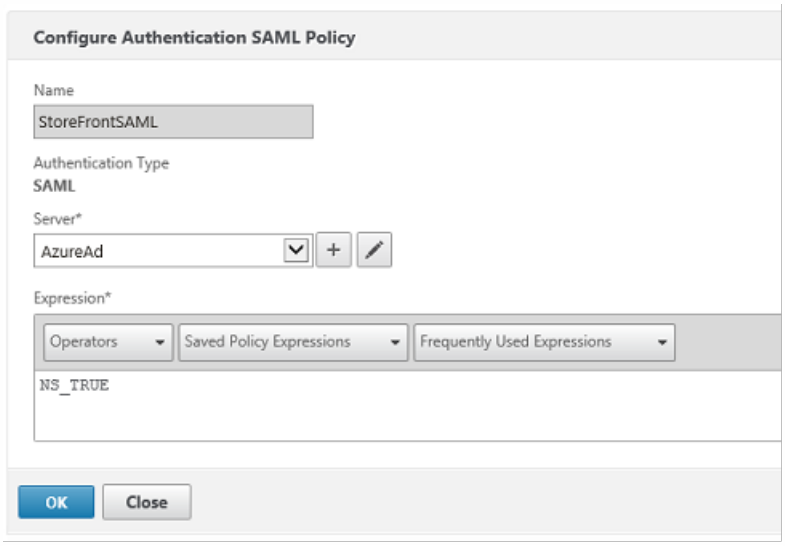
Vérifier le déploiement NetScaler

Connectez-vous à NetScaler et vérifiez le succès de l'authentification et du lancement avec le nom d'utilisateur et mot de passe.



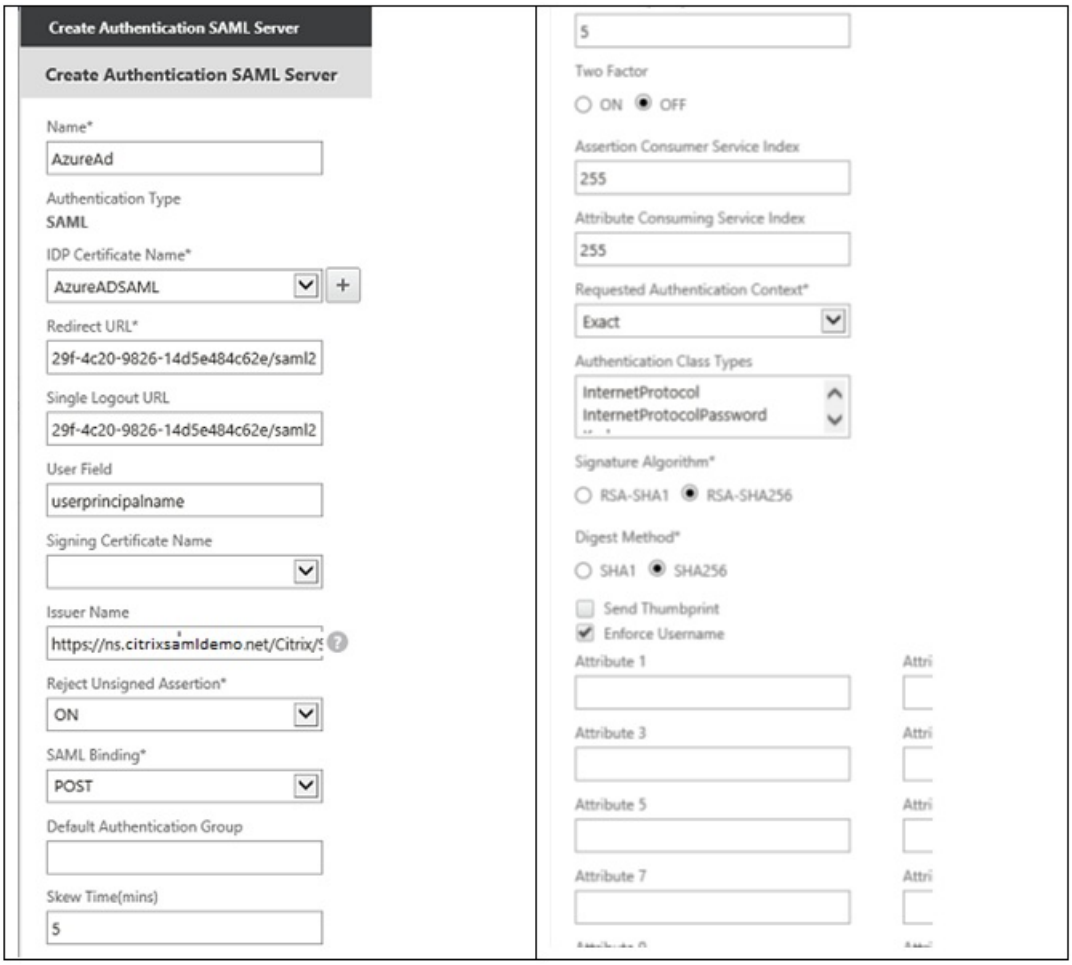
Activer la prise en charge de l'authentification SAML NetScaler

L'utilisation de SAML avec StoreFront est similaire à l'utilisation de SAML avec d'autres sites Web. Ajoutez une nouvelle stratégie SAML avec une expression **NS_TRUE**.



Configurez le nouveau serveur IdP SAML à l'aide des informations obtenues précédemment depuis Azure AD.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

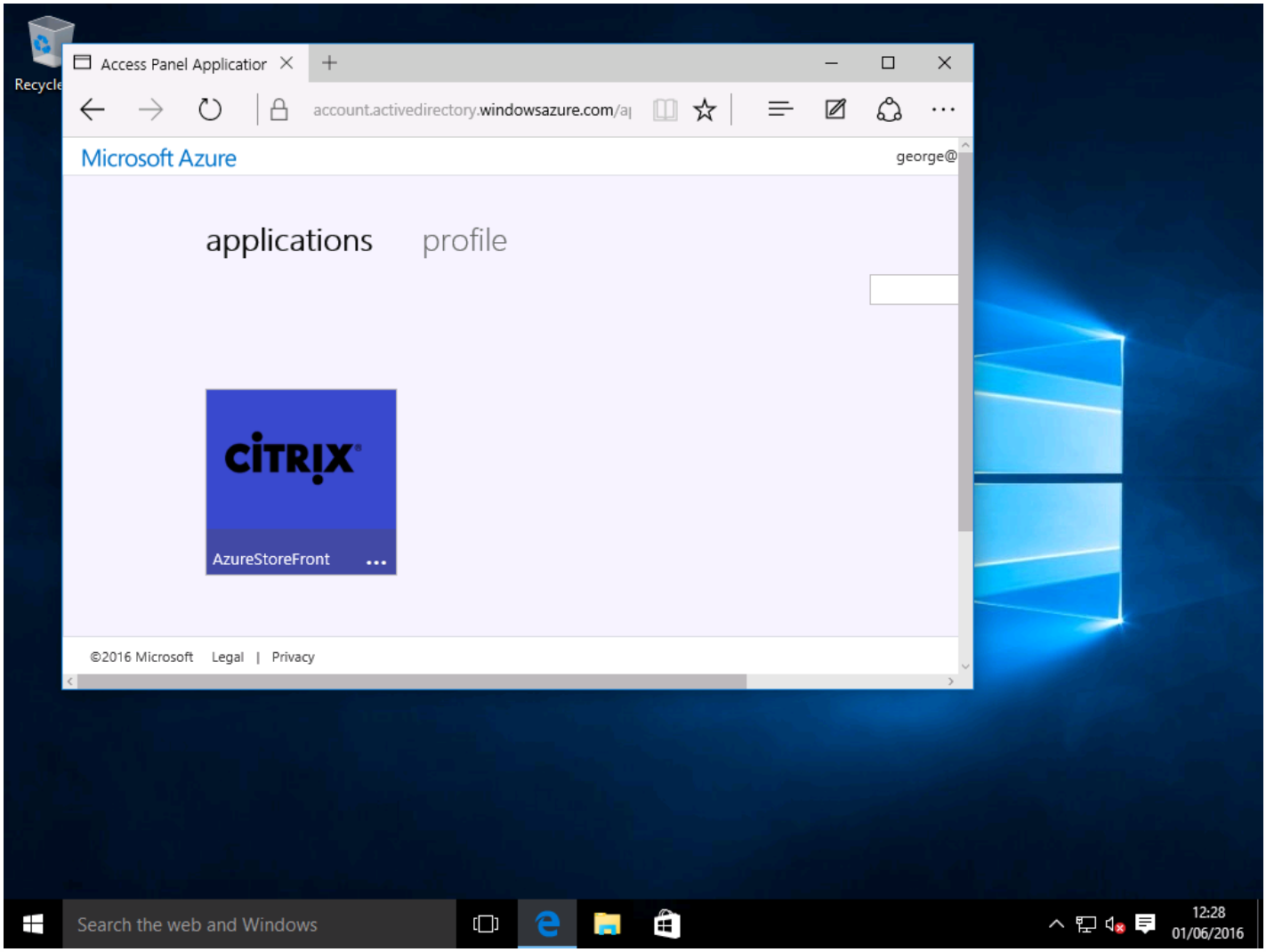


Vérifier le système de bout en bout

Ouvrez une session sur un bureau Windows 10 joint à Azure AD à l'aide d'un compte enregistré dans Azure AD. Lancez Microsoft Edge et connectez-vous à : https://myapps.microsoft.com.

Le navigateur Web devrait afficher les applications Azure AD de l'utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Vérifiez qu'un clic sur l'icône vous redirige vers un serveur StoreFront authentifié.

De même, vérifiez que les connexions directes utilisant l'URL d'authentification unique et qu'une connexion directe au site NetScaler vous redirigent vers Microsoft Azure et vice versa.

Enfin, vérifiez que les machines non jointes à Azure AD fonctionnent également avec les mêmes URL (bien qu'une authentification unique explicite à Azure AD sera utilisée pour la première connexion).

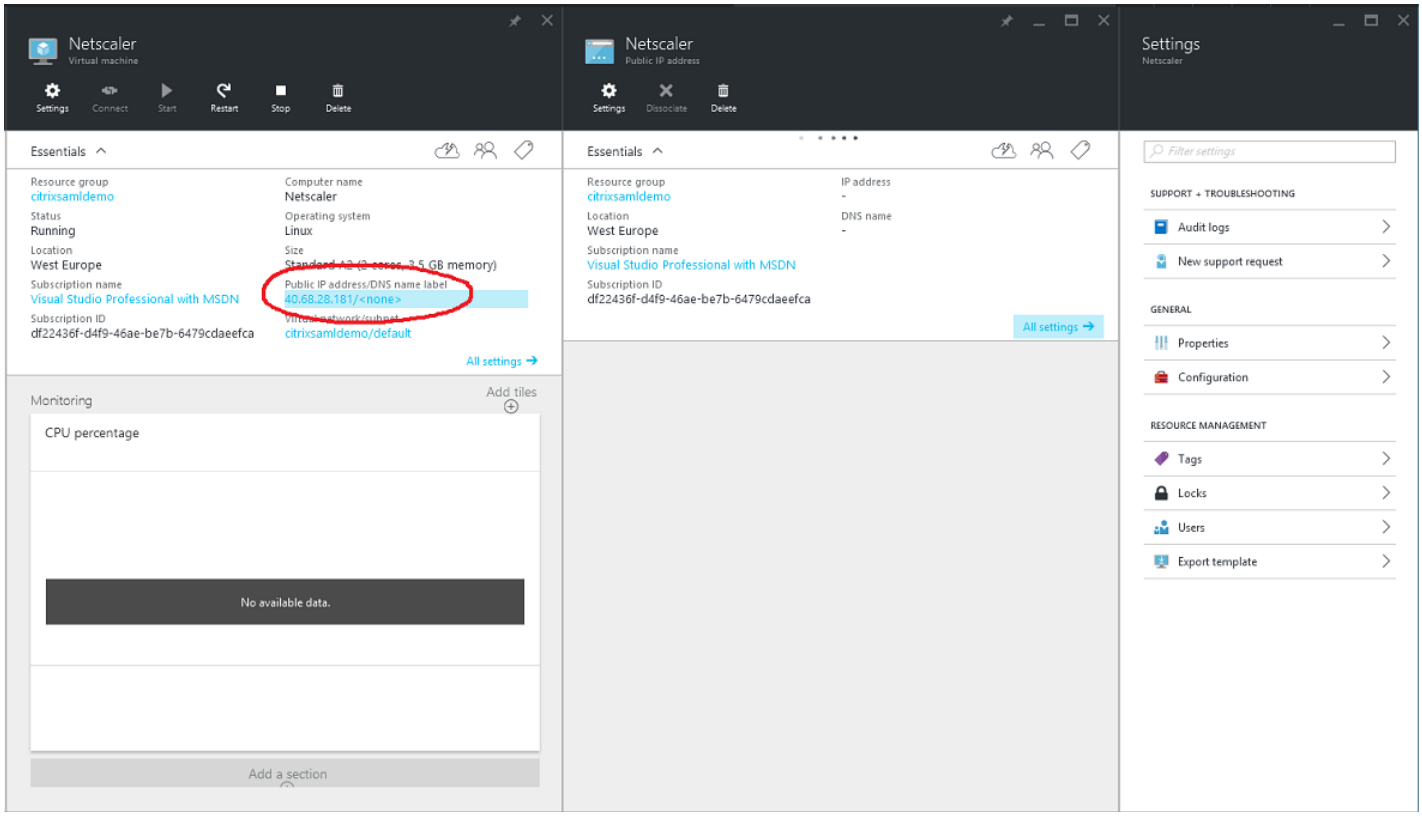
Annexe

Plusieurs options standard doivent être configurées lors de la création d'une VM dans Azure.

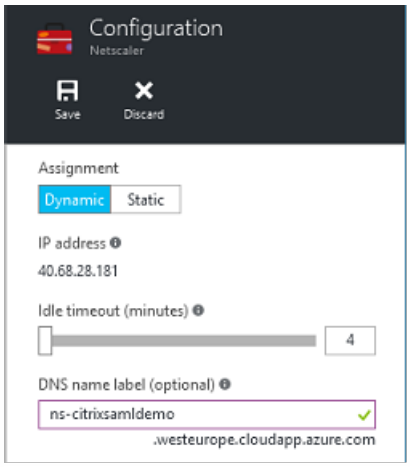
Fournir une adresse IP publique et une adresse DNS

Azure attribue à toutes les VM une adresse IP sur le sous-réseau interne (10.*.*.* dans cet exemple). Par défaut, une adresse IP publique est également fournie et cette dernière peut être référencée par un nom DNS mis à jour de manière dynamique.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Dans **Configuration**, sélectionnez **Public IP address/DNS name label**. Choisissez une adresse DNS publique pour la VM. Elle peut être utilisée pour les références CNAME dans d'autres fichiers de zone DNS, pour s'assurer que tous les enregistrements DNS pointent toujours vers la VM, même si l'adresse IP est réallouée.



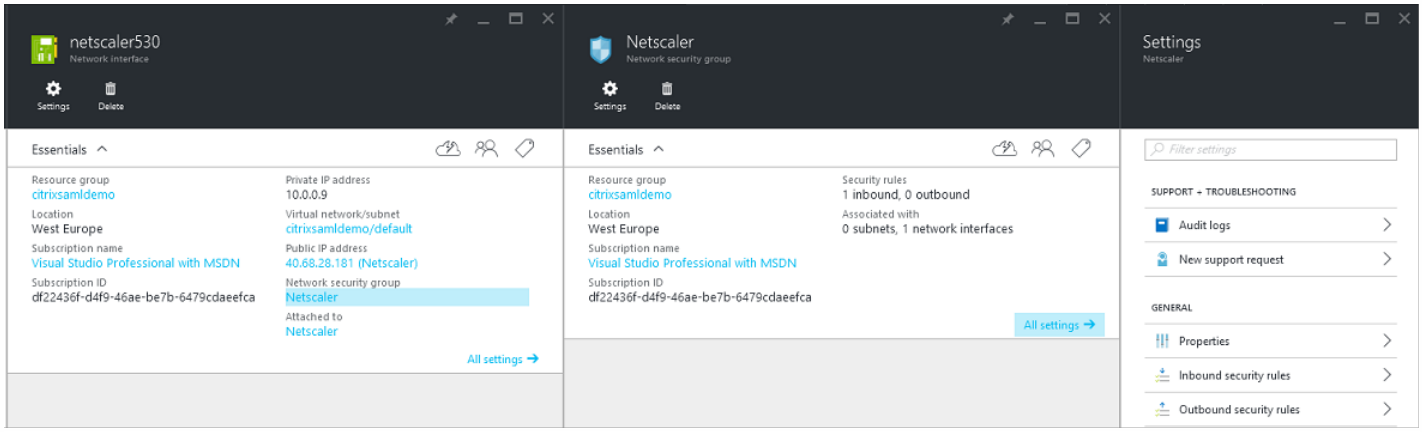
Configurer des règles de pare-feu (groupe de sécurité)

Chaque VM dans un cloud contient un ensemble de règles de pare-feu appliquées automatiquement, connues sous le nom de groupe de sécurité. Le groupe de sécurité contrôle le trafic transféré depuis l'adresse publique vers l'adresse IP privée. Par défaut, Azure permet à RDP d'être transféré à toutes les VM. Les serveurs NetScaler et ADFS doivent également transférer le trafic TLS (443).

Ouvrez **Network Interfaces** pour une VM et cliquez sur **Network Security Group**. Configurez l'option **Inbound**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

security rules pour autoriser le trafic réseau approprié.



Informations connexes

- L'article Service d'authentification fédérée est le document de référence principal pour obtenir des informations sur l'installation et la configuration du FAS.
- Les déploiements FAS courants sont décrits dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée.
- Des informations pratiques sont disponibles dans l'article Configuration et gestion du service d'authentification fédérée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Guide pratique sur le Service d'authentification fédérée : configuration et gestion

Aug 22, 2016

Les articles suivants fournissent des informations de configuration et de gestion avancées pour le Service d'authentification fédérée (FAS) :

- Protection de clé privée
- Configuration de l'autorité de certification
- Gestion du réseau et de la sécurité
- Résoudre les problèmes d'ouverture de session Windows
- Fichiers d'aide de l'applet de commande du SDK PowerShell

Informations connexes :

- L'article Service d'authentification fédérée est le document de référence principal pour obtenir des informations sur l'installation et la configuration du FAS.
- L'article Vue d'ensemble des architectures du Service d'authentification fédérée propose un résumé des principales architectures FAS, ainsi que des liens vers d'autres articles sur les architectures plus complexes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration de l'autorité de certification du Service d'authentification fédérée

Jul 13, 2016

Cet article décrit la configuration avancée du Service d'authentification fédérée Citrix (FAS) pour l'intégration avec les serveurs d'autorité de certification (CA) qui ne sont pas pris en charge par la console de gestion FAS. Les instructions utilisent les API PowerShell fournies par FAS. Vous devez disposer de connaissances de base sur PowerShell avant d'exécuter les instructions de cet article.

Définir plusieurs serveurs d'autorité de certification à utiliser dans FAS

Cette section décrit comment configurer un serveur FAS unique pour qu'il utilise plusieurs serveurs d'autorité de certification pour émettre des certificats. Cela permet l'équilibrage de charge et le basculement des serveurs d'autorité de certification.

Étape 1 : Découvrir combien de serveurs d'autorité de certification FAS peut localiser

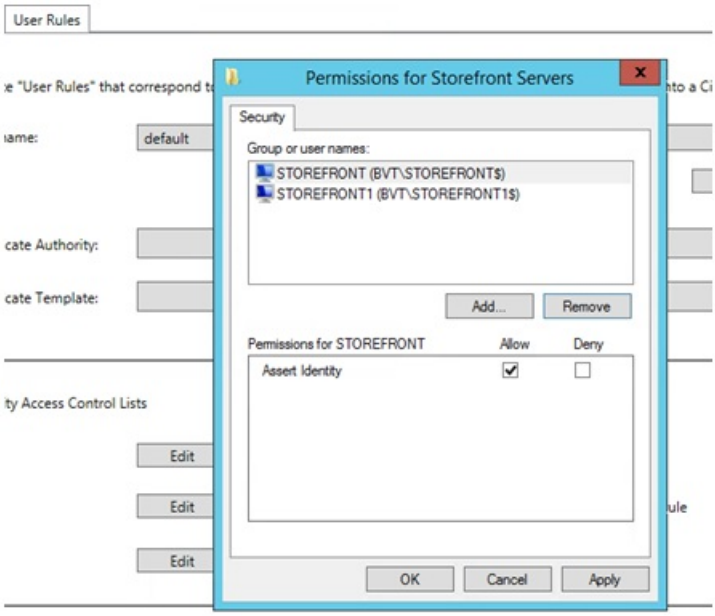
Utilisez l'applet de commande Get-FASMsCertificateAuthority pour déterminer les serveurs d'autorité de certification auxquels FAS peut se connecter. Dans l'exemple suivant, FAS peut se connecter à trois serveurs d'autorité de certification.

```
PS > Add-PSSnapin Citrix*
PS > Get-FASMsCertificateAuthority

Address                          IsDefault PublishedTemplates
-------                          --------- ------------------
DC1.bvt.local\bvt-DC1-CA             False {Citrix_SmartcardLogon, Citrix_Regis...
ca1.bvt.local\CA1.bvt.local          False {Citrix_SmartcardLogon, Citrix_Regis...
ca2.bvt.local\ca2.bvt.local          False {Citrix_SmartcardLogon, Citrix_Regis...
```

Étape 2 : Modifier la définition de certificat existante

Citrix vous recommande de créer un rôle à l'aide de la console de gestion FAS, plutôt qu'à l'aide de PowerShell pour créer le rôle. Cela évite d'avoir à ajouter le SDL manuellement ultérieurement. Dans l'exemple suivant, un rôle appelé « default » est créé à l'aide de la règle d'accès configurée :

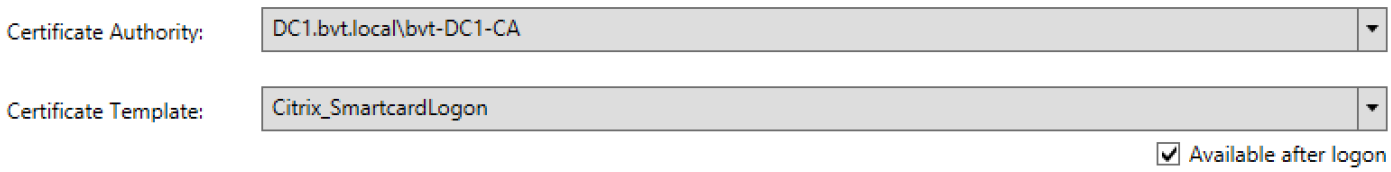
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Pour ajouter plusieurs autorités de certification au champ d'autorité de certification (ce qui n'est pas pris en charge dans cette version), vous devez configurer la définition de certificat. Tout d'abord, vous devez connaître le nom de la définition de certificat. Le nom ne peut pas être déterminé à partir de la console de gestion ; utilisez l'applet de commande Get-FASCertificateDefinition.

```
PS > Get-FASCertificateDefinition

Name                    : default_Definition
CertificateAuthorities  : {DC1.bvt.local\bvt-DC1-CA}
MsTemplate              : Citrix_SmartcardLogon
AuthorizationCertificate : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids              : {}
InSession               : True
```

L'équivalent dans l'interface utilisateur est :



Une fois que vous avez le nom de la définition de certificat, modifiez la définition de certificat pour obtenir une liste de CertificateAuthorities, plutôt qu'un seul certificat :

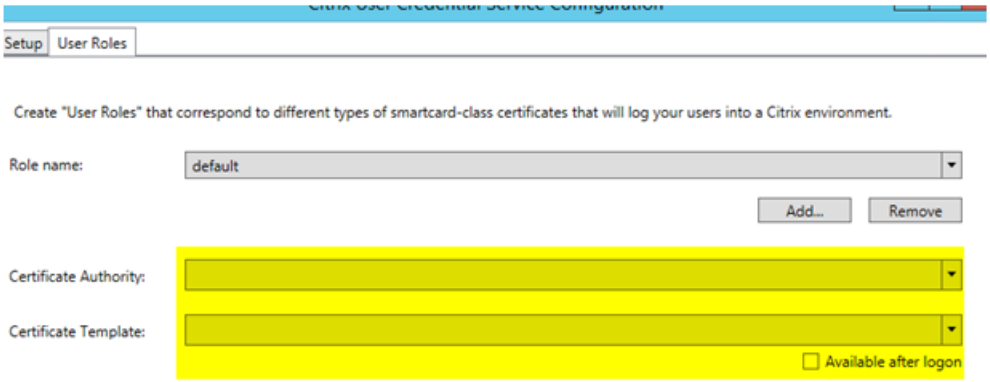
```
PS > Set-FASCertificateDefinition -Name default_Definition -CertificateAuthorities @("DC1.bvt.
local\bvt-DC1-CA", "ca1.bvt.local\CA1.bvt.local", "ca2.bvt.local\ca2.bvt.local")
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

L'applet de commande Get-FASCertificateDefinition renvoie maintenant :

```
PS > Get-FASCertificateDefinition
Name                    : default_Definition
CertificateAuthorities  : {DC1.bvt.local\bvt-DC1-CA, ca1.bvt.local\CA1.bvt.local, ca2.bvt.local\ca2.bvt.local}
MsTemplate              : Citrix_SmartcardLogon
AuthorizationCertificate : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids              : {}
InSession               : True
```

Remarque : votre console de gestion FAS ne sera pas opérationnelle après cette opération. Vous verrez un champ vide dans « Certificate Authority » et « Certificate Template » après le chargement :



FAS fonctionne toujours. Si vous utilisez la console pour modifier la règle d'accès, il vous suffit de répéter l'étape 2 pour afficher toutes les autorités de certification.

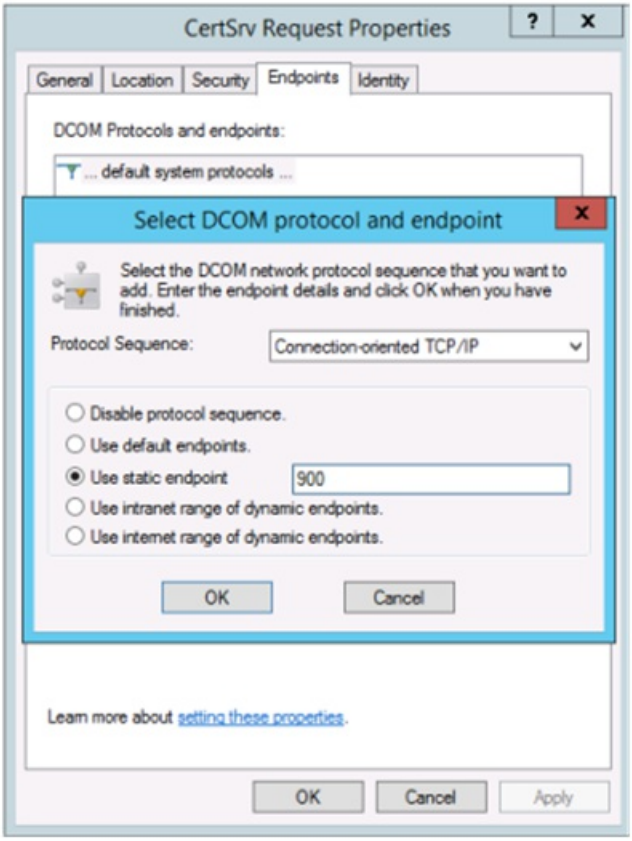
Changements de comportement attendus

Une fois que vous avez configuré le serveur FAS avec de multiples serveurs d'autorité de certification, la génération de certificat utilisateur est distribuée entre tous les serveurs d'autorité de certification configurés. De plus, si l'un des serveurs d'autorité de certification configurés échoue, le serveur FAS bascule vers un autre serveur d'autorité de certification disponible.

Configurer l'autorité de certification Microsoft pour l'accès TCP

Par défaut, l'autorité de certification Microsoft utilise DCOM pour l'accès. Cela peut compliquer la mise en place d'un pare-feu de sécurité, par conséquent Microsoft permet le basculement vers un port TCP statique. Sur l'autorité de certification Microsoft, ouvrez le panneau de configuration de DCOM et modifiez les propriétés de l'application « CertSrv DCOM » :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Modifiez les points de terminaison (endpoints) pour sélectionner un point de terminaison statique et spécifiez un numéro de port TCP (900 dans l'illustration ci-dessus).

Redémarrez l'autorité de certification Microsoft et envoyez une demande de certificat. Si vous exécutez «netstat –a –n –b », vous verrez que certsvr écoute désormais le port 900 :

```
  TCP    0.0.0.0:636            dc:0                   LISTENING
[lsass.exe]
  TCP    0.0.0.0:900            dc:0                   LISTENING
[certsrv.exe]
  TCP    0.0.0.0:3268           dc:0                   LISTENING
[lsass.exe]
  TCP    0.0.0.0:3269           dc:0                   LISTENING
```

Il n'est pas nécessaire de configurer le serveur FAS (ou toute autre machine utilisant l'autorité de certification), car DCOM a une étape de négociation utilisant le port RPC. Lorsqu'un client doit utiliser DCOM, il se connecte au service DCOM RPC sur le serveur de certificats et demande l'accès à un serveur DCOM particulier. Cela déclenche l'ouverture du port 900 et le serveur DCOM indique au serveur FAS comment se connecter.

Pré-générer les certificats utilisateur

La durée d'ouverture de session pour les utilisateurs peut nettement s'améliorer lorsque les certificats utilisateur sont pré-générés dans le serveur FAS. Les sections suivantes décrivent comment y procéder, pour un ou plusieurs serveurs FAS.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

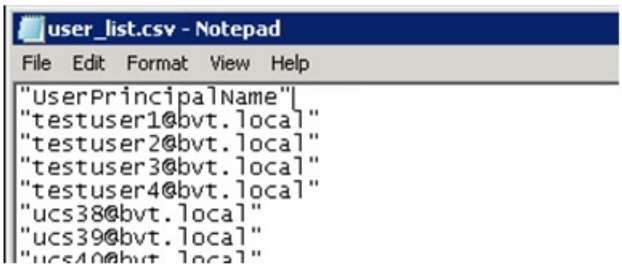
Vous pouvez améliorer la génération de certificat en interrogeant AD et en stockant la liste des utilisateurs dans un fichier (par exemple, un fichier .csv), comme illustré dans l'exemple suivant.

```
Import-Module ActiveDirectory

$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for Users, leave it blank to search all
$filename = “user_list.csv” # Filename to save

if ($searchbase –ne “”) {
   Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")} -SearchBase $searchbase -Properties
UserPrincipalName |Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter ","
$filename
} else {
   Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")}  -Properties UserPrincipalName
|Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter "," $filename
}
```

Get-ADUser est une applet de commande qui envoie une requête de liste d'utilisateurs. L'exemple ci-dessus contient un argument de filtre pour inclure uniquement les utilisateurs disposant d'un UserPrincipalName et avec un état de compte « activé ».

L'argument SearchBase spécifie la partie d'Active Directory dans laquelle rechercher des utilisateurs. Vous pouvez ignorer cette option si vous voulez inclure tous les utilisateurs présents dans Active Directory. Remarque : cette requête peut renvoyer un grand nombre d'utilisateurs.

Le fichier CSV ressemble à l'exemple ci-dessous :



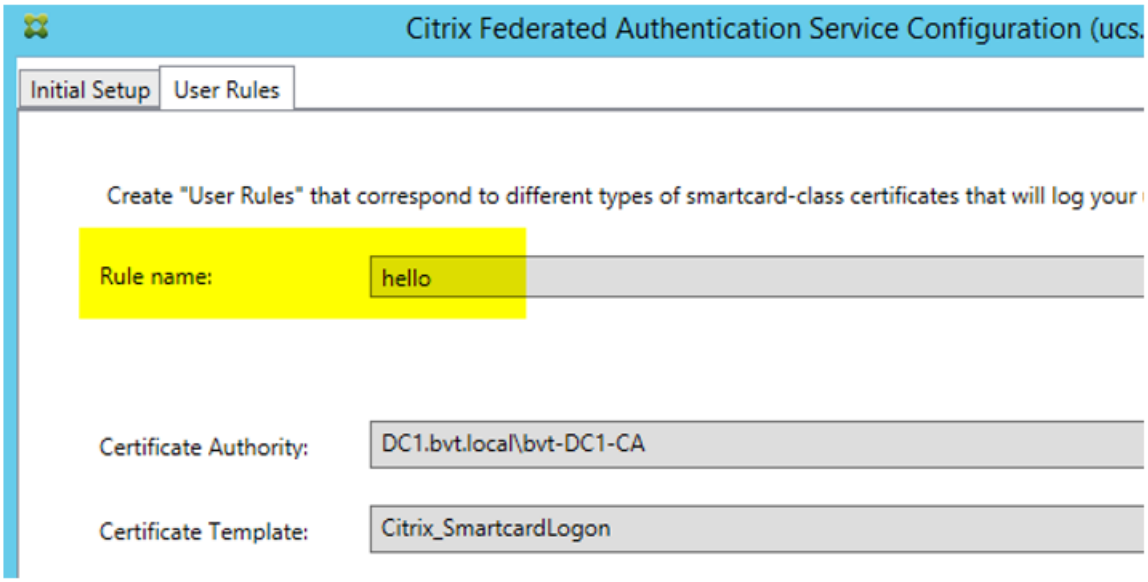
Le script PowerShell utilise la liste d'utilisateurs générée et crée une liste de certificats utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
Add-PSSnapin Citrix.A*

$csv = "user_list.csv"
$rule = "default" #rule/role in your admin console
$users = Import-Csv  -encoding utf8 $csv

foreach ( $user in $users )
{
  $server = Get-FASServerForUser -UserPrincipalNames $user.UserPrincipalName
  if ( $server.Server -ne $NULL ){
     New-FASUserCertificate -Address $server.Server -UserPrincipalName $user.UserPrincipalName -
CertificateDefinition $rule"_Definition" -Rule $rule
  }
  if ( $server.Failover -ne $NULL ){
     New-FASUserCertificate -Address $server.Failover -UserPrincipalName $user.UserPrincipalName -
CertificateDefinition $rule"_Definition" -Rule $rule
  }
}
```

Si vous disposez de plusieurs serveurs FAS, le certificat d'un utilisateur particulier est généré deux fois : une fois sur le serveur principal et une autre sur le serveur de basculement.

Le script ci-dessus inclut une règle « default ». Si votre règle porte un autre nom (par exemple, « hello »), il vous suffit de modifier la variable $rule dans le script.



Renouveler les certificats d'autorité d'inscription

Si plusieurs serveurs FAS sont utilisés, vous pouvez renouveler un certificat d'autorisation FAS sans affecter les utilisateurs connectés. Remarque : bien que vous puissiez également utiliser l'interface utilisateur pour annuler et renouveler

© 1999-2017 Citrix Systems, Inc. All rights reserved.

l'autorisation FAS, cela a pour effet de réinitialiser les options de configuration FAS.

Effectuez la procédure suivante dans l'ordre indiqué :

1. Créer un nouveau certificat d'autorisation :

    New-FasAuthorizationCertificate

2. Noter le GUID du nouveau certificat d'autorisation, renvoyé par :

    Get-FasAuthorizationCertificate

3. Placer le serveur FAS en mode de maintenance :

    Set-FasServer –Address -MaintenanceMode $true

4. Changer le nouveau certificat d'autorisation :

    Set-FasCertificateDefinition –AuthorizationCertificate

5. Retirer le serveur FAS du mode de maintenance :

    Set-FasServer –Address -MaintenanceMode $false

6. Supprimer l'ancien certificat d'autorisation :

    Remove-FasAuthorizationCertificate

Informations connexes

- L'article Service d'authentification fédérée est le document de référence principal pour obtenir des informations sur l'installation et la configuration du FAS.
- Les déploiements FAS courants sont décrits dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée.
- D'autres informations pratiques sont disponibles dans l'article Configuration et gestion du service d'authentification fédérée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Protection des clés privées du service d'authentification fédérée

Jul 13, 2016

Introduction

Les clés privées sont stockées par le biais du compte de service réseau et marquées comme non-exportables par défaut.

Il existe deux types de clés privées :

- La clé privée associée au certificat de l'autorité d'inscription (RA), à partir du modèle de certificat Citrix_RegistrationAuthority.
- Les clés privées associées aux certificats utilisateur, à partir du modèle de certificat Citrix_SmartcardLogon.

Il existe en fait deux certificats d'autorité d'inscription : Citrix_RegistrationAuthority_ManualAuthorization (valide pendant 24 heures par défaut) et Citrix_RegistrationAuthority (valide pendant deux ans par défaut).

> Lors de l'étape 3 de la configuration initiale dans la console de gestion FAS, lorsque l'administrateur clique sur « Autoriser », le serveur FAS génère une paire de clés et envoie une demande de signature de certificat (CSR) à l'autorité de certification pour le certificat Citrix_RegistrationAuthority_ManualAuthorization. Il s'agit d'un certificat temporaire, valide pendant 24 heures par défaut. L'autorité de certification n'émet pas automatiquement ce certificat ; son émission doit être manuellement autorisée sur l'autorité de certification par un administrateur. Une fois que le certificat a été généré sur le FAS serveur, FAS utilise le certificat Citrix_RegistrationAuthority_ManualAuthorization pour obtenir automatiquement le certificat Citrix_RegistrationAuthority (valide pendant deux ans par défaut). Le serveur FAS supprime le certificat et la clé pour Citrix_RegistrationAuthority_ManualAuthorization dès qu'il obtient le certificat Citrix_RegistrationAuthority.

La clé privée associée au certificat RA est particulièrement sensible car la stratégie de certificat RA permet à toute personne qui dispose de la clé privée d'émettre des demandes de certificat pour le groupe d'utilisateurs configuré dans le modèle. En conséquence, toute personne qui contrôle cette clé peut se connecter à l'environnement en tant qu'utilisateur du groupe.

Vous pouvez configurer le serveur FAS pour protéger les clés privées selon les besoins de sécurité de votre organisation, à l'aide de l'une des configurations suivantes :

- Microsoft Enhanced RSA and AES Cryptographic Provider ou Microsoft Software Key Storage Provider pour le certificat RA et les clés privées des certificats utilisateur.
- Microsoft Platform Key Storage Provider avec une puce Trusted Platform Module (TPM) pour la clé privée du certificat RA et Microsoft Enhanced RSA and AES Cryptographic Provider ou Microsoft Software Key Storage Provider pour les clés privées des certificats utilisateur.
- Un fournisseur de service cryptographique ou un fournisseur de stockage de clés de module de sécurité matérielle (HSM) avec le périphérique HSM pour le certificat RA et les clés privées des certificats utilisateur.

Paramètres de configuration des clés privées

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurez FAS pour utiliser l'une des trois options. Utilisez un éditeur de texte pour modifier le fichier Citrix.Authentication.FederatedAuthenticationService.exe.config. L'emplacement par défaut du fichier est le dossier Program Files\Citrix\Federated Authentication Service sur le serveur FAS.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Le FAS lit le fichier de configuration uniquement lorsque le service démarre. Si des valeurs sont modifiées, le FAS doit être redémarré avant qu'il reflète les nouveaux paramètres.

Définissez les valeurs appropriées dans le fichier Citrix.Authentication.FederatedAuthenticationService.exe.config comme suit :

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp** (basculement entre API CAPI et CNG)

Valeur	Comment
true	Utiliser les API CAPI
false (valeur par défaut)	Utiliser les API CNG

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**NomFournisseur** (nom du fournisseur à utiliser)

Valeur	Comment
Microsoft Enhanced RSA and AES Cryptographic Provider	Fournisseur CAPI par défaut
Microsoft Software Key Storage Provider	Fournisseur CNG par défaut

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft Platform Key Storage Provider	Fournisseur TPM par défaut Veuillez noter que TPM n'est pas recommandé pour les clés utilisateur. Utilisez TPM uniquement pour la clé RA. Si vous prévoyez d'exécuter votre serveur FAS dans un environnement virtualisé, demandez à votre fournisseur d'hyperviseur et de puce TPM si la virtualisation est prise en charge.
HSM_Vendor CSP/Fournisseur de stockage de clés	Fourni par le fournisseur HSM. La valeur diffère d'un fournisseur à l'autre. Si vous prévoyez d'exécuter votre serveur FAS dans un environnement virtualisé, demandez à votre fournisseur HSM si la virtualisation est prise en charge.

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**TypeFournisseur** (requis uniquement avec une API CAPI)

Valeur	Comment
24	Default. Fait référence à la propriété Microsoft KeyContainerPermissionAccessEntry.ProviderType PROV_RSA_AES 24. Doit être toujours 24, sauf si vous utilisez un HSM avec CAPI et que le fournisseur HSM en décide autrement.

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProtectionClé** (lorsque FAS doit effectuer une opération de clé privée, il utilise la valeur spécifiée ici) Contrôle l'indicateur « exportable » des clés privées. Permet l'utilisation de stockage de clé TPM, s'il est pris en charge par le matériel.

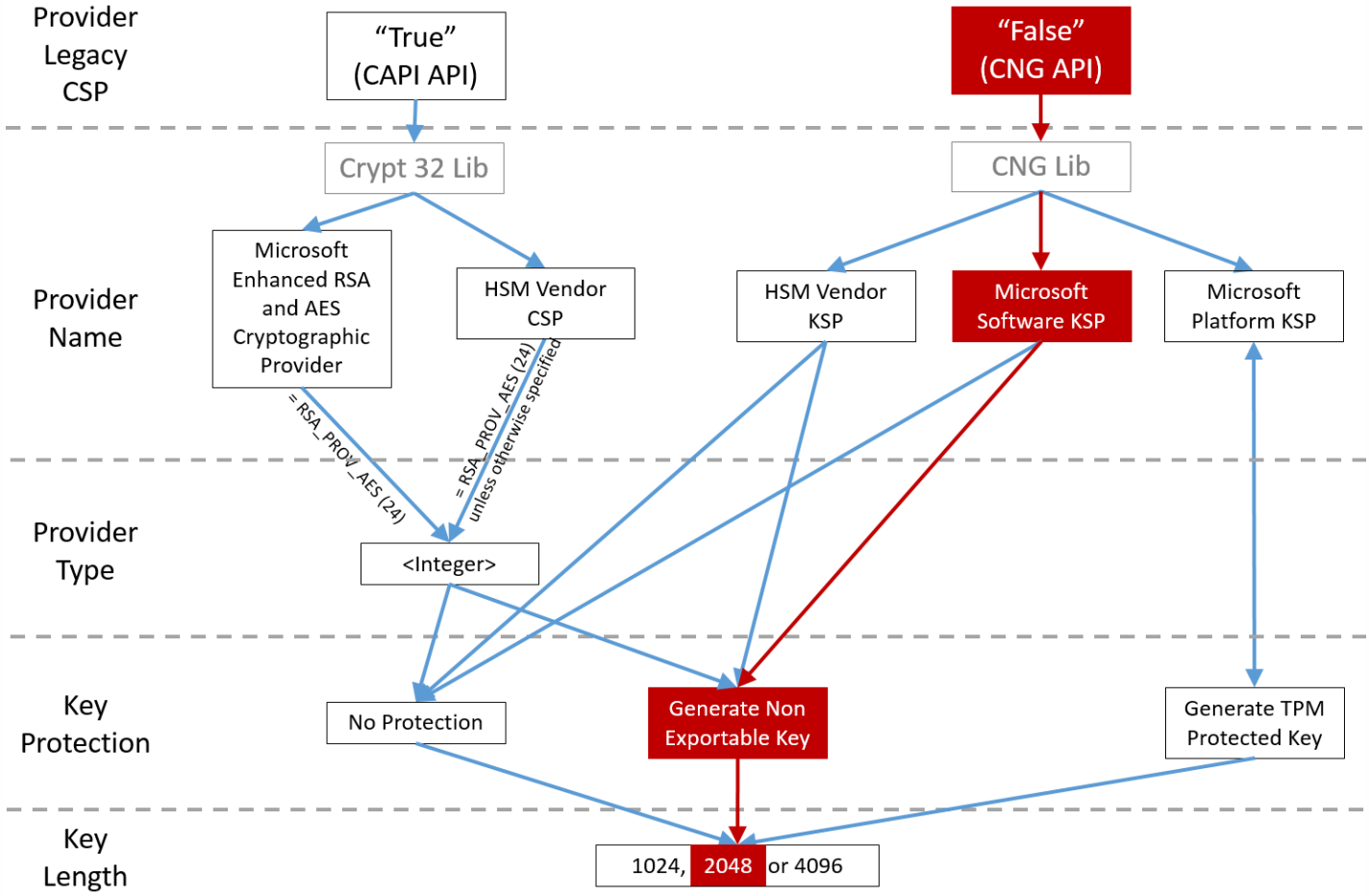
Valeur	Comment
NoProtection	La clé privée peut être exportée.
GenerateNonExportableKey	Default. La clé privée ne peut pas être exportée.
GenerateTPMProtectedKey	La clé privée sera gérée à l'aide de TPM. La clé privée est stockée via le nom de fournisseur que vous avez spécifié dans NomFournisseur (par exemple, Microsoft Platform Key Storage Provider).

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**LongueurClé** (spécifiez la taille de la clé privée en bits)

Valeur	Comment
2048	Default. 1024 ou 4096 peut également être utilisé.

Les paramètres du fichier de configuration sont représentés sous forme de graphiques comme suit (les valeurs par défaut d'installation apparaissent en rouge) :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Exemples de scénario de configuration

Cet exemple concerne la clé privée du certificat RA et les clés privées des certificats utilisateur à l'aide de Microsoft Software Key Storage Provider

Il s'agit de la configuration post-installation par défaut. Aucune configuration de clé privée supplémentaire n'est requise.

Cet exemple illustre la clé privée de certificat RA stockée dans la puce TPM matérielle de la carte mère du serveur FAS via Microsoft Platform Key Storage Provider et les clés privées des certificats utilisateur stockées à l'aide de Microsoft Software Key Storage Provider.

Ce scénario part du principe que la puce TPM sur la carte mère de votre serveur FAS a été activée dans le BIOS selon la documentation du fabricant de la puce TPM et initialisée dans Windows ; consultez la section https://technet.microsoft.com/en-gb/library/cc749022(v=ws.10).aspx.

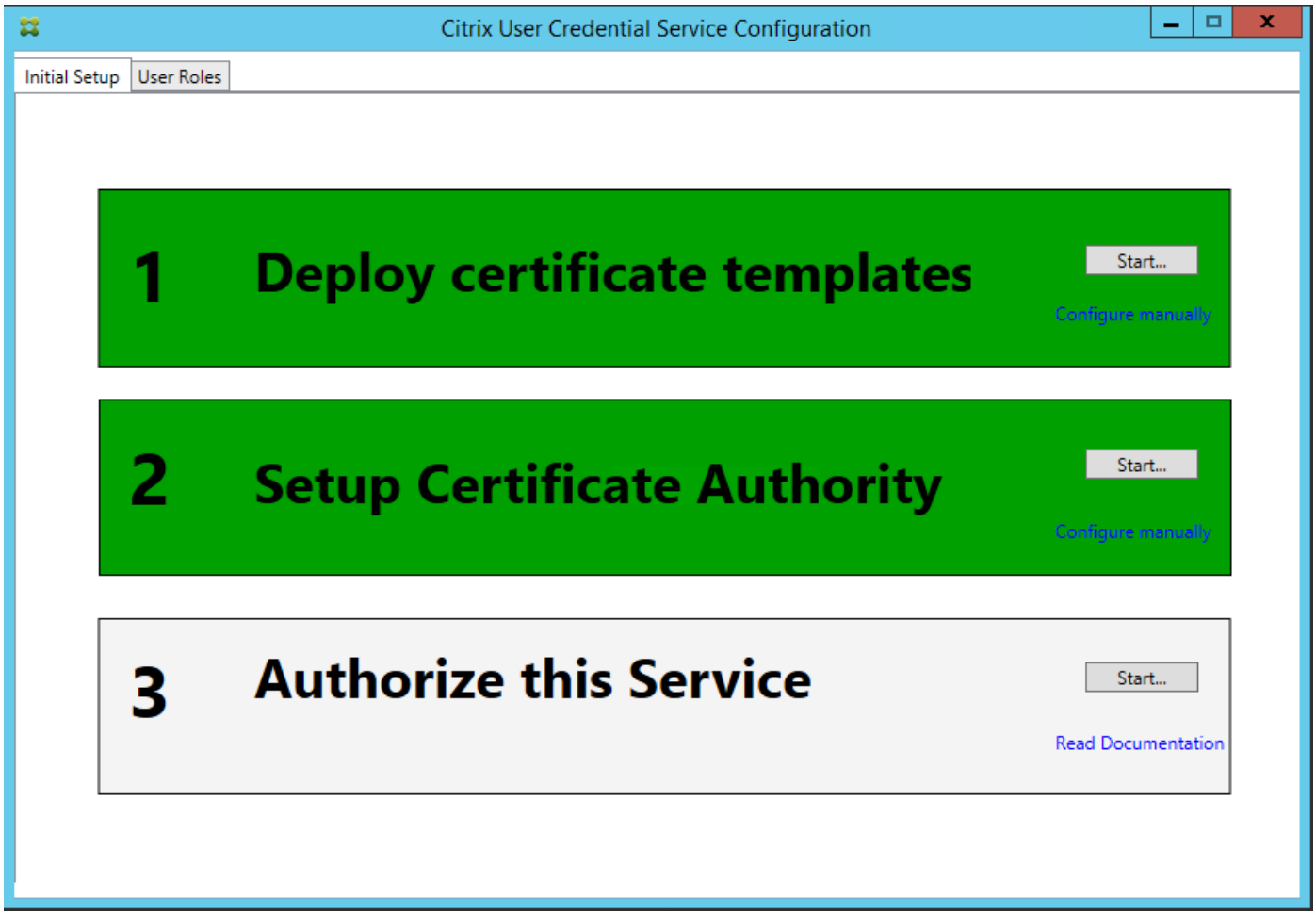
Utilisation de PowerShell (recommandé)

Le certificat RA peut être demandé en mode déconnecté à l'aide de PowerShell. Cette option est recommandée pour les

© 1999-2017 Citrix Systems, Inc. All rights reserved.

entreprises qui ne souhaitent pas que l'autorité de certification émette un certificat RA via une demande de signature de certificat en ligne. Une demande de signature de certificat RA en mode déconnecté ne peut pas être effectuée à l'aide de la console de gestion FAS.

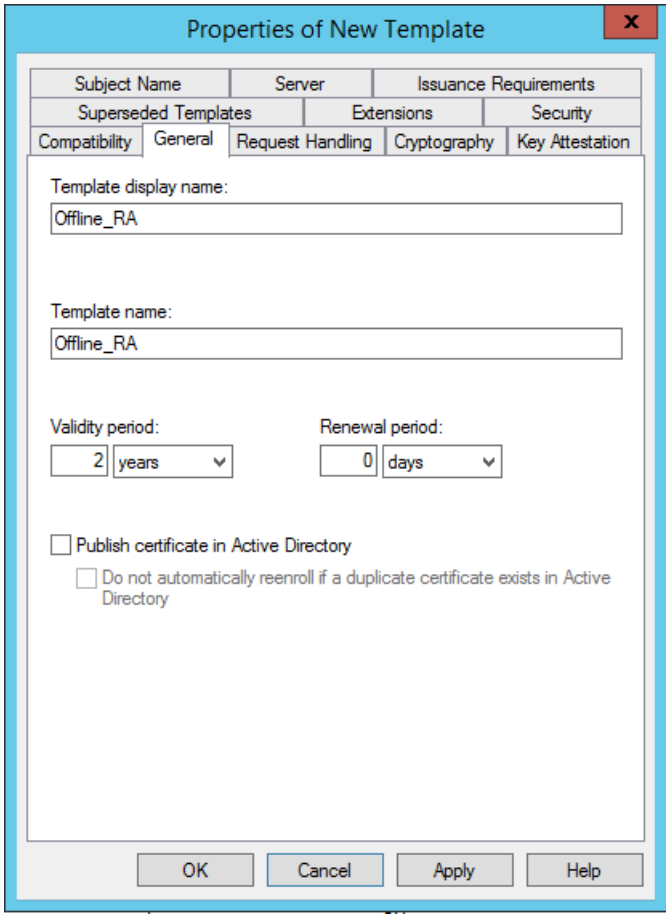
Étape 1 : lors de la configuration initiale du FAS à l'aide de la console de gestion, effectuez uniquement les deux premières étapes : « Déployer les modèles de certificat » et « Configurer l'autorité de certification ».



Étape 2 : sur le serveur d'autorité de certification, ajoutez le composant logiciel enfichable MMC des modèles de certificat. Cliquez avec le bouton droit sur le modèle **Citrix_RegistrationAuthority_ManualAuthorization** et sélectionnez **Dupliquer le modèle**.

Sélectionnez l'onglet **Général**. Modifiez le nom et la période de validité. Dans cet exemple, le nom est Offline_RA et la période de validité est de 2 ans :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Étape 3 : sur le serveur d'autorité de certification, ajoutez le composant logiciel enfichable MMC d'autorité de certification. Cliquez avec le bouton droit sur **Modèles de certificats**. Sélectionnez **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**. Choisissez le modèle que vous venez de créer.

Étape 4 : chargez les applets de commande PowerShell suivantes sur le serveur FAS :

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationServices.V1
```

Étape 5 : générez la paire de clés RSA dans la puce TPM du serveur FAS et créez la CSR en entrant l'applet de commande PowerShell suivante sur le FAS serveur. **Remarque** : certaines puces TPM limitent la longueur de clé. La valeur par défaut est une longueur de 2048 bits. Veillez à spécifier une longueur de clé prise en charge par votre matériel.

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address
```

Par exemple :

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.auth.net
```

Les éléments suivants sont affichés :

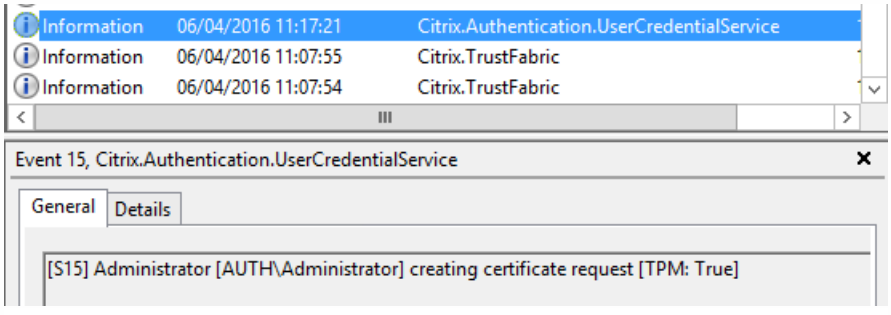
© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
PS C:\Users\Administrator.AUTH> New-UcsAuthorizationCertificateRequest -UseTPM $true -address ucshsm.auth.local

Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfROXW
                      lhCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAflbInFPgrz+
                      vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V7DcEYthxB8CfbaN9MHOEFbepoSYOCAfunXW
                      snwIbXD9lc/fGyN/3f94P4fbNrjEIOHc+4Oy/WsPgPBgcq9XBwRjzpGjOgOWRoJS9g22OY5PwD77
                      7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaE1WXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWHlvztpjxPeJzAVDsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICU8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
                      YlITNOtmcHFKt4Loz5D5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4l32xlmQrP/4XQvr1F+TD15PM5Fxjj6PEKWopWTYZXGzSC1ufxevcO1K
                      +tTH9tQYJM6xw3+6TIcfuWDjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TATO3XG/AB7o=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval


PS C:\Users\Administrator.AUTH> _
```

Remarques :

- L'ID GUID (dans cet exemple, « 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39 ») est requis dans une étape suivante.
- Considérez cette applet de commande PowerShell comme un « remplacement » à usage unique, utilisé pour générer la clé privée pour le certificat RA.
- Lors de l'exécution de cette applet de commande, les valeurs qui sont lues à partir du fichier de configuration lorsque le service FAS démarre sont vérifiées pour déterminer la longueur de clé à utiliser (la valeur par défaut est de 2048).
- Étant donné que -UseTPM est défini sur $true dans cette opération manuelle de clé privée de certificat RA initiée par PowerShell, le système ignore les valeurs du fichier qui ne correspondent pas aux paramètres requis pour utiliser une puce TPM.
- L'exécution de cette applet de commande ne modifie pas les paramètres du fichier de configuration.
- Durant les opérations automatiques de clé privée de certificat utilisateur initiées par FAS, les valeurs qui ont été lues à partir du fichier lorsque le service FAS a démarré seront utilisées.
- Il est également possible de définir la valeur KeyProtection dans le fichier de configuration sur GenerateTPMProtectedKey lorsque le serveur FAS émet des certificats utilisateur pour générer des clés privées de certificat utilisateur protégées par la puce TPM.

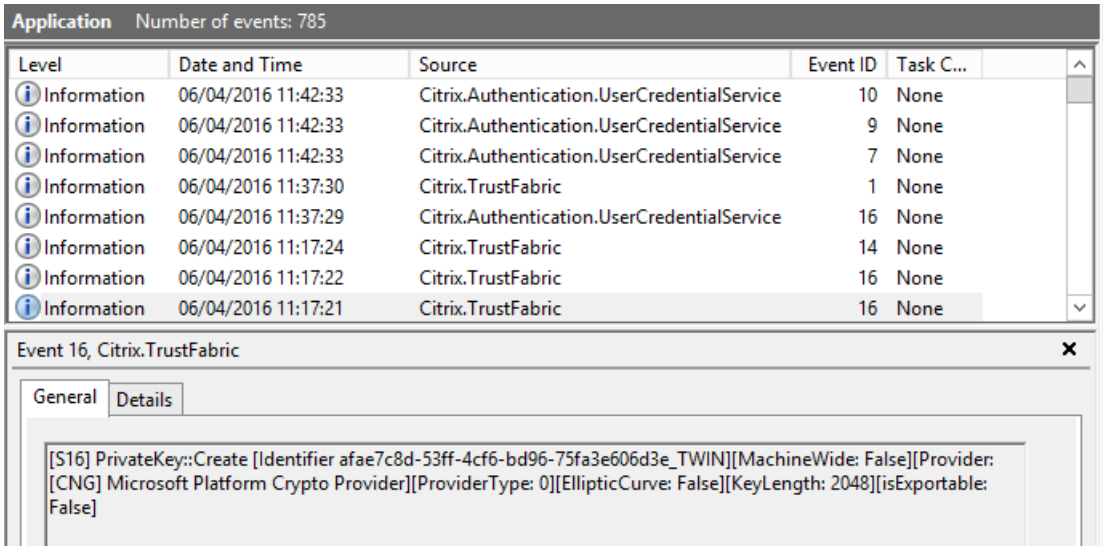
Pour vérifier que la puce TPM a été utilisée pour générer la paire de clés, consultez le journal d'application dans l'observateur d'événements de Windows sur le serveur FAS, à l'heure où la paire de clés a été générée.



Notez « [TPM: True] »

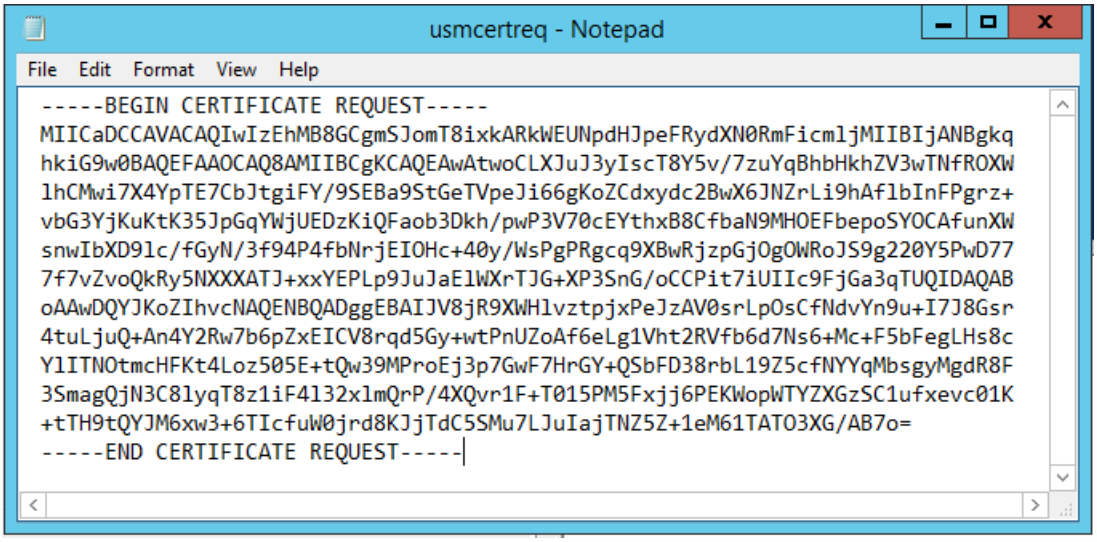
Suivi de :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Notez « Provider: [CNG] Microsoft Platform Crypto Provider »

Étape 6 : copiez la section de requête de certificat dans un éditeur de texte et enregistrez-la sur disque en tant que fichier texte.



Étape 7 : envoyez la demande de signature de certificat à l'autorité de certification (CA) en tapant les commandes suivantes dans PowerShell sur le serveur FAS :

```
certreq -submit -attrib "certificatetemplate:"
```

Par exemple :

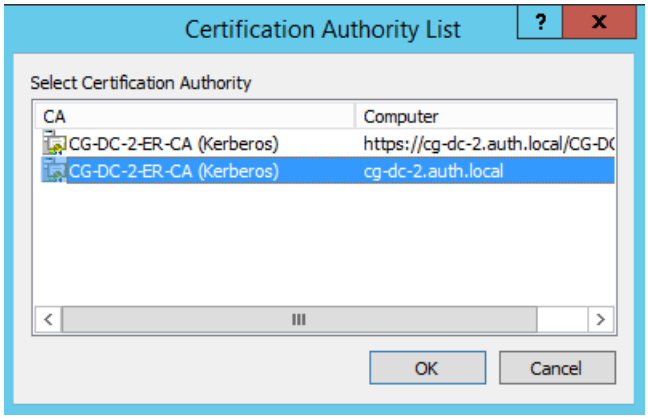
```
certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
```

Les éléments suivants sont affichés :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DBDC-4D21-A4FD-2E29502177C2}
  ldap:
```

À ce stade, une fenêtre contenant une liste d'autorités de certification peut s'afficher. Dans cet exemple, les inscriptions http (haut) et DCOM (bas) sont activées toutes les deux pour l'autorité de certification. Sélectionnez l'option DCOM, si elle est disponible :



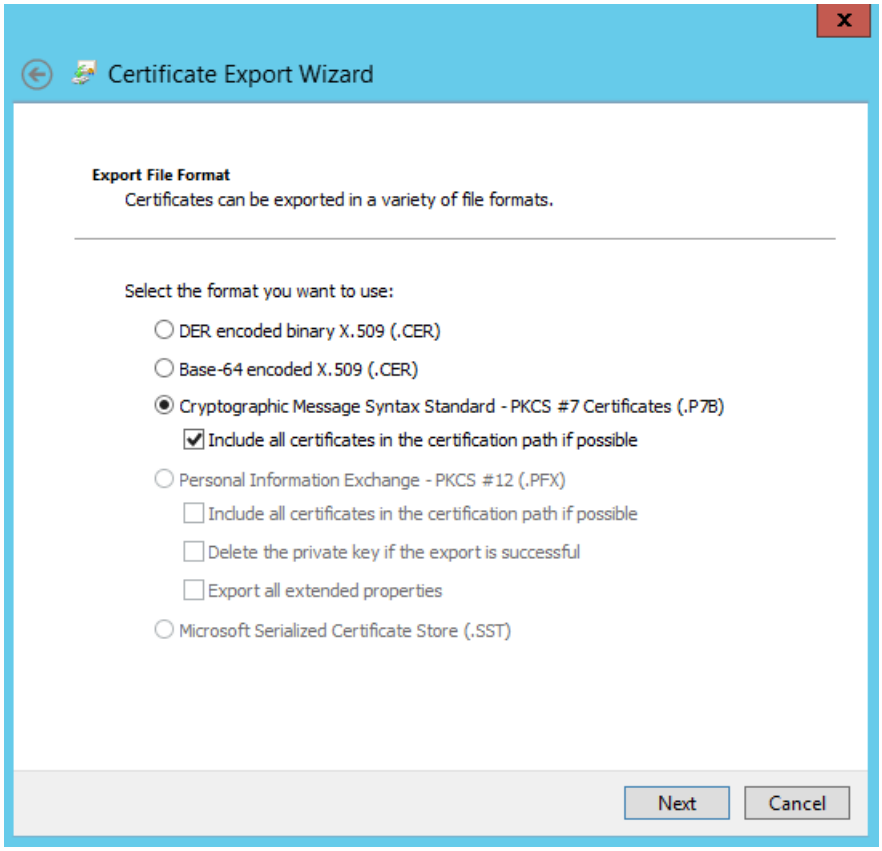
Après que l'autorité de certification (CA) a été spécifiée, PowerShell affiche la RequestID :

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DBDC-4D21-A4FD-2E29502177C2}
  ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH> _
```

Étape 8 : sur le serveur de l'autorité de certification (CA), dans le composant logiciel enfichable MMC CA, cliquez sur **Demandes en attente**. Notez l'ID de la demande, RequestID. Puis cliquez avec le bouton droit sur la demande et choisissez **Délivrer**.

Étape 9 : sélectionnez le nœud **Certificats délivrés**. Recherchez le certificat qui vient d'être émis (l'ID de demande doit correspondre). Cliquez deux fois pour ouvrir le certificat. Sélectionnez la page de l'onglet **Détails**. Cliquez sur **Copier dans un fichier**. L'Assistant d'exportation de certificat s'ouvre. Cliquez sur **Suivant**. Choisissez les options suivantes pour le format de fichier :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Le format doit être **Standard de syntaxe de message cryptographique – Certificate PKCS #7 (.P7B)** et **Inclure tous les certificats dans le chemin d'accès de certification, si possible** doit être sélectionné.

Étape 10 : copiez le fichier de certificat exporté sur le serveur FAS.

Étape 11 : importez le certificat RA dans le registre du serveur FAS en entrant l'applet de commande PowerShell suivante sur le serveur FAS :

```
Import-FasAuthorizationCertificateResponse -address <FQDN of FAS server> -Id <ID
GUID from step 5> -Pkcs7CertificateFile <Certificate file from step 10>
```

Par exemple :

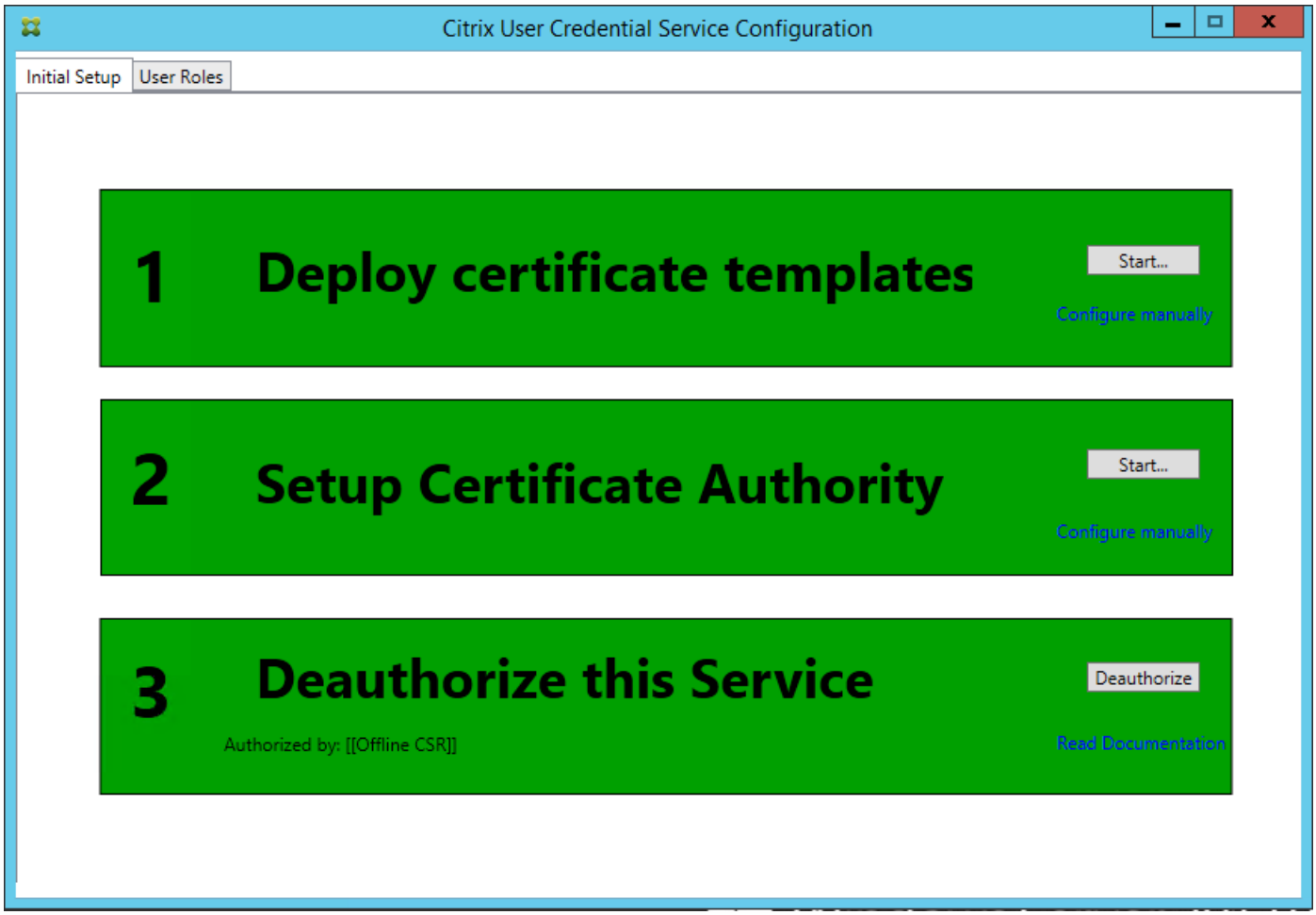
```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-
b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile
C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```

Les éléments suivants sont affichés :

```
PS C:\Users\Administrator.AUTH> Import-UcsAuthorizationCertificateResponse -address ucshsm.auth.local -Id 5ac3d8bd-b484-
4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_UCS_Cert.p7b


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           : a5c27fcc-1dd7-4c2b-8963-16ec311020fc
CertificateRequest :
Status              : Ok
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Étape 12 : fermez la console de gestion FAS, puis redémarrez-la.



Vous remarquerez que l'étape « Authorize this Service » est indiquée en vert, et affiche maintenant « Deauthorize this Service ». L'entrée en-dessous indique « Authorized by: Offline CSR »:

Étape 13 : sélectionnez l'onglet **User Roles** dans la console de gestion FAS et modifiez les paramètres décrits dans l'article FAS principal.

Remarque : annuler l'autorisation du FAS par le biais de la console de gestion supprime la règle de l'utilisateur.

Utilisation de la console de gestion FAS

La console de gestion ne peut pas effectuer de requête de signature de certificat en mode déconnecté ; son utilisation n'est donc pas recommandée si votre organisation ne permet pas les requêtes CSR en mode connecté pour les certificats RA.

Lorsque vous effectuez les étapes de configuration initiale du FAS, après le déploiement des modèles de certificat et la configuration de l'autorité de certification, mais avant d'autoriser le service (étape 3 dans la séquence de configuration) :

Étape 1 : modifiez le fichier de configuration en modifiant la ligne suivante comme suit :

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateTPMProtectedKey"/>
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Le fichier doit maintenant s'afficher comme suit :

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Certaines puces TPM limitent la longueur de clé. La valeur par défaut est une longueur de 2048 bits. Veillez à spécifier une longueur de clé prise en charge par votre matériel.

Étape 2 : autorisez le service.

Étape 3 : émettez manuellement la requête de certificat en attente depuis le serveur de l'autorité de certification. Une fois que le certificat RA a été obtenu, l'étape 3 dans la séquence d'installation de la console de gestion doit être indiquée en vert. À ce stade, la clé privée du certificat RA est générée dans la puce TPM. Le certificat sera valide pendant 2 ans par défaut.

Étape 4 : modifiez le fichier de configuration comme suit :

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateNonExportableKey"/>
```

Remarque : bien que FAS puisse générer des certificats utilisateur avec des clés protégées TPM, le matériel TPM peut être trop lent pour les déploiements de grande envergure.

Étape 5 : redémarrez le Service d'authentification fédérée Citrix. Cela oblige le service à relire le fichier de configuration et à refléter les valeurs modifiées. Les opérations de clé privée automatiques suivantes affecteront les clés de certificat utilisateur ; ces opérations ne stockeront pas les clés privées dans la puce TPM, mais utiliseront Microsoft Software Key Storage Provider.

Étape 6 : sélectionnez l'onglet User Roles dans la console de gestion FAS et modifiez les paramètres décrits dans l'article FAS principal.

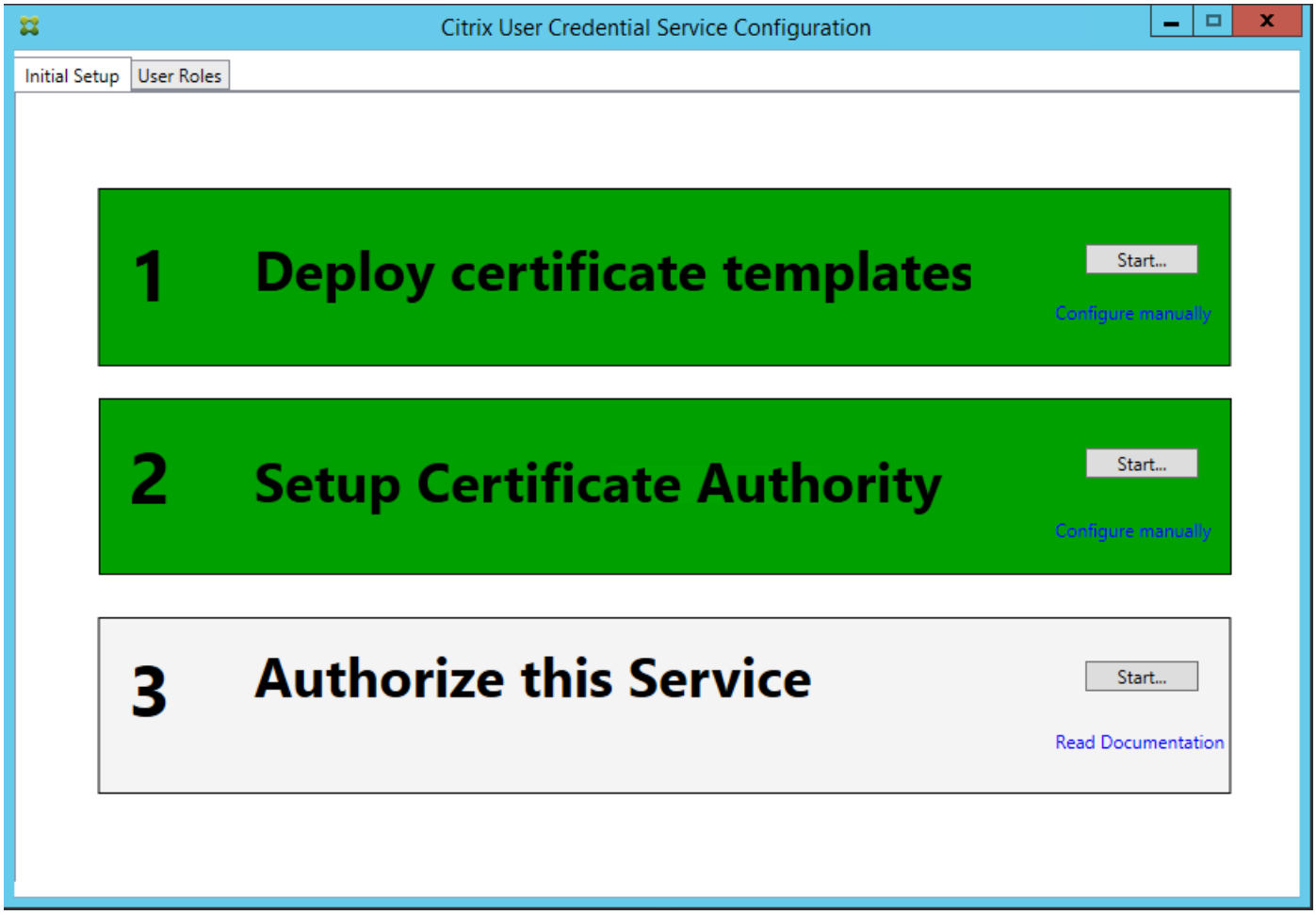
Remarque : annuler l'autorisation du FAS par le biais de la console de gestion supprime la règle de l'utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cet exemple illustre une clé privée de certificat RA et les clés privées de certificats utilisateur stockées dans un HSM. Cet exemple suppose un HSM configuré. Votre HSM aura un nom de fournisseur, par exemple « HSM_Vendor's Key Storage Provider ».

Si vous prévoyez d'exécuter votre serveur FAS dans un environnement virtualisé, demandez à votre fournisseur HSM si l'hyperviseur est pris en charge.

Étape 1. Lors de la configuration initiale du FAS à l'aide de la console de gestion, effectuez uniquement les deux premières étapes : « Déployer les modèles de certificat » et « Configurer l'autorité de certification ».



Étape 2 : consultez la documentation de votre fournisseur HSM pour déterminer ce que doit être la valeur ProviderName de votre HSM. Si votre HSM utilise CAPI, le fournisseur peut être désigné dans la documentation comme fournisseur de service cryptographique (CSP). Si votre HSM utilise CNG, le fournisseur peut être désigné comme Key Storage Provider (KSP).

Étape 3 : modifiez le fichier de configuration comme suit :

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
value="HSM_Vendor's Key Storage Provider"/>
```

Le fichier doit maintenant s'afficher comme suit :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Ce scénario part du principe que votre HSM utilise CNG de sorte que la valeur ProviderLegacyCsp est définie sur false. Si votre HSM utilise CAPI, la valeur ProviderLegacyCsp devrait être définie sur true. Consultez la documentation de votre fournisseur HSM pour déterminer si votre HSM utilise CAPI ou CNG. De plus, consultez la documentation de votre fournisseur HSM sur les longueurs de clé prises en charge pour la génération de clé asymétrique RSA. Dans cet exemple, la longueur de clé est définie sur la valeur par défaut de 2048 bits. Assurez-vous que la longueur de clé que vous avez spécifiée est prise en charge par votre matériel.

Étape 4 : redémarrez le Service d'authentification fédérée Citrix pour lire les valeurs à partir du fichier de configuration.

Étape 5 : générez la paire de clés RSA dans le HSM et créez la demande de signature de certificat en cliquant sur **Autoriser** dans l'onglet Initial Setup de la console de gestion FAS.

Étape 6 : pour vérifier que la paire de clés a été générée dans le HSM, vérifiez les entrées d'application dans le journal d'événements Windows :

```
[S16] PrivateKey::Create [Identifier e1608812-6693-4c54-a937-91a2e27df75b_TWIN][MachineWide: False][Provider: [CNG] HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

Note : [Provider: [CNG] HSM_Vendor's Key Storage Provider]

Étape 7 : sur le serveur de l'autorité de certification (CA), dans la MMC CA, sélectionnez le nœud **Demandes en attente**.

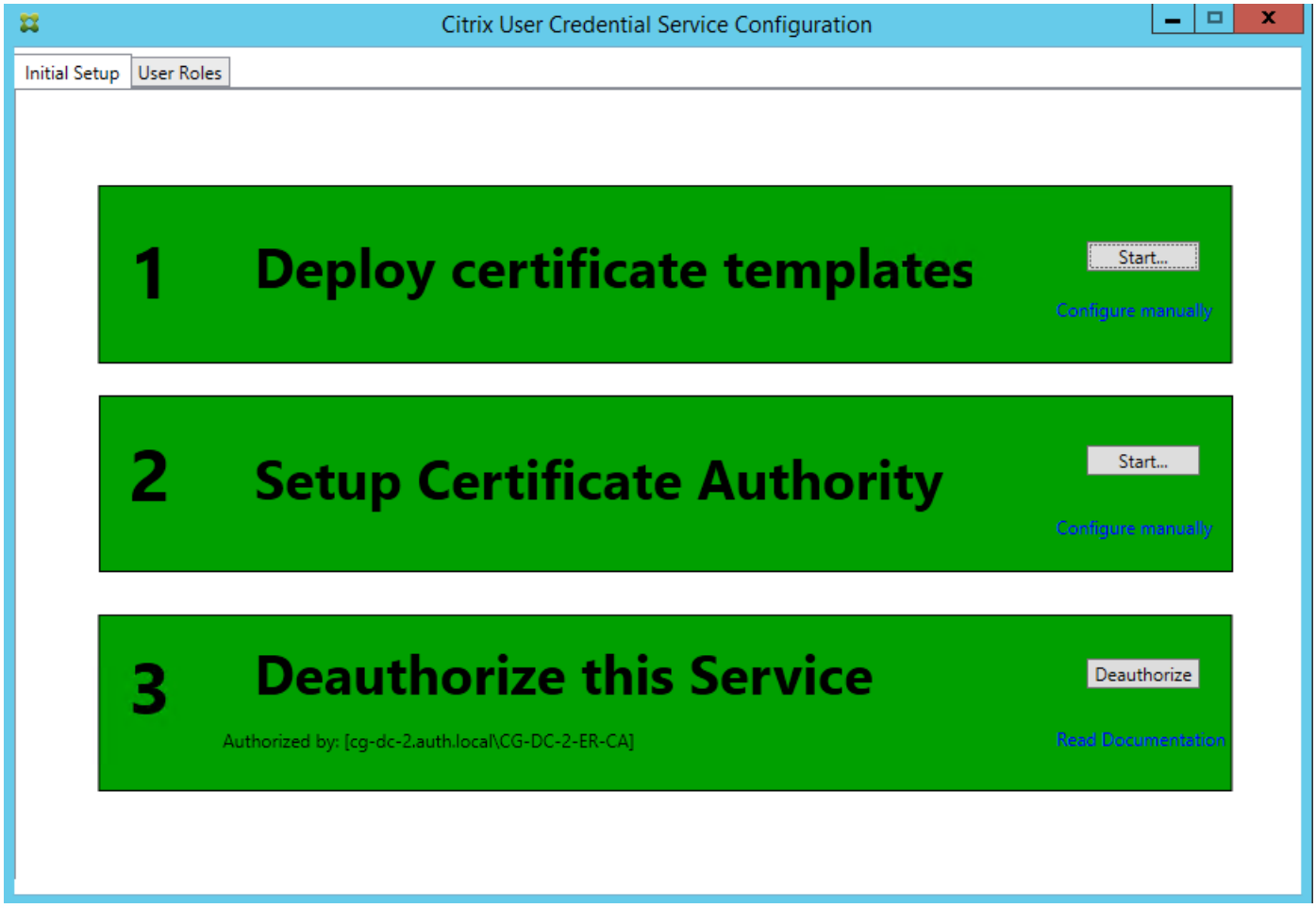
Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region
107	-----BEGIN NE...	The operation compl...	Taken Under Submission	07/04/2016 14:04	AUTH\UCSHSM$	

Cliquez avec le bouton droit sur la demande et choisissez **Délivrer**.

Vous remarquerez que l'étape « Authorize this Service » est indiquée en vert, et affiche maintenant « Deauthorize this

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Service ». L'entrée en-dessous indique « Authorized by: [] »:



Étape 8 : sélectionnez l'onglet **User Roles** dans la console de gestion FAS et modifiez les paramètres décrits dans l'article FAS principal.

Remarque : annuler l'autorisation du FAS par le biais de la console de gestion supprime la règle de l'utilisateur.

Stockage de certificats FAS

FAS n'utilise pas le magasin de certificats Microsoft sur le serveur FAS pour stocker ses certificats. Il utilise le registre.

Remarque : lorsque vous utilisez un HSM pour stocker des clés privées, les conteneurs HSM sont identifiés par un GUID. Le GUID pour la clé privée dans le HSM correspond au GUID du certificat équivalent dans le registre.

Pour déterminer le GUID du certificat RA, entrez les applets de commande PowerShell suivantes sur le serveur FAS :

```
Add-pssnapin Citrix.a*

Get-FasAuthorizationCertificate –address
```

Par exemple :

```
Get-FasAuthorizationCertificate –address cg-fas-2.auth.net
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
PS C:\Users\Administrator.AUTH> Get-UcsAuthorizationCertificate -address cg-ucs-2.auth.local


Id                  : a3958424-b8c3-4cac-ba0d-7eb3ce24591c
Address             : cg-dc-2.auth.local\CG-DC-2-ER-CA
TrustArea           : 3df77088-00e0-4dca-a47a-28060dc16986
CertificateRequest  :
Status              : MaintenanceDue

Id                  : fcb185f9-5069-4e34-8625-a333ac126535
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe
                      Rmm/xOVM6cNKsLbew3dYlbo+vdgWg86DFRVxTORhollV86iazDZyOiYGgxe9/s8YZzCspVWN1nB1
                      zXOUJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
                      ECz/CbXROOuiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfd/lBb3elZKA4OOoi9Ou64Q916
                      3ba9BnihqxIgvwWILOmyUfiJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhqL7Ppn1wIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKqgcJNJO/MU7/7X
                      bZB46drLPFzpzF88DkmfoCEgOxlbzFX9waaiFs9CHC/AcEzblN925y1gqljsfC3l5TCKBAeLFoMl
                      PSEkfYMQUOSBYCuLlkFn1LXLSeQ3qJTzSvptYROawFmUMQLffwLSR1vOuS8DJSrpASrwdXJk3TOa
                      GlO/xJo/NRMOwMH+AvGbBsgp3l+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC
                      H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIyOMLGZOOaiER+z8=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval
```

Pour obtenir une liste de certificats utilisateur, entrez :

Get-FasUserCertificate –address

Par exemple :

Get-FasUserCertificate –address cg-fas-2.auth.net

```
PS C:\Users\Administrator.AUTH> Get-UcsUserCertificate -address cg-ucs-2.auth.local


ThumbPrint            : 7BA22879F40EE92125A2F96E7DD2D52C73820459
UserPrincipalName     : walter@adfs.ext
Role                  : default
CertificateDefinition : default_Definition
ExpiryDate            : 05/04/2016 12:02:13
```

Informations connexes

- L'article Service d'authentification fédérée est le document de référence principal pour obtenir des informations sur l'installation et la configuration du FAS.
- Les déploiements FAS courants sont décrits dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée.
- D'autres informations pratiques sont disponibles dans l'article Configuration et gestion du service d'authentification fédérée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration du réseau et de la sécurité du Service d'authentification fédérée

Jul 13, 2016

Le Service d'authentification fédérée de Citrix (FAS) est étroitement intégré à Microsoft Active Directory et à l'autorité de certification Microsoft (CA). Il est essentiel de vous assurer que le système est géré et sécurisé de manière appropriée, en développant une stratégie de sécurité comme vous le feriez pour un contrôleur de domaine ou toute autre infrastructure critique.

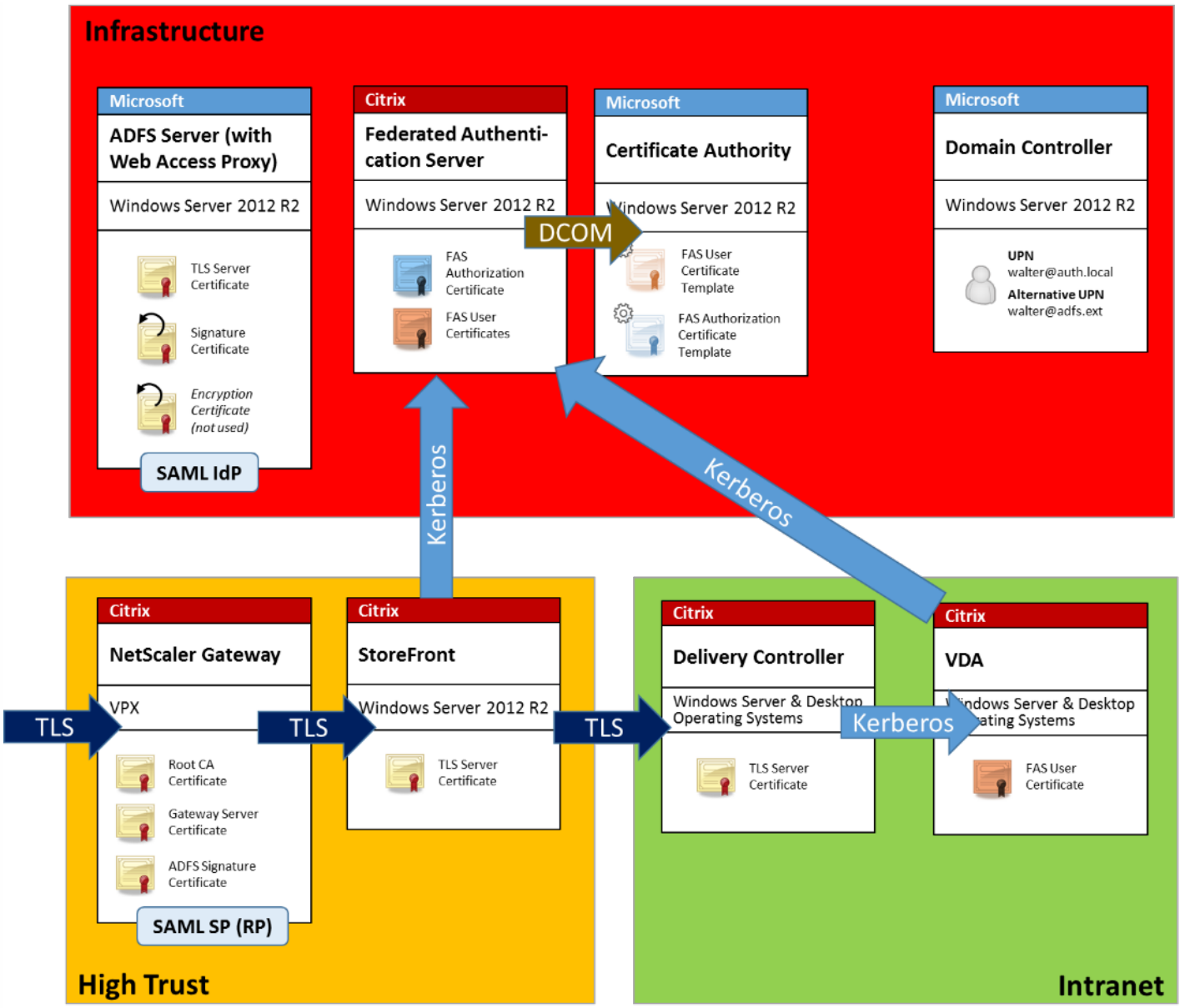
Ce document présente les problèmes de sécurité à prendre en compte lorsque vous déployez FAS. Il offre également une vue d'ensemble des fonctionnalités qui peuvent vous aider à sécuriser votre infrastructure.

Architecture réseau

Le diagramme suivant illustre les composants principaux et les limites de sécurité utilisés dans un déploiement FAS.

Le serveur FAS doit être considéré comme faisant partie de l'infrastructure de sécurité, tout comme l'autorité de certification et le contrôleur de domaine. Dans un environnement fédéré, Citrix NetScaler et Citrix StoreFront sont des composants approuvés pour authentifier les utilisateurs ; les autres composants de XenApp et XenDesktop ne sont pas affectés par l'introduction du service FAS.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Sécurité du réseau et pare-feu

Les communications entre les composants NetScaler, StoreFront et Delivery Controller doivent être protégées par TLS sur le port 443. Le serveur StoreFront se charge uniquement des connexions sortantes, et NetScaler Gateway doit uniquement accepter les connexions via Internet utilisant HTTPS sur le port 443.

Le serveur StoreFront contacte le serveur FAS sur le port 80 à l'aide de l'authentification mutuelle Kerberos . L'authentification utilise l'identité Kerberos HOST/fqdn du serveur FAS, et l'identité du compte de machine Kerberos du serveur StoreFront. Ceci génère un « handle d'informations d'identification » à usage unique requis par le Citrix Virtual Delivery Agent (VDA) pour connecter l'utilisateur.

Lorsqu'une session HDX est connectée au VDA, le VDA contacte également le serveur FAS sur le port 80. L'authentification utilise l'identité Kerberos HOST/fqdn du serveur FAS, et l'identité de la machine Kerberos du VDA. En outre, le VDA doit

© 1999-2017 Citrix Systems, Inc. All rights reserved.

fournir le « handle d'informations d'identification » pour accéder au certificat et à la clé privée.

L'autorité de certification Microsoft accepte les communications à l'aide du DCOM authentifié auprès de Kerberos, qui peut être configuré pour utiliser un port TCP fixe. L'autorité de certification requiert également que le serveur FAS fournisse un paquet CMC signé par un certificat d'agent d'inscription approuvé.

Port	Ports du pare-feu
Service d'authentification fédérée	[entrant] Kerberos via HTTP depuis StoreFront et VDA [sortant] DCOM vers autorité de certification Microsoft
Netscaler	[entrant] HTTPS depuis les machines clientes [entrant/sortant] HTTPS depuis/vers un serveur StoreFront [sortant] HDX vers VDA
StoreFront	[entrant] HTTPS depuis NetScaler [sortant] HTTPS vers Delivery Controller [sortant] HTTP Kerberos vers FAS
Delivery Controller	[entrant] HTTPS depuis un serveur StoreFront [entrant/sortant] Kerberos via HTTP depuis des VDA
VDA	[entrant/sortant] Kerberos via HTTP depuis Delivery Controller [entrant] HDX depuis NetScaler Gateway [sortant] HTTP Kerberos vers FAS
Microsoft CA	[entrant] DCOM et signé depuis FAS

Responsabilités en matière d'administration

L'administration de l'environnement peut être divisée dans les groupes suivants :

Nom	Responsabilité
Administrateur d'entreprise	Installer et sécuriser les modèles de certificat dans la forêt

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administrateur de domaine	Configurer les paramètres de stratégie de groupe
Administrateur d'autorité de certification	Configurer l'autorité de certification
Administrateur FAS	Installer et configurer le serveur FAS
Administrateur StoreFront/Netscaler	Configurer l'authentification utilisateur
Administrateur XenDesktop	Configurer les VDA et les Controller

Chaque administrateur contrôle différents aspects du modèle de sécurité, ce qui assure une protection approfondie du système.

Paramètres de stratégie de groupe

Les machines FAS approuvées sont identifiées par une table de recherche « numéro d'index -> FQDN » configurée via la stratégie de groupe. Lors de la communication avec un serveur FAS, les clients vérifient l'identité Kerberos HOST\ du serveur FAS. Tous les serveurs qui accèdent au serveur FAS doivent posséder les mêmes configurations de nom domaine complet (FQDN) pour le même index ; dans le cas contraire, il est possible que StoreFront et les VDA contactent des serveurs FAS différents.

Pour éviter toute erreur de configuration, Citrix recommande d'appliquer une seule stratégie à toutes les machines dans l'environnement. Soyez prudent lors de la modification de la liste des serveurs FAS, plus particulièrement lors de la suppression ou de la réorganisation d'entrées.

Le contrôle de cet objet de stratégie de groupe doit être limité aux administrateurs FAS (et/ou aux administrateurs de domaine) qui installent et désactivent des serveurs FAS. Prenez soin de ne pas réutiliser le nom de domaine complet (FQDN) d'une machine peu de temps après avoir désactivé un serveur FAS.

Modèles de certificats

Les modèles de certificats sont installés « à l'échelle de la forêt » par l'administrateur de l'entreprise. Il existe quatre considérations de sécurité.

Installation des modèles d'autorité d'inscription

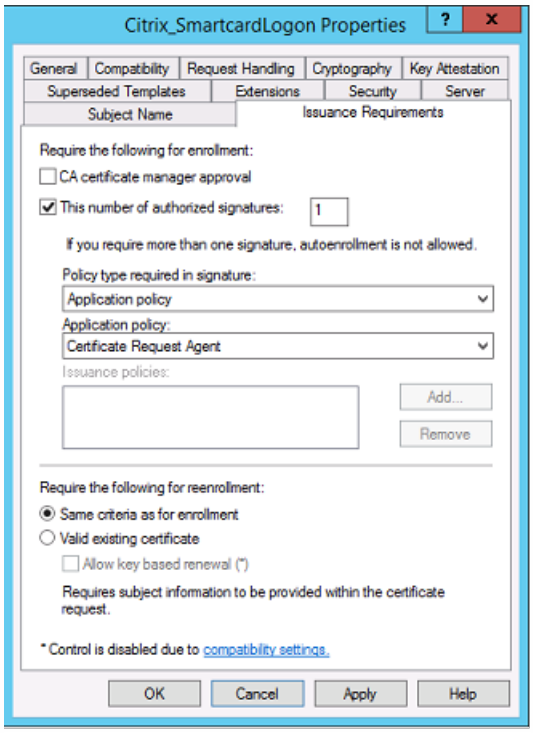
Le programme d'installation FAS offre deux types de modèles de certificats : les modèles d'autorité d'inscription (RA) et le modèle d'ouverture de session par carte à puce.

Seul le modèle d'ouverture de session par carte à puce est nécessaire au moment de l'exécution, par conséquent les autres modèles RA peuvent ne pas être installés (ce qui signifie que les certificats RA doivent être émis manuellement à l'aide d'une autorité de certification hors connexion distincte), ou peuvent être désactivés une fois qu'un serveur FAS a été autorisé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

OID de stratégie d'application

Les certificats RA sont identifiés grâce à l'inclusion d'un identificateur d'objet (OID) « Agent de demande de certificat » dans les extensions Utilisation avancée de la clé. Si cet OID est susceptible d'être utilisé par un autre système, un OID personnalisé peut être spécifié.

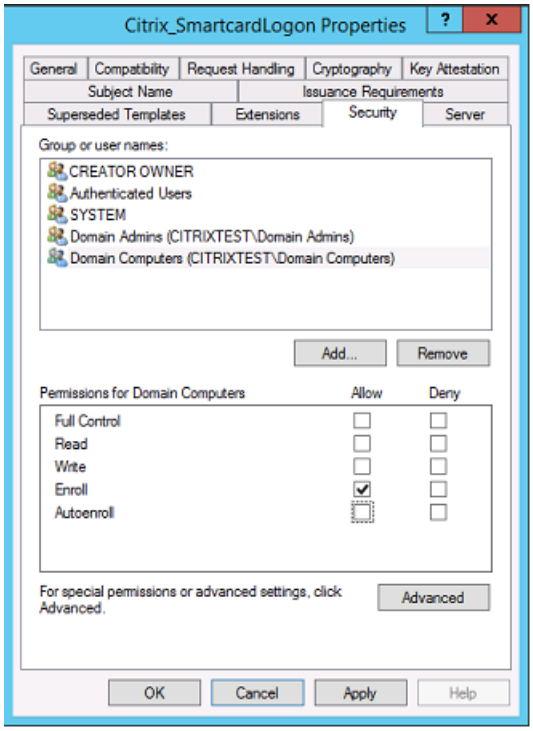


Liste de contrôle d'accès (ACL)

Chaque modèle contient une liste de contrôle d'accès qui contrôle les utilisateurs et les ordinateurs qui peuvent émettre des certificats.

Citrix recommande de reconfigurer cette liste ACL pour autoriser uniquement les comptes de machines des serveurs FAS à demander des certificats. Cela peut être limité encore plus à l'aide de stratégies de pare-feu réseau.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Contraintes liées au nom du sujet, aux extensions et au nom du chemin d'accès

Le nom du sujet et les extensions standard peuvent être configurés à l'aide des fonctionnalités RFC 5280 standard afin de contrôler à quelles fins les certificats émis peuvent être utilisés. Ceci offre un niveau de contrôle de base sur les certificats émis au travers de l'infrastructure de clé publique (PKI) qui peuvent être utilisés.

Administration de l'autorité de certification

L'administrateur de l'autorité de certification est responsable de la configuration du serveur d'autorité de certification et de l'émission de la clé privée de certificat qu'il utilise.

Publication de modèles

Pour qu'une autorité de certification puisse émettre des certificats basés sur un modèle fourni par l'administrateur de l'entreprise, l'administrateur de l'autorité de certification doit choisir de publier ce modèle.

Une simple pratique de sécurité consiste à publier uniquement les modèles de certificat RA lorsque les serveurs FAS sont installés, ou d'opter pour un processus d'émission hors connexion. Dans les deux cas, l'administrateur CA doit conserver un contrôle total sur l'autorisation des demandes de certificat RA, et disposer d'une stratégie pour autoriser les serveurs FAS.

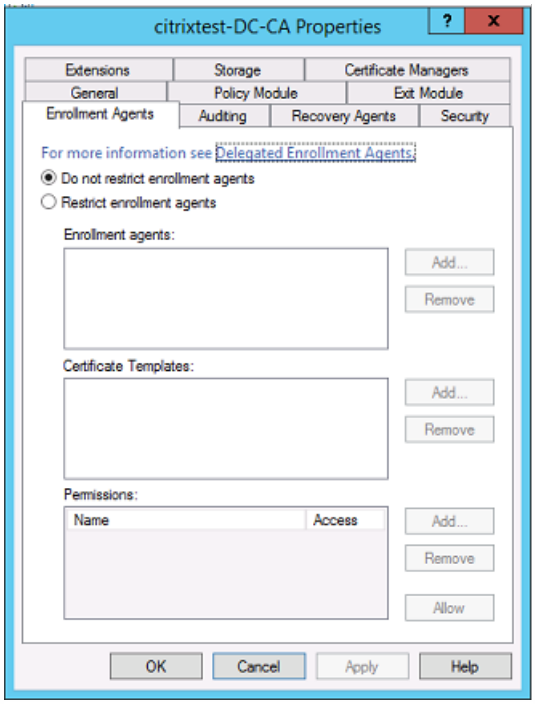
Paramètres de pare-feu

En général, l'administrateur CA contrôlera également les paramètres de pare-feu réseau de l'autorité de certification, ce qui permet de contrôler les connexions entrantes. L'administrateur de l'autorité de certification peut configurer le protocole TCP de DCOM et des règles de pare-feu de manière à ce que seuls les serveurs FAS puissent demander des certificats.

Inscription restreinte

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Par défaut, le détenteur d'un certificat RA peut émettre des certificats pour tous les utilisateurs, à l'aide d'un quelconque modèle de certificat autorisant l'accès. Ceci devrait être restreint à un groupe d'utilisateurs non privilégiés à l'aide de la propriété d'autorité de certification « Restreindre les agents d'inscription ».



Modules de stratégie et d'audit

Pour les déploiements avancés, des modules de sécurité personnalisés peuvent être utilisés pour assurer le suivi et interdire l'émission de certificats.

Administration du FAS

Le FAS possède plusieurs fonctions de sécurité.

Restreindre StoreFront, les utilisateurs et les VDA via une liste de contrôle d'accès

Au centre du modèle de sécurité du FAS figure le contrôle grâce auquel les comptes Kerberos peuvent accéder aux fonctionnalités :

Vecteur d'accès	Description
StoreFront [fournisseur d'identité]	Ces comptes Kerberos sont approuvés pour déclarer qu'un utilisateur a été correctement authentifié. Si l'un de ces comptes est compromis, des certificats peuvent être créés et utilisés pour les utilisateurs autorisés par la configuration du FAS.
VDA [partie de confiance]	Il s'agit des machines qui sont autorisées à accéder aux certificats et aux clés privées. Un handle d'informations d'identification récupéré par le fournisseur d'identité est également nécessaire, de façon à limiter les possibilités d'attaque du système par un compte VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	compromis dans ce groupe.
Utilisateurs	Contrôle les utilisateurs qui peuvent être certifiés par le fournisseur d'identité. Veuillez noter qu'il existe un chevauchement avec les options de configuration « Restreindre les agents d'inscription » de l'autorité de certification. En règle générale, il est conseillé d'inclure uniquement des comptes non privilégiés dans cette liste. Ceci empêche un compte StoreFront compromis de réaffecter des privilèges à un niveau administratif plus élevé. En particulier, les comptes d'administrateur de domaine ne doivent pas être autorisés par cette ACL.

Configurer des règles

Les règles sont utiles si plusieurs déploiements XenApp ou XenDesktop indépendants utilisent la même infrastructure de serveur FAS. Chaque règle dispose d'options de configuration distinctes ; en particulier, les ACL peuvent être configurées indépendamment.

Configurer l'autorité de certification et les modèles

Différents modèles de certificats et autorités de certification peuvent être configurés afin d'octroyer des droits d'accès différents. Des configurations avancées peuvent choisir d'utiliser plus ou moins de certificats puissants, en fonction de l'environnement. À titre d'exemple, les utilisateurs identifiés en tant que « externes » peuvent posséder un certificat avec moins de privilèges que les utilisateurs « internes ».

Certificats d'authentification et dans la session

L'administrateur FAS peut contrôler si le certificat utilisé pour l'authentification peut être utilisé dans la session de l'utilisateur. Par exemple, ceci peut être utilisé pour mettre uniquement à disposition des certificats « de signature » dans la session, afin de réserver le certificat « d'ouverture de session » plus puissant uniquement pour l'ouverture de session.

Protection de clé privée et longueur de clé

L'administrateur FAS peut configurer FAS afin de stocker les clés privées dans un module de sécurité matériel (HSM) ou un module de plateforme sécurisée (TPM). Citrix recommande de protéger au moins une clé privée de certificat RA en la stockant dans un TPM ; cette option est fournie dans le cadre du processus de demande de certificat « hors connexion ».

De même, les clés privées de certificat utilisateur peuvent être stockées dans un module TPM ou HSM. Toutes les clés doivent être générées en tant que « non exportables » et d'une longueur minimum de 2 048 bits.

Journaux d'événements

Le serveur FAS fournit des informations détaillées sur la configuration et des journaux d'événements, qui peuvent être utilisés pour l'audit et la détection des intrusions.

Accès administratif et outils d'administration

Le FAS comprend des fonctionnalités d'administration à distance (authentification mutuelle Kerberos) ainsi que des outils. Les membres du « groupe Administrateurs local » exercent un contrôle total sur la configuration du FAS. Cette liste doit être soigneusement tenue à jour.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administrateurs XenApp, XenDesktop et VDA

En général, l'utilisation du FAS ne modifie pas le modèle de sécurité des administrateurs Delivery Controller et VDA, car le « handle d'informations d'identification » du FAS remplace simplement le « mot de passe Active Directory. » Les groupes d'administration de Controller et de VDA doivent contenir uniquement des utilisateurs approuvés. L'audit et les journaux d'événements doivent être tenus à jour.

Sécurité des serveurs Windows

Tous les correctifs doivent avoir été installés sur tous les serveurs, de même que des pare-feu et des logiciels antivirus. Les serveurs d'infrastructure critiques à la sécurité doivent être conservés dans un endroit sécurisé, et un soin tout particulier doit être apporté au cryptage du disque et aux options de maintenance des machines virtuelles.

L'audit et les journaux d'événements doivent être stockés de manière sécurisée sur une machine distante.

L'accès RDP doit être limité aux administrateurs autorisés. Dans la mesure du possible, les comptes utilisateur doivent demander une ouverture de session par carte à puce, plus particulièrement pour les comptes d'administrateur de domaine et d'autorité de certification.

Informations connexes

- L'article Service d'authentification fédérée est le document de référence principal pour obtenir des informations sur l'installation et la configuration du FAS.
- Les architectures FAS sont présentées dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée.
- D'autres informations pratiques sont disponibles dans l'article Configuration et gestion du Service d'authentification fédérée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Service d'authentification fédérée - Résoudre les problèmes d'ouverture de session Windows

Aug 22, 2016

Dans cet article :

- Certificats et infrastructure de clé publique
- Nom UPN et mappage de certificat
- Sélection du contrôleur de domaine d'ouverture de session
- Activer les événements d'audit de compte
- Journaux de validation de certificat
- Journaux Kerberos
- Messages des journaux d'événements
- Messages d'erreur de l'utilisateur final
- Informations connexes

Cet article décrit les journaux et les messages d'erreur Windows lorsqu'un utilisateur ouvre une session à l'aide de certificats et/ou de cartes à puce. Ces journaux fournissent des informations que vous pouvez utiliser pour résoudre les échecs d'authentification.

Certificats et infrastructure de clé publique

Windows Active Directory propose plusieurs magasins de certificats qui gèrent les certificats pour les utilisateurs qui ouvrent une session.

- **Magasin de certificats NTAuth** : pour s'authentifier auprès de Windows, l'autorité de certification émettant les certificats utilisateur (aucune chaîne n'est prise en charge) doit être placée dans le magasin NTAuth. Pour afficher ces certificats, depuis le programme certutil, entrez : certutil –viewstore –enterprise NTAuth.
- **Magasins de certificats racine et intermédiaires** : en règle générale, les systèmes d'ouverture de session par certificat peuvent fournir un seul certificat. Donc, si une chaîne est utilisée, le magasin de certificats intermédiaires sur toutes les machines doit inclure ces certificats. Le certificat racine doit être dans le magasin racine de confiance et l'avant-dernier certificat doit être dans le magasin NTAuth.
- **Extensions de certificat d'ouverture de session et stratégie de groupe** : Windows peut être configuré pour appliquer la vérification des EKU et d'autres stratégies de certificat. Consultez la documentation Microsoft : https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx.

Stratégie du Registre	Description
AllowCertificatesWithNoEKU	Lorsqu'elle est désactivée, les certificats doivent inclure l'Utilisation améliorée de la clé (EKU) pour l'ouverture de session avec carte à puce.
AllowSignatureOnlyKeys	Par défaut, Windows filtre les clés privées de certificats qui ne

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	permettent pas le décryptage RSA. Cette option remplace ce filtre.
AllowTimeInvalidCertificates	Par défaut, Windows filtre les certificats expirés. Cette option remplace ce filtre.
EnumerateECCCerts	Active l'authentification à courbe elliptique.
X509HintsNeeded	Si un certificat ne contient pas de nom d'utilisateur principal (UPN) unique, ou s'il peut être ambigu, cette option permet aux utilisateurs de spécifier manuellement leur compte d'ouverture de session Windows.
UseCachedCRLOnlyAnd IgnoreRevocationUnknownErrors	Désactive la vérification de la révocation des certificats (généralement définie sur le contrôleur de domaine).

- **Certificats du contrôleur de domaine** : pour authentifier les connexions Kerberos, tous les serveurs doivent avoir des certificats « Contrôleur de domaine » appropriés. Ils peuvent être demandés depuis le menu du composant logiciel enfichable MMC « Local Computer Certificate Personal Store » (magasin personnel de certificats de l'ordinateur local).

Nom UPN et mappage de certificat

Il est recommandé que les certificats utilisateur incluent un nom d'utilisateur principal (UPN) unique dans l'extension Nom de sujet alternatif.

Noms UPN dans Active Directory

Par défaut, chaque utilisateur d'Active Directory est associé à un UPN implicite, basé sur le modèle @ et @. Les domaines disponibles et les noms de domaine complets sont inclus dans l'entrée RootDSE de la forêt. Veuillez noter qu'un seul domaine peut disposer de plusieurs noms de domaine complets enregistrés dans RootDSE.

En outre, chaque utilisateur d'Active Directory a un nom UPN explicite et des altUserPrincipalNames. Ce sont des entrées LDAP qui spécifient le nom d'utilisateur principal (UPN) pour l'utilisateur.

Lors d'une recherche d'utilisateurs par UPN, Windows recherche d'abord dans le domaine courant (en fonction de l'identité du processus de recherche de l'UPN) les UPN explicites, puis les UPN alternatifs. S'il n'existe pas de correspondance, il recherche l'UPN implicite, qui peut se résoudre sur différents domaines de la forêt.

Service de mappage de certificat

Si un certificat ne contient pas d'UPN explicite, Active Directory peut stocker un certificat public exact pour chaque utilisation dans un attribut « x509certificate ». Pour résoudre un tel certificat pour un utilisateur, un ordinateur peut interroger cet attribut directement (par défaut, dans un seul domaine).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

L'utilisateur peut spécifier un compte d'utilisateur qui accélère la recherche et permet également à cette fonctionnalité d'être utilisée dans un environnement inter-domaines.

S'il existe plusieurs domaines dans la forêt et que l'utilisateur ne spécifie pas explicitement un domaine, Active Directory rootDSE spécifie l'emplacement du service de mappage de certificat. Il est généralement situé sur une machine de catalogue global et bénéficie d'une vue en cache de tous les attributs x509certificate de la forêt. Cet ordinateur peut être utilisé pour rechercher efficacement un compte utilisateur dans tout domaine, en se basant uniquement sur le certificat.

Sélection du contrôleur de domaine d'ouverture de session

Lorsqu'un environnement contient plusieurs contrôleurs de domaine, il est utile de voir et de restreindre le contrôleur de domaine qui est utilisé pour l'authentification, de façon à ce que les journaux puissent être activés et récupérés.

Contrôler la sélection du contrôleur de domaine

Pour forcer Windows à utiliser un contrôleur de domaine Windows spécifique pour l'ouverture de session, vous pouvez explicitement définir la liste des contrôleurs de domaine qu'une machine Windows utilise en configurant le fichier lmhosts : \Windows\System32\drivers\etc\lmhosts.

Il existe généralement un exemple de fichier nommé « lmhosts.sam » dans cet emplacement. Il vous suffit d'inclure une ligne :

1.2.3.4 dcnetbiosname #PRE #DOM:mondomaine

Où « 1.2.3.4 » est l'adresse IP du contrôleur de domaine nommé « dcnetbiosname » dans le domaine « mondomaine ».

Après un redémarrage, la machine Windows utilise ces informations pour ouvrir une session sur mondomaine. Notez que cette configuration doit être rétablie lors d'un débogage.

Identifier le contrôleur de domaine utilisé

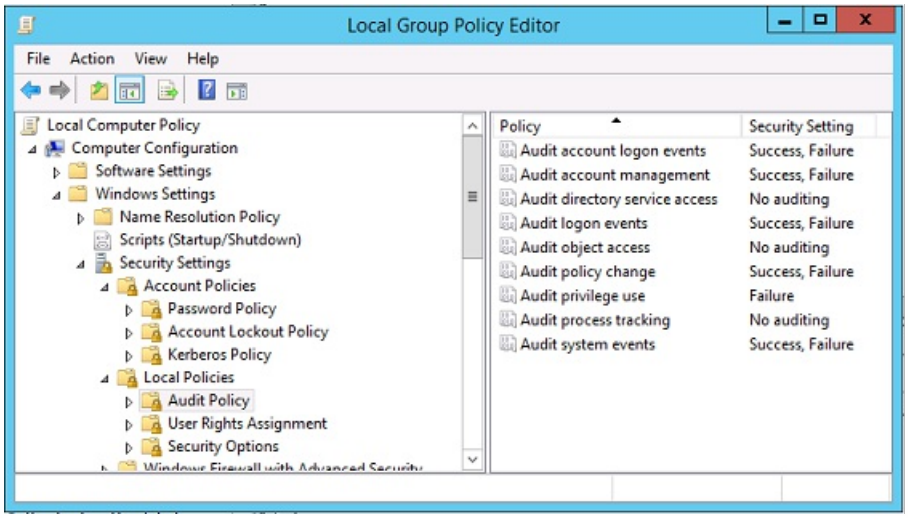
À l'ouverture de session, Windows définit une variable d'environnement MSDOS avec le contrôleur de domaine qui a ouvert la session de l'utilisateur. Pour la voir, démarrez l'invite de commande avec la commande : **echo %LOGONSERVER%**.

Les journaux liés à l'authentification sont stockés sur l'ordinateur renvoyé par cette commande.

Activer les événements d'audit de compte

Par défaut, les contrôleurs de domaine Windows n'activent pas les journaux d'audit de compte complets. Ce réglage peut être contrôlé par le biais des stratégies d'audit dans les paramètres de sécurité dans l'éditeur de stratégie de groupe. Une fois qu'ils sont activés, le contrôleur de domaine génère des informations supplémentaires dans le journal d'événements de sécurité.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Journaux de validation de certificat

Vérifier la validité du certificat

Si un certificat de carte à puce est exporté en tant que certificat DER (sans clé privée), vous pouvez le valider avec la commande : certutil –verify user.cer

Activer la journalisation CAPI

Sur le contrôleur de domaine et les machines utilisateur, ouvrez l'observateur d'événements et activez la journalisation pour Microsoft/Windows/CAPI2/Operational Logs.

Vous pouvez contrôler la journalisation CAPI avec les clés de registre dans : CurrentControlSet\Services\crypt32.

Valeur	Description
DiagLevel (DWORD)	Niveau de détail (0 à 5)
DiagMatchAnyMask (QUADWORD)	Filtre d'événements (utiliser 0xffffff pour tout)
DiagProcessName (MULTI_SZ)	Filtre par nom du processus (par exemple, LSASS.exe)

Journaux CAPI

Message	Description
Build Chain	CertGetCertificateChain appelé par LSA (comprend résultat)
Verify Revocation	CertVerifyRevocation appelé par LSA (comprend résultat)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

X509 Objects	En mode détaillé, les certificats et les listes de révocation de certificats (CRL) sont placés dans AppData\LocalLow\Microsoft\X509Objects
Verify Chain Policy	CertVerifyChainPolicy appelé par LSA (comprend paramètres)

Messages d'erreur

Code d'erreur	Description
Certificat non approuvé	Le certificat de carte à puce n'a pas pu être créé à l'aide de certificats contenus dans les magasins de certificats racine approuvés et intermédiaires de l'ordinateur.
Erreur de vérification de la révocation de certificats	La liste de révocation de certificats pour la carte à puce n'a pas pu être téléchargée à partir de l'adresse spécifiée par le point de distribution de la liste de révocation de certificat. Si la vérification de la révocation des certificats est obligatoire, l'ouverture de session échoue. Consultez la section Certificats et infrastructure de clé publique.
Erreurs d'utilisation de certificat	Le certificat n'est pas approprié pour l'ouverture de session. Par exemple, il peut s'agir d'un certificat de serveur ou d'un certificat de signature.

Journaux Kerberos

Pour activer la journalisation Kerberos, sur le contrôleur de domaine et la machine utilisateur, créez les valeurs de registre suivantes :

Ruche	Nom de la valeur	Valeur [DWORD]
CurrentControlSet\Control\Lsa\Kerberos\Parameters	LogLevel	0x1
CurrentControlSet\Control\Lsa\Kerberos\Parameters	KerbDebuglevel	0xffffffff
CurrentControlSet\Services\Kdc	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

© 1999-2017 Citrix Systems, Inc. All rights reserved.

La journalisation Kerberos est écrite dans le journal d'événements système.

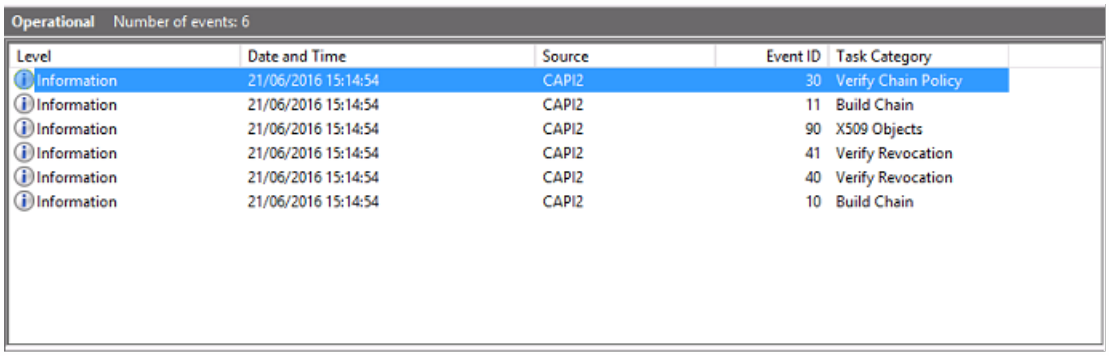
- Les messages tels que « certificat non approuvé » (untrusted certificate) devraient être faciles à diagnostiquer.
- Deux codes d'erreur sont des messages d'informations et peuvent être ignorés :
  - KDC_ERR_PREAUTH_REQUIRED (utilisé pour la rétrocompatibilité avec les contrôleurs de domaine plus anciens)
  - Erreur inconnue 0x4b

Messages des journaux d'événements

Cette section décrit les entrées de journal attendues sur le contrôleur de domaine et la station de travail lorsque l'utilisateur ouvre une session avec un certificat.

- Journal CAPI2 du contrôleur de domaine
- Journaux de sécurité du contrôleur de domaine
- Journal de sécurité VDA
- Journal CAPI VDA
- Journal système VDA

Lors d'une ouverture de session, le contrôleur de domaine valide le certificat de l'appelant, produisant une séquence d'entrées de journal comme illustré ci-dessous.



Le dernier message du journal d'événements indique que lsass.exe sur le contrôleur de domaine construit une chaîne en fonction du certificat fourni par le VDA et vérifie sa validité (y compris la révocation). Le résultat est « ERROR_SUCCESS ».

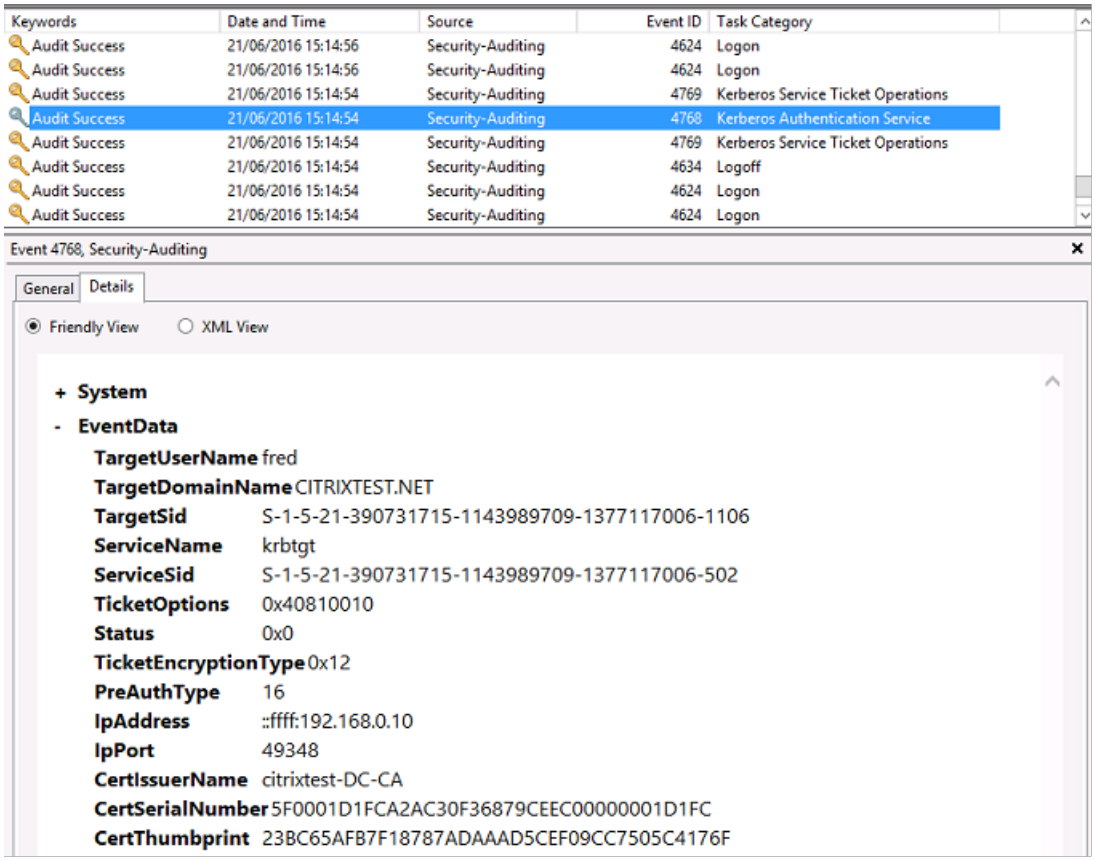
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **CertVerifyCertificateChainPolicy**
  - **Policy**
    - [**type**] CERT_CHAIN_POLICY_NT_AUTH
    - [**constant**] 6
  - **Certificate**
    - [**fileRef**] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    - [**subjectName**] fred
  - **CertificateChain**
    - [**chainRef**] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}
  - **Flags**
    - [**value**] 0
  - **Status**
    - [**chainIndex**] -1
    - [**elementIndex**] -1
  - **EventAuxInfo**
    - [**ProcessName**] lsass.exe
  - **CorrelationAuxInfo**
    - [**TaskId**] {F5E7FD3F-628F-4C76-9B1C-49FED786318F}
    - [**SeqNumber**] 1
  - **Result**
    - [**value**] 0

Le contrôleur de domaine présente une séquence des événements d'ouverture de session, l'événement clé étant 4768, dans lequel le certificat est utilisé pour émettre le ticket Kerberos Ticket Granting (krbtgt).

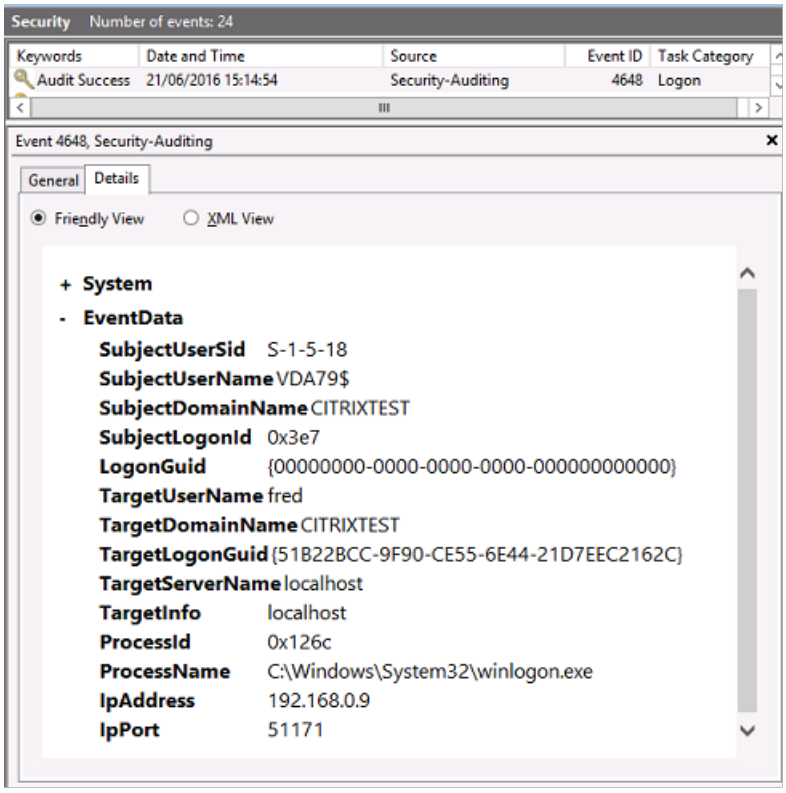
Les messages précédents indiquent que le compte de machine du serveur s'authentifie auprès du contrôleur de domaine. Les messages suivants indiquent le compte d'utilisateur appartenant au nouveau krbtgt utilisé pour s'authentifier auprès du contrôleur de domaine.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

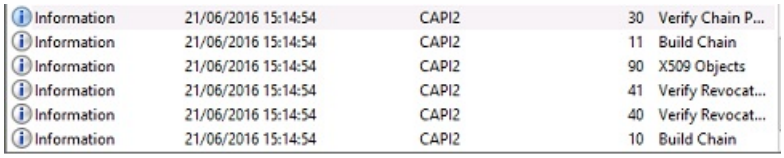


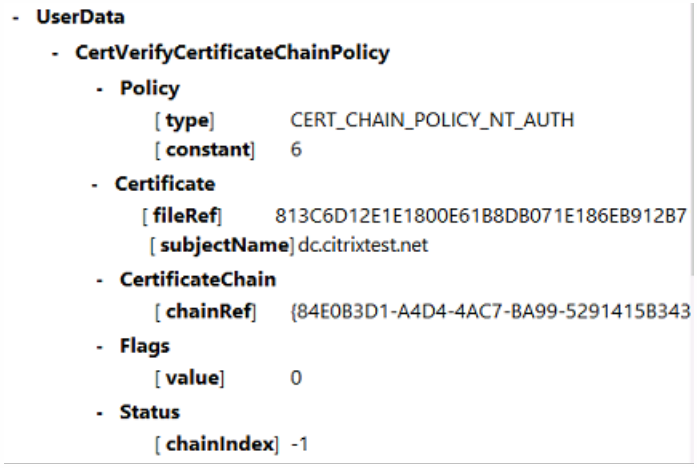
Le journal d'audit de sécurité VDA correspondant à l'événement d'ouverture de session est l'entrée avec l'ID 4648, provenant de winlogon.exe.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



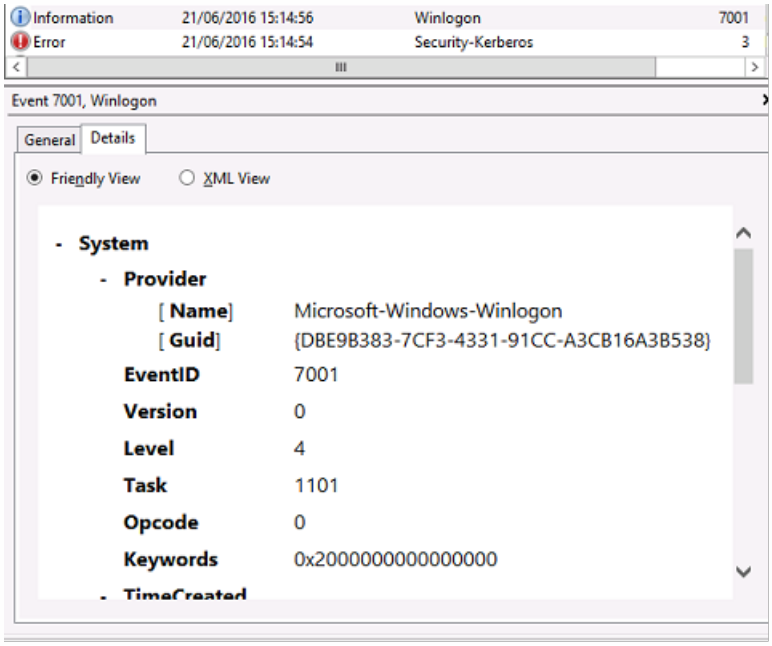
Cet exemple de journal CAPI VDA présente une séquence de création de chaîne et de vérification depuis lsass.exe, validant le certificat du contrôleur de domaine (dc.citrixtest.net).





 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Lorsque l'ouverture de session Kerberos est activée, le journal système affiche l'erreur KDC_ERR_PREAUTH_REQUIRED (qui peut être ignorée) et une entrée de Winlogon, indiquant que l'ouverture de session Kerberos a réussi.



Messages d'erreur de l'utilisateur final

Cette section dresse la liste des messages d'erreur courants s'affichant sur la page d'ouverture de session Windows.

Message d'erreur affiché	Description et référence
Nom d'utilisateur ou mot de passe non valide	L'ordinateur détecte que vous disposez d'un certificat et d'une clé privée valides, mais le contrôleur de domaine Kerberos a rejeté la connexion. Consultez la section Journaux Kerberos de cet article.
Le système n'a pas pu vous connecter. Impossible de vérifier les informations d'identification. La requête n'est pas prise en charge.	Le contrôleur de domaine ne peut pas être contacté, ou les certificats appropriés ne sont pas installés sur le contrôleur de domaine. Réinscrivez les certificats « Contrôleur de domaine » et « Authentification du contrôleur de domaine » sur le contrôleur de domaine, comme décrit dans la section CTX206156. Cette réinscription est recommandée, même lorsque les certificats existants semblent valides.
Le système n'a pas pu vous connecter. Le certificat de carte à puce utilisé pour l'authentification n'est pas approuvé.	Les certificats racine et intermédiaire ne sont pas installés sur l'ordinateur local. Consultez l'article CTX206156 pour obtenir des instructions sur l'installation de certificats de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	carte à puce sur des ordinateurs n'appartenant pas à un domaine. Consultez aussi la section Certificats et infrastructure de clé publique dans cet article.
Vous ne pouvez pas ouvrir de session car l'ouverture de session par carte à puce n'est pas prise en charge par votre compte.	Un compte utilisateur de groupe de travail n'a pas été complètement configuré pour l'ouverture de session par carte à puce.
La clé requise n'existe pas	Un certificat fait référence à une clé privée qui n'est pas accessible. Cela peut se produire lorsqu'une carte PIV n'est pas correctement configurée et que le fichier CCC ou CHUID est manquant.
Une erreur s'est produite lors de la tentative d'utilisation de la carte à puce	Le middleware de carte à puce n'a pas été correctement installé. Consultez l'article CTX206156 pour des instructions d'installation de carte à puce.
Insérez une carte à puce.	Le lecteur ou la carte à puce n'a pas été détecté. Si la carte à puce est insérée, ce message indique un problème de matériel ou de middleware. Voir CTX206156 pour des instructions d'installation de carte à puce.
Le code PIN est incorrect	La carte à puce a rejeté un code PIN entré par l'utilisateur.
Aucun certificat de carte à puce valide n'a été trouvé.	Les extensions du certificat peuvent ne pas être correctement configurées, ou la clé RSA est trop courte (<2 048 bits). Consultez l'article CTX206901 pour de plus amples informations sur la génération de certificats de carte à puce valides.
La carte à puce est bloquée	Une carte à puce a été verrouillée (par exemple, la saisie d'un code PIN incorrect plusieurs fois). Un administrateur peut avoir accès au code de déverrouillage du code PIN (puk) pour la carte et peut réinitialiser le code PIN de l'utilisateur à l'aide d'un outil du fournisseur de carte à puce. Si le code puk n'est pas disponible ou verrouillé, la carte doit être réinitialisée sur ses paramètres d'usine.
Demande incorrecte	Une clé privée de carte à puce ne prend pas en charge la cryptographie requise par le contrôleur de domaine. Par

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	exemple, le contrôleur de domaine peut avoir demandé un « décryptage de clé privée », mais la carte à puce ne prend en charge que la signature. Ceci indique habituellement que les extensions sur le certificat ne sont pas définies correctement, ou que la clé RSA est trop courte (<2 048 bits). Consultez la section CTX206901 pour de plus amples informations sur la génération de certificats de carte à puce valides.

Informations connexes

- Configuration d'un domaine pour l'ouverture de session par carte à puce : http://support.citrix.com/article/CTX206156
- Stratégies d'ouverture de session par carte à puce : https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx
- Activation de la journalisation CAPI : http://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx
- Activation de la journalisation Kerberos : https://support.microsoft.com/en-us/kb/262177
- Recommandations pour l'activation de l'ouverture de session par carte à puce avec des autorités de certification tierces : https://support.microsoft.com/en-us/kb/281245

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SDK PowerShell du Service d'authentification fédérée

Aug 22, 2016

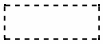
Vous pouvez utiliser la console d'administration Service d'authentification fédérée pour les déploiements simples, toutefois l'interface PowerShell offre des options plus avancées. Si vous prévoyez d'utiliser des options qui ne sont pas disponibles dans la console, Citrix recommande d'utiliser uniquement PowerShell pour la configuration.

La commande suivante ajoute les applets de commande PowerShell du FAS :

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

Dans une fenêtre PowerShell, vous pouvez utiliser Get-Help <*nom cmdlet*> pour afficher l'aide de l'applet de commande.

Le lien vers le fichier zip ci-dessous contient des fichiers d'aide pour toutes les applets de commande du SDK PowerShell du FAS. Pour l'utiliser, cliquez sur le lien pour télécharger le fichier zip. Extrayez ensuite le contenu du fichier sur un dossier local. Le fichier index.html répertorie toutes les applets de commande, avec des liens vers les fichiers d'aide d'applet de commande individuels.



Fichiers d'aide de l'applet de commande du PowerShell du Service d'authentification fédérée

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Imprimer

Jul 15, 2016

La gestion des imprimantes dans votre environnement est un processus à plusieurs étapes :

1. Familiarisation avec les concepts d'impression, si ce n'est pas déjà le cas.
2. Planifiez votre architecture d'impression. Cela comprend l'analyse des besoins de votre entreprise, votre infrastructure d'impression existante, la façon dont vos utilisateurs et applications interagissent avec l'impression aujourd'hui et le modèle de gestion de l'impression qui s'applique le mieux à votre environnement.
3. Configurez votre environnement d'impression en sélectionnant une méthode de provisioning de l'imprimante et en créant des stratégies pour déployer votre solution d'impression. Mettez à jour des stratégies lorsque de nouveaux employés ou serveurs sont ajoutés.
4. Testez la configuration du pilote d'impression avant de le déployer auprès des utilisateurs.
5. Gérez votre environnement d'impression Citrix en gérant des pilotes d'imprimante et en optimisant les performances d'impression.
6. Résolvez les problèmes qui peuvent se produire.

Avant de commencer à planifier votre déploiement, assurez-vous que vous comprenez ces concepts majeurs pour l'impression :

- Les types suivants de provisioning de l'imprimante sont disponibles
- comment les tâches sont routées ;
- les bases de la gestion de pilotes d'impression.

Concepts d'impression créés sur les concepts d'impression Windows. Pour configurer et gérer l'impression correctement dans votre environnement, vous devez comprendre le fonctionnement de l'impression réseau et cliente Windows et ce que cela signifie en comportement d'impression dans cet environnement.

Dans cet environnement, toutes les impressions sont lancées (par l'utilisateur) sur les machines hébergeant les applications. Les tâches d'impression sont redirigées via le serveur d'impression réseau ou la machine utilisateur vers le périphérique d'impression.

Lorsqu'un utilisateur effectue l'impression :

- Détermine les imprimantes à fournir à l'utilisateur. Ceci est appelé provisioning de l'impression ;
- restaure les préférences d'impression de l'utilisateur ;
- détermine la nature de l'imprimante par défaut pour la session.

Vous pouvez personnaliser la manière dont vous souhaitez réaliser ces tâches en configurant des options pour le provisioning de l'impression, le routage des tâches d'impression, la rétention des propriétés d'imprimante et la gestion de pilotes. Veillez à évaluer la manière dont les paramètres des options peuvent modifier les performances d'impression dans votre environnement, ainsi que l'expérience de l'utilisateur.

Le processus par lequel les imprimantes sont mises à disposition dans une session est appelé provisioning. Le provisioning de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

l'imprimante est généralement traité de manière dynamique. En d'autres termes, les imprimantes qui s'affichent dans une session ne sont pas prédéterminées et stockés. Au lieu de cela, les imprimantes sont assemblées et basées sur les stratégies, au fur et à mesure que la session est créée lors de l'ouverture de session et la reconnexion. Par conséquent, les imprimantes peuvent changer selon la stratégie, l'emplacement de l'utilisateur, et les modifications de réseau, s'ils sont reflétés dans les stratégies. Par conséquent, les utilisateurs itinérants vers un autre emplacement peuvent voir les modifications apportées à leur espace de travail.

Le système surveille également les imprimantes côté client et ajuste dynamiquement les imprimantes créées automatiquement dans les sessions en fonction des ajouts, suppressions et modifications apportées aux imprimantes côté client. Cette découverte dynamique des imprimantes présente un avantage pour les utilisateurs itinérants lorsqu'ils se connectent à partir de divers périphériques.

Les méthodes les plus courantes de provisioning de l'imprimante sont :

- **Serveur d'impression universelle** : le serveur d'impression universelle Citrix fournit la prise en charge de l'impression universelle pour les imprimantes réseau. Le serveur d'impression universelle utilise le pilote d'impression universelle. Cette solution vous permet d'utiliser un pilote unique sur une machine avec OS de serveur pour permettre l'impression réseau à partir de n'importe quel périphérique.

  Citrix recommande d'utiliser le serveur d'impression universelle Citrix pour les scénarios de serveur d'impression distants. Le serveur d'impression universelle transfère la tâche d'impression sur le réseau selon un format optimisé et compressé, réduisant ainsi l'utilisation du réseau et améliorant l'expérience utilisateur.

  La fonctionnalité Serveur d'impression universelle comprend :

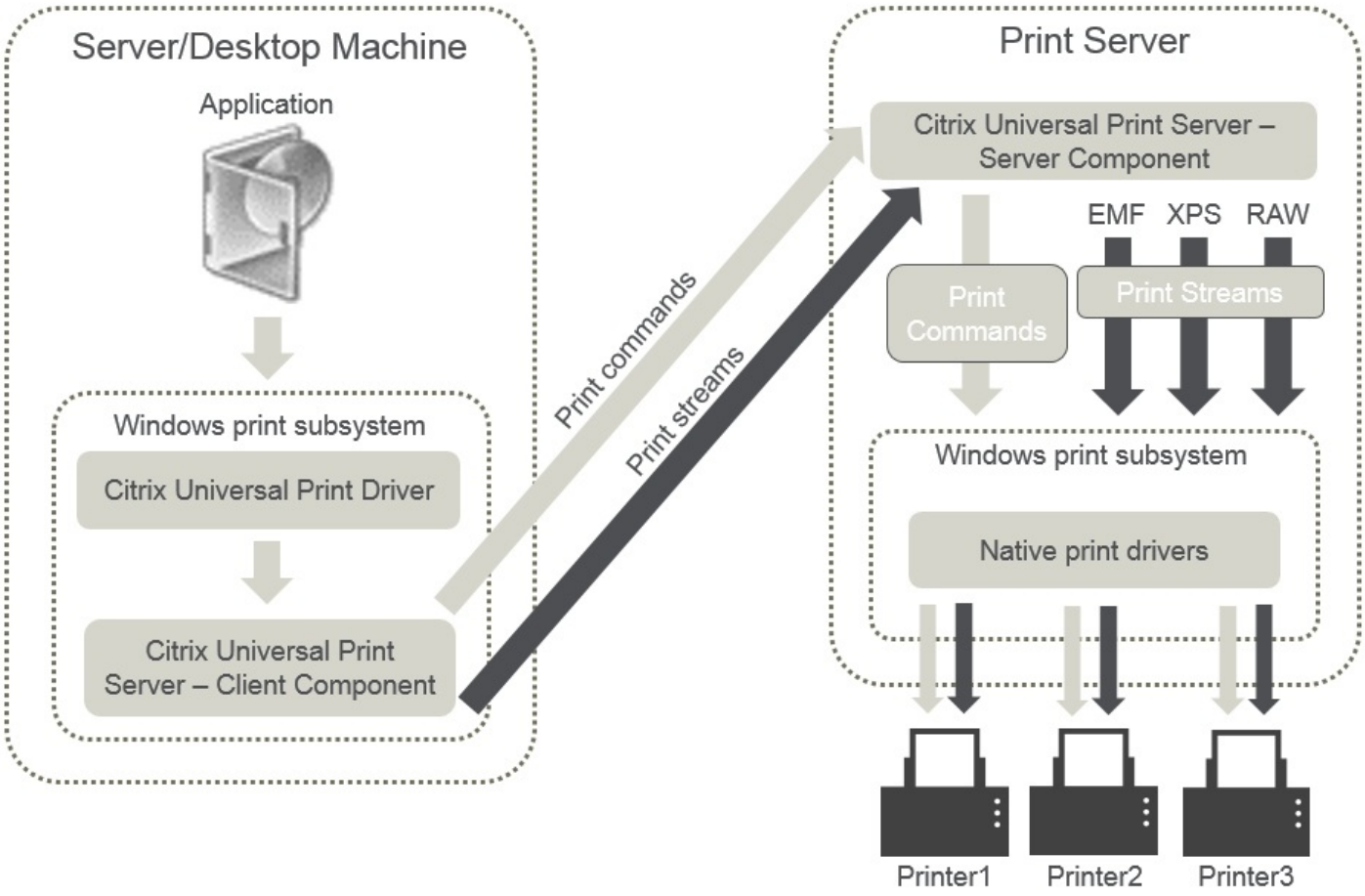
  Un composant client, **UPClient** : activez UPClient sur chaque machine avec OS de serveur qui provisionne les imprimantes réseau de session et utilise le pilote d'impression universelle.

  Un composant serveur, **UPServer** : installez UPServer sur chaque serveur d'impression qui provisionne les imprimantes réseau de session et qui utilise le pilote d'impression universelle pour les imprimantes de session (que les imprimantes de session soient provisionnées de manière centralisées ou non).

Pour la configuration requise du serveur d'impression universelle et les détails d'installation, reportez-vous aux articles Configuration système requise et Installation.

L'illustration suivante affiche le flux de travail classique pour un réseau en fonction de l'imprimante réseau dans un environnement qui utilise le serveur d'impression universelle.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Lorsque vous activez le Serveur d'impression universelle Citrix, toutes les imprimantes réseau connectées en tirent parti automatiquement via la découverte automatique.

Remarque : le Serveur d'impression universelle est également pris en charge pour VDI-in-a-Box 5.3. Pour plus d'informations sur l'installation du serveur d'impression universelle avec VDI-in-a-Box, reportez-vous à la documentation VDI-in-a-Box.

- **Création automatique** : le terme *Création automatique* fait référence aux imprimantes crées automatiquement au début de chaque session. À la fois les imprimantes réseaux distantes et les imprimantes clientes locales peuvent être créées automatiquement. Envisagez la création automatique uniquement de l'imprimante cliente par défaut pour les environnements possédant un grand nombre d'imprimantes par utilisateur. La création automatique d'un plus petit nombre d'imprimantes utilise moins de traitement de mémoire et de processeur sur les machines avec OS de serveur. La réduction des imprimantes créées automatiquement permet également de réduire les durées d'ouverture de session de l'utilisateur.
  Les imprimantes créées automatiquement sont basées sur :

  - les imprimantes installées sur la machine utilisateur ;
  - toutes les stratégies qui s'appliquent à la session.
    Les paramètres de stratégie de création automatique vous permettent de limiter le nombre ou le type d'imprimantes créées automatiquement. Par défaut, les imprimantes mises à disposition dans les sessions lors de la configuration automatique de toutes les imprimantes sur la machine cliente, y compris celles connectées localement et les imprimantes réseau.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Après que l'utilisateur ait mis fin à la session, les imprimantes de cette session sont supprimées.

La création automatique de l'imprimante cliente et réseau possède une maintenance associée. Par exemple, l'ajout d'une imprimante requiert que vous effectuiez les opérations suivantes :

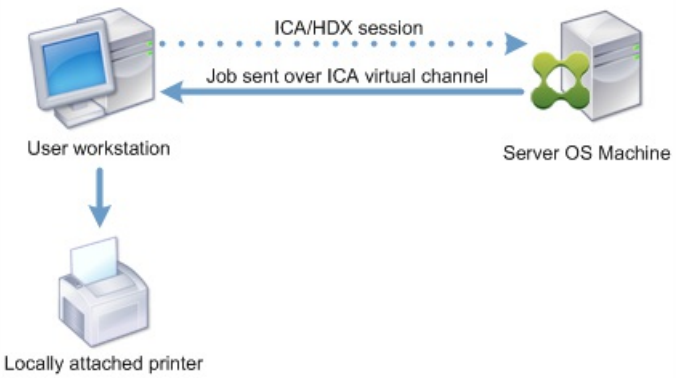
- Mettre à jour le paramètre de stratégie Imprimantes de session.
- Ajouter le pilote à toutes les machines avec OS de serveur utilisant le paramètre de stratégie Mappage et compatibilité du pilote d'imprimante.

Le terme piste d'impression regroupe à la fois le chemin suivant lequel les tâches d'impression sont routées et l'emplacement dans lequel les tâches d'impression sont spoulées. Les deux aspects de ce concept sont importants. Le routage affecte le trafic réseau. La mise en file d'attente affecte l'utilisation des ressources locales sur la machine qui traite la tâche d'impression.

Dans cet environnement, les tâches d'impression peuvent prendre deux chemins d'accès vers un périphérique d'impression : via le client ou via un serveur d'impression réseau. Ces chemins d'accès sont appelées piste d'impression cliente et piste d'impression réseau. Le chemin d'accès sélectionné par défaut dépend du type d'imprimante utilisé.

Imprimantes connectées localement

Le système route les tâches vers des imprimantes connectées localement à partir de la machine avec OS de serveur, au travers du client, puis vers le périphérique d'impression. Le protocole ICA optimise et compresse le trafic de la tâche d'impression. Lorsqu'un périphérique d'impression est connecté localement à la machine utilisateur, les tâches d'impression sont routées via le canal virtuel ICA.



Imprimantes réseau

Par défaut, toutes les tâches d'impression sont destinées à la route d'imprimantes réseau à partir de la machine avec OS de serveur, au travers du réseau, et directement vers le serveur d'impression. Cependant, les tâches d'impression sont routées automatiquement via la connexion ICA dans les cas suivants :

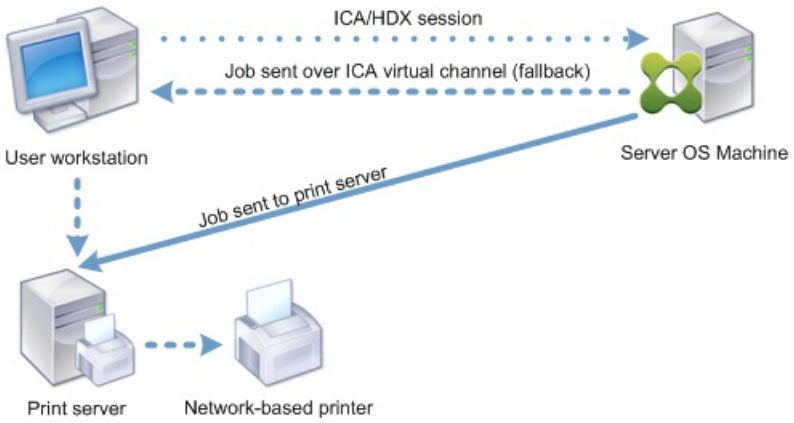
- Si le bureau virtuel ou l'application ne peuvent pas contacter le serveur d'impression.
- Si le pilote d'imprimante natif n'est pas disponible sur la machine avec OS de serveur.

Si le serveur d'impression universelle n'est pas activé, la configuration de la piste d'impression cliente pour l'impression réseau est utile pour les connexions à faible bande passante, telles que les réseaux étendus, qui peuvent bénéficier de l'optimisation et de la compression du trafic résultant en l'envoi de tâches via la connexion ICA.

La piste d'impression cliente vous permet également de limiter le trafic ou de restreindre la bande passante allouée aux

© 1999-2017 Citrix Systems, Inc. All rights reserved.

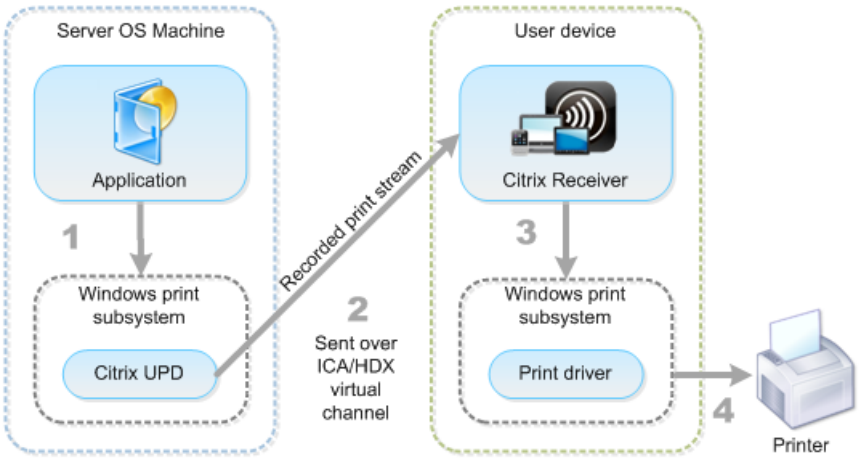
tâches d'impression. Si le routage de tâches via la machine utilisateur n'est pas possible, tel que pour les clients légers sans les fonctionnalités d'impression, la qualité de service doit être configurée pour favoriser le trafic ICA/HDX et assurer une bonne expérience de l'utilisateur dans les sessions.



Pour simplifier l'impression dans ces environnements, Citrix vous recommande d'utiliser le pilote d'impression universelle Citrix. Le pilote d'impression universelle est un pilote indépendante du périphérique qui prend en charge un périphérique d'impression, simplifiant ainsi l'administration en réduisant le nombre de pilotes requis.

Le pilote d'imprimante universelle Citrix XPS prend en charge les fonctionnalités d'impression avancées, telles que l'agrafage et la sélection de l'alimentation papier. Ces fonctionnalités sont disponibles si le pilote natif les rend disponibles à l'aide de la technologie d'impression de Microsoft. Le pilote natif doit utiliser les mots clés du schéma d'impression standard dans le fichier XML des fonctionnalités d'impression. Si des mots-clés non standard sont utilisés, les fonctionnalités d'impression avancées ne seront pas disponibles à l'aide du pilote d'imprimante universelle Citrix XPS.

L'illustration suivante affiche les composants du pilote d'impression universelle et un flux de travail typique pour une imprimante connectée localement sur un périphérique.



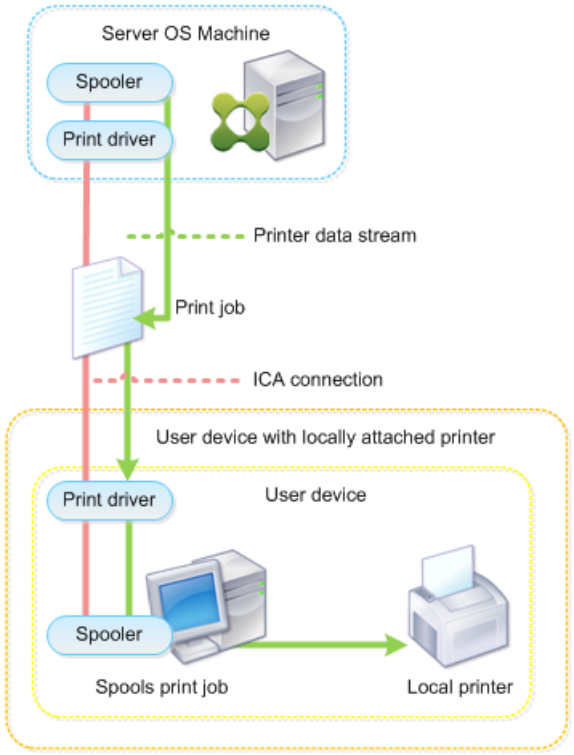
Lors de la planification de votre stratégie de gestion de pilote, déterminez si vous allez prendre en charge le pilote d'impression universelle, le pilote spécifique à la machine, ou les deux. Si vous prenez en charge les pilotes standards, vous devrez également déterminer :

Lors de la création automatique des imprimantes, si le système détecte une nouvelle imprimante locale connectée à une

© 1999-2017 Citrix Systems, Inc. All rights reserved.

machine utilisateur, il vérifie la présence du pilote d'imprimante requis sur la machine avec OS de serveur. Par défaut, si un pilote natif Windows n'est pas disponible, le système utilise le pilote d'impression universelle.

Le pilote d'imprimante de la machine avec OS de serveur et le pilote de la machine utilisateur doivent correspondre pour que l'impression réussisse. Le diagramme qui suit démontre comment le pilote d'imprimante est utilisé à deux endroits pour l'impression cliente.



- Les types de pilotes à prendre en charge.
- Indiquez si vous devez installer les pilotes d'imprimante automatiquement lorsqu'ils sont manquants sur les machines avec OS de serveur.
- Indiquer s'il faut créer des listes de compatibilité du pilote.

- Exemple de configuration de l'impression
- Recommandations, considérations en matière de sécurité et opérations par défaut
- Imprimer les stratégies et préférences
- Provisionner les imprimantes
- Gérer l'environnement d'impression

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Exemple de configuration de l'impression

Jul 07, 2016

Le choix d'options de configuration d'impression les plus appropriées à vos besoins et à l'environnement peut simplifier l'administration. Bien que la configuration d'impression par défaut permet aux utilisateurs d'imprimer dans la plupart des environnements, les valeurs par défaut peuvent ne pas fournir la meilleure expérience utilisateur attendue ou l'utilisation du réseau et de surcharge de gestion pour votre environnement.

Votre configuration d'impression dépend des facteurs suivants :

- Les besoins de votre entreprise et votre infrastructure d'impression existante.
  Concevez votre configuration d'impression selon les besoins de votre organisation. Votre implémentation d'impression existante (capacité des utilisateurs à ajouter des imprimantes, quels utilisateurs ont accès à quelles imprimantes, etc) peut être un guide utile lors de la définition de la configuration de l'impression.

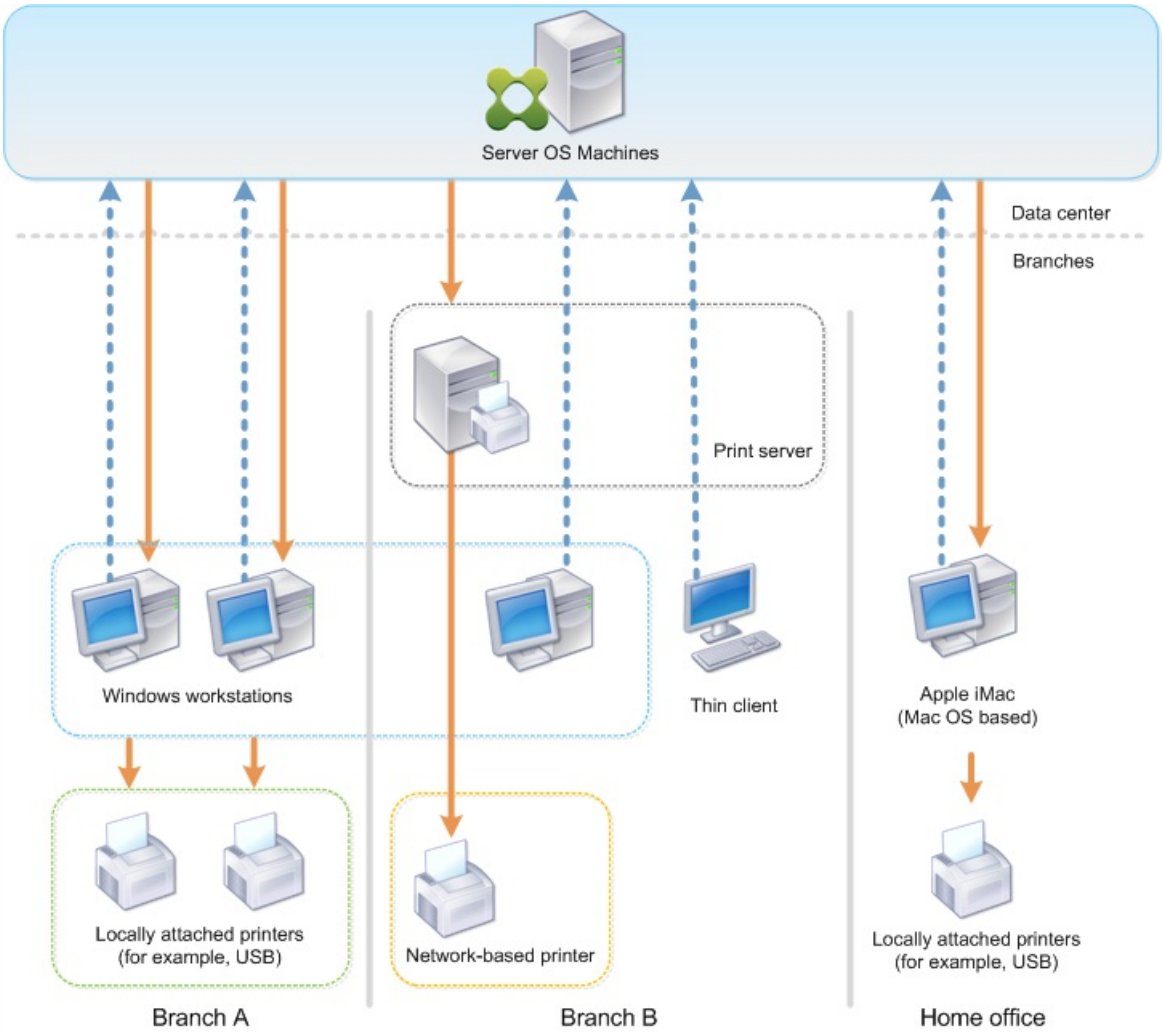
- Si votre entreprise possède des stratégies de sécurité qui réservent des imprimantes pour certains utilisateurs (par exemple, des imprimantes pour le département des ressources humaines ou finance).
- Si les utilisateurs doivent imprimer alors qu'ils sont éloignés de leur emplacement de travail principal ; par exemple, les travailleurs qui se déplacent entre stations de travail ou sont en voyage d'affaire.

Lors de la conception de votre configuration d'impression, essayez de fournir aux utilisateurs la même expérience en session qu'ils rencontrent lorsqu'ils impriment depuis leurs machines utilisateur locales.

L'illustration suivante affiche le déploiement pour ces cas d'utilisation :

- **Succursale A** : une petite succursale à l'étranger avec quelques stations de travail Windows. Chaque utilisateur station de travail possède une imprimante privée, connectée localement.
- **Succursale B** : une succursale importante avec des clients légers et des stations de travail Windows. Pour une meilleure efficacité, les utilisateurs de cette succursale partagent des imprimantes réseau (une par étage). Des serveurs d'impression Windows situés dans la succursale gèrent les files d'attente d'impression.
- **Bureau à domicile** : un bureau à domicile avec une machine utilisateur Mac OS qui accède à l'infrastructure Citrix de l'entreprise. La machine utilisateur dispose d'une imprimante connectée localement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Les sections suivantes décrivent les configurations qui réduisent la complexité de l'environnement et simplifient sa gestion.

Dans la succursale A, tous les utilisateurs travaillent sur des stations de travail Windows, par conséquent, les imprimantes clientes créées automatiquement et le pilote d'imprimante universelle sont utilisés. Ces technologies fournissent ces avantages :

- Performances : les tâches d'impression sont fournies via le canal ICA d'impression et les données d'impression peuvent être compressées pour économiser la bande passante.
  Pour vous assurer qu'un seul utilisateur imprimant un document important ne peut dégrader les performances de session des autres utilisateurs, une stratégie Citrix est configurée pour spécifier la bande passante d'impression maximale.

  Une autre solution consiste à tirer parti d'une connexion multi-stream ICA, dans laquelle le trafic d'impression est transféré vers une autre connexion TCP à basse priorité. Multi-stream ICA est une option lorsque la qualité de service (QoS) n'est pas implémentée sur la connexion de réseau étendu.

- Flexibilité : l'utilisation du pilote d'imprimante universelle Citrix assure que toutes les imprimantes connectées à un client peuvent également être utilisées à partir d'un bureau virtuel ou la session d'application sans intégrer un nouveau pilote d'imprimante dans le centre de données.

Dans la succursale B, toutes les imprimantes sont basées sur le réseau et leurs files d'attente sont gérées sur un serveur

© 1999-2017 Citrix Systems, Inc. All rights reserved.

d'impression Windows, et le Serveur d'impression universelle Citrix est ainsi le plus efficace de la configuration.

Tous les pilotes d'imprimante requis sont installés et gérés sur le serveur d'impression par les administrateurs locaux. Le mappage des imprimantes dans le bureau virtuel ou la session d'application fonctionne comme suit :

- Pour les stations de travail Windows : l'équipe informatique locale permet aux utilisateurs de connecter l'imprimante réseau à leurs stations de travail Windows. Cela permet aux utilisateurs d'imprimer à partir des applications installées localement.
  Lors d'une session application ou de bureau virtuel, les imprimantes de session configurées localement sont énumérées via la création automatique. Le bureau virtuel ou l'application se connectent au serveur d'impression en tant que connexion réseau directe si possible.

  Les composants du serveur d'impression universelle Citrix sont installés et activés, ainsi les pilotes d'imprimante natifs ne sont pas requis. Si un pilote est mis à jour ou une file d'attente d'imprimante est modifiée, aucune configuration supplémentaire n'est requise dans le centre de données.

- Pour les clients fins : pour les utilisateurs des clients légers, les imprimantes doivent être connectées au sein de la session de bureau virtuel ou d'application. Pour fournir aux utilisateurs l'expérience d'impression la plus simple, les administrateurs configurent une stratégie Citrix Imprimante de session unique par étage pour connecter une imprimante par étage en tant qu'imprimante par défaut.
  Pour vous assurer que l'imprimante appropriée est connectée, même si les utilisateurs itinèrent entre les étages, les stratégies sont filtrées en fonction du sous-réseau ou du nom du client léger. Cette configuration, appelée impression de proximité, permet la maintenance du pilote d'imprimante locale (en fonction du modèle d'administration déléguée).

  Si une file d'attente d'imprimante doit être modifiée ou ajoutée, les administrateurs Citrix doivent modifier la stratégie Imprimante de session correspondante au sein de l'environnement.

Étant donné que le trafic d'impression réseau sera envoyé en dehors du canal virtuel ICA, la qualité de service (QoS) est implémentée. Le trafic réseau entrant et sortant sur les ports utilisés par le trafic ICA/HDX sont prioritaires sur tous les autres trafics réseau. Cette configuration permet d'assurer que les sessions utilisateur ne sont pas affectées par les tâches d'impression importantes.

Pour les bureaux à domicile sur lesquels les utilisateurs travaillent sur des stations de travail non standard et utilisent des périphériques d'impression non gérés, l'approche la plus simple consiste à utiliser les imprimantes clientes créées automatiquement et le pilote d'imprimante universelle.

Dans le récapitulatif, l'exemple de déploiement est configuré comme suit :

- Aucun des pilotes d'imprimante n'est installé sur les machines avec OS de serveur. Seul le pilote d'imprimante universelle Citrix est utilisé. Le retour à l'impression native et l'installation automatique des pilotes d'imprimantes est désactivé.
- Une stratégie est configurée pour créer automatiquement toutes les imprimantes clientes pour tous les utilisateurs. Les machines avec OS de serveur se connecteront directement aux serveurs d'impression par défaut. La seule configuration requise est l'activation des composants du serveur d'impression universelle.
- Une stratégie d'imprimante de session est configurée pour chaque étage de la succursale B et appliquée à tous les clients légers de l'étage respectif.
- QoS est implémentée pour la succursale B afin d'assurer une excellente expérience utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Recommandations, considérations en matière de sécurité et opérations par défaut

Jul 07, 2016

De nombreux facteurs déterminent la meilleure solution d'impression pour un environnement particulier. Certaines de ces recommandations risquent de ne pas s'appliquer à votre site.

- Utilisez le Serveur d'impression universelle Citrix.
- Utilisez le pilote d'imprimante universelle ou les pilotes natifs Windows.
- Réduisez le nombre de pilotes d'imprimante installés sur les machines avec OS de serveur.
- Utilisez le mappage de pilote pour les pilotes natifs.
- Ne jamais installer de pilotes d'imprimante non testés sur un site de production.
- Évitez de la mise à jour de pilote. Essayez toujours de désinstaller un pilote, redémarrer le serveur d'impression, puis installer le pilote de remplacement.
- Désinstallez les pilotes non utilisées ou utilisez la stratégie Mappage et compatibilité du pilote d'imprimante pour empêcher la création d'imprimantes avec le pilote.
- Essayez d'éviter d'utiliser la version 2 des pilotes en mode noyau.
- Pour savoir si un modèle d'imprimante est pris en charge, contactez le fabricant ou consultez le guide du produit Citrix Ready sur www.citrix.com/ready.
  En général, les pilotes d'imprimante fourni par Microsoft sont testées avec les services Terminal Server et sont garantis de fonctionner avec Citrix. Toutefois, avant d'utiliser un pilote d'impression tiers, consultez votre fournisseur de pilote d'imprimante pour vous assurer que le pilote est certifié pour les services Terminal Server par le programme Windows Hardware Quality Labs (WHQL). Citrix ne certifie pas les pilotes d'imprimante.

Les solutions d'impression Citrix sont sécurisées dès leur conception.

- Le service du Gestionnaire d'impression Citrix surveille en permanence et répond aux événements de session, tels que l'ouverture et la fermeture de session, la déconnexion, la reconnexion et la terminaison d'une session. Il gère les demandes de service en imitant la session utilisateur courante.
- L'impression Citrix affecte un espace de noms unique à chaque imprimante dans une session.
- L'impression Citrix définit le descripteur de sécurité par défaut pour les imprimantes créées automatiquement pour vous assurer que les imprimantes clientes créées automatiquement dans une session ne sont pas accessibles aux utilisateurs exécutés dans d'autres sessions. Par défaut, les utilisateurs administratifs ne peuvent pas accidentellement d'imprimer vers une autre session d'imprimante cliente, même s'ils peuvent afficher et ajuster manuellement les permissions des imprimantes clientes.

Par défaut, si vous ne configurez aucune règle de stratégie, le comportement d'impression est le suivant :

- La fonctionnalité Serveur d'impression universelle est désactivée.
- Toutes les imprimantes configurées sur la machine utilisateur sont automatiquement créées au début de chaque session. Ce comportement est équivalent à la configuration du paramètre de stratégie Citrix Créer automatiquement les imprimantes clientes avec l'option Créer automatiquement toutes les imprimantes clientes.
- Le système route toutes les tâches d'impression mises en file d'attente sur les imprimantes connectées localement vers

© 1999-2017 Citrix Systems, Inc. All rights reserved.

les machines clientes en tant que tâches d'impression clientes (c'est-à-dire, via le canal ICA et au travers de la machine utilisateur).

- Le système route toutes les tâches d'impression mises en file d'attente vers les imprimantes réseau directement depuis les machines avec OS de serveur. Si le système ne peut pas router les tâches sur le réseau, il les routera au travers de la machine utilisateur sous la forme d'une tâche d'impression cliente redirigée.
  Ce comportement est équivalent à la désactivation du paramètre de stratégie Citrix Diriger les connexions vers les serveurs d'impression.

- Le système tente de stocker les propriétés d'impression, une combinaison des préférences d'impression de l'utilisateur et des paramètres d'impression spécifiques à la machine, sur la machine cliente. Si le client ne prend pas en charge cette opération, le système stocke les propriétés d'impression dans les profils utilisateur sur la machine avec OS de serveur.
  Ce comportement est équivalent à la configuration du paramètre de stratégie Citrix Rétention des propriétés de l'imprimante avec l'option Contenu dans le profil uniquement si non enregistré sur le client.

- Le système utilise la version de Windows du pilote d'imprimante si elle est disponible sur la machine avec OS de serveur. Si le pilote d'imprimante n'est pas disponible, le système tente d'installer le pilote à partir du système d'exploitation Windows. Si le pilote n'est pas disponible sous Windows, il utilise un pilote d'impression universelle Citrix.
  Ce comportement est équivalent à l'activation du paramètre de stratégie Citrix Installation automatique de pilotes d'imprimante fournis avec Windows et à la configuration du paramètre Impression universelle avec l'option Utiliser l'impression universelle uniquement si le pilote requis n'est pas disponible.

  L'activation de l'installation automatique de pilotes d'imprimante fournis avec Windows peut entraîner l'installation de nombreux pilotes d'imprimante natifs.

Remarque : si vous n'êtes pas sûr des paramètres par défaut de livraison pour l'impression, vous pouvez les afficher en créant une nouvelle stratégie et en définissant toutes les règles de stratégie d'impression sur Activé. L'option qui s'affiche est l'option par défaut.

Une fonctionnalité de journalisation permanente est disponible pour le serveur d'impression et le sous-système d'impression sur le VDA.

Pour regrouper les journaux au format ZIP pour l'envoi par e-mail, ou pour charger automatiquement les journaux vers Citrix Insight Services, utilisez l'applet de commande PowerShell **Start-TelemetryUpload**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Stratégies et préférences d'impression

Jul 07, 2016

Lorsque les utilisateurs accèdent aux imprimantes à partir des applications publiées, vous pouvez configurer des stratégies Citrix pour spécifier :

- comment les imprimantes sont approvisionnées (ou ajoutées aux sessions) ;
- comment les tâches sont routées ;
- comment les pilotes d'imprimante sont gérés.

Vous pouvez posséder plusieurs configurations d'impression pour différentes machines utilisateur, utilisateurs ou tout autre objet sur lequel les stratégies sont filtrées.

La plupart des fonctions d'impression sont configurées au travers des paramètres de stratégie d'impression Citrix. Les paramètres d'impression sont conformes au comportement de stratégie Citrix standard.

XenDesktop peut écrire les paramètres de l'imprimante dans l'objet d'imprimante à la fin de la session ou sur le périphérique d'impression cliente, étant donné que le compte réseau de l'utilisateur possède les permissions suffisantes. Par défaut, Citrix Receiver utilise les paramètres stockés dans l'objet d'imprimante de la session, avant de rechercher dans d'autres emplacements les paramètres et préférences.

Par défaut, le magasin store, ou conserve, des propriétés d'imprimante sur la machine utilisateur (si elle est prise en charge par la machine) ou dans le profil utilisateur de la machine avec OS de serveur. Lorsqu'un utilisateur modifie les propriétés de l'imprimante au cours d'une session, ces modifications sont mises à jour dans le profil de l'utilisateur sur la machine. La prochaine fois que l'utilisateur ouvre une session ou se reconnecte, la machine utilisateur hérite de ces paramètres conservés. En d'autres termes, les modifications apportées aux propriétés de l'imprimante sur la machine utilisateur n'affectent pas la session courante tant que l'utilisateur n'a pas fermé puis rouvert une session.

Dans les environnements d'impression Windows, les modifications apportées aux préférences d'impression peuvent être stockées sur l'ordinateur local ou dans un document. Dans cet environnement, lorsque les utilisateurs modifient leurs paramètres d'impression, ils peuvent être stockés aux emplacements suivants :

- **Sur la machine utilisateur elle-même** : les utilisateurs Windows peuvent modifier les paramètres d'un périphérique sur la machine utilisateur en cliquant avec le bouton droit de la souris sur l'imprimante dans le Panneau de configuration, en sélectionnant Préférences d'impression. Par exemple, si Paysage est sélectionné en tant qu'orientation de page de l'imprimante, paysage est désormais enregistré en tant que préférence d'orientation de page par défaut pour cette imprimante.
- **Dans un document** : dans les programmes de traitement de texte et de publication assistée par ordinateur, les paramètres du document, tels que l'orientation de page, sont souvent stockés à l'intérieur des documents. Par exemple, une fois un document placé dans la file d'attente d'un document, Microsoft Word stocke généralement les préférences d'impression spécifiées, telles que l'orientation de page, et le nom de l'imprimante dans le document. Ces paramètres s'affichent par défaut la prochaine fois que vous imprimez ce document.
- **À partir des modifications effectuées par un utilisateur lors d'une session** : le système conserve uniquement les modifications apportées aux paramètres d'impression d'une imprimante créée automatiquement si la modification a été apportée dans le Panneau de configuration dans la session ; c'est-à-dire, sur la machine avec OS de serveur.
- **Sur la machine avec OS de serveur** : ce sont les paramètres par défaut associés à un pilote d'imprimante spécifique sur la machine.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Les paramètres préservés dans tout environnement Windows varient selon l'emplacement dans lequel l'utilisateur a effectué les modifications. Ceci signifie également que les paramètres d'impression qui s'affichent à un endroit, tel qu'un tableur, peuvent être différents de ceux qui s'affichent à d'autres endroits, tels que des documents. Ainsi, les paramètres d'impression appliqués à une imprimante spécifique peuvent changer dans une session.

Les préférences d'impression pouvant être stockées à plusieurs endroits, le système les traite selon une priorité spécifique. Il est également important de noter que les paramètres de la machine sont traités différemment des paramètres du document (et ont habituellement priorité sur ces derniers).

Par défaut, le système applique toujours tout paramètre d'impression modifié par un utilisateur lors d'une session, c'est-à-dire, les paramètres conservés, avant de considérer tout autre paramètre. Lorsque l'utilisateur effectue l'impression, le système fusionne et applique les paramètres de l'imprimante par défaut stockés sur la machine avec OS de serveur avec tout paramètre d'imprimante cliente ou conservé.

Citrix vous recommande de ne pas modifier l'emplacement de stockage des propriétés de l'imprimante. Le paramètre par défaut, qui enregistre les propriétés de l'imprimante sur la machine cliente, est la manière la plus facile d'assurer des propriétés d'impression cohérentes. Si le système n'a pas pu enregistrer les propriétés sur la machine utilisateur, il retourne automatiquement au profil utilisateur sur la machine avec OS de serveur.

Vérifiez le paramètre de stratégie Conservation des propriétés d'imprimante si ces scénarios s’appliquent :

- Si vous utilisez des plug-ins d'ancienne génération qui n'autorisent pas les utilisateurs à stocker des propriétés d'imprimante sur une machine utilisateur.
- Si vous utilisez des profils obligatoires sur votre réseau Windows et que vous souhaitez conserver les propriétés d'imprimante de l'utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Provisionner les imprimantes

Jul 15, 2016

Il existe trois méthodes de provisioning de l'imprimante :

- Serveur d'impression universelle Citrix
- Imprimantes clientes créées automatiquement
- Imprimantes de session affectées à l'administrateur

Lorsque vous déterminez la meilleure solution d'impression pour votre environnement, tenez compte de ce qui suit :

- Le serveur d'impression universelle fournit des fonctionnalités ne sont pas disponibles pour le fournisseur d'impression Windows : la mise en cache des images et des polices, la compression avancée, l'optimisation et la prise en charge de la qualité de service (QoS).
- Le pilote d'impression universelle prend en charge les paramètres indépendants de machine publics définis par Microsoft. Si les utilisateurs ont besoin d'accéder à des paramètres qui sont spécifiques au fabricant d'un pilote d'impression, le Serveur d'impression universelle associé à un pilote natif Windows peut être la meilleure solution. Avec cette configuration, vous conservez les avantages du Serveur d'impression universelle tout en offrant aux utilisateurs l'accès aux fonctionnalités d'impression spécialisées. Un compromis à prendre en compte est que les pilotes natifs Windows nécessitent une certaine maintenance.
- Le serveur d'imprimante universel Citrix fournit une prise en charge de l'impression universelle pour les imprimantes réseau. Le serveur d'impression universelle utilise le pilote d'impression universelle, un seul pilote sur la machine avec OS de serveur qui permet l'impression locale ou réseau à partir de n'importe quel périphérique, y compris des clients légers et des tablettes.

Pour utiliser le Serveur d'impression universelle avec un pilote natif Windows, activez le serveur d'impression universelle. Par défaut, si le pilote natif Windows est disponible, il est utilisé. Sinon, le pilote d'impression universelle est utilisé. Pour spécifier les modifications apportées à ce comportement, par exemple pour utiliser uniquement les pilotes natifs Windows ou le pilote d'impression universelle, mettez à jour le paramètre de stratégie Utilisation du pilote d'impression universelle.

Installer le serveur d'impression universelle

Pour utiliser le serveur d'impression universelle, installez le composant UpsServer sur vos serveurs d'impression, comme décrit dans les documents d'installation et configurez-le. Pour de plus amples informations, consultez les sections Installer à l'aide de l'interface graphique et Installer à l'aide de la ligne de commande.

Dans les environnements dans lesquels vous voulez déployer le composant UPClient séparément, par exemple avec **XenApp 6.5** :

1. Téléchargez le package autonome XenApp et XenDesktop Virtual Delivery Agent (VDA) pour OS de bureau ou de serveur Windows.
2. Extrayez le VDA à l'aide des instructions de ligne de commande décrites dans la section Utiliser le programme d'installation VDA autonome.
3. Installez les composants requis depuis \Image-Full\Support\VcRedist_2013_RTM
   - Vcredist_x64 / vcredist_x86
     - Exécutez x86 pour 32 bits uniquement, et les deux packages pour les déploiements 64 bits
4. Installez le composant requis cdf depuis \Image-Full\x64\Virtual Desktop Components ou \Image-Full\x86\Virtual

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Desktop Components.
- Cdf_x64 / Cdf_x86
  - x86 pour 32 bits, x64 pour 64 bits

5. Localisez le composant UPClient dans \Image-Full\x64\Virtual Desktop Components ou \Image-Full\x86\Virtual Desktop Components.
6. Installez le composant UPClient en extrayant et en lançant le MSI du composant.
7. Un redémarrage est nécessaire après l'installation du composant UPClient.

Refuser de prendre part au programme CEIP pour le serveur d'impression universelle

Vous êtes automatiquement inscrit au Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) lorsque vous installez le serveur d'impression universelle. Le premier chargement de données s'effectue sept jours après la date et heure d'installation.

Pour ne plus participer au programme CEIP, modifiez la clé de registre **HKLM\Software\Citrix\Universal Print Server\CEIPEnabled** et définissez la valeur **DWORD** sur **0**.

Pour participer à nouveau, définissez la valeur DWORD sur 1.

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

Pour de plus amples informations, consultez Citrix Insight Services.

Configurer le serveur d'impression universelle

Utilisez les paramètres de stratégie Citrix suivants pour configurer le serveur d'impression universelle. Pour plus d'informations, reportez-vous à l'aide des paramètres de stratégie à l'écran.

- **Activer le serveur d'impression universelle**. Le serveur d'impression universelle est désactivé par défaut. Lorsque vous activez le serveur d'impression universelle, vous pouvez choisir d'utiliser le fournisseur d'impression Windows si le serveur d'impression universelle n'est pas disponible. Après avoir installé le serveur d'impression universelle, un utilisateur peut ajouter et énumérer des imprimantes réseau au travers des interfaces du fournisseur d'impression Windows et du fournisseur Citrix.
- **Port (CGP) du flux de données d'impression du serveur d'impression universelle**. Spécifie le numéro de port TCP utilisé par l'écouteur CGP (Common Gateway Protocol) du flux de données d'impression Serveur d'impression universelle. La valeur par défaut est **7229**.
- **Port (HTTP/SOAP) du service Web du serveur d'impression universelle**. Spécifie le numéro de port TCP utilisé par l'écouteur Serveur d'impression universelle pour les requêtes HTTP/SOAP entrantes. La valeur par défaut est **8080**.

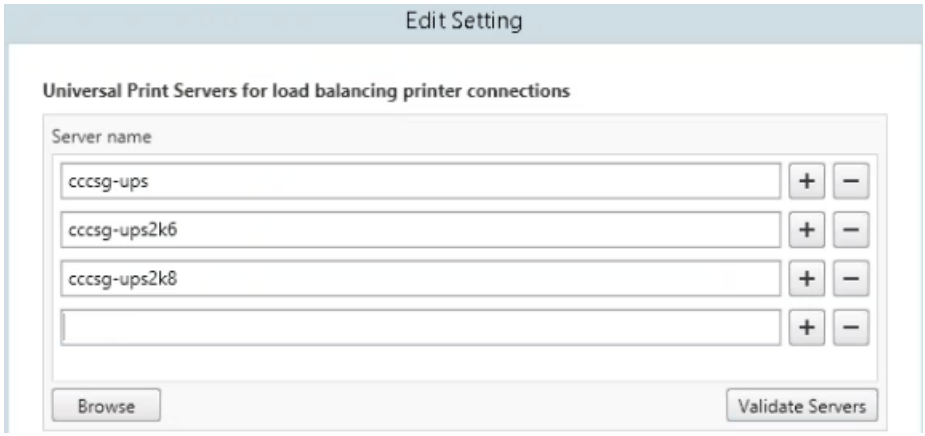
Pour modifier le port par défaut HTTP 8080 pour les communications du serveur d'impression universelle vers des VDA XenApp et XenDesktop, le registre suivant doit également être créé et la valeur du numéro de port doit être modifiée sur l'ordinateur du serveur d'impression universelle :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies
"UpsHttpPort"=DWORD:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ce numéro de port doit correspondre à la stratégie HDX, le port du service Web du serveur d'impression universelle (HTTP/SOAP), dans Studio.

- **Limite de bande passante d'entrée du flux d'impression du serveur d'impression universelle (kpbs)**. Spécifie la limite supérieure (en kilobits par seconde) pour le transfert des données d'impression délivrées depuis chaque tâche d'impression vers le Serveur d'impression universelle à l'aide de CGP. La valeur par défaut est 0 (illimitée).
- **Serveurs d'impression universelle d'équilibrage de la charge**. Ce paramètre dresse la liste des serveurs d'impression universelle à utiliser pour répartir la charge des connexions aux imprimantes établies lors du lancement de la session, après l'évaluation d'autres paramètres de stratégie d'impression Citrix. Pour optimiser la durée de création des imprimantes, Citrix recommande que les mêmes imprimantes partagées soient installées sur tous les serveurs d'impression. Cliquez sur **Valider les serveurs** pour vérifier que chaque serveur est un serveur d'impression et que tous les serveurs possèdent un ensemble identique d'imprimantes partagées. Cette opération peut prendre un certain temps.



- **Seuil au-delà duquel les serveurs d'impression universelle sont hors service**. Indique la durée pendant laquelle l'équilibrage de charge attend le rétablissement de la connexion à un serveur d'impression universelle avant de considérer que le serveur est hors connexion et de répartir sa charge sur d'autres serveurs d'impression disponibles. Le délai par défaut est de 180 secondes.

Une fois les stratégies d'impression modifiées sur le Delivery Controller, l'application des modifications de stratégie aux VDA peut prendre quelques minutes. Pour de plus amples informations consultez la section Paramètres de stratégie Serveur d'impression universelle.

Interactions avec d'autres paramètres de stratégie : le serveur d'impression universelle respecte les autres paramètres de stratégie d'impression Citrix et interagit avec eux comme indiqué dans le tableau suivant. Les informations fournies supposent que si le paramètre de stratégie Serveur d'impression universelle est activé, les composants Serveur d'impression universelle sont installés, et les paramètres de stratégie sont appliqués.

Paramètre de stratégie	Interaction
Redirection d'imprimante cliente, Créer automatiquement les imprimantes clientes	Si le Serveur d'impression réseau est activé, les imprimantes réseau clientes peuvent être créées à l'aide du pilote d'imprimante universelle, au lieu des pilotes natifs. Les utilisateurs aperçoivent le même nom d'imprimante qu'avant.
Imprimantes de session	Lors de l'utilisation de la solution du serveur d'impression universelle

© 1999-2017 Citrix Systems, Inc. All rights reserved.

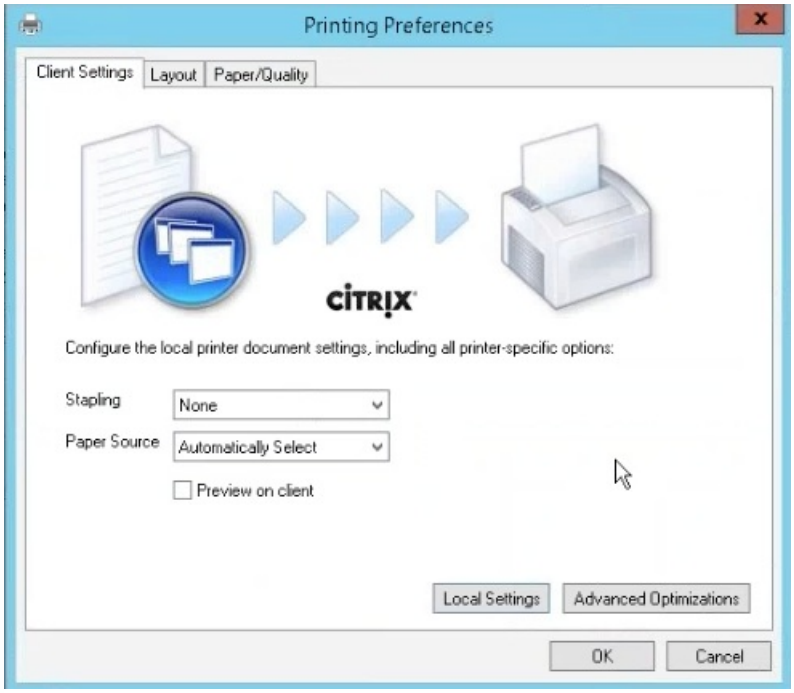
	Citrix, les paramètres de stratégie du pilote d'imprimante universelle sont appliqués.
Connexions directes au serveur d'impression	Lorsque le serveur d'impression réseau est activé et que le paramètre de stratégie d'utilisation des pilotes d'imprimante universelle est configuré pour utiliser l'impression universelle uniquement, une imprimante réseau directe peut être créée sur le serveur d'impression, à l'aide du pilote d'impression universelle.
Préférence UPD	Prend en charge les pilotes EMF et XPS.

Effets sur les interfaces utilisateur : le pilote d'impression universelle Citrix utilisé par le serveur d'impression universelle désactive les contrôles d'interface utilisateur suivants :

- dans la boîte de dialogue Propriétés d'imprimante, le bouton Paramètres d'imprimante local ;
- dans la boîte de dialogue Propriétés du document, les boutons Paramètres d'imprimante locale et Aperçu sur le client.

Le pilote d'imprimante universelle Citrix XPS prend en charge les fonctionnalités d'impression avancées, telles que l'agrafage et la source papier. L'utilisateur peut sélectionner les options Agrafage ou Alimentation papier dans la boîte de dialogue d'impression UDP personnalisée si le client ou les imprimantes réseau qui sont mappés sur le pilote d'imprimante universelle (UDP) dans la session prennent en charge ces fonctionnalités.

Ces fonctionnalités sont disponibles si le pilote natif les rend disponibles à l'aide de la technologie d'impression de Microsoft. Le pilote natif doit utiliser les mots clés du schéma d'impression standard dans le fichier XML des fonctionnalités d'impression. Si des mots-clés non standard sont utilisés, les fonctionnalités d'impression avancées ne seront pas disponibles à l'aide du pilote d'imprimante universelle Citrix XPS.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Lors de l'utilisation du serveur d'impression universelle, l'assistant d'ajout d'imprimante du fournisseur d'impression Citrix est le même que l'assistant d'ajout d'imprimante du fournisseur d'impression Windows, avec les exceptions suivantes :

- Lors de l'ajout d'une imprimante par nom ou adresse, vous pouvez fournir un numéro de port HTTP/SOAP pour le serveur d'impression. Ce numéro de port devient une partie du nom d'imprimante et apparaît dans les affichages.
- Si le paramètre de stratégie d'utilisation du pilote d'impression universelle Citrix spécifie que l'impression universelle doit être utilisée, le nom du pilote d'imprimante universelle s'affiche lors de la sélection d'une imprimante. Le fournisseur d'impression Windows ne peut utiliser le pilote d'impression universelle.

Le fournisseur d'impression Citrix ne prend pas en charge la restitution côté client.

Pour de plus amples informations sur le serveur d'impression universelle, consultez l'article CTX200328.

Ces solutions d'impression universelle sont fournies pour les imprimantes clientes :

- **Imprimante universelle Citrix** : une imprimante générique créée au début des sessions qui n'est associée à aucun périphérique d'impression. L'imprimante universelle Citrix n'est pas requise pour énumérer les imprimantes clientes disponibles lors de l'ouverture de session, ce qui permet de réduire considérablement l'utilisation des ressources et de diminuer les durées d'ouverture de session de l'utilisateur. L'imprimante universelle peut imprimer sur n'importe quel périphérique d'impression côté client.
  L'imprimante universelle Citrix peut ne pas fonctionner pour toutes les machines utilisateur ou Citrix Receiver de votre environnement. L'imprimante universelle Citrix requiert un environnement Windows et ne prend pas en charge Citrix Offline Plug-in ou les applications livrées en streaming vers le client. Utilisez les imprimantes clientes créées automatiquement et le pilote d'impression universelle pour de tels environnements.

  Si vous souhaitez utiliser une solution d'impression universelle pour Citrix Receivers non Windows, utilisez l'un des autres pilotes d'impression universelle, qui sont basés sur postscript/PCL et sont automatiquement installés.

- **Pilotes d'impression universelle Citrix :** un pilote d'imprimante indépendant du périphérique. Si vous configurez un pilote d'impression universelle Citrix, le système utilise un pilote d'impression EMF par défaut.
  Le pilote d'impression universelle Citrix peut alors créer des tâches d'impression plus petites à l'inverse des pilotes d'imprimante plus anciens ou moins avancés. Toutefois, un pilote spécifique à la machine peut être nécessaire pour optimiser les tâches d'impression pour une imprimante spécialisée.

Configurer l'impression universelle : utilisez les paramètres de stratégie Citrix suivants pour configurer l'impression universelle. Pour plus d'informations, reportez-vous à l'aide des paramètres de stratégie à l'écran.

- Utilisation du pilote d'impression universelle Indique quand utiliser l'impression universelle.
- Créer automatiquement l'imprimante universelle générique. Active ou désactive la création automatique de l'objet d'imprimante universelle Citrix générique pour les sessions lorsqu'une machine utilisateur compatible avec l'impression universelle est en cours d'utilisation. Par défaut, l'objet Imprimante universelle générique n'est pas créé automatiquement.
- Préférence de pilote universel Spécifie l'ordre dans lequel le système tente d'utiliser les pilotes d'impression universelle, en commençant par la première entrée de la liste. Vous pouvez ajouter, modifier ou supprimer des pilotes et changer leur ordre dans la liste.
- Préférence d'aperçu d'impression universelle. Spécifie s'il convient d'utiliser la fonction d'aperçu d'impression pour les imprimantes universelles génériques ou créées automatiquement.
- Mode de traitement EMF de l'impression universelle. Contrôle la méthode de traitement du fichier de spoul EMF sur la machine utilisateur Windows. Par défaut, les enregistrements EMF sont spoulés directement sur l'imprimante. Le spoulage directement vers l'imprimante permet au spouleur de traiter les enregistrements plus rapidement et utiliser

© 1999-2017 Citrix Systems, Inc. All rights reserved.

moins de ressources d'UC.

Vous trouverez des stratégies supplémentaires dans la section Optimiser les performances d'impression. Pour modifier les valeurs par défaut des paramètres tels que la taille du papier, la qualité du papier, la couleur, l'impression recto verso et le nombre de copies, consultez l'article CTX113148.

Créer automatiquement des imprimantes depuis la machine de l'utilisateur : au début de la session, le système crée automatiquement toutes les imprimantes sur la machine utilisateur par défaut. Vous pouvez contrôler quels types, le cas échéant, d'imprimantes sont provisionnés auprès des utilisateurs et empêchent la création automatique.

Utilisez le paramètre de stratégie Citrix Créer automatiquement les imprimantes clientes pour contrôler la création automatique. Vous pouvez spécifier l'un des éléments suivants :

- toutes les imprimantes visibles pour la machine cliente, y compris les imprimantes connectées localement et les imprimantes réseau, sont créées automatiquement au début de chaque session (valeur par défaut) ;
- toutes les imprimantes locales connectées physiquement à la machine cliente sont créées automatiquement ;
- seule l'imprimante par défaut de la machine cliente est créée automatiquement.
- La création automatique est désactivée pour toutes les imprimantes clientes

Le paramètre Créer automatiquement les imprimantes clientes nécessite que le paramètre Redirection d'imprimante cliente soit Autorisé (valeur par défaut).

Par défaut, les imprimantes réseau de la machine cliente sont créées automatiquement au début des sessions. Le système vous permet de réduire le nombre d'imprimantes réseau énumérées et mappées en spécifiant les imprimantes réseau à créer dans chaque session. Certaines de ces imprimantes sont appelées Imprimantes de session.

Vous pouvez filtrer des stratégies d'imprimante de session par adresse IP pour offrir l'impression de proximité. L'impression de proximité permet aux utilisateurs se trouvant dans une plage d'adresses IP spécifiée d'accéder automatiquement aux périphériques d'impression réseau existant dans la même plage. L'impression de proximité est fournie par le Serveur d'impression universelle Citrix et ne nécessite pas la configuration décrite dans cette section.

L'impression de proximité peut impliquer le scénario suivant :

- Le réseau d'entreprise interne fonctionne avec un serveur DHCP qui attribue automatiquement les adresses IP aux utilisateurs.
- Tous les services d'une entreprise possèdent des plages d'adresses IP désignées uniques.
- Des imprimantes réseau existent dans la plage d'adresses IP de chaque service.

Lorsque l'impression de proximité est configurée et un employé voyage d'un service à un autre, aucune autre configuration du périphérique d'impression n'est requise. Lorsque la machine utilisateur est reconnue dans la plage d'adresse IP du nouveau service, elle a accès à toutes les imprimantes réseau de cette plage.

Configurer des imprimantes spécifiques devant être redirigées dans les sessions : pour créer des imprimantes attribuées à l'administrateur, configurez le paramètre de stratégie Citrix Imprimantes de session. Ajoutez une imprimante réseau à cette stratégie à l'aide de l'une des méthodes suivantes :

- Entrez le chemin UNC de l'imprimante au format \\nomserveur\nomimprimante.
- Rechercher un emplacement d'imprimante sur le réseau.
- Recherchez des imprimantes sur un serveur spécifique. Entrez le nom du serveur selon le format \\nomserveur et cliquez sur Parcourir.

Important : le serveur fusionne tous les paramètres d'imprimantes de session activés de toutes les stratégies appliquées en

© 1999-2017 Citrix Systems, Inc. All rights reserved.

commençant par celles dont la priorité est la plus élevée. Lorsqu'une imprimante est configurée dans plusieurs objets de stratégie, les paramètres personnalisés par défaut ne sont utilisés qu'à partir de l'objet de stratégie ayant la plus haute priorité dans laquelle cette imprimante est configurée.
Les imprimantes réseau créées à l'aide du paramètre Imprimantes de session peuvent varier selon les conditions dans lesquelles la session a été initiée, en appliquant un filtre sur les objets comme les sous-réseaux.

Spécifiez une imprimante réseau par défaut pour une session : par défaut, l'imprimante principale de l'utilisateur est utilisée comme imprimante par défaut pour la session. Utilisez le paramètre de stratégie Citrix Imprimante par défaut pour changer la façon dont l'imprimante par défaut sur la machine utilisateur est établie dans une session.

1. Sur la page de paramètres Imprimante par défaut, sélectionnez un paramètre pour Choisir l'imprimante par défaut du client :
   - Nom d'imprimante réseau. Les imprimantes ajoutées avec le paramètre de stratégie Imprimantes de session s'affichent dans ce menu. Sélectionnez l'imprimante réseau à utiliser comme valeur par défaut de cette stratégie.
   - Ne pas ajuster l'imprimante par défaut de l'utilisateur. Utilise le réglage du profil utilisateur courant pour l'imprimante par défaut. Pour plus d'informations, reportez-vous à l'aide des paramètres de stratégie à l'écran.
2. Appliquez la stratégie au groupe d'utilisateurs (ou autres objets filtrés) que vous souhaitez attribuer.

Configurer l'impression de proximité : l'impression de proximité est également fournie par le Serveur d'impression universelle Citrix, qui ne nécessite pas la configuration décrite ici.

1. Créez une stratégie distincte pour chaque sous-réseau (ou pour correspondre à l'emplacement de l'imprimante).
2. Dans chacune de ces stratégies, ajoutez les imprimantes de l'emplacement géographique de ce sous-réseau au paramètre Imprimantes de session.
3. Attribuez au paramètre Imprimante par défaut la valeur Ne pas ajuster l'imprimante par défaut de l'utilisateur.
4. Filtrez les stratégies par adresse IP cliente. Veillez à mettre à jour ces stratégies pour refléter les modifications apportées aux plages d'adresses IP DHCP.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Gérer l'environnement d'impression

Jul 07, 2016

La gestion de votre environnement d'impression comprend :

- Gestion des pilotes d'imprimante
- Optimisation des performances d'impression
- Affichage de l'imprimante et gestion des files d'attente d'impression

Pour réduire les coûts administratifs et les éventuels problèmes de pilote d'impression, Citrix vous recommande d'utiliser le pilote d'imprimante universelle Citrix.

Si la création automatique échoue, par défaut, le système installe un pilote d'imprimante natif Windows fourni avec Windows. Si un pilote n'est pas disponible, le système retourne au pilote d'impression universelle. Pour de plus amples informations sur les valeurs par défaut du pilote d'imprimante, veuillez consulter la section Recommandations, considérations en matière de sécurité et opérations par défaut.

Si le pilote d'impression universelle Citrix n'est pas une option pour tous les scénarios, mappez les pilotes d'imprimante pour réduire la quantité de pilotes installés sur les machines avec OS de serveur. En outre, le mappage des pilotes d'imprimante vous permet de :

- autoriser les imprimantes spécifiques à utiliser uniquement les pilotes d'impression universelle Citrix ;
- autoriser ou empêcher la création d'imprimantes avec un pilote spécifique ;
- remplacer les pilotes d'imprimante appropriés par des pilotes altérés ou périmés ;
- remplacer un pilote disponible sur le serveur Windows par un nom de pilote client.

Empêcher l'installation automatique des pilotes d'imprimante : l'installation automatique de pilotes d'impression doit être désactivée pour assurer la cohérence entre les machines avec OS de serveur. Cela peut être assuré au travers des stratégies Citrix, Microsoft ou les deux. Pour empêcher l'installation automatique des pilotes d'imprimante natifs Windows, désactivez le paramètre de stratégie Citrix Installation automatique de pilotes d'imprimante fournis avec Windows.

Mappage des pilotes d'imprimante des clients : chaque client fournit des informations sur les imprimantes côté client au cours de l'ouverture de session, notamment le nom du pilote d'imprimante. Lors de la création automatique de l'imprimante client, le nom des pilotes d'imprimantes des serveurs Windows sont sélectionnés de manière à correspondre aux noms des modèles d'imprimante fournis par le client. Le processus de création automatique utilise ensuite les pilotes d'imprimantes identifiés et disponibles de manière à créer les files d'impression des clients redirigés.

Le processus général de définition des règles de remplacement de pilotes et de modification des paramètres d'impression pour les pilotes d'imprimantes clientes mappées est le suivant .

1. Pour spécifier les règles de remplacement des pilotes pour les imprimantes clientes créées automatiquement, configurez le paramètre de stratégie Citrix Mappage et compatibilité du pilote d'imprimante en ajoutant le nom du pilote d'imprimante cliente et en sélectionnant le pilote de serveur à utiliser à la place du pilote d'imprimante cliente dans le menu Rechercher un pilote d'imprimante. Vous pouvez utiliser des caractères génériques dans ce paramètre. Par exemple, pour obliger toutes les imprimantes HP à utiliser un pilote spécifique, spécifiez HP* dans le paramètre de stratégie.
2. Pour interdire un pilote d'imprimante, sélectionnez le nom de pilote et choisissez le paramètre Ne pas créer.
3. Le cas échéant, vous pouvez modifier un mappage existant, supprimer un mappage ou modifier l'ordre des entrées de pilote dans la liste.
4. Pour modifier les paramètres d'impression pour les pilotes d'imprimantes clientes mappées, sélectionnez le pilote

© 1999-2017 Citrix Systems, Inc. All rights reserved.

d'imprimante, cliquez sur Paramètres, puis spécifiez les paramètres tels que la qualité d'impression, l'orientation et la couleur. Si vous spécifiez une option d'impression que le pilote d'imprimante ne prend pas en charge, cette option n'a aucun effet. Ce paramètre écrase les paramètres d'imprimante définis par l'utilisateur durant une session précédente.

5. Citrix vous recommande de tester le comportement des imprimantes en détail après le mappage des pilotes, car certaines fonctionnalités d'imprimante peuvent être disponibles uniquement avec un pilote spécifique.

Lorsque les utilisateurs ouvrent une session, le système vérifie la liste de compatibilité des pilotes d'imprimantes clients avant de configurer les imprimantes clientes.

Pour optimiser les performances d'impression, utilisez le Serveur d'impression universelle et un pilote d'impression universelle. Les stratégies suivantes contrôlent l'optimisation et la compression de l'impression :

- Valeurs par défaut de l'optimisation de l'impression universelle. Spécifie les valeurs par défaut de l'imprimante universelle lorsqu'elle est créée pour une session :
  - Qualité d'image souhaitée spécifie la limite de compression d'image par défaut appliquée à l'impression universelle. Par défaut, Qualité standard est activée, signifiant que les utilisateurs peuvent uniquement imprimer des images à l'aide des compressions standard ou de qualité réduite.
  - Activer la compression lourde active ou désactive la réduction de la bande passante au-delà du niveau de compression défini par l'option Qualité d'image souhaitée, sans perte de qualité d'image. Par défaut, la compression intensive est désactivée.
  - Les paramètres Cache d'image et de police spécifient si oui ou non vous pouvez cacher des images et des polices qui s'affichent plusieurs fois dans le flux d'impression, assurant ainsi que chaque image ou police est envoyée à l'imprimante une seule fois. Par défaut, les images incorporées et les polices sont mises en cache.
  - Autoriser les non-administrateurs à modifier ces paramètres spécifie si les utilisateurs peuvent ou non modifier les paramètres d'optimisation d'impression dans une session. Par défaut, les utilisateurs ne sont pas autorisés à modifier les paramètres par défaut d'optimisation de l'impression.
- Limite de compression d'image de l'impression universelle. Définit la qualité maximale et le niveau de compression minimal disponibles pour les images imprimées avec le pilote d'imprimante universelle. Par défaut, la limite de compression d'image est définie sur Qualité optimale (compression sans perte).
- Limite de qualité d'impression de l'impression universelle. Spécifie le nombre maximal de points par pouce (dpi) disponible pour l'impression dans la session. Par défaut, aucune limite n'est spécifiée.

Par défaut, toutes les tâches d'impression sont destinées à la route d'imprimantes réseau à partir de la machine avec OS de serveur, au travers du réseau, et directement vers le serveur d'impression. Envisagez le routage des tâches d'impression via la connexion ICA si le réseau possède une certaine latence ou une bande passante limitée. Pour ce faire, désactivez le paramètre de stratégie Citrix Connexions directes aux serveurs d'impression. Les données envoyées aux clients via la connexion ICA sont compressées. Les transmissions de données sur le réseau étendu nécessitent donc moins de bande passante.

Améliorer les performances de session en limitant la bande passante d'impression : lors de l'impression de fichiers depuis des machines avec OS de serveur vers les imprimantes utilisateur, il se peut que d'autres canaux virtuels (vidéo, par exemple) peuvent rencontrer une baisse des performances en raison de compétition de la bande passante, spécialement si les utilisateurs accèdent à des serveurs via des réseaux lents. Pour empêcher ce type de dégradation, vous pouvez limiter la bande passante utilisée par l'impression cliente. En limitant la vitesse de transfert des données d'impression, vous pouvez augmenter la bande passante disponible dans le flux de données HDX pour le transfert des données vidéo et des informations relatives aux frappes clavier et aux clics de souris.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Important : si une limite de bande passante d'impression est définie, elle est respectée même lorsqu'aucun autre canal n'est utilisé.
Utilisez les paramètres d'imprimante de la stratégie Citrix Bande passante pour configurer les limites de session de bande passante d'impression. Pour définir les limites pour le site, réalisez cette tâche à l'aide de Studio. Pour définir les limites pour des serveurs individuels, effectuez cette tâche à l'aide de la console de gestion des stratégies de groupe dans Windows localement sur chaque machine avec OS de serveur.

- Le paramètre Limite de bande passante de redirection d'imprimante permet de spécifier la bande passante en kilobits par seconde (kbps) disponible pour l'impression.
- Le paramètre Pourcentage de limite de bande passante de redirection de l'imprimante permet de limiter la bande passante disponible pour l'impression à un pourcentage de la bande passante générale disponible.
  Remarque : pour spécifier la bande passante sous forme de pourcentage à l'aide du paramètre Pourcentage de limite de bande passante de redirection de l'imprimante, activez également le paramètre Limite de bande passante de session générale.
  Si vous entrez des valeurs pour les deux paramètres, le paramètre le plus restrictif (ayant la valeur la plus faible) est appliqué.

Pour obtenir des informations en temps réel sur la bande passante d'impression, utilisez Citrix Director.

La solution de serveur d'impression universelle peut monter en charge en ajoutant davantage de serveurs d'impression dans la solution d'équilibrage de charge. Il n'existe aucun point de défaillance unique car chaque VDA dispose de son propre équilibreur de charge pour répartir la charge d'impression auprès de tous les serveurs d'impression.

Utilisez les paramètres de stratégie, Serveurs d'impression universelle d'équilibrage de la charge et Seuil au-delà duquel les serveurs d'impression universelle sont hors service, pour répartir la charge de l'impression auprès de tous les serveurs d'impression dans la solution d'équilibrage de charge.

En cas de défaillance imprévue d'un serveur d'impression, le mécanisme de basculement de l'équilibreur de charge de chaque VDA répartit automatiquement les connexions d'imprimantes attribuées aux serveurs d'impression défaillants aux autres serveurs d'impression disponibles de façon à ce que toutes les sessions existantes et entrantes fonctionnent normalement sans affecter l'expérience de l'utilisateur et sans nécessiter l'intervention immédiate de l'administrateur.

Les administrateurs peuvent surveiller l'activité des serveurs d'impression d'équilibrage de charge à l'aide d'un ensemble de compteurs de performances pour suivre les indicateurs suivants sur le VDA :

- Liste des serveurs d'impression dont la charge est équilibrée sur le VDA et leur état (disponible, indisponible)
- Nombre de connexions d'imprimantes acceptées par chaque serveur d'impression
- Nombre d'échecs de connexions d'imprimantes sur chaque serveur d'impression
- Nombre de connexions d'imprimantes actives sur chaque serveur d'impression
- Nombre de connexions d'imprimantes en attente sur chaque serveur d'impression

Le tableau suivant récapitule l'emplacement d'affichage des imprimantes et de gestion des files d'attente dans votre environnement.

	Piste d'impression	UAC activé ?	L'Emplacement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Imprimantes clientes (imprimantes connectées à la machine utilisateur)	Piste d'impression cliente	UAC activé ?	L'emplacement Le composant logiciel enfichable Gestion d'impression dans la console Microsoft Management Console
		Off	Pré-Windows 8 : Panneau de configuration Windows 8 : composant logiciel enfichable Gestion de l'impression
Imprimantes réseau (Imprimantes sur un serveur d'impression réseau)	Piste d'impression réseau	On	Composant logiciel enfichable Serveur d'impression > Gestion de l'impression dans la console Microsoft Management Console
		Off	Serveur d'impression > Panneau de configuration
Imprimantes réseau (Imprimantes sur un serveur d'impression réseau)	Piste d'impression cliente	On	Composant logiciel enfichable Serveur d'impression > Gestion de l'impression dans la console Microsoft Management Console
		Off	Pré-Windows 8 : Panneau de configuration Windows 8 : composant logiciel enfichable Gestion de l'impression
Imprimantes serveur réseau locales (Imprimantes d'un serveur d'impression réseau qui sont ajoutées à une machine avec OS de serveur)	Piste d'impression réseau	On	Serveur d'impression > Panneau de configuration
		Off	Serveur d'impression > Panneau de configuration

Remarque : les files d'attente d'impression des imprimantes réseau utilisant la piste d'impression réseau sont privées et ne peuvent être gérées au travers du système.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HDX

Jul 07, 2016

Citrix HDX intègre une large gamme de technologies conçues pour apporter une expérience utilisateur haute définition.

Sur la machine	HDX s'appuie sur les capacités informatiques des machines utilisateur pour améliorer et optimiser l'expérience utilisateur. La technologie HDX MediaStream offre aux utilisateurs un rendu fluide et transparent du contenu multimédia disponible sur leur bureau ou application virtuels. Le contrôle de l'espace de travail permet aux utilisateurs de suspendre les applications et les bureaux virtuels et de continuer à travailler à partir d'une autre machine, à l'endroit où ils l'ont laissé.
Sur le réseau	HDX offre des fonctionnalités d'accélération et d'optimisation pour mettre à disposition les meilleures performances réseau, y compris sur les connexions à faible bande passante ou en réseau étendu présentant une forte latence. Les fonctionnalités HDX s'adaptent aux modifications de l'environnement, en équilibrant les performances et la bande passante en appliquant les meilleures technologies possibles à chaque scénario, que le bureau ou l'application soit accessible localement sur le réseau d'entreprise ou à distance, en dehors du pare-feu de l'entreprise.
Dans le centre de données	HDX tire profit de la puissance de calcul et de l'évolutivité des serveurs de façon à offrir des performances graphiques avancées, quelles que soient les capacités de la machine utilisateur. Les informations multimédia compressées sont envoyées directement à la machine utilisateur dans leur format natif. La surveillance du canal HDX, fournie par Citrix Director, affiche le statut des canaux HDX connectés sur les machines utilisateur. HDX Insight, l'intégration de Network Inspector et de Performance Management avec Director, capture des données sur le trafic ICA et offre un tableau de bord des données d'historique en temps réel, telles que la latence de session ICA côté client et côté serveur, la consommation de bande passante des canaux ICA et la durée des boucles ICA de chaque session.

Pour bénéficier des capacités HDX de votre bureau virtuel :

- Voir comment HDX diffuse des vidéos riches en contenu sur les bureaux virtuels : afficher une vidéo sur un site Web contenant des vidéos haute définition, par exemple, http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.
- Voir comment la redirection Flash accélère la mise à disposition de contenu Flash multimédia :
  1. Téléchargez le lecteur Adobe Flash (http://get.adobe.com/flashplayer/) et installez-le sur le bureau virtuel et la machine utilisateur.
  2. Dans la barre d'outils de Desktop Viewer, cliquez sur Préférences. Dans la boîte de dialogue Préférences de Desktop Viewer, cliquez sur l'onglet Flash puis sélectionnez Optimiser le contenu.
  3. Pour bénéficier de la manière dont la redirection Flash accélère la mise à disposition du contenu Flash multimédia vers des bureaux virtuels, affichez une vidéo sur votre bureau à partir d'un site Web contenant des vidéos Flash, comme YouTube. La Redirection Flash est conçue pour être transparente, si bien que les utilisateurs ne savent pas quand elle s'exécute. Vous pouvez toutefois savoir si la Redirection Flash est en cours d'utilisation en recherchant un bloc de couleur qui apparaît momentanément avant le démarrage du lecteur Flash.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Voir comment HDX diffuse l'audio à définition élevée :
  1. Configurez le client Citrix pour une qualité audio maximale ; consultez la documentation relative à Citrix Receiver pour plus de détails.
  2. Lire les fichiers musicaux à l'aide d'un lecteur audio numérique (tels que iTunes) sur votre bureau.

HDX offre des graphiques et une expérience vidéo supérieurs pour la plupart des utilisateurs par défaut, sans configuration requise. Les paramètres de stratégie Citrix qui offrent la meilleure expérience possible à la plupart des cas d'utilisation sont activés par défaut.

- HDX sélectionne automatiquement la meilleure méthode de mise à disposition basée sur le client, la plate-forme, l'application et la bande passante réseau, puis ajuste le tout basé sur la modification des conditions.
- HDX optimise les performances de graphiques 2D et 3D et de la vidéo.
- HDX diffuse une expérience Windows Aéro aux utilisateurs de bureaux virtuels sur n'importe quel client.
- HDX permet aux machines utilisateur de livrer en streaming des fichiers multimédia directement à partir du fournisseur source sur Internet ou Intranet, plutôt qu'au travers du serveur hôte. Si la configuration requise pour la récupération de contenu côté client n'est pas présente, la mise à disposition multimédia retourne à la redirection Windows Media pour lire les fichiers runtime multimédia sur les machines utilisateur plutôt que sur le serveur hôte. Dans la plupart des cas, aucune modification aux stratégies de fonctionnalité Windows Media n'est nécessaire.

À savoir :

- Pour plus d'informations sur la prise en charge et la configuration requise pour les fonctionnalités HDX, consultez l'article Configuration système requise. Sauf mention contraire, les fonctionnalités HDX sont disponibles pour les machines avec OS de serveur Windows et avec OS de bureau Windows et les bureaux Remote PC Access pris en charge.
- Ce contenu décrit comment optimiser davantage l'expérience utilisateur, améliorer l'extensibilité du serveur ou réduire les besoins en bande passante. Pour de plus amples informations sur l'utilisation des stratégies Citrix et des paramètres de stratégie, consultez les documents relatifs aux
  — stratégies Citrix
  pour cette version.
- Pour obtenir des instructions qui incluent l'utilisation du Registre, faites attention : la modification du Registre peut entraîner de sérieux problèmes qui pourraient nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

Par défaut, HDX offre une expérience de bureau Windows Aéro ou Windows 8 très réactive sur les bureaux virtuels accessibles à partir de machines utilisateur Windows prises en charge. Pour ce faire, HDX tire parti de l'unité de traitement graphique (GPU) ou du processeur graphique intégré (IGP) sur les machines utilisateur pour la restitution des graphiques DirectX locaux. Cette fonctionnalité, appelée Redirection Desktop Composition, conserve une haute évolutivité sur le serveur. Pour plus d'informations, consultez la section Comment faire avec tous ces choix dans http://blogs.citrix.com/2013/11/06/go-supersonic-with-xendesktop-7-x-bandwidth-supercodecs/.

Pour réduire la bande passante requise dans les sessions utilisateur, considérez apporter les réglages de stratégie Citrix suivants. Gardez à l'esprit que toute modification apportée à ces paramètres peut réduire la qualité de l'expérience utilisateur.

- La **Redirection Desktop Composition** : s'applique uniquement aux machines avec OS Windows Desktop, accessible à partir de machines utilisateur Windows et s'applique uniquement à la composition du bureau Windows. Les fenêtres d'application sont restituées sur le serveur, sauf si le paramètre de stratégie Citrix Autoriser l'accès aux applications locales est Autorisé.
- La **qualité graphique de Redirection Desktop Composition** : utilise des graphiques de qualité élevée pour la

© 1999-2017 Citrix Systems, Inc. All rights reserved.

composition du bureau, sauf si les applications transparentes ou l'accès aux applications locales sont activés. Pour réduire les besoins en bande passante, réduisez la qualité des graphiques.

- **Aperçu de fenêtres dynamiques** : contrôle l'affichage des fenêtres transparentes en modes d'aperçu de fenêtres Flip, Flip 3D, Taskbar Preview et Peek. Pour réduire les besoins en bande passante, désactivez ce paramètre de stratégie.

Les paramètres de stratégie d'affichage visuel suivants contrôlent la qualité des images envoyées depuis des bureaux virtuels vers les machines utilisateur.

- Qualité visuelle. Contrôle la qualité visuelle des images affichées sur la machine utilisateur : moyenne, élevée, toujours sans perte, sans perte si possible (valeur par défaut = moyenne).
- Taux de trames cible. Spécifie le nombre maximal de trames par seconde envoyées depuis le bureau virtuel vers la machine utilisateur (valeur par défaut = 30). Dans de nombreux cas, vous pouvez améliorer l'expérience utilisateur en spécifiant une valeur plus élevée. Pour les périphériques avec des UC plus lents, la spécification d'une valeur inférieure permet d'améliorer l'expérience de l'utilisateur.
- Limite de mémoire d'affichage. Spécifie la taille maximale de la mémoire tampon vidéo (en kilo-octets) pour la session (valeur par défaut = 65536 Ko). Pour les connexions nécessitant un nombre de couleurs et une résolution élevés, augmentez la limite. Vous pouvez calculer la mémoire maximale nécessaire. Des nombres de couleurs autres que 32 bits sont uniquement disponibles si la stratégie de mode graphique d'ancienne génération est activée.

La compression vidéo de webcam HDX permet d'améliorer l'efficacité de la bande passante et la tolérance à la latence pour les webcams durant la visioconférence dans une session. Cette technologie diffuse le trafic de la webcam sur un canal virtuel multimédia dédié ; il utilise beaucoup moins de bande passante par rapport à la prise en charge de Plug-n-Play HDX isochrones et fonctionne bien sur des connexions en réseau étendu.

Toutefois, les utilisateurs de Citrix Receiver peuvent remplacer le comportement par défaut en choisissant le paramètre Mic & Webcam de Desktop Viewer Ne pas utiliser mon micro ou ma webcam. Pour empêcher les utilisateurs de basculer depuis la compression vidéo de webcam HDX, désactivez la redirection du périphérique USB en utilisant les paramètres de stratégie sous ICA > Périphériques USB.

La compression vidéo de webcam HDX est activée par défaut sur Citrix Receiver pour Windows, mais doit être configurée sur Citrix Receiver pour Linux. Pour plus d'informations, reportez-vous à la documentation relative à Citrix Receiver. La compression vidéo de webcam HDX nécessite que les paramètres de stratégie suivants soient activés (tous sont activés par défaut).

- Redirection audio du client
- Redirection du microphone client
- Conférences multimédia
- Redirection Windows Media

Si une webcam prend en charge le codage matériel H.264, la compression vidéo HDX utilise le codage matériel par défaut. Le codage matériel utilise de la bande passante supplémentaire et n'est pas approprié pour un réseau à bande passante réduite. Pour forcer la compression logicielle sur des réseaux à faible bande passante, ajoutez la valeur de clé DWORD suivante à la clé de registre : HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1.

Pour les déploiements dans lesquels l'extensibilité du serveur est supérieure à l'expérience utilisateur, vous pouvez utiliser le système graphique d'ancienne génération en ajoutant le paramètre de stratégie Mode graphique d'ancienne génération et

© 1999-2017 Citrix Systems, Inc. All rights reserved.

en configurant des paramètres de stratégie de graphiques d'ancienne génération individuels. L'utilisation d'un système graphique d'ancienne génération affecte particulièrement l'expérience de l'utilisateur sur des connexions de réseau étendu et mobiles.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mode de compatibilité Thinwire

Jul 07, 2016

Le mode de compatibilité Thinwire utilise de nouvelles techniques de décomposition de l'écran et de mise en cache, qui contribuent à réduire la consommation de bande passante et à augmenter la capacité à monter en charge du serveur sans compromettre l'expérience utilisateur.

Le mode de compatibilité Thinwire comprend les fonctionnalités suivantes :

- Correspondance de bitmap intelligente pour un fournisseur de bitmap.
  - Analyse de traduction de bitmap pour un déplacement et un défilement efficaces des fenêtres.
- Rétrocompatibilité. La mise à niveau du client ou de Citrix Receiver n'est pas nécessaire, de même que l'accélération matérielle.
  - Testé sur un éventails d'anciens clients légers vieux de 5 ans et plus.
- Optimisé pour réduire la consommation d'UC du serveur et augmenter la capacité à monter en charge du serveur.
- Mode émulé 16 bits, qui réduit la bande passante de 15 à 20 % pour les charges typiques.
- Détection des transitoires du contenu vidéo rendu sur le serveur.
  - Traitement des transitoires multiples pour une expérience multimédia améliorée. Par exemple, lors du visionnage de vidéos multiples ou de bandes de téléscripteur.
  - Augmentation sélective de la netteté pour les régions qui sortent d'un état transitoire.
- Optimisé pour l'accélération CloudBridge. Lors des tests, nous avons observé un ratio de réduction de la bande passante de l'ordre de 6:1 sur des charges de type Office.
- Affichage adaptatif, qui peut être réglé dans les paramètres de stratégie. Pour plus d'informations veuillez consulter **Compression d'images en mouvement** dans Paramètres de stratégie des images en mouvement.
- Prise en charge des VDA et systèmes d'exploitation Windows jusqu'aux VDA Windows 10.
- Nouveau mode « Sans perte si possible » pour 3D Pro, qui améliore la réactivité, l'interactivité, et l'augmentation interruptible de la netteté afin d'offrir une meilleure expérience utilisateur sur les connexions à faible bande passante.
- Qualité par défaut des images photographiques statiques supérieure à celle du Mode graphique d'ancienne génération.

Pour les paramètres de qualité visuelle « Faible », « Moyenne » (défaut) et « Élevée », le détecteur des transitoires évalue de façon dynamique les mises à jour de l'écran pour déterminer si les zones hautement animées doivent être transmises à une résolution plus faible, conformément à la stratégie d'affichage adaptatif, afin d'améliorer les performances du client et réduire la consommation de bande passante.

Pour la qualité visuelle **Sans perte si possible**, le mode de compatibilité Thinwire utilise une approche « fuzzy-first » pour la mise à jour d'un grand nombre d'écrans. Ce paramètre est destiné aux utilisateurs 3D Pro qui manipulent des modèles 3D ou d'autres applications gourmandes en ressources graphiques. Si l'activité persiste, un mode transitoire est utilisé et la zone affectée est améliorée et mise en cache une fois que l'activité transitoire s'arrête. Pour la première modification de grande taille, une brève analyse d'image est effectuée sur la zone de modification pour déterminer si une transition irrégulière ou lisse (sans perte) est utilisée, par exemple lorsqu'une maquette est pivotée. Il est plus efficace, en termes de FPS (images par seconde) et de bande passante, d'encoder des images simples à l'aide du codec sans perte de Citrix, et aucune perte de qualité ne se produit.

L'étape d'amélioration sans perte du mode Sans perte si possible est également différente. Plutôt que d'améliorer la zone concernée en une seule fois, la zone est améliorée en blocs prédéterminés afin de faciliter l'interactivité et de garantir une expérience utilisateur optimale. L'amélioration d'une large zone de modification en milieu de transition, par exemple le déplacement d'un modèle 3D qui s'arrête brièvement avant de reprendre, pouvait préalablement entraîner un blocage, plus

© 1999-2017 Citrix Systems, Inc. All rights reserved.

particulièrement pour les connexions à faible bande passante. La taille des blocs d'amélioration dépend de la manière dont la qualité a été réduite pour conserver le taux de trame minimum cible (un paramètre de stratégie d'affichage adaptatif). Si la qualité est fortement diminuée, la taille des blocs d'amélioration sera plus petite, avec une taille minimum de 128 x 128 pixels. Si la qualité n'a pas été réduite, lorsque le client a suffisamment de puissance de traitement et de bande passante par exemple, la taille des blocs d'amélioration peut être une taille maximale de 384 x 384 pixels.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Canal virtuel Framehawk

Jul 07, 2016

Introduction

Le canal virtuel Framehawk optimise la mise à disposition d'applications et de bureaux virtuels pour les utilisateurs sur connexions sans fil à haut débit et connexions réseau longue distance à haut débit avec perte, lorsque des pertes de paquets ou des congestions se produisent. Vous pouvez utiliser les stratégies Citrix pour mettre en œuvre Framehawk ou Thinwire pour un ensemble d'utilisateurs en fonction des caractéristiques de votre réseau et des attentes en matière d'évolutivité et de performances.

En général, le taux de trame et la qualité visuelle sont les deux éléments de base d'une expérience utilisateur positive. Framehawk améliore la définition pour aussi prendre en compte la linéarité. Les utilisateurs doivent pouvoir profiter de l'expérience et ne pas être gênés. En cas de problèmes de réseau, les utilisateurs doivent faire face à l'effet d'« élastique » qui affecte tous les protocoles. Cet effet désigne notamment le syndrome « taper-attendre-taper » : ne sachant pas si l'écran va répondre, l'utilisateur commence à cliquer de façon aléatoire, multipliant ainsi les résultats indésirables. Framehawk améliore ces expériences, particulièrement dans des conditions de réseau contraignantes.

Les connexions Internet domestiques à haut débit rencontrent souvent des problèmes de performance, à cause de collisions avec des signaux Wi-Fi à proximité ou d'interférences spectrales provenant d'appareils sans fil, entre autres. De plus en plus d'utilisateurs se connectent à des applications hébergées et à des données via les réseaux cellulaires 3G ou 4G/LTE ou à l'aide de services Internet à bord d'un avion. D'autres aiment bénéficier de points de connexion Wi-Fi publics lorsqu'ils sont au café ou à l'hôtel, où l'engorgement est un problème courant.

Avec Framehawk, les utilisateurs remarquent une expérience plus interactive (un écho plus linéaire des caractères) à des latences élevées.

Imaginez Framehawk comme une implémentation logicielle de l'œil humain, observant ce qui se trouve dans le tampon de trame et identifiant les différents types de contenu sur l'écran. Qu'est-ce qui est important pour l'utilisateur ? Pour les zones de l'écran qui changent rapidement, comme les vidéos ou les graphiques animés, il n'est pas très important pour l'œil humain que quelques pixels se perdent en route, car ils sont rapidement remplacés par de nouvelles données.

Toutefois, pour les zones statiques de l'écran, telles que les icônes dans la barre d'outils ou d'état ou un texte qui s'affiche après défilement par l'utilisateur pour atteindre son point de lecture, l'œil humain est très exigeant ; l'utilisateur attend une perfection au pixel près. À l'inverse des protocoles qui recherchent la précision technique, Framehawk vise à s'adapter à l'être humain utilisant la technologie.

Framehawk comprend un amplificateur de signal (QoS) nouvelle génération ainsi qu'une carte thermique temporelle pour une identification plus précise et plus efficace des charges de travail. Il utilise des transformations autonomiques à réparation spontanée en plus de la compression de données, et évite la retransmission des données pour maintenir une réponse rapide aux clics, la linéarité et une cadence régulière. Sur une connexion réseau avec perte, Framehawk peut masquer la perte avec une interpolation, permettant à l'utilisateur de continuer à percevoir une bonne qualité d'image tout en bénéficiant d'une expérience plus fluide. En outre, les algorithmes Framehawk peuvent faire la distinction entre les différents types de perte de paquets ; par exemple, perte aléatoire (envoi de données supplémentaires pour compenser) ou

© 1999-2017 Citrix Systems, Inc. All rights reserved.

perte avec congestion (arrêt de l'envoi de données, car le canal est déjà saturé).

Le moteur Framehawk Intent Engine fait la distinction entre le défilement vers le haut ou vers le bas, le zoom, le déplacement vers la gauche ou vers la droite, la lecture, la saisie et autres actions courantes, et gère les communications vers le Virtual Delivery Agent (VDA) à l'aide d'un dictionnaire partagé. Si l'utilisateur lit un texte, la qualité visuelle du texte doit être excellente. Si l'utilisateur fait défiler l'écran, le mouvement doit être rapide et fluide. Par ailleurs, il doit pouvoir être interrompu, de façon à ce que l'utilisateur puisse constamment contrôler l'interaction avec l'application ou le bureau.

En mesurant la cadence sur la connexion réseau (ce que nous appelons « engrenage », par analogie avec la tension d'une chaîne de vélo), la logique de Framehawk peut réagir plus rapidement, offrant une expérience supérieure sur des connexions à latence élevée. Ce système d'engrenage unique et breveté offre un retour permanent sur les conditions du réseau, ce qui permet à Framehawk de réagir immédiatement aux changements de bande passante, à la latence et à la perte de données.

Considérations relatives à la conception avec Thinwire et Framehawk

Bien que Thinwire soit leader du secteur en termes d'efficacité de bande passante et soit adapté à un large éventail de scénarios d'accès et de conditions de réseau, il se fonde sur TCP pour des communications de données fiables et doit par conséquent retransmettre les données en cas de réseau avec perte ou saturé, entraînant un décalage pour l'utilisateur.

Framehawk étant basé sur UDP, le plus gros des efforts a lieu à la transmission de données. UDP ne représente qu'une petite partie de la façon dont Framehawk traite les problèmes de perte, comme vous pouvez le voir en comparant les performances de Framehawk avec d'autres protocoles basés sur UDP ; il joue cependant un rôle fondamental pour les techniques centrées sur l'être humain qui distinguent Framehawk du reste.

Quelle quantité de bande passante est requise par Framehawk ?

Une connexion sans fil haut débit repose sur plusieurs facteurs, y compris le nombre d'utilisateurs qui partagent la connexion, la qualité de la connexion et les applications en cours d'utilisation. Pour des performances optimales, Citrix suggère une configuration de base de 4 ou 5 Mbits/s ainsi que 150 Kbits/s par utilisateur.

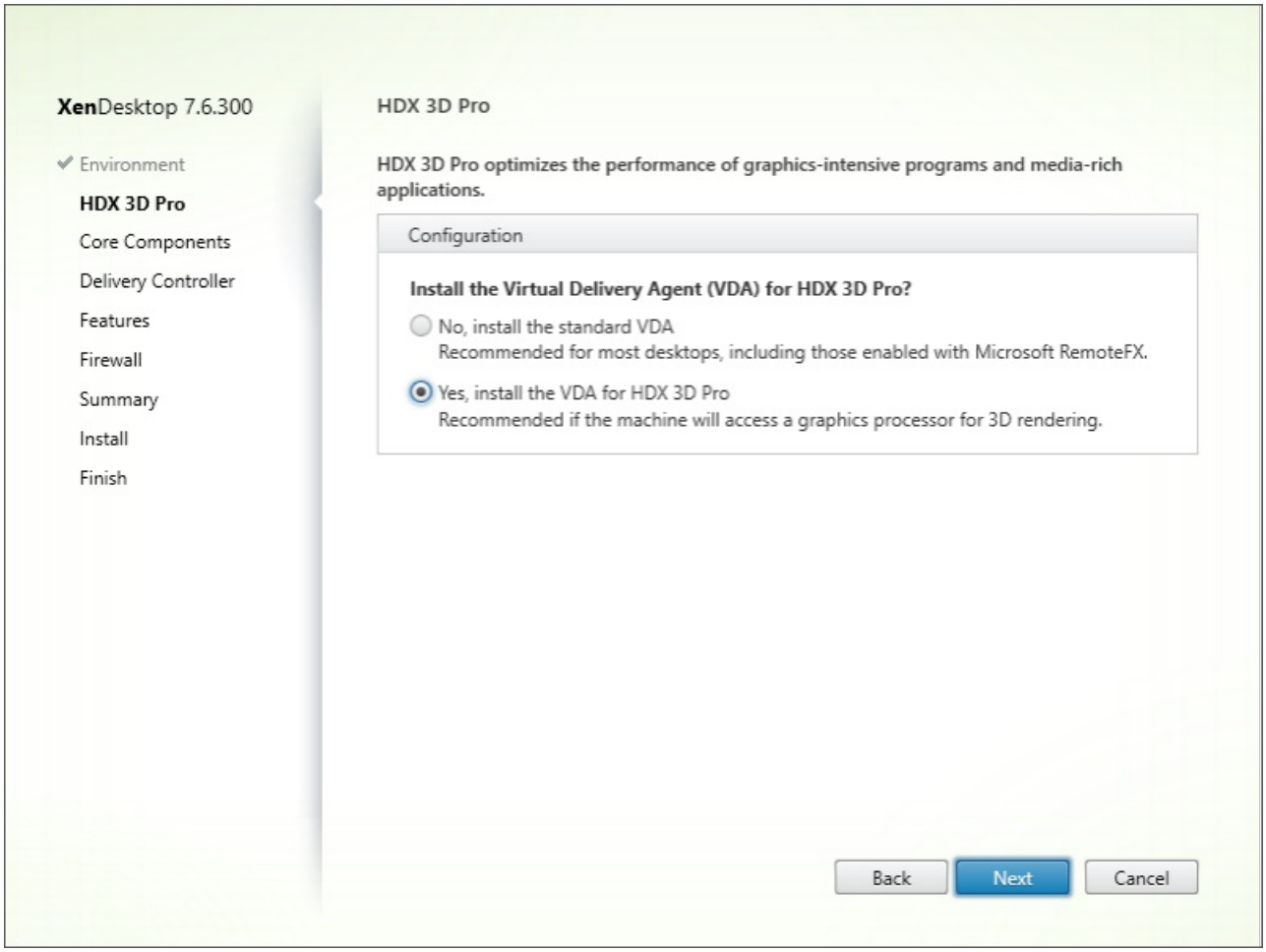
Pour Thinwire, Citrix recommande une bande passante de 1,5 Mbits/s ainsi que 150 Kbits/s par utilisateur (pour plus de détails, reportez-vous au blog sur la bande passante XenApp et XenDesktop) ; mais avec une perte de paquets de 3 %, vous remarquerez que Thinwire requiert beaucoup plus de bande passante que Framehawk pour garantir une expérience utilisateur positive.

Remarque : Thinwire reste le canal de communication à distance d'écran principal dans le protocole ICA. Framehawk est désactivé par défaut. Citrix recommande de l'activer pour répondre aux scénarios d'accès sans fil haut débit dans votre organisation.

Framehawk prend désormais en charge tous les cas d'utilisation de HDX 3D Pro, pour XenApp (OS de serveur) et XenDesktop (OS de bureau). Dans les premières préversions, il a été validé dans des environnements client avec 400-500 ms de latence et 1-2 % de perte de paquet, offrant une bonne interactivité à l'aide d'applications de modélisation 3D standard telles que AutoCAD, Siemens NX et autres. Cette prise en charge améliore la capacité d'afficher et de manipuler des modèles CAD de grande taille en déplacement ou en cas de travail délocalisé ou de conditions de réseau insatisfaisantes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

L'activation de cette fonctionnalité ne nécessite pas de tâches de configuration supplémentaires. Lors de l'installation du VDA, sélectionnez l'option 3DPro au début de l'installation :



Configuration requise et considérations

Framehawk requiert au minimum VDA 7.6.300 et Gestion de stratégie de groupe 7.6.300.

Le point de terminaison doit disposer au minimum de Citrix Receiver pour Windows 4.3.100 ou Citrix Receiver pour iOS 6.0.1.

Par défaut, Framehawk utilise une plage de ports UDP bidirectionnelle (3224-3324) pour échanger les données du canal d'affichage Framehawk avec Citrix Receiver ; la plage peut être personnalisée dans un paramètre de stratégie appelé « Plage de ports du canal d'affichage Framehawk ». Chaque connexion simultanée entre le client et le bureau virtuel requiert un port unique. Dans les environnements de système d'exploitation multi-utilisateurs, tels que les serveurs XenApp, vous devez définir suffisamment de ports pour prendre en charge le nombre maximal de sessions utilisateur simultanées. Pour un système d'exploitation à utilisateur unique, tels que les bureaux VDI, il suffit de définir un port UDP unique. Framehawk tente d'abord d'utiliser le premier port défini et progresse jusqu'au dernier port spécifié dans la plage. Ce comportement s'applique à la fois à la communication via NetScaler Gateway et aux connexions internes directes vers le serveur StoreFront.

Pour l'accès à distance, NetScaler Gateway doit être déployé. Par défaut, NetScaler utilise le port UDP 443 pour les communications cryptées entre les Citrix Receiver du client et Gateway. Ce port doit être ouvert sur les pare-feu externes

© 1999-2017 Citrix Systems, Inc. All rights reserved.

pour permettre les communications sécurisées dans les deux sens. La fonctionnalité est appelée Datagram Transport Security (DTLS).

Remarque : les connexions Framehawk/DTLS ne sont pas prises en charge sur les boîtiers FIPS.

Les connexions Framehawk chiffrées sont prises en charge, depuis NetScaler Gateway version 11.0.62 et NetScaler Unified Gateway version 11.0.64.34 ou version ultérieure.

Tenez compte des recommandations suivantes avant la mise en œuvre de canaux virtuels Framehawk :

- Contactez votre administrateur de sécurité pour vérifier que les ports UDP définis pour Framehawk sont bien ouverts sur le pare-feu. Le processus d'installation ne configure pas automatiquement le pare-feu.
- Dans de nombreux cas, NetScaler Gateway peut être installé dans la DMZ, entouré de pare-feu du côté externe ainsi que du côté interne. Assurez-vous que le port UDP 443 est ouvert sur le pare-feu externe, et que les ports UDP 3224-3324 sont ouverts sur le pare-feu interne si votre environnement utilise les plages de port par défaut.

Configuration

Attention : Citrix vous recommande d'activer Framehawk uniquement pour les utilisateurs rencontrant une perte importante de paquets. Il est recommandé de ne pas activer Framehawk en tant que stratégie universelle pour tous les objets du site.

Le canal virtuel Framehawk est désactivé par défaut. Lorsque cette option est activée, le serveur tente d'utiliser le canal virtuel Framehawk pour les graphiques et la saisie. Si les conditions requises ne sont pas réunies pour quelque raison que ce soit, la connexion est établie à l'aide du mode par défaut (Thinwire).

Les paramètres de stratégie suivants affectent Framehawk :

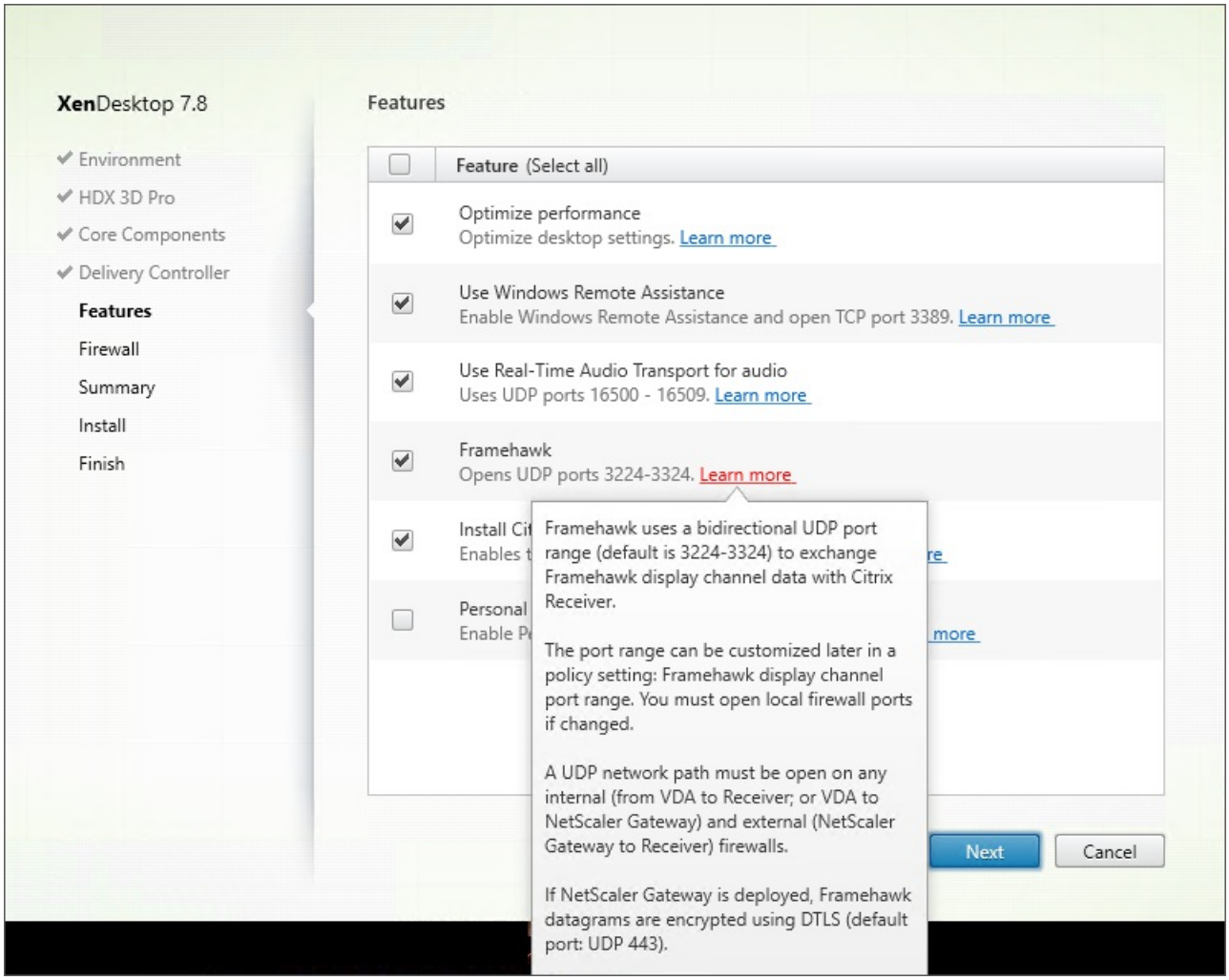
- Canal d'affichage Framehawk : active ou désactive la fonctionnalité.
- Plage de ports du canal d'affichage Framehawk : spécifie la plage de numéros de port UDP (le numéro de port le plus bas vers le numéro de port le plus élevé) que le VDA peut utiliser pour échanger les données de canal d'affichage Framehawk avec la machine utilisateur. Le VDA tente d'utiliser chaque port, en commençant par le numéro de port le plus bas et en remontant pour chaque tentative. Le port gère le trafic entrant et sortant.

Dans la version 7.8, une nouvelle option est disponible pour reconfigurer le pare-feu lors de l'étape **Fonctionnalités** du programme d'installation du VDA. Cette case à cocher ouvre les ports UDP 3224-3324 sur le pare-feu Windows, si elle est sélectionnée. Veuillez noter que la configuration manuelle des pare-feux est requise dans certaines circonstances :

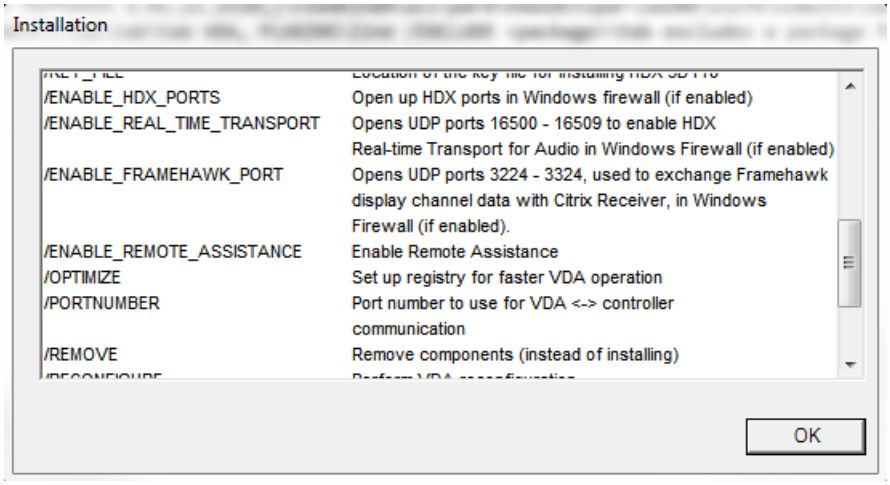
- pour les pare-feux de réseau ou
- si la plage de ports par défaut est personnalisée.

Pour ouvrir ces ports UDP, sélectionnez la case à cocher **Framehawk**

© 1999-2017 Citrix Systems, Inc. All rights reserved.



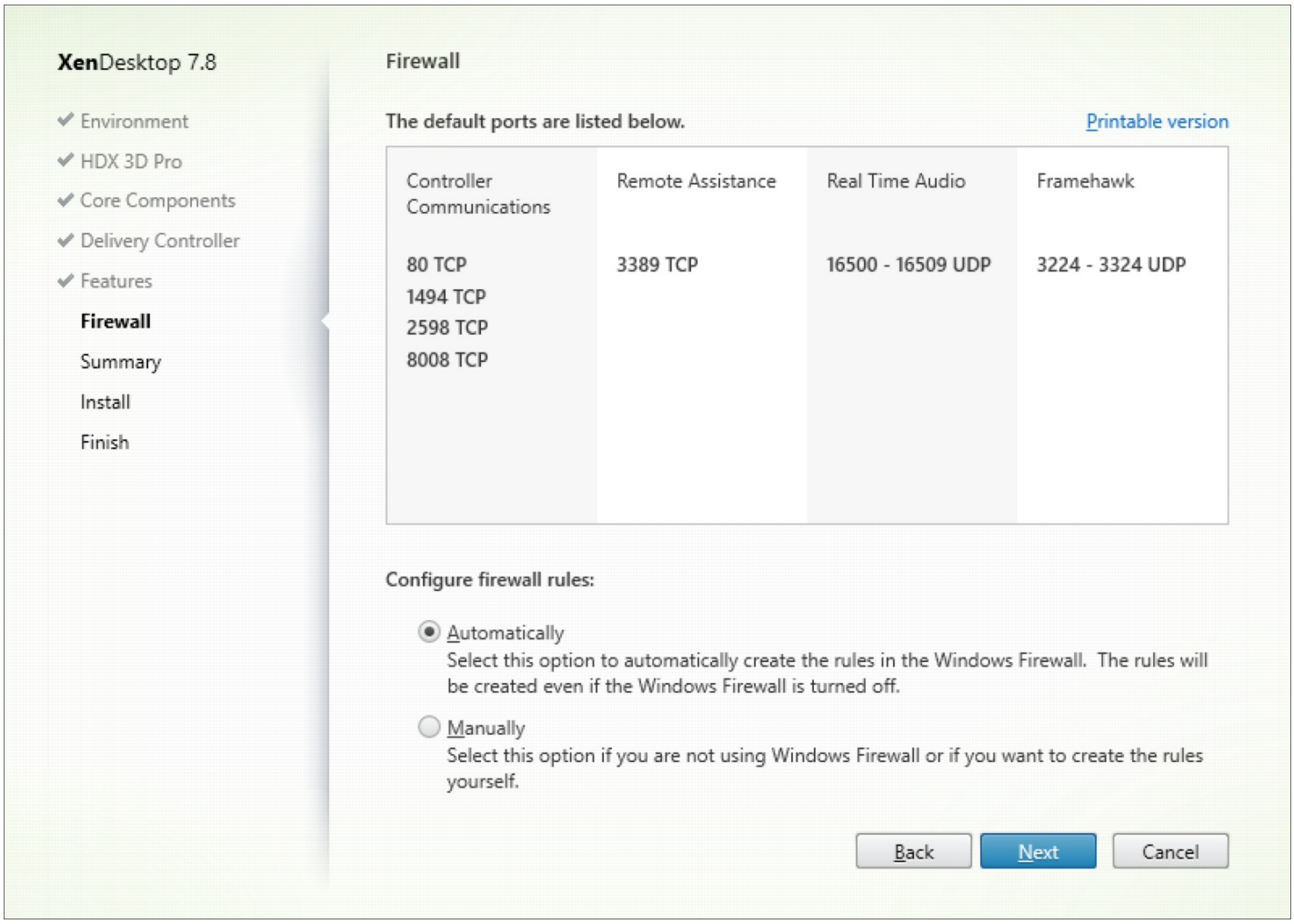
Vous pouvez également utiliser la ligne de commande pour ouvrir les ports UDP pour le canal virtuel Framehawk à l'aide de **/ENABLE_FRAMEHAWK_PORT** :



Vérification des attributions de port UDP Framehawk

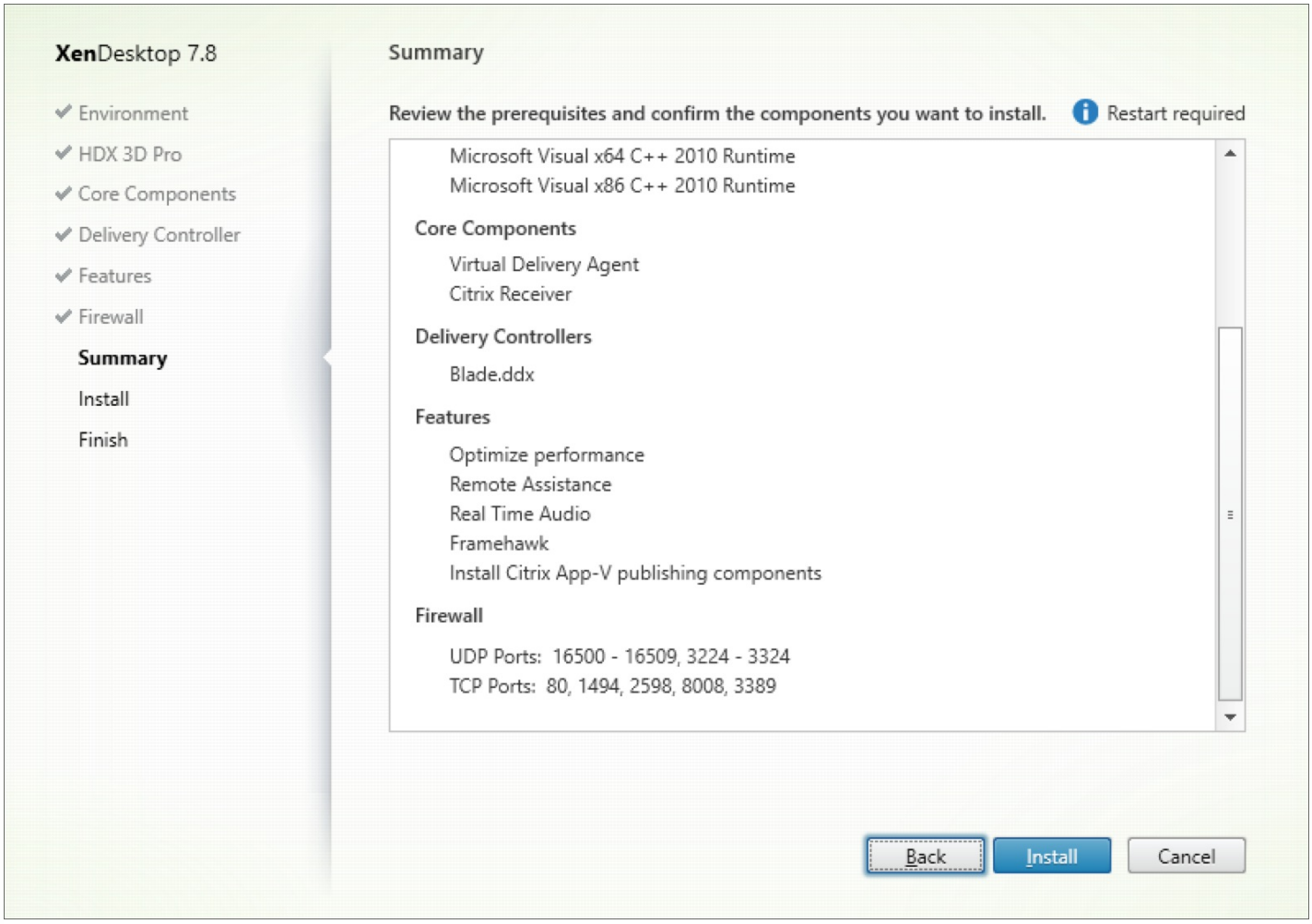
Lors de l'installation, vous pouvez vérifier les ports UDP attribués au canal virtuel Framehawk dans l'écran **Pare-feu** :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



L'écran **Résumé** indique si la fonctionnalité de canal virtuel Framehawk est activée :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Prise en charge de NetScaler Gateway pour Framehawk

Le trafic Framehawk crypté est pris en charge sur NetScaler Gateway 11.0.62.10 ou version ultérieure, et NetScaler Unified Gateway 11.0.64.34 ou version ultérieure.

- NetScaler Gateway fait référence à l'architecture de déploiement dans laquelle le VPN vServer de passerelle est directement accessible depuis la machine cliente ; une adresse IP publique est attribuée au VPN vServer et l'utilisateur se connecte directement à cette adresse IP.
- NetScaler avec Unified Gateway fait référence au déploiement dans lequel le VPN vServer de passerelle est lié en tant que cible au vServer de basculement du contenu (CS). Dans ce déploiement, CS vServer dispose de l'adresse IP publique et le vServer VPN de passerelle dispose d'une adresse IP fictive.

Pour activer la prise en charge de Framehawk sur NetScaler Gateway, le paramètre DTLS au niveau du vServer VPN de passerelle doit être activé. Une fois que ce paramètre est activé et que les composants sur XenApp ou XenDesktop sont mis à jour correctement, le trafic audio, vidéo et interactif Framehawk est crypté entre le VPN vServer de passerelle et la machine utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway, Unified Gateway et NetScaler Gateway + équilibrage de charge de serveur global sont pris en charge avec Framehawk.

Les scénarios suivants ne sont pas pris en charge avec Framehawk :

- HDX Insight
- NetScaler Gateway en mode IPv6
- NetScaler Gateway Double Hop
- Plusieurs Secure Ticket Authority (STA) sur NetScaler Gateway
- NetScaler Gateway avec haute disponibilité
- NetScaler Gateway avec la configuration en cluster

Scénario	Prise en charge de Framehawk
NetScaler Gateway	Oui
NetScaler + équilibrage de charge de serveur global	Oui
NetScaler avec Unified Gateway	Oui Remarque : Unified Gateway version 11.0.64.34 et supérieure est prise en charge.
HDX Insight	Non
NetScaler Gateway en mode IPv6	Non
NetScaler Gateway Double Hop	Non
Plusieurs Secure Ticket Authority (STA) sur NetScaler Gateway	Non
NetScaler Gateway avec haute disponibilité	Non
NetScaler Gateway avec la configuration en cluster	Non

Pour activer la prise en charge de Framehawk sur NetScaler Gateway, le paramètre DTLS au niveau du vServer VPN de passerelle doit être activé. Une fois que ce paramètre est activé et que les composants sur XenApp ou XenDesktop sont mis à jour correctement, le trafic audio, vidéo et interactif Framehawk est crypté entre le VPN vServer de passerelle et la machine utilisateur.

Cette configuration est nécessaire si vous activez le cryptage UDP sur NetScaler Gateway pour l'accès distant.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Lors de la configuration de NetScaler pour la prise en charge de Framehawk :

- S'assurer que le port UDP 443 est ouvert sur les pare-feu externes
- S'assurer que le port CGP (par défaut 2598) est ouvert sur les pare-feu externes
- Activer DTLS dans les paramètres pour le serveur virtuel VPN
- Annuler puis rétablir la liaison de la paire cert-clé SSL ; cette procédure n'est pas obligatoire si vous utilisez NetScaler version 11.0.64.34 ou version ultérieure.

Pour configurer NetScaler Gateway pour la prise en charge de Framehawk :

1. Déployez et configurez NetScaler Gateway pour communiquer avec StoreFront et authentifier les utilisateurs pour XenApp et XenDesktop.
2. Dans l'onglet de configuration NetScaler, développez NetScaler Gateway et sélectionnez **Serveurs virtuels**.
3. Cliquez sur **Modifier** pour afficher les paramètres de base pour le serveur virtuel VPN ; vérifiez l'état du paramètre DTLS.
4. Cliquez sur **Plus** pour afficher d'autres options de configuration :
5. Sélectionnez **DTLS** pour assurer la sécurité des communications pour les protocoles UDP tels que Framehawk. Cliquez sur **OK**. La zone Paramètres de base pour le serveur virtuel VPN indique que l'indicateur DTLS est défini sur la valeur **True**.
6. Ouvrez de nouveau l'écran Server Certificate Binding et cliquez sur **+** pour lier la paire de clés de certificat.
7. Choisissez la paire de clés de certificat requise et cliquez sur **Select**.
8. Enregistrez les modifications apportées à la liaison du certificat du serveur.
9. Après l'enregistrement, la paire de clés de certificat s'affiche. Cliquez sur **Bind**.
10. Ignorez le message « No usable ciphers configured on the SSL vserver/service » s'il s'affiche.

Étapes supplémentaires pour les anciennes versions de NetScaler Gateway

Si vous utilisez une version de NetScaler Gateway antérieure à 11.0.64.34 :

1. Ouvrez de nouveau l'écran Server Certificate Binding et cliquez sur + pour lier la paire de clés de certificat.
2. Choisissez la paire de clés de certificat requise et cliquez sur Select.
3. Enregistrez les modifications apportées à la liaison du certificat du serveur.
4. Après l'enregistrement, la paire de clés de certificat s'affiche. Cliquez sur Bind.
5. Ignorez le message « No usable ciphers configured on the SSL vserver/service » s'il s'affiche.

Pour configurer Unified Gateway pour la prise en charge de Framehawk :

1. Assurez-vous que Unified Gateway est installé et correctement configuré. Pour de plus amples informations, reportez-vous à la section Unified Gateway sur le site de documentation des produits Citrix.
2. Activez le paramètre DTLS sur le *vServer* VPN qui est lié au vServer CS en tant que *vServer* cible.

NetScaler Gateway est le seul produit VPN SSL qui prend en charge le cryptage UDP requis par Framehawk. La stratégie Framehawk peut ne pas s'appliquer si un autre VPN SSL ou une version incorrecte de NetScaler Gateway est utilisé(e). Les produits VPN IPSec traditionnels prennent en charge Framehawk sans nécessiter de modifications.

Configurer Citrix Receiver pour iOS pour la prise en charge de Framehawk

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour configurer Citrix Receiver pour iOS pour la prise en charge de Framehawk, vous devez manuellement modifier default.ica.

1. Sur le serveur StoreFront, accédez au répertoire App_Data de votre magasin dans c:\inetpub\wwwroot\.
2. Ouvrez le fichier default.ica et ajoutez la ligne suivante dans la section WFClient : Framehawk=On
3. Enregistrez les modifications.

Cela permet aux sessions Framehawk d'être établies depuis un Citrix Receiver compatible sur des appareils iOS. Cette étape n'est pas nécessaire si vous utilisez Citrix Receiver pour Windows.

Contrôle de Framehawk

Vous pouvez contrôler l'utilisation et les performances de Framehawk depuis Citrix Director. La vue Détails du canal virtuel HDX contient des informations utiles pour la résolution des problèmes et le contrôle du canal virtuel Framehawk dans une session. Pour afficher les statistiques concernant Framehawk, sélectionnez **Graphiques - Framehawk**.

Si la connexion avec Framehawk est établie, vous voyez **Provider=VD3D** et **Connected=True** dans la page des détails. Il est normal que l'état du canal virtuel soit inactif car il surveille le canal de signalisation, qui est uniquement utilisé durant la négociation initiale. Cette page fournit également d'autres statistiques utiles relatives à la connexion.

Si vous rencontrez des problèmes, consultez le blog de résolution des problèmes Framehawk.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HDX 3D Pro

Jul 07, 2016

HDX 3D Pro vous permet de mettre à disposition des bureaux et applications qui rendent un meilleur effet avec une unité de traitement graphique (GPU) pour l'accélération matérielle, y compris les applications graphiques 3D professionnelles basées sur OpenGL et DirectX. Le VDA standard prend uniquement en charge l'accélération GPU de DirectX. Pour de plus amples informations sur le choix de l'édition du VDA, standard ou HDX 3D Pro, consultez la section Que spécifier lors de l'installation d'un VDA dans l'article Préparer l'installation.

Les applications professionnelles 3D exemples comprennent :

- les applications de conception, de fabrication et d'ingénierie assistées par ordinateur (CAD/CAM/CAE) ;
- les logiciels GIS (Geographical Information System) ;
- PACS (Picture Archiving Communication System) pour l'imagerie médicale ;
- les applications utilisant les dernières versions OpenGL, DirectX, NVidia CUDA, OpenCL et WebGL ;
- les applications non graphiques consommant énormément de ressources informatiques qui utilisent des GPU NVIDIA CUDA (Compute Unified Device Architecture) pour le traitement en parallèle.

HDX 3D Pro offre la meilleure expérience utilisateur possible sur toute bande passante :

- Sur les connexions sur réseau étendu (WAN) : mettez à disposition une expérience utilisateur interactive sur des connexions WAN avec des bandes passantes de 1,5 Mbps seulement.
- Sur les connexions sur réseau local (LAN) : mettez à disposition une expérience utilisateur équivalente à celle d'un bureau local sur des connexions LAN avec des bandes passantes de 100 Mbps.
  Vous pouvez remplacer les stations de travail complexes et coûteuses par des machines utilisateur beaucoup plus simples et transférer le traitement graphique vers le centre de données pour une gestion centralisée.

HDX 3D Pro offre une accélération GPU des machines avec OS Windows Desktop et des machines avec OS Windows Server. Lorsqu'il est utilisé avec des GPU Citrix XenServer et NVIDIA GRID, HDX 3D Pro offre une accélération vGPU (Virtual GPU) pour les machines avec OS Windows Desktop. Pour les versions de XenServer prises en charge, consultez Citrix Virtual GPU Solution.

Utilisez l'outil Moniteur HDX (qui remplace l'outil de contrôle d'intégrité) pour valider l'opération et la configuration des technologies de visualisation HDX et pour diagnostiquer et résoudre les problèmes HDX. Pour télécharger l'outil et en apprendre davantage sur celui-ci, consultez https://taas.citrix.com/hdx/download/.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Redirection Flash

Jul 07, 2016

La redirection Flash transfère le traitement de la plupart du contenu Adobe Flash (y compris les animations, les vidéos et les applications) vers les réseaux locaux ou étendus des machines Windows des utilisateurs, ce qui réduit la charge serveur et réseau. Ce résultat augmente la capacité à monter en charge tout en garantissant une expérience utilisateur haute définition. Configuration de la redirection Flash requiert des paramètres côté client et côté serveur.

Avertissement : la redirection Flash requiert une interaction significative entre la machine utilisateur et les composants serveur. Utilisez cette fonctionnalité uniquement dans des environnements dans lesquels la séparation de sécurité entre la machine utilisateur et le serveur n'est pas nécessaire. Vous pouvez également configurer des machines utilisateur pour pouvoir utiliser cette fonctionnalité uniquement avec des serveurs de confiance. Étant donné que la redirection Flash requiert l'installation du lecteur Flash Player sur la machine utilisateur, cette fonctionnalité doit uniquement être activée si le lecteur Flash Player lui-même est sécurisé.

Les versions de deuxième génération et d'ancienne génération de la redirection Flash sont des solutions indépendantes et s'exécutent sur des canaux virtuels distincts.

- Les fonctionnalités de redirection Flash d'ancienne génération sont prises en charge du côté client uniquement. Si une version antérieure de Flash Player est installée sur la machine utilisateur, ou si le lecteur Flash Player ne peut être installé, le contenu Flash est restitué sur le serveur.
- La redirection Flash de deuxième génération est prise en charge à la fois sur les clients et les serveurs. Si le client prend en charge la redirection Flash de deuxième génération, le contenu Flash est restitué sur le client. Les fonctionnalités de redirection Flash de deuxième génération comprennent la prise en charge des connexions utilisateur sur le réseau étendu, le retour intelligent, et une liste de compatibilité d'adresses URL ; consultez la section ci-dessous pour plus de détails.

La redirection Flash utilise la journalisation d'événements Windows sur le serveur pour consigner les événements Flash. Le journal d'événements indique si la redirection Flash est utilisée et fournit des détails sur les problèmes. Voici une liste commune à tous les événements journalisés par la redirection Flash :

- La redirection Flash signale les événements au journal d'applications.
- Sur les systèmes Windows 8 et Windows 7, un journal spécifique à la redirection Flash s'affiche dans le nœud Journaux des applications et des services.
- La valeur Source est Flash.
- La valeur Catégorie est Aucune.

Pour les dernières mises à jour de compatibilité HDX Flash, reportez-vous à l'article CTX136588.

Pour configurer la redirection Flash sur le serveur, utilisez les paramètres de stratégie Citrix suivants : Pour de plus amples informations, consultez la section Paramètres de stratégie de la redirection Flash.

- Le comportement Flash par défaut vous permet de définir le comportement par défaut de l'accélération Flash. Par défaut, la redirection Flash est activée. Pour modifier ce comportement par défaut pour des pages Web individuelles et des instances Flash, utilisez le paramètre Liste de compatibilité d'adresses URL Flash.
- Le retour intelligent Flash : détecte des instances de petits films Flash (telles que ceux fréquemment utilisés pour lire les publicités) et les restituer sur le serveur, au lieu de les rediriger pour restitution sur la machine utilisateur. Il n'entraîne ni interruption, ni échec du chargement de la page Web ou de l'application Flash. Par défaut, le retour intelligent Flash est activé. Pour rediriger toutes les instances de contenu Flash pour la restitution sur la machine utilisateur, désactivez ce paramètre de stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- La Liste d'adresse URL de récupération de contenu Flash côté serveur vous permet de spécifier des sites Web dont le contenu Flash peut être téléchargé vers le serveur puis transmis vers la machine utilisateur pour restitution. (Par défaut, la redirection Flash télécharge du contenu Flash vers la machine utilisateur où il est lu.) Ce paramètre fonctionne en conjonction avec (et requiert) le paramètre Activer la récupération de contenu côté serveur sur la machine utilisateur et est conçu pour être utilisé avec des sites intranet et des applications Flash internes ; consultez la section ci-dessous pour plus de détails. Il fonctionne également avec la plupart des sites Internet et peut être utilisé lorsque la machine utilisateur ne possède pas d'accès direct à Internet (par exemple, lorsque le serveur XenApp ou XenDesktop offre cette connexion). Remarque : la récupération de contenu côté serveur ne prend pas en charge les applications Flash utilisant le protocole RTMP (Real Time Messaging Protocol) ; au lieu de cela, la restitution côté serveur est utilisée, et prend en charge le protocole HTTP et HTTPS.
- La liste de compatibilité d'adresses URL Flash : spécifie l'emplacement où le contenu Flash provenant des sites Web répertoriés est restitué : sur la machine utilisateur, sur le serveur, ou bloqué.
- La liste de couleur d'arrière-plan Flash : vous permet de faire correspondre les couleurs des pages Web et des instances Flash, ce qui améliore l'apparence de la page Web lors de l'utilisation de la redirection Flash.

Installez Citrix Receiver et Adobe Flash Player sur la machine utilisateur. Aucune configuration supplémentaire n'est requise sur la machine utilisateur.

Vous pouvez modifier les paramètres par défaut à l'aide d'objets de stratégie de groupe Active Directory. Importez et ajoutez la Redirection HDX MediaStream Flash : modèle d'administration client (HdxFlashClient.adm), qui est disponible dans les dossiers suivants :

- Pour les ordinateurs 32 bits : %Program Files%\Citrix\ICA Client\Configuration\langue.
- Pour les ordinateurs 64 bits : %Program Files (x86)%\Citrix\ICA Client\Configuration\langue.

Les paramètres de stratégie s'affichent sous Modèles d'administration > Modèles d'administration classiques (ADM) > Redirection HDX MediaStream Flash - Client. Consultez la documentation Microsoft Active Directory pour obtenir des détails sur les objets de stratégie de groupe et les modèles.

Modifier le moment où la redirection Flash est utilisée

En conjonction avec les paramètres côté serveur, le paramètre de stratégie Activer la redirection HDX MediaStream Flash sur la machine utilisateur détermine si le contenu Adobe Flash est redirigé vers la machine utilisateur pour restitution locale. Par défaut, la redirection Flash est activée et utilise la détection réseau intelligente pour déterminer à quel moment lire le contenu Flash sur la machine utilisateur.

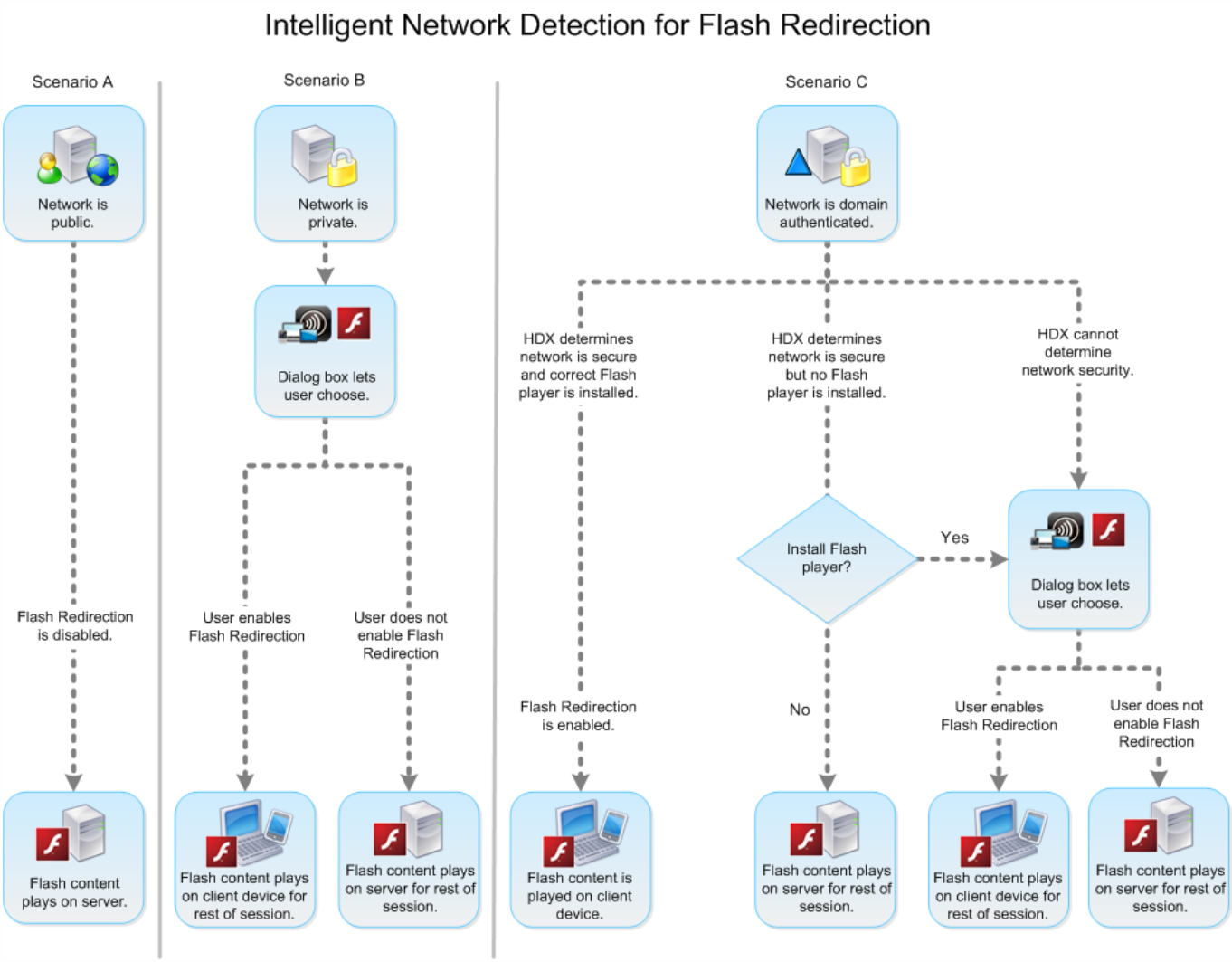
Si aucune configuration n'est définie et Desktop Lock est utilisé, la redirection Flash est activée sur la machine utilisateur par défaut.

Pour modifier le moment où la redirection Flash est utilisée ou pour désactiver la redirection Flash sur la machine utilisateur :

1. Dans la liste Paramètre, sélectionnez Activer la redirection Flash HDX MediaStream sur la machine utilisateur et cliquez sur paramètre de stratégie.
2. Sélectionnez Non configuré, Activé ou Désactivé.
3. Si vous sélectionnez Activé, choisissez une option dans la liste Utiliser la redirection HDX MediaStream Flash :
   - Pour utiliser la dernière version de la fonctionnalité de redirection Flash lorsque la configuration requise est présente, et retourner à la restitution côté serveur lorsqu'elle n'est pas utilisée, sélectionnez Uniquement avec la deuxième génération.
   - Pour toujours utiliser la redirection Flash, sélectionnez Toujours. Le contenu Flash est lu sur la machine utilisateur.
   - Pour ne jamais utiliser la redirection Flash, sélectionnez Jamais. Le contenu Flash est lu sur le serveur.

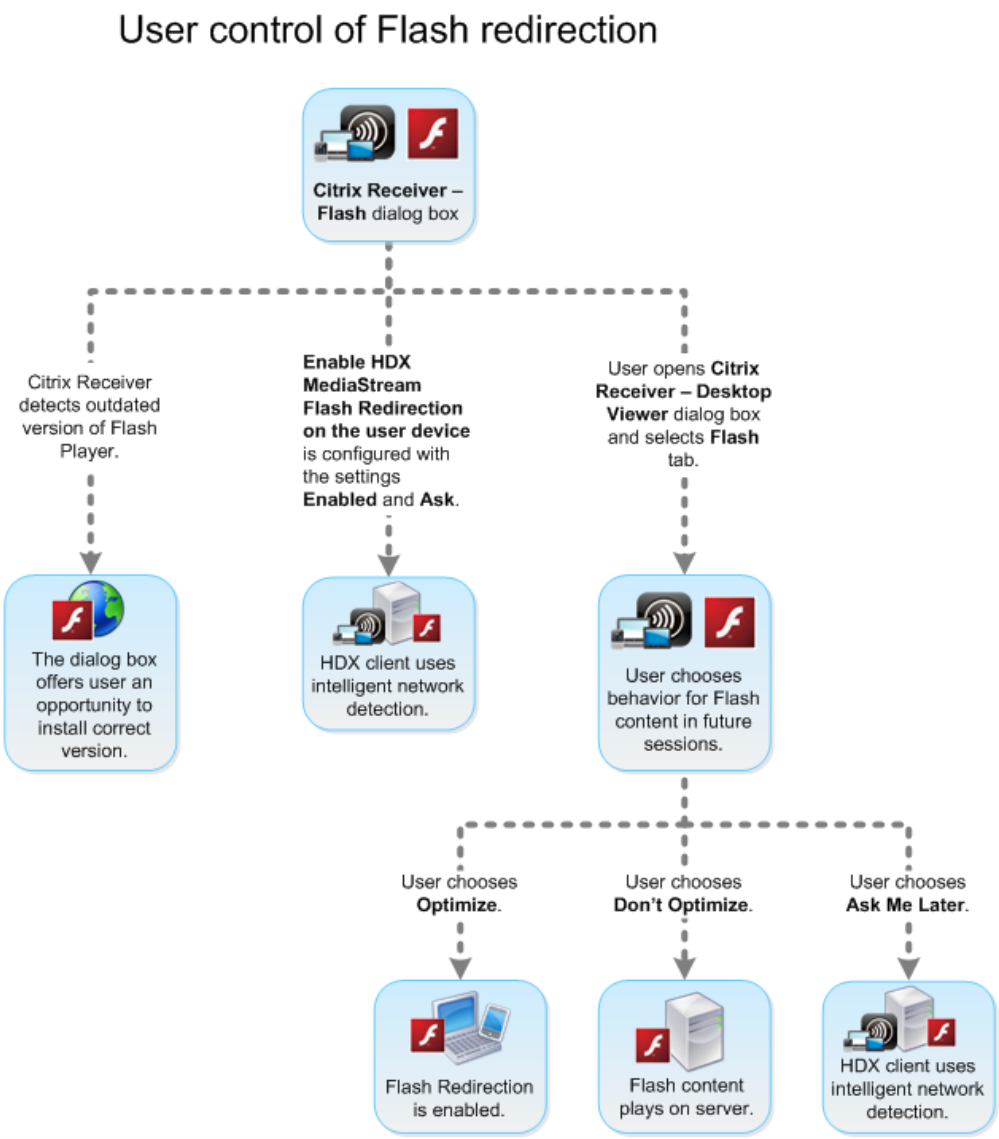
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Pour utiliser la détection réseau intelligente pour évaluer le niveau de sécurité du réseau côté client pour déterminer le moment où utiliser la redirection Flash est approprié, sélectionnez Demander (la valeur par défaut). Si la sécurité du réseau ne peut pas être déterminée, l'utilisateur est invité à utiliser la redirection Flash. Si le niveau de sécurité réseau ne peut pas être déterminé, l'utilisateur est invité à choisir d'utiliser la redirection Flash.
  L'illustration suivante indique comment la redirection Flash est prise en charge pour les différents types de réseau.



Les utilisateurs peuvent remplacer la détection réseau intelligente à partir de la boîte de dialogue Citrix Receiver : Préférences de Desktop Viewer, en sélectionnant Optimiser ou Ne pas Optimiser dans l'onglet Flash. Les choix disponibles varient en fonction de la manière dont la redirection Flash est configurée sur la machine utilisateur, comme illustré ci-dessous.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Synchroniser les cookies HTTP côté client avec ceux côté serveur

La synchronisation des cookies HTTP côté client avec ceux côté serveur est désactivée par défaut. Activez la synchronisation pour télécharger des cookies HTTP depuis le serveur ; ces cookies HTTP sont alors utilisés pour la récupération du contenu côté client et sont disponibles, pour des sites contenant du contenu Flash.
Remarque : les cookies côté client ne sont pas remplacés lors de la synchronisation ; ils restent disponibles même si la stratégie de synchronisation est désactivée plus tard.

1. Dans la liste Paramètre, sélectionnez Activer la synchronisation des cookies HTTP côté client avec ceux côté serveur et cliquez sur paramètre de stratégie.
2. Sélectionnez Non configuré, Activé ou Désactivé (valeur par défaut).

Activer la récupération de contenu côté serveur

Par défaut, la redirection Flash télécharge le contenu Flash vers la machine utilisateur où il est lu. L'activation de la récupération de contenu côté serveur provoque le téléchargement du contenu Flash vers le serveur, puis son envoi vers la machine utilisateur. À moins qu'il n'existe une stratégie de remplacement, telle qu'un site bloqué par le paramètre de stratégie Liste de compatibilité d'adresses URL Flash, le contenu Flash sera lu sur la machine utilisateur.

La récupération de contenu côté serveur est fréquemment utilisée lorsque la machine utilisateur se connecte à des sites internes via NetScaler Gateway et lorsque la machine utilisateur ne possède pas d'accès direct à Internet.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Remarque : la récupération de contenu côté serveur ne prend pas en charge les applications Flash qui utilisent le protocole RTMP (Real Time Messaging Protocol). Au lieu de cela, la restitution côté serveur est utilisée pour de tels sites.
La redirection Flash de deuxième génération prend en charge trois options, pour la récupération de contenu côté serveur. Deux de ces options permettent de mettre en cache du contenu côté serveur sur la machine utilisateur, ce qui améliore les performances car le contenu qui est réutilisé est déjà disponible sur la machine utilisateur pour restitution. le contenu présent dans ce cache est stocké séparément des autres contenus HTTP mis en cache sur la machine utilisateur.

Avec la redirection Flash de seconde génération, le retour vers la récupération de contenu côté serveur démarre automatiquement lorsque n'importe laquelle des options d'activation ci-dessus est sélectionnée et la récupération côté client de fichiers .swf échoue.

L'activation de la récupération de contenu côté serveur requiert des paramètres sur la machine cliente et le serveur.

1. Dans la liste Paramètre, sélectionnez Activer l'extraction de contenu côté serveur et cliquez sur paramètre de stratégie.
2. Sélectionnez Non configuré, Activé ou Désactivé (valeur par défaut). Si vous activez ce paramètre, choisissez une option dans la liste État de récupération de contenu côté serveur :

Option	Description
Désactivée	Désactive la récupération de contenu côté serveur et écrase le paramètre Liste d'URL de récupération de contenu Flash côté serveur sur le serveur. Le retour vers la récupération de contenu côté est également désactivé.
Activé	Active la récupération de contenu côté serveur pour les pages Web et les applications Flash identifiées dans la Liste d'URL de récupération de contenu Flash côté serveur. Retour vers la récupération de contenu côté serveur est disponible, mais le contenu Flash n'est pas mis en cache.
Activée (mise en cache permanente)	Active la récupération de contenu côté serveur pour les pages Web et les applications Flash identifiées dans la Liste d'URL de récupération de contenu Flash côté serveur. Le retour vers la récupération de contenu côté est disponible. Le contenu obtenu via la récupération de contenu côté serveur est mis en cache sur la machine utilisateur et stocké d'une session à l'autre.
Activée (mise en cache temporaire)	Active la récupération de contenu côté serveur pour les pages Web et les applications Flash identifiées dans la Liste d'URL de récupération de contenu Flash côté serveur. Le retour vers la récupération de contenu côté est disponible. Le contenu obtenu via la récupération de contenu côté serveur est mis en cache sur la machine utilisateur et supprimé à la fin de la session.

3. Sur le serveur, activez le paramètre de stratégie Liste d'URL de récupération de contenu Flash côté serveur et remplissez-le avec des adresses URL cibles.

Rediriger les machines utilisateur vers d'autres serveurs pour la récupération de contenu côté client

Pour rediriger une tentative d'obtention de contenu Flash à l'aide du paramètre Règles de réécriture d'URL pour la récupération de contenu côté client, qui est une fonctionnalité de redirection Flash de deuxième génération. Lors de la configuration de cette fonctionnalité, vous fournissez deux modèles d'adresse URL ; lorsque la machine utilisateur tente de récupérer du contenu provenant d'un site Web correspondant au premier modèle (le modèle d'adresse URL correspondant), le contenu est redirigé vers le site Web spécifié par le second modèle (le format de réécriture d'adresse

© 1999-2017 Citrix Systems, Inc. All rights reserved.

URL).

Vous pouvez utiliser ce paramètre pour pallier les déficiences des réseaux de diffusion de contenu (CDN). Certains sites Web qui diffusent du contenu Flash utilisent la redirection CDN pour permettre à l'utilisateur d'obtenir le contenu à partir du groupe de serveurs contenant le même contenu le plus proche. Lors de l'utilisation de la fonctionnalité de récupération de contenu côté client de la redirection Flash, le contenu Flash est requis auprès de la machine utilisateur, tandis que le reste de la page Web sur laquelle le contenu Flash réside est requis par le serveur. Si CDN est utilisé, la requête serveur est redirigée vers le serveur le plus proche et la requête de la machine utilisateur suit le même chemin. Notez que cette valeur peut ne pas représenter l'emplacement le plus proche de la machine utilisateur ; selon la distance, il peut exister un délai significatif entre le chargement de la page Web et la lecture du contenu Flash.

1. Dans la liste Paramètre, sélectionnez Règles de réécriture d'URL pour la récupération de contenu côté client et cliquez sur paramètre de stratégie.
2. Sélectionnez Non configurée, Activée ou Désactivée. Non configurée est la valeur par défaut ; Désactivée provoque l'ignorance de toutes les règles de réécriture d'URL configurées dans l'étape suivante.
3. Si vous activez ce paramètre, cliquez sur Afficher. À l'aide d'une syntaxe d'expression régulière Perl, saisissez le modèle de correspondance d'adresse URL dans la zone Nom de valeur et le format de réécriture d'adresse URL dans la zone Valeur.

Vous pouvez ajouter des paramètres de registre pour spécifier la version minimale requise pour la redirection Flash pour les machines clientes qui accèdent à des VDA à l'aide de Citrix Receiver pour Windows et Citrix Receiver pour Linux.

> ## Avertissement
>
> La modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter de réinstaller votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

ServerFlashPlayerVersionMinimum est une valeur de chaîne qui spécifie la version minimale du lecteur Flash Player sur le serveur ICA (VDA).

ClientFlashPlayerVersionMinimum est une valeur de chaîne qui spécifie la version minimale du lecteur Flash Player sur le client ICA (Citrix Receiver).

Ces chaînes de version peuvent être "10" ou "10.2" ou "10.2.140". Actuellement, seuls les numéros de version majeur, mineur et de build sont comparés. Le numéro de révision est ignoré. Par exemple, pour une chaîne de version de 10 avec spécification du numéro majeur uniquement, il est supposé que les numéros mineur et de build correspondent à zéro.

FlashPlayerVersionComparisonMask est une valeur DWORD qui, lorsqu'elle est définie sur 0, désactive la comparaison de la version du lecteur Flash Player sur le client ICA avec la version du lecteur Flash Player sur le serveur ICA. Le masque de comparaison a d'autres valeurs, mais ces dernières ne doivent pas être utilisées car la signification d'un masque autre que zéro peut changer. Il est recommandé de configurer le masque de comparaison sur zéro uniquement pour les clients souhaités. Il n'est pas recommandé de configurer le masque de comparaison sous les paramètres indépendants du client. Si un masque de comparaison n'est pas spécifié, la redirection Flash requiert que le client ICA ait un lecteur Flash Player de version supérieure ou égale à la version de Flash Player sur le serveur ICA. La comparaison s'effectue uniquement au niveau du numéro de version majeur du lecteur Flash.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour que la redirection s'effectue, les vérifications minimums de client et de serveur doivent réussir en plus de la vérification à l'aide du masque de comparaison.

La sous-clé ClientID0x51 spécifie le client ICA Linux. La sous-clé ClientID0x1 spécifie le client ICA Windows. Le nom de cette sous-clé est formé en ajoutant l'ID du produit client hexadécimal (sans les zéros du début) à la chaîne « ClientID ». Une liste complète des ID client est disponible dans la documentation Mobile SDK pour Windows Apps http://www.citrix.com/mobilitysdk/docs/clientdetection.html

Exemple de configuration de registre VDA 32 bits

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] Paramètres indépendants du client

"ClientFlashPlayerVersionMinimum"="13.0" Version minimum requise pour le client ICA
"ServerFlashPlayerVersionMinimum"="13.0" Version minimum requise pour le serveur ICA
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1] Paramètres du client ICA Windows

"ClientFlashPlayerVersionMinimum"="16.0.0" Spécifie la version minimum requise de Flash Player pour le client Windows
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51] Paramètres du client ICA Linux

"FlashPlayerVersionComparisonMask"=dword:00000000 : désactive la comparaison de version pour le client Linux (vérifie que le client a une version de Flash Player plus récente que le serveur) "ClientFlashPlayerVersionMinimum"="11.2.0" : spécifie la version minimum de Flash Player pour le client Linux.

Exemple de configuration de registre VDA 64 bits

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]

"ClientFlashPlayerVersionMinimum"="13.0" "ServerFlashPlayerVersionMinimum"="13.0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1]

"ClientFlashPlayerVersionMinimum"="16.0.0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51]

"FlashPlayerVersionComparisonMask"=dword:00000000 "ClientFlashPlayerVersionMinimum"="11.2.0"

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Accélération GPU pour OS de bureau Windows

Jul 15, 2016

Avec HDX 3D Pro vous pouvez mettre à disposition des applications au graphisme intensif dans le cadre des applications ou bureaux hébergés sur des machines avec OS de bureau. HDX 3D Pro prend en charge les ordinateurs hôtes physiques, (y compris les bureaux, les lames et les stations de travail en rack) et les VM XenServer avec GPU Passthrough et les machines virtuelles XenServer avec Virtual GPU (vGPU).

À l'aide de la fonctionnalité GPU Passthrough de XenServer, vous pouvez créer des VM bénéficiant d'un accès exclusif à du matériel de traitement graphique dédié. Vous pouvez installer plusieurs processeurs graphiques sur l'hyperviseur et affecter individuellement des VM à chacun de ces processeurs graphiques.

À l'aide de XenServer vGPU, plusieurs machines virtuelles peuvent accéder directement à la puissance de traitement graphique d'un processeur graphique physique unique. Le partage du matériel GPU offre des bureaux Windows 7 ou Windows 10 adaptés aux utilisateurs ayant des besoins complexes et exigeants en matière de design. Pris en charge pour les cartes NVIDIA GRID (voir NVIDIA GRID), le partage GPU utilise les mêmes pilotes graphiques NVIDIA que ceux déployés sur des systèmes d'exploitation non virtualisés. Également pris en charge pour les processeurs Intel de 5ème et 6ème génération avec Intel Iris Pro Graphics. Pour de plus amples informations sur ces familles de processeurs Intel, consultez Processeurs Intel Core de 5ème génération et Processeurs Intel Core de 6ème génération.

HDX 3D Pro offre les fonctionnalités suivantes :

- Compression approfondie H.264 adaptative pour des performances de réseau étendues et sans fil optimales. HDX 3D Pro utilise la compression poussée basée sur l'UC en tant que technique de compression par défaut pour le codage. Ceci offre une compression optimale qui s'adapte de manière dynamique aux conditions du réseau.
  Le codec de compression profonde H.264 n'est plus à la hauteur des graphiques restitués pour les noyaux CUDA sur le GPU NVIDIA. Le codec de compression profonde s'exécute sur l'UC et offre une efficacité de bande passante supérieure.

- Option de compression sans perte pour les cas d'utilisation spécialisés. HDX 3D Pro offre également un codec UC sans perte pour prendre en charge les applications pour lesquelles les graphiques gourmands en pixels sont nécessaires, comme l'imagerie médicale. La compression sans perte est recommandée uniquement pour les scénarios d'utilisation spécifiques car elle consomme davantage de ressources réseau et de traitement.
  Lors de l'utilisation de la compression sans perte :
  - L'indicateur sans perte, une icône dans la barre d'état système, vous avertit si l'écran affiché est une trame avec ou sans perte. Cela est utile lorsque le paramètre de stratégie Qualité visuelle spécifie Sans perte si possible. L'indicateur sans perte devient vert lorsque les images envoyées sont sans perte.
  - Le commutateur sans perte permet à l'utilisateur de passer en mode Toujours sans perte à tout moment dans la session. Pour sélectionner ou désélectionner le mode sans perte à tout moment au cours d'une session, cliquez avec le bouton droit sur l'icône ou utilisez le raccourci ALT + MAJ + 1.
    Pour la compression sans perte : HDX 3D Pro utilise le codec sans perte pour la compression quel que soit le codec sélectionné au travers de la stratégie.

    Pour la compression avec perte : HDX 3D Pro utilise le codec original, soit celui par défaut, soit celui sélectionné via la stratégie.

    les paramètres du commutateur Sans perte ne sont pas conservés pour les sessions ultérieures. Pour utiliser le codec sans perte pour chaque connexion, sélectionnez Toujours sans perte dans le paramètre de stratégie Qualité visuelle.

- Vous pouvez remplacer le raccourci par défaut, ALT+MAJ+1, pour sélectionner ou désélectionner Sans perte dans une session. Configurez un nouveau paramètre de registre pour HKLM\SOFTWARE\Citrix\HDX3D\LLIndicator.
  - Nom : HKLM_HotKey, Type : chaîne
  - Le format de configuration d'une combinaison de touches de raccourci est C=0|1, A=0|1, S=0|1, W=0|1, K=val. Les clés doivent être séparées par une virgule (,). L'ordre des touches n'est pas important.
  - A, C, S, W et K représentent des touches, où C=Contrôle, A=ALT, S=MAJ, W=Win et K=une touche valide. Les valeurs autorisées pour K sont 0-9, a-z, et tout code clavier virtuel. Pour de plus amples informations sur les codes clavier virtuel, consultez la section Virtual-Key Codes sur MSDN.
  - Par exemple :
    - Pour F10, définissez K=0x79
    - Pour Ctrl + F10, définissez C=1, K=0x79
    - Pour Alt + A, définissez A=1, K=a ou A=1, K=A ou K=A, A=1
    - Pour Ctrl + Alt + 5, définissez C=1, A=1, K=5 ou A=1, K=5, C=1
    - Pour Ctrl + Maj + F5, définissez A=1, S=1, K=0x74

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

- Prise en charge de multiples moniteurs haute résolution. Pour les bureaux Windows 10, 8 et 7, HDX 3D Pro prend en charge les machines utilisateur avec jusqu'à quatre moniteurs. Les utilisateurs peuvent organiser leurs moniteurs selon n'importe quelle configuration et peuvent combiner des moniteurs ayant différentes résolutions et orientations. Le nombre de moniteurs n'est limité que par les capacités du processeur graphique de l'ordinateur hôte, de la machine utilisateur et de la bande passante disponible. HDX 3D Pro prend en charge toutes les résolutions de moniteur et n'est limité que par les capacités du processeur graphique sur l'ordinateur hôte.
  HDX 3D Pro offre également une prise en charge limitée d'accès à plusieurs moniteurs pour les bureaux Windows XP. Pour de plus amples informations sur ce sujet, consultez la section VDA sur les machines exécutant Windows XP ou Windows Vista.

- Résolution dynamique. Vous pouvez redimensionner la fenêtre de bureau virtuel ou d'application sur n'importe quelle résolution. **Remarque** : la seule méthode prise en charge permettant de changer la résolution consiste à redimensionner la fenêtre de session VDA. La modification de la résolution dans une session VDA (à l'aide de Panneau de configuration > Apparence et personnalisation > Affichage > Résolution d'écran) n'est pas prise en charge.

- Prise en charge de l'architecture NVIDIA Kepler. HDX 3D Pro prend en charge les cartes NVIDIA GRID (voir NVIDIA GRID) pour GPU passthrough et le partage GPU. NVIDIA GRID vGPU permet à plusieurs machines virtuelles d'avoir un accès direct simultané à un GPU unique physique, à l'aide des mêmes pilotes graphiques NVIDIA qui sont déployés sur des systèmes d'exploitation non virtualisés.
- Prise en charge de VMware vSphere et VMware ESX à l'aide de l'accélération graphique virtuelle (vDGA) : vous pouvez utiliser HDX 3D Pro avec vDGA pour les RDS et les charges de travail VDI.
- Prise en charge des processeurs Intel de 5ème et 6ème génération avec graphiques Intel Iris Pro. HDX 3D Pro prend en charge plusieurs moniteurs (maximum de trois), l'occultation de la console, une résolution personnalisée et une haute fréquence d'images. Pour de plus amples informations sur les familles de processeurs Intel prises en charge, consultez Processeurs Intel Core de 5ème génération et Processeurs Intel Core de 6ème génération.

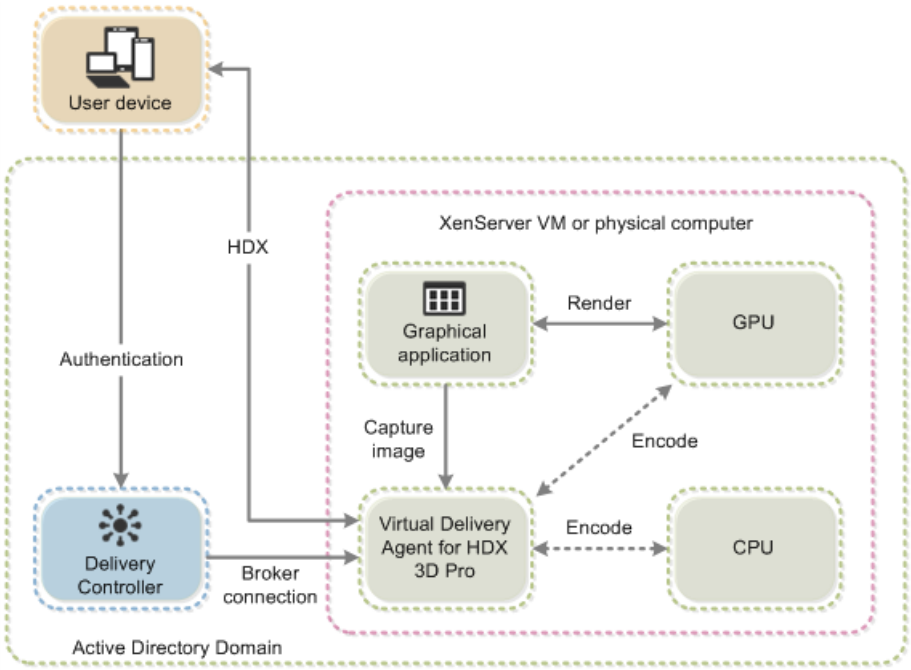
Comme indiqué dans l'illustration suivante :

- L'ordinateur hôte doit résider dans le même domaine Active Directory que le Delivery Controller.
- Lorsqu'un utilisateur ouvre une session sur Citrix Receiver et accède au bureau ou à l'application virtuelle, le Controller authentifie l'utilisateur et contacte le VDA pour HDX 3D Pro afin de négocier une connexion à l'ordinateur qui héberge l'application graphique.

  Le VDA pour HDX 3D Pro utilise le matériel approprié sur l'hôte pour compresser des vues du bureau complet ou de l'application graphique seule.

- Ces vues de bureau et d'application et les interactions de l'utilisateur avec elles sont transmises entre l'ordinateur hôte et la machine utilisateur via une connexion HDX directe entre Citrix Receiver et le VDA pour HDX 3D Pro.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Lorsque vous utilisez l'interface graphique du programme d'installation pour l'installation d'un VDA pour OS de bureau Windows, sélectionnez Oui sur la page HDX 3D Pro. Lors de l'utilisation de l'interface de ligne de commande, incluez l'option /enable_hdx_3d_pro avec la commande XenDesktop VdaSetup.exe.

Pour mettre à niveau HDX 3D Pro, désinstallez le composant HDX 3D for Professional Graphics et le VDA avant d'installer la dernière version de VDA pour HDX 3D Pro. De même, pour passer de l'édition standard de VDA pour OS Windows Desktop à VDA pour HDX 3D Pro, désinstallez le VDA standard, puis installez le VDA pour HDX 3D Pro.

L'API GRID NVIDIA offre un accès direct au tampon de trame du GPU, fournissant le taux de trame le plus rapide possible pour une expérience utilisateur fluide et interactive. Si vous installez des pilotes NVIDIA avant d'installer un VDA avec HDX 3D Pro, NVIDIA GRID est activé par défaut.

Pour activer NVIDIA GRID sur une VM, désactivez Microsoft Basic Display Adapter dans le Gestionnaire de périphériques. Exécutez la commande suivante, puis redémarrez le VDA : Montereyenable.exe -enable -noreset

Si vous installez des pilotes NVIDIA après avoir installé un VDA avec HDX 3D Pro, NVIDIA GRID est désactivé. Activez NVIDIA GRID à l'aide de l'outil Montereryenable fourni par NVIDIA.

Pour désactiver NVIDIA GRID, exécutez la commande suivante, puis redémarrez le VDA : Montereyenable.exe -disable -noreset

Cette étape est requise uniquement si vous installez des pilotes Intel après avoir installé un VDA avec HDX 3D Pro, ou si le pilote Intel a été mis à jour.

Afin d'activer les pilotes Intel requis pour la prise en charge de moniteurs multiples, exécutez la commande suivante à l'aide

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de GfxDisplayTool.exe, puis redémarrez le VDA : **GfxDisplayTool.exe -vd enable**

GfxDisplayTool.exe est inclus avec le programme d'installation du VDA. L'exécutable GfxDisplayTool.exe se trouve dans C:\Program Files\Citrix\ICAServices.

> ## Remarque
>
> La désinstallation des pilotes NVIDIA ou Intel dans les sessions ICA n'est pas prise en charge.

Pour utiliser HDX 3D Pro avec plusieurs moniteurs, assurez-vous que l'ordinateur hôte est configuré avec au moins autant de moniteurs que sont connectés aux machines utilisateur. Les moniteurs connectés à l'ordinateur hôte peuvent être physiques ou virtuels.

Ne connectez pas de moniteur (qu'il soit physique ou virtuel) à un ordinateur hôte alors qu'un utilisateur est connecté au bureau ou à l'application virtuel(le) fournissant l'application graphique. Car ceci peut provoquer une instabilité pour toute la durée de la session de l'utilisateur.

Faites savoir à vos utilisateurs que les modifications apportées à la résolution du bureau (par eux ou une application) ne sont pas prises en charge lorsqu'une session d'application graphique est en cours d'exécution. Après fermeture de la session d'application, un utilisateur peut modifier la résolution de la fenêtre Desktop Viewer dans Citrix Receiver : Préférences de Desktop Viewer.

Lorsque plusieurs utilisateurs partagent une connexion disposant d'une bande passante limitée (par exemple dans une succursale), Citrix vous recommande d'utiliser le paramètre de stratégie Limite de bande passante de session générale pour limiter la bande passante disponible pour chaque utilisateur. Cela évite les trop fortes fluctuations de la bande passante au fur et à mesure que les utilisateurs ouvrent une session ou se déconnectent. Comme HDX 3D Pro s'adapte automatiquement pour utiliser toute la bande passante disponible, de fortes variations de celle-ci pendant les sessions des utilisateurs peuvent avoir un impact négatif sur les performances.

Ainsi, si 20 utilisateurs partagent une connexion de 60 Mbps, la bande passante disponible pour chaque utilisateur peut varier entre 3 Mbps et 60 Mbps en fonction du nombre d'utilisateurs simultanés. Pour optimiser l'expérience utilisateur dans ce scénario, déterminez la bande passante requise par utilisateur aux heures de pointe et limitez en permanence les utilisateurs à cette valeur.

Pour les utilisateurs de souris 3D, Citrix recommande d'augmenter la priorité du canal virtuel Generic USB Redirection à 0. Pour plus d'informations sur la modification de la priorité du canal virtuel, consultez l'article CTX128190.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Accélération GPU pour OS de serveur Windows

Jul 07, 2016

HDX 3D Pro permet aux applications exigeantes en ressources graphiques exécutées dans de sessions d'OS de serveur Windows d'être restituées sur le processeur graphique du serveur (GPU). En déplaçant la restitution OpenGL, DirectX, Direct3D et Windows Presentation Foundation (WPF) sur le processeur graphique du serveur, l'unité centrale du serveur n'est pas ralentie par la restitution des graphiques. Par ailleurs, le serveur est capable de traiter davantage de graphiques car la charge est partagée entre le processeur graphique et l'unité centrale.

Lors de l'utilisation de HDX 3D Pro, plusieurs utilisateurs peuvent partager des cartes graphiques. Lorsque HDX 3D Pro est utilisé en conjonction avec la fonctionnalité GPU Pass-through de XenServer, un seul serveur héberge de multiples cartes graphiques, à raison d'une par machine virtuelle.

Pour les procédures qui impliquent la modification du registre, faites attention : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter de réinstaller votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

Le partage GPU active la restitution matérielle de l'unité de traitement graphique (GPU) des applications OpenGL et DirectX dans les sessions de bureau à distance ; il possède les caractéristiques suivantes :

- Peut être utilisée sur des machines bare metal ou virtuelles pour améliorer l'évolutivité et les performances des applications.
- Permet plusieurs sessions simultanées pour partager les ressources GPU (la plupart des utilisateurs ne requièrent pas les performances de restitution d'un processeur graphique dédié).
- Ne requiert aucun paramètre spécial.

Vous pouvez installer plusieurs processeurs graphiques sur un hyperviseur et affecter des VM à chacun de ces processeurs graphiques : soit installez une carte graphique possédant plus d'un processeur graphique, soit installez plusieurs cartes graphiques avec au moins un processeur graphique chacune. Le mélange de cartes graphiques hétérogènes sur le serveur n'est pas recommandé.

Les machines virtuelles requièrent un accès intermédiaire direct à un processeur graphique, qui est disponible avec Citrix XenServer ou VMware vSphere. Lorsque HDX 3D est utilisé avec un GPU Pass-through, chaque processeur graphique du serveur prend en charge une machine virtuelle multi-utilisateur.

Le partage GPU ne dépend pas d'une carte graphique spécifique.

- Lors de l'exécution sur un hyperviseur, sélectionnez une plate-forme matérielle et des cartes graphiques qui sont compatibles avec l'implémentation GPU Pass-through de votre hyperviseur. La liste matérielle qui a réussi le test de certification avec un GPU Pass-through XenServer est disponible dans la section Machines GPU Pass-through.
- Lors de l'exécution sur des machines bare metal, il est recommandé de n'activer qu'une seule carte vidéo par système d'exploitation. Si plusieurs processeurs graphiques sont installés sur le matériel, désactivez-les tous sauf un à l'aide de Device Manager.

L'évolutivité utilisant le partage GPU dépend de plusieurs facteurs :

- les applications étant exécutées ;
- la quantité de mémoire vive vidéo qu'elles consomment ;

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- la puissance de traitement de la carte graphique.

Par exemple, l'évolutivité se situe dans une plage de 8 à 10 utilisateurs signalés sur des cartes NVIDIA Q6000 et M2070Q exécutant des applications telles qu'ESRI ArcGIS. Ces cartes offrent 6 Go de mémoire vive vidéo. Les cartes NVIDIA GRID les plus récentes offrent 8 Go de mémoire vive vidéo et une puissance de traitement beaucoup plus élevée (plus de noyaux CUDA). Avec les cartes NVIDIA GRID K2, de bonnes performances ont été observées avec un maximum de 20 utilisateurs par carte GRID K2. D'autres applications peuvent évoluer de manière plus importante, jusqu'à 32 utilisateurs simultanés sur un processeur graphique haut de gamme.

certaines applications gèrent les insuffisances de RAM vidéo mieux que d'autres. Si le matériel devient extrêmement surchargé, ceci provoquera une instabilité ou un vidage du pilote de la carte graphique. Limitez le nombre d'utilisateurs simultanés pour éviter de tels problèmes.

Pour confirmer que l'accélération GPU se produit, utilisez un outil tiers tel que GPU-Z. GPU-Z est disponible à l'adresse http://www.techpowerup.com/gpuz/.

La restitution DirectX, Direct3D et WPF est uniquement disponible sur les serveurs dotés d'un processeur graphique prenant en charge les versions DDI 9ex, 10 ou 11.

- Sur Windows Server 2008 R2, DirectX et Direct3D ne requièrent aucun paramètre spécial pour utiliser un seul processeur graphique.
- Sur Windows Server 2012, les sessions de Services Bureau à distance (RDS) des sessions sur le serveur hôte de session Bureau à distance utilisent le pilote de rendu de base Microsoft en tant qu'adaptateur par défaut. Pour utiliser le processeur graphique dans les sessions de services Bureau à distance dans Windows Server 2012, activez le paramètre Utiliser la carte graphique matérielle par défaut pour toutes les sessions des services Bureau à distance dans la stratégie de groupe Stratégie ordinateur local > Configuration ordinateur > Modèles d'administration> Composants Windows > Services Bureau à distance > Hôte de la session Bureau à distance > Environnement de session à distance.
- Pour activer les applications WPF pour effectuer la restitution à l'aide du GPU du serveur, créez les paramètres suivants dans le registre du serveur exécutant les sessions de système d'exploitation Windows Server :
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\ Multiple Monitor Hook] "EnableWPFHook"=dword:00000001
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\ Multiple Monitor Hook] "EnableWPFHook"=dword:00000001

L'accélération GPU d'applications CUDA et OpenCL exécutées dans une session utilisateur est prise en charge à des fins d'évaluation uniquement. Cette prise en charge est désactivée par défaut, mais vous pouvez l'activer à des fins de test et d'évaluation.

Pour utiliser les fonctionnalités d'évaluation d'accélération CUDA, activez les paramètres de Registre suivants :

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA"=dword:00000001

Pour utiliser les fonctionnalités d'évaluation d'accélération OpenCL, activez les paramètres de Registre suivants :

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Accélération logicielle OpenGL

Jul 07, 2016

L'accélérateur logiciel OpenGL est un logiciel de rastérisation pour des applications OpenGL comme ArcGIS, Google Earth, Nehe, Maya, Fusion, Voxler, CAD et CAM. Dans certains cas, l'accélérateur logiciel OpenGL peut éliminer le besoin d'utiliser des cartes graphiques pour offrir une expérience utilisateur optimale avec des applications OpenGL.

Important : l'accélérateur logiciel OpenGL est fourni « tel quel », et doit être testé avec toutes les applications. Il risque de ne pas fonctionner avec certaines applications et a pour objectif d'apporter une solution au cas où le rastériseur Windows OpenGL ne fournirait pas des performances adéquates. Si l'accélérateur logiciel OpenGL fonctionne avec vos applications, il permet d'éviter des investissements coûteux en matériel GPU.

L'accélérateur OpenGL logiciel est fourni dans le dossier Support du support d'installation et est pris en charge sur toutes les plates-formes valides de VDA.

Quand utiliser l'accélérateur logiciel OpenGL ?

- Si les performances des applications OpenGL exécutées dans les machines virtuelles sur XenServer ou d'autres hyperviseurs posent un problème, essayez d'utiliser OpenGL Accelerator. Pour certaines applications, l'accélérateur OpenGL surpasse la rastérisation logicielle OpenGL de Microsoft qui est incluse avec Windows car l'accélérateur OpenGL tire parti de SSE4.1 et AVX. L'accélérateur OpenGL prend également en charge les applications à l'aide des versions OpenGL jusqu'à la version 2.1.
- Pour les applications exécutées sur une station de travail, essayez tout d'abord la version par défaut de la prise en charge OpenGL fournie par la carte graphique de la station de travail. Si la carte graphique possède la dernière version disponible, dans la plupart des cas, elle va mettre à disposition les meilleures performances possibles. Si la carte graphique est d'une version antérieure ou ne met pas à disposition des performances satisfaisantes, essayez alors d'utiliser l'accélérateur logiciel OpenGL.
- Les applications 3D OpenGL qui ne sont pas mises à disposition de manière adéquate à l'aide d'un logiciel de rastérisation sur l'UC peuvent bénéficier de l'accélération matérielle GPU OpenGL. Cette fonctionnalité peut être utilisée sur des machines bare metal ou virtuelles.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Fonctionnalités audio

Jul 07, 2016

Vous pouvez configurer et ajouter les paramètres de stratégie Citrix suivants pour une stratégie qui optimise les fonctionnalités audio HDX. Pour de plus amples informations sur l'utilisation et les relations et dépendances avec d'autres paramètres de stratégie, consultez la section Paramètres de stratégie audio et Paramètres de stratégie de bande passante et Paramètres de stratégie Connexions Multi-Stream.

Important : la plupart des fonctionnalités audio sont transportées à l'aide du flux ICA et sont sécurisées de la même façon que tout autre trafic ICA. L'audio UDP utilise un mécanisme de transport distinct et non sécurisé lorsque NetScaler Access Gateway ne se trouve pas sur le chemin. Si NetScaler Access Gateway est configuré pour accéder aux ressources XenApp et XenDesktop, le trafic audio entre la machine de point de terminaison et NetScaler Access Gateway est sécurisé à l'aide du protocole DTLS.

En règle générale, une qualité sonore plus élevée consomme plus de bande passante et a une utilisation de l'UC serveur supérieure par le volume des données audio envoyées aux machines utilisateur. La compression du son vous permet d'équilibrer la qualité sonore sur les performances générales de session ; utilisez les paramètres de stratégie Citrix pour configurer les niveaux de compression à appliquer aux fichiers sonores.

Par défaut, le paramètre de stratégie de qualité audio est défini sur Élevée : audio à définition élevée. Ce paramètre offre une qualité audio stéréo haute fidélité mais consomme plus de bande passante que les autres paramètres de qualité audio. N'utilisez pas cette qualité audio pour les chats vocaux ou les applications de chat vidéo (par exemple téléphones logiciels) non optimisés, car elle risque d'introduire une latence dans le chemin audio ne convenant pas aux communications en temps réel.

Considérez la création de stratégies distinctes pour des groupes d'utilisateurs se connectant par modem et pour des groupes d'utilisateurs se connectant via un réseau local ou étendu. Pour les connexions par modem, pour lesquelles la bande passante est généralement limitée, la vitesse de téléchargement est souvent plus importante pour les utilisateurs que la qualité sonore. Il se peut que vous souhaitiez créer une stratégie pour les connexions par modem, qui applique des niveaux de compression audio élevés et une stratégie pour les connexions via réseau local où étendu, qui applique un niveau de compression moins élevé.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie audio. N'oubliez pas d'activer les Paramètres audio du client sur la machine utilisateur ; voir Stratégies de configuration audio pour les machines utilisateur.

Pour autoriser des utilisateurs à recevoir l'audio d'une application sur un serveur au travers de haut-parleurs ou autres périphériques audio, (tels que des casques) sur la machine utilisateur, ajoutez le paramètre Redirection audio du client, qui est autorisé par défaut.

Le mappage audio du client peut provoquer une charge importante sur les serveurs et le réseau ; toutefois, l'interdiction de la redirection audio du client désactive toutes les fonctionnalités HDX audio.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie audio. N'oubliez pas d'activer les paramètres audio du client sur la machine utilisateur ; voir Stratégies de configuration audio pour les machines utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour permettre aux utilisateurs d'enregistrer de l'audio à l'aide de périphériques d'entrée tels que des microphones sur la machine utilisateur, ajoutez le paramètre Redirection du microphone client, qui est autorisé par défaut.

Pour des raisons de sécurité, les utilisateurs sont avertis si des serveurs non approuvés par leurs machines utilisateur essaient d'accéder à leurs microphones et peuvent choisir d'autoriser ou de refuser l'accès avant d'utiliser le microphone. Les utilisateurs peuvent désactiver cette alerte sur Citrix Receiver.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie audio. N'oubliez pas d'activer les Paramètres audio du client sur la machine utilisateur ; voir Stratégies de configuration audio pour les machines utilisateur.

Le paramètre de stratégie Plug N Play audio permet d'autoriser ou d'empêcher l'utilisation de plusieurs périphériques audio pour enregistrer et lire les sons. Cette option est activée par défaut.

Ce paramètre s'applique uniquement aux machines équipées du système d'exploitation Windows Server.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie audio.

Le paramètre de stratégie de Limite de bande passante de redirection audio spécifie la bande passante maximale (en kilobits par seconde) pour la lecture et l'enregistrement audio dans une session. Le paramètre Pourcentage de limite de bande passante de la redirection audio spécifie la bande passante maximale pour la redirection audio sous forme de pourcentage de la bande passante totale disponible. Par défaut, aucun maximum (zéro) n'est spécifié pour les deux paramètres. Si les deux paramètres sont configurés, celui possédant la limite de bande passante la plus basse est utilisé.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie de bande passante. N'oubliez pas d'activer les Paramètres audio du client sur la machine utilisateur ; voir Stratégies de configuration audio pour les machines utilisateur.

Par défaut, Transport en temps réel audio via UDP est Autorisé (s'il est sélectionné au moment de l'installation), ouvrant un port UDP sur le serveur pour les connexions qui utilisent le transport en temps réel audio via UDP. Citrix recommande de configurer l'audio UDP/RTP pour vous assurer la meilleure expérience utilisateur possible dans le cas d'une surcharge du réseau ou une perte de paquets.
Important : les données audio transmises via UDP ne sont pas cryptées lorsque NetScaler Access Gateway ne se trouve pas sur le chemin. Si NetScaler Access Gateway est configuré pour accéder aux ressources XenApp et XenDesktop, le trafic audio entre la machine de point de terminaison et NetScaler Access Gateway est sécurisé à l'aide du protocole DTLS.
La Plage de port UDP audio spécifie la plage de numéros de ports que le Virtual Delivery Agent (VDA) utilise pour échanger des données de paquet audio avec la machine utilisateur.

Par défaut, la plage se situe entre 16500 et 16509.

Pour plus d'informations sur le paramètre Transport en temps réel audio via UDP, voir Paramètres de stratégie audio ; pour plus de détails sur Plage de port UDP audio, veuillez consulter la section Paramètres de stratégie Connexions Multi-Stream. N'oubliez pas d'activer les Paramètres audio du client sur la machine utilisateur ; voir Stratégies de configuration audio pour les machines utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Chargez les modèles de stratégie de groupe en suivant les instructions de Configuration de Receiver avec le modèle d'objet de stratégie de groupe.
2. Dans l'éditeur de stratégie de groupe, développez Modèles d'administration > Composants Citrix > Citrix Receiver > Expérience utilisateur.
3. Pour les **paramètres audio du client**, sélectionnez **Non configuré**, **Activé** ou **Désactivé**.
   - **Non configuré**. Par défaut, la redirection audio est activée avec une qualité audio supérieure ou des paramètres audio personnalisés configurés précédemment.
   - **Activé**. La redirection audio est activée avec les options sélectionnées.
   - **Désactivé**. La redirection audio est désactivée.
4. Si vous sélectionnez **Activé**, choisissez une qualité audio. Pour l'audio UDP, utilisez **Moyen** (valeur par défaut).
5. Pour l'audio UDP, sélectionnez **Activer transport en temps réel** et définissez la plage de ports entrants à ouvrir dans le pare-feu Windows.
6. Pour utiliser l'audio UDP avec NetScaler Access Gateway, sélectionnez **Autoriser le transport en temps réel via NetScaler Gateway**. NetScaler Access Gateway doit être configuré avec DTLS. Pour de plus amples informations, consultez la section Audio UDP via un NetScaler Gateway.

En tant qu'administrateur, si vous n'avez pas de contrôle sur les machines de point de terminaison pour effectuer ces modifications, par exemple dans le cas de BYOD ou d'ordinateurs personnels, utilisez le fichier des attributs default.ica de StoreFront pour activer l'audio UDP.

1. Sur la machine StoreFront, ouvrez C:\inetpub\wwwroot\Citrix\\App_Data\default.ica à l'aide d'un éditeur de texte tel que Bloc-notes.
2. Ajoutez les entrées ci-dessous dans la section [Application].

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
; This is to enable Real-Time Transport

EnableRtpAudio=true

; This is to Allow Real-Time Transport Through gateway

EnableUDPThroughGateway=true

; This is to set audio quality to Medium

AudioBandwidthLimit=1-

; UDP Port range

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509
```

Si l'audio UDP est activé en modifiant le fichier default.ica, l'audio UDP est activé pour tous les utilisateurs qui utilisent ce magasin.

Les utilisateurs dans des conférences audio ou vidéo peuvent entendre un écho. Des échos se produisent généralement lorsque les haut-parleurs et les microphones sont trop proches l'un de l'autre. Pour cette raison, Citrix recommande l'utilisation de casques pour les conférences audio et vidéo.

HDX offre une option d'annulation de l'écho (activée par défaut), qui réduit l'écho. L'efficacité de l'annulation de l'écho est liée à la distance entre les haut-parleurs et le microphone ; les périphériques ne doivent pas se trouver trop proches ou trop éloignés l'un de l'autre.

Vous pouvez modifier un paramètre de registre pour désactiver l'annulation de l'écho. Lorsque vous travaillez dans le registre, faites très attention : la modification du Registre peut entraîner de sérieux problèmes qui pourraient nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

1. À l'aide de l'Éditeur du Registre sur la machine utilisateur, sélectionnez l'une des options suivantes :
   - Ordinateurs 32 bits : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
   - Ordinateurs 64 bits: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
2. Modifiez le champ de données Valeur sur FALSE.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Priorités du trafic réseau

Jul 07, 2016

Les priorités sont attribuées au trafic réseau sur plusieurs connexions pour une session à l'aide de routeurs prenant en charge la qualité de service (QoS). Quatre flux TCP/IP (en temps réel, interactifs, arrière-plan et en bloc) et un flux UDP/RTP (pour la voix) sont disponibles pour transporter le trafic ICA entre la machine utilisateur et le serveur. Chaque canal virtuel est associé à une priorité spécifique et transporté dans la connexion correspondante. Vous pouvez définir les canaux indépendamment, en fonction du numéro de port TCP utilisé pour la connexion.

Les connexions en streaming de canal multiples sont prises en charge pour les Virtual Delivery Agents (VDA) installés sur les machines Windows 8 et Windows 7. Travaillez avec votre administrateur réseau pour vous assurer que les ports CGP configurés dans le paramètre Stratégie Multi-Port sont correctement attribués sur les routeurs réseau.

La qualité de service n'est prise en charge que lorsque des ports de fiabilité de session multiples, ou des ports CGP, sont configurés.

Avertissement : lors de l'utilisation de cette fonctionnalité, assurez-vous que le transport est sécurisé. Citrix vous recommande d'utiliser Internet Protocol Security (IPsec) ou Transport Layer Security (TLS). Les connexions TLS sont prises en charge uniquement lorsque les connexions traversent une passerelle NetScaler Gateway qui prend en charge multi-stream. Sur un réseau d'entreprise interne, les connexions multi-stream avec TLS ne sont pas prises en charge.
Pour définir la qualité de service pour plusieurs connexions en streaming, ajoutez les paramètres de stratégie Citrix suivants pour une stratégie (voir Paramètres de stratégie Connexions Multi-Stream pour plus de détails) :

- Stratégie Multi-Port : ce paramètre spécifie les ports pour le trafic ICA au travers de plusieurs connexions et établit des priorités de réseau.
  - Sélectionnez une priorité dans la liste Priorité de port CGP par défaut ; par défaut, le port principal (2598) a une priorité Élevée.
  - Entrez des ports CGP supplémentaires dans Port1 CGP, port2 CGP et port3 CGP le cas échéant et attribuez-leur des priorités. Chaque port doit disposer d'une priorité unique.

  Configurez explicitement les pare-feu sur les VDA pour autoriser le trafic TCP supplémentaire.

- Paramètre d'ordinateur Multi-Stream : ce paramètre est désactivé par défaut. Si vous utilisez Citrix Cloudbridge avec prise en charge Multi-Stream dans votre environnement, vous n'avez pas besoin de configurer ce paramètre. Configurez ce paramètre de stratégie lorsque vous utilisez des routeurs tiers ou des Branch Repeater d'ancienne génération pour réaliser la qualité de service désirée.
- Paramètre utilisateur Multi-Stream : ce paramètre est désactivé par défaut.

Pour que les stratégies contenant ces paramètres soient appliquées, les utilisateurs doivent fermer leur session, puis ouvrir une session sur le réseau.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Considérations USB et de lecteur client

Jul 07, 2016

À l'aide de la redirection de périphérique USB HDX, un utilisateur peut connecter un lecteur flash à un ordinateur local et y accéder à distance à partir d'un bureau virtuel où d'une application hébergée de bureau. Pendant une session, les utilisateurs peuvent utiliser des périphériques plug-and-play, y compris des périphériques Picture Transfer Protocol (PTP), tels que des appareils photo numériques, des périphériques MTP (Media Transfer Protocol), tels que des lecteurs audio numériques ou lecteurs multimédias portables et des périphériques de point de vente (POS).

Le périphérique USB double-hop n'est pas pris en charge pour les sessions d'application hébergée de bureau.

La redirection USB est disponible pour Citrix Receiver pour Windows et Citrix Receiver pour Linux.

Par défaut, la redirection USB est autorisée pour certaines classes de périphériques USB et refusée pour d'autres ; veuillez consulter la documentation relative à Citrix Receiver pour plus de détails. Vous pouvez limiter les types de périphériques USB disponibles pour un bureau virtuel en mettant à jour la liste des périphériques USB pris en charge pour la redirection.

> **Important**
>
> dans les environnements dans lesquels la séparation de la sécurité entre la machine utilisateur et le serveur est nécessaire, fournissez des instructions aux utilisateurs sur les types de périphériques USB à éviter.

Des canaux virtuels optimisés sont disponibles pour rediriger les périphériques USB les plus populaires. Ils améliorent les performances et la bande passante via un réseau étendu. Le niveau de prise en charge fourni dépend du Citrix Receiver installé sur la machine utilisateur. Les canaux virtuels optimisés sont généralement la meilleure option, notamment dans les environnements à latence élevée.

À des fins de redirection USB, le produit utilise une carte intelligente SMART identique à celle de la souris.

Le produit prend en charge l'utilisation de canaux virtuels optimisés avec des périphériques USB 3.0 et des ports USB 3.0, tel qu'un canal virtuel CDM (utilisé pour visualiser des fichiers sur une caméra ou pour fournir l'audio à un casque). Le produit prend également en charge la redirection USB générique de périphériques USB 3.0 connectés à un port USB 2.0.

Les périphériques spécialisés pour lesquels il n'existe aucun canal virtuel optimisé sont pris en charge grâce à l'utilisation d'un canal virtuel USB générique qui fournit une redirection USB brute. Pour plus d'informations sur les périphériques USB testés avec XenDesktop, veuillez consulter l'article CTX123569.

Certaines des fonctionnalités spécifiques avancées, telles que les boutons des périphériques d'interface utilisateur (HID) sur une webcam, peuvent ne pas fonctionner correctement avec le canal virtuel optimisé ; si vous rencontrez ce problème, utilisez le canal virtuel USB générique.

Certains périphériques ne sont pas redirigés par défaut et sont uniquement disponibles pour la session locale. Par exemple, il n'est pas approprié de rediriger une carte d'interface réseau qui est connectée à la carte système de la machine utilisateur par USB interne.

Les paramètres de stratégie Citrix suivants contrôlent la prise en charge USB :

- **Règles d'optimisation de périphérique USB client**. Le mode d'optimisation est pris en charge pour les périphériques d'entrée de classe=03, les périphériques de signature numérique et les tablettes graphiques par exemple. Si aucune règle n'est spécifiée, le périphérique est traité en mode interactif (02). Le mode capture (04) est la méthode recommandée pour les périphériques de signature.
- **Redirection de périphérique USB client** : La valeur par défaut est Interdit.
- **Règles de redirection de périphérique USB client** : les règles s'appliquent uniquement à l'aide de la redirection de périphériques USB génériques ; par conséquent, les règles ne sont pas appliquées aux périphériques à l'aide d'une redirection spécialisée ou optimisée, comme CDM.
- **Redirection de périphérique Plug and Play USB client** : la valeur par défaut est Autorisé, pour permettre le plug-and-play de périphériques PTP, MTP et POS dans une session utilisateur.
- **Limite de bande passante de redirection du périphérique USB client** : la valeur par défaut est 0 (aucun maximum).
- **Pourcentage de limite de bande passante de redirection du périphérique USB client** : la valeur par défaut est 0 (aucun maximum).

La redirection USB générique est destinée aux périphériques USB spécialisés pour lesquels il n'existe aucun canal virtuel optimisé. Cette fonctionnalité redirige les périphériques USB arbitraires depuis les machines clientes vers des bureaux virtuels ; avec cette nouvelle fonctionnalité, les utilisateurs finaux ont la possibilité d'interagir avec une large sélection de périphériques USB génériques dans la session de bureau comme si les périphériques étaient physiquement connectés.

Avec la redirection USB générique :

- Il n'est pas nécessaire pour les utilisateurs d'installer des pilotes de périphériques sur la machine utilisateur.
- Les pilotes clients USB sont installés sur la machine VDA.

Cette fonctionnalité est prise en charge pour les sessions de bureau à compter de VDA pour OS de bureau, version 7.6 au minimum.

Cette fonctionnalité est également prise en charge pour les sessions de bureau à compter de VDA pour OS de serveur, version 7.6 au minimum, avec les restrictions suivantes :

- La machine VDA doit exécuter Windows Server 2012 R2.
- Seuls les scénarios à relais unique (single-hop) sont pris en charge.
- Les pilotes clients USB doivent être compatibles avec RDSH pour Windows 2012 R2.
- Les périphériques de stockage USB, périphériques audio, lecteurs de carte à puce et périphériques qui ne sont pas complètement virtualisés ne sont pas pris en charge.

Pour plus d'informations sur la configuration de la redirection USB générique, consultez CTX137939.

1. Ajoutez le paramètre Redirection de périphérique USB client à une stratégie et définissez sa valeur sur Autorisé.
2. (Facultatif). Pour mettre à jour la liste des périphériques USB disponibles pour l'accès à distance, ajoutez le paramètre Règles de redirection de périphérique USB client à une stratégie et spécifiez les règles de stratégie USB.
3. Activez la prise en charge USB lorsque vous installez Citrix Receiver sur les machines utilisateur. Si vous avez spécifié des règles de stratégie USB pour le VDA à l'étape précédente, spécifiez les mêmes règles de stratégie pour Citrix Receiver. pour les clients légers, consultez le fabricant pour obtenir des détails sur la prise en charge USB et sur la configuration requise.

Les périphériques USB sont automatiquement redirigés lorsque la prise en charge USB est activée et que les paramètres de préférences de l'utilisateur USB sont définis pour la connexion automatique aux périphériques USB. Les périphériques USB sont également automatiquement redirigés lorsqu'ils se trouvent en mode Desktop Appliance et que la barre de connexion est absente. Dans certaines

© 1999-2017 Citrix Systems, Inc. All rights reserved.

instances, cependant, il se peut que vous ne souhaitiez pas rediriger automatiquement tous les périphériques USB. Pour obtenir davantage d'informations, veuillez consulter la section CTX123015.

Les utilisateurs peuvent rediriger explicitement les périphériques qui ne sont pas automatiquement redirigés en les sélectionnant dans la liste des périphériques USB. Pour empêcher les périphériques USB d'être répertoriés ou redirigés, vous pouvez spécifier des règles de périphérique sur le client et sur le VDA, comme expliqué ci-dessous.

Vous pouvez mettre à jour la liste des périphériques USB disponibles pour l'accès à distance en spécifiant les règles de redirection de périphérique USB pour Citrix Receiver et le VDA pour remplacer les règles de stratégie USB par défaut.

- Modifiez le registre de la machine utilisateur. Un modèle administratif (fichier ADM) est inclus dans le support d'installation pour vous permettre d'effectuer des modifications sur la machine utilisateur via une stratégie de groupe Active Directory : dvd root \os\lang\Support\Configuration\icaclient_usb.adm.
- Modifiez les règles de remplacement de l'administrateur pour les machines avec OS de serveur à l'aide de règles de stratégie de groupe. La console de gestion des stratégies de groupe est incluse sur le support d'installation :
  - Pour x64 : dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - Pour x86 : dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

Avertissement

La modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

Les règles par défaut du produit sont stockées dans HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. ne modifiez pas les règles par défaut du produit. Au lieu de cela, utilisez-les pour créer des règles de remplacement de l'administrateur comme expliqué ci-dessous. Les règles de remplacement d'objets de stratégie de groupe de substitution sont évaluées avant les règles par défaut du produit.

Les règles de remplacement de l'administrateur sont stockées dans HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules. Les règles de stratégies GPO sont au format {Allow:|Deny:} et sont suivies d'un ensemble d'expressions tag=value (balise=valeur) séparées par des espaces. Les balises suivantes sont prises en charge :

Balise	Description
VID	ID fournisseur du descripteur de périphérique
PID	ID de produit du descripteur de périphérique
REL	ID de version du descripteur de périphérique
Class	Classe du descripteur de périphérique ou d'un descripteur d'interface ; veuillez consulter le site Web USB sur http://www.usb.org/ pour les codes de classe USB disponibles
SubClass	Sous-classe du descripteur de périphérique ou d'un descripteur d'interface
Prot	Protocole à partir du descripteur de périphérique ou d'un descripteur d'interface

Lors de la création de nouvelles règles de stratégies, tenez compte de ce qui suit.

- Les règles ne sont pas sensibles à la casse.
- Les règles peuvent éventuellement comporter un commentaire, introduit par #, à la fin. Aucun délimiteur n'est requis et le commentaire est ignoré en cas de correspondance.
- Les espaces vides et les lignes de commentaires pures sont ignorés.
- L'espace est utilisé comme séparateur, mais il ne peut pas apparaître au milieu d'un nombre ou d'un identificateur. Par exemple, Deny: Class = 08 SubClass=05 est une règle valide, mais Deny: Class=0 Sub Class=05 ne l'est pas.
- Les balises doivent utiliser l'opérateur de correspondance =. Par exemple, VID=1230.
- Chaque règle doit commencer sur une nouvelle ligne ou faire partie d'une liste séparée par des points-virgules.

Important

si vous utilisez le fichier modèle ADM, vous devez créer des règles sur une seule ligne sous forme de liste séparée par des points-virgules.

Lors de l'utilisation de machines optimisées, tels que le stockage de masse, vous redirigez habituellement la machine à l'aide d'un canal CDM spécialisé, plutôt qu'avec des règles de stratégie. Toutefois, vous pouvez ignorer ce comportement à l'aide de l'une des méthodes suivantes :

- Redirigez manuellement le périphérique optimisé à l'aide de la redirection USB générique, en choisissant Basculer en mode générique dans l'onglet Périphériques de la boîte de dialogue Préférences.
- Redirigez automatiquement le périphérique optimisé à l'aide de la redirection USB générique, en définissant la redirection automatique du périphérique de stockage (par exemple, AutoRedirectStorage = 1) et en définissant les paramètres de préférences de l'utilisateur USB afin de se connecter automatiquement aux périphériques USB ; pour de plus amples informations, consultez l'article CTX123015.

Exemples :

- Cet exemple illustre une règle de stratégie USB définie par l'administrateur pour des identificateurs de fabricant et de produit :
  Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products
- Cet exemple illustre une règle de stratégie USB définie par l'administrateur pour une classe, une sous-classe et un protocole définis :
  Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices

Par défaut, les périphériques USB sont automatiquement redirigés lorsque la prise en charge USB est activée et que les paramètres de préférences de l'utilisateur USB sont définis pour la connexion automatique aux périphériques USB. Les périphériques USB sont également automatiquement redirigés pour les sites Desktop Appliance ou les applications hébergées de bureau. Dans certaines instances, cependant, il se peut que vous ne souhaitiez pas rediriger automatiquement tous les périphériques USB. Pour obtenir davantage d'informations, veuillez consulter la section CTX123015.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Les utilisateurs Desktop Viewer peuvent rediriger les périphériques qui ne sont pas automatiquement redirigés en les sélectionnant dans la liste des périphériques USB. Pour empêcher les périphériques USB d'être répertoriés ou redirigés, spécifiez des règles de périphérique sur la machine utilisateur et le VDA.

Vous pouvez mettre à jour la liste des périphériques USB disponibles pour l'accès à distance en spécifiant les règles de redirection de périphérique USB pour Citrix Receiver et le VDA pour remplacer les règles de stratégie USB par défaut. Les règles sont appliquées pour Citrix Receiver et le VDA. Veillez à modifier toutes les deux afin que l'accès à distance au périphérique fonctionne comme vous le souhaitez.

- Modifiez le registre de la machine utilisateur (ou les fichiers .ini dans le cas de Citrix Receiver pour Linux). Un modèle administratif (fichier ADM) est inclus dans le support d'installation pour vous permettre d'effectuer des modifications sur la machine utilisateur via une stratégie de groupe Active Directory : dvd root \os\lang\Support\Configuration\icaclient_usb.adm.
- Modifiez les règles de remplacement de l'administrateur dans le registre VDA sur les machines avec OS de serveur. Un fichier ADM est inclus dans le support d'installation pour vous permettre d'effectuer des modifications sur le VDA via une stratégie de groupe Active Directory : dvd root \os\lang\Support\Configuration\vda_usb.adm.

Avertissement

La modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

Les règles par défaut du produit sont stockées dans HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. ne modifiez pas les règles par défaut du produit. Au lieu de cela, utilisez-les pour créer des règles de remplacement de l'administrateur comme expliqué ci-dessous. Les règles de remplacement d'objets de stratégie de groupe de substitution sont évaluées avant les règles par défaut du produit.

Les règles de remplacement de l'administrateur sont stockées dans HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules. Les règles de stratégies GPO sont au format {Allow:|Deny:} et sont suivies d'un ensemble d'expressions tag=value (balise=valeur) séparées par des espaces. Les balises suivantes sont prises en charge :

Balise	Description
VID	ID fournisseur du descripteur de périphérique
PID	ID de produit du descripteur de périphérique
REL	ID de version du descripteur de périphérique
Class	Classe du descripteur de périphérique ou d'un descripteur d'interface ; veuillez consulter le site Web USB sur http://www.usb.org/ pour les codes de classe USB disponibles
SubClass	Sous-classe du descripteur de périphérique ou d'un descripteur d'interface
Prot	Protocole à partir du descripteur de périphérique ou d'un descripteur d'interface

Lors de la création de nouvelles règles de stratégies, tenez compte de ce qui suit.

- Les règles ne sont pas sensibles à la casse.
- Les règles peuvent éventuellement comporter un commentaire, introduit par #, à la fin. Aucun délimiteur n'est requis et le commentaire est ignoré en cas de correspondance.
- Les espaces vides et les lignes de commentaires pures sont ignorés.
- L'espace est utilisé comme séparateur, mais il ne peut pas apparaître au milieu d'un nombre ou d'un identificateur. Par exemple, Deny: Class = 08 SubClass=05 est une règle valide, mais Deny: Class=0 Sub Class=05 ne l'est pas.
- Les balises doivent utiliser l'opérateur de correspondance =. Par exemple, VID=1230.
- Chaque règle doit commencer sur une nouvelle ligne ou faire partie d'une liste séparée par des points-virgules.

Important

si vous utilisez le fichier modèle ADM, vous devez créer des règles sur une seule ligne sous forme de liste séparée par des points-virgules.

Lors de l'utilisation de machines optimisées, tels que le stockage de masse, vous redirigez habituellement la machine à l'aide d'un canal CDM spécialisé, plutôt qu'avec des règles de stratégie. Toutefois, vous pouvez ignorer ce comportement à l'aide de l'une des méthodes suivantes :

- Redirigez manuellement le périphérique optimisé à l'aide de la redirection USB générique, en choisissant Basculer en mode générique dans l'onglet Périphériques de la boîte de dialogue Préférences.
- Redirigez automatiquement le périphérique optimisé à l'aide de la redirection USB générique, en définissant la redirection automatique du périphérique de stockage (par exemple, AutoRedirectStorage = 1) et en définissant les paramètres de préférences de l'utilisateur USB afin de se connecter automatiquement aux périphériques USB ; pour de plus amples informations, consultez l'article CTX123015.

Exemples :

- Cet exemple illustre une règle de stratégie USB définie par l'administrateur pour des identificateurs de fabricant et de produit :
  Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products
- Cet exemple illustre une règle de stratégie USB définie par l'administrateur pour une classe, une sous-classe et un protocole définis :
  Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices

Les utilisateurs peuvent se connecter un périphérique USB avant ou après le démarrage d'une session virtuelle.

Lors de l'utilisation de Citrix Receiver pour Windows, ce qui suit s'applique :

- Les périphériques connectés après démarrage d'une session apparaissent immédiatement dans le menu USB de Desktop Viewer.
- Si un périphérique USB n'est pas correctement redirigé, vous pouvez essayer de résoudre le problème en attendant que la session virtuelle ait démarré avant de connecter le périphérique.
- Pour éviter la perte de données, utilisez l'icône « Retirer le périphérique en toute sécurité » Windows avant de supprimer le périphérique USB.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour les périphériques de stockage de masse uniquement, l'accès distant est également disponible au travers du mappage de lecteurs clients, où les lecteurs de la machine utilisateur sont automatiquement mappés vers les lettres de lecteur sur le bureau virtuel lorsque les utilisateurs ouvrent une session. Les lecteurs sont affichés sous la forme de dossiers partagés associés à des lettres de lecteur mappé. Pour configurer le mappage des lecteurs du client, utilisez le paramètre Lecteurs amovibles clients de la section Paramètres de stratégie de la redirection de fichier des Paramètres de stratégie ICA.

Les différences principales entre les deux types de stratégie à distance sont les suivantes :

Fonctionnalité	Données du mappage des lecteurs clients	Redirection USB générique
Activée par défaut	Oui	Non
Accès en lecture uniquement configurable	Oui	Non
Le périphérique peut être retiré en toute sécurité au cours d'une session	Non	Oui, étant donné que les utilisateurs suivent les recommandations du système d'exploitation pour un retrait en toute sécurité.

Si les stratégies de mappage USB générique et de lecteurs clients sont activées, alors lorsqu'un périphérique de stockage de masse est inséré avant ou après le démarrage d'une session, il sera redirigé à l'aide du mappage de lecteur client. Lorsque les stratégies de mappage USB générique et de lecteurs clients sont activées et qu'un périphérique est configuré pour une redirection automatique (voir http://support.citrix.com/article/CTX123015) et un périphérique de stockage de masse est inséré avant ou après le démarrage d'une session, il sera redirigé à l'aide d'USB générique.

> **Remarque**
>
> La redirection USB est prise en charge sur les connexions de bande passante faible, par exemple de 50 Kbps ; toutefois, la copie de fichiers volumineux ne fonctionnera pas.

Vous pouvez contrôler si les utilisateurs peuvent copier des fichiers à partir de leurs environnements virtuels vers leurs machines utilisateur. Par défaut, les fichiers et dossiers sur les lecteurs clients mappés sont disponibles en mode de lecture/écriture au sein de la session.

Pour empêcher les utilisateurs d'ajouter ou de modifier des fichiers et dossiers sur les lecteurs clients mappés, activez le paramètre de stratégie Accès en lecture unique sur le lecteur client. Lorsque vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est défini sur Autorisé et est également ajouté à la stratégie.

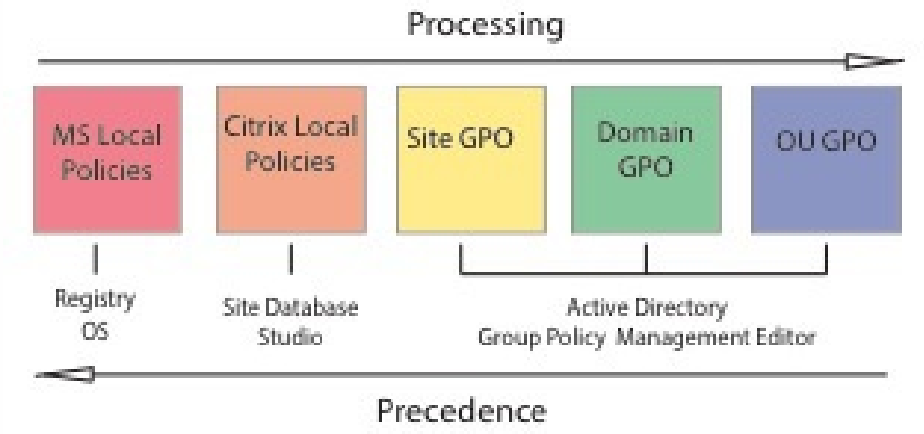
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Stratégies

Jul 07, 2016

Les stratégies sont un ensemble de paramètres qui définissent la façon dont les sessions, la bande passante et la sécurité sont gérées pour un groupe d'utilisateurs, de machines, ou de types de connexion.

Vous pouvez appliquer des paramètres de stratégie à des machines physiques et virtuelles ou à des utilisateurs. Vous pouvez appliquer des paramètres à des utilisateurs individuels au niveau local ou dans les groupes de sécurité dans Active Directory. Les configurations définissent des critères et des règles spécifiques, et si vous n'attribuez pas spécifiquement les stratégies, les paramètres sont appliqués à toutes les connexions.



Vous pouvez appliquer des stratégies sur différents niveaux du réseau. Les paramètres de stratégie placés au niveau de l'objet de stratégie de groupe de l'unité d'organisation prennent la plus haute priorité sur le réseau. Les stratégies au niveau de l'objet de stratégie de groupe du domaine remplacent les stratégies au niveau de l'objet de stratégie de groupe du site, qui remplacent les stratégies en conflit sur les deux niveaux Microsoft et Stratégies locales Citrix.

Toutes les stratégies locales Citrix sont créées et gérées dans la console Studio Citrix et stockées dans la base de données du site, alors que les stratégies de groupe sont créées et gérées à l'aide de la console de gestion des stratégies de groupe (GPMC) et sont stockées dans Active Directory. Les stratégies locales Microsoft sont créées dans le système d'exploitation Windows et sont stockées dans le Registre.

Studio utilise un assistant de modélisation pour aider les administrateurs à comparer les paramètres de configuration dans les modèles et stratégies pour vous aider à éliminer tout paramètre en conflit ou redondant. Les administrateurs peuvent définir leurs objets de stratégie de groupe à l'aide de GPMC pour configurer les paramètres et les appliquer à un ensemble cible d'utilisateurs à différent niveaux du réseau.

Ces objets de stratégie de groupe sont enregistrés dans Active Directory, et l'accès à l'administration de ces paramètres est généralement limité pour la plupart des services informatiques pour des raisons de sécurité.

Les paramètres sont fusionnés selon leur priorité et leur condition. Tout paramètre désactivé remplace un paramètre d'une priorité plus faible activé. Tout paramètre de stratégie non configuré est ignoré et ne remplace pas les paramètres de priorité inférieure.

Les stratégies locales peuvent également être en conflit avec des stratégies de groupe dans Active Directory, qui peuvent se remplacer entre elles, selon le cas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Toutes les stratégies sont traitées dans l'ordre suivant :

1. L'utilisateur ouvre une session sur une machine à l'aide des informations d'identification de domaine.
2. Les informations d'identification sont envoyées au contrôleur de domaine.
3. Active Directory applique toutes les stratégies (utilisateur final, point de terminaison, unité d'organisation et domaine).
4. L'utilisateur ouvre une session sur Receiver et accède à une application ou à un bureau.
5. Citrix et les stratégies Microsoft sont traitées pour l'utilisateur et la machine qui héberge la ressource.
6. Active Directory détermine la priorité pour les paramètres de stratégie et les applique aux registres de la machine de point de terminaison et à la machine hébergeant la ressource.
7. L'utilisateur ferme sa session sur la ressource. Les stratégies Citrix pour l'utilisateur et la machine de point de terminaison ne sont plus actives.
8. L'utilisateur ferme sa session sur la machine utilisateur, ce qui libère les stratégies utilisateur de l'objet de stratégie de groupe.
9. L'utilisateur éteint le périphérique, ce qui libère les stratégies de machine de l'objet de stratégie de groupe.

Lorsque vous créez des stratégies pour des groupes d'utilisateurs, des périphériques et des machines, certains membres peuvent avoir différents besoins et auraient besoin d'exceptions à certains paramètres de stratégie. Les exceptions sont effectuées via des filtres dans Studio et le GPMC qui déterminent ce qui est affecté par la stratégie.

Remarque : le mélange de stratégies Windows et Citrix dans le même objet de stratégie de groupe n'est pas pris en charge.

- Utilisation des stratégies
- Modèles de stratégie
- Créer des stratégies
- Comparer, donner un ordre de priorité, modéliser et résoudre les problèmes des stratégies
- Paramètres de stratégie par défaut
- Référence des paramètres de stratégie

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Utilisation des stratégies

Jul 07, 2016

Configurez des stratégies Citrix pour contrôler l'accès utilisateur ou les environnements de session. Les stratégies Citrix constituent la méthode la plus efficace pour contrôler les paramètres de connexion, de sécurité et de bande passante. Vous pouvez créer des stratégies relatives à des groupes d'utilisateurs, des machines ou des types de connexion spécifiques. Chaque stratégie peut contenir plusieurs paramètres.

Vous pouvez utiliser les outils suivants pour fonctionner avec les stratégies Citrix.

- **Studio** : si vous êtes un administrateur Citrix ne disposant pas de permissions de gérer la stratégie de groupe, utilisez Studio pour créer des stratégies pour votre site. Les stratégies créés avec Studio sont enregistrées dans la base de données du site et les mises à jour sont déployées vers le bureau virtuel soit lorsque celui-ci s'enregistre auprès du broker, soit lorsque l'utilisateur se connecte à ce bureau virtuel.
- **Éditeur de stratégie de groupe locale** (composant logiciel enfichable Microsoft Management Console) : si votre environnement réseau utilise Active Directory et que vous avez l'autorisation de gérer la stratégie de groupe, vous pouvez utiliser l'éditeur de stratégie de groupe local pour créer des stratégies pour votre site. Les paramètres que vous configurez affectent les objets de stratégie de groupe que vous spécifiez via la console de gestion des stratégies de groupe.
  Important : vous devez utiliser l'éditeur de stratégie de groupe local pour configurer certains paramètres de stratégie, y compris ceux associés à l'enregistrement des VDA auprès d'un Controller et ceux associés aux serveurs Microsoft App-V.

Les paramètres de stratégie de groupe sont traités dans l'ordre suivant :

1. GPO local
2. Objet de stratégie de groupe du site XenApp ou XenDesktop (stocké dans la base de données du site)
3. GPO au niveau du site
4. GPO au niveau du domaine
5. Unités d'organisation

Cependant, si un conflit se produit, les paramètres de stratégie qui sont traités en dernier peuvent remplacer ceux qui sont traités en premier. Ceci signifie que les paramètres de stratégie sont prioritaires dans l'ordre suivant :

1. Unités d'organisation
2. GPO au niveau du domaine
3. GPO au niveau du site
4. Objet de stratégie de groupe du site XenApp ou XenDesktop (stocké dans la base de données du site)
5. GPO local

Par exemple, un administrateur Citrix utilise Studio pour créer une stratégie (Stratégie A) qui active la redirection de fichier client pour les employés du département Ventes de l'entreprise. Pendant ce temps, un autre administrateur utilise l'éditeur de stratégie de groupe pour créer une stratégie (Stratégie B) qui désactive la redirection de fichier client pour les employés des ventes. Lorsque les employés des ventes ouvrent une session sur les bureaux virtuels, la Stratégie B est appliquée et la Stratégie A est ignorée car la Stratégie B a été traitée au niveau du domaine et la Stratégie A a été traitée au niveau du GPO de site XenApp ou XenDesktop.

Toutefois lorsqu'un utilisateur lance une session ICA ou RDP (Protocole Bureau à distance), les paramètres de la session

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix remplacent les mêmes paramètres configurés dans une stratégie Active Directory ou à l'aide de la Configuration d'hôte de session Bureau à distance. Ceci comprend les paramètres liés aux paramètres de connexion client RDP standard tels que Papier peint du bureau, Animation de menu et Afficher le contenu de la fenêtre lors d'un cliquer déplacer.

Lors de l'utilisation de plusieurs stratégies, vous pouvez établir des priorités pour les stratégies qui contiennent des paramètres conflictuels ; voir Comparer, donner un ordre de priorité, modéliser et résoudre les problèmes des stratégies pour plus de détails.

Le processus de configuration des stratégies est le suivant :

1. Créez la stratégie.
2. Configurez les paramètres de stratégie.
3. Affectez la stratégie aux objets machine et utilisateur.
4. Définissez l'ordre de priorité de la stratégie.
5. Vérifiez la stratégie effective en exécutant l'assistant Modélisation de stratégie de groupe Citrix.

Dans l'éditeur de stratégie de groupe local, les stratégies et les paramètres apparaissent dans deux catégories : Configuration ordinateur et Configuration utilisateur. Chaque catégorie a un nœud Stratégies Citrix. Consultez la documentation Microsoft pour plus de détails sur la navigation et l'utilisation de ce composant logiciel enfichable.

Dans Studio, les paramètres de stratégie sont triés dans des catégories en fonction de la fonctionnalité ou fonction qu'ils affectent. Par exemple, la section Profile Management contient des paramètres de stratégie pour Profile Management.

- Les paramètres Ordinateur (paramètres de stratégie s'appliquant aux machines) définissent le comportement des bureaux virtuels et sont appliqués lorsqu'un bureau virtuel démarre. Ces paramètres s'appliquent même s'il n'y a pas de session utilisateur active sur le bureau virtuel. Les paramètres utilisateur définissent l'expérience de l'utilisateur lors de la connexion à l'aide du protocole ICA. Les stratégies utilisateur sont appliquées lorsqu'un utilisateur se connecte ou se reconnecte à l'aide du protocole ICA. Les stratégies utilisateur ne sont pas appliquées si un utilisateur se connecte à l'aide de RDP ou ouvre une session directement sur la console.
  Pour accéder aux stratégies, paramètres ou modèles, sélectionnez Stratégies dans le panneau de navigation de Studio.
  - L'onglet **Stratégies** répertorie toutes les stratégies. Lorsque vous sélectionnez une stratégie, les onglets de droite affichent : Présentation (nom, priorité, statut activé/désactivé et description), Paramètres (liste des paramètres configurés) et Attribués à (objets utilisateur et machine auxquels la stratégie est actuellement affectée). Pour de plus amples informations, consultez la section Créer des stratégies.
  - L'onglet **Modèles** répertorie des modèles fournis par Citrix et personnalisés que vous avez créés. Lorsque vous sélectionnez un modèle, les onglets de droite affichent : Description (la raison pour laquelle vous souhaitez utiliser le modèle) et Paramètres (liste des paramètres configurés). Pour plus d'informations, veuillez consulter la section Modèles de stratégie.
  - L'onglet **Comparaison** vous permet de comparer les paramètres d'une stratégie ou d'un modèle avec ceux des autres stratégies ou modèles. Par exemple, il se peut que vous souhaitiez vérifier les valeurs des paramètres pour assurer la compatibilité avec les meilleures pratiques. Pour plus d'informations, consultez la section Comparer, donner un ordre de priorité, modéliser et résoudre les problèmes des stratégies.
  - À partir de l'onglet **Modélisation**, vous pouvez simuler des scénarios de connexion avec les stratégies Citrix. Pour plus d'informations, consultez la section Comparer, donner un ordre de priorité, modéliser et résoudre les problèmes des stratégies.

  Pour rechercher un paramètre dans une stratégie ou un modèle :
  1. Sélectionnez la stratégie ou le modèle.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Sélectionnez Modifier la stratégie ou Modifier le modèle dans le volet Actions.
3. Sur la page Paramètres, commencez à taper le nom du paramètre.
   Vous pouvez affiner votre recherche en sélectionnant une version spécifique du produit, en sélectionnant une catégorie (par exemple, Bande passante), ou en sélectionnant la case à cocher Afficher sélectionné uniquement ou en sélectionnant pour ne rechercher que les paramètres qui ont été ajoutés à la stratégie sélectionnée. Pour une recherche non filtrée, sélectionnez Tous les paramètres.

- Pour rechercher un paramètre dans une stratégie :
  1. Sélectionnez la stratégie.
  2. Sélectionnez l'onglet Paramètres, commencez à taper le nom du paramètre.

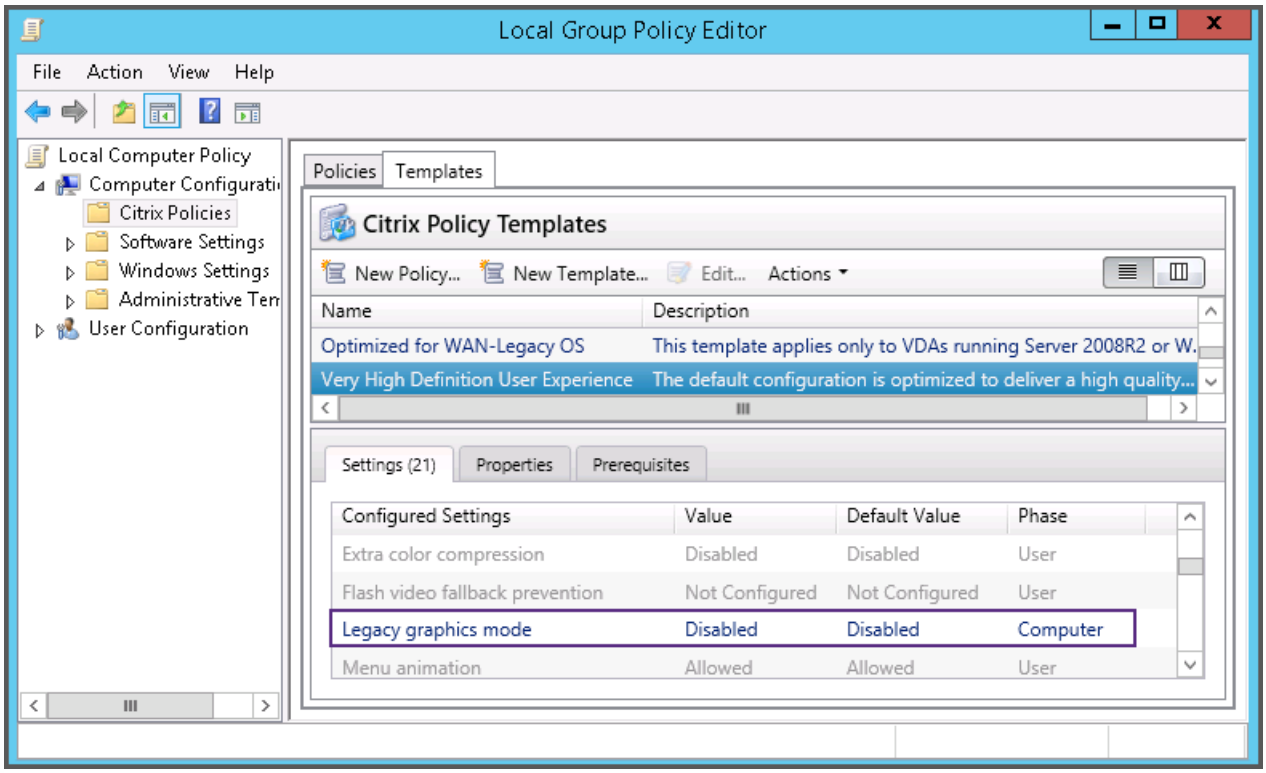
Vous pouvez affiner votre recherche en sélectionnant une version spécifique du produit ou en sélectionnant une catégorie. Pour une recherche non filtrée, sélectionnez Tous les paramètres.

Une stratégie, une fois qu'elle a été créée, est complètement indépendante du modèle utilisé. Vous pouvez utiliser le champ Description d'une nouvelle stratégie pour le suivi de la source modèle utilisé.

Dans Studio, les stratégies et les modèles sont affichés dans une liste unique, qu'ils contiennent des paramètres Utilisateur, Ordinateur ou les deux types de paramètres et peuvent être appliqués à l'aide de filtres Utilisateur et Ordinateur.

Dans l'éditeur de stratégie de groupe, les paramètres Ordinateur et Utilisateur doivent être appliqués séparément, même s'ils ont été créés à partir d'un modèle qui contient les deux types de paramètres. Dans cet exemple, vous choisissez d'utiliser le paramètre Expérience utilisateur très haute définition dans Configuration ordinateur :

- Le Mode graphique d'ancienne génération est un paramètre Ordinateur qui sera utilisé dans une stratégie créée à partir de ce modèle.
- Les paramètres Utilisateur, grisés, ne seront pas utilisés dans une stratégie créée à partir de ce modèle.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Modèles de stratégie

Jul 07, 2016

Les modèles sont utilisés pour créer des stratégies à partir d'un point de départ prédéfini. Les modèles Citrix incorporés, optimisés pour des environnements ou des conditions réseau spécifiques, peuvent être utilisés en tant que :

- Source pour créer vos propres stratégies et modèles à partager entre les sites.
- Référence pour comparer en toute facilité les résultats entre déploiements en vous permettant de faire état des résultats, par exemple, « ...lors de l'utilisation du modèle Citrix x ou y... »
- Méthode permettant de transmettre des stratégies au support Citrix ou à des tiers de confiance en important ou exportant des modèles.

Les modèles de stratégies peuvent être importés ou exportés. Pour de plus amples informations sur les modèles et/ou sur les mises à jour apportées aux modèles incorporés, consultez l'article CTX202000.

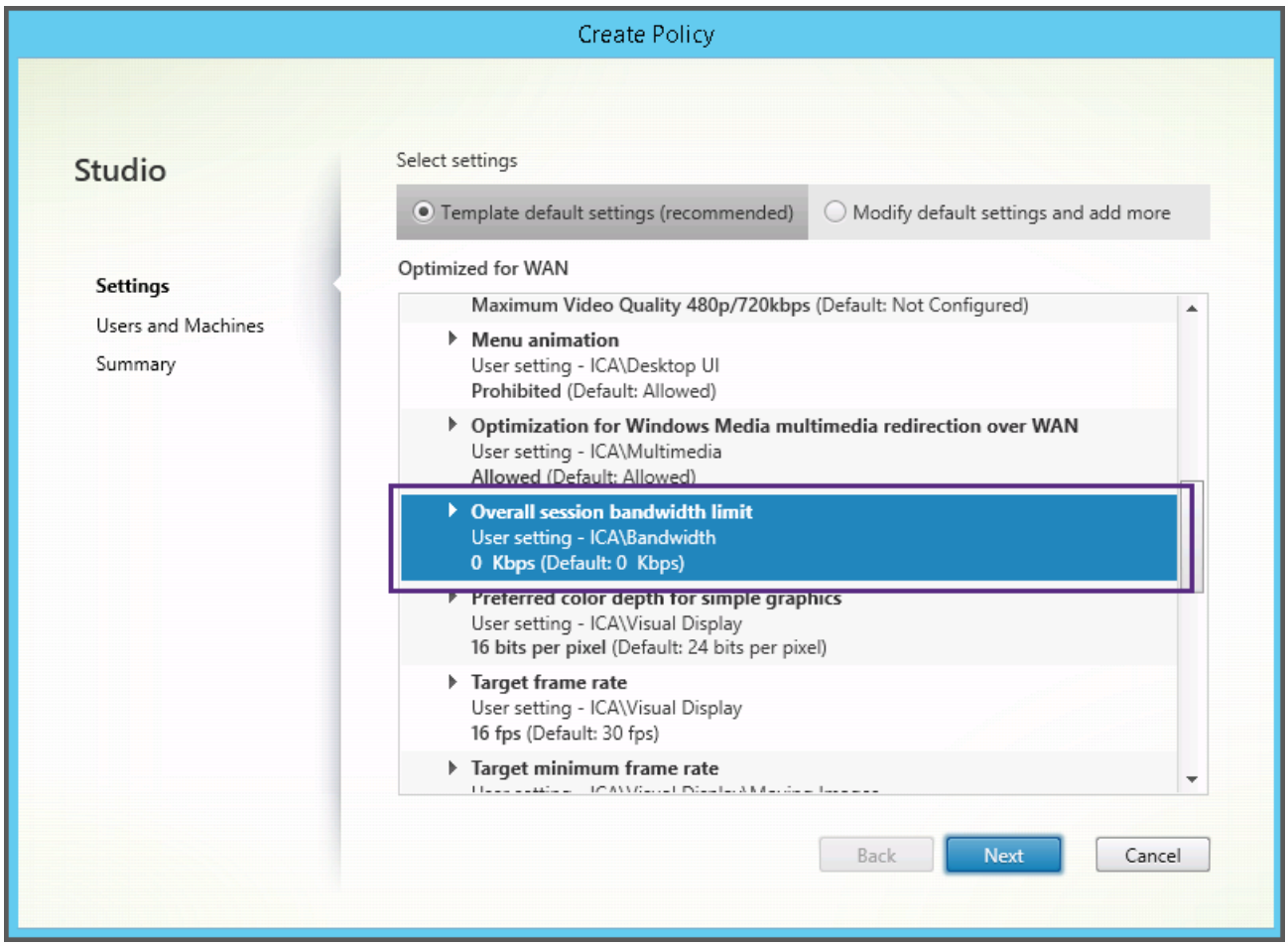
Pour les considérations à prendre en compte lors de l'utilisation de modèles pour créer des stratégies, veuillez consulter l'article CTX202330.

Les modèles de stratégie suivants sont disponibles :

- **Expérience utilisateur très haute définition**. Ce modèle applique les paramètres par défaut ce qui optimise l'expérience utilisateur. Utilisez ce modèle dans les scénarios dans lesquels plusieurs stratégies sont traitées par ordre de priorité.
- **Montée en charge du serveur élevée**. Appliquez ce modèle pour économiser les ressources du serveur. Ce modèle assure un excellent compromis entre expérience utilisateur et montée en charge du serveur. Il offre une expérience utilisateur des plus satisfaisantes tout en augmentant le nombre d'utilisateurs que vous pouvez héberger sur un seul serveur. Ce modèle n'utilise pas le codec vidéo pour la compression de graphiques et empêche la génération de multimédia côté serveur.
- **Montée en charge du serveur élevée - anciens systèmes d'exploitation**. Ce modèle de montée en charge du serveur élevée s'applique uniquement aux VDA exécutant Windows Server 2008 R2 ou Windows 7 et versions antérieures. Ce modèle s'appuie sur le Mode graphique d'ancienne génération qui est plus efficace pour ces systèmes d'exploitation.
- **Optimisé pour les connexions WAN**. Ce modèle est conçu pour les utilisateurs qui travaillent dans des succursales (connexions WAN partagées) ou depuis des sites distants utilisant des connexions à faible bande passante qui accèdent à des applications dotées d'interfaces graphiques simples et contenant très peu de contenu multimédia. Ce modèle optimise l'efficacité de la bande passante au détriment de l'expérience de lecture vidéo et de la montée en charge du serveur.
- **Optimisé pour les connexions WAN – anciens systèmes d'exploitation**. Ce modèle s'applique uniquement aux VDA exécutant Windows Server 2008 R2 ou Windows 7 et versions antérieures. Ce modèle s'appuie sur le Mode graphique d'ancienne génération qui est plus efficace pour ces systèmes d'exploitation.
- **Sécurité et contrôle**. Utilisez ce modèle dans les environnements dans lesquels la tolérance aux risques est faible, de façon à limiter les fonctionnalités activées par défaut dans XenApp et XenDesktop. Ce modèle contient des paramètres qui désactivent l'accès à l'impression, au Presse-papiers, aux périphériques, au mappage de lecteurs, à la redirection de port et à l'accélération Flash sur les machines utilisateur. L'application de ce modèle peut consommer plus de bande passante et réduire le nombre d'utilisateurs par serveur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Bien que nous recommandions d'utiliser les modèles Citrix intégrés avec leurs paramètres par défaut, vous trouverez des paramètres pour lesquels aucune valeur spécifique n'a été recommandée, par exemple « Limite de bande passante de session générale », inclus dans les modèles Optimisé pour les connexions WAN. Dans ce cas, le modèle expose le paramètre de façon à faire comprendre à l'administrateur que ce paramètre est susceptible de s'appliquer au scénario.



Si vous travaillez avec un déploiement (gestion de la stratégie et VDA) antérieur à XenApp et XenDesktop 7.6 FP3, et avez besoin de modèles Montée en charge du serveur élevée et Optimisé pour les connexions WAN, utilisez les anciennes versions de systèmes d'exploitation de ces modèles lorsqu'ils s'appliquent.

> ## Remarque
>
> Les modèles incorporés sont créés et mis à jour par Citrix. vous ne pouvez ni modifier ni supprimer ces modèles.

Pour créer un nouveau modèle à partir d'un autre modèle :

1. Sélectionnez **Stratégies** dans le volet de navigation de Studio.
2. Cliquez sur l'onglet **Modèles**, puis sélectionnez le modèle depuis lequel vous souhaitez créer le nouveau modèle.
3. Sélectionnez **Créer un modèle** dans le volet Actions.
4. Sélectionnez et configurez les paramètres de stratégie que vous souhaitez inclure dans le modèle. Supprimez tout

© 1999-2017 Citrix Systems, Inc. All rights reserved.

paramètre existant qui ne devrait pas être inclus. Entrez un nom pour le modèle.

Lorsque vous cliquez sur **Terminer**, le nouveau modèle s'affiche sur la page de l'onglet **Modèles**.

Pour créer un nouveau modèle à partir d'une stratégie :

1. Sélectionnez **Stratégies** dans le volet de navigation de Studio.
2. Sélectionnez l'onglet **Stratégies**, puis sélectionnez la stratégie à partir de laquelle vous souhaitez créer le nouveau modèle.
3. Sélectionnez **Enregistrer en tant que modèle** dans le volet Actions.
4. Sélectionnez et configurez tout nouveau paramètre de stratégie que vous souhaitez inclure dans le modèle. Supprimez tout paramètre existant qui ne devrait pas être inclus. Entrez un nom et une description pour le modèle, puis cliquez sur **Terminer**.

Pour importer un modèle :

1. Sélectionnez **Stratégies** dans le volet de navigation de Studio.
2. Sélectionnez l'onglet **Modèles**, puis sélectionnez **Importer un modèle**.
3. Sélectionnez le fichier de modèle à importer, puis cliquez sur **Ouvrir**. Si vous importez un modèle du même nom qu'un modèle existant, vous pouvez choisir de remplacer le modèle existant ou d'enregistrer le modèle sous un nom différent qui est généré automatiquement.

Pour exporter un modèle :

1. Sélectionnez **Stratégies** dans le volet de navigation de Studio.
2. Sélectionnez l'onglet **Modèles**, puis sélectionnez **Exporter le modèle**.
3. Sélectionnez l'emplacement dans lequel vous souhaitez enregistrer le modèle, puis cliquez sur **Enregistrer**.

Un fichier .gpt est créé à l'emplacement spécifié.

Dans l'éditeur de stratégie de groupe, développez le nœud Configuration ordinateur ou Configuration utilisateur. Développez le nœud Stratégies, puis sélectionnez Stratégies Citrix. Choisissez l'action appropriée ci-dessous.

Tâche	Instruction
Créer un nouveau modèle à partir d'une stratégie existante	Sur l'onglet Stratégies, sélectionnez la stratégie et sélectionnez Actions > Enregistrer en tant que modèle.
Créer une nouvelle stratégie à partir d'un modèle existant	Sur l'onglet Modèles, sélectionnez le modèle, puis cliquez sur Nouvelle stratégie.
Créer un nouveau modèle à partir d'un modèle existant	Sur l'onglet Modèles, sélectionnez le modèle, puis cliquez sur Nouveau modèle.
Importer un modèle	Sur l'onglet Modèles, sélectionnez Actions > Importer.
Exporter un modèle	Sur l'onglet Modèles, sélectionnez Actions > Exporter.
Afficher les paramètres de modèle	Sur l'onglet Modèles, sélectionnez le modèle, puis cliquez sur l'onglet

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Tâche	Instruction
Afficher un récapitulatif des propriétés du modèle	Sur l'onglet Modèles, sélectionnez le modèle, puis cliquez sur l'onglet Propriétés.
Afficher les pré-requis de modèle	Sur l'onglet Modèles, sélectionnez le modèle, puis cliquez sur l'onglet Pré-requis.

Les modèles de stratégie sont stockés sur la machine sur laquelle le pack de gestion des stratégies a été installé. Cette machine est soit la machine Delivery Controller, soit la machine de gestion des objets de stratégie de groupe (et non la base de données du site XenApp et XenDesktop). Cela signifie que les fichiers de modèle de stratégie sont contrôlés par les autorisations administratives Windows plutôt que par les rôles et les étendues d'administration déléguée du site.

Par conséquent, un administrateur disposant d'autorisations en lecture seule dans le site peut, par exemple, créer de nouveaux modèles. Cependant, les modèles étant des fichiers locaux, aucune modification n'est apportée à votre environnement.

Les modèles personnalisés sont uniquement visibles par le compte utilisateur qui les a créés et stockés dans le profil Windows de l'utilisateur. Pour exposer davantage un modèle personnalisé, créez une stratégie à partir de ce dernier ou exportez-le sur un emplacement partagé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Créer des stratégies

Jul 07, 2016

Avant de créer une stratégie, déterminez quel groupe d'utilisateurs ou de périphériques doit être affecté par celle-ci. Il se peut que vous souhaitiez créer une stratégie basée sur la fonction de l'utilisateur, son type de connexion, sa machine utilisateur ou son emplacement géographique. Vous pouvez aussi utiliser le même critère que vous utilisez pour les stratégies de groupe Windows Active Directory.

Si vous avez déjà créé une stratégie qui s'applique à un groupe, envisagez de la modifier et de configurer les paramètres appropriés au lieu de créer une autre stratégie. Évitez de créer une stratégie uniquement pour activer un paramètre spécifique ou pour exclure certains utilisateurs de l'application de la stratégie.

Lorsque vous créez une nouvelle stratégie, vous pouvez la baser sur les paramètres d'un modèle de stratégie et personnaliser les paramètres selon vos besoins, ou vous pouvez la créer, sans utiliser de modèle et ajouter tous les paramètres nécessaires.

Les paramètres de stratégie peuvent être activés, désactivés ou non configurés. Par défaut, les paramètres de stratégie ne sont pas configurés, c'est-à-dire qu'ils ne sont pas ajoutés à une stratégie. Les paramètres ne sont appliqués que lorsqu'ils sont ajoutés à une stratégie.

Les paramètres de stratégie peuvent affichés l'un des états suivants :

- Autorisé ou Interdit permet ou empêche l'action contrôlée par le paramètre. Dans certains cas, les utilisateurs sont autorisés ou non à gérer l'action du paramètre dans la session. Par exemple, si le paramètre Animation de menu est défini sur Autorisé, les utilisateurs peuvent contrôler les animations de menu dans leur environnement client.
- Activé ou Désactivé active ou désactive le paramètre. Si vous désactivez un paramètre, celui-ci n'est pas activé dans les stratégies de priorité inférieure.

De plus, certains paramètres contrôlent l'efficacité des paramètres dépendants. Par exemple, Redirection de lecteur client contrôle le fait que les utilisateurs sont autorisés ou non à accéder aux lecteurs de leurs machines. Pour permettre aux utilisateurs d'accéder à leurs lecteurs réseau, ce paramètre ainsi que le paramètre Lecteurs réseau clients doivent être ajoutés à la stratégie. Si le paramètre Redirection de lecteur client est désactivé, les utilisateurs ne pourront pas accéder à leurs lecteurs réseau même si le paramètre Lecteurs réseau clients est activé.

En général, les modifications apportées au paramètre de stratégie qui affectent les machines se produisent lorsque le bureau virtuel redémarre ou lorsqu'un utilisateur ouvre une session. Les modifications apportées au paramètre de stratégie qui affectent les utilisateurs se produisent la prochaine fois que les utilisateurs ouvrent une session. Si vous utilisez Active Directory, les paramètres de stratégie sont mis à jour lorsque Active Directory réévalue les stratégies à intervalles de 90 minutes et ils sont appliqués lorsque le bureau virtuel redémarre ou qu'un utilisateur ouvre une session.

Pour certains paramètres de stratégie, vous pouvez entrer ou sélectionner une valeur lorsque vous ajoutez ce paramètre à une stratégie. Vous pouvez limiter la configuration du paramètre en sélectionnant Utiliser une valeur par défaut ; ceci désactive la configuration du paramètre et ne permet à la valeur par défaut du paramètre d'être utilisé lorsque la stratégie est appliquée, quelle que soit la valeur entrée avant la sélection de l'option Utiliser la valeur par défaut.

Recommandations :

- Attribuez des stratégies aux groupes plutôt qu'aux utilisateurs individuels. Si vous attribuez des stratégies aux groupes, les attributions seront mises à jour automatiquement lorsque vous ajouterez des utilisateurs au groupe ou en

© 1999-2017 Citrix Systems, Inc. All rights reserved.

supprimerez.

- N'activez pas les paramètres de conflit ou de chevauchement dans la configuration d'hôte de session Bureau à distance. Dans certains cas, la configuration d'hôte de session Bureau à distance offre une fonctionnalité similaire pour les paramètres de stratégie Citrix. Chaque fois que possible, maintenez la cohérence de tous les paramètres (activés ou désactivés) pour faciliter la résolution des problèmes.
- Désactivez les stratégies non utilisées. Les stratégies sans paramètres ajoutés génèrent un traitement inutile.

Lors de la création d'une stratégie, vous l'attribuez à certains objets utilisateur et ordinateur, cette stratégie est appliquée aux connexions selon des critères ou des règles spécifiques. En général, vous pouvez ajouter à une stratégie autant d'affectations que vous le souhaitez, selon une combinaison de critères. Si vous ne spécifiez pas les affectations, la stratégie est appliquée à toutes les connexions.

Le tableau suivant répertorie les affectations disponibles :

Nom de l'affectation	Applique une stratégie basée sur
Type d'accès	Conditions de contrôle d'accès au travers desquelles un client se connecte. • Type de connexion : si vous souhaitez appliquer la stratégie aux connexions établies avec ou sans NetScaler Gateway. • Nom de batterie NetScaler Gateway : nom du serveur virtuel NetScaler Gateway. • Condition d'accès : nom de la stratégie d'analyse de point de terminaison ou la stratégie de session à utiliser.
Citrix CloudBridge	Indique si une session utilisateur est lancée au travers de Citrix CloudBridge. Remarque : vous pouvez ajouter une seule affectation Citrix CloudBridge à une stratégie.
Adresse IP de machine cliente	Adresse IP de la machine cliente utilisée pour se connecter à la session. • Exemples IPv4 : 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24 • Exemples IPv6 : 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
Nom du client	Nom de la machine utilisateur. • Concordance exacte : ClientABCName • Utilisation du caractère générique : Client*Name
Groupe de mise à disposition	Appartenance à un groupe de mise à disposition.
Type de groupe de mise à disposition	Type de bureau ou d'application : bureau privé, bureau partagé, application privée ou application partagée.
Unité d'organisation (UO)	Unité d'organisation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom de l'affectation	Applique une stratégie basée sur
Balise	Balises. **Remarque :** pour vous assurer que les stratégies sont correctement appliquées lors de l'utilisation de balises, installez la correction disponible sur l'article CTX142439.
Utilisateur ou groupe	Nom d'utilisateur ou de groupe.

Lorsque les utilisateurs ouvrent une session, toutes les stratégies correspondant aux affectations pour la connexion sont identifiées. Les stratégies sont triées dans un ordre de priorité et plusieurs instances de tous les paramètres sont comparées. Chaque paramètre est appliqué selon l'ordre de priorité de la stratégie. Un paramètre de stratégie qui est désactivé prévaut sur un paramètre activé doté d'une priorité plus faible. Les paramètres de stratégie qui ne sont pas configurés sont ignorés.

Important : lorsque vous configurez les stratégies Active Directory et Citrix avec la Console de gestion des stratégies de groupe, il est possible que les filtres et les paramètres ne soient pas appliqués comme prévu. Pour obtenir davantage d'informations, veuillez consulter l'article CTX127461.
Une stratégie appelée « Non filtrée » est fournie par défaut.

- Si vous utilisez Studio pour gérer les stratégies Citrix, les paramètres que vous ajoutez à la stratégie Non filtrée sont appliqués à l'ensemble des serveurs, des bureaux et des connexions d'un site.
- Si vous utilisez l'éditeur de stratégie de groupe pour gérer les stratégies Citrix, les paramètres que vous ajoutez à la stratégie Non filtrée sont appliqués à tous les sites et à toutes les connexions qui se trouvent dans l'étendue des Objets de stratégie de groupe qui contiennent la stratégie. Par exemple, L'UO Ventes contient un GPO appelé Ventes-FR qui comprend tous les membres de l'équipe de vente française. Le GPO Ventes-FR est configuré à l'aide d'une stratégie Unfiltered qui comprend plusieurs paramètres de stratégie utilisateur. Lorsque le directeur des Ventes FR ouvre une session sur le site, les paramètres de la stratégie Non filtrée sont automatiquement appliqués à la session car l'utilisateur est membre du GPO Ventes-FR.

Un mode d'affectation détermine si la stratégie est ou non appliquée uniquement aux connexions correspondant à tous les critères d'affectation. Si le mode est défini sur Autoriser (valeur par défaut), la stratégie s'applique uniquement aux connexions correspondant aux critères d'affectation. Si le mode est défini sur Refuser, la stratégie s'applique si la connexion ne correspond pas aux critères d'affectation. Les exemples suivants illustrent la manière dont les modes d'affectation affectent les stratégies Citrix lorsque plusieurs affectations sont présentes.

- **Exemple : affectations de types similaires avec des modes différents** : dans les stratégies comportant deux affectations du même type, un défini sur Autoriser et un défini sur Refuser, l'affectation définie sur Refuser a priorité, étant donné que la connexion satisfait les deux affectations. Par exemple :
  La stratégie 1 comprend les affectations suivantes :
  - L'affectation A spécifie le groupe Ventes et le mode est défini sur Autoriser.
  - L'affectation B spécifie le compte du directeur des ventes et le mode est défini sur Refuser.

  Le mode de l'affectation B étant défini sur Refuser, la stratégie n'est pas appliquée lorsque le directeur des ventes ouvre une session sur le site, bien que l'utilisateur soit membre du groupe Ventes.

- **Exemple : affectations de types différents avec des modes similaires** : dans les stratégies comportant deux affectations ou plus de types différents, défini sur Autoriser, la connexion doit satisfaire au moins une affectation de chaque type afin que la stratégie soit appliquée. Par exemple :
  La stratégie 2 comprend les affectations suivantes :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- L'affectation C est une affectation utilisateur qui spécifie le groupe Ventes et le mode est défini sur Autoriser ;
- l'affectation D est une affectation d'adresse IP cliente qui spécifie 10.8.169.* (le réseau d'entreprise) et le mode est défini sur Autoriser.

Lorsque le directeur des ventes ouvre une session sur le site depuis son bureau, la stratégie est appliquée car la connexion satisfait les deux affectations.

La stratégie 3 comprend les affectations suivantes :

- L'affectation E est une affectation utilisateur qui spécifie le groupe Ventes et le mode est défini sur Autoriser.
- L'affectation F est une affectation de type contrôle d'accès qui spécifie les conditions de connexion NetScaler Gateway et le mode est défini sur Autoriser.

Lorsque le directeur des ventes ouvre une session sur le site depuis le bureau, la stratégie n'est pas appliquée car la connexion ne satisfait pas l'affectation F.

1. Sélectionnez Stratégies dans le volet de navigation Studio.
2. Sélectionnez l'onglet Modèles, puis sélectionnez un modèle.
3. Sélectionnez Créer une stratégie à partir du modèle dans le volet Actions.
4. Par défaut, la nouvelle stratégie utilise tous les paramètres par défaut dans le modèle (le bouton radio Utiliser les paramètres de modèles par défaut est sélectionné). Si vous souhaitez modifier les paramètres, sélectionnez le bouton radio Modifier les valeurs par défaut et ajouter des paramètres, puis ajoutez ou supprimez des paramètres.
5. Spécifiez comment appliquer la stratégie en sélectionnant l'une des options suivantes :
   - Attribuer aux objets Utilisateur et Machine sélectionnés, puis sélectionnez les objets utilisateur et machine auquel la stratégie s'applique.
   - Attribuer tous les objets d'un site pour appliquer la stratégie à tous les objets utilisateur et machine dans le site.
6. Entrez un nom pour la stratégie (ou acceptez la valeur par défaut) ; considérez appeler la stratégie en fonction de ce qu'elle affecte, par exemple, Service finance ou Utilisateurs distants. Facultativement, ajoutez une description.
   La stratégie est activée par défaut, vous pouvez la désactiver. Si vous activez la stratégie, vous pouvez l'appliquer immédiatement aux utilisateurs ouvrant une session. Si vous désactivez la stratégie, elle n'est pas appliquée. Si vous avez besoin de définir la priorité de la stratégie ou d'ajouter des paramètres ultérieurement, considérez désactiver cette stratégie jusqu'à ce que vous soyez prêt à l'appliquer.

1. Sélectionnez Stratégies dans le volet de navigation Studio.
2. Sélectionnez l'onglet Stratégies.
3. Sélectionnez Créer une stratégie dans le volet Actions.
4. Ajoutez et configurez les paramètres de stratégie.
5. Spécifiez comment appliquer la stratégie en choisissant l'une des options suivantes :
   - Attribuer aux objets Utilisateur et Machine sélectionnés, puis sélectionnez les objets utilisateur et machine auquel la stratégie s'applique.
   - Attribuer tous les objets d'un site pour appliquer la stratégie à tous les objets utilisateur et machine dans le site.
6. Entrez un nom pour la stratégie (ou acceptez la valeur par défaut) ; considérez appeler la stratégie en fonction de ce qu'elle affecte, par exemple, Service finance ou Utilisateurs distants. Facultativement, ajoutez une description.
   La stratégie est activée par défaut, vous pouvez la désactiver. Si vous activez la stratégie, vous pouvez l'appliquer immédiatement aux utilisateurs ouvrant une session. Si vous désactivez la stratégie, elle n'est pas appliquée. Si vous avez besoin de définir la priorité de la stratégie ou d'ajouter des paramètres ultérieurement, considérez désactiver cette stratégie jusqu'à ce que vous soyez prêt à l'appliquer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dans l'éditeur de stratégie de groupe, développez le nœud Configuration ordinateur ou Configuration utilisateur. Développez le nœud Stratégies, puis sélectionnez Stratégies Citrix. Choisissez l'action appropriée ci-dessous.

Tâche	Instruction
Créer une nouvelle stratégie	Dans l'onglet Stratégies, cliquez sur Nouveau.
Modifier une stratégie existante	Sur l'onglet Stratégies, sélectionnez la stratégie et cliquez sur Modifier.
Modifier la priorité d'une stratégie existante	Sur l'onglet Stratégies, sélectionnez la stratégie et cliquez sur Plus élevée ou Plus basse.
Afficher les informations de synthèse sur une stratégie	Sur l'onglet Stratégies, sélectionnez la stratégie et cliquez sur l'onglet Synthèse.
Afficher et modifier les paramètres de stratégie	Sur l'onglet Stratégies, sélectionnez la stratégie et cliquez sur l'onglet Paramètres.
Afficher et modifier les filtres de stratégie	Sur l'onglet Stratégies, sélectionnez la stratégie et cliquez sur l'onglet Filtres.
Activer ou désactiver une stratégie	Sur l'onglet Stratégies, sélectionnez la stratégie, puis sélectionnez soit Actions > Activer ou Actions > Désactiver.
Créer une nouvelle stratégie à partir d'un modèle existant	Sur l'onglet Modèles, sélectionnez le modèle, puis cliquez sur Nouvelle stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Comparer, donner un ordre de priorité, modéliser et résoudre les problèmes des stratégies

Jul 07, 2016

Vous pouvez utiliser plusieurs stratégies pour personnaliser votre environnement afin de répondre aux besoins des utilisateurs, qui varient selon leur fonction, leur emplacement géographique ou leur type de connexion. Par exemple, pour des raisons de sécurité, il se peut vous deviez imposer des restrictions aux groupes d'utilisateurs qui travaillent régulièrement avec des données confidentielles. Vous pouvez créer une stratégie qui empêche les utilisateurs d'enregistrer les fichiers confidentiels sur leurs lecteurs clients locaux. Toutefois, si certains membres du groupe d'utilisateurs ont besoin de l'accès à leurs lecteurs locaux, vous pouvez créer une autre stratégie spécialement pour ces utilisateurs. Vous pouvez ensuite définir l'ordre de ces deux stratégies afin de définir laquelle des deux est prioritaire.

Lorsque vous utilisez plusieurs stratégies, vous devez déterminer comment leur accorder des priorités, créer des exceptions et visualiser la stratégie effective en cas de conflit.

En général, les stratégies ont priorité sur les paramètres similaires configurés pour la totalité du site, pour des Delivery Controller spécifiques ou sur la machine cliente. L'exception à ce principe est la sécurité. Le paramètre de cryptage le plus élevé de votre environnement, y compris le système d'exploitation, et le paramètre d'observation le plus restrictif remplace toujours les autres paramètres et stratégies.

Les stratégies Citrix interagissent avec celles que vous définissez dans votre système d'exploitation. Dans un environnement Citrix, les paramètres Citrix remplacent les mêmes paramètres configurés dans une stratégie Active Directory ou à l'aide de la Configuration d'hôte de session Bureau à distance. Ceci comprend les paramètres liés aux paramètres de connexion client RDP (Remote Desktop Protocol) standard tels que Papier peint du bureau, Animation de menu et Afficher le contenu de la fenêtre lors d'un cliquer déplacer. Certains paramètres de stratégie, tels que Secure ICA, doivent correspondre à ceux du système d'exploitation. Si un niveau plus élevé de cryptage prioritaire est défini autre part, les paramètres de stratégie Secure ICA que vous spécifiez dans la stratégie ou lorsque vous mettez à disposition une application ou des bureaux peuvent être remplacés.

Par exemple, les paramètres de cryptage que vous spécifiez lorsque vous créez des groupes de mise à disposition devraient être au même niveau que les paramètres de cryptage que vous avez spécifié au travers de votre environnement.

Remarque : dans le second hop d'un scénario double-hop, lorsqu'un VDA avec OS de bureau se connecte à un VDA avec OS de serveur, les stratégies Citrix s'appliquent sur le VDA avec OS de bureau comme s'il s'agissait de la machine utilisateur. À titre d'exemple, si des stratégies sont définies pour mettre en cache les images sur la machine utilisateur, les images mises en cache pour le second hop dans un scénario double-hop sont mises en cache sur machine sur laquelle est installé le VDA avec OS de bureau.

Vous pouvez comparer les paramètres d'une stratégie ou d'un modèle avec ceux des autres stratégies ou modèles. Par exemple, il se peut que vous deviez vérifier des valeurs de paramètres afin d'assurer la compatibilité avec les meilleures pratiques. Vous pouvez également comparer les paramètres d'une stratégie ou d'un modèle avec les paramètres par défaut fournis par Citrix.

1. Sélectionnez Stratégies dans le volet de navigation Studio.
2. Cliquez sur l'onglet Comparaison puis cliquez sur Sélectionner.
3. Sélectionnez les stratégies ou les modèles à comparer. Pour inclure les valeurs par défaut dans la comparaison, sélectionnez la case à cocher Comparer aux paramètres par défaut.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. Après avoir cliqué sur Comparer, les paramètres configurés sont affichés dans les colonnes.
5. Pour afficher tous les paramètres, sélectionnez Afficher tous les paramètres. Pour revenir à la vue par défaut, sélectionnez Afficher les paramètres courants.

La définition de priorités de stratégies vous permet de définir quelles sont les stratégies qui prévalent lorsqu'elles présentent des conflits de paramètres. Lorsque les utilisateurs ouvrent une session, toutes les stratégies correspondant aux affectations pour la connexion sont identifiées. Les stratégies sont triées dans un ordre de priorité et plusieurs instances de tous les paramètres sont comparées. Chaque paramètre est appliqué selon l'ordre de priorité de la stratégie.

Vous définissez la priorité des stratégies en leur donnant des numéros de priorité différents dans Studio. Par défaut, la priorité d'une nouvelle stratégie est plus faible que celle d'une stratégie déjà existante. Lorsque deux stratégies à appliquer ont des règles entrant en conflit, la stratégie dotée de la plus haute priorité (la valeur 1 représentant la plus haute priorité) prévaut sur la stratégie dotée de la priorité la plus faible. Les paramètres sont combinés selon leur priorité et leur condition, par exemple si le paramètre est désactivé ou activé. Tout paramètre désactivé remplace un paramètre de plus faible priorité qui est activé. Les paramètres de stratégie qui ne sont pas configurés sont ignorés ; ils ne l'emportent pas sur les paramètres dotés d'une priorité plus faible.

1. Sélectionnez Stratégies dans le volet de navigation Studio. Assurez-vous que l'onglet Stratégies est sélectionné.
2. Sélectionnez une stratégie.
3. Sélectionnez Priorité inférieure ou Priorité supérieure dans le volet Actions.

Après avoir créé des stratégies pour des groupes d'utilisateurs, des machines utilisateur ou des machines, vous constaterez peut-être qu'il est nécessaire de définir, pour certains membres de ces groupes, des exceptions à certains paramètres de stratégie. Vous pouvez créer des exceptions en :

- créant une stratégie uniquement pour ces membres de groupe qui ont besoin des exceptions, et en plaçant la priorité d'une stratégie en plus haute position que la stratégie de tout le groupe ;
- utilisant le mode Refuser pour une attribution ajoutée à la stratégie.

Une affectation avec le mode défini sur Refuser applique une stratégie uniquement aux connexions qui ne correspondent pas aux critères d'affectation. Par exemple, une stratégie contient les affectations suivantes :

- L'affectation A est une affectation d'adresse IP cliente qui spécifie la plage 208.77.88.* et le mode est défini sur Autoriser.
- L'affectation B est une affectation utilisateur qui spécifie un compte utilisateur particulier et le mode est défini sur Refuser.

La stratégie est appliquée à tous les utilisateurs qui ouvrent une session sur le site dont les adresses IP se trouvent dans la plage spécifiée dans l'affectation A. Cependant, la stratégie n'est pas appliquée à l'utilisateur ouvrant une session sur le site avec le compte d'utilisateur spécifié dans l'affectation B, même si l'ordinateur de l'utilisateur se voit attribuer une adresse IP dans la plage spécifiée dans l'affectation A.

Il arrive parfois qu'une connexion ne réponde pas comme prévu car plusieurs stratégies s'appliquent. Si une stratégie à priorité élevée s'applique également à la connexion, elle peut remplacer les paramètres configurés dans la stratégie d'origine. Vous pouvez déterminer le résultat final de la combinaison des paramètres de stratégie pour une connexion en calculant l'ensemble de stratégies résultant.

Vous pouvez calculer l'ensemble de stratégies résultant de plusieurs façons :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Utilisez l'assistant Modélisation de stratégie de groupe Citrix pour simuler un scénario de connexion et déterminer comment appliquer les stratégies Citrix. Vous pouvez spécifier les conditions d'un scénario de connexion, telles qu'un contrôleur de domaine, des utilisateurs, des valeurs d'évidence d'affectation de stratégie Citrix et des paramètres d'environnement simulé comme une connexion réseau lente. Le rapport créé par l'assistant répertorie les stratégies Citrix susceptibles de s'appliquer dans le scénario. Si vous êtes connecté au Controller en tant qu'utilisateur du domaine, l'assistant calcule l'ensemble de stratégies résultant en utilisant les paramètres de stratégie du site et les objets de stratégie de groupe (GPO) Active Directory.
- Utilisez l'outil Résultats de stratégie de groupe pour créer un rapport décrivant les stratégies Citrix en vigueur pour un utilisateur et un contrôleur donnés. L'outil Résultats de stratégie de groupe vous aide à évaluer l'état actuel des objets de stratégie de groupe dans votre environnement et génère un rapport décrivant de quelle façon ces objets, y compris les stratégies Citrix, sont appliqués à un utilisateur et à un contrôleur donnés.

Vous pouvez lancer l'assistant Modélisation de stratégie de groupe Citrix depuis le panneau Actions de Studio. Vous pouvez lancer les deux outils à partir de la Console de gestion des stratégies de groupe dans Windows.

Si vous exécutez l'assistant Modélisation de stratégie de groupe Citrix ou l'outil Résultats de stratégie de groupe à partir de la Console de gestion des stratégies de groupe, les paramètres de stratégie de site créés avec Studio ne sont pas inclus dans l'ensemble de stratégies résultant.

Pour être certain d'obtenir l'ensemble de stratégies résultant le plus complet, Citrix vous recommande de lancer l'assistant Modélisation de stratégie de groupe Citrix depuis Studio, sauf si vous ne créez des stratégies qu'avec la Console de gestion des stratégies de groupe.

Ouvrez l'Assistant Modélisation de stratégie de groupe Citrix à l'aide de l'une des options suivantes :

- Sélectionnez Stratégies dans le panneau de navigation de Studio, sélectionnez l'onglet Modélisation, puis sélectionnez Démarrer l'assistant de modélisation dans le volet Actions.
- Démarrez la console de gestion des stratégies de groupe (gpmc.msc), cliquez avec le bouton droit de la souris sur le nœud Modélisation de stratégie de groupe Citrix dans l'arborescence et sélectionnez Assistant Modélisation de stratégie de groupe Citrix.

Suivez les instructions de l'assistant pour sélectionner le contrôleur de domaine, les utilisateurs, les ordinateurs, les paramètres d'environnement et les critères d'affectation Citrix à utiliser dans la simulation. Lorsque vous cliquez sur Terminer, l'assistant produit un rapport sur les résultats de modélisation. Dans Studio, le rapport apparaît dans le panneau du milieu, sous l'onglet Modélisation.

Pour afficher le rapport, sélectionnez Afficher le rapport de modélisation.

Les utilisateurs, adresses IP et autres objets affectés peuvent posséder plusieurs stratégies qui s'appliquent de manière simultanée. Ceci peut entraîner des conflits lorsqu'une stratégie ne se comporte pas de manière attendue. Lorsque vous exécutez l'assistant Modélisation de stratégie de groupe Citrix ou l'outil Résultats de stratégie de groupe, il se peut que vous découvriez qu'aucune stratégie n'est appliquée aux connexions utilisateur. Dans ce cas, les utilisateurs se connectant à leurs applications et bureaux dans des conditions correspondant aux critères d'évaluation de stratégie ne sont affectés par aucun paramètre de stratégie. Ceci se produit lorsque :

- aucune stratégie ne possède d'affectation correspondant au critère d'évaluation de stratégie ;
- les stratégies correspondant à l'affectation ne possèdent aucun paramètre configuré ;
- les stratégies correspondant à l'affectation sont désactivées.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si vous souhaitez appliquer des paramètres de stratégie à des connexions répondant aux critères spécifiés, effectuez les opérations suivantes :

- Les stratégies que vous souhaitez appliquer à ces connexions sont activées.
- Les stratégies que vous souhaitez appliquer possèdent les paramètres appropriés configurés.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie par défaut

Aug 22, 2016

Les tableaux suivants répertorient les paramètres de stratégie, leur valeur par défaut, et les versions de Virtual Delivery Agent (VDA) auxquelles ils s'appliquent.

Nom	Paramètre par défaut	VDA
Redirection de Presse-papiers client	Autorisé	Toutes les versions VDA
Démarrages de bureau	Interdit	VDA pour OS 7 jusqu'à la version actuelle
Expiration de délai de la connexion à l'écouteur ICA	120 000 millisecondes	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Numéro de port de l'écouteur ICA	1494	Toutes les versions VDA
Lancement de programmes non publiés lors de la connexion du client	Interdit	VDA pour OS 7 jusqu'à la version actuelle
Formats autorisés d'écriture dans le Presse-papiers client	Aucun format spécifié	VDA 7.6 jusqu'à la version actuelle
Restreindre l'écriture dans le Presse-papiers client	Interdit	VDA 7.6 jusqu'à la version actuelle
Restreindre l'écriture dans le Presse-papiers de session	Interdit	VDA 7.6 jusqu'à la version actuelle
Formats autorisés d'écriture dans le Presse-papiers de session	Aucun format spécifié	VDA 7.6 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Prévention du retour à la vidéo Flash	Non configurée	VDA 7.6 FP3 jusqu'à la version actuelle
Erreur *.swf de prévention du retour à la vidéo Flash		VDA 7.6 FP3 jusqu'à la version actuelle

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Plug N Play audio	Autorisé	VDA pour OS de serveur 7 jusqu'à la version actuelle
Qualité audio	Élevé - audio haute définition	Toutes les versions VDA
Redirection audio du client	Autorisé	Toutes les versions VDA
Redirection du microphone client	Autorisé	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Reconnexion automatique des clients	Autorisé	Toutes les versions VDA
Authentification de la reconnexion automatique des clients	Ne pas requérir d'authentification	Toutes les versions VDA
Journalisation de la reconnexion automatique des clients	Ne pas journaliser les événements de reconnexion automatique	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Limite de bande passante de redirection audio	0 Kbps	Toutes les versions VDA
Pourcentage de limite de bande passante de la redirection audio	0	Toutes les versions VDA
Limite de bande passante de redirection du périphérique USB client	0 Kbps	VDA 5.5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Pourcentage de limite de bande passante de redirection du périphérique USB client	0	VDA 5.5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Limite de bande passante de redirection du Presse-papiers	0 Kbps	Toutes les versions VDA
Pourcentage de la limite de la bande	0	Toutes les versions VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
passante de redirection du Presse-papiers		
Limite de bande passante pour la redirection du port COM	0 Kbps	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.
Pourcentage de limite de bande passante de redirection du port COM	0	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.
Limite de bande passante de redirection de fichier	0 Kbps	Toutes les versions VDA
Pourcentage de limite de bande passante de redirection de fichier	0	Toutes les versions VDA
Limite de bande passante d'accélération multimédia HDX MediaStream	0 Kbps	VDA 5.5, 5.6 FP1, VDA pour OS de serveur 7 et VDA pour OS de bureau 7 à versions VDA pour OS de serveur et VDA pour OS de bureau courantes
Pourcentage de limite de bande passante d'accélération multimédia HDX MediaStream	0	VDA 5.5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Limite de bande passante pour la redirection du port LPT	0 Kbps	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.
Pourcentage de limite de bande passante de redirection du port LPT	0	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.
Limite de bande passante globale de session	0 Kbps	Toutes les versions VDA
Limite de bande passante de redirection d'imprimante	0 Kbps	Toutes les versions VDA
Pourcentage de limite de bande passante de redirection de l'imprimante	0	Toutes les versions VDA
Limite de bande passante de redirection du périphérique TWAIN	0 Kbps	VDA 5.5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Pourcentage de limite de bande passante de redirection du périphérique TWAIN	0	VDA 5.5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Cette option permet aux applications d'utiliser l'emplacement physique de la machine cliente.	Interdit	VDA 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Redirection Desktop Composition	Désactivé (7.6 FP3 jusqu'à la version actuelle) Activé (5.6 à 7.6 FP2)	VDA 5.6, VDA pour OS de bureau 7 jusqu'à la version actuelle, VDA
Qualité graphique de redirection Desktop Composition	Taille moyenne	VDA 5.6, VDA pour OS de bureau 7 jusqu'à la version actuelle
Papier peint du bureau	Autorisé	Toutes les versions VDA
Animation de menu	Autorisé	Toutes les versions VDA
Afficher le contenu de la fenêtre lors d'un cliquer déplacer	Autorisé	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Calcul des boucles ICA	Activé	Toutes les versions VDA
Calcul des boucles ICA	15 secondes	Toutes les versions VDA
Calcul des boucles ICA pour les connexions inactives	Désactivée	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Enhanced Desktop Experience	Autorisé	VDA pour OS 7 jusqu'à la version actuelle

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Connecter automatiquement les lecteurs clients	Autorisé	Toutes les versions VDA
Redirection de lecteur client	Autorisé	Toutes les versions VDA
Lecteurs fixes clients	Autorisé	Toutes les versions VDA
Lecteurs de disquette clients	Autorisé	Toutes les versions VDA
Lecteurs réseau clients	Autorisé	Toutes les versions VDA
Lecteurs optiques clients	Autorisé	Toutes les versions VDA
Lecteurs amovibles clients	Autorisé	Toutes les versions VDA
Redirection hôte vers client	Désactivée	VDA pour OS 7 jusqu'à la version actuelle
Préserver les lettres de lecteurs clients	Désactivée	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Accès en lecture unique sur le lecteur client	Désactivée	VDA 5.5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Redirection vers les dossiers spéciaux	Autorisé	Déploiements Interface Web uniquement ; VDA pour OS de serveur 7 jusqu'à la version actuelle
Utiliser les écritures asynchrones	Désactivée	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Autoriser la compression visuelle sans perte	Désactivée	VDA 7.6 jusqu'à la version actuelle
Limite de mémoire d'affichage	6553 Ko	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Préférence de dégradation du mode d'affichage	Réduire d'abord le nombre de couleurs	Toutes les versions VDA
Aperçu de fenêtres dynamiques	Activé	VDA 5.5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Cache d'image	Activé	VDA 5.5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Mode graphique d'ancienne génération	Désactivée	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Nombre de couleurs maximal autorisé	32 bits par pixel	Toutes les versions VDA
Notifier l'utilisateur lorsque le mode d'affichage se dégrade	Désactivée	VDA pour OS 7 jusqu'à la version actuelle
Mise en file d'attente et ballotage	Activé	Toutes les versions VDA
Utiliser codec vidéo pour la compression	Utiliser un codec vidéo au choix	VDA 7.6 FP3 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Seuil de cache permanent	3000000 bps	VDA pour OS 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Canal d'affichage Framehawk	Désactivée	VDA 7.6 FP2 jusqu'à la version actuelle
Plage de ports du canal d'affichage Framehawk	3224,3324	VDA 7.6 FP2 jusqu'à la version actuelle

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Délai d'expiration de persistance ICA	60 secondes	Toutes les versions VDA
Persistances ICA	Ne pas envoyer de messages de persistance ICA	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Autoriser Local App Access	Interdit	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Liste noire de redirection d'adresse URL	Aucun site n'est spécifié.	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Liste blanche de redirection d'adresse URL	Aucun site n'est spécifié.	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Affichage de clavier automatique	Interdit	VDA 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Démarrer le bureau tactile	Autorisé	VDA 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle Ce paramètre est désactivé et n'est pas disponible pour les machines Windows 10.
Contrôler la zone combinée	Interdit	VDA 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Limiter la qualité de la vidéo	Non configurée	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		jusqu'à la version actuelle
Conférences multimédia	Autorisé	Toutes les versions VDA
Optimisation pour la redirection multimédia Windows Media sur un réseau étendu	Autorisé	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Utiliser l'unité de traitement graphique (GPU) pour optimiser la redirection multimédia Windows Media sur un réseau étendu	Interdit	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Paramètre de stratégie Gestion de la charge vidéo	Non configurée	VDA 7.6 FP3 jusqu'à la version actuelle
Récupération de contenu côté client Windows Media	Autorisé	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Redirection Windows Media	Autorisé	Toutes les versions VDA
Taille de tampon de redirection Windows Media	5 secondes	VDA 5, 5.5, 5.6 FP1
Utilisation de la taille de tampon de redirection Windows Media	Désactivée	VDA 5, 5.5, 5.6 FP1

Nom	Paramètre par défaut	VDA
Audio sur UDP	Autorisé	VDA pour OS 7 jusqu'à la version actuelle
Plage de port UDP audio	16500, 16509	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Stratégie Multi-Port	Le port principal (2598) a une priorité élevée	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Paramètre d'ordinateur Multi-	Désactivée	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Stream Paramètre utilisateur Multi-Stream	Désactivée	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Connecter automatiquement les ports COM du client	Désactivée	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.
Connecter automatiquement les ports LPT du client	Désactivée	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.
Redirection de port COM client	Interdit	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.
Redirection de port LPT client	Interdit	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.

Nom	Paramètre par défaut	VDA
Redirection d'imprimante cliente	Autorisé	Toutes les versions VDA
Imprimante par défaut	Définir l'imprimante par défaut sur l'imprimante principale du client.	Toutes les versions VDA
Attributions d'imprimantes	L'imprimante actuelle de l'utilisateur est utilisée comme imprimante par défaut pour la session.	Toutes les versions VDA
Préférence de journalisation des événements de création automatique des imprimantes	Journaliser les erreurs et les avertissements	Toutes les versions VDA
Imprimantes de session	Aucune imprimante n'est spécifiée.	Toutes les versions VDA
Attendre la création d'imprimantes (bureau)	Désactivée	Toutes les versions VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA

Nom	Paramètre par défaut	VDA
Créer automatiquement les imprimantes clientes	Création automatique de toutes les imprimantes clientes	Toutes les versions VDA
Créer automatiquement l'imprimante universelle générique	Désactivée	Toutes les versions VDA
Noms des imprimantes clientes	Noms d'imprimantes standards	Toutes les versions VDA
Connexions directes aux serveurs d'impression	Activé	Toutes les versions VDA
Mappage et compatibilité du pilote d'imprimante	Aucune règle n'est spécifiée.	Toutes les versions VDA
Rétention des propriétés d'imprimante	Conservées dans le profil seulement si pas enregistrées sur la machine cliente	Toutes les versions VDA
Imprimantes clientes conservées et restaurées	Autorisé	VDA 5, 5.5, 5.6 FP1

Nom	Paramètre par défaut	VDA
Installation automatique de pilotes d'imprimante fournis avec Windows	Activé	Toutes les versions VDA
Préférence de pilote universel	EMF ; XPS ; PCL5c ; PCL4 ; PS	Toutes les versions VDA
Utilisation du pilote d'impression universelle	Utiliser l'impression universelle uniquement si le pilote requis n'est pas disponible	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Activer le serveur d'impression universelle	Désactivée	Toutes les versions VDA
Port (CGP) du flux de données d'impression du serveur d'impression	7229	Toutes les

© 1999-2017 Citrix Systems, Inc. All rights reserved.

universelle		versions VDA
Limite de bande passante d'entrée du flux d'impression du serveur d'impression universelle (kpbs)	0	Toutes les versions VDA
Port (HTTP/SOAP) du service Web du serveur d'impression universelle	8080	Toutes les versions VDA
Serveurs d'impression universelle d'équilibrage de la charge		VDA 7.9 jusqu'à la version actuelle
Seuil au-delà duquel les serveurs d'impression universelle sont hors service	180 (secondes)	VDA 7.9 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
mode de traitement EMF de l'impression universelle ;	Spouler directement vers l'imprimante	Toutes les versions VDA
limite de compression d'image de l'impression universelle ;	Meilleure qualité (compression sans perte)	Toutes les versions VDA
valeurs par défaut de l'optimisation de l'impression universelle ;	Compression d'image • Qualité d'image souhaitée = Qualité standard • Activer la compression lourde = False Cache d'image et de police • Autoriser la mise en cache des images incorporées = True • Autoriser la mise en cache des polices incorporées = True Autoriser les non-administrateurs à modifier ces paramètres = False	Toutes les versions VDA
Préférence d'aperçu d'impression universelle	Ne pas utiliser l'aperçu pour les imprimantes créées automatiquement ou universelles génériques	Toutes les versions VDA
limite de qualité d'impression de l'impression universelle ;	Aucune limite	Toutes les versions VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Niveau de cryptage minimum SecureICA	De base	VDA pour OS 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Intervalle d'horloge inactive du serveur	0 millisecondes	VDA pour OS 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Horloge de session déconnectée	Désactivée	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Intervalle d'horloge de session déconnectée	1440 minute	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Minuteur de connexion de session	Désactivée	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Intervalle de minuteur de connexion de session (Session connection timer interval)	1440 minute	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Minuteur de session inactive	Activée	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Intervalle de minuteur de session inactive	1440 minute	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Connexions de fiabilité de session	Autorisé	Toutes les versions VDA
Numéro de port de la fiabilité de session	2598	Toutes les versions VDA
Expiration de délai de la fiabilité de session	180 secondes	Toutes les versions VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Estimer l'heure locale pour les clients d'ancienne génération	Activé	VDA pour OS 7 jusqu'à la version actuelle
Utilisation de l'heure locale du client	Utiliser le fuseau horaire du serveur	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Redirection de périphérique TWAIN client	Autorisé	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Niveau de compression TWAIN	Taille moyenne	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Règles d'optimisation des périphériques USB clients	Aucune règle n'est spécifiée.	VDA 7.6 FP3 jusqu'à la version actuelle
Redirection de périphérique USB client	Interdit	Toutes les versions VDA
Règles de redirection des périphériques USB clients	Aucune règle n'est spécifiée.	Toutes les versions VDA
Redirection de périphérique Plug and Play USB client	Autorisé	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Nombre de couleurs préféré pour les graphiques simples	24 bits par pixel	VDA 7.6 FP3 jusqu'à la version actuelle

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Taux de trames cible	30 fps	Toutes les versions VDA
Qualité visuelle	Taille moyenne	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Qualité d'image minimale	Normal	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Compression d'images en mouvement	Activé	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Niveau de compression progressif	Aucun(e)	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Valeur de seuil de compression progressif	2147483647 Kbps	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Taux de trame minimum cible	10 fps	VDA 5.5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Compression couleur supplémentaire	Désactivée	Toutes les versions VDA
Seuil de compression de couleur supplémentaire	8192 Kbps	Toutes les versions VDA
Compression intensive	Désactivée	Toutes les versions VDA
Niveau de compression avec perte	Taille moyenne	Toutes les versions VDA
Valeur de seuil de compression avec perte	2147483647 Kbps	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Connexions WebSockets	Interdit	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Numéro de port WebSockets	8008	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Liste de serveurs d'origine approuvés WebSockets	Le caractère générique est utilisé pour faire confiance à toutes les adresses URL Receiver pour Web.	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Tolérance d'ouvertures de session simultanée	2	VDA pour OS de serveur 7 jusqu'à la version actuelle
Utilisation UC	Désactivée	VDA pour OS de serveur 7 jusqu'à la version actuelle
Priorité de processus exclue de l'utilisation UC	Inférieure à la normale ou Basse	VDA pour OS de serveur 7 jusqu'à la version actuelle
Utilisation du disque	Désactivée	VDA pour OS de serveur 7 jusqu'à la version actuelle
Nombre maximum de sessions	250	VDA pour OS de serveur 7 jusqu'à la version actuelle
Utilisation de mémoire	Désactivée	VDA pour OS de serveur 7 jusqu'à la version actuelle
Charge de base d'utilisation mémoire	Charge zéro : 768 Mo	VDA pour OS de serveur 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Désactiver la configuration automatique	Désactivée	Toutes les versions VDA
Fermer la session de l'utilisateur si un problème se produit	Désactivée	Toutes les versions VDA
Nombre de tentatives d'accès à des fichiers verrouillés	5	Toutes les versions VDA
Traiter les cookies Internet à la fermeture de session	Désactivée	Toutes les versions VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Réécriture active	Désactivée	Toutes les versions VDA
Activer Profile Management	Désactivée	Toutes les versions VDA
Groupes exclus	Désactivée. Tous les membres des groupes d'utilisateurs sont traités.	Toutes les versions VDA
Prise en charge de profils hors connexion	Désactivée	Toutes les versions VDA
Chemin d'accès au magasin de l'utilisateur	Windows	Toutes les versions VDA
Traiter les ouvertures de session des administrateurs locaux	Désactivée	Toutes les versions VDA
Groupes traités	Désactivée. Tous les membres des groupes d'utilisateurs sont traités.	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Paramètres multi-plateformes des groupes d'utilisateurs	Désactivée. Tous les groupes d'utilisateurs spécifiés dans Groupes traités sont traités	Toutes les versions VDA
Activer les paramètres multi-plateformes	Désactivée	Toutes les versions VDA
Chemin d'accès aux définitions multi-plateformes	Désactivée. Aucun chemin n'est spécifié.	Toutes les versions VDA
Chemin d'accès au magasin des paramètres multi-plateformes	Désactivée. Windows\PM_CM est utilisé.	Toutes les versions VDA
Source de création des paramètres multi-plateformes	Désactivée	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Liste d'exclusion - répertoires	Désactivée. Tous les dossiers du profil utilisateur sont synchronisés.	Toutes les versions VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Liste d'exclusion - fichiers	Désactivée. Tous les fichiers du profil utilisateur sont synchronisés.	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Répertoires à synchroniser	Désactivée. Seuls les dossiers non exclus sont synchronisés.	Toutes les versions VDA
Fichiers à synchroniser	Désactivée. Seuls les fichiers non exclus sont synchronisés.	Toutes les versions VDA
Dossiers à mettre en miroir	Désactivée. Aucun dossier n'est mis en miroir.	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Accorder l'accès administrateur	Désactivée	Toutes les versions VDA
Inclure le nom de domaine	Désactivée	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Chemins d'accès au dossier AppData(Roaming)	Désactivée. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier AppData(Roaming)	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie AppData(Roaming)	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Chemin d'accès au dossier Contacts	Désactivée. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Contacts	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Contacts	Toutes les versions VDA

Nom	Paramètre par défaut	VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Chemin d'accès au dossier Bureau	Désactivée. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Bureau	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Bureau	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Chemin d'accès au dossier Mes documents	Désactivée. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Mes documents	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Documents	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Chemin d'accès au dossier Téléchargements	Désactivée. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Téléchargements	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Téléchargements	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Chemin d'accès au dossier Favoris	Désactivée. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Favoris	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Favoris	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Chemin d'accès au dossier Liens	Désactivée. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Liens	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Liens	Toutes les versions VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Chemin d'accès au dossier Ma musique	Désactivée. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Ma musique	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Musique	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Chemin d'accès au dossier Mes images	Désactivée. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Mes images	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Photos	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Chemin d'accès au dossier Parties enregistrées	Désactivée. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Parties enregistrées	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Jeux enregistrés	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Chemin d'accès au dossier Recherches	Désactivée. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Recherches	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Recherches	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Chemin d'accès au menu Démarrer	Désactivée. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du menu Démarrer	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Menu Démarrer	Toutes les versions VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Chemin d'accès au dossier Vidéo	Désactivée. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection pour la vidéo	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Vidéo	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Actions Active Directory	Désactivée	Toutes les versions VDA
Informations courantes	Désactivée	Toutes les versions VDA
Avertissements courants	Désactivée	Toutes les versions VDA
Activer la journalisation	Désactivée	Toutes les versions VDA
Actions du système de fichiers	Désactivée	Toutes les versions VDA
Notifications du système de fichiers	Désactivée	Toutes les versions VDA
Fermeture de session	Désactivée	Toutes les versions VDA
Ouverture de session	Désactivée	Toutes les versions VDA
Taille maximale du fichier journal	1048576	Toutes les versions VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
Chemin d'accès au fichier journal	Désactivée. Les fichiers journaux sont enregistrés à l'emplacement par défaut ; %SystemRoot%\System32\Logfiles\UserProfileManager.	Toutes les versions VDA
Informations utilisateur personnalisées	Désactivée	Toutes les versions VDA
Valeurs de stratégie à l'ouverture et fermeture de session	Désactivée	Toutes les versions VDA
Actions du registre	Désactivée	Toutes les versions VDA
Différences de registre à la fermeture de session	Désactivée	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Délai avant la suppression des profils du cache	0	Toutes les versions VDA
Supprimer les profils mis en cache localement à la fermeture de session	Désactivée	Toutes les versions VDA
Gestion des conflits de profils locaux	Utiliser profil local	Toutes les versions VDA
Migration des profils existants	Locaux et itinérants	Toutes les versions VDA
Chemin d'accès au profil modèle	Désactivée. Les nouveaux profils utilisateur sont créés à partir du profil utilisateur par défaut sur la machine sur laquelle un utilisateur ouvre une session.	Toutes les versions VDA
Le profil modèle remplace le profil local	Désactivée	Toutes

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
		les versions VDA
Le profil modèle remplace le profil itinérant	Désactivée	Toutes les versions VDA
Profil modèle utilisé en tant que profil Citrix obligatoire pour toutes les ouvertures de session	Désactivée	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Liste d'exclusion	Désactivée. Toutes les clés de registre dans la ruche HKCU sont traitées lorsqu'un utilisateur ferme sa session.	Toutes les versions VDA
Liste d'inclusion	Désactivée. Toutes les clés de registre dans la ruche HKCU sont traitées lorsqu'un utilisateur ferme sa session.	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Toujours mettre en cache	Désactivée	Toutes les versions VDA
Toujours mettre en cache la taille	0 Mo	Toutes les versions VDA
Streaming des profils	Désactivée	Toutes les versions VDA
Groupes des profils utilisateurs streamés	Désactivée. Tous les profils utilisateur d'une unité d'organisation sont traités normalement.	Toutes les versions VDA
Délai d'expiration des fichiers de verrous de la zone d'attente (jours)	1 jour	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Liste de comptes	Aucun magasin	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom	Paramètre par défaut	VDA
StoreFront	n'est spécifié.	bureau 7 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Masque réseau IPv6 d'enregistrement du contrôleur	Aucun masque réseau n'est spécifié.	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Port d'enregistrement du contrôleur	80	Toutes les versions VDA
SID de contrôleur	Aucun SID n'est spécifié.	Toutes les versions VDA
Controller	Aucun contrôleur n'est spécifié.	Toutes les versions VDA
Activer la mise à jour automatique des contrôleurs	Activé	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Uniquement utiliser l'enregistrement du contrôleur IPv6	Désactivée	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
GUID de site	Aucun GUID n'est spécifié.	Toutes les versions VDA

Nom	Paramètre par défaut	VDA
Prise en charge du bouclage d'adresse IP virtuelle	Désactivée	VDA 7.6 jusqu'à la version actuelle
Liste de programmes de bouclage virtuel d'adresse IP virtuelle	Aucun(e)	VDA 7.6 jusqu'à la version actuelle

Nom	Paramètre par défaut	VDA
Activer sans perte	Activé	VDA 5.5, 5.6 FP1
Paramètres de qualité HDX 3D Pro		VDA 5.5, 5.6 FP1

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Référence des paramètres de stratégie

Jul 07, 2016

Les stratégies contiennent des paramètres qui sont mis en œuvre lorsqu'elles sont appliquées. Les descriptions de cette section indiquent également si des paramètres supplémentaires sont requis pour activer une fonctionnalité ou sont similaires à un paramètre.

Les tableaux suivants présentent les paramètres que vous pouvez configurer au sein d'une stratégie. Recherchez la tâche que vous souhaitez effectuer dans la colonne de gauche, puis situez le paramètre qui lui correspond dans la colonne de droite.

Audio

Pour cette tâche	Utilisez ce paramètre de stratégie
Contrôler si vous souhaitez autoriser l'utilisation de plusieurs machines audio	Plug N Play audio
Contrôler l'autorisation de l'entrée audio depuis les microphones sur la machine utilisateur	Redirection du microphone client
Contrôler la qualité audio sur la machine utilisateur	Qualité audio
Contrôler le mappage audio vers les haut-parleurs de la machine utilisateur	Redirection audio du client

Bande passante des machines utilisateur

Pour limiter la bande passante utilisée pour	Utilisez ce paramètre de stratégie
Le mappage audio du client	• Limite de bande passante de la redirection audio ou • Pourcentage de limite de bande passante de la redirection audio
La copie et le collage à l'aide du Presse-papiers local	• Limite de bande passante de redirection du Presse-papiers ou • Pourcentage de la limite de la bande passante de redirection du Presse-papiers
L'accès aux lecteurs clients locaux dans les sessions	• Limite de bande passante de redirection de fichiers

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour limiter la bande passante utilisée pour	Utilisez ce paramètre de stratégie
	ou • Pourcentage de limite de bande passante de redirection de fichier
Accélération multimédia HDX MediaStream	• Limite de bande passante d'accélération multimédia HDX MediaStream ou • Pourcentage de limite de bande passante d'accélération multimédia HDX MediaStream
Session cliente	Limite de bande passante globale de session
Impression	• Limite de bande passante de redirection d'imprimante ou • Pourcentage de limite de bande passante de redirection de l'imprimante
Périphériques TWAIN (appareils photo, scanners, etc.)	• Limite de bande passante de redirection du périphérique TWAIN ou • Pourcentage de limite de bande passante de redirection du périphérique TWAIN
Périphériques USB	• Limite de bande passante de redirection du périphérique USB client ou • Pourcentage de limite de bande passante de redirection du périphérique USB client

Redirection des lecteurs clients et de machines utilisateur

Pour cette tâche	Utilisez ce paramètre de stratégie
Contrôler la connexion des lecteurs des machines clientes lors de l'ouverture des sessions utilisateur sur le serveur	Connecter automatiquement les lecteurs clients
Contrôler le transfert des données copiées ou coupées entre le serveur et le Presse-papiers local	Redirection de Presse-papiers client
Déterminer la méthode de mappage des lecteurs de la machine utilisateur	Redirection de lecteur client
Contrôler si les disques durs locaux des utilisateurs sont disponibles dans une session	• Lecteurs de disque fixe clients et • Redirection de lecteur client

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour cette tâche	Utilisez ce paramètre de stratégie
Contrôler si les lecteurs de disquette locaux des utilisateurs sont disponibles dans une session	• Lecteurs de disquette clients et • Redirection de lecteur client
Contrôler si les lecteurs réseau des utilisateurs sont disponibles dans une session	• Lecteurs réseau clients et • Redirection de lecteur client
Contrôler si les lecteurs de CD, de DVD ou Blu-ray locaux des utilisateurs sont disponibles dans une session	• Lecteurs optiques clients et • Redirection de lecteur client
Contrôler si les lecteurs amovibles locaux des utilisateurs sont disponibles dans une session	• Lecteurs amovibles clients et • Redirection de lecteur client
Contrôler si les périphériques TWAIN des utilisateurs, tels que les scanners et les appareils photo, sont disponibles dans une session et contrôler la compression des transferts de données d'image	• Redirection de périphérique TWAIN client • Redirection de compression TWAIN
Contrôler si les périphériques USB sont disponibles dans une session	• Redirection des périphériques USB clients et • Règles de redirection des périphériques USB clients
Améliorer la vitesse d'écriture et de copie des fichiers sur les disques clients via des réseaux étendus	Utiliser les écritures asynchrones

Redirection de contenu

Pour cette tâche	Utilisez ce paramètre de stratégie
Choisir d'utiliser ou non la redirection de contenu des serveurs vers la machine cliente	Redirection hôte vers client

UI de bureau

Pour cette tâche	Utilisez ce paramètre de stratégie
Contrôler si le papier peint du bureau est utilisé dans les sessions utilisateur	Papier peint du bureau
Afficher le contenu d'une fenêtre pendant son déplacement	Afficher le contenu de la fenêtre lors d'un cliquer déplacer

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour cette tâche	Utilisez ce paramètre de stratégie

Graphiques et multimédia

Pour cette tâche	Utilisez ce paramètre de stratégie
Contrôle le nombre maximal de trames par seconde envoyées aux machines utilisateur à partir des bureaux virtuels.	Taux de trames cible
Contrôle la qualité visuelle des images affichées sur la machine utilisateur.	Qualité visuelle
Contrôler si le contenu Flash est restitué dans les sessions	Comportement Flash par défaut
Contrôler si les sites Web peuvent afficher le contenu Flash lorsqu'il est accédé dans les sessions	• Liste d'adresses URL de récupération du contenu Flash côté serveur • Liste de compatibilité d'adresses URL Flash • Paramètre de stratégie de prévention du retour à la vidéo Flash • Erreur *.swf de prévention du retour à la vidéo Flash

Définition des priorités du trafic réseau multi-stream

Pour cette tâche	Utilisez ce paramètre de stratégie
Spécifiez des ports pour le trafic ICA au travers de plusieurs connexions et établissez des priorités de réseau	Stratégie Multi-Port
Activez la prise en charge des connexions multi-stream entre les serveurs et les machines utilisateur	Multi-stream (Paramètres Ordinateur et Utilisateur)

Imprimer

Pour cette tâche	Utilisez ce paramètre de stratégie
Contrôler la création des imprimantes clientes sur les machines clientes	o Créer automatiquement des imprimantes clientes et o Redirection d'imprimante cliente

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Contrôler l'emplacement auquel les propriétés d'imprimante sont stockées	Rétention des propriétés d'imprimante
Définir si les requêtes d'impression doivent être traitées par le client ou par le serveur	Connexions directes aux serveurs d'impression
Contrôler si les utilisateurs peuvent accéder aux imprimantes connectées à leurs machines clientes	Redirection d'imprimante cliente
Contrôler l'installation de pilotes Windows natifs lors de la création automatique des imprimantes clientes et des imprimantes réseau	Installation automatique de pilotes d'imprimante fournis avec Windows
Contrôler l'utilisation du pilote d'imprimante universel	Utilisation du pilote d'impression universelle
Choisir une imprimante en fonction des informations de la session de l'utilisateur itinérant	Imprimante par défaut
Équilibrer la charge et définir des seuils de basculement pour les serveurs d'impression universelle	o Serveurs d'impression universelle d'équilibrage de la charge o Seuil au-delà duquel les serveurs d'impression universelle sont hors service

Remarque : les stratégies ne peuvent pas être utilisées pour activer un écran de veille dans une session de bureau ou d'application. Si vous souhaitez activer un écran de veille, faites-le sur la machine utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie ICA

Jul 07, 2016

La section ICA contient des paramètres de stratégie liés aux connexions de l'écouteur ICA et au mappage vers le Presse-papiers.

Ce paramètre permet d'autoriser ou d'empêcher le mappage du Presse-papiers sur la machine utilisateur au Presse-papiers du serveur.

Par défaut, la redirection du Presse-papiers est autorisée.

Pour empêcher le transfert des données par couper-coller entre une session et le Presse-papiers local, sélectionnez Interdire. Les utilisateurs peuvent toujours couper-coller des données entre les applications exécutées dans les sessions.

Une fois ce paramètre autorisé, configurez la bande passante maximale que le Presse-papiers peut consommer dans une connexion cliente en utilisant le paramètre Limite de bande passante de redirection du Presse-papiers ou Pourcentage de limite de la bande passante de redirection du Presse-papiers.

Lorsque le paramètre Restreindre l'écriture dans le Presse-papiers client est activé, les données du Presse-papiers hôte ne peuvent être partagées avec le point de terminaison client mais vous pouvez utiliser ce paramètre pour autoriser des formats de données spécifiques devant être partagés avec le Presse-papiers de point de terminaison client. Pour utiliser ce paramètre, activez-le et ajoutez les formats spécifiques à autoriser.

Les formats de Presse-papiers suivantes sont définis par le système :

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

Les formats de Presse-papiers suivants sont prédéfinis dans XenApp et XenDesktop :
- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- Format HTML

Le format HTML est désactivé par défaut. Pour activer cette fonctionnalité :

- Assurez-vous que le paramètre **Redirection de Presse-papiers client** est autorisé.
- Assurez-vous que le paramètre **Restreindre écriture dans le Presse-papiers client** est activé.
- Ajoutez une entrée pour **Format HTML** (et les formats que vous souhaitez prendre en charge) dans **Formats d'écriture autorisés dans le Presse-papiers client**.

Remarque : l'activation de la prise en charge de la copie Presse-papiers du format HTML (Format HTML) copie les scripts (s'ils existent) depuis la source du contenu copié vers la destination. Assurez-vous que vous faites confiance à la source avant d'effectuer la copie. Si vous copiez un contenu contenant des scripts, ils ne seront actifs que si vous enregistrez le fichier de destination en tant que fichier HTML et l'exécutez.

Des formats personnalisés supplémentaires peuvent être ajoutés. Le nom de format personnalisé doit correspondre aux formats à enregistrer avec le système. Les noms de format sont sensibles à la casse.

Ce paramètre ne s'applique pas si soit Redirection de Presse-papiers client soit Restreindre l'écriture dans le Presse-papiers client est défini sur Interdit.

Ce paramètre autorise ou empêche les utilisateurs qui ne sont pas des administrateurs d'un groupe d'utilisateurs DirectAccess dans un VDA de se connecter à une session sur ce VDA à l'aide de connexions ICA.

Par défaut, les utilisateurs qui ne sont pas des administrateurs ne peuvent pas se connecter à ces sessions.

Ce paramètre n'a aucun effet sur les utilisateurs qui ne sont pas des administrateurs d'un groupe d'utilisateurs DirectAccess dans un VDA et qui utilisent une connexion Bureau à distance ; ces utilisateurs peuvent se connecter au VDA que ce paramètre soit activé ou désactivé. Ce paramètre n'a aucun effet sur les utilisateurs non administrateurs qui n'appartiennent pas à un groupe d'utilisateurs DirectAccess ; ces utilisateurs ne peuvent pas se connecter au VDA que ce paramètre soit activé ou désactivé.

Remarque : ce paramètre ne s'applique que pour les Virtual Delivery Agent 5.0, 5.5 et 5.6 Feature Pack 1.

Ce paramètre spécifie le temps d'attente maximal d'établissement d'une connexion utilisant le protocole ICA.

Par défaut, le temps d'attente maximal est de 120 000 millisecondes, soit deux minutes.

Ce paramètre spécifie le numéro de port TCP/IP utilisé par le protocole ICA sur le serveur.

Le numéro port est défini par défaut sur 1494.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Les numéros de port doivent être compris entre 0 et 65535 et ne doit pas entrer en conflit avec d'autres ports identifiés. Si vous modifiez le numéro de port, redémarrez le serveur pour prendre en compte la nouvelle valeur. Si vous modifiez le numéro de port sur le serveur, vous devez également le modifier sur chaque Citrix Receiver ou plug-in qui se connecte à ce serveur.

Ce paramètre spécifie si les applications initiales peuvent être lancées via RDP sur le serveur.

Par défaut, le lancement d'applications via RDP sur le serveur n'est pas autorisé.

Si ce paramètre est Autorisé, les données du Presse-papiers hôte ne peuvent être partagées avec le point de terminaison client. Vous pouvez autoriser des formats spécifiques en activant le paramètre Formats autorisés d'écriture dans le Presse-papiers client.

Par défaut, cette option est définie sur Interdit.

Si ce paramètre est Autorisé, les données du Presse-papiers client ne peuvent être partagées dans la session utilisateur. Vous pouvez autoriser des formats spécifiques en activant le paramètre Formats autorisés d'écriture dans le Presse-papiers de session.

Par défaut, cette option est définie sur Interdit.

Lorsque le paramètre Restreindre l'écriture dans le Presse-papiers de session est défini sur Autorisé, les données du Presse-papiers client ne peuvent être partagées avec les applications de session, mais vous pouvez utiliser ce paramètre pour autoriser des formats de données spécifiques à être partagés avec le Presse-papiers de session.

Les formats de Presse-papiers suivantes sont définis par le système :

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

Les formats de Presse-papiers suivants sont prédéfinis dans XenApp et XenDesktop :
- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- Format HTML

Le format HTML est désactivé par défaut. Pour activer cette fonctionnalité :

- Assurez-vous que le paramètre **Redirection de Presse-papiers client** est autorisé.
- Assurez-vous que le paramètre **Restreindre écriture dans le Presse-papiers de session** est activé.
- Ajoutez une entrée pour **Format HTML** (et les formats que vous souhaitez prendre en charge) dans **Formats d'écriture autorisés dans le Presse-papiers de session**.

Remarque : l'activation de la prise en charge de la copie Presse-papiers du format HTML (Format HTML) copie les scripts (s'ils existent) depuis la source du contenu copié vers la destination. Assurez-vous que vous faites confiance à la source avant d'effectuer la copie. Si vous copiez un contenu contenant des scripts, ils ne seront actifs que si vous enregistrez le fichier de destination en tant que fichier HTML et l'exécutez.

Des formats personnalisés supplémentaires peuvent être ajoutés. Le nom de format personnalisé doit correspondre aux formats à enregistrer avec le système. Les noms de format sont sensibles à la casse.

This setting does not apply if either the Client clipboard redirection setting or Restrict session clipboard write setting is set to Prohibited.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Reconnexion automatique des clients

Jul 07, 2016

La section Reconnexion automatique des clients contient des paramètres de stratégie permettant de contrôler la reconnexion automatique des sessions.

Ce paramètre permet d'activer ou de désactiver la reconnexion automatique par un même client après l'interruption d'une connexion.

Par défaut, la connexion automatique est autorisée.

L'activation de la reconnexion automatique permet aux utilisateurs de retrouver leur session dans l'état dans lequel elle se trouvait lors de l'interruption de la connexion. La fonction de reconnexion automatique détecte les connexions interrompues, puis reconnecte les utilisateurs à leurs sessions.

Cependant, la fonction de reconnexion automatique peut donner lieu à l'ouverture d'une nouvelle session (au lieu de la reconnexion à une session existante) si le cookie de Citrix Receiver, contenant la clé de l'ID de session et les informations d'identification, n'est pas utilisé. Le cookie n'est pas utilisé s'il a expiré, par exemple en raison d'un délai de reconnexion ou si les informations d'identification doivent être à nouveau entrées. La reconnexion automatique du client n'est pas déclenchée lorsqu'un utilisateur se déconnecte volontairement de sa session.

Pour les sessions d'application, si la reconnexion automatique est autorisée, Citrix Receiver essaie de se reconnecter à la session jusqu'à ce que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion.

Pour les sessions de bureau, si la reconnexion automatique est autorisée, Citrix Receiver tente de se reconnecter à la session pendant une période de temps spécifiée, à moins que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion. Par défaut, cette durée est de cinq minutes. Pour modifier cette durée, modifiez le registre sur la machine utilisateur :

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>
où secondes est le nombre de secondes après lequel aucune autre tentative de reconnexion à la session n'est effectuée.

Ce paramètre requiert une authentification pour les reconnexions automatiques des clients.

Par défaut, l'authentification n'est pas requise.

Lorsqu'un utilisateur ouvre initialement une session, ses informations d'identification sont cryptées, stockées dans la mémoire et un cookie est créé contenant la clé de cryptage qui est envoyée à Citrix Receiver. Si ce paramètre est configuré, les cookies ne sont pas utilisés. Au lieu de cela, une boîte de dialogue s'affiche auprès des utilisateurs, leur demandant de fournir leurs informations d'identification lorsque Citrix Receiver tente de se reconnecter automatiquement.

Ce paramètre permet d'activer ou de désactiver l'enregistrement des reconnexions automatiques des clients dans le journal d'événements.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Par défaut, la journalisation est désactivée.

Lorsqu'elle est activée, le Journal système du ou des serveurs reçoit les informations relatives aux échecs et aux réussites des tentatives de reconnexion automatique. Un site ne fournit pas de journal combinant les événements de reconnexion de tous les serveurs.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie audio

Jul 07, 2016

La section Audio contient des paramètres de stratégie pour autoriser une machine utilisateur à recevoir et à envoyer des données audio dans une session sans altérer les performances.

Transport en temps réel audio sur UDP

Ce paramètre permet ou empêche la transmission et la réception des données audio entre le VDA et la machine utilisateur sur RTP via le protocole UDP (User Datagram Protocol). Lorsque ce paramètre est désactivé, l'audio est envoyé et reçu sur TCP.

Par défaut, l'audio sur UDP est autorisé.

Plug N Play audio

Ce paramètre autorise ou empêche l'utilisation de plusieurs machines audio destinées à enregistrer et lire du son.

Par défaut, l'utilisation de plusieurs périphériques audio est autorisée.

Ce paramètre s'applique uniquement aux machines équipées du système d'exploitation Windows Server.

Qualité audio

Ce paramètre spécifie le niveau de qualité sonore reçu dans les sessions utilisateur.

Par défaut, la qualité audio est définie sur Élevée : audio à définition élevée.

Pour contrôler la qualité du son, choisissez l'une des options suivantes :

- Sélectionnez Faible : pour les connexions à basse vitesse pour les connexions disposant d'une faible bande passante. Les sons envoyés à la machine utilisateur sont compressés jusqu'à 16 Kbps. Cette compression a pour effet de dégrader la qualité sonore de manière significative mais permet des performances convenables pour une connexion disposant d'une bande passante faible.
- Sélectionnez Moyenne : optimisée pour le son de la voix pour mettre à disposition des applications Voix sur IP (VoIP), des applications multimédia pour des connexions réseau difficiles avec des lignes à moins de 512 Kbps, ou dans lesquelles les pertes de paquets sont importantes du fait de l'encombrement. Ce codec offre des temps de codage très rapides, ce qui est idéal pour une utilisation avec des softphones et des applications de communications unifiées lorsque le traitement multimédia doit s'effectuer du côté serveur.
  L'audio envoyé vers la machine utilisateur est compressé jusqu'à 64Kbps. Cette compression s'accompagne d'une baisse modérée de la qualité de l'audio restitué sur la machine utilisateur, tout en offrant une faible latence et consommant une faible bande passante. Si la qualité VoIP n'est pas satisfaisante, assurez-vous que le paramètre de stratégie transport en temps réel audio via UDP est défini sur Autorisé.

- Pour les connexions disposant d'une bande passante élevée et pour lesquelles la qualité sonore est importante, sélectionnez Élevée : audio haute définition. Les sons sont alors transmis aux clients à leurs taux d'origine. Les sons sont compressés à un niveau de qualité similaire à la qualité CD et utilisent une bande passante maximale de 112 Kbps. La transmission d'une telle quantité de données peut solliciter l'UC de façon intensive et provoquer un engorgement du réseau.

La bande passante n'est utilisée que lors d'un enregistrement ou d'une lecture. Si les deux opérations sont effectuées en

© 1999-2017 Citrix Systems, Inc. All rights reserved.

même temps, la consommation en bande passante est doublée.

Pour spécifier la quantité maximale de bande passante, configurez le paramètre Limite de bande passante de la redirection audio ou Pourcentage de limite de bande passante de la redirection audio.

Redirection audio du client

Ce paramètre spécifie si les applications hébergées sur le serveur peuvent lire des sons par l'intermédiaire d'un périphérique audio installé sur la machine utilisateur. Ce paramètre spécifie également si les utilisateurs peuvent enregistrer l'entrée audio.

Par défaut, la redirection audio est autorisée.

Après avoir activé ce paramètre, vous pouvez limiter la bande passante utilisée par la lecture ou l'enregistrement audio. Le fait de limiter la bande passante utilisée par l'audio peut améliorer les performances des applications, mais aussi dégrader la qualité sonore. La bande passante n'est utilisée que lors d'un enregistrement ou d'une lecture. Si les deux opérations sont effectuées en même temps, la consommation de bande passante est doublée. Pour spécifier la quantité maximale de bande passante, configurez le paramètre Limite de bande passante de la redirection audio ou Pourcentage de limite de bande passante de la redirection audio.

Sur les machines équipées d'un système d'exploitation Windows Server, vous devez également vous assurer que le paramètre Plug N Play audio est Activé pour prendre en charge plusieurs périphériques audio.

Important : l'interdiction de la redirection audio du client désactive toutes les fonctionnalités HDX audio.

Redirection du microphone client

Ce paramètre active ou désactive la redirection du microphone client. Lorsqu'il est activé, les clients peuvent utiliser des microphones pour enregistrer l'entrée audio dans une session.

Par défaut, la redirection du microphone est autorisée.

Pour des raisons de sécurité, les utilisateurs sont avertis si des serveurs non approuvés par leurs machines clientes essaient d'accéder à leurs micros. Les utilisateurs peuvent alors accepter ou refuser l'accès. Les utilisateurs peuvent désactiver l'alerte sur Citrix Receiver.

Sur les machines équipées d'un système d'exploitation Windows Server, vous devez également vous assurer que le paramètre Plug N Play audio est Activé pour prendre en charge plusieurs périphériques audio.

Si le paramètre Redirection audio du client est désactivé sur la machine cliente, cette règle n'a aucun effet.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie de bande passante

Jul 07, 2016

La section Bande passante contient des paramètres de stratégie pour éviter les problèmes de performances liés à l'utilisation de la bande passante des sessions clientes.

Important : l'utilisation de ces paramètres de stratégie avec les paramètres de stratégie Multi-Stream peut produire des résultats inattendus. Si vous utilisez les paramètres Multi-Stream dans une stratégie, assurez-vous que ces paramètres de stratégie de limite de bande passante ne sont pas inclus.

Limite de bande passante de redirection audio

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour la lecture ou l'enregistrement de données audio dans une session utilisateur.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de la redirection audio, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante de la redirection audio

Ce paramètre spécifie la limite de bande passante maximale autorisée pour la lecture ou l'enregistrement de données audio sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante de la redirection audio, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante de redirection du périphérique USB client

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour la redirection des périphériques USB vers et depuis le client.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de redirection du périphérique USB client, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante de redirection du périphérique USB client

Ce paramètre spécifie la bande passante maximale autorisée pour la redirection de périphériques USB vers et depuis le client sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante de redirection du périphérique USB client, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante de redirection du Presse-papiers

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour le transfert des données entre une session et le Presse-papiers local.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de la bande passante de redirection du Presse-papiers, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de la limite de la bande passante de redirection du Presse-papiers

Ce paramètre spécifie la bande passante maximale autorisée pour le transfert de données entre une session et le Presse-papiers local sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante de redirection du Presse-papiers, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante pour la redirection du port COM

Remarque : pour Virtual Delivery Agent 7.0 à 7.8, configurez ce paramètre à l'aide du registre ; consultez la section Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.
Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour l'accès à un port COM dans une connexion cliente. Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de redirection du port COM, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante de redirection du port COM

Remarque : pour Virtual Delivery Agent 7.0 à 7.8, configurez ce paramètre à l'aide du registre ; consultez la section Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.
Ce paramètre spécifie la bande passante maximale autorisée pour l'accès aux ports COM dans une connexion cliente, sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante pour la redirection du port COM, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante de redirection de fichier

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour l'accès à un lecteur client dans une session utilisateur.

Par défaut, aucun maximum (zéro) n'est spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de redirection de fichier, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante de redirection de fichier

Ce paramètre spécifie la limite de bande passante maximale autorisée pour l'accès aux lecteurs clients sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante de redirection de fichier, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante d'accélération multimédia HDX MediaStream

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour la mise à disposition d'audio et de vidéo à l'aide de l'accélération multimédia HDX MediaStream.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante d'accélération multimédia HDX MediaStream, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante d'accélération multimédia HDX MediaStream

Ce paramètre spécifie la bande passante maximale autorisée pour la mise à disposition d'audio et de vidéo à l'aide de l'Accélération multimédia HDX MediaStream sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante d'accélération multimédia HDX MediaStream, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante pour la redirection du port LPT

Remarque : pour Virtual Delivery Agent 7.0 à 7.8, configurez ce paramètre à l'aide du registre ; consultez la section Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.
Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour les tâches d'impression utilisant un port LPT dans une session utilisateur unique.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de redirection du port LPT, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante de redirection du port LPT

Remarque : pour Virtual Delivery Agent 7.0 à 7.8, configurez ce paramètre à l'aide du registre ; consultez la section

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.

Ce paramètre spécifie la limite de bande passante pour les tâches d'impression utilisant un port LPT dans une session cliente unique sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante pour la redirection du port LPT, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante globale de session

Ce paramètre spécifie la bande passante totale disponible, en kilobits par seconde, pour les sessions utilisateur.

La limite de bande passante maximale exécutoire est de 10 Mbps (10 000 Kbps). Par défaut, aucun maximum (zéro) n'est spécifié.

Le fait de limiter la bande passante utilisée par une connexion cliente peut améliorer les performances lorsque d'autres applications en dehors de la connexion cliente sont en concurrence et que la bande passante disponible est réduite.

Limite de bande passante de redirection d'imprimante

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour l'accès aux imprimantes clientes dans une session utilisateur.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de redirection de l'imprimante, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante de redirection de l'imprimante

Ce paramètre spécifie la bande passante maximale autorisée pour l'accès aux imprimantes clientes sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante de redirection d'imprimante, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante de redirection du périphérique TWAIN

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour le contrôle des périphériques d'images TWAIN à partir d'applications publiées.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de redirection du périphérique TWAIN, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pourcentage de limite de bande passante de redirection du périphérique TWAIN

Ce paramètre spécifie la bande passante maximale autorisée pour le contrôle des périphériques d'images TWAIN à partir d'applications publiées sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante de redirection du périphérique TWAIN, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Capteurs clients

Jul 07, 2016

La section Capteurs clients contient des paramètres de stratégie permettant de contrôler la manière dont les informations de capteurs d'appareils mobiles sont gérées dans une session utilisateur.

Cette option permet aux applications d'utiliser l'emplacement physique de la machine cliente.

Ce paramètre détermine si les applications exécutées dans une session sur un appareil mobile sont autorisées à utiliser l'emplacement physique de la machine cliente.

Par défaut, l'utilisation des informations d'emplacement est interdite.

Lorsque ce paramètre est interdit, les tentatives par une application de récupération des informations d'emplacement retournent une valeur de « permission refusée ».

Lorsque ce paramètre est activé, un utilisateur peut interdire l'utilisation des informations d'emplacement en refusant une requête de Citrix Receiver pour accéder à l'emplacement. Les appareils Android et iOS invitent la saisie des informations d'emplacement lors de la première requête de chaque session.

Lors du développement d'applications hébergées qui utilisent le paramètre Permettre aux applications d'utiliser l'emplacement physique de la machine cliente, considérez ce qui suit :

- Une application pour laquelle l'emplacement est activé ne devrait pas compter sur la disponibilité des informations d'emplacement, car :
  - Il se peut qu'un utilisateur n'ait pas accès aux informations d'emplacement.
  - Il se peut que l'emplacement ne soit pas disponible ou soit modifié lors de l'exécution de l'application.
  - Il se peut qu'un utilisateur se connecte à la session d'application depuis une machine différente qui ne prend pas en charge les informations d'emplacement.
- Une application pour laquelle l'emplacement est activé doit :
  - posséder la fonctionnalité d'emplacement désactivée par défaut ;
  - offrir une option utilisateur pour permettre ou interdire la fonctionnalité lors de l'exécution de l'application ;
  - offrir une option utilisateur pour effacer les données d'emplacement cachées par l'application. (Citrix Receiver ne cache pas les données d'emplacement.)
- Une application pour laquelle l'emplacement est activé doit gérer la précision des informations d'emplacement afin que les données acquises soient appropriées aux fins de l'application et se conforme aux régulations dans tous les territoires appropriés.
- Une connexion sécurisée (par exemple, en utilisant TLS ou un VPN) devrait être mise en application lors de l'utilisation des services d'emplacement. Citrix Receiver devrait se connecter aux serveurs de confiance.
- Considérez l'obtention de conseils juridiques quant à l'utilisation des services d'emplacement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Interface utilisateur de bureau

Aug 22, 2016

La section UI de bureau contient des paramètres de stratégie qui contrôlent les effets visuels, tels que le papier peint du bureau, les animations de menu et le glisser-déplacer des images, pour gérer la bande passante utilisée dans les connexions clientes. Vous pouvez améliorer les performances des applications sur un réseau étendu en limitant la consommation de la bande passante.

Redirection Desktop Composition

Ce paramètre indique s'il faut utiliser la capacité de traitement de l'unité de traitement graphique (GPU) ou intégré processeur graphique (IGP) sur la machine utilisateur pour la restitution des graphiques DirectX locaux pour offrir aux utilisateurs une expérience de bureau Windows plus fluide. Lorsque cette option est activée, la redirection de la composition du bureau offre une expérience Windows très réactive tout en conservant une évolutivité élevée sur le serveur.

Par défaut, la redirection Desktop Composition est désactivée.

Pour désactiver la redirection Desktop Composition et réduire la bande passante requise dans les sessions utilisateur, sélectionnez Désactivée lorsque vous ajoutez ce paramètre à une stratégie.

Qualité graphique de redirection Desktop Composition

Ce paramètre spécifie la qualité des graphiques utilisés pour la redirection Desktop Composition.

Par défaut, ce paramètre est défini sur Élevée.

Choisissez entre les qualités Élevée, Moyenne, Basse ou Sans perte.

Papier peint du bureau

Ce paramètre autorise ou empêche l'affichage du papier-peint dans les sessions utilisateur.

Par défaut, les sessions utilisateur peuvent afficher le papier peint.

Pour désactiver le papier peint et réduire la bande passante requise dans les sessions utilisateur, sélectionnez Interdit lorsque vous ajoutez ce paramètre à la stratégie.

Animation de menu

Ce paramètre autorise ou empêche les animations de menu dans les sessions utilisateur.

Par défaut, l'animation de menu est autorisée.

L'animation de menu est un paramètre de préférence personnelle Microsoft destiné à faciliter l'accès. Lorsque cette option est activée, elle entraîne l'affichage d'un menu après un bref délai, en effectuant un défilement ou un fondu. Une icône de flèche s'affiche en bas du menu. Le menu s'affiche lorsque vous placez la souris sur cette flèche.

L'animation de menu est activée sur un bureau si ce paramètre de stratégie est réglé sur Autorisé et que le paramètre de préférence personnelle de Microsoft est activé.

Remarque : toute modification apportée au paramètre de préférence personnelle de Microsoft est apportée au bureau. Cela signifie que si le bureau est défini pour ignorer les modifications à la fin de la session, même si un utilisateur a activé les

© 1999-2017 Citrix Systems, Inc. All rights reserved.

animations de menu dans une session, l'animation de menu ne sera pas disponible dans les prochaines sessions sur le bureau. Pour les utilisateurs qui nécessitent l'animation de menu, activez le paramètre Microsoft dans l'image principale du bureau ou assurez-vous que le bureau conserve les modifications apportées par l'utilisateur.

Afficher le contenu de la fenêtre lors d'un cliquer déplacer

Ce paramètre autorise ou empêche l'affichage des contenus de fenêtre lors d'un glisser-déplacer d'une fenêtre au travers de l'écran.

Par défaut, l'affichage du contenu de la fenêtre est autorisé.

S'il a la valeur Autorisé, la fenêtre entière semble se déplacer lorsque vous la faites glisser. S'il a la valeur Interdit, seul le contour de la fenêtre semble se déplacer jusqu'à ce que vous relâchiez le bouton.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Contrôle de l'utilisateur final

Jul 07, 2016

La section Contrôle de l'utilisateur final contient des paramètres de stratégie permettant de mesurer le trafic de session.

Calcul des boucles ICA

Ce paramètre détermine si les calculs de boucle ICA sont exécutés pour les connexions actives.

Par défaut, les calculs des connexions actives sont activés.

Par défaut, chaque initiation de mesure des boucles ICA est retardée jusqu'à l'apparition de trafic indiquant une interaction avec l'utilisateur. Ce retard, dont la longueur peut s'avérer indéfinie, est conçu pour empêcher que la mesure des boucles ICA devienne la seule raison du trafic ICA.

Calcul des boucles ICA

Ce paramètre spécifie la fréquence d'exécution (en secondes) des calculs des boucles ICA.

Par défaut, les boucles ICA sont calculées toutes les 15 secondes.

Calcul des boucles ICA pour les connexions inactives

Ce paramètre détermine si les calculs de boucle ICA sont exécutés pour les connexions inactives.

Par défaut, les calculs ne sont pas exécutés pour les connexions inactives.

Par défaut, chaque initiation de mesure des boucles ICA est retardée jusqu'à l'apparition de trafic indiquant une interaction avec l'utilisateur. Ce retard, dont la longueur peut s'avérer indéfinie, est conçu pour empêcher que la mesure des boucles ICA devienne la seule raison du trafic ICA.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètre de stratégie Expérience de bureau améliorée

Jul 07, 2016

Les sessions du paramètre de stratégie Expérience de bureau améliorée exécutées sur des systèmes d'exploitation serveur afin de ressembler à des bureaux Windows 7 locaux, offrant aux utilisateurs une expérience de bureau améliorée.

Par défaut, ce paramètre est autorisé.

Si un profil utilisateur avec un thème Windows Classic existe déjà sur le bureau virtuel, l'activation de cette stratégie n'offre pas une expérience utilisateur améliorée pour cet utilisateur. Si un utilisateur, avec un profil utilisateur de thème Windows 7, ouvre une session sur un bureau virtuel exécutant Windows Server 2012 pour lequel cette stratégie n'est soit pas configurée soit désactivée, cet utilisateur aperçoit un message d'erreur indiquant l'échec d'application du thème.

Dans les deux cas, la réinitialisation du profil utilisateur résout le problème.

Si la stratégie change d'un état activé à désactivé sur un bureau virtuel avec des sessions utilisateur actives, l'apparence de ces sessions est incohérente avec l'expérience de bureau Windows 7 et Windows Classic. Pour éviter ce problème, assurez-vous de redémarrer le bureau virtuel après la modification de ce paramètre de stratégie. Vous devez également supprimer tous les profils itinérants sur le bureau virtuel. Citrix recommande également de supprimer tous les profils d'utilisateur sur le bureau virtuel pour éviter des incohérences entre les profils.

Si vous utilisez des profils d'utilisateurs itinérants dans votre environnement, assurez-vous que la fonctionnalité Expérience de bureau améliorée est activée ou désactivée pour tous les bureaux virtuels qui partagent un profil.

Citrix ne recommande pas de partager les profils itinérants entre bureaux virtuels exécutant des systèmes d'exploitation serveur et des systèmes d'exploitation clients. Les profils des systèmes d'exploitation clients et serveurs diffèrent et le partage des profils itinérants sur les deux types de systèmes d'exploitation peut provoquer des incohérences dans les propriétés de profil lorsqu'un utilisateur passe de l'un à l'autre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie de la redirection de fichier

Jul 07, 2016

La section Redirection de fichier contient les paramètres de stratégie liés au mappage des lecteurs clients et à leur optimisation.

Connecter automatiquement les lecteurs clients

Ce paramètre autorise ou empêche la connexion automatique des lecteurs clients lorsque les utilisateurs ouvrent une session.

Par défaut, la connexion automatique est autorisée.

Lorsque vous ajoutez ce paramètre à une stratégie, assurez-vous d'activer les paramètres pour les types de lecteurs que vous souhaitez connecter automatiquement. Par exemple, pour permettre la connexion automatique des lecteurs de CD-ROM des utilisateurs, configurez ce paramètre ainsi que le paramètre Lecteurs optiques clients.

Les paramètres de stratégie suivants sont associés :

- Redirection de lecteur client
- Lecteurs de disquette clients
- Lecteurs optiques clients
- Lecteurs fixes clients
- Lecteurs réseau clients
- Lecteurs amovibles clients

Redirection de lecteur client

Ce paramètre active ou désactive la redirection de lecteur depuis et vers les lecteurs de la machine utilisateur.

Par défaut, la redirection de fichiers est activée.

Lorsqu'il est activé, les utilisateurs peuvent enregistrer des fichiers dans tous leurs lecteurs clients. Lorsqu'il est désactivé, la redirection des fichiers est interdite, quel que soit l'état des paramètres de redirection de fichiers individuels tels que Lecteurs de disquette clients et Lecteurs réseau clients.

Les paramètres de stratégie suivants sont associés :

- Lecteurs de disquette clients
- Lecteurs optiques clients
- Lecteurs fixes clients
- Lecteurs réseau clients
- Lecteurs amovibles clients

Lecteurs fixes clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs de disque fixes de la machine utilisateur.

Par défaut, l'accès aux lecteurs fixes clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs fixes clients ne sont pas mappés et les utilisateurs ne

© 1999-2017 Citrix Systems, Inc. All rights reserved.

peuvent pas y accéder manuellement, quel que soit l'état du paramètre Lecteurs de disque fixe clients.

Pour être certain que les lecteurs de disque fixe sont automatiquement connectés lorsque les utilisateurs ouvrent une session, configurez le paramètre Connecter automatiquement les lecteurs clients.

Lecteurs de disquette clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs de disquette de la machine utilisateur.

Par défaut, l'accès aux lecteurs de disquette clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs de disquette clients ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement, quel que soit l'état du paramètre Lecteurs de disquette clients.

Pour garantir la connexion automatique des lecteurs de disquette lors de l'ouverture de session des utilisateurs, configurez le paramètre Connecter automatiquement les lecteurs clients.

Lecteurs réseau clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs réseau (distants) par l'intermédiaire de la machine utilisateur.

Par défaut, l'accès aux lecteurs réseau clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs réseau clients ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement, quel que soit l'état du paramètre Lecteurs réseau clients.

Pour garantir la connexion automatique des lecteurs réseau lors de l'ouverture de session des utilisateurs, configurez le paramètre Connecter automatiquement les lecteurs clients.

Lecteurs optiques clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs de CD-ROM, DVD-ROM et BD-ROM de la machine utilisateur.

Par défaut, l'accès aux lecteurs optiques clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs optiques ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement, quel que soit l'état du paramètre Lecteurs optiques clients.

Pour garantir la connexion automatique des lecteurs optiques lors de l'ouverture de session des utilisateurs, configurez le paramètre Connecter automatiquement les lecteurs clients.

Lecteurs amovibles clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs USB de la machine utilisateur.

Par défaut, l'accès aux lecteurs amovibles clients est autorisé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs amovibles clients ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement, quel que soit l'état du paramètre Lecteurs amovibles clients.

Pour garantir la connexion automatique des lecteurs amovibles lors de l'ouverture de session des utilisateurs, configurez le paramètre Connecter automatiquement les lecteurs clients.

Redirection hôte vers client

Ce paramètre active ou désactive les associations de type de fichier pour les URL et le contenu de certains supports devant être ouverts sur la machine utilisateur. Lorsqu'elles sont désactivées, le contenu s'ouvre sur le serveur.

Par défaut, l'association de type de fichier est désactivée.

Ces types d'URL sont ouverts localement lorsque vous activez ce paramètre :

- HTTP (Hypertext Transfer Protocol) ;
- HTTPS (Secure Hypertext Transfer Protocol) ;
- Real Player et QuickTime (RTSP) ;
- Real Player et QuickTime (RTSPU) ;
- anciennes versions de Real Player (PNM) ;
- Microsoft Media Server (MMS)

Préserver les lettres de lecteurs clients

Ce paramètre active ou désactive le mappage des lecteurs client sur la même lettre de lecteur dans la session.

Par défaut, les lettres de lecteur client ne sont pas conservées.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé.

Accès en lecture unique sur le lecteur client

Ce paramètre autorise les utilisateurs et les applications à créer ou modifier des fichiers sur les lecteurs clients mappés ou les en empêche.

Par défaut, les fichiers et les dossiers sur les lecteurs clients mappés peuvent être modifiés.

Si cette option est définie sur Activée, les fichiers et dossiers sont accessibles avec des permissions en lecture seule.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé.

Redirection vers les dossiers spéciaux

Ce paramètre autorise ou empêche les utilisateurs Citrix Receiver et l'Interface Web de voir leurs dossiers spéciaux Documents et Bureau locaux à partir d'une session.

Par défaut, la redirection vers les dossiers spéciaux est autorisée.

Ce paramètre empêche les objets filtrés via une stratégie d'être redirigés vers les dossiers spéciaux, quels que soient les paramètres existant ailleurs. Lorsque ce paramètre est interdit, tous les paramètres connexes spécifiés pour StoreFront, l'Interface Web ou Citrix Receiver sont ignorés.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour déterminer les utilisateurs autorisés à disposer d'une redirection vers les dossiers spéciaux, sélectionnez Autorisé et incluez ce paramètre dans une stratégie filtrée sur les utilisateurs que vous souhaitez voir disposer de cette fonctionnalité. Ce paramètre remplace tous les autres paramètres de redirection vers les dossiers spéciaux.

Dans la mesure où la redirection vers les dossiers spéciaux doit interagir avec la machine utilisateur, les paramètres de stratégie qui empêchent les utilisateurs d'accéder à leurs lecteurs de disque fixe locaux et d'y enregistrer des fichiers empêchent également la redirection vers les dossiers spéciaux de fonctionner.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Lecteurs fixes clients est présent et défini sur Autorisé.

Utiliser les écritures asynchrones

Ce paramètre active ou désactive les écritures asynchrones sur disque.

Par défaut, les écritures asynchrones sont désactivées.

Les écritures asynchrones sur disque peuvent accélérer la vitesse de transfert et d'écriture de fichiers sur les disques clients via des réseaux étendus, généralement caractérisés par une bande passante relativement élevée et une forte latence. Toutefois, en présence d'une erreur de connexion ou de disque, il est possible que le ou les fichiers clients en cours d'écriture se retrouvent dans un état indéfini. Si cela se produit, une fenêtre contextuelle indique à l'utilisateur les fichiers affectés. L'utilisateur peut alors prendre une mesure corrective, par exemple en redémarrant un transfert de fichiers interrompu lors de la reconnexion ou une fois l'erreur de disque corrigée.

Citrix recommande de n'activer l'écriture asynchrone sur disque que pour les utilisateurs nécessitant une connexion distante dotée d'une rapidité d'accès aux fichiers satisfaisante et capables de réparer facilement la perte de fichiers ou de données causée par une erreur de connexion ou de disque.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé. Si ce paramètre est désactivé, aucune écriture asynchrone n'aura lieu.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Redirection Flash

Jul 07, 2016

La section Redirection Flash contient les paramètres de stratégie permettant de gérer le contenu Flash dans les sessions utilisateur.

Accélération Flash

Ce paramètre permet d'activer ou de désactiver la restitution du contenu Flash sur les machines utilisateur plutôt que sur le serveur. Par défaut, la restitution du contenu Flash côté client est activée.

Remarque : ce paramètre est utilisé pour la redirection Flash d'ancienne génération avec Citrix Online Plug-in 12.1. Lorsqu'il est activé, ce paramètre réduit la charge du réseau et du serveur en restituant le contenu Flash sur la machine utilisateur. De plus, le paramètre Liste de compatibilité d'adresses URL Flash force la restitution du contenu Flash de sites Web spécifiques sur le serveur.

Sur la machine utilisateur, le paramètre Activer HDX MediaStream pour Flash sur la machine cliente doit être également activé.

Lorsque ce paramètre est désactivé, le contenu Flash de tous les sites Web, quelle que soit leur adresse URL, est restitué sur le serveur. Pour ne permettre qu'à certains sites Web de restituer du contenu Flash sur la machine utilisateur, configurez le paramètre Liste de compatibilité d'adresses URL Flash.

Liste de couleur d'arrière-plan Flash

Ce paramètre vous permet de définir les couleurs clés pour certaines adresses URL.

Par défaut, aucune couleur clé n'est spécifiée.

Les couleurs clés s'affichent à l'arrière des contenus Flash restitués sur les clients et aident à offrir une détection de région visible. Les couleurs clés spécifiées doivent être rares ; sinon, la détection de région visible risque de ne pas fonctionner correctement.

Les entrées valides consistent en une adresse URL (avec des caractères génériques facultatifs situés au début et à la fin) suivie d'un code de couleur hexadécimal 24 bits RGB. Exemple : http://citrix.com 000003.

Assurez-vous que l'adresse URL spécifiée est l'adresse URL du contenu Flash, qui peut être différente de l'adresse URL du site Web.

> **Avertissement**
>
> Une mauvaise utilisation de l'Éditeur du Registre peut entraîner de sérieux problèmes et nécessiter la réinstallation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Veillez à effectuer une copie de sauvegarde avant de modifier le registre.

Sur les VDA exécutant Windows 8 ou Windows 2012, ce paramètre peut ne pas parvenir à définir des couleurs clés pour l'adresse URL. Si cela se produit, modifiez le registre sur le VDA.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour les machines 32 bits, utilisez ce paramètre de registre :

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
"ForceHDXFlashEnabled"=dword:00000001

Pour les machines 64 bits, utilisez ce paramètre de registre :

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
"ForceHDXFlashEnabled"=dword:00000001

Compatibilité à effet rétroactif Flash

Ce paramètre active ou désactive l'utilisation des fonctionnalités de redirection Flash originales, d'ancienne génération avec d'anciennes versions de Citrix Receiver (anciennement appelé Citrix Online Plug-in).

Ce paramètre est activé par défaut.

Sur la machine utilisateur, le paramètre Activer HDX MediaStream pour Flash sur la machine cliente doit être également activé.

Les fonctionnalités de redirection Flash de seconde génération sont activées pour être utilisées avec Citrix Receiver 3.0. Les fonctionnalités de redirection d'ancienne génération sont prises en charge pour être utilisées avec Citrix Online Plug-in 12.1. Pour vous assurer que les fonctionnalités Flash de seconde génération sont utilisées, la redirection Flash de seconde génération doit être activée à la fois sur le serveur et la machine utilisateur. Si la redirection d'ancienne génération est activée soit sur le serveur soit sur la machine utilisateur, les fonctionnalités de redirection d'ancienne génération sont utilisées.

Comportement Flash par défaut

Ce paramètre établit le comportement par défaut de l'accélération Flash de seconde génération.

Par défaut, l'accélération Flash est activée.

Pour contrôler ce paramètre, choisissez l'une des options suivantes :

- Activer l'accélération Flash : la redirection Flash est utilisée.
- Bloquer le lecteur Flash : la redirection Flash et la restitution côté serveur ne sont pas utilisées. L'utilisateur ne peut visualiser aucun contenu Flash.
- Désactiver l'accélération Flash : la redirection Flash n'est pas utilisée. L'utilisateur peut visualiser le contenu Flash restitué côté serveur si une version du lecteur Adobe Flash Player compatible avec Windows Internet Explorer est installée sur le serveur.

Ce paramètre peut être remplacé pour des pages Web individuelles et des instances Flash basées sur la configuration du paramètre Liste de compatibilité d'adresses URL Flash. De plus, sur la machine utilisateur, le paramètre Activer HDX MediaStream pour Flash sur la machine cliente doit être également activé.

Journalisation d'événements Flash

Ce paramètre autorise l'enregistrement des événements Flash dans le journal d'événements d'application Windows.

Par défaut, la journalisation est autorisée.

Sur les ordinateurs exécutant Windows 7 ou Windows Vista, un journal spécifique à la redirection Flash s'affiche dans le nœud du journal Applications et services.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Retour intelligent Flash

Ce paramètre active et désactive les tentatives automatiques d'utiliser la restitution côté serveur des instances du lecteur Flash où la restitution côté client n'est soit pas nécessaire ou soit offre une expérience utilisateur appauvrie.

Ce paramètre est activé par défaut.

Seuil de latence Flash

Ce paramètre spécifie un seuil entre 0 et 30 millisecondes pour déterminer l'emplacement de restitution du contenu Adobe Flash.

Par défaut, le seuil est de 30 millisecondes.

Durant le démarrage, HDX MediaStream pour Flash mesure la latence actuelle entre le serveur et la machine utilisateur. Si la latence se trouve en dessous de ce seuil, HDX MediaStream pour Flash est utilisé pour restituer le contenu Adobe Flash sur la machine utilisateur. Si la latence se trouve au-dessus de ce seuil, le serveur réseau restitue le contenu si un lecteur Adobe Flash est disponible à cet endroit.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Compatibilité à effet rétroactif Flash est également présent et défini sur Activé.

Remarque : s'applique uniquement lors de l'utilisation de la redirection HDX MediaStream Flash en mode d'ancienne génération.

Prévention du retour à la vidéo Flash

Ce paramètre spécifie si et comment le contenu Flash « de petite taille » est restitué et affiché pour les utilisateurs.

Ce paramètre n'est pas configuré par défaut.

Pour contrôler ce paramètre, choisissez l'une des options suivantes :

- **Contenu de petite taille uniquement.** Seul le contenu de retour intelligent sera restitué sur le serveur ; tout autre contenu Flash sera remplacé par un fichier d'erreur *.swf.
- **Contenu de petite taille uniquement avec client pris en charge.** Seul le contenu de retour intelligent sera restitué sur le serveur si le client utilise la redirection Flash ; tout autre contenu sera remplacé par un fichier d'erreur *.swf.
- **Aucun contenu du côté serveur.** Tout le contenu sur le serveur sera remplacé par une erreur *swf.

Pour utiliser ce paramètre de stratégie, vous devez spécifier un fichier d'erreur *.swf. Ce fichier d'erreur *.swf remplacera tout contenu que vous ne souhaitez pas restituer sur le VDA.

Erreur *.swf de prévention du retour à la vidéo Flash

Ce paramètre spécifie l'adresse URL du message d'erreur qui s'affiche pour les utilisateurs pour remplacer des instances Flash lorsque les stratégies de gestion de charge du serveur sont en cours d'utilisation. Par exemple :

http://NomDomaine.tld/sample/path/error.swf

Liste d'adresses URL de récupération du contenu Flash côté serveur

Ce paramètre spécifie les sites Web pour lesquels le contenu Flash peut être téléchargé vers le serveur, puis transféré à la machine utilisateur pour restitution.

Par défaut, aucun site n'est spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ce paramètre est utilisé lorsque la machine utilisateur n'ait pas accès direct à Internet ; le serveur offre cette connexion. De plus, sur la machine utilisateur, le paramètre Activer la récupération de contenu côté serveur doit être activé.

La redirection Flash de seconde génération comprend un retour vers la récupération de contenu côté serveur pour les fichiers .swf Flash. Si la machine utilisateur est incapable de restituer du contenu Flash depuis un site Web, et que le site Web est spécifié dans la liste d'adresses URL de récupération de contenu côté serveur, la récupération de contenu côté serveur se produit automatiquement.

Lors de l'ajout d'adresses URL à la liste :

- Ajoutez l'adresse URL de l'application Flash au lieu de la page HTML de niveau supérieur qui initie le lecteur Flash.
- Utilisez un astérisque (*) comme caractère générique au début ou à la fin de l'adresse URL.
- Utilisez un caractère générique de fin pour autoriser toutes les adresses URL enfant (http://www.citrix.com/*).
- Les préfixes http:// ou https:// sont utilisés lorsqu'ils sont présents, mais ne sont pas requis pour des entrées de liste valides.

Liste de compatibilité d'adresses URL Flash

Ce paramètre spécifie les règles qui déterminent si le contenu Flash de certains sites Web est restitué sur la machine utilisateur, restitué sur le serveur ou si la restitution est bloquée.

Par défaut, aucune règle n'est spécifiée.

Lors de l'ajout d'adresses URL à la liste :

- Ordonnez la liste par ordre de priorité avec les adresses URL, les actions et l'emplacement de restitution les plus importants en haut de celle-ci.
- Utilisez un astérisque (*) comme caractère générique au début ou à la fin de l'adresse URL.
- Utilisez un caractère générique de fin pour faire référence à toutes les adresses URL enfant (http://www.citrix.com/*).
- Les préfixes http:// ou https:// sont utilisés lorsqu'ils sont présents, mais ne sont pas requis pour des entrées de liste valides.
- Ajoutez à cette liste les sites Web dont le contenu Flash n'est pas restitué correctement sur la machine utilisateur et sélectionnez soit l'option Restituer sur le serveur soit l'option Bloquer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Graphiques

Jul 07, 2016

La section Graphiques contient des paramètres de stratégie permettant de contrôler le traitement des images dans les sessions utilisateur.

Autoriser la compression visuelle sans perte

Ce paramètre permet d'utiliser une compression visuellement sans perte au lieu d'une compression vraie sans perte pour l'affichage des graphiques. La compression visuellement sans perte améliore les performances par rapport à la compression vraie sans perte, mais engendre une perte mineure qui ne peut être remarquée à l'œil nu. Ce paramètre change la manière dont les valeurs du paramètre « Qualité visuelle » sont utilisées.

Par défaut, ce paramètre est désactivé.

Limite de mémoire d'affichage

Ce paramètre spécifie la taille maximale de la mémoire tampon vidéo (en kilo-octets) pour la session.

Par défaut, la limite de mémoire d'affichage est de 65536 kilo-octets.

Pour les connexions nécessitant un nombre de couleurs et une résolution élevés, augmentez la limite. Calculez la mémoire maximale requise à l'aide de cette équation :

Quantité de mémoire en octets = (nombre-de-couleur-en-bits-par-pixel)/8)*(résolution-verticale-en-pixels)*(résolution-horizontale-en-pixels).

Par exemple, avec un nombre de couleurs de 32, une résolution verticale de 600 et une résolution horizontale de 800, la mémoire maximale nécessaire est (32 / 8) * (600) * (800) = 1920000 octets, qui fournit une limite de mémoire d'affichage de 1920 Ko.

Des nombres de couleurs autres que 32 bits sont uniquement disponibles si la stratégie de mode graphique d'ancienne génération est activée.

HDX alloue uniquement la quantité de mémoire d'affichage nécessaire pour chaque session. Donc, si seuls certains utilisateurs ont besoin de plus que la valeur par défaut, il n'existe aucun impact négatif sur la capacité à monter en charge par l'augmentation de la limite de mémoire d'affichage.

Préférence de dégradation du mode d'affichage

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.
Ce paramètre spécifie que le nombre de couleurs ou la résolution se dégrade en premier lorsque la limite de mémoire d'affichage de la session est atteinte.

Par défaut, le nombre de couleurs se dégrade en premier.

Lorsque la limite de mémoire de la session est atteinte, vous pouvez réduire la qualité des images affichées en indiquant si le nombre de couleurs ou la résolution se dégrade en premier. Lorsque le nombre de couleurs se dégrade en premier, les images affichées utilisent moins de couleurs. Lorsque la résolution se dégrade en premier, les images affichées utilisent moins de pixels par pouce.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour avertir les utilisateurs lorsque le nombre de couleurs ou la résolution se dégrade, configurez le paramètre Notifier l'utilisateur lorsque le mode d'affichage se dégrade.

Aperçu de fenêtres dynamiques

Ce paramètre active ou désactive l'affichage de fenêtres transparentes en modes d'aperçu de fenêtres Flip, Flip 3D, Taskbar Preview et Peek.

Option d'aperçu de Windows Aéro	Description
Taskbar Preview	Lorsque l'utilisateur place le pointeur de la souris sur l'icône de barre des tâches d'une fenêtre, une image de cette fenêtre s'affiche au-dessus de la barre des tâches.
Windows Peek	Lorsque l'utilisateur place le pointeur de la souris sur l'image d'un aperçu de la barre des tâches, une image plein écran de cette fenêtre s'affiche.
FLIP	Lorsque l'utilisateur appuie sur ALT+TAB, des petites icônes d'aperçu s'affichent pour chaque fenêtre ouverte.
Flip 3D	Lorsque l'utilisateur appuie sur la touche Windows+TAB, des grandes images des fenêtres ouvertes s'affichent en cascade sur l'écran.

Ce paramètre est activé par défaut.

Cache d'image

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.
Ce paramètre active ou désactive la mise en cache et la récupération de sections d'images dans les sessions. La mise en cache d'images dans des sections et la récupération de ces sections en cas de besoin facilite l'accès, réduit le volume de données transférées sur le réseau et réduit le traitement requis sur la machine utilisateur.

Le paramètre de mise en cache des images est activé par défaut.

Remarque : le paramètre de mise en cache des images contrôle la façon dont les images sont placées dans le cache et récupérées ; il ne contrôle pas si les images sont placées dans le cache. Les images sont placées dans le cache si le paramètre Mode graphique d'ancienne génération est activé.

Mode graphique d'ancienne génération

Ce paramètre désactive l'expérience graphique enrichie, fournissant le retour à l'expérience graphique d'ancienne génération dans le but d'améliorer l'évolutivité via un réseau étendu ou une connexion mobile.

Par défaut, ce paramètre est désactivé et les utilisateurs se voient offrir une expérience graphique enrichie.

Le mode graphique d'ancienne génération est pris en charge avec les VDA Windows 7 et Windows Server 2008 R2. Bien qu'il soit également pris en charge sur Windows 2012 et 2012 R2, cela n'est pas recommandé.

Le mode graphique d'ancienne génération n'est pas pris en charge sur Windows 10, 8.1 ou 8.

Consultez l'article CTX202687 pour de plus amples informations sur l'optimisation des modes graphiques et sur les stratégies dans XenApp et XenDesktop 7.6 FP3 ou version supérieure.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nombre de couleurs maximal autorisé

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.
Ce paramètre spécifie le nombre maximal de couleurs autorisé pour une session.

Par défaut, le nombre maximal de couleurs autorisé est de 32 bits par pixel.

Ce paramètre s'applique uniquement aux pilotes et aux connexions ThinWire. Il ne s'applique pas aux VDA qui disposent d'un pilote non-ThinWire en tant que pilote d'écran principal, tels que les VDA qui utilisent un pilote Windows Display Driver Model (pilote WDDM) en tant que pilote d'écran principal. Pour les VDA avec OS de bureau utilisant un pilote WDDM en tant que pilote d'écran principal, tel que Windows 8, ce paramètre n'a aucun effet. Pour les VDA avec OS Windows Server utilisant un pilote WDDM, tel que Windows Server 2012 R2, ce paramètre peut empêcher les utilisateurs de se connecter au VDA.

Plus le nombre de couleurs est élevé, plus la mémoire requise est importante. Pour dégrader le nombre de couleurs lorsque la limite de mémoire est atteinte, configurez le paramètre Préférence de dégradation du mode d'affichage. Lorsque le nombre de couleurs se dégrade, les images affichées utilisent moins de couleurs.

Notifier l'utilisateur lorsque le mode d'affichage se dégrade

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.
Ce paramètre permet d'afficher une brève explication pour l'utilisateur lorsque le nombre de couleurs ou la résolution se dégrade.

Par défaut, la notification des utilisateurs est désactivée.

Mise en file d'attente et ballotage

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.
Ce paramètre permet d'ignorer toute image en file d'attente qui est remplacée par une autre image.

Par défaut, la mise en file d'attente et le ballotage sont activés.

Cela améliore le temps de réponse lorsque des graphiques sont envoyés à la machine utilisateur. La configuration de ce paramètre peut provoquer une animation hachée due à des trames ignorées.

Utiliser codec vidéo pour la compression

Permet d'utiliser un codec vidéo pour compresser les graphiques lorsque le décodage vidéo est disponible sur le poste client. Si le décodage vidéo n'est pas disponible sur le poste client ou que vous avez spécifié **Ne pas utiliser de codec vidéo**, une combinaison de compression d'image fixe et de mise en cache des bitmaps est utilisée. Lorsque l'option **Utiliser un codec vidéo au choix** est sélectionnée, le système se base sur plusieurs facteurs pour effectuer un choix. Les résultats peuvent varier en fonction des versions car la méthode de sélection est améliorée.

Sélectionnez l'option **Ne pas utiliser de codec vidéo** pour optimiser la charge d'UC du serveur et pour les scénarios avec peu de rendu vidéo sur le serveur ou ne faisant pas appel à beaucoup d'applications exigeant d'importantes ressources graphique.

Sélectionnez l'option **Utiliser un codec vidéo si disponible** pour optimiser l'expérience utilisateur et la bande passante,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

particulièrement dans les cas dans lesquels le rendu vidéo sur le serveur et les graphiques 3D sont fortement sollicités.

Sélectionnez l'option **Utiliser un codec vidéo au choix** pour permettre au système de choisir les paramètres qui conviennent le mieux au scénario actuel.

La valeur par défaut est Utiliser un codec vidéo au choix.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Mise en cache

Jul 07, 2016

La section Mise en cache contient des paramètres de stratégie qui vous permettent de mettre en cache des données d'image sur les machines utilisateur lorsque les connexions clientes sont limitées en bande passante.

Seuil de cache permanent

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.
Ce paramètre met en cache les images bitmap sur le disque dur de la machine utilisateur. Ceci permet une réutilisation d'images de taille importante, fréquemment utilisées provenant de sessions précédentes.

Par défaut, le seuil est de 3000000 kilobits par seconde.

La valeur de seuil représente le point en dessous duquel la fonctionnalité de cache permanent prendra effet. Par exemple, concernant la valeur par défaut, les images bitmaps sont cachées sur le disque dur de la machine utilisateur lorsque la bande passante se trouve en dessous de 3000000 bps.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Framehawk

Jul 07, 2016

La section Framehawk contient des paramètres de stratégie permettant d'activer et de configurer le canal d'affichage Framehawk sur le serveur.

Canal d’affichage Framehawk

Lorsque cette option est activée, le serveur tente d'utiliser le canal d'affichage Framehawk pour les graphiques et la saisie à distance. Ce canal d'affichage utilise UDP pour offrir une meilleure expérience utilisateur sur les réseaux à perte et à latence élevées ; cependant, il peut également utiliser davantage de ressources serveur et de bande passante que les autres modes graphiques.

Par défaut, le canal d'affichage Framehawk est désactivé.

Plage de ports du canal d'affichage Framehawk

Ce paramètre spécifie la plage de numéros de ports UDP (sous la forme *numéro de port le plus bas,numéro de port le plus élevé*) que le VDA peut utiliser pour échanger des données de canal d'affichage Framehawk avec la machine utilisateur. Le VDA tente d'utiliser chaque port, en commençant par le numéro de port le plus bas et en remontant pour chaque tentative. Le port gère le trafic entrant et sortant.

Par défaut, la plage de ports est 3224,3324.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Persistance

Jul 07, 2016

La section Persistance contient les paramètres de stratégie pour gérer les messages de persistance ICA.

Délai d'expiration de persistance ICA

Ce paramètre spécifie le nombre de secondes entre les messages de persistance ICA successifs.

Par défaut, l'intervalle entre les messages de persistance est de 60 secondes.

Spécifiez l'intervalle (entre 1 et 3600 secondes) à utiliser pour envoyer des messages de persistance ICA. Ne configurez pas ce paramètre si votre logiciel de contrôle de réseau est responsable de la fermeture des connexions inactives.

Persistances ICA

Ce paramètre active ou désactive l'envoi périodique de messages de persistance ICA.

Par défaut, aucun message de persistance n'est envoyé.

L'activation de ce paramètre empêche la déconnexion des connexions interrompues. Si le serveur ne détecte pas d'activité, ce paramètre empêche les services Bureau à distance de déconnecter la session. Le serveur envoie des messages de persistance à quelques secondes d'intervalle pour détecter si la session est active. Si la session n'est plus active, le serveur marque la session en tant que déconnectée.

Cependant, la persistance ICA ne fonctionne pas si vous utilisez la fiabilité de session. Ne configurez la persistance ICA que pour les connexions qui n'utilisent pas la fiabilité de session.

Paramètres de stratégie liés : Connexions de fiabilité de session.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Local App Access

Jul 07, 2016

La section Local App Access contient des paramètres de stratégie qui gèrent l'intégration des applications des utilisateurs installées localement avec les applications hébergées dans un environnement de bureau hébergé.

Autoriser Local App Access

Ce paramètre autorise ou empêche l'intégration des applications installées localement avec les applications hébergées dans un environnement de bureau hébergé.

Lorsqu'un utilisateur lance une application installée localement, l'application semble être exécutée dans leur bureau virtuel, même si elle est exécutée localement.

Par défaut, l'accès à l'application locale est interdit.

Liste noire de redirection d'adresse URL

Ce paramètre spécifie les sites Web qui sont redirigés vers et lancés dans le navigateur Web local. Cela peut inclure les sites Web nécessitant des paramètres régionaux d'informations, tels que msn.com ou newsgoogle.com, ou des sites Web contenant du contenu multimédia enrichi qui sont mieux restitués sur la machine utilisateur.

Par défaut, aucun site n'est spécifié.

Liste blanche de redirection d'adresse URL

Ce paramètre spécifie les sites Web qui sont restitués dans l'environnement dans lequel elles sont lancées.

Par défaut, aucun site n'est spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Expérience mobile

Jul 07, 2016

La section Experience Mobile contient des paramètres de stratégie destinés à la gestion de Citrix Mobility Pack.

Affichage de clavier automatique

Ce paramètre active ou désactive l'affichage automatique du clavier sur les écrans des appareils mobiles.

Par défaut, l'affichage automatique du clavier est désactivé.

Démarrer le bureau tactile

Ce paramètre est désactivé et n'est pas disponible pour les machines Windows 10.

Ce paramètre détermine le comportement général de l'interface du Citrix Receiver en autorisant ou en interdisant une interface tactile optimisée pour les tablettes.

Par défaut, une interface tactile est utilisée.

Pour n'utiliser que l'interface Windows, définissez cette stratégie sur Interdit.

Contrôler la zone combinée

Ce paramètre détermine les types de zones de liste déroulante que vous pouvez afficher dans les sessions sur les appareils mobiles. Pour afficher la commande de zone combinée d'appareil native, définissez ce paramètre de stratégie sur Autorisé. Lorsque ce paramètre est autorisé, un utilisateur peut modifier un paramètre de session Citrix Receiver pour iOS afin d'utiliser la zone combinée Windows.

Par défaut, la fonctionnalité Contrôler la zone combinée est interdite.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie multimédia

Jul 07, 2016

La section Multimédia contient les paramètres de stratégie permettant de gérer les données audio et vidéo livrées en streaming dans les sessions utilisateur.

Limiter la qualité de la vidéo

Ce paramètre spécifie le niveau de qualité vidéo maximum autorisé pour une connexion HDX. Une fois configurée, la qualité vidéo maximale est limitée à la valeur spécifiée, en assurant que la qualité de service (QoS) multimédia est conservée dans un environnement.

Ce paramètre n'est pas configuré par défaut.

Pour limiter le niveau de qualité vidéo maximum autorisé, choisissez l'une des options suivantes :

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

Remarque : la lecture simultanée de plusieurs vidéos sur le même serveur utilise une quantité importante de ressources et peut avoir un impact sur la capacité à monter en charge du serveur.

Conférences multimédia

Ce paramètre autorise ou empêche la prise en charge des applications de visioconférence.

Par défaut, la prise en charge de la visioconférence est activée.

Lors de l'ajout de ce paramètre à une stratégie, vérifiez que le paramètre Redirection Windows Media est présent et défini sur Autorisé.

Lorsque vous utilisez les fonctions de conférence multimédia, assurez-vous que les conditions suivantes sont remplies :

- Les pilotes fournis par le constructeur pour la webcam utilisée pour les conférences multimédia sont installés.
- La webcam doit être connectée à la machine cliente avant d'initier une session de visioconférence. Le serveur n'utilise qu'une seule webcam installée à la fois. Si plusieurs webcams sont installées sur la machine cliente, le serveur tente d'utiliser chacune d'elles successivement jusqu'à ce qu'il réussisse à créer une session de visioconférence.

Optimisation pour la redirection multimédia Windows Media sur un réseau étendu

Ce paramètre permet le transcodage multimédia en temps réel, ce qui permet la livraison en streaming audio et vidéo vers les appareils mobiles, et l'amélioration de l'expérience utilisateur en améliorant la manière dont le contenu Windows Media est mis à disposition via un réseau étendu.

Par défaut, la mise à disposition du contenu Windows Media sur le réseau étendu est optimisée.

Lors de l'ajout de ce paramètre à une stratégie, vérifiez que le paramètre Redirection Windows Media est présent et défini sur Autorisé.

Lorsque ce paramètre est activé, le transcodage multimédia en temps réel est déployé automatiquement lorsque nécessaire pour activer la livraison en streaming de contenu multimédia, offrant une expérience utilisateur transparente, même dans

© 1999-2017 Citrix Systems, Inc. All rights reserved.

des conditions réseau extrêmes.

Utiliser l'unité de traitement graphique (GPU) pour optimiser la redirection multimédia Windows Media sur un réseau étendu

Ce paramètre active le transcodage multimédia en temps réel qui doit être effectué dans l'unité de traitement graphique (GPU) sur le Virtual Delivery Agent (VDA) pour améliorer l'extensibilité du serveur. Le transcodage sur l'unité de traitement graphique (GPU) n'est disponible que si le VDA possède une unité de traitement graphique pour l'accélération matérielle. Sinon, le transcodage retourne à l'UC.

Remarque : le transcodage GPU est pris en charge uniquement sur les GPU NVIDIA.
Par défaut, l'utilisation du GPU sur le VDA pour optimiser la mise à disposition de contenu Windows Media sur le réseau étendu est interdite.

Lorsque vous ajoutez ce paramètre à une stratégie, vérifiez que les paramètres Redirection Windows Media et Optimisation pour la redirection multimédia Windows Media sur un réseau étendu sont présent et définis sur Autorisé.

Prévention du retour à la vidéo

Les administrateurs peuvent utiliser le paramètre de prévention du retour à la vidéo pour spécifier la méthode qui sera utilisée pour livrer en streaming les contenus aux utilisateurs.

Ce paramètre n'est pas configuré par défaut. Cela autorise les retours de la « Récupération côté client » vers « RAVE » vers la « Restitution côté serveur ».

Pour contrôler ce paramètre, choisissez l'une des options suivantes :

- **Récupéré du serveur, restitué sur le serveur** Autorise les retours de la Récupération côté client vers RAVE vers la Restitution côté serveur.
- **Récupéré du serveur, restitué sur le client** Autorise le retour de la Récupération côté client vers RAVE, mais bloque le retour RAVE vers la Restitution côté serveur.
- **Récupéré du client, restitué sur le client** Bloque les retours de la Récupération côté client vers RAVE vers la Restitution côté serveur.

Lorsque le contenu ne fonctionne pas, le message d'erreur « Votre entreprise a bloqué la vidéo en raison d'un manque de ressources. » s'affiche dans la fenêtre du lecteur.

Récupération de contenu côté client Windows Media

Ce paramètre permet aux machines utilisateur de livrer en streaming des fichiers multimédia directement à partir du fournisseur source sur Internet ou Intranet, plutôt qu'au travers du serveur hôte.

Par défaut, le streaming des fichiers multimédias vers la machine utilisateur directement à partir du fournisseur source est autorisé.

L'activation de ce paramètre améliore l'utilisation du réseau et l'extensibilité du serveur en déplaçant tout traitement sur le média à partir du serveur hôte vers la machine utilisateur. Elle supprime également le besoin d'installer une infrastructure multimédia avancée tels que Microsoft DirectShow ou Media Foundation sur la machine utilisateur ; la machine utilisateur nécessite la possibilité de lire un fichier à partir d'une adresse URL

Lors de l'ajout de ce paramètre à une stratégie, vérifiez que le paramètre Redirection Windows Media est présent et défini sur Autorisé. Si ce paramètre est désactivé, le streaming des fichiers multimédias vers la machine utilisateur directement à

© 1999-2017 Citrix Systems, Inc. All rights reserved.

partir du fournisseur source est également désactivé.

Redirection Windows Media

Ce paramètre permet de contrôler et d'optimiser le mode de livraison en streaming des données audio et vidéo par les serveurs vers les utilisateurs.

Par défaut, la mise à disposition d'audio et de vidéo en streaming aux utilisateurs est autorisée.

L'activation de ce paramètre améliore la qualité de l'audio et de la vidéo restitués depuis le serveur à un niveau comparable à celui obtenu avec de l'audio et de la vidéo exécutés localement sur une machine utilisateur. le serveur livre en streaming du contenu multimédia vers le client au format compressé d'origine et permet à la machine utilisateur de décompresser et de restituer le contenu multimédia.

La redirection Windows Media optimise les fichiers multimédia encodés à l'aide de codecs conformes aux normes DirectShow, DirectX Media Objects (DMO) et Media Foundation standard de Microsoft. Pour lire un fichier multimédia donné, la machine utilisateur doit disposer d'un codec compatible avec le format d'encodage du fichier multimédia.

par défaut, l'audio est désactivé sur Citrix Receiver. Pour permettre aux utilisateurs d'exécuter des applications multimédia dans les sessions ICA, activez l'audio ou accordez aux utilisateurs l'autorisation de l'activer dans leur interface Citrix Receiver.

Sélectionnez uniquement Interdit si la qualité obtenue avec la redirection Windows Media semble inférieure à celle obtenue à l'aide de la compression ICA de base et des réglages audio standard. Cette situation est rare mais possible dans le cas de conditions où la bande passante est faible, par exemple, si le contenu multimédia dispose d'une très faible fréquence de trames clés.

Taille de tampon de redirection Windows Media

Ce paramètre spécifie une taille de tampon de 1 à 10 secondes pour l'accélération multimédia.

Par défaut, la taille du tampon est de 5 secondes.

Utilisation de la taille de tampon de redirection Windows Media

Ce paramètre active ou désactive l'utilisation de la taille de tampon définie par le paramètre Taille de tampon de redirection Windows Media.

Par défaut, la taille du tampon spécifiée n'est pas utilisée.

Si ce paramètre est désactivé ou si le paramètre Taille de tampon de redirection Windows Media n'est pas configuré, le serveur utilise la valeur de taille de tampon par défaut (5 secondes).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Connexions Multi-Stream

Jul 07, 2016

La section Connexions Multi-Stream contient des paramètres de stratégie destinés à gérer la hiérarchisation de la qualité de service (QoS) pour les multiples connexions ICA dans une session.

Audio sur UDP

Ce paramètre autorise ou empêche l'audio via UDP sur le serveur.

Par défaut, l'audio sur UDP est autorisé sur le serveur.

Lorsqu'il est activé, ce paramètre s'ouvre un port UDP sur le serveur pour prendre en charge toutes les connexions configurées pour utiliser le transport en temps réel Audio sur UDP.

Plage de port UDP audio

Ce paramètre spécifie la plage de numéros de ports (sous la forme numéro de port le plus bas, numéro de port le plus élevé) utilisés par Virtual Delivery Agent (VDA) pour échanger des données de paquet audio avec la machine utilisateur. Le VDA tente d'utiliser chaque paire de ports UDP pour échanger des données avec la machine utilisateur, en commençant par le plus bas et en incrémentant de deux pour chaque tentative ultérieure. Chaque port gère le trafic entrant et sortant.

Par défaut, cette option est définie sur 16500,16509.

Stratégie Multi-Port

Ce paramètre spécifie les ports TCP à utiliser pour le trafic ICA et établit la priorité réseau pour chaque port.

Par défaut, le port principal (2598) a une priorité élevée.

Lorsque vous configurez des ports, vous pouvez leur attribuer les priorités suivantes :

- Très élevée : réservée aux activités en temps réel, telles que les conférences Web (avec webcam).
- Élevée : réservée aux éléments interactifs, tels que l'écran, le clavier et la souris.
- Moyenne : réservée aux processus de masse, tels que le mappage des lecteurs clients.
- Faible : réservée aux activités d'arrière-plan, telles que l'impression.

Chaque port doit disposer d'une priorité unique. À titre d'exemple, vous ne pouvez pas attribuer une priorité Très élevé au port 1 CGP et au port 3 CGP.

Pour n'attribuer aucune priorité à un port, définissez le numéro de port sur 0. Vous ne pouvez ni supprimer le port principal, ni modifier son niveau de priorité.

Redémarrez le serveur après avoir configuré ce paramètre. Ce paramètre ne s'applique que lorsque le paramètre de stratégie Paramètre d'ordinateur Multi-Stream est activé.

Paramètre d'ordinateur Multi-Stream

Ce paramètre active ou désactive la fonctionnalité Multi-Stream sur le serveur.

Par défaut, Multi-Stream est désactivée.

Si vous utilisez Citrix Cloudbridge avec prise en charge Multi-Stream dans votre environnement, vous n'avez pas besoin de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

configurer ce paramètre. Configurez ce paramètre de stratégie lorsque vous utilisez des routeurs tiers ou des Branch Repeater d'ancienne génération pour réaliser la qualité de service désirée.

Une fois ce paramètre configuré, redémarrez le serveur pour que les modifications prennent effet.
Important : l'utilisation de ce paramètre de stratégie en conjonction avec les paramètres de stratégie de limite de bande passante Limite de bande passante de session générale peut produire des résultats inattendus. Lors de l'inclusion de ce paramètre dans une stratégie, assurez-vous que les paramètres de limite de bande passante ne sont pas inclus.

Paramètre utilisateur Multi-Stream

Ce paramètre active ou désactive la fonctionnalité Multi-Stream sur la machine utilisateur.

Par défaut, Multi-Stream est désactivé pour tous les utilisateurs.

Ce paramètre ne s'applique que sur les hôtes sur lesquels le paramètre de stratégie Paramètre d'ordinateur Multi-Stream est activé.
Important : l'utilisation de ce paramètre de stratégie en conjonction avec les paramètres de stratégie de limite de bande passante Limite de bande passante de session générale peut produire des résultats inattendus. Lors de l'inclusion de ce paramètre dans une stratégie, assurez-vous que les paramètres de limite de bande passante ne sont pas inclus.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie de redirection de port

Jul 07, 2016

La section Redirection de port contient les paramètres de stratégie pour le mappage des ports LPT et COM clients.

Pour les versions du Virtual Delivery Agent **antérieures à la version 7.0**, utilisez les paramètres de stratégie suivants pour configurer la redirection de port. Pour les versions VDA de **7.0 à 7.8**, configurez ces paramètres à l'aide du registre ; consultez la section Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre. Pour la version **7.9** du VDA, utilisez les paramètres de stratégie suivants.

Connecter automatiquement les ports COM du client

Ce paramètre active ou désactive la connexion automatique des ports COM sur les machines utilisateur lorsque les utilisateurs ouvrent une session sur un site.

Par défaut, les ports COM du client ne sont pas automatiquement connectés.

Connecter automatiquement les ports LPT du client

Ce paramètre active ou désactive la connexion automatique des ports LPT sur les machines utilisateur lorsque les utilisateurs ouvrent une session sur un site.

Par défaut, les ports LPT du client ne sont pas automatiquement connectés.

Redirection de port COM client

Ce paramètre autorise ou empêche l'accès aux ports COM sur la machine utilisateur.

Par défaut, la redirection des ports COM est interdite.

Les paramètres de stratégie suivants sont associés :

- Limite de bande passante pour la redirection du port COM
- Pourcentage de limite de bande passante de redirection du port COM

Redirection de port LPT client

Ce paramètre autorise ou empêche l'accès aux ports LPT sur la machine utilisateur.

Par défaut, la redirection des ports LPT est interdite.

Les ports LPT sont uniquement utilisés par les applications d'ancienne génération qui leur envoient les tâches d'impression plutôt que de les envoyer aux objets d'impression sur la machine utilisateur. La plupart des applications peuvent désormais envoyer des tâches d'impression aux objets d'imprimante. Ce paramètre de stratégie est uniquement nécessaire pour les serveurs hébergeant des applications d'ancienne génération qui impriment sur des ports LPT.

Veuillez noter que bien que la redirection des ports COM clients soit bi-directionnelle, la redirection des ports LPT est en sortie uniquement et limitée à \\client\LPT1 et \\client\LPT2 dans une session ICA.

Les paramètres de stratégie suivants sont associés :

- Limite de bande passante pour la redirection du port LPT
- Pourcentage de limite de bande passante de redirection du port LPT

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Impression

Jul 07, 2016

La section Impression contient les paramètres de stratégie qui permettent de gérer l'impression cliente.

Redirection d'imprimante cliente

Ce paramètre contrôle si les imprimantes clientes sont mappées sur un serveur lorsqu'un utilisateur ouvre une session.

Par défaut, le mappage des imprimantes clientes est autorisé. Si ce paramètre est désactivé, l'imprimante PDF pour la session n'est pas créée automatiquement.

Paramètres de stratégie liés : créer automatiquement des imprimantes clientes

Imprimante par défaut

Ce paramètre spécifie la façon dont l'imprimante par défaut est définie sur la machine utilisateur dans une session.

Par défaut, l'imprimante actuelle de l'utilisateur est utilisée comme imprimante par défaut pour la session.

Pour utiliser le paramètre de profil utilisateur des services Bureau à distance ou Windows courant pour l'imprimante par défaut, sélectionnez Ne pas ajuster l'imprimante par défaut de l'utilisateur. Si vous choisissez cette option, l'imprimante par défaut n'est pas enregistrée dans le profil et elle ne change pas selon les propriétés des autres sessions ou du client. L'imprimante par défaut d'une session sera la première imprimante créée automatiquement dans la session, à savoir :

- La première imprimante ajoutée localement au serveur Windows dans Panneau de configuration > Périphériques et imprimantes
- La première imprimante créée automatiquement, si aucune imprimante n'a été ajoutée localement sur le serveur.

Vous pouvez utiliser cette option pour présenter l'imprimante la plus proche aux utilisateurs par le biais des paramètres de profil (fonctionnalité connue sous le nom d'impression de proximité).

Attributions d'imprimantes

Ce paramètre permet d'offrir une alternative aux paramètres Imprimante par défaut et Imprimantes de session. Utilisez les paramètres Imprimante par défaut et Imprimantes de session pour configurer les comportements d'un site, d'un groupe important ou d'une unité d'organisation. Utilisez le paramètre Attributions d'imprimantes pour attribuer un groupe important d'imprimantes à plusieurs utilisateurs.

Ce paramètre spécifie la façon dont l'imprimante par défaut des machines utilisateur répertoriées est établie dans une session.

Par défaut, l'imprimante actuelle de l'utilisateur est utilisée comme imprimante par défaut pour la session.

Ce paramètre spécifie de créer automatiquement les imprimantes réseau dans une session pour chaque machine utilisateur. Par défaut, aucune imprimante n'est spécifiée.

- Lors de la définition de la valeur d'imprimante par défaut :
  Pour utiliser l'imprimante par défaut courante pour la machine utilisateur, sélectionnez Ne pas ajuster.

  Pour utiliser le paramètre de profil utilisateur des services Bureau à distance ou Windows courant pour l'imprimante par défaut, sélectionnez Ne pas régler. Si vous choisissez cette option, l'imprimante par défaut n'est pas enregistrée dans le

© 1999-2017 Citrix Systems, Inc. All rights reserved.

profil et elle ne change pas selon les propriétés des autres sessions ou du client. L'imprimante par défaut d'une session sera la première imprimante créée automatiquement dans la session, à savoir :

- La première imprimante ajoutée localement au serveur Windows dans Panneau de configuration > Périphériques et imprimantes
- La première imprimante créée automatiquement, si aucune imprimante n'a été ajoutée localement sur le serveur.

- Lors de la définition de la valeur des imprimantes de session : pour ajouter des imprimantes, entrez le chemin UNC de l'imprimante que vous souhaitez créer automatiquement. Après avoir ajouté l'imprimante, vous pouvez appliquer les paramètres personnalisés pour la session courante lors de chaque ouverture de session.

Préférence de journalisation des événements de création automatique des imprimantes

Ce paramètre spécifie les événements journalisés pendant le processus de création automatique de l'imprimante. Vous pouvez choisir de ne journaliser ni les erreurs ni les avertissements, uniquement les erreurs, ou les erreurs et les avertissements.

Par défaut, les erreurs et les avertissements sont journalisés.

Un exemple d'avertissement est un événement au cours duquel le pilote natif d'une imprimante n'a pas pu être installé, c'est le pilote d'impression universelle qui a été installé à la place. Pour utiliser le pilote d'impression universelle dans ce scénario, configurez le paramètre Utilisation du pilote d'impression universelle sur l'option Utiliser l'impression universelle uniquement ou Utiliser l'impression universelle uniquement si le pilote requis n'est pas disponible.

Imprimantes de session

Ce paramètre spécifie de créer automatiquement les imprimantes réseau dans une session.

Par défaut, aucune imprimante n'est spécifiée.

Pour ajouter des imprimantes, entrez le chemin UNC de l'imprimante que vous souhaitez créer automatiquement. Après avoir ajouté l'imprimante, vous pouvez appliquer les paramètres personnalisés pour la session courante lors de chaque ouverture de session.

Attendre la création d'imprimantes (bureau de serveur)

Ce paramètre autorise ou empêche l'application d'un délai lors de la connexion à une session de sorte à autoriser la création automatique des imprimantes de bureau de serveur.

Par défaut, aucun délai de connexion n'intervient.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie d'imprimantes clientes

Jul 07, 2016

La section Imprimantes clientes contient les paramètres de stratégie des imprimantes clientes, notamment les paramètres relatifs à la création automatique d'imprimantes clientes, à la rétention des propriétés d'imprimante et à la connexion aux serveurs d'impression.

Créer automatiquement les imprimantes clientes

Ce paramètre spécifie les imprimantes clientes créées automatiquement. Il remplace les paramètres par défaut de création automatique d'imprimantes clientes.

Par défaut, toutes les imprimantes clientes sont créées automatiquement.

Ce paramètre n'entre en vigueur que si le paramètre Redirection d'imprimante cliente est présent et a la valeur Autorisé.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Créer automatiquement toutes les imprimantes clientes crée automatiquement toutes les imprimantes clientes sur une machine utilisateur.
- Ne créer automatiquement que l'imprimante par défaut du client ne crée automatiquement que l'imprimante sélectionnée comme imprimante par défaut sur la machine utilisateur.
- Ne créer automatiquement que les imprimantes clientes locales (non réseau) ne crée automatiquement que les imprimantes directement connectées à la machine utilisateur via un port LPT, COM, USB, TCP/IP ou un autre port local.
- Ne pas créer les imprimantes clientes automatiquement désactive la création automatique pour toutes les imprimantes clientes lorsque les utilisateurs ouvrent une session. De ce fait, les paramètres des services Bureau à distance (RDS) liés à la création automatique d'imprimantes clientes remplacent ce paramètre dans les stratégies de priorité inférieure.

Créer automatiquement l'imprimante universelle générique

Remarque : les corrections permettant de résoudre les problèmes relatifs à ce paramètre de stratégie sont disponibles dans les articles CTX141565 et CTX141566 du centre de connaissances.
Ce paramètre active ou désactive la création automatique de l'objet d'impression générique de l'imprimante universelle Citrix pour les sessions lorsqu'une machine utilisateur compatible avec l'impression universelle est en cours d'utilisation.

Par défaut, l'objet Imprimante universelle générique n'est pas créé automatiquement.

Les paramètres de stratégie suivants sont associés :

- Utilisation du pilote d'impression universelle
- Préférence de pilote universel

Noms des imprimantes clientes

Ce paramètre permet de sélectionner la convention d'appellation pour les imprimantes clientes créées automatiquement.

Par défaut, les noms d'imprimante standard sont utilisés.

Sélectionnez Noms d'imprimantes standards pour utiliser des noms d'imprimante tels que « HPLaserJet 4 sur nomClient dans la session 3 ».

Sélectionnez Noms d'imprimantes d'ancienne génération pour utiliser les noms d'imprimantes clientes d'ancienne génération et préserver la rétrocompatibilité pour les utilisateurs et les groupes utilisant MetaFrame Presentation Server 3.0 ou une

© 1999-2017 Citrix Systems, Inc. All rights reserved.

version antérieure. Un exemple de nom d'imprimante d'ancienne génération est « Client/nomclient#/HPLaserJet 4 ». Cette option est moins sécurisée.
Remarque : cette option est fournie uniquement à des fins de compatibilité à effet rétroactif avec les anciennes versions de XenApp et XenDesktop.

Connexions directes aux serveurs d'impression

Ce paramètre permet d'activer ou de désactiver les connexions directes à partir du bureau virtuel ou du serveur hébergeant les applications vers un serveur d'impression pour les imprimantes clientes hébergées sur un partage réseau accessible.

Par défaut, les connexions directes sont activées.

Activez les connexions directes si le serveur d'impression réseau n'est pas sur un réseau étendu à partir du bureau virtuel ou du serveur hébergeant les applications. Les communications directes donnent lieu à des impressions plus rapides lorsque le serveur d'impression réseau et le bureau virtuel ou le serveur hébergeant les applications sont sur le même réseau local.

Vous pouvez désactiver les connexions directes si le réseau se trouve à l'autre extrémité d'un réseau étendu, s'il est soumis à une latence élevée ou s'il dispose d'une bande passante réduite. Les tâches d'impression sont acheminées via la machine utilisateur, puis redirigées vers le serveur d'impression réseau. Les données envoyées à la machine utilisateur sont compressées. Les transmissions de données sur le réseau étendu nécessitent donc moins de bande passante.

Si deux imprimantes réseau ont le même nom, l'imprimante située sur le même réseau que la machine utilisateur est utilisée.

Mappage et compatibilité du pilote d'imprimante

Ce paramètre spécifie les règles de remplacement de pilotes pour les imprimantes créées automatiquement.

Par défaut, aucune règle n'est spécifiée.

Lorsque vous définissez ces règles de remplacement, vous pouvez autoriser ou empêcher la création d'imprimantes avec le pilote spécifié. En outre, vous pouvez autoriser les imprimantes créées à utiliser uniquement les pilotes d'imprimantes universels. Le remplacement de pilote annule (ou mappe) le nom de pilote d'imprimante fourni par le client, en le remplaçant par un pilote équivalent sur le serveur. Cela permet à des applications exécutées sur le serveur d'accéder à des imprimantes clientes qui ont les mêmes pilotes que le serveur mais sous des noms de pilote différents.

Vous pouvez ajouter un mappage de pilote, modifier un mappage existant, remplacer les paramètres personnalisés d'un mappage, supprimer un mappage ou modifier l'ordre des entrées de pilote dans la liste. Lors de l'ajout d'un mappage, entrez le nom de pilote de l'imprimante cliente, puis sélectionnez le pilote serveur que vous souhaitez remplacer.

Rétention des propriétés d'imprimante

Ce paramètre indique si les propriétés d'imprimante sont ou non stockées et précise l'emplacement de stockage.

Par défaut, le système détermine si les propriétés d'imprimante doivent être stockées sur la machine utilisateur, le cas échéant, ou dans le profil utilisateur.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Enregistrées uniquement sur la machine cliente est une option destinée aux machines utilisateur qui possèdent un profil obligatoire ou itinérant qui n'est pas enregistré. Ne choisissez cette option que si tous les serveurs de votre batterie exécutent XenApp 5 et version ultérieure et si vos utilisateurs disposent de Citrix Online Plugin versions 9 à 12.x ou Citrix Receiver 3.x.
- Conservées uniquement dans le profil d'utilisateur est une option destinée aux machines utilisateur soumises à des contraintes de bande passante (cette option permet de réduire le trafic réseau) et de temps d'ouverture de session ou si

© 1999-2017 Citrix Systems, Inc. All rights reserved.

des utilisateurs utilisent des plug-ins d'ancienne génération. Cette option stocke les propriétés d'imprimante dans le profil utilisateur sur le serveur et empêche tout échange des propriétés avec la machine cliente. Cette option est disponible avec MetaFrame Presentation Server 3.0 (ou une version antérieure) et avec le Client MetaFrame Presentation Server 8.x (ou une version antérieure). Notez que cela ne s'applique qu'en cas d'utilisation d'un profil itinérant des services Bureau à distance (RDS).

- Le paramètre Contenu dans le profil uniquement si non enregistré sur le client permet au système de déterminer l'emplacement de stockage des propriétés d'imprimante. Les propriétés d'imprimante sont stockées sur la machine cliente, le cas échéant, ou dans le profil utilisateur. Bien que cette option soit la plus souple, elle peut aussi entraîner un ralentissement à l'ouverture de session et utiliser davantage de bande passante pour les vérifications du système.
- Ne pas conserver les propriétés des imprimantes empêche le stockage des propriétés de l'imprimante.

Imprimantes clientes conservées et restaurées

Ce paramètre permet d'activer ou de désactiver la rétention et la recréation d'imprimantes sur la machine utilisateur. Par défaut, les imprimantes clientes sont conservées automatiquement et restaurées automatiquement.

Les imprimantes conservées sont des imprimantes créées par l'utilisateur qui sont recréées, ou rappelées, au début de la session suivante. Lorsque XenApp recrée une imprimante conservée, il tient compte de tous les paramètres de stratégie, à l'exception du paramètre Créer automatiquement des imprimantes clientes.

Les imprimantes restaurées sont des imprimantes entièrement personnalisées par un administrateur, dans un état enregistré qui est connecté en permanence au port d'un client.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Pilotes

Jul 07, 2016

La section Pilotes contient des paramètres de stratégie relatifs aux pilotes d'imprimante.

Installation automatique de pilotes d'imprimante fournis avec Windows

Ce paramètre active ou désactive l'installation automatique des pilotes d'imprimante fournis avec le jeu de pilotes Windows ou provenant de packs de pilotes sur l'hôte à l'aide de pnputil.exe /a.

Par défaut, ces pilotes sont installés selon vos besoins.

Préférence de pilote universel

Ce paramètre spécifie l'ordre dans lequel les pilotes d'imprimante universels sont utilisés, en commençant par la première entrée de la liste.

Par défaut, l'ordre de préférence est le suivant :

- EMF
- XPS
- PCL5c
- PCL4
- PS

Vous pouvez ajouter, modifier ou supprimer des pilotes et changer leur ordre dans la liste.

Utilisation du pilote d'impression universelle

Ce paramètre spécifie à quel moment utiliser l'impression universelle.

Par défaut, l'impression universelle n'est utilisée que si le pilote demandé n'est pas disponible.

L'impression universelle utilise des pilotes d'imprimante génériques au lieu de pilotes spécifiques au modèle standard, simplifiant potentiellement la charge de gestion des pilotes sur les ordinateurs hôtes. La disponibilité des pilotes d'impression universels dépend des capacités de la machine utilisateur, de l'hôte et du logiciel du serveur d'impression. Dans certaines configurations, il se peut que l'impression universelle ne soit pas disponible.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Utiliser uniquement les pilotes spécifiques au modèle de l'imprimante indique que l'imprimante cliente utilise uniquement les pilotes spécifiques au modèle standard qui sont créés automatiquement lors de l'ouverture de session. Si le pilote requis n'est pas disponible, l'imprimante cliente ne peut pas être créée automatiquement.
- Utiliser l'impression universelle uniquement spécifie qu'aucun pilote spécifique au modèle standard n'est utilisé. Seuls les pilotes d'impression universelle sont utilisés pour créer des imprimantes.
- Utiliser l'impression universelle uniquement si le pilote requis n'est pas disponible utilise les pilotes spécifiques au modèle standard pour la création des imprimantes s'ils sont disponibles. Si le pilote n'est pas disponible sur le serveur, l'imprimante cliente est automatiquement créée à l'aide du pilote d'imprimante universelle approprié.
- Utiliser les pilotes spécifiques au modèle d'imprimante uniquement si impression universelle non dispo utilise le pilote d'impression universelle s'il est disponible. Si le pilote n'est pas disponible sur le serveur, l'imprimante cliente est automatiquement créée à l'aide du pilote spécifique au modèle standard approprié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Serveur d'impression universelle

Jul 07, 2016

La section Serveur d'impression universelle contient les paramètres de stratégie permettant de gérer le Serveur d'impression universelle.

Activer le serveur d'impression universelle

Ce paramètre active ou désactive la fonctionnalité Serveur d'impression universelle sur le bureau virtuel ou le serveur hébergeant les applications. Appliquez ce paramètre de stratégie aux unités d'organisation contenant le bureau virtuel ou le serveur hébergeant les applications.

Par défaut, le Serveur d'impression universelle est désactivé.

Lorsque vous ajoutez ce paramètre à une stratégie, sélectionnez l'une des options suivantes :

- **Activé avec retour à l'impression distante native de Windows**. Le service des connexions d'imprimante réseau est effectué par le serveur d'impression universelle, si possible. Si le serveur d'impression universelle n'est pas disponible, le fournisseur d'impression Windows est utilisé. Le fournisseur d'impression Windows continue de gérer toutes les imprimantes créées précédemment avec le fournisseur d'impression Windows.
- **Activé avec aucun retour à l'impression distante native de Windows**. Le service des connexions d'imprimante réseau est effectué par le serveur d'impression universelle, exclusivement. Si le serveur d'impression universelle n'est pas disponible, la connexion de l'imprimante réseau échoue. Ce paramètre désactive de manière effective l'impression réseau au travers du fournisseur d'impression Windows. Les imprimantes créées précédemment avec le fournisseur d'impression Windows ne sont pas créées tant qu'une stratégie contenant ce paramètre est active.
- **Désactivé**. La fonctionnalité Serveur d'impression universelle est désactivée. Aucune tentative de connexion avec le Serveur d'impression universelle n'est effectuée lors de la connexion à une imprimante réseau avec un nom UNC. Les connexions aux imprimantes distantes continuent d'utiliser l'outil d'impression à distance Windows natif.

Port (CGP) du flux de données d'impression du serveur d'impression universelle

Ce paramètre spécifie le numéro de port TCP utilisé par l'écouteur CGP (Common Gateway Protocol) du flux de données d'impression Serveur d'impression universelle. Appliquez ce paramètre de stratégie uniquement aux unités d'organisation contenant le serveur d'impression.

Le numéro port est défini par défaut sur 7229.

Les numéros de port valides doivent se trouver dans une plage de 1 à 65535.

Limite de bande passante d'entrée du flux d'impression du serveur d'impression universelle (kpbs)

Ce paramètre spécifie la limite supérieure (en kilobits par seconde) pour le taux de transfert des données d'impression mises à disposition depuis chaque tâche d'impression vers le Serveur d'impression universelle à l'aide de CGP. Appliquez ce paramètre de stratégie aux unités d'organisation contenant le bureau virtuel ou le serveur hébergeant les applications.

Par défaut, la valeur est 0, qui ne spécifie aucune limite supérieure.

Port (HTTP/SOAP) du service Web du serveur d'impression universelle

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ce paramètre spécifie le numéro de port TCP utilisé par l'écouteur du service Web Serveur d'impression universelle pour les requêtes (HTTP/SOAP). Le serveur d'impression universelle est un composant facultatif qui permet l'utilisation des pilotes d'impression universelle Citrix dans les scénarios d'impression réseau. Lorsque le serveur d'impression universelle est utilisé, les commandes d'impression sont envoyées depuis les hôtes XenApp et XenDesktop vers le serveur d'impression universelle via SOAP sur HTTP. Ce paramètre modifie le port TCP par défaut sur lequel le serveur d'impression universelle écoute les requêtes HTTP/SOAP entrantes.

Vous devez configurer le port HTTP du serveur d'impression et de l'hôte de façon identique. Si les ports ne sont pas configurés à l'identique, le logiciel de l'hôte ne se connectera pas au serveur d'impression universelle. Ce paramètre modifie le VDA sur XenApp et XenDesktop. Par ailleurs, vous devez modifier le port par défaut sur le serveur d'impression universelle.

Le numéro port est défini par défaut sur 8080.

Les numéros de port valides doivent se trouver dans une plage de 0 à 65535.

Serveurs d'impression universelle d'équilibrage de la charge

Ce paramètre dresse la liste des serveurs d'impression universelle à utiliser pour répartir la charge des connexions aux imprimantes établies lors du lancement de la session, après l'évaluation d'autres paramètres de stratégie d'impression Citrix. Pour optimiser la durée de création des imprimantes, Citrix recommande que les mêmes imprimantes partagées soient installées sur tous les serveurs d'impression. Il n'existe aucune limite au nombre de serveurs d'impression qui peuvent être ajoutés pour l'équilibrage de charge.

Ce paramètre s'applique également à la détection de basculement de serveur d'impression et à la récupération de connexion d'imprimante. Les serveurs d'impression contrôlent la disponibilité périodiquement. Si un serveur défaillant est détecté, ce serveur est supprimé du schéma d'équilibrage de charge, et les connexions d'imprimante sur ce serveur sont redistribuées sur d'autres serveurs d'impression disponibles. Après reprise du serveur d'impression défaillant, il reprend sa place dans le schéma d'équilibrage de charge.

Cliquez sur **Valider les serveurs** pour vérifier que chaque serveur est un serveur d'impression et que tous les serveurs possèdent un ensemble identique d'imprimantes partagées. Cette opération peut prendre un certain temps.

Seuil au-delà duquel les serveurs d'impression universelle sont hors service

Ce paramètre indique la durée pendant laquelle l'équilibrage de charge attend le rétablissement de la connexion à un serveur d'impression universelle avant de considérer que le serveur est hors connexion et de répartir sa charge sur d'autres serveurs d'impression disponibles.

Par défaut, la valeur de seuil est de 180 (secondes).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Impression universelle

Jul 07, 2016

La section Impression universelle contient des paramètres de stratégie permettant de gérer l'impression universelle.

mode de traitement EMF de l'impression universelle ;

Ce paramètre contrôle la méthode de traitement du fichier de spoule EMF sur la machine utilisateur Windows.

Par défaut, les enregistrements EMF sont spoulés directement sur l'imprimante.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Traiter à nouveau les EMF pour l'imprimante oblige le fichier de spoule EMF à être traité à nouveau et envoyé au travers du sous-système GDI sur la machine utilisateur. Vous pouvez utiliser ce paramètre pour les pilotes qui requièrent un nouveau traitement EMF mais qui peuvent ne pas être sélectionnés automatiquement dans une session.
- Spouler directement vers l'imprimante, lorsque utilisé avec le pilote d'impression universelle Citrix, assure que les données EMF sont spoulées et mises à disposition vers la machine utilisateur pour traitement. Généralement, ces fichiers de spoule EMF sont directement injectés dans la file d'attente du spoule du client. Pour les imprimantes et les pilotes qui sont compatibles avec le format EMF, ceci représente la méthode d'impression la plus rapide.

limite de compression d'image de l'impression universelle ;

Ce paramètre définit la qualité maximale et le niveau de compression minimal disponibles pour les images imprimées avec le pilote d'impression universelle Citrix.

Par défaut, la limite de compression d'image est définie sur Meilleure qualité (compression sans perte).

Si Aucune compression est sélectionnée, la compression est désactivée uniquement pour l'impression EMF.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Aucune compression
- Meilleure qualité (compression sans perte)
- Qualité élevée
- Qualité standard
- Qualité réduite (compression maximale)

Lorsque vous ajoutez ce paramètre à une stratégie qui comprend le paramètre Valeurs par défaut de l'optimisation de l'impression universelle, assurez-vous des éléments suivants :

- Si le niveau de compression du paramètre Limite de compression d'image de l'impression universelle est inférieur au niveau défini dans le paramètre Valeurs par défaut de l'optimisation de l'impression universelle, les images sont compressées à l'aide du niveau défini dans le paramètre Limite de compression d'image de l'impression universelle.
- Si la compression est désactivée, les options Qualité d'image souhaitée et Activer la compression lourde du paramètre Valeurs par défaut de l'optimisation de l'impression universelle n'ont aucun effet sur la stratégie.

valeurs par défaut de l'optimisation de l'impression universelle ;

Ce paramètre spécifie les valeurs par défaut de l'optimisation de l'impression lorsque le pilote d'impression universelle est créé pour une session.

- Qualité d'image souhaitée spécifie la limite de compression d'image par défaut appliquée à l'impression universelle. Par défaut, Qualité standard est activée, signifiant que les utilisateurs peuvent uniquement imprimer des images à l'aide des

© 1999-2017 Citrix Systems, Inc. All rights reserved.

compressions standard ou de qualité réduite.

- Activer la compression lourde active ou désactive la réduction de la bande passante au-delà du niveau de compression défini par l'option Qualité d'image souhaitée, sans perte de qualité d'image. Par défaut, la compression intensive est désactivée.
- Les paramètres Cache d'image et de police spécifient si oui ou non vous pouvez cacher des images et des polices qui s'affichent plusieurs fois dans le flux d'impression, assurant ainsi que chaque image ou police est envoyée à l'imprimante une seule fois. Par défaut, les images incorporées et les polices sont mises en cache. Notez que ces paramètres s'appliquent uniquement si la machine utilisateur prend ce comportement en charge.
- Autoriser les non-administrateurs à modifier ces paramètres spécifie si les utilisateurs peuvent ou non modifier les paramètres d'optimisation d'impression dans une session. Par défaut, les utilisateurs ne sont pas autorisés à modifier les paramètres par défaut d'optimisation de l'impression.

Remarque : toutes ces options sont prises en charge pour l'impression EMF. Pour l'impression XPS, seule l'option Qualité d'image souhaitée est prise en charge.
Lorsque vous ajoutez ce paramètre à une stratégie qui comprend le paramètre Limite de compression d'image de l'impression universelle, assurez-vous des éléments suivants :

- Si le niveau de compression du paramètre Limite de compression d'image de l'impression universelle est inférieur au niveau défini dans le paramètre Valeurs par défaut de l'optimisation de l'impression universelle, les images sont compressées à l'aide du niveau défini dans le paramètre Limite de compression d'image de l'impression universelle.
- Si la compression est désactivée, les options Qualité d'image souhaitée et Activer la compression lourde du paramètre Valeurs par défaut de l'optimisation de l'impression universelle n'ont aucun effet sur la stratégie.

Préférence d'aperçu d'impression universelle

Ce paramètre spécifie si la fonction d'aperçu d'impression doit ou non être utilisée pour les imprimantes créées automatiquement ou les imprimantes universelles génériques.

Par défaut, l'aperçu d'impression n'est pas utilisé pour les imprimantes créées automatiquement ou les imprimantes universelles génériques.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Ne pas utiliser l'aperçu pour les imprimantes créées automatiquement ou universelles génériques
- Utiliser l'aperçu d'impression pour les imprimantes créées automatiquement uniquement
- Utiliser l'aperçu d'impression pour les imprimantes universelles génériques uniquement
- Utiliser l'aperçu pour les imprimantes créées automatiquement et universelles génériques

limite de qualité d'impression de l'impression universelle ;

Ce paramètre spécifie le nombre maximal de points par pouce (ppp) disponible pour l'impression dans la session.

Par défaut, l'option Aucune limite est activée, signifiant que les utilisateurs peuvent sélectionner la qualité d'impression maximale autorisée par l'imprimante à laquelle ils se connectent.

Si ce paramètre est configuré, il limite la qualité d'impression maximale disponible auprès des utilisateurs en termes de résolution. À la fois la qualité d'impression elle-même et les capacités de qualité d'impression de l'imprimante à laquelle l'utilisateur se connecte sont restreintes au paramètre configuré. Par exemple, si la configuration est définie sur Moyenne résolution (600 PPP), les utilisateurs sont restreints à une impression d'une qualité maximale de 600 PPP et le paramètre Qualité d'impression de l'onglet Avancé de la boîte de dialogue Imprimante universelle affiche des paramètres de résolution jusqu'à Qualité moyenne (600 PPP).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Brouillon (150 PPP)
- Basse résolution (300 PPP)
- Moyenne résolution (600 PPP)
- Haute résolution (1200 PPP)
- Aucune limite

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Sécurité

Jul 07, 2016

La section Sécurité contient des paramètres de stratégie permettant de configurer le cryptage de session et des données d'ouverture de session.

Niveau de cryptage minimum SecureICA

Ce paramètre spécifie le niveau minimal auquel crypter les données de session envoyées entre le serveur et une machine utilisateur.

Important : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie peut être utilisé uniquement pour activer le cryptage des données d'ouverture de session à l'aide du cryptage RC5 128 bits. Cette option est fournie uniquement à des fins de compatibilité à effet rétroactif avec les versions d'ancienne génération de XenApp et XenDesktop.

Pour VDA 7.x, le cryptage des données de session est défini à l'aide des paramètres de base du groupe de mise à disposition du VDA. Si l'option Activer Secure ICA est sélectionnée pour le groupe de mise à disposition, les données de session sont cryptées à l'aide du cryptage RC5 (128 bits). Si l'option Activer Secure ICA n'est pas sélectionnée pour le groupe de mise à disposition, les données de session sont cryptées à l'aide du cryptage de base.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- De base crypte la connexion à l'aide d'un algorithme non RC5. Cet algorithme protège le flux de données d'une lecture directe, mais n'empêche pas le décryptage. Par défaut, le serveur utilise un cryptage de base pour le trafic client vers serveur.
- 128 bits - ouverture de session uniquement (RC5) crypte les données d'ouverture de session à l'aide du cryptage RC5 128 bits et la connexion cliente à l'aide du cryptage de base.
- 40 bits (RC5) crypte la connexion cliente à l'aide du cryptage RC5 40 bits.
- 56 bits (RC5) crypte la connexion cliente à l'aide du cryptage RC5 56 bits.
- 128 bits (RC5) crypte la connexion cliente à l'aide du cryptage RC5 128 bits.

Les paramètres que vous spécifiez pour le cryptage client-serveur peuvent interagir avec tout autre paramètre de cryptage de votre environnement et de votre système d'exploitation Windows. Si un niveau de cryptage supérieur est défini sur un serveur ou sur une machine cliente, les paramètres que vous spécifiez pour des ressources publiées peuvent être remplacés.

Vous pouvez augmenter les niveaux de cryptage afin de mieux sécuriser les communications et l'intégrité des messages pour certains utilisateurs. Si une stratégie requiert un niveau de cryptage plus élevé, les Citrix Receivers utilisant un niveau de cryptage inférieur se voient refuser la connexion.

SecureICA n'effectue pas d'authentification ni ne vérifie l'intégrité des données. Pour assurer un cryptage de bout en bout pour votre site, utilisez SecureICA avec le cryptage TLS.

SecureICA n'utilise pas d'algorithme conforme à la norme FIPS. Si cela pose un problème, configurez le serveur et Citrix Receiver pour éviter d'utiliser SecureICA.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Limites de serveur

Jul 07, 2016

La section Limites de serveur contient le paramètre de stratégie permettant de contrôler les connexions inactives.

Intervalle d'horloge inactive du serveur

Ce paramètre détermine la durée (en millisecondes) pendant laquelle une session utilisateur non interrompue pourra être maintenue si aucune entrée utilisateur n'est effectuée.

Par défaut, les connexions inactives ne sont pas déconnectées (Intervalle d'horloge inactive du serveur = 0).

> ## Remarque
>
> Lorsque ce paramètre de stratégie est utilisé, une boîte de dialogue indiquant que le minuteur d'inactivité a expiré peut s'afficher lorsque la session a été inactive pendant la durée spécifiée. Il s'agit d'une boîte de dialogue Microsoft qui n'est pas contrôlée par les paramètres de stratégie Citrix. Consultez l'article http://support.citrix.com/article/CTX118618 pour de plus amples informations.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie des limites de session

Jul 07, 2016

La section Limites de session contient des paramètres de stratégie qui permettent de contrôler la durée pendant laquelle les sessions restent connectées avant que leur fermeture soit imposée.

Horloge de session déconnectée

Ce paramètre active ou désactive une horloge permettant de déterminer la durée pendant laquelle un bureau déconnecté et verrouillé peut rester verrouillé avant fermeture de la session.

Par défaut, les sessions déconnectées ne sont pas fermées.

Intervalle d'horloge de session déconnectée

Ce paramètre détermine la durée, en minutes, pendant laquelle un bureau déconnecté et verrouillé peut rester verrouillé avant que la session ne se ferme.

Par défaut, ce délai est de 1440 minutes (24 heures).

Minuteur de connexion de session

Ce paramètre active ou désactive une horloge permettant de déterminer la durée maximale d'une connexion ininterrompue entre une machine utilisateur et un bureau.

Par défaut, ce minuteur est désactivé.

Intervalle de minuteur de connexion de session (Session connection timer interval)

Ce paramètre spécifie le nombre maximal de minutes d'une connexion ininterrompue entre une machine utilisateur et un bureau.

Par défaut, la durée maximale est de 1440 minutes (24 heures).

Minuteur de session inactive

Ce paramètre active ou désactive une horloge qui détermine la durée pendant laquelle une connexion ininterrompue entre une machine utilisateur et un bureau est maintenue si aucune entrée utilisateur n'est effectuée.

Par défaut, ce minuteur est activé.

Intervalle de minuteur de session inactive

Ce paramètre détermine la durée en minutes pour laquelle une connexion non interrompue d'une machine utilisateur vers un bureau pourra être maintenue si aucune entrée utilisateur n'est effectuée.

Par défaut, les connexions inactives sont maintenues pendant 1440 minutes (24 heures).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Fiabilité de session

Jul 07, 2016

La section Fiabilité de session contient les paramètres de stratégie permettant de gérer les connexions de fiabilité de session.

Connexions de fiabilité de session

Ce paramètre autorise ou empêche les sessions de rester ouvertes en cas de perte de connexion réseau.

Par défaut, la fiabilité de session est autorisée.

La fiabilité de session maintient les sessions actives sur l'écran de l'utilisateur lorsque la connectivité au réseau est interrompue. L'utilisateur peut donc visualiser l'application jusqu'à ce que la connexion au réseau reprenne.

Grâce à la fiabilité de session, la session reste active sur le serveur. Pour indiquer que la connexion est interrompue, l'affichage de l'utilisateur se fige et le curseur prend la forme d'un sablier jusqu'à ce que la connexion soit restaurée. L'utilisateur a toujours accès à l'affichage de l'application durant l'interruption et peut reprendre l'interaction avec l'application lorsque la connexion réseau est rétablie. La fonction de fiabilité de session permet aux utilisateurs de se reconnecter sans invite de s'authentifier à nouveau. Si vous ne souhaitez pas autoriser les utilisateurs à se reconnecter aux sessions interrompues sans authentification, configurez le paramètre Authentification de la reconnexion automatique des clients pour exiger l'authentification. Les utilisateurs sont alors invités à s'authentifier de nouveau lorsqu'ils se reconnectent à des sessions interrompues.

Si vous utilisez la fonction de fiabilité de session et la fonction de reconnexion automatique des clients, ces fonctions agissent l'une après l'autre. La fonction de fiabilité de session ferme (ou déconnecte) la session utilisateur après l'expiration de la durée spécifiée dans le paramètre Expiration de délai de la fiabilité de session. Ensuite, les paramètres de reconnexion automatique des clients s'appliquent et la fonction tente d'opérer la reconnexion de l'utilisateur à la session déconnectée.

Numéro de port de la fiabilité de session

Ce paramètre spécifie le numéro de port TCP pour les connexions de fiabilité de session entrantes.

Le numéro port est défini par défaut sur 2598.

Expiration de délai de la fiabilité de session

Ce paramètre indique la durée en secondes pendant lequel le proxy de fiabilité de session attend qu'un client se reconnecte avant d'autoriser la déconnexion de la session.

Par défaut, cette option est définie sur 180 secondes, ou trois minutes.

La durée de maintien d'une session à l'état ouvert peut être prolongée, mais le but de cette fonction consiste à éviter à l'utilisateur de devoir s'authentifier de nouveau. Si vous augmentez la durée pour laquelle une session est gardée ouverte, les risques d'accès non autorisé sont accrus : un utilisateur distrait peut s'éloigner de sa machine cliente et il est alors possible que des utilisateurs non autorisés accèdent à sa session.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Contrôle des fuseaux horaires

Jul 07, 2016

La section Contrôle de fuseau horaire contient des paramètres de stratégie liés à l'utilisation de l'heure locale dans les sessions.

Estimer l'heure locale pour les clients d'ancienne génération

Ce paramètre permet d'activer ou de désactiver l'estimation de l'heure locale des machines des utilisateurs qui envoient des informations de fuseau horaire au serveur.

Par défaut, le serveur estime le fuseau horaire local, si nécessaire.

Ce paramètre est conçu pour être utilisé avec les versions antérieures de Citrix Receiver ou clients ICA qui n'envoient pas d'informations de fuseau horaire au serveur. Lorsqu'il est utilisé avec des clients qui envoient des informations de fuseau horaire au serveur, telles que les versions prises en charge de Citrix Receiver pour Windows, ce paramètre n'a aucun effet.

Utilisation de l'heure locale du client

Ce paramètre permet de déterminer le fuseau horaire de la session utilisateur. Cela peut être soit le fuseau horaire de la session utilisateur soit le fuseau horaire de la machine utilisateur.

Par défaut, le fuseau horaire de la session de l'utilisateur est utilisé.

Pour que ce paramètre entre en vigueur, activez le paramètre Autoriser la redirection du fuseau horaire dans l'Éditeur de stratégie de groupe (Configuration Utilisateur > Modèles d'administration > Services Bureau à distance > Hôte de session Bureau à distance > Redirection de périphérique et de ressource).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Périphériques TWAIN

Jul 07, 2016

La section Périphériques TWAIN contient des paramètres de stratégie liés au mappage des périphériques TWAIN clients, tels qu'appareils photo numériques ou scanners, et à l'optimisation des transferts d'images du client au serveur.

> **Remarque**
>
> TWAIN 2.0 n'est pas pris en charge.

Redirection de périphérique TWAIN client

Ce paramètre autorise ou empêche les utilisateurs d'accéder aux périphériques TWAIN sur la machine utilisateur à partir d'applications de traitement d'image hébergées sur les serveurs. Par défaut, la redirection de périphérique TWAIN est autorisée.

Les paramètres de stratégie suivants sont associés :

- Niveau de compression TWAIN
- Limite de bande passante de redirection du périphérique TWAIN
- Pourcentage de limite de bande passante de redirection du périphérique TWAIN

Niveau de compression TWAIN

Ce paramètre spécifie le niveau de compression des transferts d'images du client au serveur. Utilisez Basse pour une qualité d'image optimale, Moyenne pour une bonne qualité d'image ou Élevée pour une faible qualité d'image. Par défaut, la compression moyenne est appliquée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Périphériques USB

Jul 07, 2016

La section Périphériques USB contient des paramètres de stratégie permettant de gérer la redirection de fichiers pour les périphériques USB.

Règles d'optimisation des périphériques USB clients

Les règles d'optimisation des périphériques USB clients peuvent être appliquées aux périphériques pour désactiver l'optimisation, ou pour modifier le mode d'optimisation.

Lorsqu'un utilisateur branche un périphérique USB, l'hôte vérifie si le périphérique est autorisé par les paramètres de stratégie USB. Si le périphérique est autorisé, l'hôte vérifie ensuite les **Règles d'optimisation de périphérique USB client** pour le périphérique. Si aucune règle n'est spécifiée, le périphérique est traité en mode interactif (02). Le mode capture (04) est la méthode recommandée pour les périphériques de signature. Consultez les descriptions ci-dessous pour connaître les modes disponibles.

À savoir

- Pour l'utilisation de tablettes et de dispositifs de signature numérique Wacom, Citrix recommande de désactiver l'écran de veille. Vous trouverez des procédures à cet effet à la fin de cette section.
- La prise en charge de l'optimisation des tablettes et des dispositifs de signature numérique Wacom STU a été préconfigurée dans l'installation de stratégies XenApp et XenDesktop.
- Les périphériques de signature fonctionnent sur XenApp et XenDesktop et ne requièrent pas de pilote pour être utilisés en tant que périphérique de signature. Wacom propose des logiciels supplémentaires qui peuvent être installés pour personnaliser le périphérique. Voir http://www.wacom.com/.
- Tablettes graphiques. Certains périphériques de dessin peuvent être considérés comme périphérique HID sur des bus PCI/ACPI et ne sont pas pris en charge. Ces périphériques doivent être connectés sur un contrôleur d'hôte USB sur le client pour être redirigés dans une session XenDesktop.

Les règles de stratégies sont au format tag=value (balise=valeur) séparées par des espaces. Les balises suivantes sont prises en charge :

Nom de balise	Description
Mode	Le mode d'optimisation est pris en charge pour les périphériques d'entrée pour une classe=**03**. Les modes pris en charge sont les suivants : Aucune optimisation - valeur **01**. Mode interactif - valeur **02**. Recommandé pour les périphériques tels que des tablettes à stylet et des souris 3D Pro. Mode capture - valeur **04**. Mode préféré pour les périphériques tels que les dispositifs de signature numérique.
VID	ID fournisseur du descripteur de périphérique.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

PID	ID de produit du descripteur de périphérique.
REL	ID de version du descripteur de périphérique.
Class	Classe du descripteur de périphérique ou d'un descripteur d'interface.
SubClass	Sous-classe du descripteur de périphérique ou d'un descripteur d'interface.
Prot	Protocole à partir du descripteur de périphérique ou d'un descripteur d'interface.

Exemples

Mode=00000004 VID=1230 PID=1230 class=03 #Périphérique fonctionnant en mode capture

Mode=00000002 VID=1230 PID=1230 class=03 #Périphérique fonctionnant en mode interactif (valeur par défaut)

Mode=00000001 VID=1230 PID=1230 class=03 #Périphérique fonctionnant sans optimisation

Mode=00000100 VID=1230 PID=1230 #Optimisation de la configuration du périphérique désactivée (valeur par défaut)

Mode=00000200 VID=1230 PID=1230 #Optimisation de la configuration du périphérique activée

Désactivation du mode d'optimisation à l'aide d'un paramètre de registre

Le mode d'optimisation peut être désactivé sur tout le système par un indicateur de registre :

HKLM\System\CurrentControlSet\Services\Icausbb\Parameters

DisableInputOptimization DWORD - régler la valeur sur **1**

Un redémarrage système est requis pour que ces modifications prennent effet.

Désactivation de l'écran de veille des dispositifs de signature numérique Wacom

Pour l'utilisation de tablettes et de dispositifs de signature numérique Wacom, Citrix recommande de désactiver l'écran de veille comme suit :

1. Installez **Wacom-STU-Driver** après la redirection du périphérique.
2. Installez **Wacom-STU-Display MSI** pour pouvoir accéder au panneau de configuration du dispositif de signature.
3. Accédez à **Control Panel > Wacom STU Display > STU430** ou **STU530** et sélectionnez l'onglet de votre modèle.
4. Cliquez sur **Change**, puis sélectionnez **Yes** lorsque la fenêtre de sécurité de compte utilisateur (UAC) s'affiche.
5. Sélectionnez **Disable slideshow**, puis **Apply**.

Une fois que le paramètre est défini pour un modèle de dispositif de signature numérique, il est appliqué à tous les modèles.

Redirection de périphérique USB client

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ce paramètre permet d'autoriser ou d'empêcher la redirection de périphériques USB vers et depuis la machine utilisateur.

Par défaut, les périphériques USB ne sont pas redirigés.

Règles de redirection des périphériques USB clients

Ce paramètre spécifie les règles de redirection des périphériques USB.

Par défaut, aucune règle n'est spécifiée.

Lorsqu'un utilisateur connecte un périphérique USB, la machine hôte vérifie celui-ci par rapport à chacune des règles de stratégie jusqu'à ce qu'une correspondance soit trouvée. La première correspondance trouvée pour un périphérique est considérée comme définitive. Si la première correspondance est une règle Autoriser, le périphérique est envoyé vers le bureau virtuel. Si la première correspondance est une règle Refuser, le périphérique n'est disponible que pour le bureau local. Si aucune correspondance n'est trouvée, les règles par défaut sont utilisées.

Les règles de stratégies sont au format {Allow:|Deny:} et sont suivies d'un ensemble d'expressions tag=value (balise=valeur) séparées par des espaces. Les balises suivantes sont prises en charge :

Nom de balise	Description
VID	ID fournisseur du descripteur de périphérique
PID	ID de produit du descripteur de périphérique
REL	ID de version du descripteur de périphérique
Class	Classe du descripteur de périphérique ou d'un descripteur d'interface
SubClass	Sous-classe du descripteur de périphérique ou d'un descripteur d'interface
Prot	Protocole à partir du descripteur de périphérique ou d'un descripteur d'interface

Lors de la création de nouvelles règles de stratégie, rappelez-vous ce qui suit :

- Les règles ne sont pas sensibles à la casse.
- Les règles peuvent éventuellement comporter un commentaire, introduit par #, à la fin.
- Les espaces vides et les lignes de commentaires pures sont ignorés.
- Les balises doivent utiliser l'opérateur de correspondance = (par exemple, VID=1230_).
- Chaque règle doit commencer sur une nouvelle ligne ou faire partie d'une liste séparée par des points-virgules.
- Reportez-vous aux codes de classe USB disponibles sur le site Web USB Implementers Forum, Inc.

Exemples de règles de stratégie USB définies par l'administrateur :

- Allow: VID=1230 PID=0007 # ANOther Industries, ANOther Flash Drive
- Deny: Class=08 subclass=05 # Mass Storage
- Pour créer une règle qui refuse tous les périphériques USB, utilisez « DENY: » sans aucune autre balise.

Redirection de périphérique Plug and Play USB client

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ce paramètre permet d'autoriser ou d'empêcher l'utilisation de périphériques Plug and Play comme les appareils photo ou les périphériques de point de vente dans une session cliente.

Par défaut, la redirection de périphériques Plug and Play est autorisée. Lorsque l'option a la valeur Autorisé, tous les périphériques Plug and Play d'un utilisateur ou d'un groupe spécifique sont redirigés. Lorsque l'option a la valeur Interdit, aucun périphérique n'est redirigé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Affichage visuel

Jul 07, 2016

La section Affichage visuel contient des paramètres de stratégie permettant de contrôler la qualité des images envoyées depuis des bureaux virtuels vers la machine utilisateur.

Nombre de couleurs préféré pour les graphiques simples

Permet de réduire le nombre de couleurs à partir duquel les graphiques simples sont envoyés à **16 bits par pixel**, tout en améliorant potentiellement le temps de réponse sur les connexions à faible bande passante, en contrepartie d'une légère dégradation de la qualité de l'image. Cette option est uniquement prise en charge lorsqu'aucun codec vidéo n'est utilisé pour compresser les graphiques.

Par défaut, la valeur est de 24 bits par pixel.

Taux de trames cible

Ce paramètre spécifie le nombre maximal de trames par seconde envoyées depuis le bureau virtuel vers la machine utilisateur.

La valeur maximale par défaut est de 30 trames par seconde.

La définition d'un nombre élevé de trames par seconde (par exemple 30) améliore l'expérience utilisateur mais exige plus de bande passante. La réduction du nombre de trames par seconde (par exemple 10) augmente la capacité du serveur à monter en charge au détriment de l'expérience utilisateur. Pour les machines utilisateur possédant des UC plus lents, spécifiez une valeur inférieure pour améliorer l'expérience de l'utilisateur.

Qualité visuelle

Ce paramètre spécifie la qualité visuelle désirée pour les images affichées sur la machine utilisateur.

Par défaut, cette option est définie sur Moyenne.

Pour spécifier la qualité des images, choisissez l'une des options suivantes :

- **Faible**
- **Moyen** : offre les meilleures performances et une bande passante optimale dans la plupart des cas d'utilisation
- **Élevée** : recommandé si vous avez besoin de qualité d'image visuelle sans perte
- **Sans perte si possible** : envoie des images avec perte à la machine utilisateur durant les périodes de forte activité réseau et des images sans perte après réduction de l'activité réseau ; ce paramètre améliore les performances des connexions réseau avec une bande passante réduite
- **Toujours sans perte** : dans les cas où la préservation des données d'images est vitale (par exemple, lors de l'affichage de radiographies où la perte de qualité est inacceptable), sélectionnez Toujours sans perte pour vous assurer que les données avec perte ne sont jamais envoyées à la machine utilisateur.

Si le paramètre **Mode graphique d'ancienne génération** est activé, le paramètre **Qualité visuelle** n'a aucun effet dans cette stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie des images en mouvement

Aug 22, 2016

La section Images en mouvement contient des paramètres qui vous permettent de supprimer ou de modifier la compression des images dynamiques.

> ## Remarque
>
> Pour les versions VDA 7.0 à 7.6, les paramètres de stratégie **Compression d'images en mouvement** et **Taux de trame minimum cible** s'appliquent uniquement lorsque le **Mode graphique d'ancienne génération** est activé. Pour les versions VDA 7.6 FP1 et versions ultérieures, ces paramètres s'appliquent lorsque le mode graphique d'ancienne génération est activé ou désactivé.

Compression d'images en mouvement

Ce paramètre spécifie si l'affichage adaptatif est activé ou non. L'affichage adaptatif ajuste automatiquement la qualité d'image des vidéos et des diapositives de transition des diaporamas en fonction de la bande passante disponible. Lorsque l'affichage adaptatif est activé, les utilisateurs doivent voir des présentations fluides sans réduction de qualité.
Par défaut, l'affichage adaptatif est activé.

Pour les versions VDA 7.0 à 7.6, ce paramètre s'applique uniquement lorsque le mode graphique d'ancienne génération est activé. Pour les versions VDA 7.6 FP1 et versions ultérieures, ce paramètre s'applique lorsque le mode graphique d'ancienne génération est activé, ou lorsque le mode graphique d'ancienne génération est désactivé et qu'aucun codec vidéo n'est utilisé pour compresser les graphiques.

Lorsque le mode graphique d'ancienne génération est activé, la session doit être redémarrée pour que les modifications prennent effet. L'affichage adaptatif et l'affichage progressif sont mutuellement exclusifs ; l'activation de l'affichage adaptatif désactive l'affichage progressif et vice versa. Il est cependant possible de désactiver l'affichage progressif et l'affichage adaptatif en même temps. L'utilisation de l'affichage progressif en tant que fonctionnalité d'ancienne génération n'est pas recommandée avec XenApp ou XenDesktop. La définition du niveau de seuil de l'affichage progressif désactive l'affichage adaptatif.

Taux de trame minimum cible

Ce paramètre spécifie le taux de trame minimum par seconde que le système tente de conserver, des images dynamiques, dans des conditions de bande passante faible.
Par défaut, cette option est définie sur 10 fps.

> ## Remarque
>
> Pour Virtual Delivery Agent 7.x, les paramètres de stratégie suivants s'appliquent uniquement lorsque le paramètre de stratégie **Mode graphique d'ancienne génération** est activé.

Qualité d'image minimale

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ce paramètre spécifie la qualité d'image minimale acceptable pour l'affichage adaptatif. La qualité des images est d'autant plus élevée que la compression est faible. Choisissez entre les valeurs de compression Ultra élevée, Très élevée, Élevée, Normale et Basse.
Par défaut, cette option est définie sur Normale.

Niveau de compression progressif

Ce paramètre permet un affichage initial d'images moins détaillé, mais plus rapide.
Par défaut, la compression progressive n'est pas appliquée.

L'image plus détaillée définie par le paramètre de compression avec perte normale, s'affiche lorsqu'elle devient disponible. Utilisez une compression très élevée ou extrêmement élevée pour un affichage optimal des images à utilisation intensive de la bande passante, telles que des photographies.

Pour que la compression progressive soit efficace, son niveau de compression doit être supérieur à celui du paramètre Niveau de compression avec perte.
Remarque : le niveau amélioré de compression associé à la compression progressive optimise également l'interactivité des images dynamiques via les connexions clientes. La qualité d'une image dynamique, telle qu'un modèle pivotant à trois dimensions, est temporairement réduite jusqu'à ce que l'image devienne fixe, moment auquel le paramètre de compression avec perte normale est appliqué.
Les paramètres de stratégie suivants sont associés :

- Valeur de seuil de compression progressif
- Compression lourde progressive

Valeur de seuil de compression progressif

Ce paramètre représente la bande passante maximale, en kilobits par seconde, pour une connexion à laquelle la compression progressive est appliquée. Cela ne concerne que les connexions clientes liées à cette bande passante.
Par défaut, la valeur de seuil est de 2147483647 kilobits par seconde.

Les paramètres de stratégie suivants sont associés :

- Valeur de seuil de compression progressif
- Compression lourde progressive

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Images immobiles

Aug 22, 2016

La section Images immobiles contient des paramètres qui vous permettent de supprimer ou de modifier la compression des images statiques.

> ## Remarque
>
> Pour Virtual Delivery Agent 7.x, ces paramètres de stratégie s'appliquent uniquement lorsque le paramètre de stratégie **Mode graphique d'ancienne génération** est activé.

Compression couleur supplémentaire

Ce paramètre active ou désactive l'utilisation d'une compression de couleur supplémentaire sur les images mises à disposition sur les connexions côté client qui sont limitées en bande passante, améliorant les temps de réponse en réduisant la qualité des images affichées.
Par défaut, la compression de couleur supplémentaire est désactivée.

Lorsqu'elle est activée, la compression de couleur supplémentaire est appliquée uniquement lorsque la bande passante de connexion cliente se trouve en dessous de la valeur du Seuil de compression de couleur supplémentaire. Lorsque la bande passante de connexion cliente se trouve en dessus de la valeur de seuil ou que Désactivé est sélectionné, la compression de couleur supplémentaire n'est pas appliquée.

Seuil de compression de couleur supplémentaire

Ce paramètre représente la bande passante maximale, en kilobits par seconde, pour une connexion en dessous de laquelle la compression de couleur supplémentaire est appliquée. Si la bande passante de connexion cliente tombe en dessous de la valeur définie, la compression de couleur supplémentaire, si activée, est appliquée.
Par défaut, la valeur de seuil est de 8192 kilobits par seconde.

Compression intensive

Ce paramètre vous permet d'activer ou de désactiver la réduction de bande passante au-delà de la compression progressive sans perte de qualité d'image, en utilisant un algorithme graphique plus évolué, mais qui nécessite des ressources processeur importantes.
Par défaut, la compression intensive est désactivée.

Lorsqu'elle est activée, la compression intensive s'applique à tous les paramètres de compression avec perte. Elle est prise en charge sur Citrix Receiver, mais n'a aucun effet sur les autres plug-ins.

Les paramètres de stratégie suivants sont associés :

- Niveau de compression progressif
- Valeur de seuil de compression progressif

Niveau de compression avec perte

Ce paramètre permet de contrôler le niveau de compression avec perte utilisé sur des images fournies sur des connexions clientes à bande passante limitée. Le cas échéant, l'affichage des images sans compression risque d'être ralenti.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Par défaut, la compression moyenne est sélectionnée.

Pour améliorer la réactivité avec des images à utilisation intensive de la bande passante, utilisez une compression élevée. Si la conservation des données d'images est un élément essentiel, par exemple lors de l'affichage de radiographies où la perte de qualité ne peut pas être tolérée, il est préférable de ne pas utiliser une compression avec perte.

Paramètre de stratégie connexe : valeur de seuil de compression avec perte

Valeur de seuil de compression avec perte

Ce paramètre représente la bande passante maximale, en kilobits par seconde, pour une connexion à laquelle la compression avec perte est appliquée.
Par défaut, la valeur de seuil est de 2147483647 kilobits par seconde.

L'ajout du paramètre Niveau de compression avec perte à une stratégie et l'inclusion d'un seuil non spécifié peut améliorer la vitesse d'affichage des bitmaps comprenant un nombre de détails élevés, tels que les photographies, dans un réseau local.

Paramètre de stratégie connexe : niveau de compression avec perte

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie WebSockets

Jul 07, 2016

La section WebSockets contient des paramètres de stratégie pour accéder aux bureaux virtuels et aux applications hébergées avec Citrix Receiver pour HTML5. La fonctionnalité WebSockets renforce la sécurité et réduit la charge en réalisant une communication bidirectionnelle entre les applications et les serveurs de navigateur sans ouvrir plusieurs connexions HTTP.

Connexions WebSockets

Ce paramètre autorise ou interdit les connexions WebSockets.

Par défaut, les connexions WebSockets sont interdites.

Numéro de port WebSockets

Ce paramètre identifie le port pour les connexions WebSockets entrantes.

La valeur par défaut est 8008.

Liste de serveurs d'origine approuvés WebSockets

Ce paramètre fournit une liste séparée par des virgules des serveurs d'origine de confiance, habituellement Citrix Receiver pour Web, exprimée sous la forme d'adresses URL. Seules les connexions WebSockets provenant de l'un de ces adresses est accepté par le serveur.

Par défaut, des caractères génériques sont utilisés pour faire confiance à toutes les adresses URL Citrix Receiver pour Web.

Si vous choisissez d'entrer une adresse dans la liste, utilisez la syntaxe suivante :

<protocole>://<Nom de domaine complet de l'ordinateur hôte>:[port]

Le protocole doit être HTTP ou HTTPS. Si le port n'est pas spécifié, le port 80 pour HTTP et le port 443 est utilisé pour HTTPS.

Le caractère générique * peut être utilisé dans l'adresse URL, sauf dans le cadre d'une adresse IP (10.105. *. *).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Gestion de la charge

Jul 07, 2016

La section Gestion de la charge contient des paramètres de stratégie pour l'activation et la configuration de la gestion de la charge entre les serveurs mettant à disposition des machines avec OS Windows Server.

Pour de plus amples informations sur le calcul de l'index de calculateur de charge, consultez l'article CTX202150.

Tolérance d'ouvertures de session simultanée

Ce paramètre spécifie le nombre maximal d'ouvertures de session simultanées qu'un serveur peut accepter.

Par défaut, cette option est définie sur 2.

Utilisation UC

Ce paramètre spécifie le niveau d'utilisation de l'UC, sous la forme d'un pourcentage, à laquelle le serveur signale une pleine charge. Lorsque cette option est activée, la valeur par défaut à laquelle le serveur signale une pleine charge est 90%.

Par défaut, ce paramètre est désactivé et l'utilisation de l'UC est exclue du calcul de la charge.

Priorité de processus exclue de l'utilisation UC

Ce paramètre spécifie le niveau de priorité auquel l'utilisation de l'UC est exclue de l'index de charge de l'utilisation de l'UC.

Par défaut, cette option est définie sur Inférieure à la normale ou Basse.

Utilisation du disque

Ce paramètre spécifie la longueur de la file d'attente à laquelle le serveur signale une pleine charge 75%. Lorsque cette option est activée, la valeur par défaut de file d'attente du disque est de 8.

Par défaut, ce paramètre est désactivé et l'utilisation du disque est exclue du calcul des charges.

Nombre maximum de sessions

Ce paramètre spécifie le nombre maximal de sessions qu'un serveur peut héberger. Lorsqu'il est activé, le paramètre par défaut pour le nombre maximal de sessions qu'un serveur peut héberger est 250.

Ce paramètre est activé par défaut.

Utilisation de mémoire

Ce paramètre spécifie le niveau d'utilisation de la mémoire, sous la forme d'un pourcentage, à laquelle le serveur signale une pleine charge. Lorsque cette option est activée, la valeur par défaut à laquelle le serveur signale une pleine charge est 90%.

Par défaut, ce paramètre est désactivé et l'utilisation de mémoire est exclue du calcul de la charge.

Charge de base d'utilisation mémoire

Ce paramètre spécifie une approximation de l'utilisation de la mémoire du système d'exploitation de base et définit, en Mo, l'utilisation de la mémoire en dessous de laquelle un serveur est considéré comme ayant une charge de zéro.

Par défaut, cette option est définie sur 768 Mo

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Profile Management

Jul 07, 2016

La section Profile Management contient les paramètres de stratégie pour l'activation de Profile Management et la spécification des groupes à inclure et à exclure du traitement Profile Management.

D'autres informations (telles que les noms des paramètres du fichier .ini et la version de Profile Management requise pour un paramètre de stratégie spécifique) sont disponibles dans Stratégies de Profile Management.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Avancés

Jul 07, 2016

La section Paramètres avancés contient les paramètres de stratégie liés à la configuration avancée de Profile Management.

Désactiver la configuration automatique

Ce paramètre permet d'activer Profile Management pour examiner votre environnement ; par exemple, pour vérifier la présence de Personal vDisks, et configurer la stratégie de groupe en conséquence. Seules les stratégies Profile Management dans l'état Non configuré sont ajustées, de sorte que toutes les personnalisations effectuées précédemment sont conservées. Cette fonctionnalité accélère le déploiement et simplifie l'optimisation. Aucune configuration de la fonctionnalité n'est nécessaire, mais vous pouvez désactiver la configuration automatique lors de la mise à niveau (pour conserver les paramètres à partir de versions antérieures) ou lors de la résolution des problèmes. La configuration automatique ne fonctionne pas dans XenApp ou d'autres environnements.

Par défaut, la configuration automatique est autorisée.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, la configuration automatique est activée afin que les paramètres de Profile Management puissent être modifiés si votre environnement change.

Fermer la session de l'utilisateur si un problème se produit

Ce paramètre permet à Profile Management de fermer la session d'un utilisateur lorsqu'un problème est détecté, par exemple, si le magasin de l'utilisateur n'est pas disponible. Lorsqu'il est activé, un message d'erreur est affiché à l'utilisateur avant que sa session soit fermée. Lorsqu'il est désactivé, les utilisateurs se voient attribuer un profil temporaire.

Par défaut, ce paramètre est désactivé et un profil temporaire est attribué aux utilisateurs lorsqu'un problème est détecté.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, un profil temporaire est fourni.

Nombre de tentatives d'accès à des fichiers verrouillés

Ce paramètre spécifie le nombre de tentatives effectuées par Profile Management pour accéder à des fichiers verrouillés.

Par défaut, ce paramètre est défini sur 5 tentatives.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, la valeur par défaut est utilisée.

Traiter les cookies Internet à la fermeture de session

Ce paramètre permet d'activer Profile Management pour traiter le fichier index.dat lors de l'ouverture de session pour supprimer les cookies Internet dans le système de fichiers après la navigation intensive qui peuvent entraîner la saturation du profil. Étant donné que ce paramètre augmente la durée de fermeture de session, ne l'activez que si vous rencontrez ce problème.

Par défaut, ce paramètre est désactivé, Profile Management ne traite pas le fichier index.dat lors de la fermeture de session.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, index.dat n'est pas traité.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie De base

Jul 07, 2016

La section Paramètres de base contient des paramètres de stratégie liés à la configuration de base de Profile Management.

Réécriture active

Ce paramètre permet de modifier les fichiers et dossiers (mais pas les paramètres de registre) devant être synchronisés avec le magasin utilisateur durant une session, avant la fermeture de session.

Par défaut, la synchronisation avec le magasin d'utilisateur durant une session est désactivée.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, il est activé.

Activer Profile Management

Ce paramètre permet d'activer Profile Management pour traiter les ouvertures et les fermetures de session.

Par défaut, ce paramètre est désactivé pour faciliter le déploiement.

Important : Citrix recommande d'activer Profile Management uniquement après avoir terminé toutes les autres tâches de configuration et testé le comportement des profils utilisateur Citrix dans votre environnement.
Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, Profile Management ne traite pas les profils utilisateur Windows.

Groupes exclus

Ce paramètre spécifie les groupes d'ordinateurs locaux et les groupes de domaines (locaux, globaux et universels) exclus du traitement Profile Management.

Lorsque cette option est activée, Profile Management ne traite pas les membres des groupes d'utilisateurs spécifiés.

Par défaut, ce paramètre est désactivé, les membres de tous les groupes d'utilisateurs sont traités.

Spécifiez les groupes de domaines au format : <NOM DE DOMAINE>\<NOM DE GROUPE>

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les membres de tous les groupes d'utilisateurs sont traités.

Prise en charge de profils hors connexion

Ce paramètre permet d'activer la prise en charge de profil hors connexion, ce qui permet la synchronisation des profils avec le magasin de l'utilisateur à la première opportunité après une déconnexion du réseau.

Par défaut, la prise en charge des profils déconnectés est désactivée.

Ce paramètre s'applique à un ordinateur portable ou aux utilisateurs mobiles itinérants. Lorsque la connexion au réseau est interrompue, les profils restent inchangés sur l'ordinateur portable ou le périphérique même après redémarrage ou mise en veille prolongée. Au fur et à mesure que les utilisateurs mobiles travaillent, leurs profils sont mis à jour localement et

© 1999-2017 Citrix Systems, Inc. All rights reserved.

synchronisés avec le magasin de l'utilisateur lorsque la connexion réseau est rétablie.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, la prise en charge des profils hors connexion est désactivée.

Chemin d'accès au magasin de l'utilisateur

Ce paramètre spécifie le chemin d'accès au répertoire (magasin de l'utilisateur) dans lequel les paramètres utilisateur, tels que les paramètres de registre et les fichiers synchronisés, sont enregistrés.

Par défaut, le répertoire Windows du lecteur de base est utilisé.

Si ce paramètre est désactivé, les paramètres utilisateur sont enregistrés dans le sous-répertoire Windows du répertoire de base.

Le chemin d'accès peut être :
- **Un chemin relatif**. Il doit être relatif au répertoire de base (qui est généralement configuré en tant qu'attribut #homeDirectory# pour un utilisateur dans Active Directory).
- **Un chemin UNC absolu**. Spécifie généralement un partage de serveurs ou un espace de noms DFS.
- **Désactivé ou non configuré**. Dans ce cas, la valeur #homeDirectory#\Windows est utilisée.

Utiliser les types de variables suivants lors de la configuration de ce paramètre de stratégie :
- Variables d'environnement système entourées de symboles pourcentage (par exemple, %ProfVer%). Veuillez noter que les variables d'environnement système requièrent généralement une configuration supplémentaire.
- Attributs de l'objet utilisateur Active Directory entourés de hachages (par exemple, #sAMAccountName#).
- Variables Profile Management. Pour plus d'informations, consultez la documentation relative à Profile Management.

Vous pouvez également utiliser les variables d'environnement utilisateur %username% et %userdomain% et créer des attributs personnalisés pour définir des variables d'organisation telles que l'emplacement ou les utilisateurs. Les attributs sont sensibles à la casse.

Exemples :
- \\server\share\#sAMAccountName# stocke les paramètres utilisateur dans le chemin UNC \\server\share\JohnSmith (si #sAMAccountName# correspond à JohnSmith pour l'utilisateur actuel)
- \\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_PROFILEVER!!CTX_OSBITNESS! peut s'étendre à \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\v2x64

Important : quels que soient les attributs ou variables que vous utilisez, vérifiez que ce paramètre est appliqué au dossier de niveau supérieur du dossier contenant NTUSER.DAT. Par exemple, si ce fichier figure dans \\serveur\profils$\JohnSmith.Finance\v2x64\UPM_Profile, définissez le chemin d'accès au magasin de l'utilisateur comme tel : \\serveur\profils$\JohnSmith.Finance\v2x64 (en n'incluant pas le sous-dossier \UPM_Profile).
Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, le répertoire Windows du lecteur de base est utilisé.

Traiter les ouvertures de session des administrateurs locaux

ce paramètre spécifie si les ouvertures de session des membres du groupe BUILTIN\Administrators sont traitées. Cela permet aux utilisateurs de domaine avec des droits d'administrateur local, généralement utilisateurs XenDesktop avec des bureaux virtuels attribués d'ignorer le traitement, d'ouvrir une session et de résoudre les problèmes liés à un bureau avec Profile Management.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si ce paramètre est désactivé ou qu'il n'est pas configuré sur les systèmes d'exploitation serveur, Profile Management suppose que les ouvertures de session des utilisateurs du domaine doivent être traitées, mais pas celles des administrateurs locaux. Sur les systèmes d'exploitation de bureau, les ouvertures de session des administrateurs locaux sont traitées.

Par défaut, ce paramètre est désactivé, et les ouvertures de session des administrateurs locaux ne sont pas traitées.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les ouvertures de session des administrateurs locaux ne sont pas traitées.

Groupes traités

Ce paramètre spécifie les groupes d'ordinateurs locaux et les groupes de domaines (locaux, globaux et universels) qui sont inclus dans le traitement Profile Management.

Lorsque cette option est activée, Profile Management traite uniquement les membres des groupes d'utilisateurs spécifiés.

Par défaut, ce paramètre est désactivé, les membres de tous les groupes d'utilisateurs sont traités.

Spécifiez les groupes de domaines au format : <NOM DE DOMAINE>\<NOM DE GROUPE>

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les membres de tous les groupes d'utilisateurs sont traités.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Multi-plateformes

Jul 07, 2016

La section Multi-plateformes contient des paramètres de stratégie liés à la configuration de la fonctionnalité de paramètres multi-plateformes de Profile Management.

Paramètres multi-plateformes des groupes d'utilisateurs

Ce paramètre spécifie les groupes d'utilisateurs Windows dont les profils sont traités lorsque la fonctionnalité de paramètres multi-plateformes est activée.

Par défaut, ce paramètre est désactivé et tous les groupes d'utilisateurs traités spécifiés dans le paramètre de stratégie Groupes traités sont traités.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, tous les groupes d'utilisateurs sont traités.

Activer les paramètres multi-plateformes

Ce paramètre active ou désactive la fonctionnalité de paramètres au travers des plates-formes, qui vous permet de migrer les profils des utilisateurs et d'assurer leur itinérance lorsque l'utilisateur se connecte à la même application exécutée sur de multiples systèmes d'exploitation.

Cette fonctionnalité de paramètres au travers des plates-formes est désactivée par défaut.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun paramètre multi-plateforme n'est appliqué.

Chemin d'accès aux définitions multi-plateformes

Ce paramètre spécifie l'emplacement réseau, sous la forme d'un chemin d'accès UNC, de la définition des fichiers copiés à partir du pack de téléchargement.

Remarque : les utilisateurs doivent posséder un accès en lecture, et les administrateurs un accès en écriture à cet emplacement et il doit être un partage de fichiers SMB (Server Message Block) ou CIFS (Common Internet File System).
Par défaut, aucun chemin n'est spécifié.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun paramètre multi-plateforme n'est appliqué.

Chemin d'accès au magasin des paramètres multi-plateformes

Ce paramètre spécifie le chemin d'accès au magasin multi-plateformes, le dossier dans lequel les paramètres multi-plateformes des utilisateurs sont enregistrés. Le chemin peut être soit un chemin UNC vers le répertoire de base ou relatif à celui-ci.

Remarque : les utilisateurs doivent posséder un accès en écriture à ce magasin.
Par défaut, ce paramètre est désactivé et le chemin d'accès Windows\PM_CP est utilisé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, la valeur par défaut est utilisée.

Source de création des paramètres multi-plateformes

Ce paramètre spécifie une plate-forme en tant que plate-forme de base si ce paramètre est activé pour l'unité d'organisation de cette plate-forme. Les données provenant des profils de la plate-forme de base sont migrées vers le magasin de paramètres multi-plateformes.

Le jeu de profils de chaque plate-forme est stocké dans une unité d'organisation distincte. Ceci signifie que vous devez décider quelles données de profil de la plate-forme utiliser pour amorcer le magasin de paramètres multi-plateformes. On parle de plate-forme de base.

Lorsque cette option est activée, Profile Management fait migrer les données du profil à plate-forme unique vers le magasin si le magasin des paramètres multi-plateformes contient un fichier de définition sans aucune donnée, ou que les données cachées dans un profil à plate-forme unique sont plus récentes que les données de définition du magasin.

Important : si ce paramètre est activé dans plusieurs unités d'organisation, ou plusieurs objets d'utilisateur ou de machine, la plate-forme sur laquelle le premier utilisateur ouvre une session devient le profil de base.
Par défaut, ce paramètre est désactivé, et Profile Management ne fait pas migrer les données depuis le profil à plate-forme unique vers le magasin.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Système de fichiers

Jul 07, 2016

La section Système de fichiers contient des paramètres de stratégie permettant de configurer les fichiers et les répertoires dans le profil utilisateur qui sont synchronisés entre le système sur lequel le profil est installé et le magasin de l'utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Exclusions

Jul 07, 2016

La section Exclusions contient des paramètres de stratégie permettant de configurer les fichiers et les répertoires dans un profil utilisateur sont exclus du processus de synchronisation.

Liste d'exclusion - répertoires

Ce paramètre spécifie une liste de dossiers dans le profil d'utilisateur qui sont ignorées durant la synchronisation.

Spécifiez les noms de dossier en tant que chemins d'accès relatifs au profil utilisateur (USERPROFILE%%).

Par défaut, ce paramètre est désactivé et tous les dossiers du profil utilisateur sont synchronisés.

Exemple : Desktop ignore le dossier Desktop dans le profil utilisateur.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, tous les dossiers du profil utilisateur sont synchronisés.

Liste d'exclusion - fichiers

Ce paramètre spécifie une liste de fichiers dans le profil d'utilisateur qui sont ignorées durant la synchronisation.

Par défaut, ce paramètre est désactivé et tous les fichiers du profil utilisateur sont synchronisés.

Spécifiez les noms de fichiers en tant que chemins d'accès relatifs au profil utilisateur (USERPROFILE%%). Notez que les caractères génériques sont autorisés et sont appliqués de manière récursive.

Exemple : Desktop\Desktop.ini ignore le fichier Desktop.ini dans le dossier Bureau.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, tous les fichiers du profil utilisateur sont synchronisés.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Synchronisation

Jul 07, 2016

La section Synchronisation contient des paramètres de stratégie pour spécifier les fichiers et les dossiers dans un profil utilisateur qui sont synchronisés entre le système sur lequel le profil est installé et le magasin de l'utilisateur.

Répertoires à synchroniser

Ce paramètre spécifie tous les fichiers, qui figurent dans des dossiers exclus, que vous voulez que Profile Management inclue dans le processus de synchronisation. Par défaut, Profile Management synchronise tout ce qui se trouve dans le profil utilisateur. Il n'est pas nécessaire d'inclure de sous-dossiers dans le profil utilisateur en les ajoutant à cette liste. Pour plus d'informations, veuillez consulter information la section Inclure et exclure des éléments.

Les chemins d'accès de cette liste doivent être relatifs au profil utilisateur.

Exemple : Desktop\exclude\include s'assure que le sous-dossier appelé include est synchronisé même si le dossier appelé Desktop\exclude ne l'est pas.

Par défaut, ce paramètre est désactivé et aucun dossier n'est spécifié.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, seuls les dossiers non exclus dans le profil utilisateur sont synchronisés.

Fichiers à synchroniser

Ce paramètre spécifie tous les fichiers, qui figurent dans des dossiers exclus, que vous voulez que Profile Management inclue dans le processus de synchronisation. Par défaut, Profile Management synchronise tout ce qui se trouve dans le profil utilisateur. Il n'est pas nécessaire d'inclure de fichiers dans le profil utilisateur en les ajoutant à cette liste. Pour plus d'informations, veuillez consulter information la section Inclure et exclure des éléments.

Les chemins d'accès de cette liste doivent être relatifs au profil utilisateur. Les chemins relatifs sont interprétés comme étant relatifs au profil utilisateur. Les caractères génériques peuvent être utilisés mais sont uniquement autorisés pour les noms de fichiers. Les caractères génériques ne peuvent pas être imbriqués et sont appliqués de manière récursive.

Exemples :

- AppData\Local\Microsoft\Office\Access.qat spécifie un fichier sous un dossier exclus dans la configuration par défaut.
- AppData\Local\MyApp*.cfg spécifie tous les fichiers avec l'extension .cfg dans le dossier de profil AppData\Local\MyApp et ses sous-dossiers.

Par défaut, ce paramètre est désactivé et aucun fichier n'est spécifié.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, seuls les fichiers non exclus dans le profil utilisateur sont synchronisés.

Dossiers à mettre en miroir

Ce paramètre spécifie les dossiers relatifs au profil de l'utilisateur par rapport à un dossier racine de l'utilisateur à mettre en

© 1999-2017 Citrix Systems, Inc. All rights reserved.

miroir. La configuration de cette stratégie permet de faciliter la résolution des problèmes rencontrés avec tout dossier transactionnel (également appelé dossier référentiel), un dossier contenant des fichiers interdépendants, dans lequel un fichier fait référence aux autres.

La mise en miroir de dossiers permet à Profile Management de traiter un dossier transactionnel et son contenu en tant qu'entité unique, ce qui évite l'engorgement du profil. Dans ces cas de figure, tenez compte du fait que le modèle « Last Write Wins » s'applique, ce qui veut dire que les fichiers présents dans les dossiers mis en miroir qui ont été modifiés dans plus d'une session seront écrasés par la dernière mise à jour, ce qui se traduit par la perte des modifications apportées au profil.

Vous pouvez par exemple mettre en miroir le dossier cookies d'Internet Explorer de manière à ce que le fichier Index.dat soit synchronisé avec les cookies qu'il indexe.

Si l'utilisateur a ouvert deux sessions Internet Explorer, chacune sur un serveur différent, et qu'il visite des sites différents dans chaque session, les cookies de chaque site sont ajoutés au serveur approprié. Lorsque l'utilisateur se déconnecte de la première session (ou au milieu d'une session, si la fonctionnalité de réécriture active est configurée), les cookies de la seconde session devraient remplacer ceux de la première session. Au lieu de cela, ils sont fusionnés et les références aux cookies dans index.dat deviennent obsolètes. Lorsque l'utilisateur accède de nouveau à des sites dans les nouvelles sessions, cela entraîne davantage de fusionnements et l'engorgement du dossier de cookies.

La mise en miroir du dossier permet de résoudre ce problème en remplaçant les cookies avec ceux de la dernière session chaque fois que l'utilisateur ferme une session, ce qui fait que index.dat reste constamment à jour.

Par défaut, ce paramètre est désactivé et aucun dossier n'est mis en miroir.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si cette stratégie n'est pas configurée ici où dans le fichier .ini, aucun dossier n'est mis en miroir.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Redirection de dossiers

Jul 07, 2016

La section Redirection de dossier contient des paramètres de stratégie permettant de spécifier si vous souhaitez rediriger les dossiers qui apparaissent communément dans des profils vers un emplacement réseau partagé.

Accorder l'accès administrateur

Ce paramètre permet à un administrateur d'accéder au contenu des dossiers redirigés des utilisateurs.

Par défaut, ce paramètre est désactivé et les utilisateurs disposent d'un accès exclusif au contenu de leurs dossiers redirigés.

Inclure le nom de domaine

Ce paramètre permet d'activer l'inclusion de la variable d'environnement %userdomain% dans le chemin d'accès UNC spécifié pour la redirection de dossiers.

Par défaut, ce paramètre est désactivé et la variable d'environnement %userdomain% n'est pas incluse dans le chemin d'accès UNC spécifié pour la redirection de dossiers.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie AppData(Roaming)

Jul 07, 2016

La section AppData(Roaming) contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier AppData(Roaming) vers un emplacement réseau partagé.

Chemins d'accès au dossier AppData(Roaming)

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier AppData(Roaming) est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier AppData(Roaming)

Ce paramètre spécifie comment rediriger le contenu du dossier AppData(Roaming).

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Contacts

Jul 07, 2016

La section Contacts contient les paramètres de stratégie destinés à spécifier si vous souhaitez rediriger le contenu du dossier Contacts vers un emplacement réseau partagé.

Chemin d'accès au dossier Contacts

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Contacts est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Contacts

Ce paramètre spécifie comment rediriger le contenu du dossier Contacts.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Bureau

Jul 07, 2016

La section Bureau contient des paramètres de stratégie destinés à spécifier si vous souhaitez rediriger le contenu du dossier Bureau vers un emplacement réseau partagé.

Chemin d'accès au dossier Bureau

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Desktop est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Bureau

Ce paramètre spécifie comment rediriger le contenu du dossier Bureau.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Documents

Jul 07, 2016

La section Documents contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Documents vers un emplacement réseau partagé.

Chemin d'accès au dossier Mes documents

Ce paramètre spécifie l'emplacement réseau vers lequel les fichiers du dossier Documents sont redirigés.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Le paramètre Chemin d'accès au dossier Documents doit être activé non seulement pour rediriger les fichiers vers le dossier Documents, mais aussi pour rediriger les fichiers vers les dossiers Musique, Images et Vidéos.

Paramètres de redirection du dossier Mes documents

Ce paramètre spécifie la manière de rediriger le contenu du dossier Documents.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Pour contrôler la manière de rediriger le contenu du dossier Documents, choisissez l'une des options suivantes :

- Rediriger vers le chemin UNC suivant. Redirections de contenu pour le chemin d'accès UNC spécifié dans le paramètre de stratégie Chemin d'accès au dossier Documents.
- Rediriger vers le répertoire de base de l'utilisateur. Redirections de contenu pour le répertoire de base utilisateur, généralement configuré en tant qu'attribut #homeDirectory# pour un utilisateur dans Active Directory.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Télécharge les stratégies de groupe

Jul 07, 2016

La section Téléchargements contient les paramètres de stratégie destinés à spécifier si vous souhaitez rediriger le contenu du dossier Téléchargements vers un emplacement réseau partagé.

Chemin d'accès au dossier Téléchargements

Ce paramètre spécifie l'emplacement réseau vers lequel les fichiers du dossier Documents sont redirigés.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Téléchargements

Ce paramètre spécifie la redirection du contenu du dossier Téléchargements.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Favoris

Jul 07, 2016

La section Favoris contient des paramètres de stratégie destinés à spécifier si vous souhaitez rediriger le contenu du dossier Favoris vers un emplacement réseau partagé.

Chemin d'accès au dossier Favoris

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Favoris est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Favoris

Ce paramètre spécifie la façon de rediriger le contenu du dossier Favoris.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Liens

Jul 07, 2016

La section Liens contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Liens vers un emplacement réseau partagé.

Chemin d'accès au dossier Liens

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Liens est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Liens

Ce paramètre spécifie comment rediriger le contenu du dossier Liens.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Musique

Jul 07, 2016

La section Musique contient les paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Musique vers un emplacement réseau partagé.

Chemin d'accès au dossier Ma musique

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Musique est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Ma musique

Ce paramètre spécifie comment rediriger le contenu du dossier Musique.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Pour contrôler comment rediriger le contenu du dossier Musique, choisissez l'une des options suivantes :

- Rediriger vers le chemin UNC suivant. Permet de rediriger du contenu vers le chemin d'accès UNC spécifié dans le paramètre de stratégie Chemin d'accès au dossier Musique.
- Rediriger en fonction du dossier Documents. Permet de rediriger du contenu vers un dossier relatif au dossier Documents.

Pour rediriger du contenu vers un dossier relatif au dossier Documents, le paramètre Chemin d'accès au dossier Documents doit être activé.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Images

Jul 07, 2016

La section Images contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Images vers un emplacement réseau partagé.

Chemin d'accès au dossier Mes images

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Images est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Mes images

Ce paramètre spécifie la façon de rediriger le contenu du dossier Images.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Pour contrôler la manière dont le contenu du dossier Images est redirigé, choisissez l'une des options suivantes :

- Rediriger vers le chemin UNC suivant. Permet de rediriger du contenu vers le chemin d'accès UNC spécifié dans le paramètre de stratégie Chemin d'accès au dossier Images.
- Rediriger en fonction du dossier Documents. Permet de rediriger du contenu vers un dossier relatif au dossier Documents.

Pour rediriger du contenu vers un dossier relatif au dossier Documents, le paramètre Chemin d'accès au dossier Documents doit être activé.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Parties enregistrées

Jul 07, 2016

La section Parties enregistrées contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Parties enregistrées vers un emplacement réseau partagé.

Paramètres de redirection du dossier Parties enregistrées

Ce paramètre spécifie comment rediriger le contenu du dossier Parties enregistrées.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Chemin d'accès au dossier Parties enregistrées

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Parties enregistrées est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Recherches

Jul 07, 2016

La section Recherches contient des paramètres de stratégie destinées à spécifier si vous souhaitez rediriger le contenu du dossier Recherches vers un emplacement réseau partagé.

Paramètres de redirection du dossier Recherches

Ce paramètre spécifie comment rediriger le contenu du dossier Recherches.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Chemin d'accès au dossier Recherches

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Recherches est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Menu Démarrer

Jul 07, 2016

La section Menu Démarrer contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Menu Démarrer vers un emplacement réseau partagé.

Paramètres de redirection du menu Démarrer

Ce paramètre spécifie comment rediriger le contenu du dossier Menu Démarrer.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Chemin d'accès au menu Démarrer

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Menu Démarrer est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Vidéo

Jul 07, 2016

La section Vidéo contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Vidéo vers un emplacement réseau partagé.

Paramètres de redirection pour la vidéo

Ce paramètre spécifie comment rediriger le contenu du dossier Vidéo.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Pour contrôler comment rediriger le contenu du dossier Vidéo, choisissez l'une des options suivantes :

- Rediriger vers le chemin UNC suivant. Permet de rediriger du contenu vers le chemin d'accès UNC spécifié dans le paramètre de stratégie Chemin d'accès au dossier Vidéo.
- Rediriger en fonction du dossier Documents. Permet de rediriger du contenu vers un dossier relatif au dossier Documents.

Pour rediriger du contenu vers un dossier relatif au dossier Documents, le paramètre Chemin d'accès au dossier Documents doit être activé.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Chemin d'accès au dossier Vidéo

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Vidéo est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Journal

Jul 07, 2016

La section Journal contient des paramètres de stratégie permettant de configurer la journalisation Profile Management.

Actions Active Directory

Ce paramètre active ou désactive la journalisation détaillée des actions effectuées dans Active Directory.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Informations courantes

Ce paramètre active ou désactive la journalisation détaillée des informations courantes.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Avertissements courants

Ce paramètre active ou désactive la journalisation détaillée des avertissements courants.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Activer la journalisation

Ce paramètre active ou désactive la journalisation de Profile Management en mode (journalisation détaillée) de débogage. En mode de débogage, les informations d'état complètes sont journalisées dans les fichiers journaux situées dans "%SystemRoot%\System32\Logfiles\UserProfileManager".

Par défaut, ce paramètre est désactivé et seules les erreurs sont journalisées.

Citrix vous recommande d'activer ce paramètre uniquement si vous effectuez la résolution des problèmes de Profile Management.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, seules les erreurs sont consignées.

Actions du système de fichiers

Ce paramètre active ou désactive la journalisation détaillée des actions effectuées dans le système de fichiers.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Notifications du système de fichiers

Ce paramètre active ou désactive la journalisation détaillée des notifications des systèmes de fichiers.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Fermeture de session

Ce paramètre active ou désactive la journalisation détaillée des fermetures de session de l'utilisateur.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Ouverture de session

Ce paramètre active ou désactive la journalisation détaillée des ouvertures de session d'utilisateur.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Taille maximale du fichier journal

Ce paramètre spécifie la taille maximale autorisée pour le fichier journal de Profile Management, en octets.

Par défaut, ce paramètre est défini sur 1048576 octets (1Mo).

Citrix recommande d'augmenter la taille de ce fichier à 5 Mo ou plus, si vous disposez de suffisamment d'espace disque. Si le

© 1999-2017 Citrix Systems, Inc. All rights reserved.

fichier journal dépasse la taille maximale, le fichier de sauvegarde existant (.bak) est supprimé, le fichier journal est renommé .bak et un nouveau fichier journal est créé.

Le fichier journal est créé dans %SystemRoot%\System32\Logfiles\UserProfileManager.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, la valeur par défaut est utilisée.

Chemin d'accès au fichier journal

Ce paramètre spécifie un chemin alternatif sur lequel enregistrer le fichier journal de Profile Management.

Par défaut, ce paramètre est désactivé et les fichiers journaux sont enregistrés à l'emplacement par défaut : %SystemRoot%\System32\Logfiles\UserProfileManager.

Le chemin peut pointer vers un lecteur local ou un lecteur réseau distant (chemin d'accès UNC). Les chemins d'accès distants peuvent s'avérer utiles dans les environnements de grande taille distribués, mais ils peuvent engendrer un volume important de trafic réseau, ce qui ne convient pas aux fichiers journaux. Pour les machines virtuelles pré-configurées dotées d'un disque dur persistant, définissez un chemin d'accès local à ce lecteur. Cela garantit la préservation des fichiers journaux lorsque la machine redémarre. Pour les machines virtuelles qui ne sont pas équipées d'un disque dur persistant, la définition d'un chemin d'accès UNC vous permet de conserver les fichiers journaux mais le compte système des machines doit disposer d'un accès en écriture au partage UNC. Utilisez un chemin d'accès local pour les ordinateurs portables gérés par la fonctionnalité de profils déconnectés.

Si un chemin d'accès UNC est utilisé pour les fichiers journaux, Citrix recommande d'appliquer une liste de contrôle d'accès appropriée au dossier du fichier journal de manière à ce que seuls les comptes d'ordinateur ou d'utilisateur autorisés puissent accéder aux fichiers stockés.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, l'emplacement par défaut %SystemRoot%\System32\Logfiles\UserProfileManager est utilisé.

Informations utilisateur personnalisées

Ce paramètre active ou désactive la journalisation détaillée des informations utilisateur personnalisées.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Valeurs de stratégie à l'ouverture et fermeture de session

Ce paramètre active ou désactive la journalisation détaillée des valeurs de stratégie lorsqu'un utilisateur ouvre ou ferme une session.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Actions du registre

Ce paramètre active ou désactive la journalisation détaillée des actions effectuées dans le Registre.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Différences de registre à la fermeture de session

Ce paramètre active ou désactive la journalisation détaillée des différences dans le registre lorsqu'un utilisateur ferme sa session.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Gestion des profils

Jul 07, 2016

La section Traitement des profils contient des paramètres de stratégie qui spécifient la manière dont Profile Management gère les profils utilisateur.

Délai avant la suppression des profils du cache

Ce paramètre spécifie une extension facultative pour le délai, en minutes, avant que Profile Management supprime les profils mis en cache localement à la fermeture de session.

Une valeur de 0 supprime les profils immédiatement, à la fin du processus de fermeture de session. Profile Management vérifie les fermetures de session toutes les minutes, ainsi une valeur de 60 garantit que les profils sont supprimés entre une et deux minutes après que les utilisateurs aient fermé leur session (en fonction du moment où la dernière vérification a été effectué). L'extension du délai est utile si vous savez qu'un processus conserve les fichiers ou que la ruche du Registre de l'utilisateur est ouverte durant la fermeture de session. Avec des profils importants, cela peut également accélérer la fermeture de session.

Par défaut, cette option est définie sur 0 et Profile Management supprime les profils mis en cache localement immédiatement.

Lorsque vous activez ce paramètre, assurez-vous que l'option Supprimer les profils mis en cache localement à la fermeture de session est également activée.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les profils sont immédiatement supprimés.

Supprimer les profils mis en cache localement à la fermeture de session

Ce paramètre spécifie si les profils mis en cache localement sont supprimés après qu'un utilisateur ferme sa session.

Si ce paramètre est activé, le cache de profil local d'un utilisateur est supprimé après fermeture de leur session. Citrix vous recommande d'activer ce paramètre pour les serveurs Terminal Server.

Par défaut, ce paramètre est désactivé, le cache de profil local d'un utilisateur est conservé après la fermeture de session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les profils mis en cache ne sont pas supprimés.

Gestion des conflits de profils locaux

Ce paramètre configure le comportement de Profile Management si un profil utilisateur existe dans le magasin de l'utilisateur et en tant que profil utilisateur Windows local (pas un profil utilisateur Citrix).

Par défaut, Profile Management utilise le profil Windows local mais n'y apporte aucune modification.

Pour contrôler le comportement de Profile Management, choisissez l'une des options suivantes :

- Utiliser profil local. Profile Management utilise le profil local, mais n'y apporte aucune modification.
- Supprimer profil local. Profile Management supprime le profil utilisateur Windows local, puis importe le profil utilisateur Citrix à partir du magasin de l'utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Renommer profil local. Profile Management renomme le profil utilisateur Windows local (à des fins de sauvegarde) et importe le profil utilisateur Citrix à partir du magasin de l'utilisateur.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les profils locaux existants sont utilisés.

Migration des profils existants

Ce paramètre spécifie les types de profil migrés vers le magasin de l'utilisateur lors de l'ouverture de session si un utilisateur ne dispose d'aucun profil courant dans le magasin de l'utilisateur.

Profile Management peut effectuer la migration des profils existants « à la volée » durant l'ouverture de session si l'utilisateur ne dispose d'aucun profil dans le magasin de l'utilisateur. Une fois ce processus terminé, le profil du magasin de l'utilisateur est utilisé par Profile Management dans la session en cours et toute autre session configurée avec le chemin d'accès au même magasin de l'utilisateur.

Par défaut, les profils locaux et itinérants sont migrés vers le magasin de l'utilisateur lors de l'ouverture de session.

Pour spécifier les types de profil migrés vers le magasin de l'utilisateur lors de l'ouverture de session, choisissez l'une des options suivantes :
- Profils locaux et itinérants
- Local
- Itinérance
- Aucun (désactivé)

Si vous sélectionnez Aucun, le système utilise le mécanisme Windows existant de création de nouveaux profils, comme dans un environnement dans lequel Profile Management n'est pas installé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les profils locaux et itinérants existants sont migrés.

Chemin d'accès au profil modèle

Ce paramètre spécifie le chemin d'accès au profil que vous souhaitez que Profile Management utilise comme modèle pour la création de nouveaux profils utilisateur.

Le chemin d'accès spécifié doit être le chemin d'accès complet au dossier contenant le fichier de registre NTUSER.DAT ainsi que tout autre dossier et fichier requis pour le profil modèle.
Remarque : n'incluez pas NTUSER.DAT dans le chemin d'accès. Par exemple, avec le fichier \\nomserveur\mesprofils\modèle\ntuser.dat, définissez l'emplacement en tant que \\nomserveur\mesprofils\modèle.
Utilisez des chemins d'accès absolus. Il peut s'agir de chemins UNC où de chemins sur la machine locale. Vous pouvez utiliser ces derniers pour spécifier, par exemple, un profil modèle de manière permanente sur une image Citrix Provisioning Services. les chemins d’accès relatifs ne sont pas pris en charge.

Remarque : ce paramètre ne prend pas en charge l'expansion d'attributs Active Directory, de variables d'environnement système ou des variables %USERNAME% et %USERDOMAIN%.
Par défaut, ce paramètre est désactivé et les nouveaux profils utilisateur sont créés à partir du profil utilisateur par défaut sur la machine sur laquelle un utilisateur ouvre une session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun modèle n'est utilisé.

Le profil modèle remplace le profil local

Ce paramètre active le profil modèle pour remplacer le profil local lors de la création de nouveaux profils utilisateur.

Si un utilisateur ne dispose d'aucun profil utilisateur Citrix, mais qu'un profil utilisateur Windows local existe, le profil local est utilisé par défaut (et migré vers le magasin de l'utilisateur, si ce paramètre n'est pas désactivé). L'activation de cette stratégie permet au profil modèle de remplacer le profil local utilisé lors de la création de nouveaux profils utilisateur.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun modèle n'est utilisé.

Le profil modèle remplace le profil itinérant

Ce paramètre active le profil modèle pour remplacer un profil itinérant lors de la création de nouveaux profils utilisateur.

Si un utilisateur ne dispose d'aucun profil utilisateur Citrix, mais qu'un profil utilisateur Windows itinérant existe, le profil itinérant est utilisé par défaut (et migré vers le magasin de l'utilisateur, si ce paramètre n'est pas désactivé). L'activation de ce paramètre de stratégie permet au profil modèle de remplacer le profil itinérant utilisé lors de la création de nouveaux profils utilisateur.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun modèle n'est utilisé.

Profil modèle utilisé en tant que profil Citrix obligatoire pour toutes les ouvertures de session

Ce paramètre permet d'activer Profile Management de manière à utiliser le profil modèle comme profil par défaut pour la création de tous les nouveaux profils utilisateur.

Par défaut, ce paramètre est désactivé et les nouveaux profils utilisateur sont créés à partir du profil utilisateur par défaut sur la machine sur laquelle un utilisateur ouvre une session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun modèle n'est utilisé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Registre

Jul 07, 2016

La section Registre contient des paramètres de stratégie permettant de spécifier les clés de Registre qui sont inclues et exclues du traitement Profile Management.

Liste d'exclusion

Ce paramètre spécifie la liste des clés de registre dans la ruche HKCU exclues du traitement Profile Management lorsqu'un utilisateur ferme sa session.

Lorsque cette option est activée, des clés spécifiées dans cette liste sont exclues du traitement lorsqu'un utilisateur ferme sa session.

Par défaut, ce paramètre est désactivé, et toutes les clés de registre dans la ruche HKCU sont traitées lorsqu'un utilisateur ferme sa session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucune clé de registre n'est exclue du traitement.

Liste d'inclusion

Ce paramètre spécifie la liste des clés de registre dans la ruche HKCU inclues dans le traitement Profile Management lorsqu'un utilisateur ferme sa session.

Lorsqu'il est activé, seules les clés spécifiées dans cette liste sont traitées lorsqu'un utilisateur ferme sa session.

Par défaut, ce paramètre est désactivé, et toutes les clés de registre dans la ruche HKCU sont traitées lorsqu'un utilisateur ferme sa session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, toutes les entrées de HKCU sont traitées.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Profils utilisateur streamés

Jul 07, 2016

La section Profils utilisateur streamés contient des paramètres de stratégie spécifiant la manière dont Profile Management traite les profils utilisateur livrés en streaming.

Toujours mettre en cache

Ce paramètre spécifie si Profile Management met en cache les fichiers streamés dès que possible après qu'un utilisateur ouvre une session. La mise en cache de fichiers après qu'un utilisateur ouvre une session économise de la bande passante réseau, améliorant ainsi l'expérience utilisateur.

Utilisez ce paramètre avec le paramètre Streaming des profils.

Par défaut, ce paramètre est désactivé et les fichiers streamés ne sont pas mis en cache dès que possible après qu'un utilisateur ouvre une session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, il est désactivé.

Toujours mettre en cache la taille

Ce paramètre spécifie une limite inférieure, en méga-octets, à la taille des fichiers streamés. Profile Management met en cache les fichiers de taille égale ou supérieure dès que possible après qu'un utilisateur ouvre une session.

Par défaut, cette option est définie sur 0 (zéro) et la fonctionnalité de mise en cache du profil entier est utilisée. Lorsque la fonctionnalité de mise en cache du profil entier est activée, Profile Management récupère le contenu des profils dans le magasin de l'utilisateur, lorsqu'un utilisateur ouvre une session, en arrière-plan.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, il est désactivé.

Streaming des profils

Ce paramètre active ou désactive la fonctionnalité de profils utilisateur streamés Citrix. Lorsqu'il est activé, les fichiers et les dossiers contenus dans un profil sont récupérés depuis le magasin de l'utilisateur sur l'ordinateur local uniquement lorsque les utilisateurs y accèdent après avoir ouvert une session. Les entrées de registre et les fichiers dans la zone d'attente sont récupérés immédiatement.

Par défaut, le streaming des profils est désactivé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, il est désactivé.

Groupes des profils utilisateurs streamés

Ce paramètre spécifie les profils utilisateur qui sont livrés en streaming au sein d'une unité d'organisation, en fonction des groupes d'utilisateurs Windows.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Lorsque ce paramètre est activé, seuls les profils utilisateur dans les groupes d'utilisateurs spécifiés sont livrés en streaming. Tous les autres profils utilisateur sont traités normalement.

Par défaut, ce paramètre est désactivé et tous les profils utilisateur au sein d'une unité d'organisation sont traités normalement.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, tous les profils utilisateur sont traités.

Délai d'expiration des fichiers de verrous de la zone d'attente

Ce paramètre spécifie la période (en jours) après laquelle les fichiers des utilisateurs sont écrits dans le magasin de l'utilisateur à partir de la zone d'attente au cas où le magasin de l'utilisateur reste verrouillé lorsqu'un serveur ne répond plus. Cela évite l'engorgement dans la zone d'attente et garantit que le magasin de l'utilisateur contient toujours la dernière version des fichiers.

Par défaut, ce paramètre est défini sur 1 (un) jour.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, la valeur par défaut est utilisée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Receiver

Jul 07, 2016

Remarque : sauf spécification contraire, « Receiver » fait référence à Citrix Receiver.

La section Receiver contient des paramètres de stratégie qui spécifient une liste d'adresses StoreFront à distribuer vers Citrix Receiver pour Windows exécuté sur le bureau virtuel.

Liste de comptes StoreFront

Ce paramètre spécifie une liste d'administrateurs de magasins StoreFront qui peuvent choisir de distribuer Citrix Receiver pour Windows exécuté sur le bureau virtuel. Lors de la création d'un groupe de mise à disposition, les administrateurs peuvent sélectionner les magasins pour distribuer Citrix Receiver pour Windows exécuté sur des bureaux virtuels dans ce groupe.

Par défaut, aucun magasin n'est spécifié.

Pour chaque magasin, spécifiez les informations suivantes en tant qu'entrée séparés par des points-virgules :

- Nom du magasin. Le nom affiché pour les utilisateurs du magasin.
- Adresse URL du magasin. L'adresse URL du magasin.
- État activé du magasin. Indique si le magasin est disponible ou non pour les utilisateurs. Ceci est activé ou désactivé.
- Description du magasin. La description affichée pour les utilisateurs du magasin.

Par exemple : Magasin des ventes;https://ventes.monentreprise.com/Citrix/Magasin/découverte;Activé;Personnel des ventes du magasin

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Virtual Delivery Agent

Jul 07, 2016

La section Virtual Delivery Agent (VDA) contient des paramètres de stratégie qui contrôlent les communications entre le VDA et les contrôleurs d'un site.

Important : le VDA requiert des informations fournies par ces paramètres pour s'enregistrer auprès d'un Delivery Controller, si vous n'utilisez pas la fonctionnalité de mise à jour automatique. Comme ces informations sont requises pour l'enregistrement, vous devez configurer les paramètres suivants avec l'éditeur de stratégie de groupe, à moins que vous ne fournissiez ces informations pendant l'installation du VDA :

- Masque réseau IPv6 d'enregistrement du contrôleur
- Port d'enregistrement du contrôleur
- SID de contrôleur
- Controller
- Uniquement utiliser l'enregistrement du contrôleur IPv6
- GUID de site

Ce paramètre de stratégie permet aux administrateurs de restreindre le VDA uniquement à un sous-réseau favori (plutôt qu'une adresse IP globale, si elle est enregistrée). Ce paramètre spécifie l'adresse IPv6 et le réseau où le VDA s'enregistrera. Le VDA s'enregistre uniquement sur la première adresse qui correspond au masque de sous-réseau spécifié. Ce paramètre est uniquement valide si le paramètre de stratégie Uniquement utiliser l'enregistrement du contrôleur IPv6 est activé.

Par défaut, ce paramètre est vide.

Utilisez ce paramètre uniquement si le paramètre de stratégie Activer la mise à jour automatique des contrôleurs est désactivé.

Ce paramètre spécifie le numéro de port TCP/IP que le VDA utilise pour s'enregistrer auprès d'un Controller, en cas d'utilisation de l'enregistrement basé sur le registre.

Le numéro port est défini par défaut sur 80.

Utilisez ce paramètre uniquement si le paramètre de stratégie Activer la mise à jour automatique des contrôleurs est désactivé.

Ce paramètre spécifie une liste d'identificateurs de sécurité (SID) de Controller séparés par des espaces que le VDA utilise pour s'enregistrer auprès d'un Controller, en cas d'utilisation de l'enregistrement basé sur le registre. Il s'agit d'un paramètre facultatif, qui peut être utilisé avec le paramètre Contrôleurs pour limiter la liste des contrôleurs utilisés pour l'enregistrement.

Par défaut, ce paramètre est vide.

Utilisez ce paramètre uniquement si le paramètre de stratégie Activer la mise à jour automatique des contrôleurs est

© 1999-2017 Citrix Systems, Inc. All rights reserved.

désactivé.

Ce paramètre spécifie une liste de noms de domaines complets (FQDN) de contrôleurs séparés par des espaces que le VDA utilise pour s'enregistrer auprès d'un Controller, en cas d'utilisation de l'enregistrement basé sur le registre. Il s'agit d'un paramètre facultatif, qui peut être utilisé avec le paramètre SID de Controller.

Par défaut, ce paramètre est vide.

Ce paramètre permet d'activer le VDA pour s'enregistrer auprès d'un Controller automatiquement après l'installation.

Après l'enregistrement du VDA, le Controller auquel il s'enregistre envoie une liste des domaines complets (FQDN) et le SID de ce contrôleur au VDA Le VDA inscrit cette liste dans le stockage permanent. Chaque Controller vérifie également la base de données du site toutes les 90 minutes pour des informations sur le Controller ; si un Controller a été ajouté ou supprimé depuis la dernière vérification ou, si une modification de stratégie s'est produite, le Controller envoie les listes mises à jour vers les VDA enregistrés. Le VDA acceptera les connexions provenant de tous les Controller figurant dans la dernière liste reçue.

Ce paramètre est activé par défaut.

Ce paramètre détermine le format d'adresse utilisé par le VDA pour s'enregistrer avec le Controller :

- lorsque cette option est activée, le VDA s'enregistre auprès du Controller à l'aide de l'adresse IPv6 de la machine. Lorsque le VDA communique avec le Controller, il utilise l'ordre d'adresse suivant : adresse IP globale, adresse locale unique (ULA), adresse locale au lien (si aucune autre adresse IPv6 n'est disponible).
- Lorsque cette stratégie est désactivée, le VDA s'enregistre et communique avec le Controller à l'aide de l'adresse IPv4 de la machine.

Par défaut, ce paramètre est désactivé.

Utilisez ce paramètre uniquement si le paramètre de stratégie Activer la mise à jour automatique des contrôleurs est désactivé.

Ce paramètre spécifie le GUID (Globally Unique Identifier) du site que le VDA utilise pour s'enregistrer auprès d'un Controller en cas d'utilisation de l'enregistrement à partir d'Active Directory.

Par défaut, ce paramètre est vide.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie HDX 3D Pro

Jul 07, 2016

La section HDX 3D Pro contient des paramètres de stratégie permettant d'activer et de configurer l'outil de configuration de la qualité d'image pour vos utilisateurs. Cet outil permet aux utilisateurs d'optimiser l'utilisation de la bande passante disponible en ajustant en temps réel l'équilibre entre la qualité d'image et le temps de réponse.

Ce paramètre détermine si les utilisateurs peuvent ou non activer ou désactiver la compression sans perte à l'aide de l'outil de configuration de la qualité d'image. Par défaut, les utilisateurs n'ont pas la possibilité d'activer la compression sans perte.

Lorsqu'un utilisateur active la compression sans perte, la qualité d'image est automatiquement définie sur la valeur maximale disponible dans l'outil de configuration de la qualité d'image. Par défaut, il est possible d'utiliser la compression basée sur le processeur graphique ou sur l'UC, en fonction des possibilités de la machine utilisateur et de l'ordinateur hôte.

Ce paramètre spécifie les valeurs maximale et minimale qui déterminent la plage de réglages de la qualité d'image accessible aux utilisateurs dans l'outil de configuration de la qualité d'image.

Indiquez des valeurs de qualité entre 0 et 100 (inclus). La valeur maximale doit être supérieure ou égale à la valeur minimale.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie Adresse IP virtuelle

Jul 07, 2016

La section Adresse IP virtuelle contient des paramètres de stratégie permettant de contrôler si les sessions ont leur propre adresse virtuelle de bouclage.

Lorsque ce paramètre est activé, chaque session possède sa propre adresse virtuelle de bouclage. Lorsqu'il est désactivé, les sessions n'ont pas d'adresses de bouclage individuelles.

Par défaut, ce paramètre est désactivé.

Ce paramètre spécifie les exécutables d'application susceptibles d'utiliser les adresses de bouclage virtuelles. Lorsque vous ajoutez des programmes à la liste, spécifiez uniquement le nom de l'exécutable, vous ne devez pas spécifier le chemin d'accès complet.

Par défaut, aucun exécutable n'est spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre

Jul 07, 2016

Dans les versions VDA 7.0 à 7.8, les paramètres du port COM et LPT sont uniquement configurables à l'aide du Registre. Pour les versions VDA antérieures à la version 7.0 et le VDA version 7.9, ces paramètres sont configurables dans Studio. Pour de plus amples informations, consultez la section Paramètres de stratégie de redirection de port et Paramètres de stratégie de bande passante.

Les paramètres de stratégie pour la redirection du port COM et du port LPT sont situés sous HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated sur l'image ou la machine VDA.

Pour activer la redirection des ports COM et LPT, ajoutez de nouvelles clés de Registre de type REG_DWORD, comme suit : Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

Clé de Registre	Description	Valeurs autorisées
AllowComPortRedirection	Autoriser ou interdire la redirection de port COM	1 (Autoriser) ou 0 (Interdire)
LimitComBw	Limite de bande passante pour le canal de redirection du port COM	Valeur numérique
LimitComBWPercent	Limite de bande passante pour le canal de redirection du port COM sous forme de pourcentage de la bande passante totale de session	Valeur numérique comprise entre 0 et 100
AutoConnectClientComPorts	Connecter automatiquement les ports COM de la machine utilisateur	1 (Autoriser) ou 0 (Interdire)
AllowLptPortRedirection	Autoriser ou interdire la redirection de port LPT	1 (Autoriser) ou 0 (Interdire)
LimitLptBw	Limite de bande passante pour le canal de redirection du port LPT	Valeur numérique
LimitLptBwPercent	Limite de bande passante pour le canal de redirection du port LPT sous forme de pourcentage de la bande passante totale de session	Valeur numérique comprise entre 0 et 100
AutoConnectClientLptPorts	Connecter automatiquement les ports LPT de la machine utilisateur	1 (Autoriser) ou 0 (Interdire)

Après la configuration de ces paramètres, modifiez les catalogues de machines pour utiliser la nouvelle image principale ou la

© 1999-2017 Citrix Systems, Inc. All rights reserved.

machine physique mise à jour. Les bureaux sont mis à jour avec les nouveaux paramètres lors de la fermeture de session suivante.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres de stratégie de Connector pour Configuration Manager 2012

Jul 07, 2016

La section Connector pour Configuration Manager 2012 contient des paramètres de stratégie pour la configuration de l'agent Citrix Connector 7.5.

Important : les stratégies d'avertissement, de fermeture de session et de message de redémarrage s'appliquent uniquement aux déploiements de catalogues de machines avec OS de serveur qui sont gérés manuellement ou par Provisioning Services Pour ces catalogues de machines, le service Connector alerte les utilisateurs lorsqu'ils sont en attente d'une installation d'application ou de mises à jour logicielles.
Pour les catalogues gérés par MCS, utilisez Studio pour avertir les utilisateurs. Pour gérer des catalogues avec OS de bureau manuellement, utilisez le gestionnaire de configuration pour avertir les utilisateurs. Pour des catalogues avec OS de bureau gérés par Provisioning Services, utilisez Provisioning Services pour avertir les utilisateurs.

Ce paramètre définit l'intervalle entre les apparitions du message d'avertissement avancé auprès des utilisateurs.

Les intervalles sont définis selon le format jjj.hh:mm:ss, où :
- jjj représente les jours, un paramètre facultatif, avec une plage de 0 à 999.
- hh représente les heure avec une plage de 0 à 23.
- mm représente les minutes avec une plage de 0 à 59.
- ss représente les secondes avec une plage de 0 à 59.

Par défaut, le paramètre d'intervalle est de 1 heure (01:00:00).

Ce paramètre contient le texte modifiable du message qui s'affiche aux utilisateurs pour les notifier de mises à jour logicielles ou de tâches de maintenance à venir nécessitant qu'ils ferment leur session.

Par défaut, le message est : {TIMESTAMP} Please save your work. Le serveur sera placé en mode déconnecté à des fins de maintenance dans {TIMELEFT}.

Ce paramètre contient le texte modifiable de la barre de titre du message d'avertissement avancé pour les utilisateurs.

Par défaut, le titre est Upcoming Maintenance.

Ce paramètre définit combien de temps avant la maintenance où le premier message d'avertissement avancé s'affiche.

Le temps est défini selon le format jjj.hh:mm:ss, où :
- jjj représente les jours, un paramètre facultatif, avec une plage de 0 à 999.
- hh représente les heure avec une plage de 0 à 23.
- mm représente les minutes avec une plage de 0 à 59.
- ss représente les secondes avec une plage de 0 à 59.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Par défaut, le paramètre est de 16 heures (16:00:00), ce qui indique que le premier message d'avertissement avancé s'affiche approximativement 16 heures avant la maintenance.

Ce paramètre contient le texte modifiable du message alertant les utilisateurs qu'une ouverture de session forcée a commencé.

Par défaut, le message est : The server is currently going offline for maintenance (Le serveur est actuellement en mode déconnecté pour maintenance).

Ce paramètre contient le texte modifiable de la barre de titre du message final de fermeture de session forcée.

Par défaut, le titre est : Notification From IT Staff (Notification du personnel informatique).

Ce paramètre définit la période de temps entre la notification de fermer leur session aux utilisateurs et l'implémentation de la fermeture de session forcée pour traiter la maintenance en attente.

Le temps est défini selon le format jjj.hh:mm:ss, où :
- jjj représente les jours, un paramètre facultatif, avec une plage de 0 à 999.
- hh représente les heure avec une plage de 0 à 23.
- mm représente les minutes avec une plage de 0 à 59.
- ss représente les secondes avec une plage de 0 à 59.

Par défaut, le paramètre force logoff grace period est de 5 minutes (00:05:00).

Ce paramètre contient le texte modifiable du message demandant aux utilisateurs d'enregistrer leur travail et de fermer leur session avant le début d'une fermeture de session forcée.

Par défaut, le message contient ce qui suit : {TIMESTAMP}Please save your work and log off (Veuillez enregistrer votre travail et fermer votre session). Le serveur sera placé en mode déconnecté à des fins de maintenance dans {TIMELEFT}.

Ce paramètre contient le texte modifiable de la barre de titre du message de fermeture de session forcée.

Par défaut, le titre est : Notification From IT Staff (Notification du personnel informatique).

L'agent Connector détecte automatiquement s'il est en cours d'exécution sur une machine clone gérée par Provisioning Services ou MCS. L'agent bloque de l'agent les mises à jour Configuration Manager sur les clones dont l'image est gérée et installe automatiquement les mises à jour sur l'image principale du catalogue.

Après mise à jour d'une image principale, utilisez Studio pour orchestrer le redémarrage des clones de catalogue MCS. L'Agent du Connector orchestre automatiquement le redémarrage des clones du catalogue PVS lors des fenêtres de maintenance Configuration Manager. Pour remplacer ce comportement afin que le logiciel soit installé sur des clones de catalogue par Configuration Manager, changez le mode Image gérée en Désactivé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ce paramètre contient le texte modifiable du message notifiant les utilisateurs lorsque le serveur est sur le point d'être redémarré.

Par défaut, le message est : The server is currently going offline for maintenance (Le serveur est actuellement en mode déconnecté pour maintenance).

Ce paramètre détermine la fréquence d'exécution de la tâche d'agent Citrix Connector.

Le temps est défini selon le format jjj.hh:mm:ss, où :

- jjj représente les jours, un paramètre facultatif, avec une plage de 0 à 999.
- hh représente les heure avec une plage de 0 à 23.
- mm représente les minutes avec une plage de 0 à 59.
- ss représente les secondes avec une plage de 0 à 59.

Par défaut, le paramètre d'intervalle de temps régulier est de 5 minutes (00:05:00).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Gérer

Jul 07, 2016

La gestion d'un site XenApp ou XenDesktop couvre un grand nombre d'éléments et de tâches.

Système de licences

Une connexion valide avec le serveur de licences Citrix est requise lorsque vous créez un site. Plus tard, vous pourrez effectuer plusieurs opérations de gestion de licences à partir de Studio, y compris l'ajout de licences, la modification des types ou modèles de licences et la gestion des administrateurs de licences. Vous pourrez également accéder à la console License Administration Console à partir de Studio.

Applications

Permet de gérer les applications dans les groupes de mise à disposition et éventuellement, les groupes d'applications.

Zones

Dans un déploiement réparti sur différents sites géographiques, vous pouvez utiliser des zones pour que les applications et les bureaux se trouvent à proximité des utilisateurs finaux, ce qui peut améliorer les performances. Lorsque vous installez et configurez un site, tous les Controller, les catalogues de machines et les connexions hôtes se trouvent dans une zone principale. Plus tard, vous pourrez utiliser Studio pour créer des zones satellite contenant ces éléments. Une fois que votre site comporte plusieurs zones, vous pouvez indiquer dans quelle zone les catalogues de machines et les connexions hôtes créés ou les Controller ajoutés doivent être placés. Vous pouvez aussi déplacer les éléments entre les zones.

Connexions et ressources

Si vous utilisez un hyperviseur ou un service de cloud pour héberger les machines qui mettront à disposition les applications et les bureaux auprès des utilisateurs, vous devez créer votre première connexion à l'hyperviseur ou au service de cloud lorsque vous créez un site. Les détails de stockage et de réseau pour cette connexion forment ses *ressources*. Plus tard, vous pourrez modifier la connexion et ses ressources, et créer de nouvelles connexions. Vous pourrez également gérer les machines qui utilisent une connexion configurée.

Location de connexions

La fonctionnalité de location de connexions complète les meilleures pratiques de la haute disponibilité du serveur SQL Server en permettant aux utilisateurs de se connecter et de se reconnecter à leurs applications et bureaux les plus récemment utilisés, même lorsque la base de données du site n'est pas disponible. Si la location de connexions peut améliorer la résilience de connexion et la productivité des utilisateurs, cet article traite des considérations relatives à la disponibilité, au fonctionnement et aux performances d'autres fonctionnalités lorsqu'un Controller est en mode de location de connexions.

Adresses IP virtuelles et bouclage virtuel

La fonctionnalité d'adresse IP virtuelle Microsoft fournit une application publiée avec une adresse IP unique attribuée dynamiquement à chaque session. La fonctionnalité de bouclage virtuel Citrix vous permet également de configurer des applications qui dépendent des communications avec localhost (127.0.0.1 par défaut) pour utiliser une adresse de bouclage virtuel unique dans la plage localhost (127.*).

Delivery Controller

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Avant qu'un VDA puisse effectuer la mise à disposition d'applications et de bureaux, il doit s'enregistrer (établir la communication) auprès d'un Controller. Les adresses des Controller peuvent être spécifiées lorsque vous installez le VDA, dans les paramètres de stratégie Citrix, les paramètres de registre et de plusieurs autres manières. Il est d'une importance critique que les VDA obtiennent des informations actualisées au fur et à mesure que des Controller sont ajoutés, déplacés et supprimés sur le site. Cet article explique comment et quand les VDA peuvent s'enregistrer, les méthodes de mise à jour des informations sur le Controller et comment ajouter, supprimer et déplacer des Controller.

Sessions

La gestion de l'activité de session est critique pour offrir la meilleure expérience utilisateur possible. Plusieurs fonctionnalités peuvent optimiser la fiabilité des sessions, réduire les désagréments, les temps d'arrêt et la perte de productivité.

- Fiabilité de session
- Reconnexion automatique des clients
- Persistance ICA
- Le contrôle de l'espace de travail
- Itinérance de session

Utilisation de la fonction de recherche dans Studio

Lorsque vous souhaitez afficher des informations sur les machines, sessions, catalogues de machines, applications ou groupes de mise à disposition dans Studio, vous pouvez utiliser la fonctionnalité de recherche flexible.

Balises

Utilisez des balises pour identifier des éléments tels que des machines, applications, groupes et stratégies. Vous pouvez ensuite configurer certaines opérations pour qu'elles s'appliquent aux éléments avec une balise spécifique.

IPv4/ipv6

Cette version de XenApp and XenDesktop prend en charge les déploiements IPv4 purs, IPv6 purs et double pile qui utilisent des réseaux IPv4 et IPv6 qui se chevauchent. Cet article explique et illustre ces déploiements. Il décrit également les paramètres de stratégie Citrix qui déterminent l'utilisation de IPv4 ou IPv6.

Redirection de dossiers clients

La redirection de dossiers clients modifie la manière dont les fichiers côté client sont accessibles sur la session côté hôte. Lorsque vous activez uniquement le mappage de lecteur client sur le serveur, les volumes complets côté client sont automatiquement mappés sur les sessions en tant que liens UNC (Universal Naming Convention). Lorsque vous activez la redirection de dossiers clients sur le serveur et que l'utilisateur la configure sur la machine de bureau Windows, la partie du volume local spécifié par l'utilisateur est redirigée.

Profils utilisateur

Par défaut, Citrix Profile Management est installé automatiquement lorsque vous installez un VDA. Si vous utilisez cette solution de gestion des profils, consultez cet article pour des informations générales et reportez-vous à la documentation relative à Profile Management pour plus de détails.

Citrix Insight Services

Citrix Insight Services (CIS) est la plate-forme Citrix depuis laquelle vous pouvez générer des informations d'instrumentation, de télémétrie et autres données stratégiques.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Système de licences

Jul 07, 2016

Vous pouvez utiliser Studio pour gérer et suivre les licences, à condition que le serveur de licences se trouve dans le même domaine que Studio, ou dans un domaine approuvé. Pour de plus amples informations sur les autres tâches liées aux licences, consultez la documentation relative au système de licences.

Vous devez être un administrateur de licence complet pour effectuer les tâches décrites ci-dessous, à l'exception de l'affichage des informations de licence. Pour afficher les informations de licence dans Studio, un administrateur doit avoir au moins l'autorisation d'administration déléguée de licence en lecture ; l'Administrateur complet intégré et des rôles d'administrateur en lecture seule ont cette autorisation.

Le tableau suivant dresse la liste des versions prises en charge et les modèles de licences :

Produits	Éditions	Modèles de licence
XenApp	• Platinum • Enterprise • Advanced	Simultanée
XenDesktop	• Platinum • Enterprise • App • VDI	• Utilisateur/Machine • Simultanée

Pour afficher les informations de licence, sélectionnez **Configuration > Licences** dans le panneau de navigation de Studio. Un récapitulatif de l'utilisation des licences et des paramètres du site est affiché, ainsi qu'une liste de toutes les licences actuellement installées sur le serveur de licences spécifié.

Pour télécharger une licence Citrix :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Sélectionnez **Allouer des licences** dans le volet Actions.
3. Entrez le code d'accès aux licences que Citrix vous a envoyé par e-mail.
4. Sélectionnez un produit et cliquez sur **Allouer des licences**. Toutes les licences disponibles pour ce produit sont allouées et téléchargées. Veuillez noter qu'après avoir alloué et téléchargé toutes les licences pour un code d'accès aux licences spécifique, vous ne pouvez plus utiliser ce code. Si vous devez effectuer d'autres transactions avec ce code, ouvrez une session sur My Account.

Pour ajouter des licences qui sont stockées sur votre ordinateur local ou sur le réseau :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Sélectionnez **Ajouter des licences** dans le volet Actions.
3. Accédez à un fichier de licences et ajoutez-le au serveur de licences.

Pour changer de serveur de licences

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Sélectionnez **Changer le serveur de licences** dans le volet Actions.
3. Tapez l'adresse du serveur de licences sous la forme nom:port, où nom est une adresse DNS, NetBIOS ou IP. Si vous n'indiquez pas de numéro de port, le port par défaut (27000) est utilisé.

Pour sélectionner le type de licence à utiliser :

- Lors de la configuration du site, après avoir spécifié le serveur de licences, vous êtes invité à sélectionner le type de licence à utiliser. S'il n'y a aucune licence sur le serveur, l'option d'utilisation du produit pour une période d'évaluation de 30 jours est automatiquement sélectionnée.
- Si le serveur comporte des licences, leurs détails sont affichés et vous pouvez sélectionner l'une d'elles. Vous pouvez également ajouter un fichier de licences au serveur et le sélectionner.

Pour changer l'édition du produit et le modèle de licence :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Sélectionnez **Modifier l'édition du produit** dans le volet Actions.
3. Mettez à jour les options appropriées.

Pour accéder à la console License Administration Console, dans le volet Actions, sélectionnez **License Administration Console**. La console soit apparaît immédiatement soit, si le tableau de bord est configuré comme protégé par un mot de passe, vous êtes invité à entrer les informations d'identification de la console License Administration Console. Pour plus de détails sur l'utilisation de la console, veuillez consulter la documentation concernant les licences.

Pour ajouter un administrateur de licences :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Sélectionnez l'onglet Administrateurs de licences dans le panneau central.
3. Sélectionnez **Ajouter un administrateur de licences** dans le volet Actions.
4. Recherchez le nom de l'utilisateur que vous souhaitez ajouter en tant qu'administrateur et choisissez les autorisations.

Pour modifier les autorisations d'un administrateur de licences ou supprimer un administrateur de licences :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Sélectionnez l'onglet Administrateurs de licences dans le panneau central, puis sélectionnez l'administrateur.
3. Sélectionnez **Modifier l'administrateur de licences** ou **Supprimer l'administrateur de licences** dans le volet Actions.

Pour ajouter un groupe d'administrateurs de licences :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Sélectionnez l'onglet Administrateurs de licences dans le panneau central.
3. Sélectionnez **Ajouter un groupe d'administrateurs de licences** dans le volet Actions.
4. Recherchez le groupe que vous souhaitez voir opérer en tant qu'administrateur de licences et choisissez les autorisations. L'ajout d'un groupe Active Directory donne à l'administrateur de licences des autorisations d'accès aux utilisateurs dans ce groupe.

Pour modifier les autorisations d'un groupe d'administrateurs de licences ou supprimer un groupe d'administrateurs de licences :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Sélectionnez l'onglet Administrateurs de licences dans le panneau central, puis sélectionnez le groupe d'administrateurs.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Sélectionnez **Modifier le groupe d'administrateurs de licences** ou **Supprimer le groupe d'administrateurs de licences** dans le volet Actions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Applications

Jul 07, 2016

Introduction

Si votre déploiement utilise uniquement des groupes de mise à disposition (et aucun groupe d'applications), vous devez ajouter des applications aux groupes de mise à disposition. Si vous disposez également de groupes d'application, vous devez, en règle générale, ajouter des applications aux groupes d'applications. Ces recommandations permettent de faciliter l'administration. Une application doit toujours appartenir à au moins un groupe de mise à disposition ou groupe d'applications.

Dans l'assistant Ajouter des applications, vous pouvez sélectionner un ou plusieurs groupes de mise à disposition, ou un ou plusieurs groupes d'applications, mais pas les deux. Bien que vous puissiez par la suite modifier l'association à un groupe d'applications (par exemple, transférer une application d'un groupe d'applications sur un groupe de mise à disposition), cela n'est pas recommandé pour des raisons de complexité. Gardez vos applications dans un type de groupe.

Lorsque vous associez une application à plusieurs groupes de mise à disposition ou groupes d'applications, vous risquez de rencontrer un problème de visibilité si vous ne disposez pas d'autorisations suffisantes pour afficher l'application dans tous ces groupes. Dans de tels cas, consultez un administrateur disposant des autorisations appropriées ou demandez une extension de vos autorisations à tous les groupes auxquels l'application est associée.

Si vous publiez deux applications du même nom (provenant de groupes différents) vers les mêmes utilisateurs, modifiez la propriété Nom de l'application (pour l'utilisateur) dans Studio ; sinon, les utilisateurs verront des noms en double s'afficher dans Citrix Receiver.

Vous pouvez modifier les propriétés d'une application (paramètres) lorsque vous l'ajoutez ou ultérieurement. Vous pouvez également modifier le dossier dans lequel l'application est placée, lorsque vous ajoutez l'application, ou ultérieurement.

Pour de plus amples informations sur :

- les groupes de mise à disposition, consultez l'article Créer des groupes de mise à disposition.
- les groupes d'applications, consultez l'article Créer des groupes d'applications.
- les balises, que vous pouvez ajouter aux applications, consultez l'article Balises.

Ajouter des applications

Vous pouvez ajouter des applications lorsque vous créez un groupe de mise à disposition ou un groupe d'applications ; ces procédures sont détaillées dans les articles Créer des groupes de mise à disposition et Créer des groupes d'applications. La procédure suivante explique comment ajouter des applications après la création d'un groupe.

À savoir :

- vous ne pouvez pas ajouter d'applications aux groupes de mise à disposition Remote PC Access.
- Vous ne pouvez pas utiliser l'assistant Ajouter une application pour supprimer des applications de groupes de mise à disposition ou de groupes d'applications. Il s'agit d'une opération distincte.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une ou plusieurs applications :

1. Sélectionnez **Applications** dans le panneau de navigation Studio, puis sélectionnez **Ajouter des applications** dans le volet Actions.
2. L'assistant Ajouter des applications démarre sur une page **Introduction**, que vous pouvez supprimer des futurs démarrages de cet assistant.
3. L'assistant vous guide à travers les pages Groupes, Applications, et Résumé décrites ci-dessous. Lorsque vous avez terminé chaque page, cliquez sur **Suivant** jusqu'à la page de résumé.

Alternatives à l'étape 1 si vous souhaitez ajouter des applications à un seul groupe de mise à disposition ou groupe d'applications :

- Pour ajouter des applications à un seul groupe de mise à disposition, dans l'étape 1, sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio, puis sélectionnez un groupe de mise à disposition dans le volet central, puis sélectionnez **Ajouter des applications** dans le volet Actions. L'assistant n'affichera pas la page **Groupes**.
- Pour ajouter des applications à un seul groupe d'applications, dans l'étape 1, sélectionnez **Applications** dans le volet de navigation de Studio, puis sélectionnez un **groupe d'applications** dans le volet central, puis sélectionnez **Ajouter des applications** dans le volet Actions. L'assistant n'affichera pas la page **Groupes**.

Cette page dresse la liste de tous les groupes de mise à disposition dans le site. Si vous avez également créé des groupes d'applications, la page dresse la liste des groupes d'applications et des groupes de mise à disposition. Vous pouvez choisir dans l'un ou l'autre des groupes, mais pas dans les deux groupes. En d'autres termes, vous ne pouvez pas ajouter d'applications à un groupe d'applications et à un groupe de mise à disposition. En général, si vous utilisez des groupes d'application, les applications doivent être ajoutées à des groupes d'applications plutôt qu'à des groupes de mise à disposition.

Lorsque vous ajoutez une application, vous devez sélectionner la case à cocher en regard d'au moins un groupe de mise à disposition (ou groupe d'applications, le cas échéant), car chaque application doit toujours être associée à au moins un groupe.

Cliquez sur la liste déroulante **Ajouter** pour afficher les sources des applications.

Source	Description
Depuis le menu Démarrer	Applications qui sont découvertes sur une machine dans les groupes de mise à disposition sélectionnés. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des applications découvertes. Sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**. Cette source ne peut pas être sélectionnée si vous avez (1) sélectionné des groupes d'applications qui ne sont associés à aucun groupe de mise à disposition, (2) sélectionné des groupes d'applications avec des groupes de mise à disposition associés qui ne contiennent aucune machine, ou (3) sélectionné un groupe de mise à disposition ne contenant aucune machine.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Manuellement définies	Applications qui se trouvent dans le site ou ailleurs dans votre réseau. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez taper le chemin d'accès de l'exécutable, le répertoire de travail, les arguments de la ligne de commande (facultatifs), et les noms affichés des administrateurs et des utilisateurs. Après avoir entré ces informations, cliquez sur **OK**.
Machines existantes	Applications déjà ajoutées au site. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des applications découvertes. Sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**. Cette source ne peut pas être sélectionnée si le site ne dispose d'aucune application.
App-V	Applications dans des packages App-V. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez sélectionner le serveur App-V ou la bibliothèque d'applications. À partir de l'écran qui s'affiche, sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**. Pour plus d'informations, veuillez consulter l'article App-V. Cette source ne peut pas être sélectionnée lorsque App-V n'est pas configuré pour le site.
Groupe d'applications	Groupes d'applications. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des groupes d'applications. (Bien que l'affichage dresse également la liste des applications de chaque groupe, vous ne pouvez sélectionner que le groupe, et non pas des applications individuelles.) Toutes les applications actuelles et futures dans les groupes sélectionnés seront ajoutées. Sélectionnez les cases à cocher des groupes d'applications à ajouter, puis cliquez sur **OK**. Cette source ne peut pas être sélectionnée s'il (1) n'existe aucun groupe d'applications, ou (2) si les groupes de mise à disposition sélectionnés ne prennent pas en charge les groupes d'applications (par exemple, les groupes de mise à disposition avec des machines attribuées de manière statique).

Comme indiqué dans le tableau, certaines sources dans la liste déroulante Ajouter ne peuvent pas être sélectionnées s'il n'existe source valide de ce type. Les sources qui ne sont pas compatibles (par exemple, vous ne pouvez pas ajouter des groupes d'applications à des groupes d'applications) ne sont pas incluses dans la liste déroulante. Les applications qui ont déjà été ajoutées aux groupes que vous avez choisis ne peuvent pas être sélectionnées.

Vous pouvez modifier les propriétés d'une application (paramètres) sur cette page ou ultérieurement.

Par défaut, les applications que vous ajoutez sont placées dans le dossier appelé Applications. Vous pouvez modifier l'application sur cette page ou ultérieurement. Si vous essayez d'ajouter une application et qu'une application avec le même nom existe déjà dans le même dossier, vous êtes invité à renommer l'application que vous ajoutez. Vous pouvez accepter le nouveau nom proposé ou refuser et renommer l'application, ou sélectionner un autre dossier. Par exemple, si « application » existe déjà dans le dossier Applications, et que vous essayez d'ajouter une autre application appelée « application » à ce

© 1999-2017 Citrix Systems, Inc. All rights reserved.

dossier, le nouveau nom proposé sera « application_1 ».

Si vous ajoutez 10 applications ou moins, leurs noms sont répertoriés dans **Applications à ajouter**. Si vous ajoutez plus de 10 applications, le nombre total est spécifié.

Consultez les informations récapitulatives, puis cliquez sur **Terminer**.

Modifier l'association d'un groupe d'applications

Après l'ajout d'une application, vous pouvez modifier les groupes de mise à disposition et groupes d'applications auxquels l'application est associée.

Vous pouvez utiliser le glisser-déplacer pour associer une application à un autre groupe. Ceci est une alternative à l'utilisation des commandes dans le volet Actions.

Si une application est associée à plus d'un groupe de mise à disposition ou plus d'un groupe d'applications, la priorité attribuée au groupe est utilisée pour spécifier l'ordre dans lequel plusieurs groupes sont vérifiés afin de trouver des applications. Par défaut, tous les groupes ont la priorité 0 (priorité la plus élevée). La charge des groupes ayant le même niveau de priorité est équilibrée.

Une application peut être associée à des groupes de mise à disposition contenant des machines partagées (non privées) qui peuvent mettre à disposition des applications. Vous pouvez également sélectionner des groupes de mise à disposition contenant des machines partagées qui mettent uniquement à disposition des bureaux, si (1) le groupe de mise à disposition contient des machines partagées et a été créé avec une version antérieure de XenDesktop 7.x, et (2) vous disposez de l'autorisation Modifier le groupe de mise à disposition. Le type de groupe de mise à disposition est automatiquement converti en « bureaux et applications » lorsque la boîte de dialogue des propriétés est validée.

1. Sélectionnez **Applications** dans le volet de navigation de Studio, puis sélectionnez l'application dans le panneau central.
2. Sélectionnez **Propriétés** dans le volet Actions.
3. Sélectionnez la page **Groupes**.
4. Pour ajouter un groupe, cliquez sur la liste déroulante **Ajouter** et sélectionnez **Groupes d'applications** ou **Groupes de mise à disposition**. (Si vous n'avez pas créé de groupes d'applications, la seule entrée sera Groupes de mise à disposition). Puis sélectionnez un ou plusieurs groupes disponibles. Les groupes qui ne sont pas compatibles avec l'application, ou qui sont déjà associés à l'application ne peuvent pas être sélectionnés.
5. Pour supprimer un groupe, sélectionnez un ou plusieurs groupes et cliquez sur **Supprimer**. Si la suppression de l'association de groupe a pour conséquence que l'application n'est plus être associée à un groupe d'applications ou groupe de mise à disposition, vous serez averti que l'application va être supprimée.
6. Pour modifier la priorité d'un groupe, sélectionnez le groupe, puis cliquez sur **Modifier la priorité**. Sélectionnez une valeur de priorité puis cliquez sur **OK**.
7. Lorsque vous avez terminé, cliquez sur **Appliquer** pour appliquer la modification et quitter la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Dupliquer, activer/désactiver, renommer ou supprimer une application

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Utilisation de ces actions :

- **Dupliquer** : il se peut que vous souhaitiez dupliquer une application pour créer une version différente avec des propriétés ou paramètres différents. Lorsque vous dupliquez une application, elle est automatiquement renommée avec un suffixe unique et placée de manière adjacente à l'original. Vous pouvez également vouloir dupliquer une application et l'ajouter à un autre groupe. (Après la duplication, la manière la plus facile de déplacer une application est de la glisser-déposer.)
- **Activer ou désactiver** : activer/désactiver une application ne signifie pas activer/désactiver un groupe de mise à disposition ou groupe d'applications.
- **Renommer** : vous ne pouvez renommer qu'une seule application à la fois. Si vous essayez de renommer une application et qu'une application avec le même nom existe déjà dans le même dossier ou groupe, vous êtes invité à spécifier un nom différent.
- **Supprimer** : la suppression d'une application supprime cette dernière des groupes de mise à disposition et groupes d'applications avec lesquels elle a été associée, mais pas de la source qui a été utilisée pour ajouter l'application à l'origine. Supprimer une application ne signifie pas supprimer une application d'un groupe de mise à disposition ou groupe d'applications.

Pour dupliquer, activer/désactiver, renommer ou supprimer une application :

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez une ou plusieurs applications dans le panneau du milieu, puis sélectionnez la tâche appropriée dans le volet Actions.
3. Confirmez l'action lorsque vous y êtes invité.

Supprimer des applications d'un groupe de mise à disposition

Une application doit être associée (appartenir) à au moins un groupe de mise à disposition ou groupe d'applications. Si vous tentez de supprimer une application d'un groupe de mise à disposition qui supprimerait l'association de cette application avec un groupe de mise à disposition ou groupe d'applications, vous êtes averti que l'application va être supprimée si vous continuez. Lorsque cela se produit, si vous souhaitez mettre à disposition cette application, vous devez l'ajouter à nouveau à partir d'une source valide.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe de mise à disposition. Dans le panneau inférieur central, sélectionnez l'onglet **Applications**, puis sélectionnez l'application que vous souhaitez supprimer.
3. Sélectionnez **Supprimer l'application** dans le panneau Actions.
4. Confirmez la suppression.

Supprimer des applications d'un groupe d'applications

Une application doit appartenir à au moins un groupe de mise à disposition ou groupe d'applications. Si vous tentez de supprimer une application d'un groupe d'applications qui aurait pour conséquence que cette application n'appartiendrait plus à aucun groupe de mise à disposition ou groupe d'applications, vous êtes averti que l'application va être supprimée si vous continuez. Lorsque cela se produit, si vous souhaitez mettre à disposition cette application, vous devez l'ajouter à nouveau à partir d'une source valide.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez le groupe d'applications dans le volet central, puis sélectionnez une ou plusieurs applications dans le panneau central.
3. Sélectionnez **Supprimer du groupe d'applications** dans le volet Actions.
4. Confirmez la suppression.

Modifier les propriétés de l'application

Vous pouvez modifier les propriétés d'une seule application à la fois.

Pour modifier les propriétés d'une application :

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez une application, puis sélectionnez **Modifier les propriétés d'application** dans le volet Actions.
3. Sélectionnez la page contenant la propriété que vous souhaitez modifier.
4. Lorsque vous avez terminé, cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Propriété	Sélectionner cette page
Catégorie/dossier dans lequel l'application s'affiche dans Receiver	Mise à disposition
Arguments de ligne de commande	L'Emplacement
Les groupes de mise à disposition et groupes d'applications dans lesquels l'application est disponible	Groupes
Description	Identification
Extensions de fichier et association de type de fichier : extensions que l'application ouvre automatiquement	Association de type de fichier
Icône	Mise à disposition
Mots clés pour StoreFront	Identification
Limites (consultez la section Configurer les limites d'application)	Mise à disposition
Nom : noms que l'utilisateur et l'administrateur voient	Identification

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Chemin vers l'exécutable	L'Emplacement
Raccourci sur le bureau de l'utilisateur : activer ou désactiver	Mise à disposition
Visibilité : limite les utilisateurs autorisés à voir l'application dans Citrix Receiver (une application non visible peut toujours être démarrée ; pour la rendre non disponible ainsi qu'invisible, ajoutez-la à un groupe différent)	Limiter la visibilité
Répertoire de travail	L'Emplacement

Les modifications apportées aux applications peuvent ne pas prendre effet pour les utilisateurs d'applications courantes tant qu'ils n'ont pas fermé leur session.

Configurer les limites d'application

Configurez les limites d'application pour vous aider à gérer l'utilisation des applications. Par exemple, vous pouvez utiliser les limites d'application pour gérer le nombre d'utilisateurs pouvant accéder à une application simultanément. De même, les limites d'application peuvent être utilisées pour gérer le nombre d'instances simultanées d'applications très consommatrices de ressources, ce qui peut vous aider à gérer les performances des serveurs et à empêcher la détérioration du service.

Important : cette fonctionnalité limite le nombre de démarrages d'application qui sont négociés par le Controller (par exemple, à partir de Citrix Receiver et StoreFront), et non pas le nombre d'applications qui peuvent être lancées par d'autres méthodes. Par conséquent, les limites d'application aident les administrateurs à gérer l'utilisation simultanée, mais ne peuvent pas être appliquées de force dans tous les scénarios. Par exemple, les limites d'application ne peuvent pas être appliquées lorsque le Controller se trouve en mode de location de connexion.

Par défaut, il n'existe aucune limite sur le nombre d'instances d'application qui peuvent être exécutées simultanément. Il existe deux paramètres de limite d'application ; vous pouvez en configurer un ou les deux :

- Le nombre maximal d'instances simultanées d'une application par tous les utilisateurs du groupe de mise à disposition.
- Une instance de l'application par utilisateur dans le groupe de mise à disposition

Si une limite est configurée, un message d'erreur est généré lorsqu'un utilisateur tente de démarrer une instance de l'application qui dépasse la limite configurée.

Exemples d'utilisation des limites d'application :

- **Nombre maximal d'instances simultanées.** Dans un groupe de mise à disposition, vous configurez le nombre maximal d'instances d'applications simultanées Alpha sur 15. Plus tard, les utilisateurs de ce groupe de mise à disposition ont 15 instances de cette application en cours d'exécution en même temps. Si un utilisateur de ce groupe de mise à disposition tente de lancer Alpha, un message d'erreur est généré et l'application Alpha n'est pas lancée car la limite d'instances d'applications simultanées (15) aurait été dépassée.
- **Une instance d'application par utilisateur.** Dans un autre groupe de mise à disposition, vous activez l'option une

© 1999-2017 Citrix Systems, Inc. All rights reserved.

instance par utilisateur pour l'application Beta. L'utilisateur Tony lance l'application Beta avec succès. Plus tard, alors que l'application est toujours en cours d'exécution dans la session de Tony, il tente de démarrer une autre instance de Beta. Un message d'erreur est généré et Beta n'est pas lancé car la limite d'une instance par utilisateur aurait été dépassée.

- **Nombre maximal d'instances simultanées et une instance par utilisateur.** Dans un autre groupe de mise à disposition, vous configurez un nombre maximal d'instances simultanées de 10 et activez l'option une instance par utilisateur pour l'application Delta. Plus tard, lorsque dix utilisateurs de ce groupe de mise à disposition exécutent chacun une instance de Delta, les autres utilisateurs de ce groupe de mise à disposition qui tentent de lancer Delta reçoivent un message d'erreur et Delta n'est pas démarré. Si un des dix utilisateurs de Delta tente de démarrer une seconde instance de cette application, il reçoit un message d'erreur et la deuxième instance ne peut pas être démarrée.

Si des instances de l'application sont également lancées par d'autres méthodes que la négociation Controller (par exemple, lorsqu'un Controller se trouve en mode de location de connexion) et que les limites configurées sont dépassées, les utilisateurs ne pourront pas lancer d'instances supplémentaires jusqu'à ce qu'ils ferment suffisamment d'instances pour ne plus dépasser la limite. Les instances qui ont dépassé la limite ne sont pas arrêtées ; elles peuvent continuer jusqu'à ce que les utilisateurs les ferment.

Si vous désactivez l'itinérance de session, désactivez la limite d'application « Une seule instance par utilisateur ». Si vous activez la limite d'application « Une seule instance par utilisateur », ne configurez pas les deux valeurs qui permettent de nouvelles sessions sur de nouvelles machines. Pour de plus amples informations sur l'itinérance, consultez l'article Sessions.

Pour configurer les limites d'application :

1. Sélectionnez **Applications** dans le volet de navigation de Studio, puis sélectionnez une application.
2. Sélectionnez **Modifier les propriétés d'application** dans le volet Actions.
3. Sur la page **Mise à disposition**, choisissez l'une des options ci-dessous. Lorsque vous avez terminé, cliquez sur **OK** ou **Appliquer**. (**OK** applique la modification et ferme la boîte de dialogue Modifier les propriétés d'application ; **Appliquer** applique la modification et quitte la boîte de dialogue ouverte.)

- Autoriser l'utilisation illimitée de l'application. Il n'existe aucune limite au nombre d'instances exécutées en même temps. Il s'agit de l'option par défaut.
- Définir des limites pour l'application. Il existe deux types de limite ; spécifiez-en une ou les deux.
  - Spécifier le nombre maximal d'instances pouvant être exécutées simultanément
  - Limiter à une instance d'application par utilisateur

Gérer les dossiers d'applications

Par défaut, les applications que vous ajoutez à des groupes de mise à disposition sont placées dans un dossier nommé **Applications**. Vous pouvez spécifier un dossier différent lorsque vous créez le groupe de mise à disposition, lorsque vous ajoutez une application ou plus tard.

À savoir :

- Vous ne pouvez pas renommer ou supprimer le dossier Applications, mais vous pouvez déplacer toutes les applications qu'il contient vers d'autres dossiers que vous créez.
- Un nom de dossier peut contenir entre 1 et 64 caractères. Les espaces sont autorisés.
- Les dossiers peuvent être imbriqués jusqu'à cinq niveaux.
- Les dossiers n'ont pas à contenir d'applications, des dossiers vides sont autorisés.
- Les dossiers sont répertoriés par ordre alphabétique dans Studio, sauf si vous les déplacer ou spécifiez un emplacement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

différent lorsque vous les créez.

- Vous pouvez posséder plus d'un dossier du même nom, tant que chacun possède un dossier parent différent. De même, vous pouvez posséder plus d'une application du même nom, tant que chacune se trouve dans un dossier différent.
- Vous devez disposer de l'autorisation Afficher l'application pour voir les applications dans des dossiers, et vous devez posséder l'autorisation Modifier les propriétés d'application pour toutes les applications dans le dossier pour déplacer, renommer ou supprimer un dossier qui contient des applications.
- La plupart des procédures suivantes requièrent des actions depuis le panneau Actions de Studio. Éventuellement, vous pouvez utiliser les menus du bouton droit de la souris ou le glisser-déplacer. Par exemple, si vous créez ou déplacez un dossier dans un emplacement indésirable, vous pouvez le faire glisser et le déposer à l'emplacement approprié.

Pour gérer les dossiers d'applications, sélectionnez **Applications** dans le volet de navigation de Studio. Utilisez la liste ci-dessous pour plus d'informations.

- Pour afficher tous les dossiers (mis à part les dossiers incorporés), cliquez sur **Afficher tout** au-dessus de la liste de dossiers.
- Pour afficher un dossier au niveau le plus élevé (non imbriqué), sélectionnez le dossier Applications. Pour placer le nouveau dossier sous un dossier existant autre que le dossier Applications, sélectionnez ce dossier. Sélectionnez ensuite **Créer un dossier** dans le volet Actions. Entrez un nom.
- Pour déplacer un dossier, sélectionnez le dossier, puis sélectionnez **Déplacer le dossier** dans le volet Actions. Vous pouvez déplacer un seul dossier à la fois, à moins que le dossier contienne des dossiers incorporés. Conseil : la manière la plus facile de déplacer un dossier est d'utiliser le glisser-déplacer.
- Pour renommer un dossier, sélectionnez le dossier, puis sélectionnez **Renommer le dossier** dans le volet Actions. Entrez un nom.
- Pour supprimer un dossier, sélectionnez le dossier, puis sélectionnez **Supprimer le dossier** dans le volet Actions. Lorsque vous supprimez un dossier qui contient des applications et d'autres dossiers, ces objets sont également supprimés. La suppression de l'application supprime l'attribution de l'application depuis le groupe de mise à disposition, elle ne supprime pas l'application de la machine.
- Pour déplacer des applications dans un dossier, sélectionnez une ou plusieurs applications. Ensuite, sélectionnez **Déplacer l'application** dans le panneau Actions. Sélectionnez le dossier.

Vous pouvez également placer les applications que vous ajoutez dans un dossier spécifique (même un nouveau dossier) sur la page **Application** des assistants Créer un groupe de mise à disposition et Créer un groupe d'applications. Par défaut, les applications ajoutées sont placées dans le dossier Applications ; cliquez sur **Modifier** pour sélectionner ou créer un dossier.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Zones

Jul 07, 2016

Les déploiements répartis sur différents emplacements géographiques et connectés à un réseau étendu peuvent rencontrer des problèmes de latence réseau et de fiabilité. Il existe deux options pour pallier ces problèmes :

- Déployer plusieurs sites, chacun avec sa propre base de données de site SQL Server.

  Cette option est recommandée pour les déploiements de grande taille. Plusieurs sites sont gérés séparément et chacun requiert sa propre base de données de site SQL Server. Chaque site est un déploiement XenApp distinct.

- Configurer plusieurs zones au sein d'un seul site.

  La configuration de zones peut aider les utilisateurs situés dans des régions éloignées à se connecter à des ressources sans que leurs connexions soient obligées de traverser des segments importants de réseau étendu. L'utilisation de zones permet une gestion efficace de site à partir d'une seule console Citrix Studio, de Citrix Director et de la base de données du site. Vous économisez ainsi les coûts liés au déploiement, au personnel, aux licences et à l'exploitation de sites contenant des bases de données distinctes dans des emplacements distants.

  Les zones peuvent s'avérer utiles dans les déploiements de toutes tailles. Vous pouvez utiliser des zones pour que les applications et les bureaux se trouvent à proximité des utilisateurs finaux, ce qui améliore les performances. Une zone peut disposer d'un ou de plusieurs Controller installés localement pour assurer la redondance et la résilience, mais cette configuration n'est pas obligatoire.

Dans cet article, le terme « local » fait référence à la zone dont il est question. Par exemple, « Un VDA s'enregistre auprès d'un Controller local » signifie qu'un VDA s'enregistre auprès d'un Controller dans la zone dans laquelle le VDA est situé.

Les zones de cette version sont semblables, mais pas identiques aux zones de XenApp 6.5 et versions antérieures. Par exemple, dans cette implémentation de zones, il n'existe aucun collecteur de données. Tous les Controller du site communiquent avec une seule base de données du site dans la zone principale. En outre, les zones de basculement et les zones préférées fonctionnent différemment dans cette version.

Types de zone

Un site dispose toujours d'une zone principale. Il peut également disposer d'une ou de plusieurs zones satellite. Les zones satellite peuvent être utilisées pour la récupération d'urgence, des centres de données distants, des succursales, un cloud ou une zone de disponibilité dans un cloud.

Zone principale

La zone principale est appelée « Principale » par défaut et contient la base de données du site SQL Server (et des serveurs SQL haute disponibilité, le cas échéant), Studio, Director, StoreFront, le serveur de licences Citrix et NetScaler Gateway. La base de données du site doit toujours se trouver dans la zone principale.

La zone principale doit également disposer d'au moins deux Controller pour assurer la redondance et peut disposer d'un ou de plusieurs VDA avec des applications qui sont étroitement liées avec la base de données et l'infrastructure.

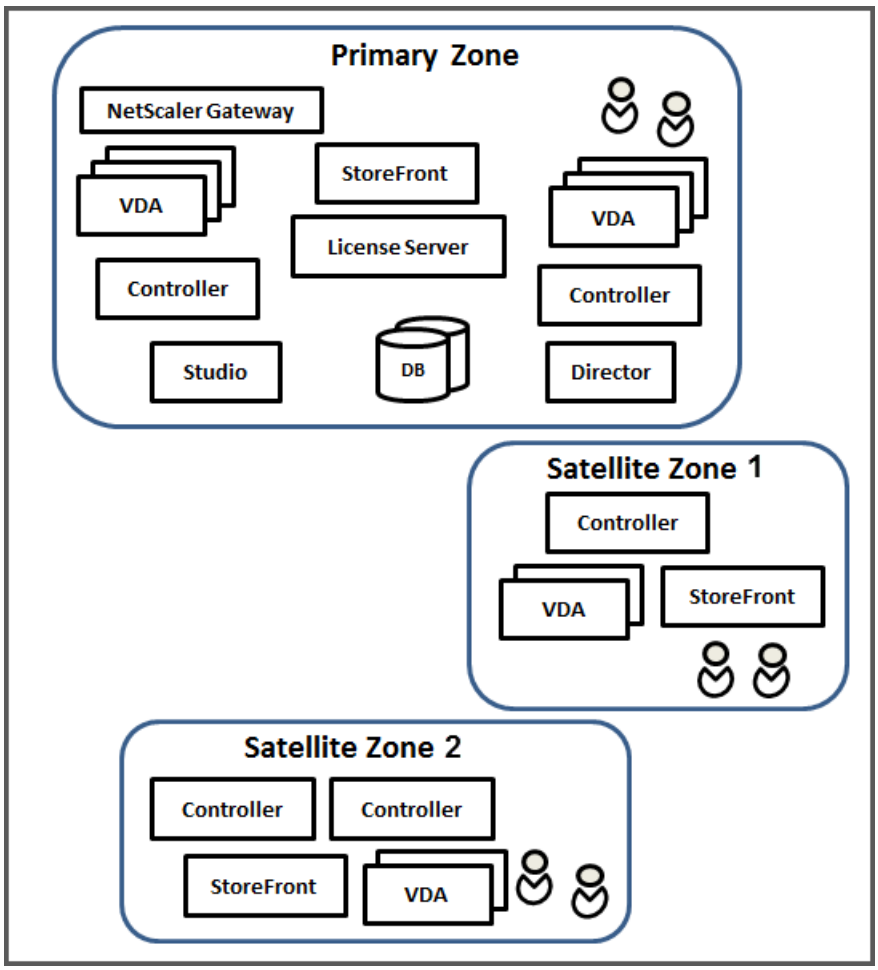
Zone satellite

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Une zone satellite contient un ou plusieurs VDA, Controller, serveurs StoreFront et serveurs NetScaler Gateway. Dans des conditions de fonctionnement normales, les Controller d'une zone satellite communiquent directement avec la base de données située dans la zone principale.

Une zone satellite, en particulier une zone de grande taille, peut également contenir un hyperviseur qui est utilisé pour provisionner et/ou stocker des machines pour cette zone. Lorsque vous configurez une zone satellite, vous pouvez lui associer une connexion à un hyperviseur ou à un service de cloud (Assurez-vous que les catalogues de machines qui utilisent cette connexion se trouvent dans la même zone).

Un site peut contenir différents types de zones satellite, en fonction de vos besoins et de votre environnement. La figure suivante illustre une zone principale et des exemples de zones satellite.



- La zone principale contient deux Controller, Studio, Director, StoreFront, le serveur de licences et la base de données du site (plus des déploiements SQL Server haute disponibilité). La zone principale contient également plusieurs VDA et un boîtier NetScaler Gateway.
- Zone satellite 1 - VDA avec Controller

  La zone satellite 1 contient un Controller, des VDA et un serveur StoreFront. Les VDA de cette zone satellite s'enregistrent auprès du Controller local. Le Controller local communique avec la base de données du site et le serveur de licences de la zone principale.

  Si le réseau étendu échoue, la fonctionnalité de location de connexion permet au Controller de la zone satellite de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

continuer la négociation des connexions avec les VDA de cette zone. Un tel déploiement peut être efficace dans un bureau où les utilisateurs utilisent un site StoreFront local et le Controller local pour accéder à leurs ressources locales, même si la liaison WAN connectant leur bureau au réseau d'entreprise échoue.

- Zone satellite 2 - VDA avec Controller redondants

  La zone satellite 2 contient deux Controller, des VDA et un serveur StoreFront. Il s'agit du type de zone le plus robuste, offrant une protection contre un échec simultané du réseau étendu et de l'un des Controller locaux.

Enregistrement des VDA et basculement des Controller

Dans un site contenant des zones principale et satellite, avec des VDA à la version 7.7 au minimum :

- Un VDA de la zone principale s'enregistre auprès d'un Controller de la zone principale. Un VDA de la zone principale ne tentera jamais de s'enregistrer auprès d'un Controller situé dans une zone satellite.
- Un VDA situé dans une zone satellite s'enregistre auprès d'un Controller local, si possible (Il est considéré comme Controller préféré). Si aucun Controller local n'est disponible (par exemple, lorsque les Controller locaux ne peuvent pas accepter d'enregistrements VDA supplémentaires ou si les Controller locaux ont échoué), le VDA tente de s'enregistrer auprès d'un Controller de la zone principale. Dans ce cas, le VDA reste dans la zone principale sans être enregistré, même si un Controller de la zone satellite devient de nouveau disponible. Un VDA situé dans une zone satellite ne tentera jamais de s'enregistrer auprès d'un Controller situé dans une autre zone satellite.
- Lorsque la mise à jour automatique est activée pour la découverte VDA de Controller, et que vous spécifiez une liste d'adresses de Controller lors de l'installation du VDA, un Controller est sélectionné de façon aléatoire à partir de cette liste pour l'enregistrement initial (quelle que soit la zone dans laquelle le Controller réside). Une fois que la machine avec ce VDA est redémarrée, le VDA s'enregistre de préférence auprès d'un Controller de sa zone locale.
- Si un Controller d'une zone satellite échoue, il bascule vers un autre Controller local, si possible. Si aucun Controller local n'est disponible, il bascule vers un Controller de la zone principale.
- Si vous déplacez un Controller dans ou hors d'une zone, et que la mise à jour automatique est activée, les VDA des deux zones reçoivent des listes mises à jour qui indiquent quels Controller sont locaux et lesquels se trouvent dans la zone principale, de façon à ce qu'ils sachent avec lesquels ils peuvent s'enregistrer et accepter des connexions.
- Si vous déplacez un catalogue de machines vers une autre zone, les VDA de ce catalogue s'enregistrent auprès des Controller situés dans la zone dans laquelle vous avez déplacé le catalogue (Lorsque vous déplacez un catalogue, assurez-vous que vous déplacez aussi toute connexion hôte associée à la même zone).
- Les Controller de la zone principale conservent les données de location de connexion pour toutes les zones. Les Controller situés dans des zones satellite conservent les données de location de connexion pour leur propre zone et la zone principale, mais pas les données des autres zones satellite.

Pour les sites contenant des VDA de versions antérieures à la version 7.7 :

- Un VDA situé dans une zone satellite accepte les requêtes de Controller situés dans sa zone locale et la zone principale (Les VDA à partir de la version 7.7 peuvent accepter les demandes de Controller d'autres zones satellite).
- Un VDA situé dans une zone satellite s'enregistre auprès d'un Controller situé dans la zone principale ou la zone locale de façon aléatoire. (Les VDA à partir de la version 7.7 préfèrent la zone locale).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Considérations, configurations requises et recommandations

- Vous pouvez placer les éléments suivants dans une zone : Controller, catalogues de machines et connexions hôte. Si un catalogue de machines utilise une connexion hôte, le catalogue et la connexion doivent se trouver dans la même zone.
- Lorsque vous créez un site de production, puis créez le premier catalogue de machines et le premier groupe de mise à disposition, tous les éléments se trouvent dans la zone principale ; vous ne pouvez pas créer de zones satellite tant que cette configuration initiale n'a pas été effectuée (Si vous créez un site vide, la zone principale contient initialement un seul Controller ; vous pouvez créer des zones satellite avant ou après la création d'un catalogue de machines et d'un groupe de mise à disposition).
- Lorsque vous créez la première zone satellite contenant un ou plusieurs éléments, tous les autres éléments de votre site restent dans la zone principale.
- La zone principale est appelée « Principale » par défaut ; vous pouvez changer ce nom. Bien que Studio indique quelle zone est la zone principale, il est recommandé d'utiliser un nom facile à identifier pour la zone principale. Vous pouvez réaffecter la zone principale (c'est-à-dire définir une autre zone comme zone principale), mais elle doit toujours contenir la base de données du site et les serveurs haute disponibilité.
- La base de données du site doit toujours se trouver dans la zone principale.
- Après avoir créé une zone, vous pouvez déplacer les éléments d'une zone à une autre. Veuillez noter que cette flexibilité vous permet de potentiellement séparer les éléments qui fonctionnent mieux lorsqu'ils sont à proximité ; par exemple, le déplacement d'un catalogue de machines vers une autre zone que la connexion (hôte) qui crée les machines dans le catalogue peut affecter les performances. Par conséquent, prenez en compte les effets potentiels du déplacement d'éléments entre les zones. Gardez un catalogue et la connexion hôte qu'il utilise dans la même zone.
- Pour des performances optimales, installez Studio et Director uniquement dans la zone principale. Si vous souhaitez utiliser une autre instance de Studio dans une zone satellite (par exemple, si une zone satellite contenant des Controller est utilisée pour le basculement au cas où la zone principale serait inaccessible), exécutez Studio en tant qu'application publiée localement. Vous pouvez également accéder à Director à partir d'une zone satellite car il s'agit d'une application Web.
- Dans l'idéal, NetScaler Gateway situé dans une zone satellite doit être utilisé pour les connexions utilisateur entrant dans cette zone depuis d'autres zones ou des emplacements externes, mais vous pouvez l'utiliser pour les connexions à l'intérieur de la zone.

Créer et gérer des zones

Un administrateur complet peut effectuer toutes les tâches de création et de gestion de zone. Toutefois, vous pouvez également créer un rôle personnalisé qui vous permet de créer, modifier ou supprimer une zone. Le déplacement d'éléments entre les zones ne nécessite pas d'autorisations liées à la zone (à l'exception des autorisations en lecture) ; cependant, vous devez disposer d'une autorisation de modification pour les éléments que vous déplacez. Par exemple, pour déplacer un catalogue de machines d'une zone vers une autre, vous devez disposer d'une autorisation de modification pour ce catalogue de machines. Pour plus d'informations, veuillez consulter l'article Administration déléguée.

Si vous utilisez Provisioning Services : étant donné que la console Provisioning Services fournie avec cette version ne sait pas identifier les zones, Citrix vous recommande d'utiliser Studio pour créer des catalogues de machines que vous souhaitez placer dans des zones satellite. Utilisez l'assistant Studio pour créer le catalogue, et spécifiez la zone satellite

© 1999-2017 Citrix Systems, Inc. All rights reserved.

appropriée. Puis, utilisez la console Provisioning Services pour provisionner des machines dans ce catalogue (Si vous créez le catalogue à l'aide de l'assistant Provisioning Services, il sera placé dans la zone principale et vous devrez utiliser Studio pour le déplacer vers la zone satellite ultérieurement).

1. Sélectionnez **Configuration > Zones** dans le volet de navigation de Studio.
2. Sélectionnez **Créer une zone** dans le volet Actions.
3. Entrez un nom pour la zone et une description (facultatif). Le nom doit être unique dans le site.
4. Sélectionnez les éléments à placer dans la nouvelle zone. Vous pouvez filtrer ou effectuer une recherche dans la liste des éléments à partir de laquelle vous sélectionnez. Vous pouvez également créer une zone vide ; dans ce cas, ne sélectionnez pas d'éléments.
5. Cliquez sur **Save**.

Une autre méthode consiste à sélectionner un ou plusieurs éléments dans Studio, puis à sélectionner **Créer une zone** dans le volet Actions.

1. Sélectionnez **Configuration > Zones** dans le volet de navigation de Studio.
2. Sélectionnez une zone, puis sélectionnez **Modifier la zone** dans le volet Actions.
3. Modifiez le nom et/ou la description de la zone. Si vous modifiez le nom de la zone principale, assurez-vous que la zone reste facile à identifier comme zone principale.
4. Cliquez sur **OK** ou **Appliquer**.

1. Sélectionnez **Configuration > Zones** dans le volet de navigation de Studio.
2. Sélectionnez un ou plusieurs éléments.
3. Effectuez l'une des actions suivantes : faites glisser les éléments vers la zone de destination, ou sélectionnez **Déplacer des éléments** dans le panneau Actions et spécifiez la zone vers laquelle les déplacer.

Un message de confirmation dresse la liste des éléments que vous avez sélectionnés et demande si vous êtes sûr de vouloir déplacer tous ces éléments.

Rappel : si un catalogue de machines utilise une connexion hôte vers un hyperviseur ou un service de cloud, le catalogue et la connexion doivent se trouver dans la même zone. Sinon, les performances peuvent être affectées. Si vous déplacez un élément, déplacez l'autre.

Une zone doit être vide pour pouvoir être supprimée. Vous ne pouvez pas supprimer la zone principale.

1. Sélectionnez **Configuration > Zones** dans le volet de navigation de Studio.
2. Sélectionnez une zone.
3. Sélectionnez **Supprimer la zone** dans le volet Actions. Si la zone n'est pas vide (elle contient des éléments), vous êtes invité à choisir la zone vers laquelle ces éléments seront déplacés.
4. Confirmez la suppression.

Lorsque vous ajoutez une connexion hôte ou que vous créez un catalogue de machines (à un autre moment que lors de la

© 1999-2017 Citrix Systems, Inc. All rights reserved.

création du site), vous pouvez spécifier une zone à laquelle l'élément sera attribué, si vous avez déjà créé au moins une zone satellite.

Dans la plupart des cas, la zone principale est la valeur par défaut. Lors de l'utilisation de Machine Creation Services pour créer un catalogue de machines, la zone qui est configurée pour la connexion hôte est sélectionnée automatiquement.

Si le site ne contient aucune zone satellite, il est supposé que la zone principale sera utilisée et la sélection de zone ne s'affiche pas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Connexions et ressources

Aug 22, 2016

Dans cet article :

- Introduction
- Emplacement des informations sur les types de connexion
- Stockage hôte
- Créer une connexion et des ressources
- Créer une connexion et des ressources à partir d'une connexion existante
- Modifier les paramètres de connexion
- Activer ou désactiver le mode maintenance pour une connexion
- Supprimer une connexion
- Renommez ou de test de la connexion
- Afficher les détails des machines sur une connexion
- Gérer les machines sur une connexion
- Modifier un espace de stockage
- Supprimer, renommer ou test des ressources
- Utiliser les connexions IntelliCache pour XenServer
- Horloges de connexion

Introduction

Vous pouvez éventuellement créer votre première connexion pour héberger des ressources lorsque vous créez un site. Plus tard, vous pouvez modifier cette connexion et en créer de nouvelles. La configuration d'une connexion implique de sélectionner le type de connexion parmi les hyperviseurs et les services de cloud pris en charge. Le stockage et le réseau que vous sélectionnez constituent les ressources de cette connexion.

Les administrateurs en lecture seule peuvent afficher les détails de connexion et de ressources ; vous devez être un administrateur complet pour effectuer la connexion et des tâches de gestion des ressources. Pour plus d'informations, veuillez consulter l'article Administration déléguée.

Vous pouvez utiliser les plates-formes de virtualisation prises en charge pour héberger et gérer des machines dans votre environnement XenApp ou XenDesktop. L'article Configuration système requise répertorie les types pris en charge. Vous pouvez utiliser les solutions de déploiement cloud prises en charge pour héberger les composants du produit et provisionner des machines virtuelles. Ces ressources informatiques de pool de solutions destinées à créer des clouds d'infrastructure as a service (IaaS) publics, privés et hybrides.

Pour de plus amples informations, consultez les sources d'informations suivantes.

VMware

- Article Environnements de virtualisation VMware.
- Documentation du produit VMware.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft Hyper-V

- Article Environnements de virtualisation Microsoft System Center Virtual Machine Manager.
- Documentation Microsoft.

Microsoft Azure

- Article Environnements de virtualisation Microsoft Azure.
- Documentation Microsoft.

services Web Amazon (AWS)

- Citrix XenDesktop sur AWS.
- Documentation AWS.
- Lorsque vous créez une connexion dans Studio, vous devez fournir la clé API et la clé secrète. Vous pouvez exporter le fichier de clé contenant ces valeurs à partir d'AWS, puis les importer. Vous devez également fournir la région, la zone de disponibilité, le nom du VPC, les adresses de sous-réseau, le nom du domaine, les noms de groupe de sécurité et les informations d'identification.
- Le fichier d'informations d'identification pour le compte AWS de racine, (récupéré à partir de la console AWS) n'est pas au même format que les fichiers d'informations d'identification téléchargés pour les utilisateurs standard AWS. Par conséquent, Studio ne peut pas utiliser le fichier pour remplir les champs de clé API et de clé secrète. Vérifiez que vous utilisez les fichiers d'informations d'identification AWS IAM.

Citrix CloudPlatform

- Documentation Citrix CloudPlatform.
- Lorsque vous créez une connexion dans Studio, vous devez fournir la clé API et la clé secrète. Vous pouvez exporter le fichier de clé contenant ces valeurs à partir de CloudPlatform, puis importer ces valeurs dans Studio.

Citrix XenServer

- Documentation Citrix XenServer.
- Lorsque vous créez une connexion, vous devez fournir les informations d'identification d'un administrateur avancé de VM ou d'un utilisateur de niveau plus élevé.
- Citrix vous recommande d'utiliser HTTPS pour sécuriser les communications avec XenServer. Pour utiliser HTTPS, vous devez remplacer le certificat SSL par défaut installé sur XenServer ; consultez l'article CTX128656.
- Vous pouvez configurer la haute disponibilité si elle est activée sur XenServer. Citrix vous recommande de sélectionner tous les serveurs du pool (dans Modifier les serveurs HA) pour permettre la communication avec XenServer au cas où le pool principal échoue.
- Vous pouvez sélectionner un type et un groupe de processeur graphique, ou de pass-through, si XenServer prend en charge vGPU. La vue indique si la sélection possède des ressources GPU dédiées.

Nutanix Acropolis

- Article Environnements de virtualisation Nutanix. (En anglais)
- Documentation Nutanix.

Stockage hôte

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Lors du provisioning de machines, les données sont classées par type :

- Données du système d'exploitation, ce qui comprend les images principales.
- Données temporaires, ce qui comprend toutes les données non persistantes écrites sur les machines provisionnées avec MCS, les fichiers de pages Windows, les données du profil utilisateur et les données qui sont synchronisées avec ShareFile. Ces données sont supprimées chaque fois qu'une machine redémarre.
- Données stockées sur les Personal vDisks.

La mise à disposition d'espaces de stockage distincts pour chaque type de données peut réduire la charge et améliorer les performances IOPS (opérations E/S par seconde) sur chaque périphérique de stockage, ce qui permet d'utiliser les ressources disponibles de l'hôte de manière optimale. Cela permet également d'utiliser un stockage approprié pour les différents types de données : la persistance et la résilience sont des facteurs plus importants pour certaines données que pour d'autres.

Le stockage peut être partagé (centralisé, séparé de l'hôte, utilisé par tous les hôtes) ou local sur un hyperviseur. Par exemple, un stockage partagé central peut être un ou plusieurs volumes de stockage en cluster Windows Server 2012 (avec ou sans stockage attaché), ou l'appliance d'un fournisseur de stockage. Le stockage central peut également fournir ses propres optimisations telles que des chemins de contrôle de stockage de l'hyperviseur et un accès direct au travers de plug-ins de partenaires.

Le stockage des données temporaires localement évite d'avoir à traverser le réseau pour accéder à un espace de partagé. Cela permet également de réduire la charge ((opérations E/S par seconde) sur le périphérique de stockage partagé. Le stockage partagé peut être plus coûteux, par conséquent le stockage des données localement peut réduire les dépenses. Ces avantages doivent être pondérés par rapport à la disponibilité d'un stockage suffisant sur les serveurs hyperviseur.

Lorsque vous créez une connexion, vous devez choisir l'une des deux méthodes de gestion du stockage : stockage partagé par les hyperviseurs, ou stockage local sur l'hyperviseur.

Remarque : lorsque vous utilisez le stockage local sur un ou plusieurs hôtes XenServer pour le stockage des données temporaires, assurez-vous que chaque emplacement de stockage du pool a un nom unique. (Pour modifier un nom dans XenCenter, cliquez avec le bouton droit sur le stockage et modifiez le nom de la propriété.)

La méthode de stockage partagé par les hyperviseurs stocke centralement les données qui doivent être archivées à long terme, ce qui offre une gestion et une sauvegarde centralisées. Ce stockage contient les disques de système d'exploitation et les disques Personal vDisk.

Lorsque vous sélectionnez cette méthode, vous pouvez choisir d'utiliser le stockage local (sur les serveurs dans le même pool d'hyperviseurs) pour les données temporaires qui ne nécessitent pas d'être archivées ou d'autant de résilience que les données dans le stockage partagé. Ceci s'appelle la *mise en cache des données temporaires*. Le disque local permet de réduire le trafic vers le stockage du système d'exploitation principal. Ce disque est effacé après chaque redémarrage de machine. Le disque est accessible via un cache mémoire en écriture continue. Gardez à l'esprit que si vous utilisez le stockage local pour les données temporaires, le VDA provisionné est associé à un hyperviseur hôte spécifique ; si cet hôte échoue, la VM ne peut pas démarrer.

Exception : si vous utilisez des volumes de stockage en cluster (CSV), Microsoft System Center Virtual Machine Manager n'autorise pas la création de disques de mise en cache des données temporaires sur le stockage local.

Lorsque vous créez une connexion, si vous activez l'option permettant de stocker les données temporaires localement, vous

© 1999-2017 Citrix Systems, Inc. All rights reserved.

pouvez activer et configurer des valeurs autres que les valeurs par défaut pour la taille de disque et de mémoire pour chaque VM lorsque vous créez un catalogue de machines qui utilise cette connexion. Toutefois, les valeurs par défaut sont adaptées au type de connexion, et sont suffisantes pour la plupart des cas. Consultez l'article Créer des catalogues de machines pour plus de détails.

L'hyperviseur peut également fournir des technologies d'optimisation par le biais d'une mise en cache de lecture locale des images de disque ; par exemple, XenServer offre IntelliCache. Cela peut également réduire le trafic réseau vers le stockage central.

La méthode de stockage local sur l'hyperviseur stocke les données localement sur l'hyperviseur. Avec cette méthode, les images principales et les autres données d'OS sont transférées vers tous les hyperviseurs utilisés dans le site, aussi bien pour la création initiale d'une machine que pour les mises à jour futures des images. Cela se traduit par un trafic important sur le réseau de gestion. Les transferts d'images sont également chronophages, et les images deviennent disponibles auprès de chaque hôte à un moment différent.

Lorsque vous sélectionnez cette méthode, vous pouvez choisir d'utiliser un stockage partagé pour les Personal vDisks, afin de fournir la résilience et la prise en charge de systèmes de sauvegarde et de récupération d'urgence.

Créer une connexion et des ressources

Vous pouvez éventuellement créer la première connexion lorsque vous créez le site. L'Assistant de création de site contient les pages de connexion décrites ci-dessous : connexion, gestion du stockage, sélection du stockage et le réseau.

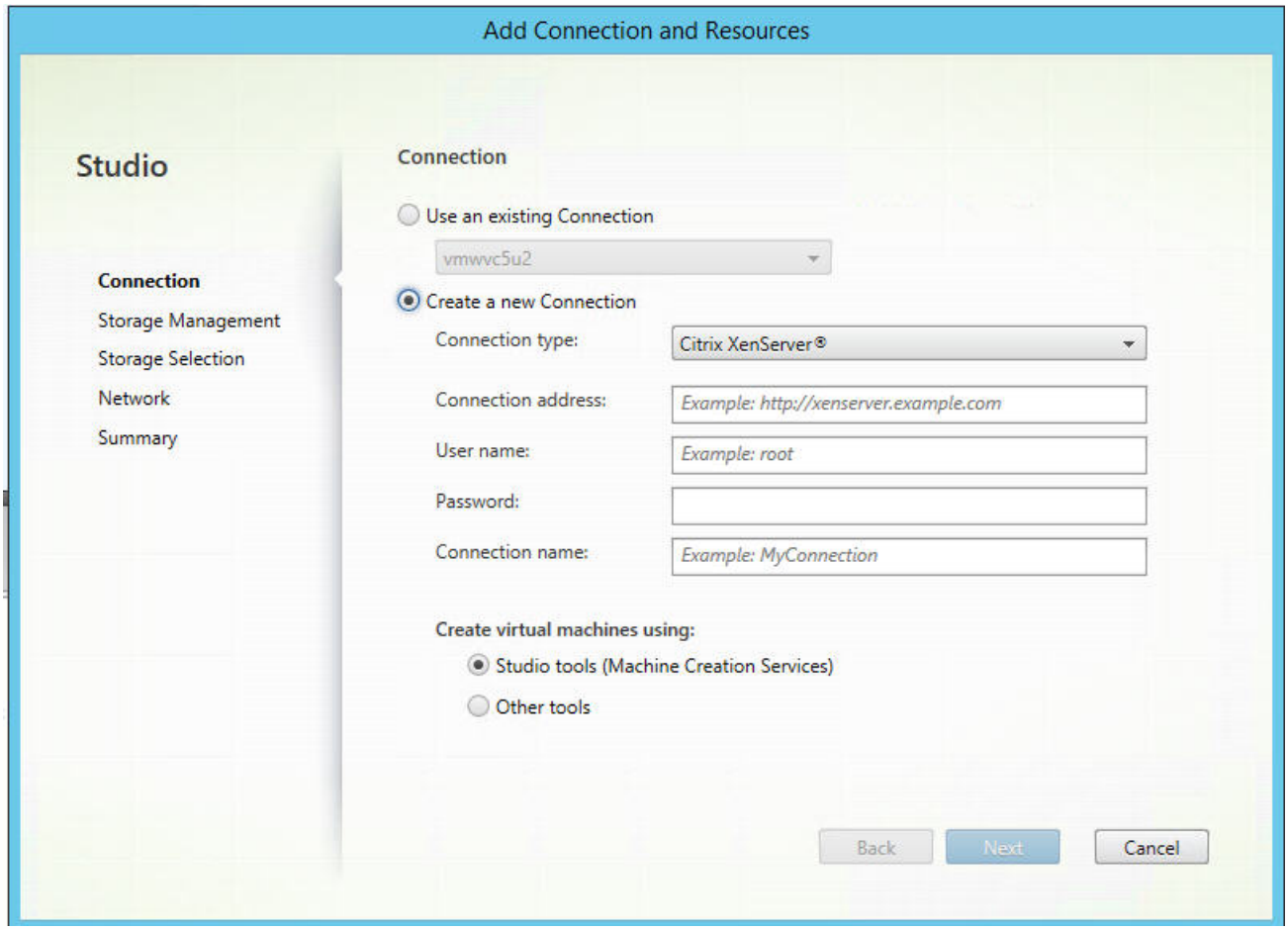
Si vous créez une connexion après la création du site, commencez à l'étape 1 ci-dessous.

Si vous créez une connexion basée sur la même configuration d'hôte que celle d'une connexion existante, utilisez cette procédure.

Important : les ressources hôte (stockage et réseau) doivent être disponibles avant de créer une connexion.

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez **Ajouter une connexion et des ressources** dans le volet Actions.
3. Sélectionnez **Créer une nouvelle connexion**.
4. L'assistant vous guide à travers les pages suivantes (le contenu dess page dépend du type de connexion sélectionné). Après avoir complété chaque page, cliquez sur **Suivant** jusqu'à la page Résumé.

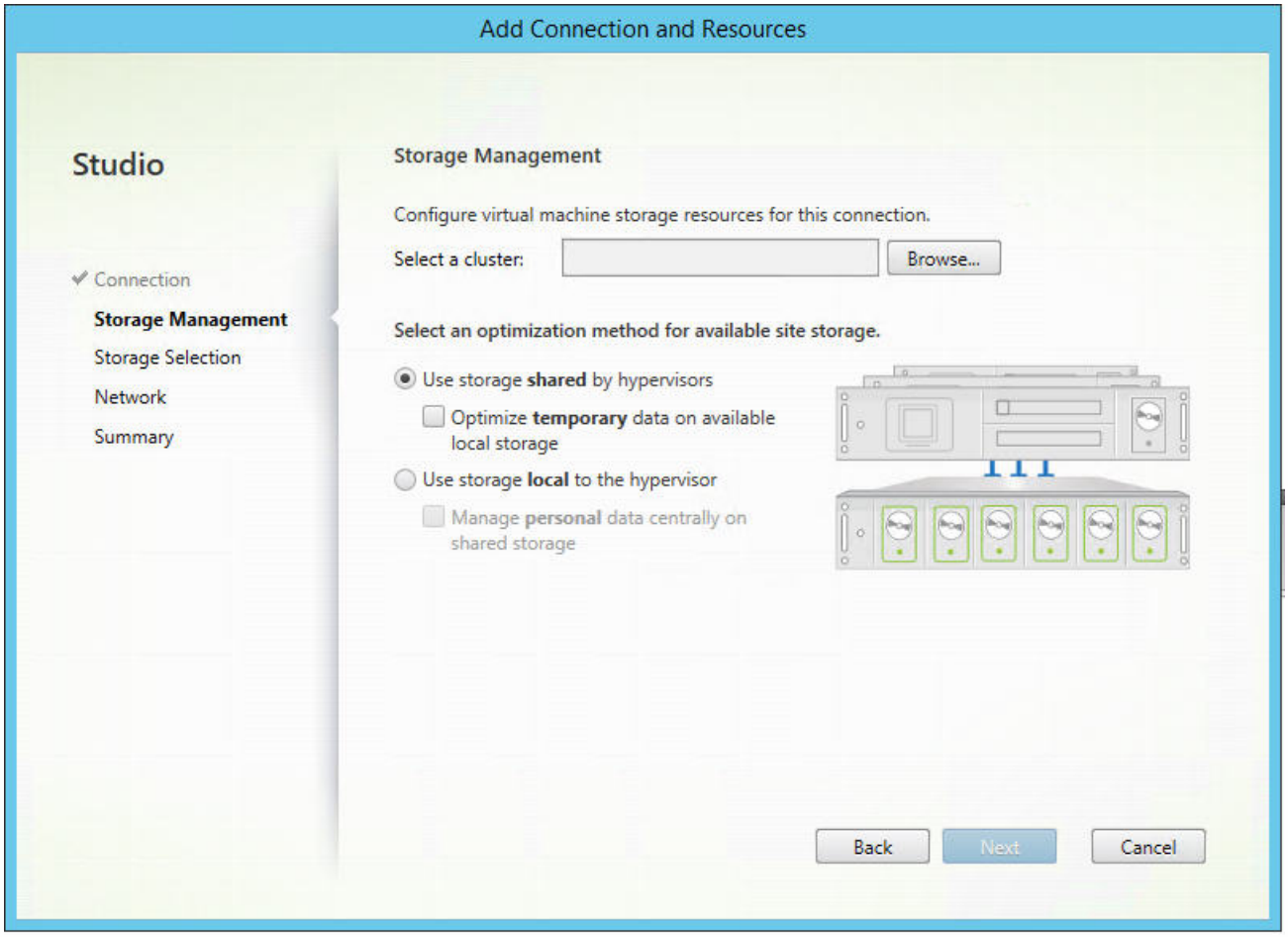
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Sur la page **Connexion** :

- Sélectionnez l'hyperviseur ou le service de cloud que vous utilisez dans le champ **Type de connexion**.
- Les champs relatifs à l'adresse de connexion et aux informations d'identification diffèrent en fonction du type de connexion sélectionné. Entrez les informations requises.
- Entrez un nom pour la connexion. Ce nom apparaît dans Studio.
- Choisissez l'outil que vous utilisez pour créer des machines virtuelles : les outils Studio (Machine Creation Services ou Provisioning Services) ou d'autres outils.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Pour de plus amples informations sur les types et méthodes de gestion du stockage, consultez la section Stockage hôte.

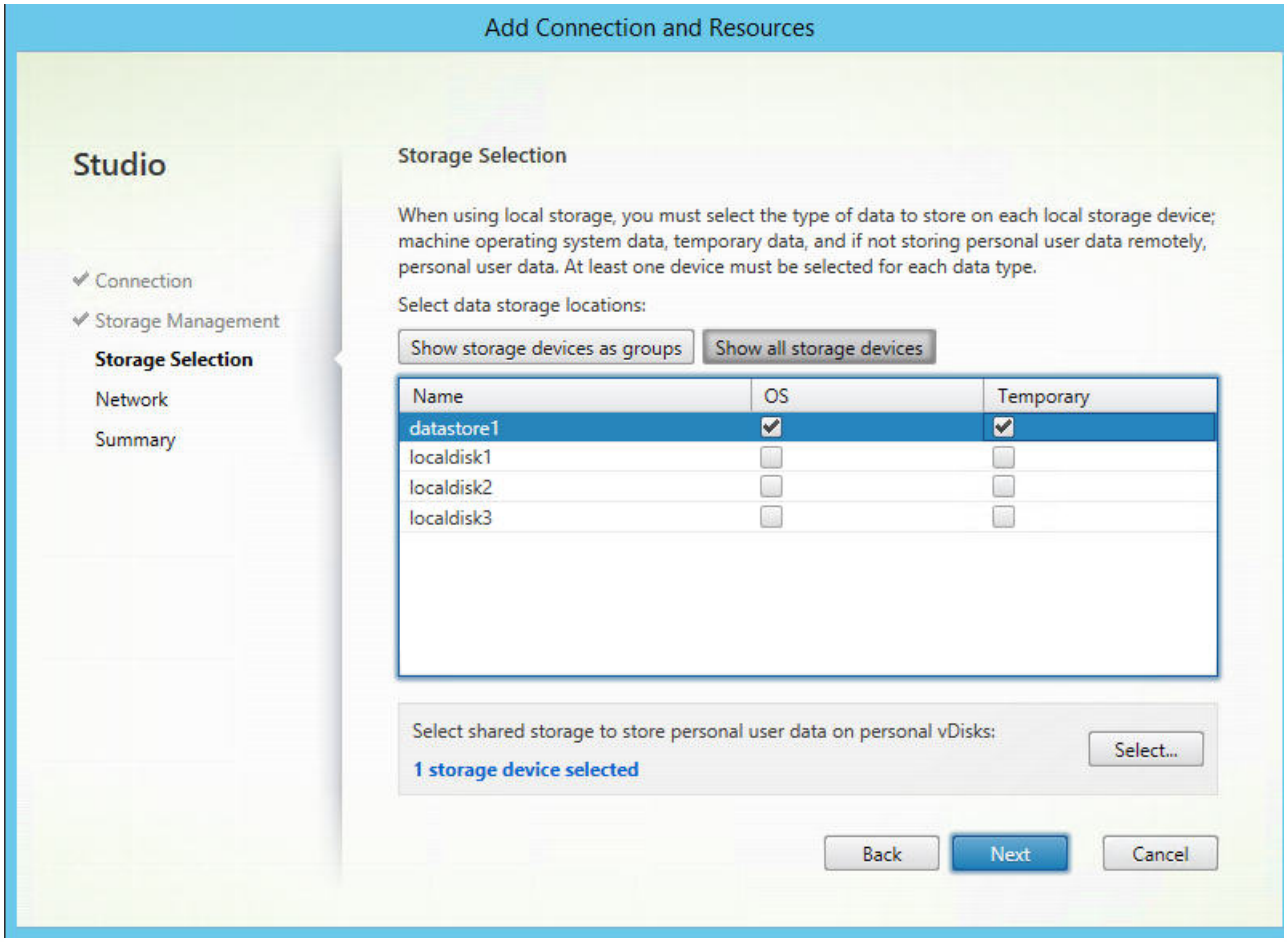
Si vous configurez une connexion à un hôte Hyper-V ou VMware, sélectionnez un nom de cluster. D'autres types de connexion ne nécessitent pas de nom de cluster.

Sélectionnez une méthode de gestion du stockage : stockage partagé par les hyperviseurs ou stockage local sur l'hyperviseur.

- Si vous choisissez le stockage partagé par les hyperviseurs, indiquez si vous souhaitez conserver les données temporaires sur l'espace de stockage local disponible. (Vous pouvez spécifier des tailles de stockage temporaire autres que les valeurs par défaut dans les catalogues de machines qui utilisent cette connexion.) **Exception** : lors de l'utilisation de volumes de stockage en cluster (CSV), Microsoft System Center Virtual Machine Manager n'autorise pas la création de disques de mise en cache des données temporaires sur le stockage local, par conséquent la configuration de la gestion du stockage échouera dans Studio.
- Si vous choisissez le stockage local sur l'hyperviseur, indiquez si vous souhaitez gérer des données personnelles (Personal vDisk) sur l'espace de stockage partagé.

Si vous utilisez un espace de stockage partagé sur un hyperviseur XenServer, indiquez si vous souhaitez utiliser IntelliCache pour réduire la charge sur le périphérique de stockage partagé. Consultez la section Utiliser les connexions IntelliCache pour XenServer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Pour de plus amples informations sur la sélection du stockage, consultez la section Stockage hôte.

Sélectionnez au moins un périphérique de stockage hôte pour chaque type de données disponible. La méthode de gestion du stockage que vous avez sélectionnée sur la page précédente affecte les types de données disponibles sur cette page. Vous devez sélectionner au moins un périphérique de stockage pour chaque type de données pris en charge avant de pouvoir passer à la page suivante de l'assistant.

La partie inférieure de la page **Sélectionner un stockage** contient des options de configuration supplémentaires si vous avez sélectionné l'une des options suivantes sur la page précédente.

- Si vous avez choisi le stockage partagé par les hyperviseurs, et activé la case **Optimiser les données temporaires sur le stockage local disponible**, vous pouvez sélectionner les périphériques de stockage local (dans le même pool d'hyperviseurs) à utiliser pour des données temporaires.
- Si vous avez choisi le stockage local sur l'hyperviseur et activé la case **Gérer les données personnelles centralement sur le stockage partagé**, vous pouvez sélectionner les périphériques partagés à utiliser pour les données personnelles (PvD).

Le nombre de périphériques de stockage actuellement sélectionnés est affiché (dans le diagramme ci-dessus, « 1 périphérique de stockage sélectionné »). Lorsque vous placez le curseur sur cette entrée, les noms des périphériques sélectionnés s'affichent (sauf si aucun périphérique n'est configuré).

1. Cliquez sur **Sélectionner** pour modifier les périphériques de stockage à utiliser.
2. Dans la boîte de dialogue **Sélectionner un stockage**, activez ou désactivez les cases de périphérique de stockage, puis

© 1999-2017 Citrix Systems, Inc. All rights reserved.

cliquez sur **OK**.

Entrez un nom pour les ressources ; ce nom apparaît dans Studio pour identifier la combinaison stockage et réseau associée à la connexion.

Sélectionnez un ou plusieurs réseaux que les machines virtuelles utiliseront.

Vérifiez vos sélections ; si vous souhaitez apporter des modifications, revenez sur les pages précédentes de l'assistant. Une fois que vous avez terminé avec votre évaluation, cliquez sur **Terminer**.

Rappel : si vous avez choisi de stocker les données temporaires localement, vous pouvez configurer des valeurs autres que les valeurs par défaut pour le stockage des données temporaires lorsque vous créez le catalogue de machines contenant les machines utilisant cette connexion. Consultez l'article Créer des catalogues de machines.

Créer une connexion et des ressources à partir d'une connexion existante

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez **Ajouter une connexion et des ressources** dans le volet Actions.
3. Sélectionnez **Utiliser une connexion existante**, puis choisissez la connexion appropriée.
4. L'assistant vous guide à travers les pages décrites dans la section Créer une connexion et des ressources.

Modifier les paramètres de connexion

N'utilisez pas cette procédure pour renommer une connexion ou pour créer une nouvelle connexion. Ces opérations sont différentes. Modifiez l'adresse uniquement si la machine hôte actuelle possède une nouvelle adresse ; si vous entrez l'adresse d'une autre machine, cela mettra fin à la connexion avec les catalogues de machines.

Vous ne pouvez pas modifier les paramètres GPU d'une connexion, car les catalogues de machines qui accèdent à cette ressource doivent utiliser une image principale appropriée spécifique au GPU. Créez une nouvelle connexion.

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez la connexion, puis sélectionnez **Modifier la connexion** dans le volet Actions.
3. Vous trouverez ci-dessous les paramètres disponibles lorsque vous modifiez une connexion.
4. Lorsque vous avez terminé, cliquez sur**Appliquer**pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Page **Propriétés de la connexion** :

- Pour modifier l'adresse et les informations d'identification de connexion, sélectionnez **Modifier les paramètres** et entrez de nouvelles informations.
- Pour spécifier les serveurs haute disponibilité pour une connexion XenServer, sélectionnez **Modifier les serveurs HA**. Citrix vous recommande de sélectionner tous les serveurs du pool pour permettre la communication avec XenServer au

© 1999-2017 Citrix Systems, Inc. All rights reserved.

cas où le pool principal échoue.

Page **Avancé** :

Pour un type de connexion Microsoft System Center Configuration Manager (ConfMgr) Wake on LAN, qui est utilisé avec Remote PC Access, entrez les informations ConfMgr Wake Proxy, des paquets magiques et des transmissions de paquets.

Les paramètres de seuil de limitation vous permettent de spécifier un nombre maximal d'actions d'alimentation autorisées sur une connexion. Ces paramètres peuvent aider lorsque les paramètres de gestion de l'alimentation autorisent trop ou trop peu de machines à démarrer en même temps. Chaque type de connexion possède des valeurs par défaut qui sont appropriées pour la plupart des cas et ne doivent généralement pas être modifiées.

Les paramètres **Actions simultanées (tous types)** et **Mises à jour d'inventaire Personal vDisk simultanées** définissent deux valeurs : le nombre maximal absolu pouvant se produire simultanément sur cette connexion, et un pourcentage maximal de toutes les machines utilisant cette connexion. Vous devez spécifier les deux valeurs, absolue et pourcentage ; la limite réelle appliquée est la plus faible des valeurs.

Par exemple, dans un déploiement de 34 machines, si **Actions simultanées (tous types)** sont définies sur une valeur absolue de 10 et une valeur de pourcentage de 10, la limite réelle appliquée est de 3 (10 pour cent de 34 arrondis au nombre entier le plus proche, qui est inférieure à la valeur absolue de 10 machines).

Le **nombre maximal de nouvelles actions par minute** est un nombre absolu ; il n'existe pas de valeur de pourcentage.

Remarque : entrez les informations dans le champ **Options de connexion** uniquement selon les directives d'un représentant de l'assistance Citrix.

Activer ou désactiver le mode maintenance pour une connexion

Le fait d'activer le mode de maintenance pour une connexion empêche toute nouvelle action d'alimentation d'affecter les machines stockées sur cette connexion. Les utilisateurs ne peuvent pas se connecter à une machine lorsqu'elle est en mode de maintenance. Si les utilisateurs sont déjà connectés, le mode maintenance prend effet lorsqu'ils ferment leur session.

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez la connexion. Pour activer le mode de maintenance, sélectionnez **Activer le mode de maintenance** dans le volet Actions. Pour désactiver le mode de maintenance, sélectionnez **Désactiver le mode de maintenance**.

Vous pouvez également activer ou désactiver le mode de maintenance pour des machines individuelles. De plus, vous pouvez activer ou désactiver le mode de maintenance sur les machines dans les catalogues de machines ou les groupes de mise à disposition.

Supprimer une connexion

Avertissement : la suppression d'une connexion peut entraîner la suppression de nombreuses machines et la perte de données. Assurez-vous que les données utilisateur sur les machines affectées sont sauvegardées ou ne sont plus nécessaires.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Avant de supprimer une connexion, assurez-vous que :

- Tous les utilisateurs ont fermé leur session sur les machines stockées sur la connexion.
- Aucune session utilisateur déconnectée n'est en cours d'exécution.
- Le mode de maintenance est activé pour les machines regroupées et dédiées.
- Toutes les machines des catalogues de machines utilisées par la connexion sont hors tension.

Un catalogue de machines devient inutilisable lorsque vous supprimez une connexion référencée par ce catalogue. Si cette connexion est référencée par un catalogue, vous avez la possibilité de supprimer le catalogue. Avant de supprimer un catalogue, assurez-vous qu'il n'est pas utilisé par d'autres connexions.

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez la connexion, puis sélectionnez **Supprimer la connexion** dans le volet Actions.
3. Si cette connexion possède des machines stockées sur celle-ci, vous êtes invité à indiquer si elles doivent être supprimées. Si elles doivent être supprimées, spécifiez la procédure à suivre pour les comptes d'ordinateurs Active Directory associés.

Renommer ou tester une connexion

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez la connexion puis sélectionnez **Renommer la connexion** ou **Tester la connexion** dans le volet Actions.

Afficher les détails des machines sur une connexion

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez la connexion, puis sélectionnez **Afficher les machines** dans le volet Actions.

Le volet supérieur dresse la liste des machines accessibles via la connexion. Sélectionnez une machine pour afficher les détails correspondants dans le volet inférieur. Les détails de session sont également fournis pour les sessions ouvertes.

Utilisez la fonctionnalité de recherche pour trouver des machines rapidement. Soit sélectionnez une recherche enregistrée dans la liste en haut de la fenêtre, soit créez une nouvelle recherche. Vous pouvez effectuer la recherche en tapant le nom de la machine ou une partie de celui-ci, ou créer une expression que vous utiliserez ensuite dans une recherche avancée. Pour créer une expression, cliquez sur le bouton de **développement**, puis sélectionnez dans les listes de propriétés et d'opérateurs.

Gérer les machines sur une connexion

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez une connexion, puis sélectionnez **Afficher les machines** dans le volet Actions.
3. Sélectionnez l'une des options suivantes dans le volet Actions. Certaines actions risquent de ne pas être disponibles, en fonction de l'état de la machine et le type d'hôte de la connexion.

- **Démarrer** : démarre la machine si celle-ci est hors tension ou suspendue.
- **Suspendre** : pause la machine sans la fermer et actualise la liste de machines.
- **Arrêter** : requiert la fermeture du système d'exploitation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Forcer l'arrêt** : force l'arrêt de la machine et actualise la liste des machines.
- **Redémarrer** : requiert la fermeture du système d'exploitation de la machine, puis redémarrage de la machine. Si le système d'exploitation ne peut pas répondre, le bureau reste dans son état actuel.
- **Activer le mode de maintenance :** arrête temporairement les connexions à une machine. Les utilisateurs ne peuvent pas se connecter à une machine dans cet état. Si les utilisateurs sont connectés, le mode maintenance prend effet lorsqu'ils ferment leur session. (Vous pouvez aussi activer ou désactiver le mode de maintenance sur toutes les machines accessibles via une connexion, comme décrit ci-dessus.)
- **Supprimer du groupe de mise à disposition** : la suppression d'une machine d'un groupe de mise à disposition n'est pas supprimée du catalogue de machines que le groupe de mise à disposition utilise. Vous pouvez supprimer une machine uniquement si aucun utilisateur n'y est connecté ; activez le mode de maintenance pour empêcher temporairement les utilisateurs de se connecter lors de la suppression de la machine.
- **Supprimer** : lorsque vous supprimez une machine, les utilisateurs n'y ont plus accès et la machine disparaît du catalogue de machines. Avant de supprimer une machine, assurez-vous que toutes les données utilisateur sont sauvegardées ou ne sont plus nécessaires. Vous pouvez supprimer une machine uniquement si aucun utilisateur n'y est connecté ; activez le mode de maintenance pour empêcher temporairement les utilisateurs de se connecter lors de la suppression de la machine.

Pour les actions qui impliquent la fermeture de la machine, si la machine ne se ferme pas dans les 10 minutes, elle est mise hors tension. Si Windows tente d'installer des mises à jour durant la fermeture, il y a un risque que la machine soit mise hors tension avant la fin des mises à jour.

Modifier un espace de stockage

Vous pouvez afficher l'état des serveurs utilisés pour stocker les données du système d'exploitation, les données temporaires et les données personnelles (PvD) des machines virtuelles qui utilisent une connexion. Vous pouvez également spécifier les serveurs que vous souhaitez utiliser pour le stockage de chaque type de données.

1. Sélectionnez Configuration > Hébergement dans le volet de navigation de Studio.
2. Sélectionnez la connexion, puis sélectionnez Modifier le stockage dans le volet Actions.
3. Dans le panneau de gauche, sélectionnez le type de données : système d'exploitation, Personal vDisk, ou temporaires.
4. Cochez ou décochez les cases à cocher d'un ou plusieurs périphériques de stockage pour le type de données sélectionné.
5. Cliquez sur OK.

Chaque périphérique de stockage dans la liste inclut son nom et l'état du stockage. Les valeurs d'état du stockage valides sont les suivantes :

- **En cours d'utilisation** : le stockage est utilisée pour la création de nouvelles machines.
- **Remplacé** : le stockage est utilisé uniquement pour des machines existantes. Aucune nouvelle machine ne sera ajoutée à ce stockage.
- **Non utilisé** : le stockage n'est pas utilisé pour la création de machines.

Si vous désactivez la case à cocher d'un périphérique qui est actuellement **en cours d'utilisation**, son état passera à **Remplacé**. Les machines existantes continueront à utiliser ce périphérique de stockage (et peuvent écrire des données dessus), par conséquent, il est possible que cet emplacement atteigne sa pleine capacité même après qu'il cesse d'être utilisé pour la création de nouvelles machines.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Supprimer, renommer ou test des ressources

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez la ressource puis sélectionnez l'entrée appropriée dans le volet Actions : **Supprimer les ressources**, **Renommer les ressources** ou **Tester les ressources**.

Utiliser les connexions IntelliCache pour XenServer

À l'aide d'IntelliCache, les déploiements VDI hébergés sont plus rentables car ils vous permettent d'utiliser une combinaison de stockage partagé et de stockage local. Cela améliore les performances et réduit le trafic réseau. Le stockage local met en cache l'image principale depuis le stockage partagé ; cela réduit le nombre de lectures sur le stockage partagé. Pour les bureaux partagés, les écritures sur les disques de différenciation s'effectuent sur le stockage local sur l'hôte et non sur le stockage partagé.

- Le stockage partagé doit être de type NFS si vous utilisez IntelliCache.
- Citrix vous recommande d'utiliser un périphérique de stockage local à hautes performances pour assurer un transfert de données optimal.

Pour utiliser IntelliCache, vous devez l'activer dans ce produit et XenServer.

- Lors de l'installation de XenServer, sélectionnez **Enable thin provisioning (Optimized storage for XenDesktop)**. Citrix ne prend pas en charge les regroupements mixtes de serveurs avec IntelliCache activé et de serveurs sans IntelliCache activé. Pour plus d'informations, veuillez consulter la documentation de XenServer.
- Dans XenApp et XenDesktop, IntelliCache est désactivé par défaut. Vous pouvez modifier le paramètre uniquement lors de la création d'une connexion XenServer ; vous ne pouvez pas désactiver IntelliCache ultérieurement. Lorsque vous ajoutez une connexion XenServer depuis Studio :
  - Sélectionnez **Partagé** en tant que type de stockage.
  - Sélectionnez la case à cocher **Utiliser IntelliCache**.

Horloges de connexion

Vous pouvez utiliser des paramètres de stratégie permettant de configurer trois horloges de connexion:

- **Minuteur de connexion maximal** : détermine la durée maximale d'une connexion non interrompue entre une machine utilisateur et un bureau virtuel. Utilisez les paramètres de stratégies **Horloge de connexion de session** et **Intervalle d'horloge de connexion de session**.
- **Minuteur de connexion inactif** : détermine la durée pendant laquelle une connexion non interrompue d'une machine utilisateur à un bureau virtuel sera maintenue si aucune entrée utilisateur n'est effectuée. Utilisez les paramètres de stratégie **Horloge inactive de session** et **Intervalle d'horloge inactive de session**.
- **Horloge de déconnexion** : détermine la durée pendant laquelle un bureau virtuel déconnecté et verrouillé peut rester verrouillé avant que la session ne se ferme. Utilisez les paramètres de stratégie **Horloge de session déconnectée** et **Intervalle d'horloge de session déconnectée**.

Lorsque vous mettez à jour l'un de ces paramètres, vous devez vous assurer qu'ils sont cohérents sur votre déploiement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Consultez la documentation sur les paramètres de stratégie pour plus d'informations.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Location de connexions

Jul 07, 2016

Pour vous assurer que la base de données du site est toujours disponible, Citrix recommande de commencer par un déploiement SQL Server ayant une tolérance aux pannes en suivant la haute disponibilité des meilleures pratiques de Microsoft. Cependant, les problèmes et les interruptions réseau peuvent empêcher les Delivery Controller d'accéder à la base de données, ce qui fait que des utilisateurs ne vont pas pouvoir se connecter à leurs applications ou bureaux.

La fonctionnalité de location de connexion complète les meilleures pratiques de la haute disponibilité du serveur SQL Server en permettant aux utilisateurs de se connecter et de se reconnecter à leurs applications et bureaux les plus récemment utilisés, même lorsque la base de données du site n'est pas disponible.

Bien que les utilisateurs puissent posséder un nombre important de ressources publiées disponibles, ils n'utilisent souvent que quelques-unes régulièrement. Lorsque vous activez la location de connexion, chaque Controller met en cache les connexions utilisateur vers les applications et bureaux utilisés récemment lors d'opérations normales (lorsque la base de données est disponible).

Les baux générés sur chaque Controller sont téléchargées vers la base de données du site pour la synchronisation périodique vers d'autres Controller du site. Outre le bail, chaque Controller du cache contient l'application, le bureau, l'icône et les informations du travailleur. Le bail et les informations associées sont stockés sur le disque local de chaque Controller. Si la base de données devient indisponible, le Controller entre en mode de connexion de location et « relit » les opérations de mise en cache lorsqu'un utilisateur tente de se connecter ou se reconnecter à une application ou d'un bureau récemment utilisé(e) depuis StoreFront.

Les connexions sont mises en cache pour une période de bail de deux semaines. Par conséquent, si la base de données devient non disponible, les bureaux et les applications qui ont été lancés par l'utilisateur dans les deux semaines précédentes restent accessibles pour cet utilisateur via StoreFront. Toutefois, des bureaux et des applications qui n'ont pas été lancés pendant la dernière période de bail de deux semaines ne sont pas accessibles lorsque la base de données n'est pas disponible. Par exemple, si une application a été lancée par un utilisateur il y a trois semaines, son bail a expiré et l'application ne peut pas être lancée par cet utilisateur si la base de données devient désormais indisponible. Les baux de sessions actives de longue durée, ou d'application de déconnexion ou de sessions de bureaux sont étendus afin de ne pas être considérés comme expiré.

Par défaut, la location de connexion affecte l'ensemble du site ; cependant, vous pouvez révoquer tous les baux pour certains utilisateurs, ce qui leur évite d'accéder à des applications ou des bureaux lorsque le Controller se trouve en mode de connexion louée. Plusieurs autres paramètres du Registre s'appliquent sur une base de Controller.

Tandis que la location de connexion peut améliorer la résilience de connexion et la productivité des utilisateurs, il existe des considérations relatives à la disponibilité, opération, et performances d'autres fonctionnalités.

La location de connexion est prise en charge pour les applications et les bureaux hébergés sur le serveur et les bureaux statiques (attribués) ; elle n'est pas prise en charge pour les bureaux VDI regroupés ou pour les utilisateurs qui n'ont pas été attribués à un bureau lorsque la base de données devient indisponible.

Lorsque le Controller se trouve en mode de connexion loué :

- Les administrateurs ne peuvent pas utiliser Studio, Director, ou la console PowerShell.
- Le contrôle de l'espace de travail n'est pas disponible. Lorsqu'un utilisateur ouvre une session sur Citrix Receiver, les

© 1999-2017 Citrix Systems, Inc. All rights reserved.

sessions ne sont pas automatiquement reconnectées, l'utilisateur doit redémarrer l'application.

- Si un nouveau bail est créé avant que la base de données ne devienne indisponible, mais que les informations de bail n'ont pas encore été synchronisées entre les Controller, l'utilisateur peut ne pas être en mesure de démarrer cette ressource après que la base de données soit devenue indisponible.
- Les utilisateurs d'applications et de bureaux hébergés sur le serveur peuvent utiliser plus de sessions que leurs limites de session configurées. Par exemple :
  - Une session ne peut pas itinérer lorsqu'un utilisateur la démarre à partir d'une machine (connexion au travers de NetScaler Gateway) lorsque le Controller ne se trouve pas en mode de connexion loué puis se connecte à partir d'une autre machine sur le réseau local où le contrôleur se trouve en mode de connexion loué.
  - La reconnexion de session peut échouer si une application démarre juste avant que la base de données ne devienne indisponible ; dans ce cas, une nouvelle session et instance d'application sont lancées.
- L'alimentation des bureaux statiques (attribués) n'est pas gérée. Les VDA qui sont mis hors tension lorsque le Controller entre en mode de connexion loué restent indisponibles tant que la connexion à la base de données n'est pas restaurée, sauf si l'administrateur les place manuellement sous tension.
- Si le pré-lancement de session et la persistance de session sont activés, les nouvelles sessions de pré-lancement ne sont pas démarrés. Le pré-lancement de session et la persistance de session ne seront pas terminés selon les seuils configurés alors que la base de données n'est pas disponible.
- La gestion de la charge dans le site peut être affectée. Les connexions de serveur sont routées vers le VDA le plus récemment utilisé. Les calculateurs de charge (et plus particulièrement les règles du nombre de sessions) risquent d'être dépassés.
- Le Controller n'entrera pas en mode de connexion louée si vous utilisez SQL Server Management Studio pour mettre la base de données hors connexion. Au lieu de cela, utilisez l'une des instructions Transact-SQL suivantes :
  - ALTER DATABASE <nom-base-de-données> SET OFFLINE WITH ROLLBACK IMMEDIATE
  - ALTER DATABASE <nom-base-de-données> SET OFFLINE WITH ROLLBACK AFTER <secondes>

  Les deux instructions annulent toutes les transactions en attente et provoquent la perte de sa connexion à la base de données par le Controller. Le Controller entre alors en mode de connexion louée.

Lorsque la location de connexion est activée, il existe deux brefs intervalles de temps pendant lesquels les utilisateurs ne peuvent pas se connecter ou se reconnecter : (1) du moment où la base de données devient indisponible au moment où le Controller entre en mode de connexion louée, et (2) du moment où le Controller change d'un mode de connexion louée au moment où l'accès à la base de données est entièrement restauré et les VDA ont se sont réinscrits.

Si vous configurez une valeur autre que la valeur par défaut d'itinérance de session, la reconnexion de session retourne à sa valeur par défaut lorsqu'un Controller entre en mode de location de connexion. Pour de plus amples informations, consultez la section Location de connexion et itinérance de session.

Consultez l'article Zones pour de plus amples informations sur l'emplacement où les données de location de connexion sont conservées.

Pour de plus amples informations, consultez la rubrique Considérations à prendre en compte lors de la conception d'une location de connexion XenDesktop 7.6.

Lors de la configuration de votre déploiement pour prendre en charge la location de connexion :

- La version des VDA doit être de 7.6 au minimum et les catalogues de machines et groupes de mise à disposition qui utilisent ces machines doivent être à ce niveau minimum (ou une version ultérieure prise en charge).
- La taille de la base de données du site augmentera.
- Chaque Controller a besoin de plus d'espace disque pour la mise en cache des fichiers du bail.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

La location de connexion est activée par défaut.

Vous pouvez activer ou désactiver la location de connexion à partir du kit de développement PowerShell ou du Registre. Depuis le kit de développement PowerShell, vous pouvez également supprimer des baux d'en cours. Les applets de commande PowerShell suivantes affectent la location des connexions ; voir l'aide de l'applet de commande pour plus de détails.

- Set-BrokerSite -ConnectionLeasingEnabled $true|$false - Active ou désactive la fonction de location de connexion. Valeur par défaut = $true
- Get-BrokerServiceAddedCapability - Place « ConnectionLeasing » à l'emplacement spécifié pour le Controller local.
- Get-BrokerLease - Récupère l'ensemble (ou une série filtrée) des baux actuels.
- Remove-BrokerLease - Marque un bail ou une série filtrée de baux pour suppression.
- Update-BrokerLocalLeaseCache – Met à jour le cache de location de connexion sur le Controller local. Les données sont resynchronisées lors de la prochaine opération de synchronisation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Adresses IP virtuelles et bouclage virtuel

Jul 07, 2016

Remarque : ces fonctionnalités ne sont valides que pour les machines Windows Server 2008 R2 et Windows Server 2012 R2. Elles ne s'appliquent pas aux machines avec OS de bureau Windows.

La fonctionnalité d'adresse IP virtuelle Microsoft fournit une application publiée avec une adresse IP unique attribuée dynamiquement à chaque session. La fonctionnalité de bouclage virtuel Citrix vous permet également de configurer des applications qui dépendent des communications avec localhost (127.0.0.1 par défaut) pour utiliser une adresse de bouclage virtuel unique dans la plage localhost (127.*).

Certaines applications, telles que les applications de type CRM ou CTI (Computer Telephony Integration), utilisent une adresse IP pour l'adressage, l'identification, les licences, ou à d'autres fins. Elles nécessitent par conséquent des sessions à adresse IP unique ou adresse de bouclage. D'autres applications peuvent se lier à un port statique, c'est pourquoi les tentatives de démarrage des instances d'une application dans un environnement multi-utilisateur échoueront car le port est déjà utilisé. Pour assurer un fonctionnement correct de ces applications dans l'environnement XenApp, chaque machine nécessite une adresse IP unique.

Les adresses IP virtuelles et le bouclage virtuel sont des fonctionnalités indépendantes. Vous pouvez sélectionnez ces deux options ou l'une ou l'autre.

Résumé des actions de l'administrateur :

- Pour utiliser l'adresse IP virtuelle Microsoft, activez et configurez-la sur le serveur Windows.
- Pour utiliser le bouclage virtuel Citrix, configurez deux paramètres dans une stratégie Citrix.

Lorsque l'adresse IP virtuelle est activée et configurée sur le serveur Windows, chaque application configurée en cours d'exécution dans une session dispose d'une adresse unique. Les utilisateurs peuvent accéder à ces applications sur un serveur XenApp comme ils accèdent à toute autre application publiée. Un processus nécessite une adresse IP virtuelle dans les cas suivants :

- Le processus utilise un numéro de port TCP fixe
- Le processus utilise des sockets Windows et nécessite une adresse IP unique ou un numéro de port TCP spécifié

Pour déterminer si une application doit utiliser des adresses IP virtuelles :

1. Obtenez l'outil TCP View auprès de Microsoft. Cet outil répertorie toutes les applications liées à des adresses IP et ports spécifiques.
2. Désactivez la fonction Résoudre les adresses IP afin de visualiser les adresses au lieu des noms d'hôtes.
3. Lancez l'application et utilisez l'outil TCPView pour voir quelles adresses IP et ports sont ouverts par celle-ci ainsi que les noms des processus qui ouvrent ces ports.
4. Configurez tous les processus qui ouvrent l'adresse IP du serveur, 0.0.0.0 ou 127.0.0.1.
5. Lancez une autre instance de l'application afin de vous assurer qu'elle n'ouvre pas la même adresse IP sur un port différent.

Comment la virtualisation IP des services Bureau à distance Microsoft (RD) fonctionne-t-elle ?

- L'adressage IP virtuel doit être activé sur le serveur Microsoft.
  Par exemple, dans un environnement Windows Server 2008 R2, à partir du Gestionnaire de serveur, développez Services Bureau à distance > Connexions hôtes de session Bureau à distance pour activer la fonctionnalité de virtualisation IP des services Bureau à distance et configurer les paramètres pour attribuer dynamiquement des adresses IP à l'aide du serveur

© 1999-2017 Citrix Systems, Inc. All rights reserved.

DHCP (Dynamic Host Configuration Protocol) par session ou par programme. Consultez la documentation Microsoft pour obtenir des instructions.

- Lorsque cette fonctionnalité est activée, au démarrage de la session, le serveur demande des adresses IP attribuées dynamiquement auprès du serveur DHCP.
- La fonctionnalité de virtualisation IP des services Bureau à distance attribue les adresses IP aux connexions Bureau à distance par session ou par programme. Si vous attribuez des adresses IP à de multiples programmes, ces derniers partagent une adresse IP par session.
- Après attribution d'une adresse à une session, celle-ci utilise cette adresse virtuelle plutôt que l'adresse IP principale du système en présence des appels suivants : bind¸closesocket¸connect, WSAConnect, WSAAccept, getpeername, getsockname, sendto, WSASendTo, WSASocketW, gethostbyaddr, getnameinfo, getaddrinfo

Lors de l'utilisation de la fonctionnalité de virtualisation d'adresses IP de Microsoft dans la configuration d'hôte de session Bureau à distance, les applications sont liées à des adresses IP spécifiques par l'insertion d'un composant « filtre » entre l'application et les appels de fonction Winsock. L'application ne voit ensuite que l'adresse IP qu'elle doit utiliser. Toute tentative d'écoute de communications TCP ou UDP par l'application est liée à l'adresse IP virtuelle (ou adresse de bouclage) qui lui est attribuée automatiquement. Toutes les connexions ouvertes par l'application sont établies au départ par l'adresse IP liée à l'application.

Pour les fonctions qui renvoient une adresse, telle que GetAddrInfo() (contrôlée par une stratégie Windows) si l'adresse IP de l'hôte local est demandée, la fonctionnalité d'adresse IP virtuelle intercepte l'adresse IP retournée et la remplace par l'adresse IP virtuelle de la session. Les applications qui tentent d'obtenir l'adresse IP du serveur local à travers ce type de fonctions de nom n'obtiennent que l'adresse IP virtuelle unique attribuée à la session. Cette adresse IP est souvent utilisée dans les appels de socket suivants, tels que bind ou connect.

Une application demande souvent à se lier à un port pour procéder à une écoute de l'adresse « 0.0.0.0 ». Lorsque c'est le cas et qu'une application utilise un port statique, vous ne pouvez pas ouvrir plus d'une instance de celle-ci. La fonction d'adresse IP virtuelle recherche également 0.0.0.0 dans ces types d'appels et modifie l'appel en écoute sur l'adresse IP virtuelle spécifique, ce qui permet à plusieurs applications d'écouter sur le même port sur le même ordinateur, car ils effectuent l'écoute sur des adresses différentes. Cette écoute est uniquement modifiée si une session ICA et la fonction d'adresse IP virtuelle sont activées. Par exemple, si deux instances d'une application exécutée dans des sessions différentes tentent toutes deux de se lier à toutes les interfaces (0.0.0.0) et à un port spécifique (comme 9000), elles sont liées à VIPAddress1:9000 et VIPAddress2:9000, sans aucun conflit.

L'activation des paramètres de stratégie d'adresse IP virtuelle Citrix permettent à chaque session de disposer de sa propre adresse de bouclage pour les communications. Lorsqu'une application utilise l'adresse de l'hôte local (127.0.0.1 par défaut) dans un appel Winsock, la fonctionnalité de bouclage virtuel remplace simplement 127.0.0.1 par 127.X.X.X (où X.X.X représente l'identificateur de session + 1). Par exemple, 127.0.0.8. pour un ID session de 7. Dans le cas peu probable où l'ID session dépasse le quatrième octet (plus de 255), l'adresse passe à l'octet suivant (127.0.1.0), jusqu'à 127.255.255.255 maximum.

Un processus nécessite le bouclage virtuel dans l'un des cas suivants :
- Le processus utilise l'adresse de bouclage de socket Windows 127.0.0.1 (localhost)
- Le processus utilise un numéro de port TCP fixe

Utilisez les paramètres de stratégie de bouclage virtuel pour les applications qui utilisent une adresse de bouclage pour la communication entre les processus. Aucune configuration supplémentaire n'est requise. Le bouclage virtuel n'a pas de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

dépendance à l'égard des adresses IP virtuelles, de sorte que vous n'avez pas à configurer le serveur Microsoft.

- Prise en charge du bouclage d'adresse IP virtuelle. Lorsqu'il est activé, ce paramètre de stratégie permet à chaque session de disposer de sa propre adresse de bouclage virtuel. Cette option est désactivée par défaut. Cette fonctionnalité ne s'applique qu'aux applications spécifiées avec le paramètre de stratégie Liste de programmes de bouclage virtuel d'adresse IP virtuelle.
- Liste de programmes de bouclage virtuel d'adresse IP virtuelle. Ce paramètre de stratégie spécifie les applications qui utilisent la fonctionnalité de bouclage d'adresse IP virtuelle. Ce paramètre ne s'applique que lorsque le paramètre de stratégie de prise en charge du bouclage d'adresse IP virtuelle est activé.

Autres fonctionnalités

Vous pouvez utiliser les paramètres de registre suivants pour vous assurer que le bouclage virtuel est préféré aux adresses IP virtuelles ; cela s'appelle un bouclage par défaut. Soyez, toutefois, prudent :

- Le bouclage par défaut est pris en charge sur Windows 2008 R2 uniquement.
- Utilisez le bouclage par défaut uniquement si les adresses IP virtuelles et le bouclage virtuel sont activés ; sinon, vous risquez d'obtenir des résultats inattendus.
- La modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

Exécutez regedit sur les serveurs sur lesquels les applications résident.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP (HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VIP pour machines 32 bits)
- Nom : PreferLoopback, Type : REG_DWORD, Données : 1
- Nom : PreferLoopbackProcesses, Type : REG_MULTI_SZ, Données :<liste des processus>.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Delivery Controller

Aug 22, 2016

Le Delivery Controller est le composant côté serveur qui est responsable de la gestion de l'accès utilisateur, ainsi que de la négociation et de l'optimisation des connexions. Les Controller fournissent également les services Machine Creation qui créent des images de bureau et de serveur.

Un site doit avoir au moins un Controller. Après avoir installé le Controller initial, vous pouvez ajouter des Controller supplémentaires lorsque vous créez un site, ou plus tard. Avoir plus d'un Controller dans un site présente deux avantages.

- Redondance : Il est recommandé qu'un site de production doive toujours disposer d'au moins deux Controller sur des serveurs physiques différents. Si un Controller échoue, les autres peuvent gérer les connexions et administrer le site.
- Évolutivité : au fur et à mesure que l'activité du site augmente, il en va de même pour l'utilisation de l'UC sur le Controller et l'activité de la base de données. Les Controller supplémentaires permettent de gérer plus d'utilisateurs et plus de demandes d'applications et de bureaux, et peuvent améliorer la réactivité générale.

Chaque Controller communique directement avec la base de données du site. Dans un site avec plusieurs zones, les Controller de chaque zone communiquent avec la base de données du site dans la zone principale.

Conseil : ne modifiez pas le nom de l'ordinateur ou l'appartenance à un domaine d'un Controller une fois que le site est configuré.

Comment les VDA découvrent les Controller

Avant qu'un VDA puisse être utilisé, il doit s'enregistrer (établir la communication) auprès d'un Controller sur le site. Le VDA trouve un Controller en vérifiant une liste de Controller appelée ListofDDCs. La liste ListOfDDCs se compose d'une ou plusieurs entrées DNS ou adresses IP qui pointent le VDA vers des Controller sur le site. Pour assurer l'équilibrage de charge, le VDA répartit automatiquement les connexions de manière équitable entre les Controller dans la liste.

En plus de la liste ListOfDDCs, ListOfSIDs indique les ID de sécurité (SID) de machine qui sont autorisés à contacter le VDA en tant que Controller. La liste ListOfSIDs peut être utilisée pour réduire la charge sur Active Directory ou pour éviter des menaces de sécurité provenant d'un serveur DNS non fiable.

Il est important de s'assurer que les listes ListOfSIDs et ListOfDDCs sur tous les VDA contiennent des informations à jour à mesure que des Controller sont ajoutés et supprimés dans le site. Si les listes ne sont pas mises à jour, un VDA risque de rejeter les sessions qui ont été négociées par un Controller non répertorié. La présence d'entrées non valides peut retarder le démarrage du logiciel système du bureau virtuel. Pour conserver les listes à jour, vous pouvez :

- Utiliser la fonctionnalité de mise à jour automatique, qui met automatiquement à jour les listes ListOfDDCs et ListOfSIDs à mesure que des Controller sont ajoutés ou supprimés. Par défaut, la mise à jour automatique est activée.
- Auto gérer : c'est-à-dire mettre à jour manuellement les paramètres de stratégie ou de registre qui identifient les Controller.

Les informations contenues dans les listes ListOfDDCs et ListOfSIDs peuvent provenir de plusieurs endroits dans un déploiement. Le VDA vérifie les emplacements suivants, dans l'ordre, et stoppe au premier dans lequel il trouve les listes :

1. Un emplacement de stockage persistant dont la maintenance est assurée pour la fonctionnalité de mise à jour

© 1999-2017 Citrix Systems, Inc. All rights reserved.

automatique. Cet emplacement contient des informations sur le Controller lorsque la fonctionnalité de mise à jour automatique est activée et après que le VDA s'enregistre avec succès pour la première fois après l'installation. (Ce stockage contient également des informations sur la stratégie de machine, ce qui garantit que les paramètres de stratégie sont conservés après les redémarrages). Pour son enregistrement initial après l'installation, ou lorsque la mise à jour automatique est désactivée, le VDA vérifie les emplacements suivants.

2. Les paramètres de stratégie (Controller, SID de Controller).
3. Les informations sur le Controller sous la clé Virtual Desktop Agent dans le Registre. Le programme d'installation de VDA renseigne initialement ces valeurs, en fonction des informations sur le Controller que vous spécifiez lors de l'installation du VDA.
4. Découverte de Controller basée sur l'unité d'organisation. Ceci est une méthode héritée conservée pour des raisons de rétrocompatibilité.
5. Le fichier Personality.ini créé par Machine Creation Services.

Si une liste ListOfDDCs spécifie plusieurs Controller, le VDA tente de s'y connecter aléatoirement. La liste ListOfDDCs peut également contenir des groupes de Controller, qui sont désignés par des crochets entourant deux ou plusieurs entrées de Controller. Le VDA tente de se connecter à chaque Controller dans un groupe avant de passer à d'autres entrées dans la liste ListOfDDCs.

Pour les utilisateurs XenDesktop qui ont été mis à niveau à partir de versions antérieures à la version 7.0, la fonctionnalité de mise à jour automatique remplace la fonction CNAME à partir de la version antérieure. Vous pouvez réactiver manuellement la fonction CNAME, si désiré ; cependant, pour que l'alias DNS fonctionne de manière cohérente, vous ne pouvez pas utiliser la fonctionnalité de mise à jour automatique et la fonction CNAME en même temps. Consultez l'article CTX137960 pour plus d'informations sur la réactivation de la fonctionnalité CNAME.

Consultez l'article *Zones* pour de plus amples informations sur l'emplacement où le VDA tente de s'enregistrer dans un site qui dispose de plusieurs zones.

Considérations à prendre en compte lors du choix de la mise à jour automatique ou de l'auto-gestion

Le paramètre de stratégie qui active/désactive la mise à jour automatique est activé par défaut.

Les types de déploiements suivants ne peuvent pas utiliser la mise à jour automatique et doivent être gérés de façon autonome.

- Déploiements qui utilisent des groupes de Controller.
- Déploiements qui utilisent des listes ListOfSIDs pour des raisons de sécurité. (Les déploiements qui utilisent ListOfSIDs pour réduire la charge Active Directory peuvent utiliser la mise à jour automatique).
- Déploiements qui utilisent Provisioning Services sans disque d'écriture conditionnelle.
- Déploiements qui utilisent le paramètre de stratégie des Controller ou SID de Controller.

Mise à jour automatique

Le paramètre de stratégie *Activer la mise à jour automatique des Delivery Controller* est situé dans la catégorie Virtual Delivery Agent. Pour activer la mise à jour automatique, activez le paramètre de stratégie ; il s'agit de la valeur par défaut.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour désactiver la mise à jour automatique, désactivez le paramètre de stratégie.

Lorsque la mise à jour automatique est activée et que vous installez un VDA, le VDA tente de s'enregistrer avec les valeurs d'un Controller que vous avez spécifié lorsque vous avez installé le VDA. Le programme d'installation enregistre les informations Delivery Controller que vous spécifiez pendant l'installation de VDA à la valeur de Registre ListOfDDCs.

Après l'enregistrement du VDA, le Controller auprès duquel il est enregistré envoie une liste des noms de domaine complets des Controller et des ID de sécurité (SID) au VDA. Le VDA écrit cette liste sur le stockage persistant de mise à jour automatique. Chaque Controller vérifie également la base de données de configuration de site toutes les 90 minutes pour des informations Controller : si un Controller a été ajouté ou supprimé depuis la dernière vérification ou si une modification de stratégie s'est produite, le Controller envoie les listes mises à jour au VDA auprès duquel il est enregistré. Le VDA acceptera les connexions provenant de tous les Controller figurant dans la dernière liste reçue.

Si un VDA reçoit une liste qui ne comprend pas le Controller auprès duquel il est enregistré (en d'autres termes, ce Controller a été supprimé du site), le VDA s'enregistre de nouveau, en choisissant parmi les Controller dans la liste. Après qu'un VDA s'enregistre ou se réenregistre, il reçoit une liste à jour.

Par exemple :

1. Un déploiement dispose de trois Controller : A B et C. Un VDA est installé et s'enregistre auprès du Controller B (qui a été spécifié lors de l'installation du VDA).
2. Deux Controller (D et E) sont ajoutés au site. Dans les 90 minutes qui suivent, le VDA recevra les listes mises à jour et acceptera les connexions provenant des Controller A, B, C, D et E. (La charge ne seront pas répartie de manière égale sur tous les Controller tant que les VDA ne sont pas redémarrés.)
3. Le Controller B est supprimé du site. Dans les 90 minutes qui suivent, le VDA recevra les listes mises à jour car un Controller a été modifié depuis la dernière vérification. Le VDA installé dans l'étape 1 est enregistré auprès du Controller B, qui ne figure plus sur la liste, si bien que ce VDA se réenregistre en choisissant parmi les Controller disponibles dans la liste actuelle (A, C, D et E).

Autogestion

Si vous n'utilisez pas la mise à jour automatique, vous devez mettre à jour le paramètre de stratégie Citrix ou les valeurs de registre de chaque VDA du site après avoir ajouté, déplacé ou supprimé les Delivery Controller dans le site. Les modifications apportées au registre peuvent également être mises à jour à l'aide d'un objet de stratégie de groupe.

Pour pratiquer l'autogestion à l'aide de paramètres de stratégie Citrix

1. Mettez à jour les valeurs des noms de domaine complets spécifiées dans le paramètre de stratégie Controller. Ce paramètre de stratégie est situé dans la catégorie Virtual Delivery Agent.
2. Si vous utilisez également une liste ListOfSIDs dans votre déploiement, vous devez mettre à jour les valeurs de SID spécifiées dans le paramètre SIDspolicy du Controller.

Pour pratiquer l'autogestion à l'aide du registre :

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Mettez à jour la clé de registre ListOfDDCs, qui répertorie les noms de domaine complets de tous les Controller du site. (Cette clé est l'équivalent de l'unité d'organisation du site Active Directory.) Séparez les valeurs multiples par des espaces. Entourez les groupes Controller avec crochets.
   HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)

   Si l'emplacement de registre HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent contient les clés ListOfDDCs et FarmGUID, ListOfDDCs est utilisée pour la découverte de Controller ; La clé FarmGUID est présente si une unité d'organisation de site a été spécifiée lors de l'installation du VDA.

2. Si vous le souhaitez, vous pouvez mettre à jour la clé de registre ListOfSIDs :
   HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)

Ajouter, supprimer ou déplacer des Delivery Controller

Pour ajouter, supprimer ou déplacer un Controller, vous devez disposer des autorisations de rôle de serveur et de rôle de base de données répertoriées dans l'article *Bases de données*.

Remarque : l'installation d'un Controller sur un nœud dans une installation de mise en cluster SQL ou mise en miroir SQL n'est pas prise en charge.

Si votre déploiement utilise la mise en miroir de base de données :

- Avant l'ajout, la suppression ou le déplacement d'un Controller, assurez-vous que les bases de données principale et en miroir sont en cours d'exécution. En outre, si vous utilisez les scripts avec SQL Server Management Studio, activez le mode SQLCMD avant d'exécuter les scripts.
- Pour vérifier la mise en miroir après ajout, suppression ou déplacement d'un Delivery Controller, exécutez l'applet de commande PowerShell **get-configdbconnection** pour vous assurer que le partenaire de basculement a été défini dans la chaîne de connexion sur le miroir.

Après avoir ajouté, supprimé ou déplacé un Delivery Controller :

- Si la mise à jour automatique est activée, les VDA recevront une liste actualisée des Delivery Controller dans les 90 minutes qui suivent.
- Si la mise à jour automatique n'est pas activée, vérifiez que le paramètre de stratégie du Delivery Controller ou la clé de registre ListOfDDCs sont mis à jour pour tous les VDA. Après déplacement d'un Delivery Controller vers un autre site, mettez à jour le paramètre de stratégie ou la clé de registre sur les deux sites.

Vous pouvez ajouter des Controller lorsque vous créez un site et ultérieurement. Vous ne pouvez pas ajouter des Controller installés avec une version antérieure de ce logiciel à un site qui a été créé avec cette version.

1. Exécutez le programme d'installation sur un serveur contenant un système d'exploitation pris en charge. Installez le composant Delivery Controller et les autres composants principaux requis. Suivez les instructions de l'assistant d'installation.
2. Si vous n'avez pas encore créé de site, démarrez Studio ; vous êtes invité à créer un site. Sur la page Bases de données de l'Assistant de création de site, cliquez sur le bouton Sélectionner et ajoutez l'adresse du serveur sur lequel vous avez installé le Controller supplémentaire. **Important :** si vous souhaitez générer des scripts qui initialiseront les bases de données, ajoutez les Controller avant de générer les scripts.
3. Si vous avez déjà créé un site, pointez Studio vers le serveur sur lequel vous avez installé le Controller supplémentaire. Cliquez sur **Adapter votre déploiement** et entrez l'adresse du site.

La suppression d'un Delivery Controller d'un site n'entraîne pas la désinstallation du logiciel Citrix ou de tout autre composant ; elle supprime le Delivery Controller de la base de données afin qu'il ne puisse plus être utilisé pour les connexions du broker et pour effectuer d'autres tâches. Si vous supprimez un Delivery Controller, vous pouvez le rajouter par la suite au même site ou à un autre site. Un site a besoin d'au moins un Delivery Controller ; vous ne pouvez donc pas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

supprimer le dernier Delivery Controller répertorié dans Studio.

Lorsque vous supprimez un Controller d'un site, l'ouverture de session Controller sur le serveur de base de données n'est pas supprimée. Cela évite potentiellement la suppression d'une ouverture de session utilisée par des services d'autres produits sur la même machine. L'ouverture de session doit être supprimée manuellement si elle n'est plus requise ; l'autorisation de rôle de serveur securityadmin est nécessaire pour la supprimer.

Important : ne supprimez pas le Controller depuis Active Directory tant que vous ne l'avez pas supprimé du site.

1. Assurez-vous que le Controller est sous tension afin que Studio puisse se charger en moins d'une heure. Une fois que Studio charge le Controller que vous souhaitez supprimer, placez-le Controller hors tension lorsque vous y êtes invité.
2. Sélectionnez **Configuration > Delivery Controller** dans le panneau de navigation Studio, puis sélectionnez le Controller que vous voulez supprimer.
3. Cliquez sur **Supprimer le Controller** dans le volet Actions. Si vous ne possédez pas les droits et les rôles de base de données appropriés, vous pouvez générer un script qui permet à votre administrateur de base de données de supprimer le Delivery Controller à votre place.
4. Vous devrez peut-être supprimer le compte machine du Delivery Controller du serveur de base de données. Avant de procéder de la sorte, vérifiez qu'aucun autre service n'utilise le compte.

Après utilisation de Studio pour supprimer un Controller, le trafic vers ce Controller peut rester affiché pour un laps de temps pour assurer le bon d'achèvement des tâches courantes. Si vous souhaitez forcer la suppression d'un Controller dans un bref délai, Citrix vous recommande de fermer le serveur sur lequel il a été installé, ou de supprimer ce serveur à partir d'Active Directory. Ensuite, redémarrez les autres Controller du site pour vous assurer qu'aucune autre communication avec le Controller supprimé n'est réalisée.

Si votre site contient plusieurs zones, vous pouvez déplacer un Controller vers une autre zone. Consultez l'article *Zones* pour savoir comment cela peut affecter l'enregistrement du VDA et d'autres opérations.

1. Sélectionnez **Configuration > Delivery Controller** dans le panneau de navigation Studio, puis sélectionnez le Controller que vous voulez déplacer.
2. Sélectionnez **Déplacer** dans le volet Actions.
3. Spécifiez la zone vers laquelle vous souhaitez déplacer le Controller.

Vous ne pouvez pas déplacer un Delivery Controller vers un site qui a été créé avec une version antérieure de ce logiciel.

1. Sur le site dans lequel figure le Controller (l'ancien site), sélectionnez **Configuration > Delivery Controller** dans le panneau de navigation de Studio, puis sélectionnez le Controller que vous souhaitez déplacer.
2. Cliquez sur **Supprimer le Controller** dans le volet Actions. Si vous ne possédez pas les droits et les rôles de base de données appropriés, vous pouvez générer un script qui permet à un utilisateur disposant de ces autorisations (tel qu'un administrateur de base de données) de supprimer le Delivery Controller à votre place. Un site a besoin d'au moins un Delivery Controller ; vous ne pouvez donc pas supprimer le dernier Delivery Controller répertorié dans Studio.
3. Sur le Controller que vous déplacez, ouvrez Studio, réinitialisez les services lorsque vous y êtes invité, cliquez sur **Joindre un site existant** et saisissez l'adresse du nouveau site.

Si un VDA a été provisionné à l'aide de Provisioning Services ou qu'il est une image existante, vous pouvez déplacer un VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

vers un autre site (d'un site 1 au site 2) lors de la mise à niveau, ou lors du déplacement d'une image de VDA qui a été créée dans un site test vers un site de production. Les VDA provisionnés à l'aide de Machine Creation Services (MCS) ne peuvent pas être déplacés d'un site à un autre car MCS ne prend pas en charge la modification des listes ListOfDDC que VDA vérifie pour s'enregistrer auprès d'un Controller ; les VDA provisionnés à l'aide de MCS vérifient toujours les listes ListOfDDC associées au site dans lequel ils ont été créés.

Il existe deux façons de déplacer un VDA vers un autre site : à l'aide du programme d'installation ou de stratégies Citrix.

Programme d'installation : exécutez le programme d'installation et ajoutez un Controller, en spécifiant le nom complet (entrée DNS) d'un Controller du site 2. **Important** : ne spécifiez les Controller dans le programme d'installation que lorsque le paramètre de stratégie des Controller n'est pas utilisé.

Éditeur de stratégie de groupe : l'exemple suivant déplace plusieurs VDA entre sites.

1. Créez une stratégie dans le site 1 qui contient les paramètres suivants, puis filtrez la stratégie au niveau du groupe de mise à disposition pour initier une migration VDA échelonnée entre les sites.
   Controller : contenant les noms complets (entrées DNS) d'un ou de plusieurs Controller dans le site 2.
   Activer la mise à jour automatique des Controller : défini sur désactivé.
2. Chaque VDA dans le groupe de mise à disposition reçoit une alerte dans les 90 minutes qui suivent la création de la nouvelle stratégie. Le VDA ignore la liste de Controller qu'il reçoit (car la mise à jour automatique est désactivée) : il sélectionne l'un des Controller spécifiés dans la stratégie, qui répertorie les Controller du site 2.
3. Lorsque le VDA s'enregistre avec succès auprès d'un Controller du site 2, il reçoit la liste ListOfDDCs du site 2 et les informations de stratégie, dans laquelle la mise à jour automatique est activée par défaut. Étant donné que le Controller auquel duquel le VDA s'est enregistré dans le site 1 ne figure pas sur la liste envoyée par le Controller du site 2, le VDA se réenregistre, en choisissant parmi les Controller de la liste du site 2. Dès lors, le VDA est automatiquement mis à jour avec les informations du site 2.

Découverte de Controller basée sur unité d'organisation Active Directory

Cette méthode de découverte Delivery Controller est prise en charge principalement pour la rétrocompatibilité, et est uniquement valide pour les Virtual Delivery Agent (VDA) pour OS Windows Desktop, et non pour les VDA pour OS Windows Desktop. La découverte basée sur Active Directory exige que tous les ordinateurs d'un site soient membres d'un domaine ; par ailleurs, le domaine utilisé par le Controller doit entretenir des relations de confiance avec le ou les domaines utilisés par les bureaux. Si vous utilisez cette méthode, vous devez configurer le GUID de l'unité d'organisation dans chaque registre de bureau.

Pour effectuer une découverte de Controller basée sur l'unité d'organisation, exécutez le script PowerShell Set-ADControllerDiscovery.ps1 sur le Controller (chaque Controller contient ce script dans le dossier $Env:ProgramFiles\Citrix\Broker\Service\Setup Scripts). Pour exécuter le script, vous devez disposer des autorisations CreateChild sur une unité d'organisation parente, ainsi que des droits d'administration complets.

Lorsque vous créez un site, une unité d'organisation correspondante doit être créée dans Active Directory si vous souhaitez que les bureaux reconnaissent les Controller d'un site à l'aide d'Active Directory. L'unité d'organisation peut être créée dans un domaine quelconque de la forêt contenant vos ordinateurs. Il est recommandé que l'unité d'organisation contienne également les Controller du site. Cependant, cette condition n'est pas obligatoire. Un administrateur de domaine avec des

© 1999-2017 Citrix Systems, Inc. All rights reserved.

privilèges adéquats peut créer l'unité d'organisation en tant que conteneur vide, puis déléguer les droits d'administration de l'unité d'organisation à un administrateur Citrix.

Le script crée plusieurs objets essentiels. Seuls les objets Active Directory standard sont créés et utilisés. Il n'est pas nécessaire de développer le schéma.

- Un groupe de sécurité pour les Controller. Le compte d'ordinateur de tous les Controller du site doit appartenir à ce groupe de sécurité. Les bureaux d'un site acceptent les données provenant de Controller uniquement s'ils appartiennent à ce groupe de sécurité.
  Vérifiez que tous les Controller disposent du privilège « Accéder à cet ordinateur à partir du réseau » sur l'ensemble des bureaux virtuels exécutant le VDA. Pour ce faire, vous pouvez affecter ce privilège au groupe de sécurité des Controller. Si les Controller ne disposent pas de ce privilège, les VDA ne pourront pas s'enregistrer.

- Un objet SCP (Service Connection Point) qui contient des informations sur le site, tel que son nom. Si vous utilisez l'outil d'administration Utilisateurs et ordinateurs Active Directory pour inspecter l'unité d'organisation d'un site, vous devrez sans doute activer Fonctionnalités avancées dans le menu Affichage pour afficher les objets SCP.
- Un conteneur appelé RegistrationServices, qui est créé dans l'unité d'organisation du site. Celui-ci contient un objet SCP pour chaque Controller du site. À chaque démarrage du Controller, il valide le contenu de son objet SCP et le met à jour si nécessaire.

Si différents administrateurs sont susceptibles d'ajouter et de supprimer des Controller une fois l'installation initiale effectuée, ils doivent disposer des autorisations requises pour créer et supprimer les enfants dans le conteneur RegistrationServices et les propriétés d'écriture sur le groupe de sécurité des Controller ; ces autorisations sont accordées automatiquement à l'administrateur qui exécute le script Set-ADControllerDiscovery.ps1. L'administrateur de domaine ou l'administrateur à l'origine de l'installation peuvent accorder ces autorisations. Citrix recommande la configuration d'un groupe de sécurité à cette fin.

Lorsque vous utilisez une unité d'organisation de site :

- Les informations sont écrites dans Active Directory uniquement lorsque vous installez ou désinstallez ce logiciel, ou lorsqu'un Controller démarre et doit mettre à jour les informations dans son objet SCP (par exemple, lorsque le nom du Controller ou le port de communication a été modifié). Par défaut, le script Set-ADControllerDiscovery.ps1 définit les autorisations appropriées relatives aux objets de l'unité d'organisation d'un site, en accordant à chaque Controller un accès en écriture sur leurs objets SCP. Le contenu des objets de l'unité d'organisation du site permet d'établir une relation de confiance entre les bureaux et les Controller. Assurez-vous que :
  - seuls les administrateurs autorisés peuvent ajouter ou supprimer des ordinateurs dans le groupe de sécurité des Controller à l'aide de la liste de contrôle d'accès (ACL) s'y référant ;
  - seuls les administrateurs autorisés et leur Controller respectif peuvent modifier les informations de l'objet SCP du Controller.
- Si votre déploiement utilise la réplication, tenez compte des éventuels retards ; consultez la documentation Microsoft pour plus d'informations. Ce point est particulièrement important si vous créez l'unité d'organisation du site dans un domaine contenant des contrôleurs de domaine situés dans différents sites Active Directory. En fonction de l'emplacement des bureaux, des Controller et des contrôleurs de domaine, les modifications apportées à Active Directory lors de la création initiale de l'unité d'organisation du site, de l'installation ou de la désinstallation de Controller, de la modification d'un nom de Controller ou de ports de communication, peuvent ne pas être visibles sur les bureaux tant que les informations n'ont pas été répliquées dans le contrôleur de domaine approprié. Le retard de la réplication peut entraîner, entre autres, les conséquences suivantes : les bureaux ne peuvent pas établir de contact avec les Controller, et de ce fait, ne sont pas disponibles pour les connexions utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Ce logiciel utilise plusieurs attributs d'objet ordinateur standard dans Active Directory pour gérer les bureaux. En fonction de votre déploiement, le nom de domaine complet de l'objet machine, tel qu'indiqué dans l'enregistrement Active Directory du bureau, peut être intégré aux paramètres de connexion renvoyés à l'utilisateur en vue de la connexion. Assurez-vous que les informations sont cohérentes avec les informations dans votre environnement DNS.

Pour déplacer un Controller vers un autre site à l'aide de la découverte de Controller basée sur l'unité d'organisation, suivez les instructions ci-dessus pour le déplacement d'un Delivery Controller. Lorsque vous supprimez le Controller de l'ancien site (étape 2), exécutez le script PowerShell : **Set-ADControllerDiscover –sync**. Le script assure la synchronisation entre l'unité d'organisation et l'ensemble actuel des Controller. Après avoir joint le site existant (étape 3), exécutez le même script sur un Controller dans le nouveau site.

Les autorisations requises varient selon les actions et les besoins du demandeur.

Lors de la création du site

L'administrateur de site Citrix qui exécute le script Set-ADControllerDiscovery.ps1 doit disposer de droits sur l'unité d'organisation du site pour créer des unités de sous-organisation et des objets. (Si l'unité d'organisation du site n'est pas présente, l'administrateur doit également disposer de droits lui permettant de la créer. Citrix recommande à l'administrateur de domaine AD de pré-créer cette unité d'organisation et d'en déléguer les droits à l'identité de l'administrateur du site Citrix. Les droits nécessaires (dans l'unité d'organisation uniquement) sont les suivants :

- Créer un SCP
- Créer un conteneur
- Créer un groupe de sécurité

Le script peut également créer l'unité d'organisation du site. Pour ce faire, l'identité de l'administrateur doit être autorisée à créer une unité d'organisation sur l'unité d'organisation parente de la nouvelle unité d'organisation. Toutefois, comme indiqué ci-dessus, Citrix ne recommande pas cette façon de procéder.

À ce stade, l'utilisateur étant implicitement le propriétaire des éléments créés, vous ne devriez pas avoir besoin de droits supplémentaires sur ces éléments. C'est à ce stade que vous devez définir des propriétés supplémentaires sur le nouveau groupe de sécurité créé.

Lors de l'ajout ou de la suppression d'un Controller

Ultérieurement, l'administrateur du site Citrix peut exécuter le script ADControllerDiscovery.ps1 pour ajouter ou supprimer un Controller du site. Il peut s'agir d'une identité d'administrateur différente de celle qui a créé le contenu de l'unité d'organisation à l'origine. Les droits nécessaires sont les suivants :

- Ajouter/supprimer une machine dans le groupe de sécurité « Controller »
- Créer/supprimer un objet SCP dans le conteneur « RegistrationServices »

En mode de fonctionnement normal

En mode de fonctionnement normal, les machines Controller et les machines VDA doivent disposer des droits suivants :

- Les Controller ont besoin des droits leur permettant de définir des propriétés sur leur propre objet SCP (dans le conteneur « RegistrationServices »)
- Les Controller et les VDA doivent disposer des droits d'accès en lecture à tous les objets de l'unité d'organisation et des

© 1999-2017 Citrix Systems, Inc. All rights reserved.

niveaux inférieurs.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sessions

Jul 07, 2016

La gestion de l'activité de session est critique pour offrir la meilleure expérience utilisateur possible. La perte de connectivité due à des réseaux non fiables, à des durées de latence réseau extrêmement variables ou à des limitations en termes de portée des appareils sans fil, peuvent faire naître une certaine frustration chez les utilisateurs. La possibilité de se déplacer entre plusieurs stations de travail rapidement, d'accéder aux mêmes applications chaque fois qu'ils ouvrent une session, est une priorité pour la plupart des travailleurs mobiles, tels que le personnel médical d'un hôpital.

Utilisez les fonctionnalités suivantes pour optimiser la fiabilité des sessions, réduire les désagréments, les temps d'arrêt et la perte de productivité ; à l'aide de ces fonctionnalités, les utilisateurs mobiles peuvent passer rapidement et facilement d'un périphérique à un autre.

- Fiabilité de session
- Reconnexion automatique des clients
- Persistance ICA
- Le contrôle de l'espace de travail
- Itinérance de session

La section Intervalle d'ouverture de session décrit comment modifier le paramètre par défaut.

Vous pouvez également fermer la session d'un utilisateur, déconnecter une session et configurer le pré-lancement et la persistance de session ; consultez l'article Gérer les sessions au travers des groupes de mise à disposition.

Fiabilité de session

La fiabilité de session maintient les sessions actives et visibles sur l'écran de l'utilisateur lorsque la connexion au réseau est interrompue. L'utilisateur peut donc visualiser l'application jusqu'à ce que la connexion au réseau reprenne.

Cette fonction est particulièrement utile pour les utilisateurs mobiles utilisant des connexions sans fil. Par exemple, lorsqu'un utilisateur connecté via une connexion sans fil entre dans un tunnel ferroviaire, la connexion est momentanément interrompue. D'ordinaire, la session se déconnecte et disparaît de l'écran de l'utilisateur ; ce dernier est alors contraint de se reconnecter à la session déconnectée. Grâce à la fiabilité de session, la session reste active sur la machine. Pour indiquer que la connexion est interrompue, l'affichage fourni à l'utilisateur est figé et le curseur prend la forme d'un sablier jusqu'à ce que la connexion soit rétablie de l'autre côté du tunnel. L'utilisateur a toujours accès à l'affichage de l'application durant l'interruption et peut reprendre l'interaction avec l'application lorsque la connexion réseau est rétablie. La fonction de fiabilité de session permet aux utilisateurs de se reconnecter sans avoir à s'authentifier de nouveau.

Les utilisateurs de Citrix Receiver ne peuvent pas remplacer le paramètre du Controller.

Vous pouvez utiliser la fonction de fiabilité de session avec le protocole TLS (Transport Layer Security). TLS crypte uniquement les données envoyées entre la machine utilisateur et NetScaler Gateway.

Activez et configurez la fonction de fiabilité de session avec les paramètres de stratégie suivants :

- Le paramètre de stratégie Connexions de fiabilité de session autorise ou interdit la fiabilité de session.
- Le paramètre de stratégie Expiration de délai de la fiabilité de session est réglé par défaut sur 180 secondes, ou trois minutes. Même si vous pouvez étendre la durée pendant laquelle la fonction de fiabilité de session maintient une session

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ouverte, cette fonctionnalité est conçue pour aider l'utilisateur et par conséquent ne pas demander à l'utilisateur de devoir s'authentifier à nouveau. Si vous augmentez la durée pour laquelle une session est gardée ouverte, les risques d'accès non autorisé sont accrus : un utilisateur distrait peut s'éloigner de sa machine cliente et il est alors possible que des utilisateurs non autorisés accèdent à sa session.

- Les connexions entrantes de fiabilité de session utilisent le port 2598, à moins que vous ne changiez le numéro de port défini dans le paramètre de stratégie Numéro de port de la fiabilité de session.
- Si vous ne souhaitez pas autoriser les utilisateurs à se reconnecter aux sessions interrompues sans authentification, utilisez la fonction de reconnexion automatique des clients. Vous pouvez configurer le paramètre de stratégie Authentification de la reconnexion automatique des clients pour inviter les utilisateurs à s'authentifier à nouveau lors de la reconnexion aux sessions interrompues.

Si vous utilisez la fonction de fiabilité de session et la fonction de reconnexion automatique des clients, ces fonctions agissent l'une après l'autre. La fonction de fiabilité de session ferme (ou déconnecte) la session utilisateur après la période spécifiée dans le paramètre de stratégie Expiration de délai de la fiabilité de session. Ensuite, les paramètres définis pour la fonction de reconnexion automatique des clients s'appliquent et la fonction tente d'opérer la reconnexion de l'utilisateur à la session déconnectée.

Reconnexion automatique des clients

Avec la fonction Reconnexion automatique des clients, Citrix Receiver peut détecter les déconnexions de session ICA involontaires et reconnecter automatiquement les utilisateurs à leurs sessions. Lorsque cette fonctionnalité est activée sur le serveur, les utilisateurs n'ont pas besoin de se reconnecter manuellement pour continuer à travailler.

Pour les sessions d'application, Citrix Receiver essaie de se reconnecter à la session jusqu'à ce que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion.

Pour les sessions de bureau, Citrix Receiver tente de se reconnecter à la session pendant une période de temps spécifiée, à moins que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion. Par défaut, cette durée est de cinq minutes. Pour modifier cette durée, modifiez le registre sur la machine utilisateur :

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;

où *secondes* est le nombre de secondes après lequel aucune autre tentative de reconnexion à la session n'est effectuée.

Activez et configurez la fonction de reconnexion automatique des clients avec les paramètres de stratégie suivants :

- **Reconnexion automatique des clients**. Active ou désactive la reconnexion automatique par Citrix Receiver après l'interruption d'une connexion.
- **Authentification de la reconnexion automatique des clients**. Active ou désactive l'authentification utilisateur après reconnexion automatique.
- **Journalisation de la reconnexion automatique des clients**. Active ou désactive la journalisation des événements de reconnexion dans le journal d'événements. Par défaut, la journalisation est désactivée. Lorsqu'il est activé, le Journal système du ou des serveurs reçoit les informations relatives aux échecs et aux succès des tentatives de reconnexion automatique. Chaque serveur stocke des informations sur les événements de reconnexion dans son propre Journal système ; le site ne fournit pas de journal combinant les événements de reconnexion de tous les serveurs.

La fonction de reconnexion automatique des clients intègre un mécanisme permettant une authentification basée sur les informations d'identification cryptées de l'utilisateur. Lorsqu'un utilisateur ouvre une session sur un site, le serveur crypte ses

© 1999-2017 Citrix Systems, Inc. All rights reserved.

informations d'identification, les stocke en mémoire, puis envoie un cookie contenant la clé de cryptage à Citrix Receiver. Citrix Receiver transmet la clé au serveur pour reconnexion. Celui-ci décrypte les informations d'identification et les transmet au système d'ouverture de session Windows pour authentification. Lorsqu'un cookie expire, l'utilisateur doit à nouveau fournir ses informations d'identification pour se reconnecter à sa session.

Si le paramètre Authentification de la reconnexion automatique des clients est sélectionné, aucun cookie n'est utilisé. Au lieu de cela, les utilisateurs voient s'afficher une boîte de dialogue leur demandant de fournir leurs informations d'identification lorsque Citrix Receiver tente de se reconnecter automatiquement.

Pour une protection optimale des informations d'identification et des sessions des utilisateurs, utilisez le cryptage pour toutes les communications entre les clients et le site.

Désactivez la reconnexion automatique des clients sur Citrix Receiver pour Windows en utilisant le fichier icaclient.adm. Pour de plus amples informations, consultez la documentation relative à votre version de Citrix Receiver pour Windows.

Les paramètres des connexions affectent également la fonction de reconnexion automatique des clients.

- Par défaut, la fonction de reconnexion automatique des clients est activée via les paramètres de stratégie au niveau du site, comme décrit ci-dessus. Les utilisateurs n'ont pas besoin de se réauthentifier. Toutefois, si la connexion TCP ICA d'un serveur est configurée pour réinitialiser les sessions dont une liaison de communication a été interrompue, la reconnexion automatique n'a pas lieu. La fonction de reconnexion automatique des clients fonctionne uniquement si le serveur déconnecte les sessions en cas d'interruption ou d'expiration de délai d'une connexion. Dans ce contexte, la connexion TCP ICA fait référence au port virtuel d'un serveur (et non à une connexion réseau) utilisé pour les sessions sur les réseaux TCP/IP.
- Par défaut, la connexion TCP ICA d'un serveur est configurée pour déconnecter les sessions en cas d'interruption ou d'expiration de délai de leurs connexions. Les sessions déconnectées restent intactes dans la mémoire du système et sont disponibles pour la reconnexion par le Citrix Receiver
- La connexion peut être configurée pour réinitialiser ou fermer les sessions dont les connexions sont interrompues ou dont le délai a expiré. Lorsqu'une session est réinitialisée, une tentative de reconnexion lance une nouvelle session. L'utilisateur ne retrouve pas l'application dans l'état où elle était avant la reconnexion ; l'application est relancée.
- Si le serveur est configuré pour réinitialiser les sessions, la fonction de reconnexion automatique des clients crée une nouvelle session. Ce processus nécessite que les utilisateurs fournissent leurs informations d'identification pour ouvrir une session sur le serveur.
- La reconnexion automatique peut échouer si le Citrix Receiver ou le plug-in transmettent des informations d'identification incorrectes, ce qui peut se produire lors d'une attaque, ou si le serveur estime qu'une durée trop longue s'est écoulée depuis qu'il a détecté une connexion interrompue.

Persistance ICA

L'activation de la fonctionnalité de persistance ICA empêche la déconnexion des connexions rompues. Lorsqu'elle est activée, si le serveur ne détecte plus aucune activité (par exemple, aucun changement de l'horloge, aucun mouvement de la souris, aucune mise à jour de l'écran), cette fonctionnalité empêche les services Bureau à distance de se déconnecter de cette session. Le serveur envoie des paquets de persistance à quelques secondes d'intervalle pour détecter si la session est active. Si la session n'est plus active, le serveur marque la session en tant que déconnectée.

Remarque : cependant, la persistance ICA fonctionne uniquement si vous n'utilisez pas la fiabilité de session. La fiabilité de session dispose de ses propres mécanismes pour empêcher les connexions interrompues d'être déconnectées. Ne configurez

© 1999-2017 Citrix Systems, Inc. All rights reserved.

la persistance ICA que pour les connexions qui n'utilisent pas la fiabilité de session.

Les réglages effectués dans la page Persistance ICA ont priorité sur les réglages correspondants configurés dans la Stratégie de groupe Microsoft Windows.

Activez et configurez les paramètres de persistance ICA avec les paramètres de stratégie suivants :

- **Délai d'expiration de persistance ICA**. Spécifie l'intervalle (1-3600 secondes) utilisé pour envoyer des messages de persistance ICA. Ne configurez pas cette option si vous voulez que votre logiciel de contrôle de réseau ferme les connexions inactives dans les environnements pour lesquels les interruptions de connexion sont si peu fréquentes que la reconnexion des utilisateurs aux sessions n'est pas un problème.
  L'intervalle par défaut est de 60 secondes : les paquets de persistance ICA sont envoyés aux machines utilisateur toutes les 60 secondes. Si une machine utilisateur ne répond pas après 60 secondes, l'état des sessions ICA correspondantes passe à Déconnectée.
- **Persistances ICA**. Envoie ou empêche l'envoi de messages de persistance ICA.

Le contrôle de l'espace de travail

Le contrôle de l'espace de travail permet aux bureaux et aux applications de suivre un utilisateur d'un appareil à un autre. Cette itinérance permet à un utilisateur d'accéder à tous les bureaux ou d'ouvrir des applications à partir de n'importe quel emplacement simplement en ouvrant une session, sans avoir à redémarrer les bureaux ou applications sur chaque machine. Par exemple, le contrôle de l'espace de travail permet aux employés d'un centre hospitalier de se déconnecter rapidement d'une station de travail pour se reconnecter à une autre et d'accéder aux mêmes applications chaque fois qu'ils ouvrent une session. Si vous configurez le contrôle de l'espace de travail de la sorte, le personnel médical peut se déconnecter de plusieurs applications sur une machine cliente et s'y reconnecter sur une autre machine cliente.

Le contrôle de l'espace de travail affecte les activités suivantes :

- **Ouverture de session** : par défaut, le contrôle de l'espace de travail permet aux utilisateurs de se reconnecter automatiquement à tous les bureaux et applications en cours d'exécution lors de l'ouverture de session, sans avoir à les rouvrir manuellement. Via le contrôle de l'espace de travail, les utilisateurs peuvent ouvrir des bureaux ou applications déconnectés ainsi que des applications ou bureaux qui sont actifs sur une autre machine cliente. La déconnexion d'une application ou d'un bureau n'interrompt pas son exécution sur le serveur. Si des utilisateurs itinérants doivent maintenir la connexion avec certaines applications ou certains bureaux sur une machine cliente tandis qu'ils se reconnectent à d'autres applications ou bureaux sur une autre machine cliente, vous pouvez configurer le comportement de reconnexion de façon à n'ouvrir que les applications ou bureaux dont ils se sont déconnectés.
- **Reconnexion** : après avoir ouvert une session sur le serveur, les utilisateurs peuvent se reconnecter à tous leurs bureaux ou applications à tout moment en cliquant sur le bouton Se reconnecter. Par défaut, cette option ouvre les applications et bureaux qui sont déconnectés ainsi que ceux actuellement exécutés sur une autre machine cliente. Vous pouvez configurer cette option de façon à ce qu'elle n'ouvre que les applications ou bureaux précédemment déconnectés par l'utilisateur.
- **Fermeture de session** : pour les utilisateurs ouvrant des bureaux ou applications via StoreFront, vous pouvez configurer la commande Fermer la session afin de fermer la session utilisateur de StoreFront ainsi que toutes les sessions actives ou uniquement la session de StoreFront.
- **Déconnexion** : les utilisateurs peuvent se déconnecter simultanément de toutes les applications et tous les bureaux en cours d'exécution sans avoir à déconnecter chaque application ou bureau individuellement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Le contrôle de l'espace de travail est disponible uniquement pour les utilisateurs Citrix Receiver pour accéder aux bureaux et applications via une connexion Citrix StoreFront. Par défaut, le contrôle de l'espace de travail est désactivé pour les sessions de bureau virtuel, mais activé pour les applications hébergées. Le partage de session ne se produit pas par défaut entre les bureaux publiés et toute application publiée exécutée au sein de ces bureaux.

Lorsqu'un utilisateur passe à une nouvelle machine cliente, les stratégies utilisateur, les mappages des lecteurs clients et la configuration des imprimantes changent en conséquence. Les stratégies et les mappages sont appliqués en fonction de la machine cliente à partir de laquelle l'utilisateur a ouvert la session. Par exemple, si l'employé d'un centre hospitalier ferme la session qu'il a ouverte sur une machine cliente dans la salle des urgences et en ouvre une autre sur une machine dans le Service de radiologie, les stratégies, les mappages d'imprimante et de lecteur client correspondant à la machine cliente du Service de radiologie sont appliqués à l'ouverture de session sur cette machine.

Vous pouvez personnaliser les imprimantes qui s'affichent pour les utilisateurs lorsqu'ils changent d'emplacement. Vous pouvez également contrôler si les utilisateurs peuvent imprimer sur des imprimantes locales, la quantité de bande passante consommée lorsque les utilisateurs se connectent à distance, ainsi que d'autres aspects de leur expérience d'impression.

Pour plus d'informations sur l'activation et la configuration du contrôle de l'espace de travail pour les utilisateurs, consultez la documentation StoreFront.

Itinérance de session

Par défaut, les sessions sont partagées entre les machines clientes de l'utilisateur. Lorsque l'utilisateur ouvre une session et bascule sur une autre machine, la même session est utilisée et les applications sont disponibles sur les deux machines. Les applications suivent, quelle que soit la machine ou que les sessions en cours existent ou non. Dans la plupart des cas, les imprimantes et les autres ressources attribuées à l'application suivent également.

Bien que ce comportement par défaut offre de nombreux avantages, il n'est pas toujours idéal. Vous pouvez désactiver l'itinérance de session à l'aide du SDK du PowerShell.

Exemple 1 : un professionnel de la santé utilise deux machines ; il remplit un formulaire d'assurance sur un PC de bureau et recherche des informations sur le patient sur une tablette.

- Si l'itinérance de session est activée, les applications s'affichent toutes les deux sur les deux machines (une application lancée sur une machine est visible sur toutes les machines en cours d'utilisation). Ce comportement peut ne pas répondre aux exigences de sécurité.
- Si l'itinérance de session est désactivée, le dossier du patient ne s'affiche pas sur le PC de bureau et le formulaire d'assurance ne s'affiche pas sur la tablette.

Exemple 2 : un chef de production lance une application sur le PC de son bureau. Le nom et l'emplacement de la machine déterminent les imprimantes et autres ressources qui sont disponibles pour cette session. Plus tard dans la journée, il se rend dans un bureau situé dans un autre bâtiment pour une réunion pour laquelle il devra utiliser une imprimante.

- Si l'itinérance de session est activée, le chef de production ne peut probablement pas accéder aux imprimantes à proximité de la salle de réunion, car les applications qu'il a démarrées plus tôt dans son bureau ont entraîné l'attribution d'imprimantes et d'autres ressources situées près de cet emplacement.
- Si l'itinérance de session est désactivée, lorsqu'il ouvre une session sur une autre machine (en utilisant les mêmes informations d'identification), une nouvelle session est démarrée et les imprimantes et ressources à proximité sont disponibles.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour configurer l'itinérance de session, utilisez les applets de commande de règle de stratégie d'admissibilité suivantes avec la propriété « SessionReconnection ». Si vous le souhaitez, vous pouvez également spécifier la propriété « LeasingBehavior » ; consultez la section Location de connexion et itinérance de session ci-dessous.

Pour les sessions de bureau :

> Set-BrokerEntitlementPolicyRule <*nom_groupe_mise_à_disposition*> -SessionReconnection <*valeur*> -LeasingBehavior Allowed|Disallowed

Pour les sessions d'application :

> Set-BrokerAppEntitlementPolicyRule <*nom_groupe_mise_à_disposition*> -SessionReconnection <*valeur*> -LeasingBehavior Allowed|Disallowed

Où *valeur* peut être :

- **Always**. Les sessions sont toujours itinérantes, quelle que soit la machine cliente et que la session soit connectée ou déconnectée. Il s'agit de la valeur par défaut.
- **DisconnectedOnly**. Se reconnecte uniquement aux sessions déconnectées ; sinon, démarre une nouvelle session (vous pouvez activer l'itinérance de session entre les machines clientes en les déconnectant, ou en utilisant le contrôle de l'espace de travail pour activer explicitement l'itinérance). Une session connectée active sur une autre machine cliente n'est jamais utilisée ; une nouvelle session est lancée.
- **SameEndpointOnly**. Un utilisateur obtient une session unique pour chaque machine cliente qu'il utilise. L'itinérance est complètement désactivée. Les utilisateurs peuvent se reconnecter uniquement à la machine qui a été utilisée précédemment pour la session.

La propriété « LeasingBehavior » est décrite ci-dessous.

Effets d'autres paramètres

La désactivation de l'itinérance de session est affectée par la limite d'application « Autoriser une seule instance par utilisateur » définie dans les propriétés de l'application dans le groupe de mise à disposition.

- Si vous désactivez l'itinérance de session, désactivez la limite d'application « Autoriser une seule instance par utilisateur ».
- Si vous activez la limite d'application « Autoriser une seule instance par utilisateur », ne configurez pas les deux valeurs qui permettent de nouvelles sessions sur de nouvelles machines.

Si vous ne connaissez pas bien la location de connexion, consultez l'article Location de connexion.

Lorsqu'un Controller entre en mode de location de connexions, la reconnexion de session revient à sa valeur par défaut, reconnectant l'utilisateur à une seule des sessions actives ou déconnectées pour le bureau ou l'application.

Pour une sécurité accrue, si vous avez configuré une valeur autre que celle par défaut pour l'itinérance de session et que vous disposez de plusieurs utilisateurs partageant les mêmes informations d'identification d'ouverture de session sur plusieurs machines, il est recommandé de désactiver la fonctionnalité de location de connexion pour le groupe de mise à disposition qui comprend ce compte d'utilisateur.

Pourquoi ? Dans ce scénario, une session est partagée entre toutes les machines. Cette situation n'est pas idéale si, par

© 1999-2017 Citrix Systems, Inc. All rights reserved.

exemple, une personne affiche des informations confidentielles qui ne sont pas destinées à être consultées par un autre utilisateur lorsque celui-ci se reconnecte avec les mêmes informations d'identification et que le Controller se trouve en mode de location de connexion.

La désactivation de la location de connexion dans la stratégie d'admissibilité élimine ce risque : un utilisateur ne sera pas en mesure de consulter la session d'un autre utilisateur avec les mêmes informations d'identification, même lorsque le Controller se trouve en mode de location de connexion. Les autres stratégies d'admissibilité peuvent rester inchangées ; les comptes utilisateur individuels peuvent utiliser la fonctionnalité de location de connexion via des droits distincts.

Pour désactiver la location de connexion dans une stratégie d'admissibilité, ajoutez la propriété « LeasingBehavior Disallowed » à l'applet de commande de la stratégie d'admissibilité. Si vous désactivez la location de connexion, vous devez supprimer manuellement toute location de lancement qui a déjà été créée et mise en cache pour cette stratégie d'admissibilité ; sinon, les utilisateurs seront toujours en mesure de se reconnecter au cours d'une panne de base de données.

Intervalle d'ouverture de session

Si une machine virtuelle contenant un VDA de bureau se ferme avant la fin du processus d'ouverture de session, vous pouvez attribuer plus de temps au processus. La valeur par défaut pour 7.6 et versions ultérieures est de 180 secondes (la valeur par défaut pour 7.0-7.5 est de 90 secondes).

Sur la machine (ou l'image principale utilisée dans un catalogue de machines), définissez la clé de registre suivante :

Clé : HKLM\SOFTWARE\Citrix\PortICA

Valeur : AutoLogonTimeout

Type : DWORD

Spécifiez une durée en secondes, au format décimal, dans la plage 0-3600.

Si vous modifiez une image principale, mettez à jour le catalogue.

Remarque : ce paramètre s'applique uniquement aux machines virtuelles avec VDA de bureau (station de travail) ; Microsoft contrôle le délai d'expiration de l'ouverture de session sur les machines avec VDA de serveur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Utiliser la fonction de recherche dans Studio

Jul 07, 2016

Utilisez la fonction de recherche pour afficher des informations sur des machines spécifiques, des sessions, des catalogues de machines, des applications ou des groupes de mise à disposition.

1. Sélectionnez Rechercher dans le volet de navigation de Studio.
   Remarque : vous ne pouvez pas effectuer des recherches dans les catalogues de machines ou les onglets Groupes de mise à disposition à l'aide de la zone Rechercher. Utiliser le nœud Rechercher dans le volet de navigation.
   Pour afficher des critères de recherche supplémentaires, cliquez sur le signe plus en regard des champs déroulants de recherche. Supprimer des critères de recherche en cliquant sur le bouton moins.

2. Entrez le nom ou utilisez la liste déroulante pour sélectionner une autre option de recherche pour l'élément que vous souhaitez rechercher.
3. Si vous le souhaitez, vous pouvez enregistrer votre recherche en cliquant sur Enregistrer sous. La recherche s'affiche dans la liste des recherches enregistrées.

Vous pouvez également cliquer sur l'icône Développer la recherche (crochets pointus double) pour afficher une liste déroulante des propriétés de recherche ; vous pouvez effectuer une recherche avancée en créant une expression à partir des propriétés de la liste déroulante.

Conseils pour améliorer la recherche :

- Pour afficher des caractéristiques supplémentaires à inclure dans l'affichage sur lequel vous pouvez rechercher et trier, cliquez avec le bouton droit de la souris sur une colonne et cliquez sur Sélectionner les colonnes.
- Pour localiser une machine utilisateur connectée à une machine, utilisez le client (IP) et Is, puis entrez l'adresse IP de la machine.
- Pour localiser les sessions actives, utilisez État de session, Is et Connecté
- Pour répertorier toutes les machines d'un groupe de mise à disposition, sélectionnez Groupes de mise à disposition dans le panneau de navigation, sélectionnez le groupe, puis sélectionnez Afficher les machines dans le volet Actions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Balises

Jul 07, 2016

Les balises sont des chaînes qui identifient les éléments tels que les machines, les applications, les groupes de mise à disposition et les stratégies. Après la création d'une balise, puis son ajout à un élément, vous pouvez configurer certaines opérations pour qu'elles s'appliquent uniquement aux éléments avec une balise spécifique :

- La recherche personnalisée s'affiche dans Studio.

  Par exemple, si vous souhaitez afficher uniquement les applications qui ont été optimisées pour les testeurs, ajoutez une balise appelée « test » à ces applications. Ensuite, vous pouvez filtrer la recherche Studio avec la balise « test ». De même, si vous souhaitez afficher uniquement les groupes de mise à disposition contenant des membres de l'équipe de test, ajoutez une balise « testeur » aux groupes de mise à disposition contenant des membres de l'équipe de test, puis filtrez la recherche Studio avec la balise « testeur ».

- Appliquez (allouez) des stratégies Citrix aux applications, machines ou groupes de mise à disposition qui ont (ou n'ont pas) une balise spécifique.

  Par exemple, si vous souhaitez appliquer une stratégie Citrix uniquement aux stations de travail les plus puissantes, ajoutez une balise nommée « haute puissance » à ces machines. Ensuite, sur la page Attribuer la stratégie de l'assistant Créer une stratégie, sélectionnez cette balise et la case Activer. Vous pouvez également ajouter une balise à un groupe de mise à disposition, puis appliquer une stratégie Citrix à ce groupe.

Gérer les balises

Sélectionnez une machine, une application ou un groupe de mise à disposition dans Studio, puis sélectionnez **Gérer les balises** dans le volet Actions. La boîte de dialogue Gérer les balises répertorie toutes les balises qui ont été créées dans le site, et pas seulement pour l'élément sélectionné.

- Une case à cocher activée indique que la balise a déjà été ajoutée à l'élément sélectionné.
- Si vous sélectionnez un groupe, une case à cocher contenant un trait indique que certains, mais pas tous les éléments de ce groupe d'identification, ont une balise.

Les options suivantes sont disponibles dans la boîte de dialogue Gérer les balises :

- Pour ajouter ou supprimer une balise, activez ou désactivez la case à cocher en regard des balises que vous souhaitez ajouter ou supprimer.
- Pour créer une balise, sélectionnez **Créer une balise**. Entrez un nom et une description. Les noms de balise doivent être uniques et ne sont pas sensibles à la casse. Cliquez ensuite sur **OK**.
- Pour modifier une balise, sélectionnez une balise, puis sélectionnez **Modifier la balise**. Entrez un nouveau nom et/ou une description, puis cliquez sur **Enregistrer**. Vous pouvez modifier une seule balise à la fois.
- Pour supprimer une ou plusieurs balises, sélectionnez les balises, puis sélectionnez **Supprimer les balises**. La boîte de dialogue Supprimer les balises répertorie le nombre d'éléments qui utilisent actuellement les balises que vous avez sélectionnées. Cliquez sur un élément pour afficher des informations supplémentaires ; par exemple, si deux machines sont concernées, cliquer sur cet élément affiche les noms des deux machines. Une fois que vous avez vu les éléments qui sont concernés, confirmez si vous souhaitez supprimer les balises.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Prise en charge de IPv4/IPv6

Jul 07, 2016

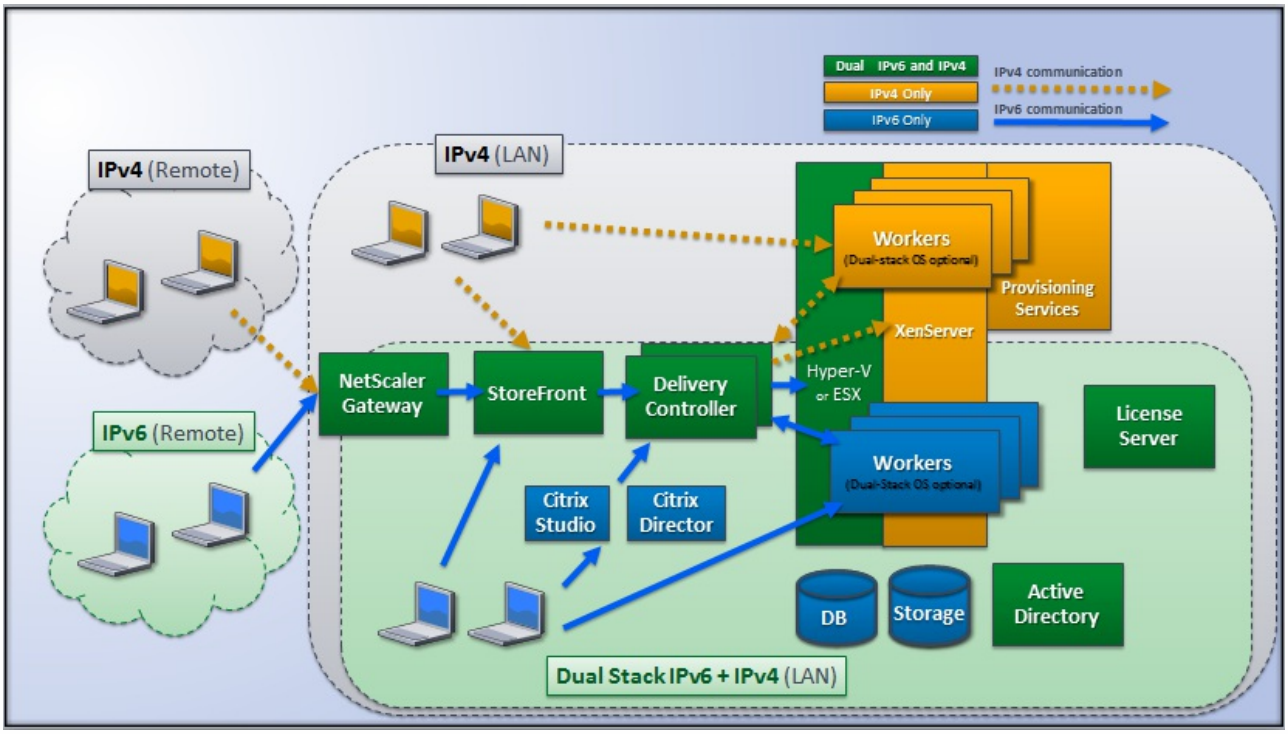
Cette version prend en charge les déploiements IPv4 purs, IPv6 purs et double pile qui utilisent des réseaux IPv4 et IPv6 qui se chevauchent.

Les communications IPv6 sont contrôlées par deux paramètres de stratégie Citrix liés à la connexion au Virtual Delivery Agent (VDA) :

- Un paramètre principal qui applique l'utilisation de IPv6 : Uniquement utiliser l'enregistrement du contrôleur IPv6.
- Un paramètre dépendant qui définit un masque de réseau IPv6 : Masque réseau IPv6 d'enregistrement du contrôleur.

Lorsque le paramètre de stratégie Uniquement utiliser l'enregistrement du contrôleur IPv6 est activé, les VDA s'enregistrent auprès d'un Delivery Controller pour les connexions entrantes à l'aide d'une adresse IPv6.

La figure suivante illustre un déploiement double pile IPv4/IPv6. Dans ce scénario, un travailleur est un VDA installé sur un hyperviseur ou sur un système physique, qui est utilisé principalement pour autoriser les connexions aux applications et bureaux. Les composants qui prennent en charge IPv6 et IPv4 sont exécutés sur des systèmes d'exploitation qui utilisent le tunneling ou un logiciel à double protocole.



Ces produits, composants et fonctionnalités Citrix prennent uniquement en charge IPv4 :

- Provisioning Services
- XenServer version 6.x
- Les VDA non contrôlés par le paramètre de stratégie **Uniquement utiliser l'enregistrement du contrôleur IPv6**
- Les versions XenApp antérieures à la version 7.5, les versions XenDesktop antérieures à la version 7, et EdgeSight

Dans ce déploiement :

- Si une équipe utilise fréquemment un réseau IPv6 et que l'administrateur souhaite qu'ils utilisent le trafic IPv6,

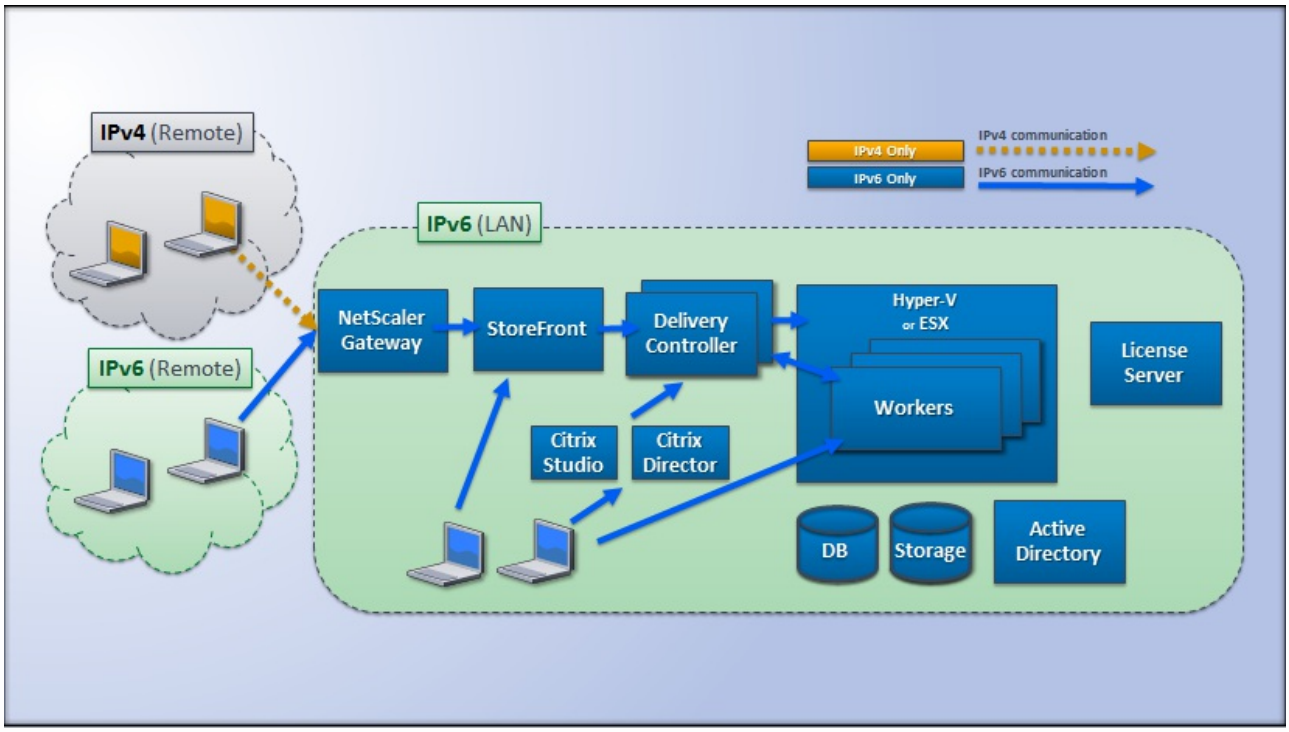
© 1999-2017 Citrix Systems, Inc. All rights reserved.

l'administrateur publie des bureaux et applications IPv6 pour ces utilisateurs basés sur une image de travail ou une unité d'organisation (UO) sur laquelle le paramètre de stratégie est IPv6 activé (c'est-à-dire, Uniquement utiliser l'enregistrement du contrôleur IPv6 est activé).

- Si une équipe utilise fréquemment un réseau IPv4, l'administrateur publie des bureaux et applications IPv4 pour ces utilisateurs basés sur une image de travail ou une unité d'organisation sur laquelle le paramètre de stratégie IPv6 est désactivé (c'est-à-dire, Uniquement utiliser l'enregistrement du contrôleur IPv6 est désactivé).

La figure suivante illustre un déploiement IPv6 pur. Dans ce scénario :

- Les composants sont exécutés sur des systèmes d'exploitation configurés pour prendre en charge un réseau IPv6.
- Le paramètre de stratégie Citrix principal (Uniquement utiliser l'enregistrement du contrôleur IPv6) est activé pour tous les VDA ; ils doivent s'enregistrer auprès du Controller à l'aide d'une adresse IPv6.



Deux paramètres de stratégie Citrix affectent la prise en charge d'une implémentation IPv6 ou double pile IPv4/IPv6. Configurez les paramètres de stratégie suivants relatifs aux connexions :

- **Uniquement utiliser l'enregistrement du contrôleur IPv6** : contrôle quelle forme d'adresse le Virtual Delivery Agent (VDA) utilise pour s'enregistrer auprès du Delivery Controller. Valeur par défaut = Désactivé
  - Lorsque le VDA communique avec le Controller, il utilise une seule adresse IPv6 choisie dans l'ordre suivant : adresse IP globale, adresse locale unique (ULA), adresse locale du lien (uniquement si aucune autre adresse IPv6 n'est disponible).
  - Lorsque cette stratégie est désactivée, le VDA s'enregistre et communique avec le Controller à l'aide de l'adresse IPv4 de la machine.
- **Masque réseau IPv6 d'enregistrement du contrôleur** : une machine peut disposer de plusieurs adresses IPv6 ; ce paramètre de stratégie permet aux administrateurs de restreindre le VDA à un sous-réseau préféré (plutôt qu'une adresse IP globale, si une telle adresse est enregistrée). Ce paramètre spécifie le réseau sur lequel le VDA va s'enregistrer : ce dernier s'enregistre uniquement sur la première adresse qui correspond au masque réseau spécifié. Ce paramètre est uniquement valide si le paramètre de stratégie Uniquement utiliser l'enregistrement du contrôleur IPv6 est activé. Valeur par défaut = chaîne vide

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Important : l'utilisation de IPv4 ou IPv6 par un VDA est déterminée uniquement par ces paramètres de stratégie. En d'autres termes, pour utiliser l'adressage IPv6, le VDA doit être contrôlé par une stratégie Citrix avec le paramètre **Uniquement utiliser l'enregistrement du contrôleur IPv6** activé.

Si votre environnement contient à la fois les réseaux IPv4 et IPv6, vous aurez besoin de configurations de groupe de mise à disposition distinctes pour les clients IPv4 et pour les clients qui peuvent accéder au réseau IPv6. Pensez à différencier les utilisateurs à l'aide de noms différents, attributions manuelles de groupes Active Directory ou filtres Smart Access.

La reconnexion à une session peut échouer si la connexion est lancée sur un réseau IPv6, puis que des tentatives de reconnexion sont effectuées à partir d'un client interne ne disposant que d'un accès IPv4.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Redirection de dossiers clients

Jul 07, 2016

La redirection de dossiers clients modifie la manière dont les fichiers côté client sont accessibles sur la session côté hôte. Lorsque vous activez uniquement le mappage de lecteur client sur le serveur, les volumes complets côté client sont automatiquement mappés sur les sessions en tant que liens UNC (Universal Naming Convention). Lorsque vous activez la redirection de dossiers clients sur le serveur et que l'utilisateur la configure sur la machine utilisateur, la partie du volume local spécifié par l'utilisateur est redirigée.

Seuls les dossiers spécifiés par l'utilisateur s'affichent sous forme de liens UNC dans les sessions au lieu du système de fichiers complet sur la machine utilisateur. Si vous désactivez les liens UNC via le registre, des dossiers clients apparaissent comme des lecteurs mappés au sein de la session.

La redirection de dossiers clients est prise en charge sur les machines avec OS de bureau Windows uniquement.

La redirection de dossiers clients d'un lecteur USB externe ne sera pas enregistrée suite à la déconnexion puis reconnexion de l'appareil.

Activez la redirection de dossiers clients sur le serveur. Ensuite, sur la machine cliente, spécifiez les dossiers à rediriger (l'application utilisée pour spécifier les options du dossier client est incluse avec Citrix Receiver fournie avec cette version).

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

1. Sur le serveur :
    1. Créez une clé : HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection.
    2. Créez une valeur REG_DWORD.
        - Nom : CFROnlyModeAvailable
        - Type : REG_DWORD
        - Données : définir sur 1
2. Sur la machine utilisateur :
    1. Vérifiez que la dernière version de Citrix Receiver est installée.
    2. À partir du répertoire d'installation de Citrix Receiver, démarrez CtxCFRUI.exe.
    3. Sélectionnez le bouton radio Personnaliser et ajoutez, modifiez ou supprimez des dossiers.
    4. Déconnectez-vous et reconnectez-vous à vos sessions pour que le paramètre prenne effet.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Profils utilisateur

Jul 07, 2016

Par défaut, Citrix Profile Management est installé de manière silencieuse sur les images principales lorsque vous installez Virtual Delivery Agent, mais vous n'avez pas à utiliser Profile Management en tant que solution de profils.

Afin de répondre aux besoins variés de vos utilisateurs, vous pouvez utiliser les stratégies XenApp et XenDesktop pour appliquer un comportement de profil différent aux machines dans chaque groupe de mise à disposition. Par exemple, un groupe de mise à disposition peut nécessiter des profils obligatoires Citrix, dont le modèle est stocké dans un emplacement réseau, mais un autre groupe de mise à disposition peut nécessiter des profils itinérants Citrix stockés dans un autre emplacement avec plusieurs dossiers redirigés.

- Si d'autres administrateurs de votre organisation sont responsables des stratégies XenApp et XenDesktop, travaillez avec eux pour vous assurer qu'ils définissent les stratégies liées aux profils sur vos groupes de mise à disposition.
- Les stratégies Profile Management peuvent également être définies dans la stratégie de groupe, dans le fichier .ini de Profile management et localement sur des machines virtuelles individuelles. Ces diverses méthodes permettant de définir le comportement de profil sont lues dans l'ordre suivant :
  1. Stratégie de groupe (fichiers .adm ou .admx)
  2. Les stratégies XenApp et XenDesktop dans le nœud Stratégie
  3. Stratégies locales sur la machine virtuelle à laquelle l'utilisateur se connecte
  4. Fichier .ini Profile Management

  Par exemple, si vous configurez la même stratégie dans le nœud Stratégie de groupe et le nœud Stratégie, le système lit le paramètre de stratégie dans la stratégie de groupe et ignore le paramètre de stratégie XenApp et XenDesktop.

Quelle que soit la solution de gestion des profils que vous choisissez, les administrateurs Director peuvent accéder à des informations de diagnostic afin de résoudre les problèmes liés aux profils utilisateur. Pour de plus amples informations, veuillez consulter la documentation de Director.

Si vous utilisez la fonctionnalité Personal vDisk, les profils utilisateur Citrix sont stockés sur les Personal vDisks des bureaux virtuels par défaut. Ne supprimez pas la copie d'un profil dans le magasin d'utilisateur alors qu'il reste une copie sur le Personal vDisk. Cela engendre une erreur Profile Management et entraîne l'utilisation d'un profil temporaire pour les ouvertures de session au bureau virtuel.

Le type de bureau est automatiquement détecté, basé sur l'installation de Virtual Delivery Agent et, en plus du choix de configuration que vous effectuez dans Studio, définit les valeurs par défaut de Profile Management en conséquence.

Les stratégies que Profile Management ajuste sont affichées dans le tableau ci-dessous. Les paramètres de stratégie autres que les paramètres par défaut sont préservés et ne sont pas écrasés par cette fonctionnalité. Consultez la documentation Profile Management pour de plus amples informations sur chaque stratégie. Les types de machines qui créent des profils affectent les stratégies qui sont modifiées. Votre choix doit se baser sur les facteurs principaux suivants : les machines sont-elles persistantes ou provisionnées, sont-elles partagées par de multiples utilisateurs ou dédiées à un seul utilisateur ?

Les systèmes persistants disposent d'un stockage local dont le contenu est conservé lorsque le système est éteint. Ils peuvent utiliser des technologies de stockage telles que les réseaux SAN pour mettre en miroir le disque local. En revanche, les systèmes provisionnés sont créés « à la volée » à partir d'un disque de base et d'un type de disque d'identité. Le stockage local est généralement imité par un disque RAM ou un disque réseau, ce dernier étant fourni la plupart du temps par un SAN

© 1999-2017 Citrix Systems, Inc. All rights reserved.

doté d'un lien à haute vitesse. La technologie de provisioning utilisée est généralement Provisioning Services ou Machine Creation Services (ou une technologie tierce). Parfois, les systèmes provisionnés sont dotés d'un stockage local persistant sous la forme de Personal vDisks ; ces derniers sont classés comme persistants.

Ensemble, ces deux facteurs définissent les types de machines suivants :

- **Persistantes et dédiées** : machines avec OS de bureau avec une attribution statique et un Personal vDisk créées avec Machine Creation Services, bureaux avec Personal vDisks créés avec VDI-in-a-Box, postes de travail physiques et ordinateurs portables.
- **Persistantes et partagées** : machines avec OS de serveur créées avec Machine Creation Services
- **Provisionnées et dédiées** : machines avec OS de bureau avec une attribution statique mais sans Personal vDisk créées avec Provisioning Services
- **Provisionnées et partagées** : machines avec OS de bureau avec une attribution aléatoire créées avec Provisioning Services, bureaux sans Personal vDisks créés avec VDI-in-a-Box.

Les paramètres de stratégie Profile Management suivants sont suggérés pour les types de machines différents. Ils sont adaptés à la plupart des cas, mais vous pouvez en choisir d'autres plus adaptés à votre déploiement.

Important : Supprimer les profils mis en cache localement à la fermeture de session, Streaming des profils et Toujours mettre en cache sont appliqués par la fonctionnalité de configuration automatique. Ajustez les autres stratégies manuellement.

Machines permanentes

Stratégie	Persistantes et dédiées	Persistantes et partagées
Supprimer les profils mis en cache localement à la fermeture de session	Désactivée	Activé
Streaming des profils	Désactivée	Activé
Toujours mettre en cache	Activée (remarque 1)	Désactivée (remarque 2)
Réécriture active	Désactivée	Désactivée (remarque 3)
Traiter les ouvertures de session des administrateurs locaux	Activé	Désactivée (remarque 4)

Machines provisionnées

Stratégie	Provisionnées et dédiées	Provisionnées et partagées
Supprimer les profils mis en cache localement à la fermeture de session	Désactivée (remarque 5)	Activé

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Stratégie	Provisionnées et dédiées	Provisionnées et partagées
Streaming des profils	Activé	Activé
Toujours mettre en cache	Désactivée (remarque 6)	Désactivée
Réécriture active	Activé	Activé
Traiter les ouvertures de session des administrateurs locaux	Activé	Activée (remarque 7)

1. Étant donné que la stratégie Streaming des profils est désactivée pour ce type de machine, le paramètre Toujours mettre en cache est toujours ignoré.
2. Désactivez Toujours mettre en cache. Toutefois, vous pouvez vous assurer que les fichiers volumineux sont chargés dans les profils dès que possible après l'ouverture de session en activant cette stratégie et en l'utilisant pour définir une limite de taille de fichier (en Mo). Tout fichier de taille égale ou supérieure est placé en cache dès que possible.
3. Désactivez Réécriture active sauf pour enregistrer des modifications dans les profils des utilisateurs qui passent d'un serveur XenApp à un autre. Dans ce cas, activez cette stratégie.
4. Désactivez Traiter les ouvertures de session des administrateurs locaux sauf pour les bureaux partagés hébergés. Dans ce cas, activez cette stratégie.
5. Désactivez Supprimer les profils mis en cache localement à la fermeture de session. Les profils mis en cache localement sont conservés. Étant donné que les machines sont réinitialisées à la fermeture de session mais attribuées à des utilisateurs individuels, les ouvertures de session sont plus rapides si leurs profils sont mis en cache.
6. Désactivez Toujours mettre en cache. Toutefois, vous pouvez vous assurer que les fichiers volumineux sont chargés dans les profils dès que possible après l'ouverture de session en activant cette stratégie et en l'utilisant pour définir une limite de taille de fichier (en Mo). Tout fichier de taille égale ou supérieure est placé en cache dès que possible.
7. Activez Traiter les ouvertures de session des administrateurs locaux sauf pour les profils des utilisateurs qui itinèrent entre serveurs XenApp et XenDesktop. Dans ce cas, désactivez cette stratégie.

La redirection de dossiers vous permet de stocker les données utilisateur sur des partages réseau autres que l'emplacement dans lequel les profils sont stockés. Cela permet de réduire la taille du profil et de la durée de chargement, mais peut avoir un impact sur la bande passante réseau. La redirection de dossiers ne nécessite pas que les profils utilisateur Citrix soient utilisés. Vous pouvez gérer les profils utilisateur vous-mêmes, et toujours rediriger les dossiers.

Configurez la redirection de dossiers à l'aide de stratégies Citrix dans Studio.

- Assurez-vous que les emplacements réseau utilisés pour stocker le contenu de ces dossiers redirigés sont disponibles et que vous avez les permissions appropriées. Les propriétés d'emplacement sont validées.
- Les dossiers redirigés sont configurés sur le réseau et leur contenu rempli depuis les bureaux virtuels des utilisateurs à l'ouverture de session.

Remarque : configurez la redirection de dossiers à l'aide des stratégies Citrix ou des objets de stratégie de groupe Active Directory, mais pas les deux. La configuration de la redirection de dossiers à l'aide des deux moteurs de stratégie peut résulter en un comportement imprévisible.

Dans les déploiements comportant plusieurs systèmes d'exploitation (OS), il se peut que vous souhaitiez partager un profil utilisateur avec chaque système d'exploitation. Le reste du profil n'est pas partagé et est uniquement utilisé par un seul

© 1999-2017 Citrix Systems, Inc. All rights reserved.

système d'exploitation. Pour assurer une expérience utilisateur cohérente sur les systèmes d'exploitation, vous devez disposer d'une autre configuration pour chaque système d'exploitation. Cette valeur est la redirection de dossiers avancée. Par exemple, les différentes versions d'une application s'exécutant sur deux systèmes d'exploitation peuvent être nécessaires pour lire ou modifier un fichier partagé, vous décidez ainsi de le rediriger vers un emplacement réseau sur lequel les deux versions peuvent y accéder. Éventuellement, car le contenu du dossier Menu Démarrer est conçu différemment dans les deux systèmes d'exploitation, si vous décidez de rediriger uniquement un dossier, mais pas les deux. Ceci sépare le dossier Menu Démarrer et son contenu sur chaque système d'exploitation, en assurant aux utilisateurs une expérience cohérente.

Si votre déploiement requiert la redirection de dossiers avancée, vous devez comprendre la structure des données de profil de vos utilisateurs et déterminer quelles parties peuvent être partagées entre systèmes d'exploitation. Ceci est important, car un comportement imprévisible peut survenir si la redirection de dossiers est utilisée.

Pour rediriger les dossiers dans les déploiements avancés :

- Utilisez un groupe de mise à disposition distinct pour chaque système d'exploitation.
- Comprenez l'emplacement où vos applications virtuelles, y compris celles se trouvant sur des bureaux virtuels, stockent des données et des paramètres utilisateur, et la façon dont les données sont structurées.
- Pour partager les données de profil qui peuvent itinérer en toute sécurité (car elles sont conçues de manière identique dans chaque système d'exploitation), redirigez les dossiers contenant dans chaque groupe de mise à disposition.
- Pour les données de profil non partagées qui ne peuvent pas itinérer, redirigez le dossier contenant uniquement dans l'un des groupes de bureaux, généralement celui avec le système d'exploitation le plus utilisé ou celui dans lequel les données sont plus pertinentes. Éventuellement, pour les données non partagées qui ne peuvent pas itinérer entre systèmes d'exploitation, redirigez les dossiers contenant sur les deux systèmes pour séparer les emplacements réseau.

Déploiement avancé exemple : ce déploiement possède des applications, y compris des versions de Microsoft Outlook et Internet Explorer, en cours d'exécution sur des bureaux et des applications Windows 8, y compris d'autres versions d'Outlook et Internet Explorer, mises à disposition par Windows Server 2008. Pour ce faire, vous avez déjà configuré deux groupes de mise à disposition pour les deux systèmes d'exploitation. Les utilisateurs souhaitent accéder à la même série de contacts et de favoris dans les deux versions de ces deux applications.
Important : les décisions et les conseils suivants sont valides pour les systèmes d'exploitation et le déploiement décrits. Dans votre organisation, les dossiers que vous choisissez de rediriger et si vous décidez de les partager dépend d'un certain nombre de facteurs qui sont uniques à votre déploiement spécifique.

- À l'aide des stratégies appliquées aux groupes de mise à disposition, vous choisissez les dossiers suivants à rediriger.

Dossier	Redirigé dans Windows 8 ?	Redirigé dans Windows Server 2008 ?
Mes documents	Oui	Oui
Application Data	Non	Non
Contacts	Oui	Oui
Bureau	Oui	Non
Téléchargements	Non	Non
Favoris	Oui	Oui

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dossier	Redirigé dans Windows 8 ?	Redirigé dans Windows Server 2008 ?
Liens	Oui	Non
Ma musique	Oui	Oui
Mes images	Oui	Oui
Mes vidéos	Oui	Oui
Recherches	Oui	Non
Parties enregistrées	Non	Non
Menu Démarrer	Oui	Non

- Pour les dossiers partagés et redirigés :
  - Une fois l'analyse de la structure des données enregistrées par les différentes versions d'Outlook et Internet Explorer, vous décidez qu'il est préférable de partager les dossiers Contacts et Favoris
  - Vous savez que la structure des dossiers Documents, Musique, Images et Vidéos est standard sur tous les systèmes d'exploitation, il est conseillé de les stocker au même emplacement réseau pour chaque groupe de mise à disposition
- Pour les dossiers non partagés et redirigés :
  - Vous ne redirigez pas les dossiers Bureau, Liens, Recherches ou Menu Démarrer dans le groupe de mise à disposition Windows Server, car les données de ces dossiers sont organisées différemment dans les deux systèmes d'exploitation. Il ne peut donc pas être partagé.
  - Pour vous assurer un comportement prévisible de ces données non partagées, vous redirigez uniquement vers le groupe de mise à disposition de Windows 8. Vous choisissez ceci, plutôt que le groupe de mise à disposition Windows Server, car Windows 8 sera utilisé plus souvent par les utilisateurs dans leur travail quotidien ; ils peuvent uniquement accéder occasionnellement aux applications mises à disposition par le serveur. Par ailleurs, dans ce cas, les données non partagées sont plus pertinentes dans un environnement de bureau plutôt qu'un environnement d'application. Par exemple, des raccourcis Bureau sont stockés dans le dossier Bureau et peuvent être utiles s'ils proviennent d'une machine Windows 8, mais pas depuis une machine Windows Server.
- Pour les dossiers non redirigés :
  - Vous ne souhaitez pas embarrasser vos serveurs avec les fichiers téléchargés de l'utilisateur, de sorte que vous choisissez de ne pas rediriger le dossier Téléchargements.
  - Les données d'applications individuelles peuvent entraîner des problèmes de compatibilité et de performances, vous décidez ainsi de ne pas rediriger le dossier Données d'application.

Pour de plus amples informations sur la redirection de dossiers, consultez la section http://technet.microsoft.com/en-us/library/cc766489%28v=ws.10%29.aspx.

Dans Citrix Profile Management (mais pas dans Studio), une amélioration des performances vous permet d'éviter que les dossiers soient traités à l'aide d'exclusions. Si vous utilisez cette fonctionnalité, n'excluez pas les dossiers redirigés. Les

© 1999-2017 Citrix Systems, Inc. All rights reserved.

fonctionnalités de redirection et d'exclusion de dossiers fonctionnent ensemble, afin de garantir qu'aucun dossier redirigé n'est exclus et permet à Profile Management de les déplacer à nouveau dans la structure de dossiers du profil, tout en conservant l'intégrité des données, si vous décidez de ne pas de les rediriger ultérieurement. Pour plus d'informations sur les exclusions, veuillez consulter la section Inclure et exclure des éléments.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Insight Services

Jul 07, 2016

Citrix Insight Services (CIS) est la plate-forme Citrix sur laquelle les informations de diagnostic et de dépannage sont recueillies. Elle permet aux utilisateurs techniques (clients, partenaires et techniciens) de diagnostiquer et de résoudre les problèmes ainsi que d'optimiser leurs environnements. Pour plus d'informations sur CIS et son fonctionnement, veuillez consulter le site https://cis.citrix.com/(informations d'identification de compte Citrix requises).

Toutes les informations chargées sur Citrix Insight Services sont utilisées à des fins de dépannage et de diagnostic, ainsi que pour améliorer la qualité, la fiabilité et les performances des produits, sous réserve de ce qui suit :

- Politique Citrix Insight Services sur https://cis.citrix.com/legal
- Déclaration de confidentialité Citrix sur http://www.citrix.com/about/legal/privacy.html

Cette version de XenApp et XenDesktop prend en charge les technologies et outils suivants.

Installer et mettre à niveau les outils d'analyse

Lorsque vous utilisez le programme d'installation du produit complet pour déployer et mettre à niveau les composants XenApp ou XenDesktop, des informations anonymes sur le processus d'installation sont collectées et stockées sur la machine sur laquelle vous installez/mettez à niveau le composant. L'assistance peut vous aider à charger ces informations, qui seront utilisées pour aider Citrix à améliorer l'expérience d'installation de ses clients.

Les informations sont stockées localement sous %ProgramData%\Citrix\.

Programme d'amélioration de l'expérience du client Citrix (CEIP)

Lorsque vous choisissez de participer au Programme d'amélioration de l'expérience utilisateur (CEIP), des informations d'utilisation et des statistiques anonymes sont envoyées à Citrix pour nous aider à améliorer la qualité et les performances des produits Citrix. Pour de plus amples informations, consultez la section http://more.citrix.com/XD-CEIP.

Vous êtes automatiquement inscrit au programme CEIP lorsque vous créez un site XenApp ou XenDesktop. Le premier chargement de données se produit approximativement sept jours après la création du site. Vous pouvez arrêter votre participation à tout moment après la création du site ; sélectionnez le nœud **Configuration** dans le panneau de navigation de Studio (onglet Assistance produit) et suivez les instructions.

Vous pouvez également participer au programme CEIP lorsque vous installez des produits, composants et technologies Citrix, tels que Provisioning Services, AppDNA, le serveur de licences Citrix, Citrix Receiver pour Windows, le serveur d'impression universelle, l'enregistrement de session. Consultez la documentation respective de chaque composant pour de plus amples informations sur l'installation et les valeurs de participation par défaut.

Lorsque vous mettez à niveau un déploiement de XenApp ou XenDesktop :

- Si vous mettez à niveau à partir d'une version qui ne prend pas en charge le programme CEIP, le système vous demandera

© 1999-2017 Citrix Systems, Inc. All rights reserved.

si vous souhaitez y prendre part.

- Si vous mettez à niveau à partir d'une version qui prend en charge le programme CEIP et que la participation a été activée, CEIP sera activé dans le site mis à niveau.
- Si vous mettez à niveau à partir d'une version qui prend en charge le programme CEIP et que la participation a été désactivée, CEIP sera désactivé dans le site mis à niveau.
- Si vous mettez à niveau à partir d'une version qui prend en charge le programme CEIP et que la participation est inconnue, le système vous demandera si vous souhaitez y prendre part.

Les informations collectées sont anonymes, de façon à ce qu'elles ne puissent pas être consultées après leur chargement auprès de Citrix Insight Services.

Call Home

Lors de l'installation de certains composants et fonctionnalités de XenApp ou XenDesktop, vous aurez la possibilité de participer à Citrix Call Home. Call Home collecte des données de diagnostic, puis charge périodiquement des paquets de télémétrie contenant ces données directement à Citrix Insight Services à des fins d'analyse et de résolution des problèmes.

Call Home s'exécute en tant que service d'arrière-plan sous le nom Service de télémétrie Citrix.

Pour de plus amples informations, consultez http://more.citrix.com/XD-CALLHOME.

Quelles informations sont collectées ?

Le traçage Citrix Diagnostic Facility (CDF) consigne les informations qui peuvent être utiles pour la résolution des problèmes. Call Home collecte un sous-ensemble des traces CDF qui peut être utile lors de la résolution des problèmes courants, par exemple, les enregistrements de VDA et le lancement d'application/bureau. Cette technologie est appelée traçage permanent (AOT). Call Home ne recueille pas d'autres informations de Suivi d'événements pour Windows (ETW), et ne peut pas être configuré pour le faire.

Call Home recueille également d'autres informations, telles que :

- Clés de registre créées par XenApp et XenDesktop sous HKEY_LOCAL_MACHINE\SOFTWARE\Citrix
- Informations Infrastructure de gestion Windows (WMI) sous l'espace de noms de Citrix
- Liste des processus en cours d'exécution
- Vidages sur incident des processus Citrix qui sont stockés dans %PROGRAM DATA%\Citrix\CDF

Les informations de trace sont compressées lorsqu'elles sont collectées. Le Service de télémétrie Citrix conserve environ 20 Mo d'informations de traçage compressées. En règle générale, cela contient des informations sur les 24-48 heures précédentes, en fonction du volume de traces généré durant cet intervalle.

- La compression des données permet à Call Home de limiter l'encombrement sur le VDA.
- Les traces sont stockées dans la mémoire pour éviter des opérations d'entrées/sortie sur les machines provisionnées.
- Le tampon de suivi utilise un mécanisme circulaire pour conserver les traces en mémoire.

Vous pouvez indiquer si vous souhaitez ou non participer à Call Home lorsque vous installez un Delivery Controller ou un VDA à l'aide de l'interface graphique du programme d'installation du produit complet.

Après l'installation des composants, vous pouvez utiliser les applets de commande PowerShell pour :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Activer les chargements planifiés de Call Home ou modifier votre calendrier actuel. Ceci comprend l'activation des chargements planifiés dans une image principale utilisée dans un catalogue de machines, ce qui évite d'avoir à configurer Call Home dans chaque VM créée.
- Collecter manuellement les données et les charger sur CIS.
- Collecter manuellement les données et les stocker localement, puis les charger ultérieurement sur CIS.

Pour obtenir une syntaxe complète des applets de commande PowerShell, consultez l'aide des applets de commande.

Si vous avez opté pour le chargement de données Call Home à intervalles réguliers et que vous chargez manuellement des informations de diagnostic sur CIS, vous devez fournir les informations d'identification d'accès au compte Citrix. CIS échange les informations d'identification contre un *jeton de chargement* qui est utilisé pour identifier le client et charger les données. Les informations d'identification ne sont pas enregistrées.

Lorsqu'un chargement se produit, une notification est envoyée par e-mail à l'adresse associée au compte Citrix.

Vous pouvez choisir de charger des données sur Call Home à intervalles réguliers lors de l'utilisation de l'assistant d'installation du produit complet ou plus tard, à l'aide d'applets de commande PowerShell. Par défaut, les données sont collectées et chargées sur CIS chaque dimanche à environ 3h00 du matin, heure locale. L'heure de chargement est aléatoire avec un intervalle de deux heures depuis l'heure spécifiée. Cela signifie qu'un chargement avec la programmation par défaut se produit entre 3h00 et 5h00.

Si vous ne souhaitez pas charger d'informations de diagnostic à intervalles réguliers, vous pouvez toujours utiliser les applets de commande PowerShell pour collecter et charger manuellement les données Call Home.

Activer des chargements programmés lors de l'installation de composants

Lorsque vous utilisez l'interface graphique du programme d'installation complet de XenApp et de XenDesktop pour installer un Controller ou un VDA, vous pouvez indiquer si vous souhaitez participer ou non au chargement programmé d'informations sur Call Home. Par défaut, la participation est sélectionnée.

- Si vous voulez participer, connectez-vous à CIS l'aide des informations d'identification de votre compte Citrix.
- Si vous ne souhaitez pas participer (ou si vous souhaitez participer, mais que les informations d'identification de votre compte Citrix n'ont pas pu être validées), refusez de participer sur la page de l'assistant. Vous pouvez vous inscrire ultérieurement après l'installation du site, à l'aide des applets de commande PowerShell.

Activer des chargements programmés à l'aide d'applets de commande PowerShell

Entrez les applets de commande suivantes pour activer le chargement programmé d'informations de diagnostic Call Home sur CIS. Si vous n'entrez pas d'applets de commande supplémentaires pour un programme personnalisé, le programme par défaut est utilisé.

```
$cred = Get-Credentials
Enable-CitrixCallHome -Credential $cred
```

Pour confirmer que les chargements programmés sont activés, entrez Get-CitrixCallHome. Cette commande devrait renvoyer IsEnabled=True et IsMasterImage=False.

Activer des chargements programmés pour des machines créées à partir d'une image principale

L'activation de chargements programmés dans une image principale vous évite d'avoir à configurer chaque machine qui est

© 1999-2017 Citrix Systems, Inc. All rights reserved.

créée dans le catalogue de machines.

```
Enable-CitrixCallHome -Credential $cred -MasterImage
```

Pour confirmer que les chargements programmés sont activés, entrez Get-CitrixCallHome. Cette commande devrait renvoyer IsEnabled=True et IsMasterImage=True.

Créer un calendrier personnalisé

Vous pouvez créer un calendrier quotidien ou hebdomadaire personnalisé.

```
$timespan = New-TimeSpan –Hours -Minutes
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek -UploadFrequency {Daily|Weekly}
```

Annuler des chargements programmés

Entrez l'applet de commande suivante pour annuler des chargements programmés. (Vous pouvez toujours charger des données de diagnostic à l'aide d'applets de commande PowerShell.)

```
Disable-CitrixCallHome
```

Pour confirmer que les chargements programmés sont désactivés, entrez Get-CitrixCallHome. Cette commande devrait renvoyer IsEnabled=False et IsMasterImage=False.

Exemples

Les applets de commande suivantes créent un programme qui collecte et charge les données à 23:20 chaque soir. Notez que le paramètre Heures utilise une horloge de 24 heures. Lorsque la valeur du paramètre UploadFrequency est Daily, le paramètre DayOfWeek est ignoré, s'il est spécifié.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

Pour confirmer le programme, entrez Get-CitrixCallHomeSchedule. Dans l'exemple ci-dessus, cette commande devrait renvoyer StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily.

Les applets de commande suivantes créent un programme qui collecte et charge les données à 23:20 chaque mercredi soir.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed -UploadFrequency Weekly
```

Pour confirmer le programme, entrez Get-CitrixCallHomeSchedule. Dans l'exemple ci-dessus, cette commande devrait renvoyer StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly.

Vous pouvez utiliser le site Web CIS pour charger des packages d'informations de diagnostic sur CIS. Vous pouvez également utiliser les applets de commande PowerShell pour collecter et charger des informations de diagnostic sur CIS.

Pour charger un package à l'aide du site Web CIS :

1. Connectez-vous à Citrix Insight Services à l'aide des informations d'identification de votre compte Citrix.
2. Sélectionnez **My Workspace**.
3. Sélectionnez **Healthcheck**, puis accédez à l'emplacement de vos données.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

CIS prend en charge plusieurs applets de commande PowerShell qui gèrent le chargement de données. Cette documentation couvre les applets de commande pour deux cas courants :

- Utilisez l'applet de commande Start-CitrixCallHomeUpload pour collecter et charger manuellement un package d'informations de diagnostic sur CIS. (Le package n'est pas enregistré localement).
- Utilisez l'applet de commande Start-CitrixCallHomeUpload pour collecter manuellement des données et stocker un package d'informations de diagnostic localement. Cela vous permet d'afficher un aperçu des données. Ensuite, à une date ultérieure, utilisez l'applet de commande Send-CitrixCallHomeBundle pour charger manuellement une copie de ce package sur CIS. (Les données que vous avez enregistrées à l'origine restent locales).

L'aide de PowerShell fournit une syntaxe complète, y compris des descriptions des applets de commande et des paramètres qui ne sont pas utilisés dans ces cas d'utilisation courants.

Lorsque vous entrez une applet de commande pour charger des données sur CIS, vous êtes invité à confirmer le chargement. Si l'applet de commande expire avant que le chargement ne soit terminé, vérifiez l'état du chargement dans le journal d'événements système. La demande de chargement peut être rejetée si le service est déjà en train d'effectuer un chargement.

Collecter des données et charger le package sur CIS

Start-CitrixCallHomeUpload [-Credential] [-InputPath] [-Description] [-IncidentTime] [-SRNumber] [-Name] [-UploadHeader] [-AppendHeaders] [-Collect] []

Collecter des données et les enregistrer localement

Start-CitrixCallHomeUpload -OutputPath [-InputPath] [-Description] [-IncidentTime] [-SRNumber] [-Name] [-UploaderHeader] [-AppendHeaders] [-Collect] []

Paramètre	Description
Credential	Dirige le chargement sur CIS.
InputPath	Emplacement du fichier zip à inclure dans le package. Il peut s'agir d'un fichier supplémentaire qui vous a été demandé par l'assistance de Citrix. Veillez à inclure l'extension .zip.
OutputPath	Emplacement où les informations de diagnostic seront enregistrées. Ce paramètre est requis lors de l'enregistrement des données Call Home localement.
Description et Incident Time	Informations sur le chargement en format libre.
SRNumber	Numéro d'incident de l'assistance technique de Citrix.
Name	Nom qui identifie le package.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

UploadHeader	Chaîne au format JSON qui spécifie les en-têtes de chargement chargés sur CIS.
AppendHeaders	Chaîne au format JSON qui spécifie les en-têtes ajoutés chargés sur CIS.
Collect	Chaîne au format JSON qui spécifie les données à collecter ou ignorer, au format {'collector':{'enabled':Boolean}}", où Boolean est true ou false. Valeurs de collecteur valides : • 'wmi' • 'process' • 'registry • "crashreport' • 'trace' • 'localdata' • 'sitedata' Si ce paramètre est omis, les données de tous les autres collecteurs sont collectées.
Common Parameters	Consultez l'aide de PowerShell.

Charger des données qui étaient préalablement enregistrées localement

```
Send-CitrixCallHomeBundle -Credential -Path []
```

Le paramètre Path spécifie l'emplacement dans lequel le package était préalablement enregistré.

Exemples

L'applet de commande suivante demande le chargement des données Call Home (à l'exception des données du collecteur WMI) sur CIS. Ces données sont liées aux échecs d'enregistrement des VDA PVS, ce qui est indiqué à 14:30 pour le ticket de support technique de Citrix 123456. En plus des données Call Home, le fichier « c:\Diagnostics\ExtraData.zip » sera incorporé au package chargé.

```
C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.zip" -Description "Registration failures with PVS VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}" -UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

L'applet de commande suivante enregistre les données Call Home liées au ticket de support technique de Citrix 223344, ce qui est indiqué à 8:15. Les données seront enregistrées dans le fichier mydata.zip sur un partage réseau. En plus des données Call Home, le fichier « c:\Diagnostics\ExtraData.zip » sera incorporé au package enregistré.

```
C:\PS>Start-CitrixCallHomeUpload -OutputPath \\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip" -Description "Diagnostics for incident number 223344" -IncidentTime "8:15" -SRNumber 223344
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

L'applet de commande suivante charge le package de données que vous avez enregistré précédemment.

```
$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \\mynetwork\myshare\mydata.zip
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Surveiller

Jul 07, 2016

Les administrateurs et le personnel d'assistance technique peuvent surveiller les sites XenApp et XenDesktop à l'aide d'un grand nombre de fonctionnalités et d'outils. À l'aide de ces outils, vous pouvez surveiller :

- les sessions utilisateur et l'utilisation des sessions ;
- les performances d'ouverture de session ;
- les connexions et les machines, y compris les échecs ;
- le calcul de charge ;
- les tendances historiques ;
- l'infrastructure.

Citrix Director

Director est un outil Web en temps réel que vous pouvez utiliser pour effectuer la surveillance et la résolution des problèmes, et réaliser des tâches d'assistance pour les utilisateurs finaux.

Pour de plus amples informations, veuillez consulter les articles Director.

Enregistrement de session

L'enregistrement de session vous permet d'enregistrer les activités à l'écran de toute session utilisateur, sur tout type de connexion, depuis n'importe quel serveur exécutant XenApp sous réserve du respect des stratégies d'entreprise et des exigences réglementaires. L'enregistrement de session enregistre, catalogue et archive les sessions pour en permettre la récupération et la lecture.

L'enregistrement de session utilise des stratégies flexibles pour déclencher l'enregistrement automatique des sessions d'application. Cela permet aux services informatiques de vérifier et d'examiner l'activité des utilisateurs sur les applications - par exemple pour des opérations financières ou des systèmes de gestion d'informations des patients dans un contexte médical - tout en assurant un contrôle interne dans un souci de conformité à la règlementation et de surveillance de la sécurité. De même, l'enregistrement de session facilite également le travail du support technique en accélérant l'identification et la résolution des problèmes.

Pour de plus amples informations, consultez les articles Enregistrement de session.

Journalisation de la configuration

La journalisation de la configuration est une fonctionnalité qui permet aux administrateurs de garder un suivi des modifications administratives apportées à un site. La journalisation de la configuration peut aider les administrateurs à identifier et résoudre les problèmes lorsque des modifications sont apportées à la configuration, à la gestion des modifications et au suivi des modifications, et à la création d'un rapport d'activité d'administration.

Vous pouvez afficher et générer des rapports sur les informations de journalisation à partir de Studio. Vous pouvez également afficher les éléments journalisés dans Director avec l'interface Trend View pour fournir des notifications des modifications apportées à la configuration. Cette fonctionnalité est utile pour les administrateurs qui n'ont pas accès à Studio.

La vue Trend View fournit des données d'historique des modifications apportées à la configuration sur une période de temps afin que les administrateurs puissent évaluer les modifications qui ont été apportées au site, lorsqu'ils ont été générés

© 1999-2017 Citrix Systems, Inc. All rights reserved.

et qui les a effectuées pour trouver la cause d'un problème. Cette vue trie les informations de configuration en trois catégories.

- Échecs de connexion
- Machines de bureau en échec
- Machines de serveur en échec

Pour de plus amples informations sur la marche à suivre pour activer et configurer la journalisation de la configuration, consultez l'article Journalisation de la configuration. Les articles Director décrivent comment afficher les informations de session à partir de cet outil.

API Monitor Service avec le protocole OData

Les administrateurs peuvent utiliser l'API de Monitor Service du site pour rechercher les données d'historique à l'aide du protocole OData. Ceci permet au département informatique d'analyser les tendances historiques à des fins de planification pour réaliser une résolution des problèmes de connexion et des échecs de machine détaillés et extraire des informations de chargement dans d'autres outils et processus.

Le schéma du service Monitor fournit les types de données suivants :

- des données liées à des échecs de connexion ;
- des machines dans un état d'échec ;
- l'utilisation de la session ;
- la durée d'ouverture de session ;
- les données d'équilibrage de charge ;

Pour de plus amples informations, consultez les articles sur l'API Monitor Service OData.

Outil de diagnostic Personal vDisk

Utilisez l'outil de diagnostic PvD afin de contrôler les modifications apportées par les utilisateurs aux parties utilisateur et application de leurs Personal vDisks, telles que les applications qu'ils ont installées et les fichiers qu'ils ont modifiés.

Pour de plus amples informations, consultez l'article Surveiller les Personal vDisks.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Enregistrement de session

Jul 07, 2016

L'enregistrement de session vous permet d'enregistrer les activités à l'écran de toute session utilisateur hébergée sur une machine VDI avec OS de serveur, avec tout type de connexion, sous réserve du respect des stratégies d'entreprise et des exigences réglementaires. L'enregistrement de session enregistre, catalogue et archive les sessions pour en permettre la récupération et la lecture.

L'enregistrement de session utilise des stratégies flexibles pour déclencher l'enregistrement automatique des sessions d'application. Cela permet aux services informatiques de vérifier et d'examiner l'activité des utilisateurs sur les applications - par exemple pour des opérations financières ou des systèmes de gestion d'informations des patients dans un contexte médical - tout en assurant un contrôle interne dans un souci de conformité à la règlementation et de surveillance de la sécurité. De même, l'enregistrement de session facilite également le travail du support technique en accélérant l'identification et la résolution des problèmes.

Avantages

Sécurité renforcée via la journalisation et la surveillance. L'enregistrement de session permet aux organisations d'enregistrer l'activité des utilisateurs à l'écran pour les applications traitant des informations sensibles. Ceci est particulièrement important dans les secteurs réglementés tels que la santé et les finances. Dans les situations dans lesquelles les informations personnelles ne doivent pas être enregistrées, un enregistrement sélectif peut être défini à l'aide de stratégies.

Contrôle des activités performant. L'enregistrement de session capture et met en archive les mises à jour d'écran, notamment les activités de la souris et le résultat visible de frappes clavier sur des fichiers vidéo sécurisés afin de fournir un enregistrement des activités d'utilisateurs, d'applications et de serveurs spécifiques.

L'enregistrement de session n'est pas conçu pour contribuer à la collecte de preuves en vue de poursuites judiciaires. Citrix recommande que les organisations utilisant l'enregistrement de session utilisent d'autres techniques pour la collecte de preuves, telles que des enregistrements vidéo conventionnels combinés avec des outils d'eDiscovery traditionnels.

Réduction de la durée de résolution de problèmes. Lorsque les utilisateurs appellent pour exposer un problème difficile à reproduire, le personnel de support technique peut activer les enregistrements des sessions utilisateur. Lorsque le problème se reproduit, l'enregistrement de session fournit un enregistrement visuel horodaté de l'erreur, qui peut être utilisé ensuite pour une résolution plus rapide des problèmes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Prise en main de l'enregistrement de session

Jul 07, 2016

Après avoir effectué les étapes suivantes, vous pouvez commencer l'enregistrement et la vérification des sessions XenApp et XenDesktop.

1. Familiarisation avec les composants d'enregistrement de session.
2. Sélection du scénario de déploiement pour votre environnement.
3. Vérification des conditions requises pour l'installation.
4. Installation des fonctionnalités et des rôles Windows requis.
5. Installation de l'enregistrement de session.
6. Configuration des composants d'enregistrement de session pour permettre l'enregistrement et l'affichage de sessions.

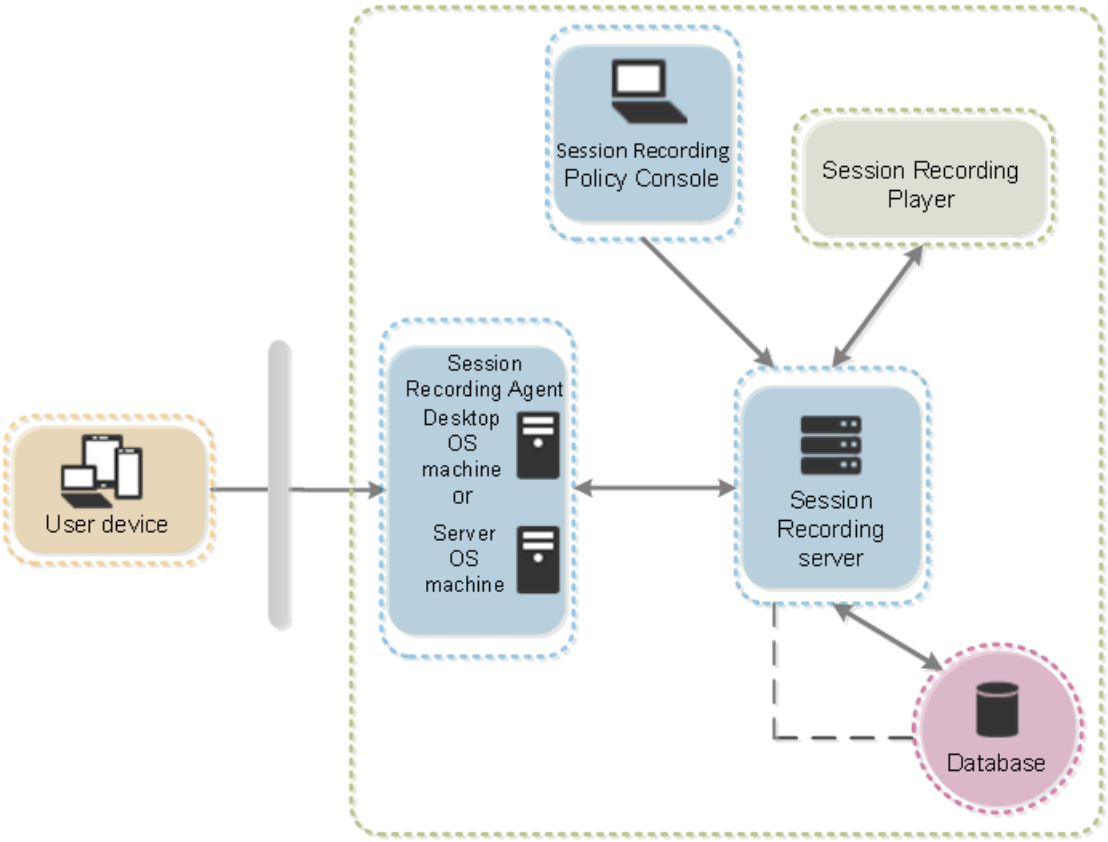
L'enregistrement de session se compose de cinq composants :

- **Agent d'enregistrement de session.** Composant installé sur chaque machine dotée d'un OS de serveur et de Server VDI pour activer l'enregistrement. Il est responsable de l'enregistrement des données de session.
- **Serveur d'enregistrement de session.** Il s'agit d'un serveur hébergeant ce composant :
  - Le broker. Une application Web IIS 6.0+ hébergée qui traite les requêtes de recherche et les demandes de fichier du lecteur d'enregistrement de session, qui gère les demandes d'administration de stratégies de la console de stratégie d'enregistrement de session et qui évalue les stratégies d'enregistrement pour chaque session XenApp et XenDesktop.
  - Le gestionnaire de stockage. Service Windows qui gère les fichiers de sessions enregistrées reçues de chaque ordinateur d'enregistrement de session exécutant XenApp et XenDesktop.
- **Lecteur d'enregistrement de session.** Il s'agit d'une interface utilisateur à laquelle les utilisateurs accèdent depuis une station de travail pour lire des fichiers de sessions XenApp et XenDesktop enregistrées.
- **Base de données d'enregistrement de session.** Composant qui gère la base de données SQL Server pour stocker les données de sessions enregistrées. Lorsque ce composant est installé, il crée une base de données appelée **CitrixSessionRecording**. Vous ne pouvez pas modifier le nom.
- **Console de stratégie d'enregistrement de session.** Console utilisée pour créer des stratégies afin de spécifier les sessions à enregistrer.

Illustration des composants d'enregistrement de session et des relations qu'ils ont entre eux.

Dans l'exemple de déploiement représenté par cette illustration, l'agent d'enregistrement de session, le serveur d'enregistrement de session, la base de données d'enregistrement de session, la console de stratégie d'enregistrement de session et le lecteur d'enregistrement de session résident sous la protection d'un pare-feu de sécurité. L'agent d'enregistrement de session est installé sur une machine dotée d'un OS de serveur. Un second serveur héberge la console de stratégie d'enregistrement de session, un troisième remplit les fonctions de serveur d'enregistrement de session, tandis qu'un quatrième serveur héberge la base de données d'enregistrement de session. Le lecteur d'enregistrement de session est installé sur une station de travail séparée. Une machine cliente, située en-dehors du pare-feu, communique avec la machine dotée de l'OS de serveur sur laquelle l'agent d'enregistrement de session est installé. À l'intérieur du pare-feu, l'agent d'enregistrement de session, la console de stratégie d'enregistrement de session, le lecteur d'enregistrement de session et la base de données d'enregistrement de session communiquent tous avec le serveur d'enregistrement de session.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Planifier votre déploiement

Jul 07, 2016

Limitations et restrictions

L'enregistrement de session ne prend pas en charge le mode d'affichage de redirection Desktop Composition (DCR). Par défaut, l'enregistrement de session désactive DCR dans une session si la session doit être enregistrée par stratégie d'enregistrement. Vous pouvez configurer ce comportement dans les propriétés de l'agent d'enregistrement de session.

En fonction de votre environnement, vous pouvez déployer les composants d'enregistrement de session selon des scénarios différents.

Un déploiement d'enregistrement de session ne se limite pas nécessairement à un seul site. À l'exception de l'agent d'enregistrement de session, tous les composants sont indépendants du site de serveur. Vous pouvez par exemple configurer plusieurs sites pour utiliser un serveur d'enregistrement de session unique.

De même, si vous avez un site de grande taille comptant de nombreux agents et que vous prévoyez d'enregistrer un grand nombre d'applications au graphisme intensif (applications AutoCAD par exemple), ou si vous avez un nombre élevé de sessions à enregistrer, il est possible qu'un serveur d'enregistrement de session doive répondre à des demandes de performances élevées. Pour remédier à tout problème de performance, vous pouvez installer plusieurs serveurs d'enregistrement de session sur des ordinateurs différents et orienter les agents d'enregistrement de session vers ces différents ordinateurs. Souvenez-vous qu'un Agent ne peut pointer que vers un seul serveur à la fois.

Suggestions de scénarios de déploiement

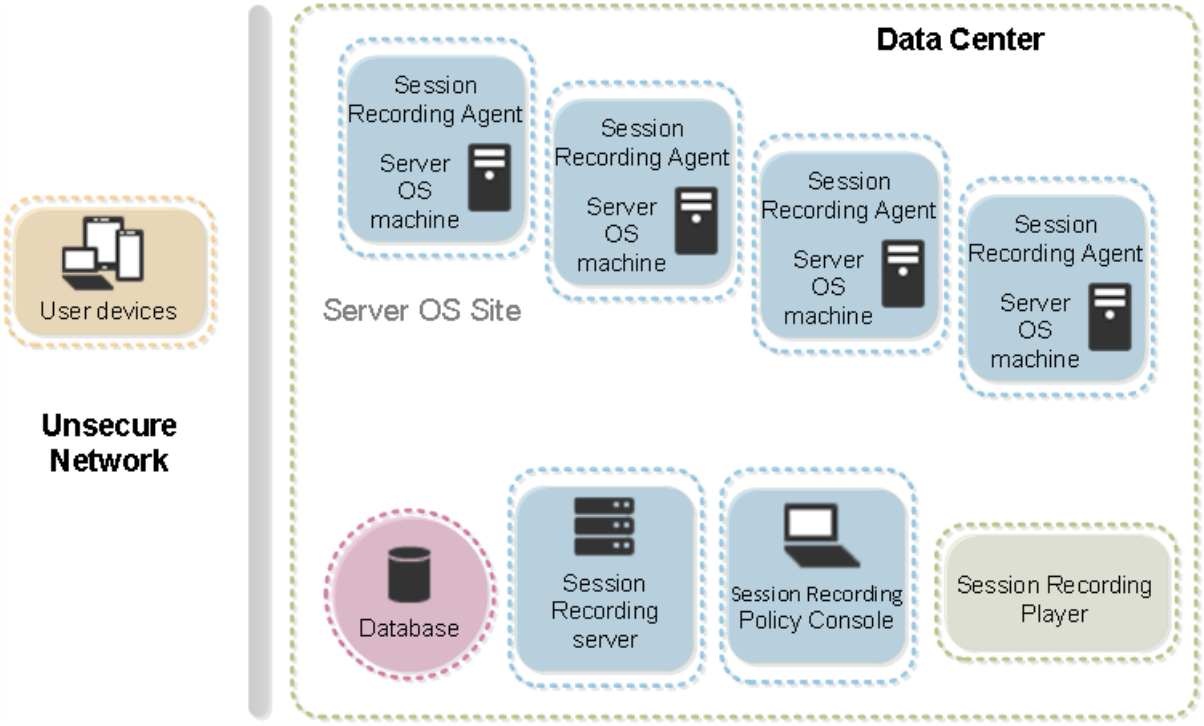
Ci-dessous figure une description succincte de deux suggestions de configuration pour un déploiement d'enregistrement de session :

- déploiement de l'agent d'enregistrement de session sur une seule machine avec OS de serveur ;
- déploiement de l'agent d'enregistrement de session sur plusieurs machines avec OS de serveur ou OS de bureau sur un site.

Déploiement d'un site de serveurs

Utilisez ce type de déploiement pour l'enregistrement de sessions pour un ou plusieurs sites. L'agent d'enregistrement de session est installé sur chaque machine dotée d'un OS de serveur dans un site. Le site réside dans un centre de données protégé par un pare-feu de sécurité. Les composants d'administration d'enregistrement de session (base de données d'enregistrement de session, serveur d'enregistrement de session, console de stratégie d'enregistrement de session) sont installés sur d'autres serveurs et le lecteur d'enregistrement de session est installé sur une station de travail, l'ensemble est protégé par le pare-feu, mais ne se trouve pas dans le centre de données. À l'extérieur du pare-feu, dans un environnement de réseau non sécurisé, se trouvent les clients XenApp, par exemple une station de travail, un PDA et un ordinateur portable.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Remarques importantes sur le déploiement

- Pour activer les composants d'enregistrement de session de manière à ce qu'ils communiquent entre eux, veillez à les installer dans le même domaine ou à travers des domaines de confiance. Le système ne peut pas être installé dans un groupe de travail ou à travers des domaines ayant une relation de confiance externe.
- Cette version ne prend pas en charge la mise en cluster de deux serveurs d'enregistrement de session ou plus dans un déploiement.
- En raison de sa nature graphique intensive et de l'utilisation faite de mémoire lors de la lecture des enregistrements de grande taille, Citrix déconseille d'installer le lecteur d'enregistrement de session en tant qu'application publiée.
- L'installation de l'enregistrement de session est configurée pour la communication TLS/HTTPS. Veillez à installer un certificat sur le serveur d'enregistrement de session et à ce que les composants d'enregistrement de session fassent confiance à la racine CA.
- Si vous installez la base de données d'enregistrement de session sur un serveur autonome exécutant SQL Server 2014 édition Express, SQL Server 2012 édition Express ou SQL Server 2008 R2 édition Express, veillez à activer le protocole TCP/IP sur le serveur et exécuter le service de navigateur SQL Server. Ces paramètres sont désactivés par défaut, mais vous devez les activer pour que le serveur d'enregistrement de session puisse communiquer avec la base de données. Veuillez consulter la documentation Microsoft pour des informations sur l'activation de ces paramètres.
- Considérez les effets du partage de session lors de la planification de votre déploiement d'enregistrement de session. Le partage de session pour les applications publiées peut entrer en conflit avec les règles de stratégie d'enregistrement de session pour les applications publiées. L'enregistrement de session fait correspondre la stratégie active à la première application publiée qu'un utilisateur ouvre. Après que l'utilisateur ouvre la première application, toute application suivante ouverte au cours de la même session continue d'observer la stratégie en vigueur pour la première application. Par exemple, si une stratégie indique que seul Outlook doit être enregistré, l'enregistrement commence lorsque l'utilisateur ouvre Outlook. Cependant, si l'utilisateur ouvre ensuite une application Microsoft Word publiée (pendant qu'Outlook est ouvert), Word est également enregistré. De la même manière, si la stratégie active n'indique pas que Word doit être enregistré, et que l'utilisateur démarre Word avant Outlook (qui devrait être enregistré, selon la stratégie), Outlook n'est pas enregistré.
- Bien que vous puissiez installer le serveur d'enregistrement de session sur un Delivery Controller, Citrix ne recommande pas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de le faire en raison de problèmes de performances.

- Vous pouvez installer la console de stratégie d'enregistrement de session sur un Delivery Controller.
- Vous pouvez installer le serveur d'enregistrement de session et la console de stratégie d'enregistrement de session sur le même système.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Recommandations de sécurité

Jul 07, 2016

L'enregistrement de session est conçu pour un déploiement au sein d'un réseau sécurisé, son accès est réservé aux administrateurs et par conséquent il est lui-même sécurisé. Le déploiement prêt à l'emploi est conçu dans un souci de simplicité et les fonctionnalités de sécurité, telles que la signature et le cryptage numériques peuvent être configurés en option.

La communication entre les composants d'enregistrement de session est assurée par les Services Internet (IIS) et Microsoft Message Queuing (MSMQ). IIS fournit la liaison de communication des services Web entre chaque composant d'enregistrement de session. MSMQ fournit un mécanisme fiable de transport des données pour l'envoi des données de session de l'agent d'enregistrement de session vers le serveur d'enregistrement de session.

Tenez compte des recommandations de sécurité suivantes lors de la planification de votre déploiement :

- Assurez-vous que vous isolez correctement les différents rôles administrateur dans le réseau de l'entreprise, dans le système d'enregistrement de session ou sur des machines individuelles. Sinon, vous vous exposez à des risques de sécurité qui peuvent avoir un impact sur la fonctionnalité du système ou entraîner une utilisation abusive du système. Citrix vous recommande d'attribuer des rôles d'administrateur différents à des personnes ou des comptes différents et de ne pas autoriser les utilisateurs de session à disposer de privilèges d'administrateur sur le système VDA.
  - Les administrateurs de XenApp et XenDesktop ne doivent pas accorder de rôle d'administrateur local VDA à des utilisateurs d'applications ou de bureaux publiés. Si le rôle d'administrateur local est requis, protégez les composants de l'agent d'enregistrement de session avec des mécanismes Windows ou des solutions tierces.
  - Attribuez séparément l'administrateur de base de données d'enregistrement de session et l'administrateur de stratégie d'enregistrement de session.
  - Citrix recommande de ne pas attribuer de privilèges d'administrateur VDA aux utilisateurs de sessions, particulièrement lors de l'utilisation de Remote PC Access.
  - Le compte d'administrateur local de serveur d'enregistrement de session doit être un compte à protection élevée.
  - Contrôlez l'accès aux machines installées avec le lecteur d'enregistrement de session. Si un utilisateur ne dispose pas du rôle Lecteur, n'accordez pas à cet utilisateur le rôle d'administrateur local pour une machine lecteur. Désactivez l'accès anonyme.
  - Citrix recommande d'utiliser une machine physique en tant que serveur de stockage pour l'enregistrement de session.
- L'enregistrement de session enregistre les activités graphiques des sessions sans tenir compte de la confidentialité des données. Dans certaines circonstances, des données sensibles (notamment, mais pas exclusivement, des informations d'identification d'utilisateur, des informations personnelles et des écrans de tierce partie) peuvent être enregistrées involontairement. Prenez les mesures suivantes pour éviter tout risque :

    + Désactivez l'image mémoire principale pour les machines des VDA sauf pour un dépannage spécifique.

        Pour désactiver l'image mémoire principale :

        1. Cliquez avec le bouton droit sur Poste de travail, puis cliquez sur Propriétés.
        2. Cliquez sur l'onglet Avancé, puis dans la section Démarrage et récupération, cliquez sur Paramètres.
        3. Sous Écriture des informations de débogage, sélectionnez (aucune).

        Consultez l'article https://support.microsoft.com/en-us/kb/307973.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

+ Assurez-vous que les informations d'identification d'ouverture de session ou les informations personnelles ne s'affichent pas dans les applications locales et Web publiées ou utilisées à l'intérieur de l'entreprise, sinon elles sont enregistrées par l'enregistrement de session.

+ Les utilisateurs doivent fermer toutes les applications qui pourraient exposer des informations confidentielles avant de basculer vers une session ICA distante.

+ Les propriétaires de session doivent avertir les participants que les logiciels de réunion en ligne et d'assistance à distance peuvent être enregistrés si une session de bureau est enregistrée.

+ Autorisez uniquement les méthodes d'authentification automatiques (par exemple, l'authentification unique, la carte à puce) pour accéder à des bureaux ou à des applications publiés.

- L'enregistrement de session s'appuie sur des matériels et une infrastructure matérielle spécifiques (par exemple, des périphériques de réseau d'entreprise, un système d'exploitation) pour fonctionner correctement et pour satisfaire aux exigences en termes de sécurité. Prenez des mesures aux différents niveaux des infrastructures pour empêcher l'endommagement ou l'abus de ces infrastructures et sécuriser la fonction d'enregistrement de session.
  - Protégez correctement l'infrastructure réseau sur laquelle repose l'enregistrement de session et assurez sa disponibilité.
  - Citrix recommande d'utiliser une solution de sécurité tierce ou un mécanisme Windows pour protéger les composants d'enregistrement de session. Les composants d'enregistrement de session sont les suivants :
    - Sur le serveur d'enregistrement de session
      - Processus : SsRecStoragemanager.exe et SsRecAnalyticsService.exe
      - Services : CitrixSsRecStorageManager et CitrixSsRecAnalyticsService
      - Tous les fichiers du dossier d'installation du serveur d'enregistrement de session
      - Clés de registre dans HKLM\Software\Citrix\SmartAuditor\Server
    - Sur l'agent d'enregistrement de session
      - Processus : SsRecAgent.exe
      - Service : CitrixSmAudAgent
      - Tous les fichiers du dossier d'installation de l'agent d'enregistrement de session
      - Clés de registre dans HKLM\Software\Citrix\SmartAuditor\Agent
- Définissez la liste de contrôle d'accès (ACL) pour Message Queuing (MSMQ) sur le serveur d'enregistrement de session afin de restreindre les machines VDA ou VDI qui peuvent envoyer des données MSMQ au serveur d'enregistrement de session et empêcher les machines non autorisées d'envoyer des données au serveur d'enregistrement de session.

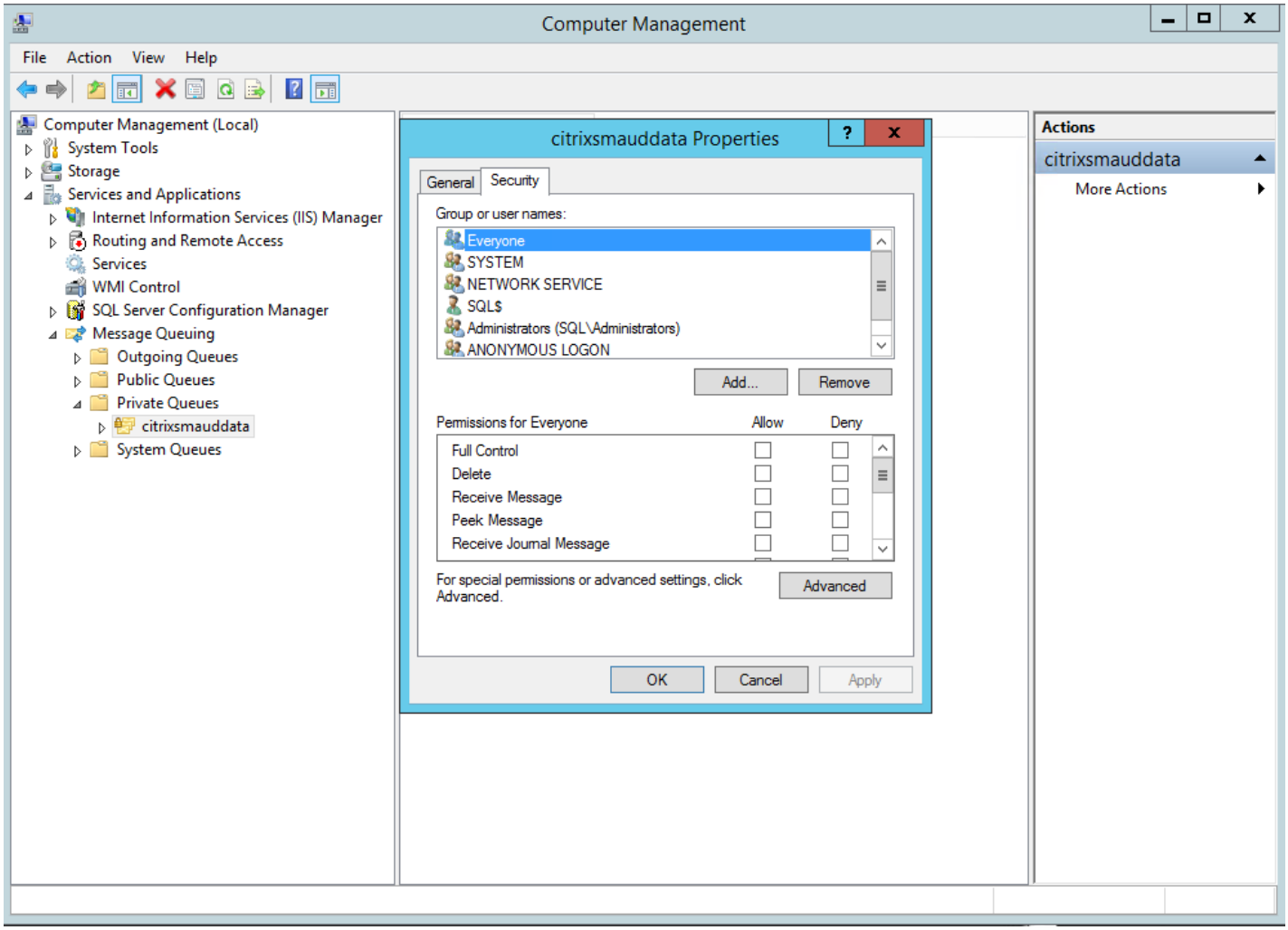
  1) Installez la fonctionnalité serveur Intégration du service d'annuaire sur chaque serveur d'enregistrement de session et la machine VDA ou VDI sur laquelle l'enregistrement de session est activé, puis redémarrez le service Message Queuing.

  2) Dans le menu **Démarrer** de Windows sur chaque serveur d'enregistrement de session, ouvrez la fenêtre **Outils d'administration > Gestion de l'ordinateur**.

  3) Ouvrez **Services et applications > Message Queuing > Files d'attente privées**.

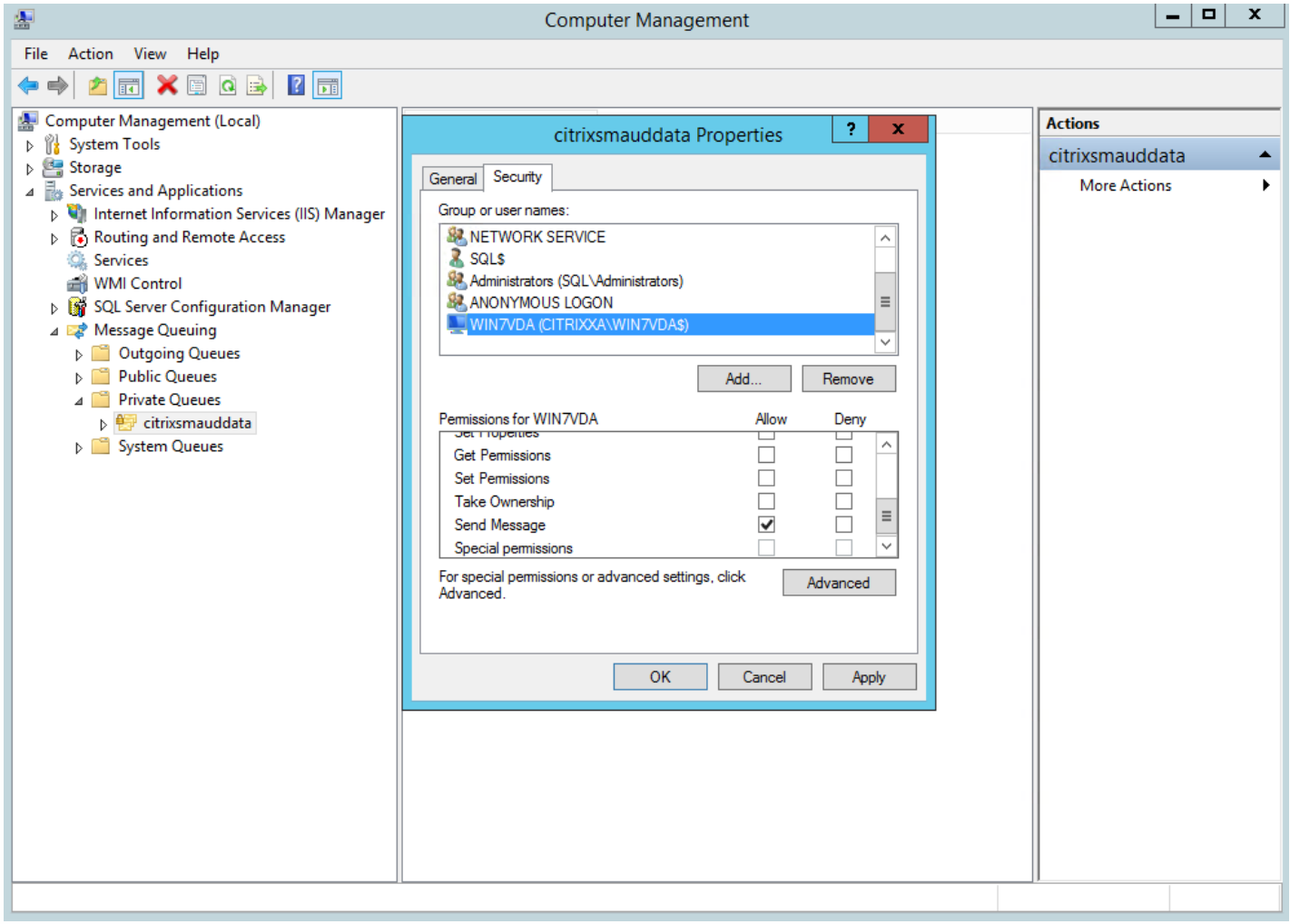
  4) Cliquez sur la file d'attente privée**citrixsmauddata** pour ouvrir la page **Propriétés** et sélectionnez l'onglet **Sécurité**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5) Ajoutez les groupes d'ordinateurs ou les groupes de sécurité des machines VDA qui enverront des données MSMQ à ce serveur et accordez-leur l'autorisation Envoyer un message.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- Protégez correctement le journal d'événements du serveur d'enregistrement de session et des agents d'enregistrement de session. Citrix recommande l'utilisation d'une solution de journalisation à distance Windows ou tierce pour protéger le journal d'événements ou rediriger le journal d'événements vers le serveur distant.
- Veillez à ce que les serveurs exécutant les composants d'enregistrement de session sont physiquement sécurisés. Si possible, verrouillez ces ordinateurs dans une pièce sécurisée dont l'accès direct ne peut être accordé qu'au personnel autorisé.
- Isolez les serveurs exécutant les composants d'enregistrement de session sur un sous-réseau ou domaine séparé.
- Protégez les données de sessions enregistrées des utilisateurs accédant à d'autres serveurs en installant un pare-feu entre le serveur d'enregistrement de session et les autres serveurs.
- Actualisez fréquemment le serveur d'administration de l'enregistrement de sessions et la base de données SQL avec les dernières mises à jour de sécurité de Microsoft.
- Interdisez les non-administrateurs de se connecter à la machine d'administration.
- Limitez strictement les personnels autorisés à modifier les stratégies d'enregistrement et à afficher les sessions enregistrées.
- Installez des certificats numériques, utilisez la fonctionnalité de signature de fichiers d'enregistrement de session et paramétrez les communications TLS dans IIS.
- Configurez MSMQ pour utiliser HTTPS en tant que transport en définissant le protocole MSMQ figurant dans la boîte de dialogue Propriétés de l'agent d'enregistrement de session sur HTTPS. Pour obtenir davantage d'informations, veuillez consulter la section Résolution des problèmes de MSMQ.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Utilisez TLS 1.0 et désactivez SSLv2, SSLv3 et le cryptage RC4 sur le serveur d'enregistrement de session et la base de données d'enregistrement de session. Pour plus d'informations, veuillez consulter les articles Microsoft http://support.microsoft.com/default.aspx?scid=kb;en-us;187498 et http://support.microsoft.com/kb/245030/en-us.
- Utilisez la fonction Protection de lecture. La fonction Protection de lecture est une fonction de l'enregistrement de session qui crypte des fichiers enregistrés avant de les télécharger sur le lecteur d'enregistrement de session. Par défaut, cette option est activée et se trouve dans les propriétés du serveur d'enregistrement de session.
- Ne déployez pas l'enregistrement de session sur un cloud public tel que Amazon Web Services (AWS).
- Suivez les recommandations du NSIT pour la longueur des clés cryptographiques et les algorithmes cryptographiques.

Pour de plus amples informations sur la configuration des fonctionnalités d'enregistrement de session, consultez l'article http://support.citrix.com/article/CTX200868.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Considérations sur la capacité à monter en charge

Jul 07, 2016

L'installation et l'exécution de l'enregistrement de session nécessitent quelques ressources supplémentaires au-delà des éléments de base nécessaires à l'exécution de XenApp. Toutefois, si vous prévoyez d'utiliser l'enregistrement de session pour enregistrer un grand nombre de sessions ou si les sessions que vous prévoyez d'enregistrer produiront des fichiers volumineux (par exemple, des applications au graphisme intensif), tenez compte des performances de votre système dans la planification de votre déploiement d'enregistrement de session.

Pour de plus amples informations sur la création d'un système d'enregistrement de session hautement évolutif, consultez la section http://support.citrix.com/article/CTX200869.

Dans cet article :

Recommandations matérielles

Disque et matériel de stockage

Capacité du réseau

Capacité de traitement de l'ordinateur

Déployer plusieurs serveurs d'enregistrement de session

Capacité à monter en charge de la base de données

Recommandations matérielles

Considérez le volume de données que vous enverrez à chaque serveur d'enregistrement de session et la rapidité des délais de traitement et de stockage de ces données par les serveurs. Le taux auquel votre système peut stocker les données entrantes doit être supérieur au taux d'entrée des données.

Pour estimer votre taux d'entrée des données, multipliez le nombre de sessions enregistrées par la taille moyenne de chaque session enregistrée, puis divisez par la durée d'enregistrement des sessions. Par exemple, vous pouvez enregistrer 5 000 sessions Microsoft Outlook de 20 Mo chacune sur une durée de 8 heures par jour ouvrable. Dans ce cas, le taux d'entrée des données sera d'environ 3,5 Mo/s. (soit 5 000 sessions X 20 Mo divisés par 8 heures, divisés par 3 600 secondes/heure.)

Vous pouvez améliorer les performances globales en optimisant celles d'un seul serveur d'enregistrement de session ou en installant plusieurs serveurs d'enregistrement de session sur des ordinateurs différents.

Disque et matériel de stockage

Le disque et le matériel de stockage sont les facteurs les plus importants à considérer dans la planification d'un déploiement d'enregistrement de session. Les performances d'écriture de votre solution de stockage est d'une importance particulière. Plus vite les données peuvent être écrites sur disques, plus élevées sont les performances du système dans son ensemble.

Les solutions de stockage convenant à une utilisation avec l'enregistrement de session comprennent une série de disques locaux contrôlés en tant que contrôleurs RAID par un contrôleur de disque local ou par un réseau dédié au stockage (SAN) connecté.

Remarque : l'enregistrement de session ne doit pas être utilisé avec un serveur NAS (Network-Attached Storage), en raison

© 1999-2017 Citrix Systems, Inc. All rights reserved.

des problèmes de performances et de sécurité liés à l'écriture les données d'enregistrement sur un lecteur réseau.
Pour une configuration de lecteur local, un contrôleur de disque avec mémoire cache intégré améliore les performances. Un contrôleur de disque de mise en cache doit posséder un dispositif de batterie de secours afin d'assurer le maintien de l'intégrité des données en cas de coupure de courant.

Capacité du réseau

Une liaison réseau de 100 Mbps convient aux connexions à un serveur d'enregistrement de session. Une connexion Ethernet en giga-octets peut améliorer les performances, mais ne se traduira pas par des performances de dix fois supérieures à une liaison 100 Mbps.

Veillez à ce que les commutateurs réseau utilisés par l'enregistrement de session ne soient pas partagés avec des applications tierces qui pourraient lui disputer la bande passante réseau disponible. Dans le meilleur des cas, les commutateurs réseau sont dédiés au serveur d'enregistrement de session.

Capacité de traitement de l'ordinateur

Tenez compte des spécifications suivantes pour l'ordinateur sur lequel un serveur d'enregistrement de session est installé :

- UC double ou UC dual-core recommandée.
- 2 Go à 4 Go de RAM recommandés.

Le dépassement de ces spécifications ne produit pas de gains significatifs en performance.

Déployer plusieurs serveurs d'enregistrement de session

Si un seul serveur d'enregistrement de session ne correspond pas à vos besoins en matière de performances, vous pouvez en installer plusieurs, sur des ordinateurs différents. Pour ce type de déploiement, chaque serveur d'enregistrement de session dispose de son propre stockage, de ses propres commutateurs réseau et de sa propre base de données. Pour répartir la charge, pointez les agents d'enregistrement de session de votre déploiement vers différents serveurs d'enregistrement de session.

Capacité à monter en charge de la base de données

La base de données d'enregistrement de session nécessite Microsoft SQL Server 2014, Microsoft SQL Server 2012, ou Microsoft SQL Server 2008 R2. Le volume de données envoyées à la base de données est minime car celle-ci ne stocke que les métadonnées sur les sessions enregistrées. Pour leur part, les fichiers des sessions enregistrées sont inscrits sur un autre disque. Généralement, chaque session enregistrée ne nécessite qu'environ 1 Ko d'espace dans la base de données, à moins que l'API d'événements de l'enregistrement de session soit utilisé pour insérer des événements avec possibilité de recherche dans la session.

Les éditions Express de Microsoft SQL Server 2014, Microsoft SQL Server 2012 et Microsoft SQL Server 2008 R2 imposent une limite de taille de base de données de 10 Go. À 1 Ko par session d'enregistrement, la base de données peut cataloguer environ quatre millions de sessions. D'autres éditions de Microsoft SQL Server n'ont pas de restrictions de taille de base de données et ne sont limitées que par la quantité d'espace disque disponible. À mesure que le nombre de sessions augmente dans la base de données, les performances de la base de données et la vitesse des recherches ne diminuent que faiblement.

Si vous ne faites pas de personnalisations par le biais de l'API d'événements de l'enregistrement de session, chaque session enregistrée génère quatre transactions sur la base de données : deux au démarrage de l'enregistrement, une lorsque l'utilisateur se connecte aux sessions actuellement enregistrées et une à l'arrêt de l'enregistrement. Si vous avez utilisé l'API d'événements de l'enregistrement de session pour personnaliser des sessions, chaque événement avec possibilité de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

recherche enregistré génère une transaction. Puisque même le déploiement de base de données le plus élémentaire est en mesure de traiter des centaines de transactions par seconde, la charge de traitement sur la base de données n'est pas considérée comme étant excessivement sollicitée. L'impact est assez minime pour que la base de données d'enregistrement de session puisse s'exécuter sur le même serveur SQL que d'autres bases de données, notamment la base de données du magasin central de XenApp ou XenDesktop.

Si votre déploiement d'enregistrement de session nécessite de cataloguer plusieurs millions de sessions enregistrées dans la base de données, suivez les consignes de Microsoft pour la montée en charge de SQL Server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Installer l'enregistrement de session

Jul 07, 2016

Cet article contient ces sections :

Check-list d'installation

Utiliser un script pour ajouter les fonctionnalités et les rôles Windows requis

Installer les composants de l'administration de l'enregistrement de session

Installer la base de données d'enregistrement de session

Installer le serveur d'enregistrement de session

Configurer Director pour utiliser le serveur d'enregistrement de session

Installer l'agent d'enregistrement de session

Installer le lecteur d'enregistrement de session

Automatisation des installations

Mettre à niveau l'enregistrement de session

Désinstaller l'enregistrement de session

Check-list d'installation

Avant de commencer l'installation, effectuez les tâches de cette liste :

✓	**Étape**
	Installez les composants requis avant de commencer l'installation. Consultez les sections Configuration requise et Utiliser un script pour ajouter les fonctionnalités et les rôles Windows requis.
	Sélectionnez les ordinateurs sur lesquels installer chaque composant d'enregistrement de session et veillez à ce que chaque ordinateur soit conforme aux configurations matérielles et logicielles requises correspondant au(x) composant(s) à y installer.
	Téléchargez l'enregistrement de session à partir de la page de téléchargement de Citrix sous XenApp > https://www.citrix.com/downloads/xenapp.html ou XenDesktop > https://www.citrix.com/downloads/xendesktop.html
	Si vous utilisez le protocole SSL pour les communications entre les composants de l'enregistrement de session, installez les certificats corrects dans votre environnement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Installez toute correction requise pour les composants de l'enregistrement de session. Les corrections sont disponibles auprès du support de Citrix.
	Configurez Director pour créer et activer des stratégies d'enregistrement de session. Pour de plus amples informations, consultez Configurer Director pour utiliser le serveur d'enregistrement de session.

Remarques :

- Citrix recommande de séparer les applications publiées dans des groupes de mise à disposition distincts en fonction des stratégies d'enregistrement car le partage de session pour les applications publiées peut entrer en conflit avec des stratégies actives si elles se trouvent dans le même groupe de mise à disposition. L'enregistrement de session fait correspondre la stratégie active à la première application publiée qu'un utilisateur ouvre.
- Si vous prévoyez d'utiliser Machine Creation Services (MCS) ou Provisioning Services avec XenApp, préparez le serveur avec une QMId unique ; consultez la description dans les problèmes connus. Si vous n'effectuez pas cette étape, vous risquez de perdre des données d'enregistrement.
- Le serveur SQL Server requiert que TCP/IP soit activé, que le service SQL Server Browser soit exécuté et que l'authentification Windows soit utilisée.
- Si vous souhaitez utiliser HTTPS, configurez des certificats de serveur pour TLS/HTTPS.

Fichiers d'installation de l'enregistrement de session :

- **Fichiers d'administration de l'enregistrement de session**
  - Broker_PowerShellSnapIn_x64.msi
  - SessionRecordingAdministrationx64.msi
- **Fichiers de l'agent d'enregistrement de session**
  - SessionRecordingAgentx64.msi
- **Fichiers du lecteur d'enregistrement de session**
  - SessionRecordingPlayer.msi

Utiliser un script pour ajouter les fonctionnalités et les rôles Windows requis

Pour que l'enregistrement de session fonctionne correctement, vous devez ajouter des fonctionnalités et des rôles Windows requis avant d'installer les composants d'enregistrement de session. Il peut être difficile de rechercher et d'installer certains de ces rôles et fonctionnalités ; c'est pourquoi cet article contient une procédure utilisant un script fourni par Citrix. Exécutez le script pour installer les fonctionnalités et les rôles Windows requis avant l'installation des composants d'enregistrement de session.

Pour installer les fonctionnalités et les rôles Windows requis

1. Si vous souhaitez utiliser les scripts Citrix, consultez la section Scripts pour les fonctionnalités et les rôles Windows requis.

2. Effectuez les opérations suivantes sur la machine sur laquelle vous allez installer les composants de l'administration d'enregistrement de session :

   A) Vérifiez que la stratégie d'exécution est définie sur **RemoteSigned** ou **Unrestricted** dans PowerShell.

   Set-ExecutionPolicy RemoteSigned

   B) Démarrez une invite de commande en tant qu'administrateur et exécutez cette commande :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

powershell.exe -file InstallPrereqsforSessionRecordingAdministration.ps1

Le script affiche les fonctionnalités qui ont été ajoutées avec succès et s'arrête.

C) Une fois que les scripts se sont exécutés, assurez-vous que la stratégie d'exécution est définie sur une valeur correcte en fonction de la stratégie de l'entreprise.

3. Effectuez les opérations suivantes sur la machine sur laquelle vous allez installer le composant de l'agent d'enregistrement de session :

A) Vérifiez que la stratégie d'exécution est définie sur **RemoteSigned** ou **Unrestricted** dans PowerShell.

Set-ExecutionPolicy RemoteSigned

B) Démarrez une invite de commande en tant qu'administrateur et exécutez cette commande :

powershell.exe -file InstallPrereqsforSessionRecordingAgent.ps1

Le script affiche les fonctionnalités qui ont été ajoutées avec succès et s'arrête.

C) Une fois que les scripts se sont exécutés, assurez-vous que la stratégie d'exécution est définie sur une valeur correcte en fonction de la stratégie de l'entreprise.

4. Une fois que les rôles et fonctionnalités de Windows sont installés, continuez l'installation de l'enregistrement de session.

Installer les composants de l'administration de l'enregistrement de session

Les composants de l'administration de l'enregistrement de session sont les suivants : base de données d'enregistrement de session, serveur d'enregistrement de session et console de stratégie d'enregistrement de session. Vous pouvez choisir lequel de ces composants installer sur un serveur.

Avant d'installer les composants de l'administration de l'enregistrement de session, assurez-vous que tous les composants requis sont installés. Consultez la section Configuration système requise pour l'enregistrement de session.

Pour améliorer la sécurité, vous pouvez supprimer ces droits après l'installation de la base de données.

1. Exécutez **Broker_PowerShellSnapIn_x64.msi** puis suivez les invites pour terminer l'installation.
2. Démarrez l'invite de commande de Windows en tant qu'administrateur, puis exécutez la commande **msiexec /i SessionRecordingAdministrationx64.msi** ou cliquez deux fois sur le fichier .msi.
3. Sur l'interface utilisateur d'installation, sélectionnez **Suivant** et acceptez le contrat de licence.
4. Sur l'écran d'installation de l'administration de l'enregistrement de session, sélectionnez les composants d'administration de l'enregistrement de session que vous voulez installer.

Installer la base de données d'enregistrement de session

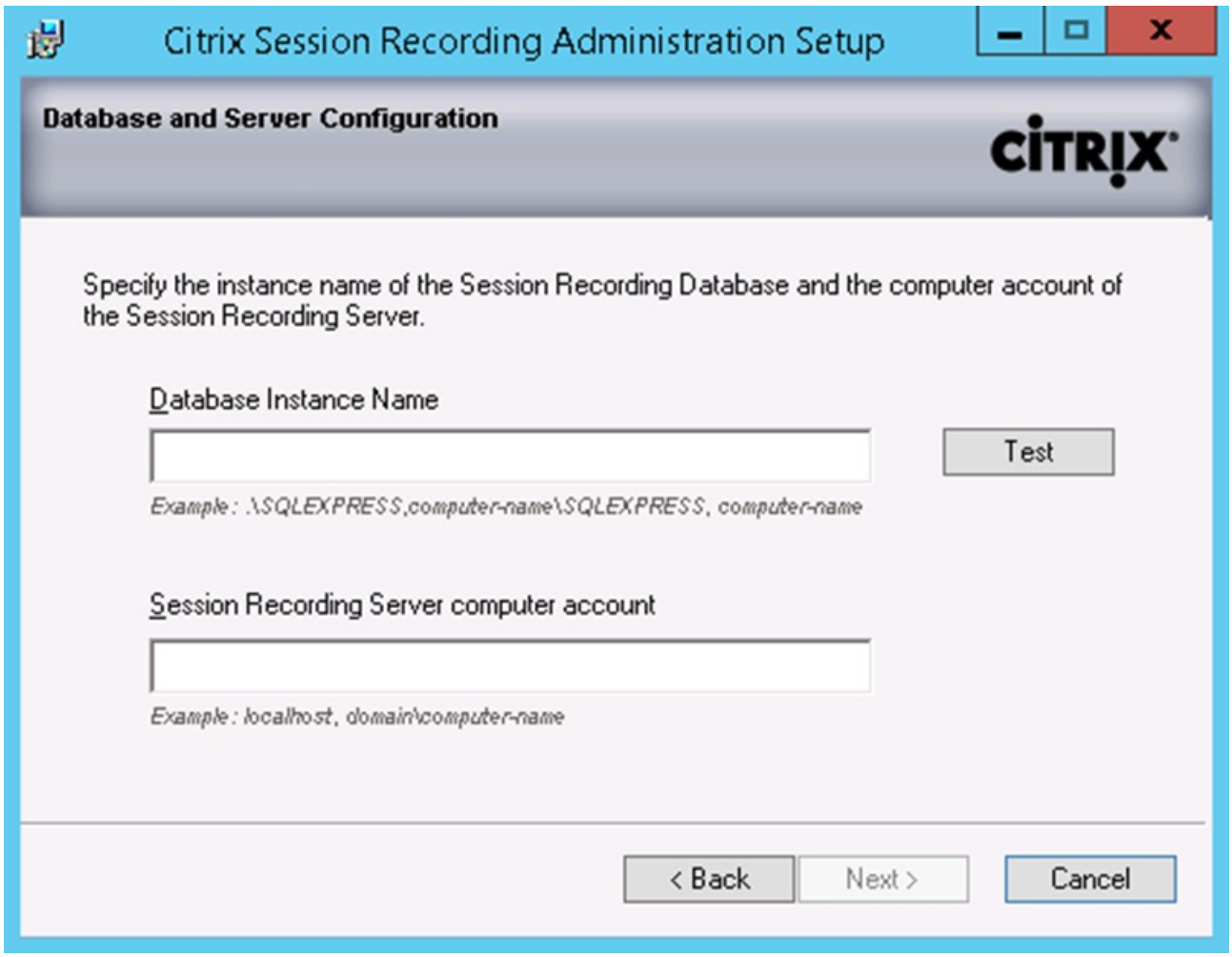
Avant d'installer la base de données d''enregistrement de session, assurez-vous que tous les composants requis sont installés. Consultez la section Configuration système requise pour l'enregistrement de session.

Il existe généralement ces trois types de déploiement composant Base de données d'enregistrement de session et Microsoft SQL Server :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Déploiement 1 : Installer le serveur d'enregistrement de session et la base de données d'enregistrement de session sur le même serveur et la base de données Microsoft SQL Server sur une machine distante (**Recommandé**)
- Déploiement 2 : Installer le serveur d'enregistrement de session, la base de données d'enregistrement de session et la base de données Microsoft SQL Server sur la même machine.
- Déploiement 3 : Installer le serveur d'enregistrement de session sur un serveur et installer la base de données d'enregistrement de session et Microsoft SQL Server sur la même machine, autre que la machine du serveur d'enregistrement de session (**Non recommandé**).

1. Sur la page Configuration de la base de données :
   - **Déploiements 1 et 2** : entrez la valeur **localhost** dans le champ du compte d'ordinateur du serveur d'enregistrement de session.
   - **Déploiement 3 :** entrez le nom de l'ordinateur hébergeant le serveur d'enregistrement de session dans le format suivant : *domaine**nom-ordinateur*. Le compte d'ordinateur du serveur d'enregistrement de session est le compte utilisateur utilisé pour accéder à la base de données.



Si l'instance de base de données n'est pas une instance nommée comme configuré lors de la configuration de l'instance, vous pouvez uniquement utiliser le nom de l'ordinateur du serveur SQL Server. Si vous avez nommé l'instance, utilisez *nom-ordinateur**nom-instance* comme nom d'instance de la base de données. Pour déterminer le nom de l'instance du serveur que vous utilisez, exécutez **select @@servername** sur SQL Server et la valeur renvoyée est le nom exact de l'instance de base de données.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cliquez sur **Tester** pour tester la connexion au serveur SQL. Assurez-vous que l'utilisateur actuel dispose de l'autorisation de rôle SQL Server public ; sinon, le test échoue pour cause d'autorisation insuffisante. Ensuite, cliquez sur **Suivant** pour continuer l'installation.

2. Suivez les instructions pour terminer l'installation. Durant l'installation, si l'utilisateur actuel n'est pas l'administrateur de la base de données, une boîte de dialogue s'affiche, demandant les informations d'identification d'un administrateur de base de données avec l'autorisation de rôle de serveur **sysadmin**. Entrez les informations d'identification correctes et cliquez sur **OK** pour continuer l'installation. L'installation crée la nouvelle base de données d'enregistrement de session et ajoute le compte de machine du serveur d'enregistrement de session en tant que **db-owner**.

Une fois l'installation terminée, l'autorisation de rôle de serveur sysadmin n'est plus nécessaire et peut être supprimée pour l'utilisateur actuel.

> ## Important
>
> Vous ne pouvez pas modifier le nom de la base de données **CitrixSessionRecording**.

Installer le serveur d'enregistrement de session

Avant d'installer le serveur d'enregistrement de session, assurez-vous que tous les composants requis sont installés. Consultez la section Configuration système requise pour l'enregistrement de session.

1. Entrez le nom de votre serveur SQL dans la case Nom de l'instance de base de données. Si vous utilisez une instance nommée, entrez *nom-ordinateur**nom-instance* ; sinon, entrez un nom-ordinateur uniquement.
2. Cliquez sur **Tester** pour tester la connexion au serveur SQL. Assurez-vous que l'utilisateur actuel dispose de l'autorisation de rôle SQL Server public ; sinon, le test échoue pour cause d'autorisation insuffisante. Ensuite, cliquez sur **Suivant** pour continuer l'installation et suivez les instructions pour terminer l'installation.
3. À la fin de l'assistant d'installation, vous pouvez indiquer si vous voulez participer au Programme d'amélioration de l'expérience utilisateur Citrix. Lorsque vous rejoignez ce programme, des statistiques anonymes et des informations d'utilisation sont envoyées à Citrix ; veuillez consulter la section À propos du Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) pour plus d'informations.

Configurer Director pour utiliser le serveur d'enregistrement de session

Vous pouvez utiliser la console Director pour créer et activer des stratégies d'enregistrement de session.

1. Dans le cas d'une connexion https, installez le certificat destiné à approuver le serveur d'enregistrement de session dans les certificats racines de confiance du serveur Director.
2. Pour configurer le serveur Director pour utiliser le serveur d'enregistrement de session, exécutez la commande : **C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording**
3. Entrez l'adresse IP/le nom de domaine complet du serveur d'enregistrement de session, le numéro de port et le type de connexion (http/https) depuis l'agent d'enregistrement de session vers le broker d'enregistrement de session sur le serveur Director.

Installer l'agent d'enregistrement de session

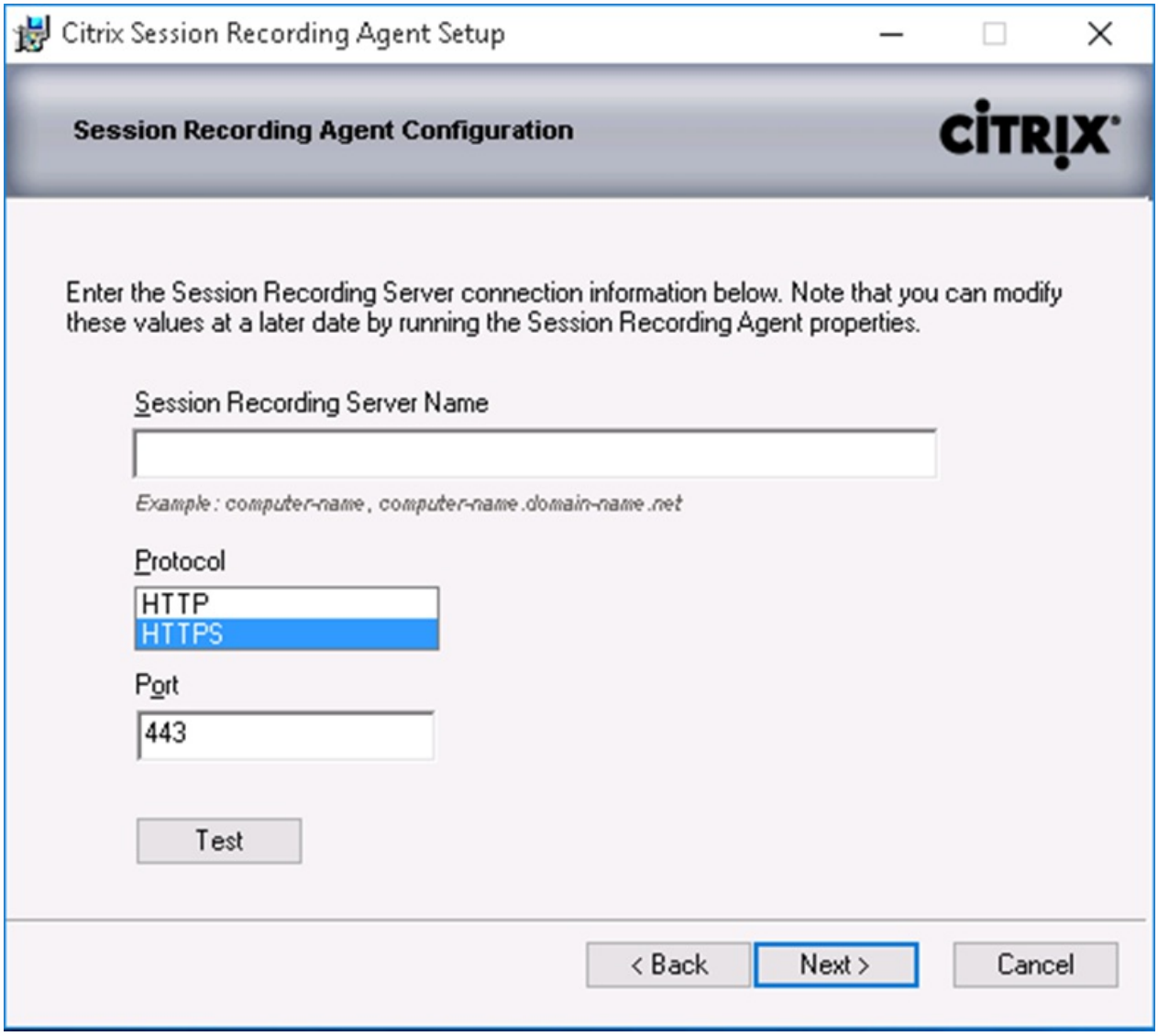
L'agent d'enregistrement de session doit être installé sur la machine VDA ou VDI sur laquelle vous voulez enregistrer les sessions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Utilisez le Gestionnaire de serveur pour installer .NET Framework 3.5 et Microsoft Message Queuing (MSMQ) avec prise en charge HTTP sur le VDA avec OS de serveur XenApp 7.8 ou le VDI XenDesktop 7.8.
2. Démarrez l'invite de commande de Windows en tant qu'administrateur, puis exécutez la commande :
   msiexec /i SessionRecordingAgentx64.msi
   ou
   msiexec /i SessionRecordingAgent.msi

   ou double-cliquez sur le fichier .msi.

   Utilisez le fichier .msi en fonction du type de plate-forme : **SessionRecordingAgent.msi** pour les systèmes 32 bits et **SessionRecordingAgentx64.msi** pour les systèmes 64 bits.
3. Sur l'interface utilisateur d'installation, sélectionnez **Suivant** et acceptez le contrat de licence.
4. Dans la page Configuration de l'agent d'enregistrement de session, entrez le nom de l'ordinateur sur lequel vous avez installé le serveur d'enregistrement de session ainsi que les informations de protocole et de port requises pour la connexion au serveur d'enregistrement de session.



L'installation de l'enregistrement de session utilise par défaut HTTPS/TLS pour sécuriser les communications. Si TLS n'est pas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

configuré, utilisez HTTP. Pour ce faire, désélectionnez SSL dans la console de gestion IIS en accédant au site du broker d'enregistrement de session. Ouvrez les paramètres SSL et décochez la case Exiger SSL.

5. Suivez les instructions pour terminer l'installation.

Installer le lecteur d'enregistrement de session

Installez le lecteur d'enregistrement de session sur le serveur d'enregistrement de session ou sur l'un ou plusieurs des postes de travail du domaine pour les utilisateurs qui visionnent les enregistrements de session.

Exécutez **SessionRecordingPlayer.msi** puis suivez les invites pour terminer l'installation.

Automatisation des installations

Pour installer l'agent d'enregistrement de session sur plusieurs serveurs, créez un script utilisant l'installation silencieuse.

La ligne de commande suivante installe l'agent d'enregistrement de session et crée un fichier journal pour capturer les informations d'installation.

Pour les systèmes 64 bits :

```
msiexec /i SessionRecordingAgentx64.msi
sessionrecordingservername=yourservername sessionrecordingbrokerprotoco=yourbrokerprotocol
 sessionrecordingbrokerport=yourbrokerport /l*v yourinstallationlog /q
```

Pour les systèmes 32 bits :

```
msiexec /i  SessionRecordingAgent.msi sessionrecordingservername=yourservername
sessionrecordingbrokerprotoco=yourbrokerprotocol sessionrecordingbrokerport=yourbrokerport /l*v yourinstallationlog /q
```

où :

nom_de_votre_serveur correspond au nom NetBIOS ou au nom de domaine complet de l'ordinateur hébergeant le serveur d'enregistrement de session. Si elle n'est pas précisée, cette valeur prend par défaut la valeur « localhost ».

protocole_de_votre_broker est soit HTTP, soit HTTPS, et représente le protocole que l'agent d'enregistrement de session utilise pour communiquer avec le broker d'enregistrement de session ; par défaut HTTPS est utilisé si le protocole n'est pas précisé.

port_de_votre_broker est un nombre entier représentant le port que l'agent d'enregistrement de session utilise pour communiquer avec le broker d'enregistrement de session. Si elle n'est pas précisée, la valeur par défaut de cette valeur est zéro, qui amène l'agent d'enregistrement de session à utiliser le numéro de port par défaut pour le protocole sélectionné : 80 pour HTTP ou 443 pour HTTPS.

/l*v spécifie l'enregistrement en mode détaillé.

votre_journal_installation indique l'emplacement du fichier journal de l'installation créé.

/q spécifie le mode silencieux.

Mettre à niveau l'enregistrement de session

Vous pouvez mettre à niveau certains déploiements vers des versions plus récentes sans devoir d'abord configurer les nouvelles machines ou sites. Vous pouvez mettre à niveau à partir de l'enregistrement de session 7.6.0 (ou version ultérieure)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

vers la dernière version (courante) de l'enregistrement de session.

Configuration requise, préparation et limites

Remarque : vous ne pouvez pas mettre à niveau à partir d'une version Technology Preview.

- Vous devez utiliser l'interface graphique ou l'interface de ligne de commande du programme d'installation de l'enregistrement de session pour mettre à niveau les composants d'enregistrement de session sur la machine sur laquelle vous avez installé les composants d'enregistrement de session correspondants.
- Avant de procéder à toute activité de mise à niveau, sauvegardez la base de données nommée CitrixSessionRecording dans l'instance de SQL Server, afin de pouvoir la restaurer en cas de problème après la mise à niveau de la base de données.
- En plus d'être un utilisateur du domaine, vous devez être un administrateur local sur les machines sur lesquelles vous mettez à niveau les composants d'enregistrement de session.
- Si le serveur d'enregistrement de session et la base de données d'enregistrement de session ne sont pas installés sur le même serveur, vous devez disposer de l'autorisation de rôle sysadmin de base de données pour mettre à niveau la base de données d'enregistrement de session ; sinon, vous êtes invité à entrer les informations d'identification du rôle sysadmin lors de la mise à niveau.
- Si vous n'envisagez pas de mettre à niveau tous les agents d'enregistrement de session en même temps, l'agent d'enregistrement de session 7.6.0 (ou une version ultérieure) peut fonctionner avec la dernière version (courante) du serveur d'enregistrement de session. Cependant, certaines nouvelles fonctionnalités et des corrections de bogues risquent de ne pas être appliquées.
- Les sessions lancées durant la mise à niveau du serveur d'enregistrement de session ne sont pas enregistrées.
- S'il existe des sessions d'enregistrement actives lorsque le processus de mise à niveau démarre, l'enregistrement risque de ne pas se terminer.
- Vérifiez la séquence de mise à niveau ci-dessous afin de pouvoir planifier et réduire tout problème potentiel.

Séquence de mise à niveau

1. Si la base de données d'enregistrement de session et le serveur d'enregistrement de session sont installés sur des serveurs différents, arrêtez le service Gestionnaire de stockage d'enregistrement de session manuellement sur le serveur d'enregistrement de session, puis mettez à niveau la base de données d'enregistrement de session.
2. Assurez-vous que le broker d'enregistrement de session est exécuté avec le service IIS. Mettez à niveau le serveur d'enregistrement de session. Si la base de données d'enregistrement de session et le serveur d'enregistrement de session sont installés sur le même serveur, la base de données d'enregistrement de session doit également être mise à niveau.
3. Le service d'enregistrement de session est automatiquement reconnecté lorsque la mise à niveau du serveur d'enregistrement de session est terminée.
4. Mettez à niveau l'agent d'enregistrement de session (sur l'image principale).
5. Mettez à niveau la console de stratégie d'enregistrement de session avec ou après le serveur d'enregistrement de session.
6. Mettez à niveau le lecteur d'enregistrement de session.

Désinstaller l'enregistrement de session

Pour supprimer tous les composants d'enregistrement de session d'un serveur ou d'une station de travail, utilisez la capacité de désinstallation ou de suppression des programmes disponible au travers du Panneau de configuration Windows. Pour supprimer la base de données d'enregistrement de session, vous devez avoir les mêmes droits d'administrateur système SQL Server sysadmin que lorsque vous l'avez installée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Scripts permettant d'ajouter les fonctionnalités et les rôles Windows requis

Jul 07, 2016

Vous pouvez utiliser les scripts suivants pour installer les rôles et fonctionnalités Windows requis pour que l'enregistrement de session fonctionne correctement. Pour de plus amples informations, consultez la section Utiliser un script pour ajouter les fonctionnalités et les rôles Windows requis.

Installer les composants requis pour l'administration de l'enregistrement de session COPIER

```
<#
.Synopsis
    Installs Prereqs for Session Recording Administration
.Description
    Supports Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2.
    Install below windows feature on this machine:
    -Application Development - ASP.NET 4.5 on Server 2012 and Server 2012 R2, Application Development - ASP.NET on Server 2008 R2
    -Security - Windows Authentication
    -Management Tools - IIS 6 Management Compatibility
        IIS 6 Metabase Compatibility
        IIS 6 WMI Compatibility
        IIS 6 Scripting Tools
        IIS 6 Management Console
 -Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled.
#>
function AddFeatures($featurename)
{
    try
    {
        $feature=Get-WindowsFeature | ? {$_.DisplayName -eq $featurename -or $_.Name -eq $featurename}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        Add-WindowsFeature $feature
    }
    catch
    {
        Write-Host "Addition of Windows feature $featurename failed"
        Exit 1
    }
    Write-Host "Addition of Windows feature $featurename succeeded"
}

$system= gwmi win32_operatingSystem | select name

if (-not (($system -Like '*Microsoft Windows Server 2012*') -or ($system -Like '*Microsoft Windows Server 2008 R2*')))
{
    Write-Host("This is not a supported server platform. Installation aborted.")
    Exit
}

# Start to install Windows feature
Import-Module ServerManager

if ($system -Like '*Microsoft Windows Server 2012*')
{
    AddFeatures('Web-Asp-Net45') #ASP.NET 4.5
}
if($system -like '*Microsoft Windows Server 2008 R2*')
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    AddFeatures('Web-Asp-Net') #ASP.NET
}
AddFeatures('Web-Mgmt-Console') #IIS Management Console
AddFeatures('Web-Windows-Auth') # Windows Authentication
AddFeatures('Web-Metabase') #IIS 6 Metabase Compatibility
AddFeatures('Web-WMI') #IIS 6 WMI Compatibility
AddFeatures('Web-Lgcy-Scripting')#IIS 6 Scripting Tools
AddFeatures('Web-Lgcy-Mgmt-Console') #IIS 6 Management Console
AddFeatures('MSMQ-HTTP-Support') #MSMQ HTTP Support
```

Installer les composants requis pour l'agent d'enregistrement de session

COPIER

```
<#
.Synopsis
    Installs Prereqs for Session Recording Administration
.Description
    Supports Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows 7, Windows 8, Windows 8.1 and Windo
    Install below windows feature on this machine:
 -Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled.
#>
function AddFeatures($featurename)
{
    try
    {
        $feature=Get-WindowsFeature | ? {$_.DisplayName -eq $featurename -or $_.Name -eq $featurename}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        Add-WindowsFeature $feature
    }
    catch
    {
        Write-Host "Addition of Windows feature $featurename failed"
        Exit 1
    }
    Write-Host "Addition of Windows feature $featurename succeeded"
}

# Start to install Windows feature
$system= gwmi win32_operatingSystem | select name

if (-not (($system -Like '*Microsoft Windows Server 2012*') -or ($system -Like '*Microsoft Windows Server 2008 R2*')-or ($system -Like '*
{
    Write-Host("This is not a supported platform. Installation aborted.")
    Exit
}

if ($system -Like '*Microsoft Windows Server*')
{
    Import-Module ServerManager
    AddFeatures('MSMQ') #Message Queuing
    AddFeatures('MSMQ-HTTP-Support')#MSMQ HTTP Support
}
else
{
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    try
    {
        if($system -Like '*Microsoft Windows 7*')
        {
            dism /online /enable-feature /featurename:IIS-WebServerRole /featurename:IIS-WebServer /featurename:IIS-IIS6ManagementCo
            dism /online /enable-feature /featurename:MSMQ-Container
            dism /online /enable-feature /featurename:MSMQ-Server
            dism /online /enable-feature /featurename:MSMQ-HTTP
        }
        else
        {
            dism /online /enable-feature /featurename:MSMQ-HTTP /all
        }
    }
    catch
    {
        Write-Host "Addition of Windows feature MSMQ HTTP Support failed"
        Exit 1
    }
    write-Host "Addition of Windows feature MSMQ HTTP Support succeeded"
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurer l'enregistrement de session

Jul 07, 2016

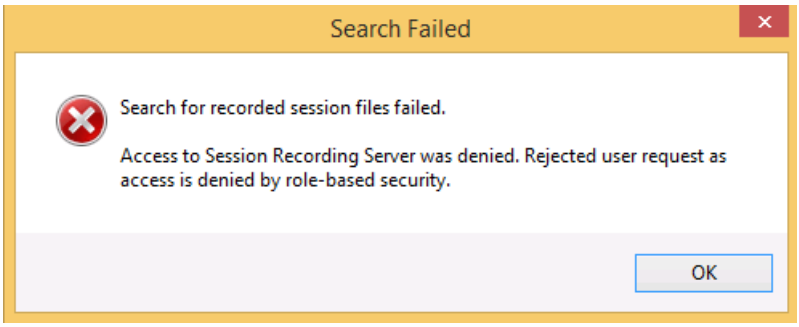
Configurer l'enregistrement de session pour lire et enregistrer des sessions

Après avoir installé les composants d'enregistrement de session, effectuez les étapes suivantes pour configurer l'enregistrement de session pour enregistrer des sessions XenApp ou XenDesktop et pour permettre aux utilisateurs de les visionner :

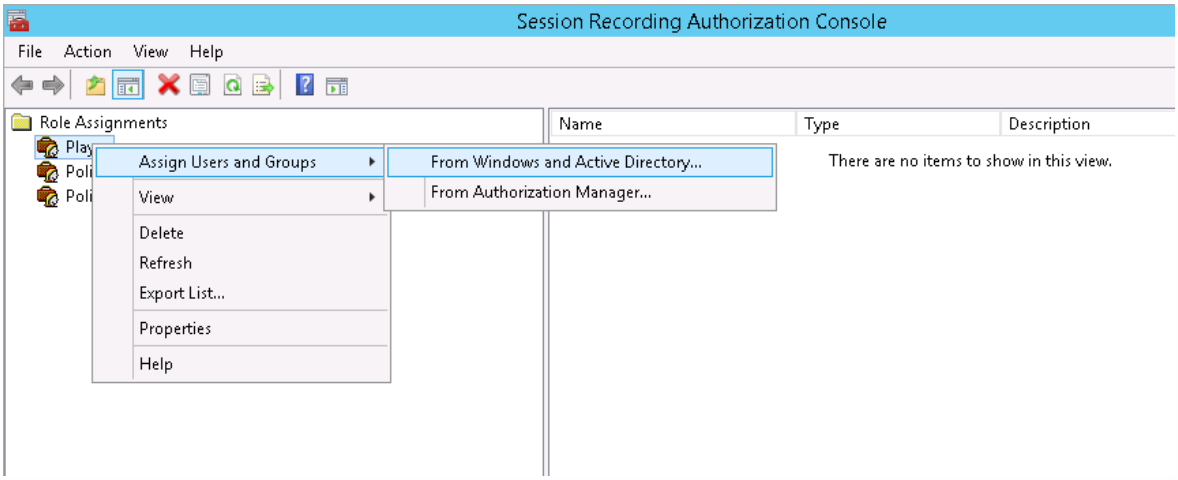
- Autorisez les utilisateurs à lire les enregistrements.
- Autorisez les utilisateurs à gérer les stratégies d'enregistrement.
- Définissez la stratégie d'enregistrement active sur une stratégie enregistrant les sessions.
- Configurer des stratégies personnalisées
- Configurez le lecteur d'enregistrement de session pour la connexion au serveur d'enregistrement de session.

Autorisez les utilisateurs à lire les sessions enregistrées.

Lorsque vous installez l'enregistrement de session, aucun utilisateur n'est autorisé à lire les sessions enregistrées. Vous devez attribuer cette autorisation à chaque utilisateur, y compris l'administrateur. Un utilisateur qui n'est pas autorisé à lire des sessions enregistrées reçoit le message d'erreur suivant lorsqu'il essaye de lire une session enregistrée :



1. Ouvrez une session en tant qu'administrateur sur l'ordinateur hébergeant le serveur d'enregistrement de session.
2. Démarrez la console d'autorisation d'enregistrement de session.
3. Dans la console d'autorisation d'enregistrement de session, sélectionnez Lecteur.
4. Ajoutez les utilisateurs et les groupes que vous voulez autoriser à afficher les sessions enregistrées et ils seront ajoutés au panneau de droite.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Autorisez les utilisateurs à gérer les stratégies d'enregistrement.

Lorsque vous installez l'enregistrement de session, les administrateurs de domaine accordent par défaut l'autorisation de contrôler les stratégies d'enregistrement. Vous pouvez modifier le paramètre d'autorisation.

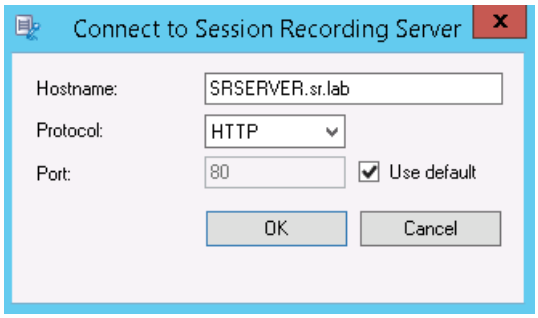
1. Ouvrez une session en tant qu'administrateur sur l'ordinateur hébergeant le serveur d'enregistrement de session.
2. Démarrez la console d'autorisation d'enregistrement de session et sélectionnez PolicyAdministrators.
3. Ajoutez les utilisateurs et les groupes qui peuvent gérer les stratégies d'enregistrement.

Paramétrez la stratégie d'enregistrement active de manière à enregistrer les sessions.

La stratégie d'enregistrement active précise les modalités d'enregistrement des sessions sur tous les VDA ou VDI sur lesquels l'agent d'enregistrement de session est installé et connecté au serveur d'enregistrement de session. Lorsque vous installez l'enregistrement de session, la stratégie d'enregistrement active est **Ne pas enregistrer**. Les sessions ne pourront pas être enregistrées avant que vous ne changiez la stratégie d'enregistrement active.

Important : une stratégie peut contenir de multiples règles, mais une seule stratégie active peut être exécutée à la fois.

1. Ouvrez une session en tant qu'administrateur de stratégie autorisé sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session.
3. Si vous observez une fenêtre indépendante Connexion au serveur d'enregistrement de session, veillez à ce que le nom de l'ordinateur hébergeant le serveur d'enregistrement de session, le protocole et le port sont corrects.



4. Dans la console de stratégie d'enregistrement de session, développez Stratégies d'enregistrement. Ceci permet d'afficher les stratégies d'enregistrement disponibles lorsque vous installez l'enregistrement de session, la stratégie active étant cochée :
   - Ne pas enregistrer. Il s'agit de la stratégie par défaut. Si vous ne précisez pas d'autre stratégie, aucune session n'est enregistrée.
   - Enregistrer tout le monde avec notification. Si vous choisissez cette stratégie, toutes les sessions sont enregistrées. Une fenêtre indépendante s'affiche pour notifier les utilisateurs qu'un enregistrement est en cours.
   - Enregistrer tout le monde sans notification. Si vous choisissez cette stratégie, toutes les sessions sont enregistrées. Aucune fenêtre indépendante ne s'affiche pour notifier les utilisateurs qu'un enregistrement est en cours.
5. Sélectionnez la stratégie que vous souhaitez rendre active.
6. Dans la barre de menus, choisissez Action > Activer la stratégie.

Remarque : l'enregistrement de session vous permet de créer votre propre stratégie d'enregistrement. Les stratégies d'enregistrement que vous créez s'affichent dans le dossier Stratégies d'enregistrement de la console de stratégie d'enregistrement de session.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Il est possible que la stratégie d'enregistrement générique ne réponde pas à vos besoins. Vous pouvez configurer des stratégies et des règles basées sur des utilisateurs, des serveurs VDA et VDI, des groupes de mise à disposition et des applications. Pour de plus amples informations sur les stratégies personnalisées, veuillez consulter la section Créer des stratégies d'enregistrement personnalisées.

Configurer le lecteur d'enregistrement de session

Avant qu'un lecteur d'enregistrement de session puisse lire des sessions, vous devez le configurer de manière à ce qu'il puisse se connecter au serveur d'enregistrement de session qui stocke les sessions enregistrées. Chaque lecteur d'enregistrement de session peut être configuré avec la capacité de se connecter à plusieurs serveurs d'enregistrement de session, mais ne peut se connecter qu'à un seul serveur d'enregistrement de session à la fois. Si le lecteur est configuré avec la capacité de se connecter à plusieurs serveurs d'enregistrement de session, les utilisateurs peuvent changer de serveur d'enregistrement de session auquel connecter le lecteur en cochant la case correspondante sous l'onglet **Connexions** dans **Outils > Options**.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Démarrez le lecteur d'enregistrement de session.
3. Dans la barre de menus du lecteur d'enregistrement de session, choisissez Outils > Options.
4. Dans l'onglet Connexions, cliquez sur Ajouter.
5. Dans le champ Nom de l'hôte, entrez le nom ou l'adresse IP (Internet protocol) de l'ordinateur hébergeant le serveur d'enregistrement de session et sélectionnez le protocole. L'enregistrement de session est configuré par défaut pour utiliser HTTPS/SSL afin de sécuriser les communications. Si SSL n'est pas configuré, sélectionnez HTTP.
6. Si vous souhaitez configurer le lecteur d'enregistrement de session avec la capacité de se connecter à plus d'un seul serveur d'enregistrement de session, répétez les étapes 4 et 5 pour chaque serveur d'enregistrement de session.
7. Veillez à cocher la case correspondant au serveur d'enregistrement de session auquel vous souhaitez vous connecter.

Configurer la connexion au serveur d'enregistrement de session

La connexion entre l'agent d'enregistrement de session et le serveur d'enregistrement de session est généralement configurée lorsque l'agent d'enregistrement de session est installé. Pour configurer cette connexion après l'installation de l'agent d'enregistrement de session, utilisez les propriétés de l'agent d'enregistrement de session.

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Propriétés de l'agent d'enregistrement de session**.
3. Cliquez sur l'onglet **Connexions**.
4. Dans le champ **Serveur d'enregistrement de session**, entrez le nom du serveur ou son adresse IP (Internet protocol).
5. Dans la section **File d'attente des messages du gestionnaire de stockage d'enregistrement de session**, sélectionnez le protocole utilisé par le gestionnaire de stockage d'enregistrement de session pour communiquer et modifier le numéro de port par défaut, si nécessaire.
6. Dans le champ **Durée de validité des messages**, acceptez la valeur par défaut de 7200 secondes (deux heures) ou tapez une nouvelle valeur pour indiquer la durée en secondes pendant laquelle chaque message est conservé dans la file d'attente en cas de panne de communication. À l'issue de cette période, le message est supprimé et le fichier n'est lisible que jusqu'au point où la perte des données s'est produite.
7. Dans la section **Broker d'enregistrement de session**, sélectionnez le protocole de communication que le broker d'enregistrement de session utilise pour communiquer et modifier le numéro de port par défaut, si nécessaire.
8. À l'invite, redémarrez le **service de l'agent d'enregistrement de session** pour accepter les modifications.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Attribuer des droits d'accès aux utilisateurs

Jul 07, 2016

Remarque : pour des raisons de sécurité, veillez à accorder uniquement aux utilisateurs les droits nécessaires à l'accomplissement de fonctions précises, comme l'affichage de sessions enregistrées par exemple.

Vous accordez ces privilèges aux utilisateurs de l'enregistrement de session en les attribuant à des rôles, par le biais de la console d'autorisation d'enregistrement de session sur le serveur d'enregistrement de session. Les utilisateurs de l'enregistrement de session ont trois rôles :

- **Lecteur.** Ce rôle donne le droit à l'utilisateur d'afficher des sessions XenApp enregistrées. Ce rôle n'est rattaché à aucune appartenance par défaut.
- **PolicyQuery (Requête de stratégie).** Cette option permet aux serveurs hébergeant l'agent d'enregistrement de session de demander des évaluations de stratégie d'enregistrement. Par défaut, les utilisateurs authentifiés sont membres de ce rôle.
- **PolicyAdministrator (administrateur de stratégie).** Ce rôle donne le droit d'afficher, de créer, de modifier, de supprimer et d'activer les stratégies d'enregistrement. Par défaut, les administrateurs de l'ordinateur hébergeant le serveur d'enregistrement de session sont membres de ce rôle.

L'enregistrement de session prend en charge les utilisateurs et les groupes définis dans Active Directory.

Pour attribuer des rôles aux utilisateurs

1. Ouvrez une session sur l'ordinateur hébergeant le serveur d'enregistrement de session, en tant qu'administrateur ou en tant que membre du rôle d'administrateur de stratégie (Policy Administrator).
2. Démarrez la console d'autorisation d'enregistrement de session.
3. Sélectionnez le rôle que vous souhaitez attribuer aux utilisateurs.
4. Dans la barre de menus, choisissez Action >Assigner des groupes et des utilisateurs Windows.
5. Ajoutez les utilisateurs et les groupes.

Toute modification apportée à la console prend effet au cours de la mise à jour, qui se produit toutes les minutes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Créer et activer des stratégies d'enregistrement

Jul 07, 2016

Utilisez la console de stratégie d'enregistrement de session pour créer et activer les stratégies qui déterminent quelles sessions sont enregistrées.

Vous pouvez activer les stratégies de système disponibles lors de l'installation de l'enregistrement de session ou créer et activer vos propres stratégies personnalisées. Les stratégies de système d'enregistrement de session appliquent une règle unique à tous les utilisateurs, à toutes les applications publiées et à tous les serveurs. Les stratégies personnalisées précisent quels utilisateurs, quelles applications publiées et quels serveurs sont enregistrés.

La stratégie active détermine quelles sessions sont enregistrées. Une seule stratégie peut être active à la fois.

Utiliser des stratégies de système

L'enregistrement de session fournit ces stratégies de système :

- **Ne pas enregistrer**. Si vous choisissez cette stratégie, aucune session n'est enregistrée. Il s'agit de la stratégie par défaut ; si vous ne spécifiez pas d'autre stratégie, aucune session n'est enregistrée.
- **Enregistrer tout le monde avec notification**. Si vous choisissez cette stratégie, toutes les sessions sont enregistrées. Une fenêtre indépendante s'affiche pour notifier les utilisateurs qu'un enregistrement est en cours.
- **Enregistrer tout le monde sans notification**. Si vous choisissez cette stratégie, toutes les sessions sont enregistrées. Aucune fenêtre indépendante ne s'affiche pour notifier les utilisateurs qu'un enregistrement est en cours.

Les stratégies de système ne peuvent être ni modifiées, ni supprimées.

Pour activer une stratégie

1. Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session.
3. Si vous observez une fenêtre indépendante Connexion au serveur d'enregistrement de session, veillez à ce que le nom du serveur d'enregistrement de session, le protocole et le port sont corrects. Cliquez sur OK.
4. Dans la console de stratégie d'enregistrement de session, développez Stratégies d'enregistrement.
5. Sélectionnez la stratégie que vous souhaitez rendre active.
6. Dans la barre de menus, choisissez Action > Activer la stratégie.

Créer des stratégies d'enregistrement personnalisées

Lorsque vous créez votre propre stratégie, vous établissez des règles précisant pour quels utilisateurs, groupes, applications publiées et serveurs les sessions sont enregistrées. Un assistant intégré à la console de stratégie d'enregistrement de session vous aide à créer des règles. Pour obtenir la liste des applications publiées et des serveurs, vous devez disposer des droits de lecture de l'administrateur du site. Configurez ces droits sur le Delivery Controller de ce site.

Pour chaque règle que vous créez, vous spécifiez une action d'enregistrement et un critère de règle. L'action d'enregistrement s'applique aux sessions qui correspondent au critère de règle.

Pour chaque règle, choisissez une action d'enregistrement :

- Ne pas enregistrer. (Choisissez Désactiver l'enregistrement de session dans l'assistant de règle). Cette action d'enregistrement précise que les sessions correspondant aux critères de la règle ne sont pas enregistrées.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Enregistrer avec notification. (Choisissez Activer l'enregistrement de session avec notification dans l'assistant de règle). Cette action d'enregistrement précise que les sessions correspondant aux critères de la règle sont enregistrées. Une fenêtre indépendante s'affiche pour notifier les utilisateurs qu'un enregistrement est en cours.
- Enregistrer sans notification. (Choisissez Activer l'enregistrement de session sans notification dans l'assistant de règle). Cette action d'enregistrement précise que les sessions correspondant aux critères de la règle sont enregistrées. Les utilisateurs ignorent que leurs activités sont enregistrées.

Pour chaque règle, choisissez au moins l'une des règles suivantes pour créer les critères de règle :

- Utilisateurs ou groupes. Vous créez une liste d'utilisateurs ou de groupes auxquels l'action d'enregistrement de la règle s'applique.
- Ressources publiées. Vous créez une liste d'applications ou de bureaux publiés auxquels l'action d'enregistrement de la règle s'applique. Dans l'assistant Règles, choisissez le ou les sites XenApp/XenDesktop sur lesquels les applications ou bureaux sont disponibles.
- Groupes de mise à disposition ou machines. Vous créez une liste de groupes de mise à disposition ou de machines auxquels l'action d'enregistrement de la règle s'applique. Dans l'assistant Règles, choisissez l'emplacement dans lequel les groupes de mise à disposition ou les machines se trouvent.

Lorsque vous créez plus d'une règle dans une stratégie d'enregistrement, il est possible que certaines sessions correspondent aux critères de plusieurs de ces règles. Dans ces cas de figure, la règle ayant la plus haute priorité est celle appliquée à la session.

L'action d'enregistrement d'une règle en détermine la priorité :

- Les règles avec l'action Ne pas enregistrer ont la plus haute priorité.
- Les règles avec l'action Enregistrer avec notification ont la seconde plus haute priorité.
- Les règles avec l'action Enregistrer sans notification ont la priorité la plus faible.

Il se peut que certaines sessions ne correspondent à aucun critère de règle d'une stratégie d'enregistrement. Pour ces sessions, l'action d'enregistrement de la règle de repli des stratégies s'applique. L'action d'enregistrement de la règle de repli est toujours Ne pas enregistrer. La règle de repli ne peut être ni modifiée, ni supprimée.

Configurer des stratégies personnalisées

1. Ouvrez une session en tant qu'administrateur de stratégie autorisé sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session et sélectionnez **Stratégies d'enregistrement** dans le panneau de gauche et, dans la barre de menu, choisissez **Action > Ajouter une nouvelle stratégie**.
3. Cliquez avec le bouton droit sur **Nouvelle stratégie** et sélectionnez **Ajouter une règle**.
4. **Sélectionnez une option d'enregistrement** : dans l'assistant Règles, sélectionnez **Activer l'enregistrement de session avec notification** (ou **sans notification**), puis cliquez sur Suivant.
5. **Sélectionnez les critères de la règle** : vous pouvez choisir une ou une combinaison de ces trois options :
   Utilisateurs ou groupes
   Ressources publiées
   Groupes de mise à disposition ou machines
6. **Modifiez les critères de la règle** : pour modifier, cliquez sur les valeurs soulignées. Les valeurs sont soulignées en fonction des critères que vous avez choisis dans l'étape précédente.
7. Suivez les instructions de l'assistant pour terminer la configuration.

Groupes Active Directory

© 1999-2017 Citrix Systems, Inc. All rights reserved.

L'enregistrement de session vous permet d'utiliser les groupes Active Directory lorsque vous créez des stratégies. Utiliser les groupes Active Directory au lieu d'utilisateurs individuels simplifie la création et la gestion des règles et des stratégies. Par exemple, si les utilisateurs du service financier de votre société sont réunis dans un groupe Active Directory intitulé « Finance », vous pouvez créer une règle concernant tous les membres de ce groupe en sélectionnant le groupe Finance dans l'Assistant de règles lors de la création de la règle.

Utilisateurs sur liste blanche

Vous pouvez créer des stratégies d'enregistrement de session qui font en sorte que certains utilisateurs de votre organisation ne sont jamais enregistrés. Cela peut se traduire par mettre ces utilisateurs en liste blanche. Les listes blanches sont utiles pour les utilisateurs qui traitent des informations de nature confidentielle ou lorsque votre organisation ne souhaite pas enregistrer les sessions d'une certaine catégorie d'employés.

Par exemple, si tous les managers d'une entreprise sont membres d'un groupe Active Directory intitulé « Cadres supérieurs », vous pouvez être faire en sorte que les sessions de ces utilisateurs ne sont jamais enregistrées en créant une règle désactivant l'enregistrement de sessions pour le groupe Cadres supérieurs. Lorsque la stratégie contenant cette règle est active, aucune session des membres du groupe Cadres supérieurs n'est enregistrée. Les sessions des autres membres de votre organisation sont enregistrées en fonction d'autres règles de la stratégie active.

Créer une nouvelle stratégie

Remarque : pour utiliser l'assistant de règles, vous pouvez être invité à « cliquer sur la valeur soulignée pour la modifier » lorsqu'aucune valeur soulignée ne s'affiche. Les valeurs soulignées s'affichent uniquement le cas échéant. Si aucune valeur soulignée ne s'affiche, ignorez l'étape.

1. Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session.
3. Si vous observez une fenêtre indépendante Connexion au serveur d'enregistrement de session, veillez à ce que le nom du serveur d'enregistrement de session, le protocole et le port sont corrects. Cliquez sur OK.
4. Dans la console de stratégie d'enregistrement de session, sélectionnez Stratégies d'enregistrement.
5. Dans le menu, choisissez Ajouter une nouvelle stratégie. Une stratégie intitulée Nouvelle stratégie s'affiche dans le volet gauche.
6. Cliquez avec le bouton droit sur la nouvelle stratégie et choisissez Renommer à partir du menu.
7. Entrez un nouveau nom pour la stratégie que vous allez créer et appuyez sur Entrée ou cliquez n'importe où hors du cadre du nouveau nom.
8. Cliquez avec le bouton droit sur la stratégie, choisissez Ajouter une nouvelle règle dans le menu de lancer l'assistant Règles.
9. Suivez les instructions pour créer les règles de cette stratégie.

Modifier une stratégie

1. Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session.
3. Si vous observez une fenêtre indépendante Connexion au serveur d'enregistrement de session, veillez à ce que le nom du serveur d'enregistrement de session, le protocole et le port sont corrects. Cliquez sur OK.
4. Dans la console de stratégie d'enregistrement de session, développez Stratégies d'enregistrement.
5. Sélectionnez la stratégie que vous souhaitez modifier. Les règles de cette stratégie s'affichent dans le volet droit.
6. Ajoutez une nouvelle règle, modifiez une règle ou supprimez une règle :
   - Dans la barre de menus, choisissez Action > Ajouter une nouvelle règle. Si cette stratégie est active, une fenêtre

© 1999-2017 Citrix Systems, Inc. All rights reserved.

indépendante s'affiche pour demander confirmation de l'action entreprise. Utilisez l'assistant de règle pour créer une nouvelle règle.

- Sélectionnez la règle que vous souhaitez modifier, cliquez avec le bouton droit de la souris et choisissez Propriétés. Utilisez l'assistant de règles pour modifier la règle.
- Sélectionnez la règle que vous souhaitez supprimer, cliquez avec le bouton droit de la souris et choisissez Supprimer la règle.

Supprimer une stratégie

Remarque : vous ne pouvez pas supprimer de stratégie de système ou une stratégie active.

1. Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session.
3. Si vous observez une fenêtre indépendante Connexion au serveur d'enregistrement de session, veillez à ce que le nom du serveur d'enregistrement de session, le protocole et le port sont corrects. Cliquez sur OK.
4. Dans la console de stratégie d'enregistrement de session, développez Stratégies d'enregistrement.
5. Dans le volet gauche, sélectionnez la stratégie que vous souhaitez supprimer. Si la stratégie est active, vous devez en activer une autre.
6. Dans la barre de menus, choisissez Action > Supprimer la stratégie.
7. Sélectionnez Oui pour confirmer l'action.

Comportement des reprises - définitions

Lorsque vous activez une stratégie, la stratégie précédemment active reste en vigueur jusqu'à la fin de la session de l'utilisateur ; dans certains cas, la nouvelle stratégie prend effet lorsque le fichier passe en reprise. Les fichiers sont repris lorsqu'ils atteignent la limite de taille maximale. Pour plus d'informations sur la taille maximale des fichiers pour les enregistrements, consultez la section Définir la taille des fichiers pour les enregistrements.

Le tableau suivant illustre en détail les événements qui se produisent lorsque vous appliquez une nouvelle stratégie pendant qu'une session est en cours d'enregistrement et qu'une reprise a lieu :

Stratégie précédente :	Nouvelle stratégie :	Stratégie en vigueur après la reprise :
Ne pas enregistrer.	Toute autre stratégie.	Pas de modification. La nouvelle stratégie ne prend effet que lorsque l'utilisateur ouvre une nouvelle session.
Enregistrer sans notification	Ne pas enregistrer.	L'enregistrement s'arrête.
	Enregistrer avec notification	L'enregistrement continue et un message de notification s'affiche.
Enregistrer avec notification	Ne pas enregistrer.	L'enregistrement s'arrête.
	Enregistrer sans notification	L'enregistrement continue. Aucun message ne s'affiche avant que l'utilisateur ouvre une nouvelle session.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Créer des messages de notification

Jul 07, 2016

Si la stratégie d'enregistrement active précise que les utilisateurs sont prévenus lorsque leurs sessions sont enregistrées, une fenêtre indépendante s'ouvre et affiche un message de notification après que les utilisateurs aient entré leurs informations d'identification. Le message suivant est la notification par défaut : « Votre activité relative aux programmes démarrés récemment est enregistrée actuellement. Si vous désapprouvez cette condition, fermez les programmes en question ». L'utilisateur clique sur OK pour fermer la fenêtre et pour continuer la session.

Le message de notification par défaut s'affiche dans la langue du système d'exploitation des ordinateurs hébergeant le serveur d'enregistrement de session.

Vous pouvez créer des notifications personnalisées dans les langues de votre choix ; toutefois, vous ne disposez que d'un message de notification par langue. Vos utilisateurs peuvent voir le message de notification dans la langue correspondant à leurs paramètres utilisateur locaux préférés.

Pour créer un nouveau message de notification

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu Démarrer, choisissez Propriétés du lecteur d'enregistrement de session.
3. Dans la fenêtre Propriétés du serveur d'enregistrement de session, cliquez sur l'onglet Notifications.
4. Cliquez sur Ajouter.
5. Choisissez la langue du nouveau message et tapez-le. Vous ne pouvez créer qu'un seul message par langue.

Une fois accepté et activé, le nouveau message s'affiche dans la boîte Messages de notification en langues étrangères.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Désactiver ou activer l'enregistrement

Jul 07, 2016

L'installation de l'agent d'enregistrement de session s'effectue sur chaque machine avec OS de serveur pour laquelle vous souhaitez enregistrer des sessions. Chaque Agent est équipé d'un paramètre permettant d'activer les enregistrements pour le serveur sur lequel il est installé. Après l'activation de la fonction d'enregistrement, l'enregistrement de session évalue la stratégie d'enregistrement active, ce qui permet de déterminer les sessions à enregistrer.

Lorsque vous installez l'agent d'enregistrement de session, la fonction d'enregistrement est activée. Citrix vous recommande de désactiver l'enregistrement de session sur les serveurs qui ne sont pas enregistrés, compte tenu du léger impact sur les performances au niveau du serveur, même si aucun enregistrement n'a lieu.

Pour désactiver ou activer l'enregistrement sur un serveur

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez Propriétés de l'agent d'enregistrement de session.
3. Sous l'option Enregistrement de session, sélectionnez ou effacez le contenu de la case Activer l'enregistrement de session pour ce VDA avec OS de serveur afin de spécifier si les sessions de ce serveur peuvent être enregistrées.
4. À l'invite, redémarrez le service de l'agent d'enregistrement de session pour accepter la modification.

Remarque : lorsque vous installez l'enregistrement de session, la stratégie active est Ne pas enregistrer (aucune session n'est enregistrée, sur aucun serveur). Pour commencer à enregistrer, utilisez la console de stratégie d'enregistrement de session pour activer une stratégie différente.

Activer l'enregistrement d'événement personnalisé

L'enregistrement de session vous permet d'utiliser des applications tierces pour insérer des données personnalisées (des événements) dans des sessions enregistrées. Ces événements s'affichent lorsque la session est visualisée à l'aide du lecteur d'enregistrement de session. Ils font partie du fichier de la session enregistrée et ne peuvent pas être modifiés une fois la session enregistrée.

Par exemple, un événement peut contenir le texte suivant : « Ouverture de navigateur par l'utilisateur ». Chaque fois qu'un utilisateur ouvre un navigateur pendant une session en cours d'enregistrement, le texte s'insère dans l'enregistrement à ce point. Lorsque la session est lue dans le lecteur d'enregistrement de session, le visualiseur peut localiser et compter le nombre de fois qu'un utilisateur a ouvert un navigateur en notant le nombre de marqueurs figurant dans la liste Événements et signets du lecteur d'enregistrement de session.

Pour insérer des événements personnalisés dans les enregistrements sur un serveur :

- Utilisez la fenêtre Propriétés de l'agent d'enregistrement de session pour activer un paramètre sur chaque serveur dans lequel vous souhaitez insérer des événements personnalisés. Vous devez activer chaque serveur séparément, l'activation générale de tous les serveurs d'un site n'étant pas autorisée.
- Générez des applications sur l'API d'enregistrement d'événements s'exécutant dans chaque session XenApp des utilisateurs (pour injecter les données dans l'enregistrement).

L'installation de l'enregistrement de session comprend une interface d'application COM (API) vous permettant d'insérer du texte provenant d'applications tierces dans un enregistrement. Vous pouvez utiliser l'API de nombreux langages de programmation, notamment Visual Basic, C++ ou C#. Le fichier .dll API des événements d'enregistrement de session est

© 1999-2017 Citrix Systems, Inc. All rights reserved.

installé dans le cadre de l'installation de l'enregistrement de session. Il se trouve à l'emplacement suivant : C:\Program Files\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll.

Pour activer l'enregistrement d'événements personnalisés sur un serveur

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Propriétés de l'agent d'enregistrement de session**.
3. Dans la fenêtre **Propriétés de l'agent d'enregistrement de session**, cliquez sur l'onglet **Enregistrement**.
4. Sous **Enregistrement d'événement personnalisé**, cochez la case **Permettre aux applications tierces d'enregistrer des données personnalisées sur ce serveur**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Activer ou désactiver la lecture de session active et la protection de lecture

Jul 07, 2016

Activer ou désactiver la lecture de session active

Avec le lecteur d'enregistrement de session, vous pouvez visualiser une session pendant son enregistrement ou après celui-ci. L'affichage d'une session en cours d'enregistrement est similaire au visionnage d'actions se déroulant en direct ; il existe toutefois un décalage d'une ou deux secondes dû à la propagation des données du serveur XenApp ou XenDesktop.

Certaines fonctionnalités ne sont pas disponibles pendant l'affichage de sessions dont l'enregistrement n'est pas terminé :

- Une signature numérique ne peut pas être attribuée tant que l'enregistrement n'est pas terminé. Si la signature numérique est activée, vous pouvez afficher les sessions actives, mais elles ne sont pas signées numériquement et vous ne pouvez pas en voir les certificats avant que la session se termine.
- La protection en lecture ne peut pas s'appliquer tant que l'enregistrement n'est pas terminé. Si la protection en lecture est activée, vous pouvez afficher les sessions actives, mais elles ne sont pas cryptées tant que la session n'est pas terminée.
- Vous ne pouvez pas mettre en cache un fichier tant que l'enregistrement n'est pas terminé.

Par défaut, la lecture de session active est activée.

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu Démarrer, choisissez Propriétés du lecteur d'enregistrement de session.
3. Dans la fenêtre Propriétés du serveur d'enregistrement de session, cliquez sur l'onglet Lecture.
4. Cochez ou désélectionnez la case Autoriser la lecture d'une session active.

Activer ou désactiver la protection de lecture

Par mesure de sécurité, l'enregistrement de session crypte automatiquement les fichiers enregistrés avant qu'ils soient téléchargés pour être affichés dans le lecteur d'enregistrement de session. Cette protection de lecture les empêche d'être copiés et visualisés par toute personne autre que l'utilisateur ayant téléchargé le fichier. Les fichiers ne peuvent pas être lus sur une autre station de travail ou par un autre utilisateur. Les fichiers cryptés sont identifiés par l'extension .icle ; les fichiers non cryptés sont identifiés par l'extension .icl. Les fichiers demeurent cryptés tant qu'ils résident dans le cache de la station de travail sur laquelle le lecteur d'enregistrement de session est installé, et ce jusqu'à ce qu'ils soient ouverts par un utilisateur autorisé.

Citrix vous recommande d'utiliser HTTPS pour protéger le transfert de données.

Par défaut, la protection de lecture est désactivée.

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du lecteur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Lecture**.
4. Cochez ou désélectionnez la case **Crypter les fichiers d'enregistrement de session téléchargés pour les lire**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Activer et désactiver les signatures numériques

Jul 07, 2016

Si vous avez installé des certificats sur les ordinateurs sur lesquels les composants d'enregistrement de session sont installés, vous pouvez augmenter la sécurité de votre déploiement d'enregistrement de session en attribuant des signatures numériques à l'enregistrement de sessions.

Par défaut, la fonction de signature numérique est désactivée. Après avoir sélectionné le certificat utilisé pour signer les enregistrements, l'enregistrement de session accorde une autorisation d'accès en lecture au Gestionnaire de stockage d'enregistrement de session.

Pour activer les signatures numériques

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu Démarrer, choisissez Propriétés du lecteur d'enregistrement de session.
3. Dans la fenêtre Propriétés du serveur d'enregistrement de session, cliquez sur l'onglet Signature.
4. Naviguez jusqu'au certificat activant la communication entre les différents ordinateurs sur lesquels les composants d'enregistrement de session sont installés.

Pour désactiver les signatures numériques

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu Démarrer, choisissez Propriétés du lecteur d'enregistrement de session.
3. Dans la fenêtre Propriétés du serveur d'enregistrement de session, cliquez sur l'onglet Signature.
4. Cliquez sur Effacer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Définir l'emplacement des enregistrements

Jul 07, 2016

Utilisez la fenêtre Propriétés du serveur d'enregistrement de session pour spécifier l'emplacement du stockage des enregistrements et l'emplacement de restauration des enregistrements restaurés.

Remarque : pour archiver les fichiers ou restaurer les fichiers supprimés, utilisez la commande icldb.

Pour préciser l'emplacement des fichiers enregistrés

Par défaut, les enregistrements sont stockés dans le répertoire lecteur:**\SessionRecordings** de l'ordinateur hébergeant le serveur d'enregistrement de session. Vous pouvez changer le répertoire de stockage des enregistrements, ajouter des répertoires supplémentaires afin d'équilibrer la charge sur plusieurs volumes ou d'optimiser l'usage d'espace supplémentaire. La présence de plusieurs répertoires dans la liste indique que l'équilibrage de la charge s'applique dans les répertoires pour les enregistrements. Vous pouvez ajouter un répertoire plusieurs fois. L'équilibrage de charge passe successivement dans tous les répertoires.

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu Démarrer, choisissez Propriétés du lecteur d'enregistrement de session.
3. Dans la fenêtre Propriétés du serveur d'enregistrement de session, cliquez sur l'onglet Stockage.
4. Utilisez la liste Répertoires de stockage des fichiers pour gérer les répertoires dans lesquels les enregistrements sont stockés.

Après la sélection des répertoires, l'enregistrement de session accorde à son service les autorisations de contrôle total sur ces répertoires.

Vous pouvez créer des répertoires de stockage de fichier sur le lecteur local, le volume réseau SAN ou un chemin réseau UNC complet. Les lettres de lecteur mappées sur réseau ne sont pas prises en charge. N'utilisez pas l'enregistrement de session avec un serveur NAS (Network-Attached Storage), en raison des sérieux problèmes de performances et de sécurité liés à l'écriture des données d'enregistrement sur un lecteur réseau.

Pour spécifier un répertoire de restauration de fichiers archivés

Par défaut, les enregistrements archivés sont restaurés sur le répertoire lecteur:**\SessionRecordingsRestore** de l'ordinateur hébergeant le serveur d'enregistrement de session. Vous pouvez changer de répertoire de stockage des enregistrements archivés.

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu Démarrer, choisissez Propriétés du lecteur d'enregistrement de session.
3. Dans la fenêtre Propriétés du serveur d'enregistrement de session, cliquez sur l'onglet Stockage.
4. Dans le champ Restaurer le répertoire des fichiers archivés, tapez le répertoire des fichiers d'archive restaurés.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Définir la taille des fichiers pour les enregistrements

Jul 07, 2016

À mesure que la taille des enregistrements augmente, les fichiers peuvent prendre plus longtemps à télécharger et réagir plus lentement lorsque vous utilisez le curseur de recherche pour naviguer pendant la lecture. Pour contrôler la taille des fichiers, spécifiez un seuil limite. Lorsque l'enregistrement atteint cette limite, l'enregistrement de session ferme le fichier et en ouvre un nouveau afin de poursuivre l'enregistrement. Cette action s'appelle une reprise.

Important : le paramètre de reprise ne s'applique pas aux sessions de bureau VDI pour XenDesktop 7.8 et l'agent d'enregistrement de session. Dans ce cas, chaque fichier d'enregistrement a une limite de taille maximale de 1 Go et les activités ne sont pas enregistrées une fois que cette limite est atteinte.

Vous pouvez préciser deux seuils pour une reprise :

- **Taille de fichier.** Lorsque le fichier atteint le nombre de méga-octets spécifié, l'enregistrement de session ferme le fichier et en ouvre un nouveau. Par défaut, les fichiers sont repris lorsqu'ils atteignent 50 mégaoctets ; toutefois vous pouvez spécifier une limite allant de 10 mégaoctets à un gigaoctet.
- **Durée.** Lorsque la durée d'enregistrement de la session atteint le nombre d'heures précisé, le fichier se ferme et un nouveau fichier s'ouvre. Par défaut, les fichiers sont repris lorsque la durée d'enregistrement atteint 12 heures, mais vous pouvez spécifier une limite allant de 1 heure à 24 heures.

L'enregistrement de session vérifie les deux champs afin de déterminer lequel des événements se produit en premier pour activer une reprise. Par exemple, si vous spécifiez une valeur de 17 Mo pour la taille de fichier et six heures pour la durée et que l'enregistrement atteint 17 Mo en trois heures, l'enregistrement de session réagit à la taille de fichier (17 Mo) pour fermer le fichier et en ouvrir un nouveau.

Pour éviter de créer trop de fichiers de petite taille, l'enregistrement de session ne procède à aucune reprise avant qu'une heure au moins ne se soit écoulée (il s'agit du nombre minimal que vous pouvez entrer), quelle que soit la valeur spécifiée pour la taille de fichier. L'exception à cette règle est si la taille du fichier dépasse un gigaoctet.

Pour préciser une limite maximale pour un fichier

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu Démarrer, choisissez Propriétés du lecteur d'enregistrement de session.
3. Dans la fenêtre Propriétés du serveur d'enregistrement de session, cliquez sur l'onglet Reprise.
4. Entrez un nombre entier compris entre 10 et 1024 pour spécifier la taille maximale des fichiers, en méga-octets.
5. Entrez un nombre entier compris entre 1 et 24 pour spécifier la durée maximale des enregistrements, en heures.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Afficher les enregistrements

Jul 07, 2016

Utilisez le lecteur d'enregistrement de session pour afficher, rechercher et créer des signets pour les sessions XenApp et XenDesktop enregistrées.

Si les sessions sont enregistrées avec la fonctionnalité de lecture active, vous pouvez afficher les sessions en cours de progression, avec un retard de quelques secondes, ainsi que les sessions terminées.

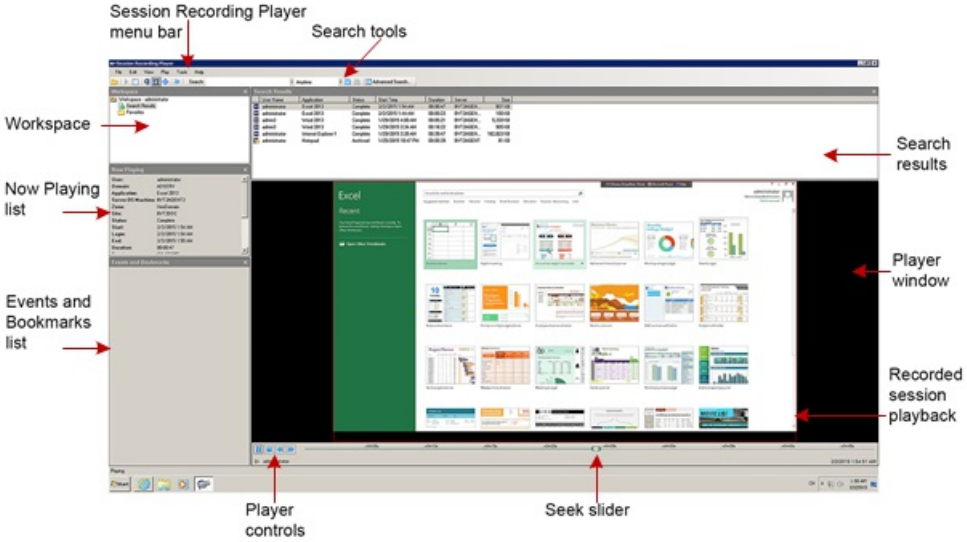
Les sessions dont la durée ou la taille de fichier est supérieure aux limites configurées par votre administrateur d'enregistrement de session s'affichent sur plusieurs fichiers de session.

Remarque : un administrateur d'enregistrement de session doit accorder aux utilisateurs le droit d'accéder aux sessions des machines avec OS de serveur. Si l'accès aux sessions vous est refusé, contactez votre administrateur d'enregistrement de session.
Lorsque le lecteur d'enregistrement de session est installé, l'administrateur d'enregistrement de session établit généralement une connexion entre le lecteur d'enregistrement de session et le serveur d'enregistrement de session. Si cette connexion n'est pas établie, vous êtres invité à l'établir à l'occasion de la première recherche de fichiers. Pour plus d'informations sur ce sujet, contactez votre administrateur d'enregistrement de session.

Pour lancer le lecteur d'enregistrement de session

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
   Le lecteur d'enregistrement de session s'affiche.

Cette illustration présente le lecteur d'enregistrement de session. Les bulles en indiquent les éléments principaux. Les fonctions de ces éléments sont décrites au fil des articles suivants.



Pour afficher ou masquer les éléments de fenêtre

Le lecteur d'enregistrement de session possède des éléments de fenêtre que vous activez et désactivez.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Dans la barre de menu du lecteur d'enregistrement de session, choisissez Affichage.
4. Choisissez les éléments que vous souhaitez afficher. La sélection d'un élément en entraîne l'affichage immédiat. Un élément sélectionné est indiqué par la case correspondante cochée.

Pour changer de serveurs d'enregistrement de session

Si l'administrateur d'enregistrement de session paramètre votre lecteur d'enregistrement de session avec la capacité de se connecter à plus d'un serveur d'enregistrement de session, vous pouvez sélectionner le serveur d'enregistrement de session auquel le lecteur d'enregistrement de session se connecte. Le lecteur d'enregistrement de session ne peut se connecter qu'à un seul serveur d'enregistrement de session à la fois.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Dans la barre de menus du lecteur d'enregistrement de session, choisissez Outils > Options > Connexions.
4. Sélectionnez le serveur d'enregistrement de session auquel vous connecter.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ouvrir et lire des enregistrements

Jul 07, 2016

Vous pouvez utiliser trois méthodes différentes pour ouvrir des enregistrements de session dans le lecteur d'enregistrement de session :

- Faites une recherche à l'aide du lecteur d'enregistrement de session. Les sessions enregistrées correspondant aux critères de recherche s'affichent dans la zone des résultats de la recherche.
- Accédez aux fichiers de session enregistrée directement sur votre disque dur local ou sur un lecteur partagé.
- Accédez aux fichiers de session enregistrée à partir d'un dossier Favoris.

Lorsque vous ouvrez un fichier enregistré sans signature numérique, un message d'avertissement s'affiche pour vous indiquer que l'origine et l'intégrité du fichier n'ont pas été vérifiées. Si vous avez confiance dans l'intégrité du fichier, cliquez sur Oui dans la fenêtre indépendante pour ouvrir le fichier.

Pour ouvrir et lire un enregistrement dans la zone de résultats de la recherche

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Faites une recherche.
4. Si les résultats de la recherche ne sont pas visibles, sélectionnez Résultats de la recherche dans le volet Espace de travail.
5. Dans la zone de résultats de la recherche, sélectionnez la session que vous souhaitez passer en lecture.
6. Effectuez l'une des opérations suivantes, au choix :
   - Double-cliquez sur la session.
   - Cliquez avec le bouton droit et sélectionnez Lire.
   - Dans la barre de menu du lecteur d'enregistrement de session, sélectionnez Lecture > Lire.

Pour ouvrir et lire un enregistrement en accédant au fichier

Les noms de fichiers de session commencent par i_, suivi d'un identifiant alphanumérique de fichier unique, suivi d'une extension de fichier .icl et .icle : .icl pour les enregistrements sans protection en lecture, .icle pour les enregistrements avec protection en lecture. L'enregistrement de session sauvegarde les fichiers de sessions enregistrées dans un répertoire incorporant la date d'enregistrement de la session. Par exemple, le fichier d'une session enregistrée le lundi 22 décembre 2014, est enregistré dans le chemin de dossier 2014\12\22.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Effectuez l'une des opérations suivantes, au choix :
   - Dans la barre de menus du lecteur d'enregistrement de session, choisissez Fichier > Ouvrir et recherchez le fichier.
   - À l'aide de Windows Explorer, naviguez jusqu'au fichier et glissez-déplacez le fichier dans la fenêtre Lecteur.
   - À l'aide de Windows Explorer, naviguez jusqu'au fichier et double-cliquez dessus.
   - Si vous avez créé un dossier Favoris dans le volet Espace de travail, sélectionnez Favoris et ouvrez le fichier qui s'y trouve de la même manière que vous ouvrez les fichiers de la zone de résultats de la recherche.

Utiliser des favoris

Créer des dossiers Favoris vous permet d'accéder rapidement à des enregistrements que vous visionnez fréquemment. Ces dossiers Favoris répertorient des fichiers de sessions enregistrées qui sont stockés sur votre station de travail ou sur un lecteur réseau. Vous pouvez importer et exporter ces fichiers vers d'autres stations de travail et partager ces dossiers avec d'autres utilisateurs du lecteur d'enregistrement de session.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Remarque : seuls les utilisateurs disposant des droits d'accès au lecteur d'enregistrement de session peuvent télécharger les fichiers de sessions enregistrées associés aux dossiers Favoris. Pour plus d'informations sur les droits d'accès, veuillez contacter votre administrateur d'enregistrement de session.
Pour créer un sous-dossier Favoris :

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Dans le lecteur d'enregistrement de session, sélectionnez le dossier Favoris de votre volet Espace de travail.
4. Dans la barre de menus, choisissez Fichier > Dossier > Nouveau dossier. Un nouveau dossier s'affiche sous le dossier Favoris.
5. Entrez le nom du dossier, puis appuyez sur Entrée ou cliquez n'importe où pour accepter le nouveau nom.

Vous pouvez utiliser les autres options qui s'affichent dans le menu Fichier > Dossier pour supprimer, renommer, copier, importer et exporter les dossiers.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Effectuer des recherches dans des sessions enregistrées

Jul 07, 2016

Le lecteur d'enregistrement de session vous permet d'effectuer des recherches rapides, des recherches avancées et de spécifier des options s'appliquant à toutes les recherches. Le résultat des recherches s'affiche dans la zone Résultats de la recherche du lecteur d'enregistrement de session.

Remarque : pour afficher toutes les sessions enregistrées disponibles, jusqu'au nombre maximum de sessions pouvant s'afficher dans une recherche, effectuez une recherche sans spécifier de paramètre de recherche précis.

Pour effectuer une recherche rapide

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Définissez vos critères de recherche :
   - Entrez le critère de recherche dans le champ Rechercher. Pour vous aider :
   - Faites glisser le pointeur de la souris sur l'étiquette Rechercher pour afficher une liste de paramètres à utiliser à titre indicatif.
   - Cliquez sur la flèche à droite du champ Rechercher pour afficher le texte des 64 dernières recherches que vous avez effectuées.
   - Utilisez la liste déroulante à droite du champ Rechercher pour sélectionner une période ou une durée indiquant quand la session a été enregistrée.
4. Cliquez sur l'icône des jumelles à droite de la liste déroulante pour démarrer la recherche.

Pour effectuer une recherche avancée

Conseil : les recherches avancées peuvent prendre jusqu'à 20 secondes pour renvoyer des résultats contenant plus de 150 000 entités. Citrix vous recommande d'utiliser des critères de recherche plus précis comme une plage de dates ou un utilisateur afin de réduire le nombre de résultats.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Dans la fenêtre du lecteur d'enregistrement de session, cliquez sur Recherche avancée dans la barre d'outils ou choisissez Outils > Recherche avancée.
4. Définissez vos critères de recherche dans les onglets de la boîte de dialogue Recherche avancée :
   - Commun vous permet de faire une recherche par domaine ou autorité de compte, par site, groupe, machine avec OS de serveur, application ou identificateur de fichier.
   - Date/Heure vous permet de faire une recherche en fonction de la date, du jour de la semaine et de l'heure.
   - Événements vous permet d'effectuer une recherche sur les événements personnalisés que votre administrateur d'enregistrement de session a inséré dans les sessions.
   - Autre vous permet de faire une recherche par nom de session, nom de client, adresse de client et durée d'enregistrement. Cet onglet vous permet aussi de spécifier, pour cette recherche, le nombre maximum de résultats affichés et d'inclure ou d'exclure les fichiers archivés.

   À mesure que vous précisez les critères de recherche, la requête que vous créez s'affiche dans le volet situé au bas de la boîte de dialogue.
5. Cliquez sur Rechercher pour démarrer la recherche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conseil : vous pouvez enregistrer et récupérer les requêtes de recherche avancée. Cliquez sur Enregistrer dans la boîte de dialogue Recherche avancée pour enregistrer la requête actuelle. Cliquez sur Ouvrir dans la boîte de dialogue Recherche avancée pour extraire une requête enregistrée. Les requêtes sont enregistrées sous forme de fichiers avec l'extension .isq.

Pour paramétrer les options de recherche

Les options de recherche du lecteur d'enregistrement de session vous permettent de limiter le nombre maximum d'enregistrements de sessions qui s'affichent dans les résultats de la recherche et de spécifier si ces résultats peuvent inclure les fichiers de sessions archivés.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Dans la barre de menus du lecteur d'enregistrement de session, choisissez Outils > Options > Recherche.
4. Dans le champ Nombre maximum de résultats à afficher, entrez le nombre de résultats de recherche que vous souhaitez afficher. Le nombre maximum de résultats pouvant être affichés est de 500.
5. Pour paramétrer l'inclusion ou l'exclusion des fichiers archivés dans les recherches, cochez ou désélectionnez la case Inclure les fichiers archivés.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Lire des sessions enregistrées

Jul 07, 2016

Après avoir ouvert une session enregistrée dans le lecteur d'enregistrement de session, vous pouvez parcourir les sessions enregistrées en utilisant les méthodes suivantes :

- Utilisez les contrôles du lecteur pour lire, arrêter, mettre en pause et pour augmenter ou réduire la vitesse de lecture.
- Utilisez le curseur de recherche pour avancer ou reculer.

Si vous avez inséré des marqueurs dans l'enregistrement ou si la session enregistrée contient des événements personnalisés, vous pouvez aussi naviguer directement dans la session jusqu'à ces marqueurs et événements.

Remarque :

- un second pointeur de souris peut apparaître pendant la lecture d'une session enregistrée. Le deuxième pointeur s'affiche dans l'enregistrement lorsque l'utilisateur navigue dans Internet Explorer, puis clique sur une image qui était à l'origine plus grande que l'écran, mais avait été automatiquement réduite par Internet Explorer. Bien qu'un seul pointeur apparaisse au cours de la session, deux peuvent apparaître pendant la lecture.
- Cette version de l'enregistrement de session ne prend pas en charge l'accélération multimédia SpeedScreen pour XenApp ou le paramètre de stratégie de réglage de la qualité Flash pour XenApp. Lorsque cette option est activée, la lecture affiche un carré noir.
- L'enregistrement de session ne peut pas enregistrer la vidéo provenant de la webcam Lync lors de l'utilisation du pack d'optimisation HDX RealTime.

Utiliser les contrôles du lecteur

Vous pouvez cliquer sur les contrôles du lecteur sous la fenêtre Lecteur ou y accéder en choisissant Lecture dans la barre de menu du lecteur d'enregistrement de session. Utilisez les contrôles du lecteur pour effectuer les opérations suivantes :

	Lire le fichier de session sélectionné.
	Suspendre la lecture.
	Arrêter la lecture. Si vous cliquez sur Arrêter, puis sur Lire, l'enregistrement redémarre depuis le début du fichier.
	Réduire la vitesse de lecture actuelle jusqu'à un quart minimum de la vitesse normale.
	Doubler la vitesse de lecture actuelle jusqu'à 32 fois maximum la vitesse normale.

Utiliser le curseur de recherche

Utilisez le curseur de recherche situé sous la fenêtre Lecteur pour sauter directement à une position différente dans la session enregistrée. Vous pouvez faire glisser le curseur de recherche jusqu'au point de l'enregistrement que vous souhaitez afficher ou vous pouvez cliquer n'importe où sur la barre du curseur pour vous déplacer dans cette direction.

Vous pouvez aussi utiliser les touches clavier suivantes pour contrôler le curseur de recherche :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Touche :	Action de recherche :
Home	Recherche du début.
Fin	Recherche à la fin.
Flèche droite	Recherche en avant (cinq secondes).
Flèche gauche	Recherche en arrière (cinq secondes).
Déplacement de la roulette de la souris d'un cran vers le bas	Recherche en avant (15 secondes).
Déplacement de la roulette de la souris d'un cran vers le haut	Recherche en arrière (15 secondes).
Ctrl + Flèche droite	Recherche en avant (30 secondes).
Ctrl + Flèche gauche	Recherche en arrière (30 secondes).
Page suivante	Recherche en avant (une minute).
Page haut	Recherche en arrière (une minute).
Ctrl + Déplacement de la roulette de la souris d'un cran vers le bas	Recherche en avant (90 secondes).
Ctrl + Déplacement de la roulette de la souris d'un cran vers le haut	Recherche en arrière (90 secondes).
Ctrl + Page suivante	Recherche en avant (six minutes).
Ctrl + Page précédente	Recherche en arrière (six minutes).

Remarque : pour régler la vitesse du curseur de recherche : dans la barre de menu du lecteur d'enregistrement de session, choisissez Outils > Options > Lecteur et faites glisser le curseur pour augmenter ou réduire le délai de réponse de la recherche. Un temps de réponse plus rapide sollicite plus de mémoire. La réponse peut être lente en fonction de la taille des enregistrements et du matériel de votre ordinateur.

Pour modifier la vitesse de lecture

Vous pouvez paramétrer le lecteur d'enregistrement de session pour une lecture en incréments exponentiels allant d'un quart à 32 fois la vitesse de lecture normale.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Dans la barre de menu du lecteur d'enregistrement de session, choisissez Lecture > Vitesse de lecture.
4. Choisissez une option de vitesse.

La vitesse s'adapte immédiatement. Un nombre indiquant la vitesse, augmentée ou réduite, s'affiche sous les contrôles de la fenêtre du lecteur. Le texte indiquant le taux exponentiel s'affiche rapidement en vert dans la fenêtre Lecteur.

Pour ignorer les espaces sans action

Le mode de consultation rapide vous permet de régler le lecteur d'enregistrement de session de manière à sauter les parties de sessions enregistrées pendant lesquelles aucune action n'a lieu. Ce réglage permet de gagner du temps pour visionner l'enregistrement ; cependant, il ne permet pas d'ignorer les séquences animées comme les mouvements de souris, les clignotements de curseur ou les horloges affichées et leurs aiguilles en mouvement.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Dans la barre de menus du lecteur d'enregistrement de session, choisissez Lecture > Mode de consultation rapide.

L'option passe de l'état activée à désactivée et vice-versa. Chaque fois que vous le choisissez, le statut s'affiche rapidement en vert dans la fenêtre Lecteur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Utiliser des événements et des signets

Jul 07, 2016

Vous pouvez utiliser les événements et les signets pour vous aider à naviguer à travers les sessions enregistrées.

Les événements sont insérés dans les sessions pendant l'enregistrement de celles-ci, à l'aide de l'API d'événements et d'une application tierce. Les événements sont enregistrés comme faisant partie du fichier de session. Vous ne pouvez pas les supprimer ou les modifier à l'aide du lecteur d'enregistrement de session.

Les signets sont des marqueurs que vous insérez dans les sessions enregistrées à l'aide du lecteur d'enregistrement de session. Les signets sont associés à la session enregistrée jusqu'à ce que vous les supprimiez, mais ils ne sont pas enregistrés comme faisant partie du fichier de session. Par défaut, chaque signet est accompagné de l'étiquette Signet, mais vous pouvez changer ce nom pour le texte d'annotation de votre choix (avec une limite maximale de 128 caractères).

Les événements et signets s'affichent sous forme de points dans la fenêtre Lecteur. Les événements sont représentés par des points jaunes, les signets par des points bleus. Déplacer la souris sur ces points permet d'afficher le texte de l'étiquette qui leur est associé. Vous pouvez aussi afficher les événements et les signets dans la liste correspondante du lecteur d'enregistrement de session. Ils s'affichent dans cette liste avec leur étiquette et l'heure de la session enregistrée à laquelle ils apparaissent, dans l'ordre chronologique.

Vous pouvez utiliser les événements et les signets pour vous aider à naviguer à travers les sessions enregistrées. En allant à un événement ou un signet, vous pouvez atteindre directement le point de la session enregistrée où l'événement ou signet a été inséré.

Pour afficher les événements et les signets dans la liste

La liste des événements et des signets contient les événements et les signets insérés dans la session enregistrée en cours de lecture. Elle peut afficher les événements, les signets seulement ou elle peut afficher Ies deux.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Déplacez le pointeur de la souris dans la zone de la liste des événements et des signets et cliquez avec le bouton droit pour afficher le menu.
4. Choisissez Afficher les événements seulement, Afficher les signets seulement ou Afficher tout.

Pour insérer un signet

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Commencez la lecture de la session enregistrée à laquelle vous souhaitez ajouter un signet.
4. Déplacez le curseur de recherche sur le point d'insertion souhaité pour le signet.
5. Déplacez le pointeur de la souris dans la zone de la fenêtre Lecteur et cliquez avec le bouton droit de la souris pour afficher le menu.
6. Ajoutez un signet avec l'étiquette Signet par défaut ou créez une annotation.
   - Pour ajouter un signet avec l'étiquette Signet par défaut, choisissez Ajouter un signet.
   - Pour ajouter un signet avec une étiquette de texte descriptif créée par vous, choisissez Annoter. Entrez le texte de l'étiquette que vous souhaitez attribuer au signet, d'une longueur maximale de 128 caractères. Cliquez sur OK.

Pour ajouter ou modifier une annotation

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Après avoir créé un signet, vous pouvez y ajouter une annotation ou en modifier une.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Commencez la lecture de la session enregistrée contenant le signet.
4. Veillez à ce que la liste des événements et des signets affiche les signets.
5. Sélectionnez le signet dans la liste des événements et des signets et cliquez avec le bouton droit pour afficher le menu.
6. Choisissez Modifier l'annotation.
7. Dans la fenêtre qui s'affiche, entrez la nouvelle annotation et cliquez sur OK.

Pour supprimer un signet

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Commencez la lecture de la session enregistrée contenant le signet.
4. Veillez à ce que la liste des événements et des signets affiche les signets.
5. Sélectionnez le signet dans la liste des événements et des signets et cliquez avec le bouton droit pour afficher le menu.
6. Choisissez Supprimer.

Pour aller à un événement ou un signet

Aller à un événement ou un signet conduit le lecteur d'enregistrement de session à aller au point de la session enregistrée où l'événement ou le signet a été inséré.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Commencez la lecture d'un enregistrement de session contenant des événements ou des signets.
4. Allez à un événement ou un signet.
   - Dans la zone située sous la fenêtre du lecteur, cliquez sur le point représentant l'événement ou le signet que vous souhaitez consulter.
   - Dans la liste des événements et des signets, double-cliquez sur un élément pour vous y rendre. Pour aller à l'événement ou au signet suivant, sélectez-en un dans la liste, cliquez avec le bouton droit pour en afficher le menu et choisissez Rechercher jusqu'au signet.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Modifier l'affichage de la lecture

Jul 07, 2016

Certaines options vous permettent de modifier le mode d'affichage des sessions enregistrées dans la fenêtre Lecteur. Vous pouvez faire un panoramique et mettre à l'échelle l'image, afficher la lecture en mode plein écran, afficher la fenêtre Lecteur dans une fenêtre séparée et afficher une bordure rouge autour de la session enregistrée pour la différencier de l'arrière-plan du lecteur.

Pour afficher la fenêtre Lecteur en format plein écran

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Dans la barre de menu du lecteur d'enregistrement de session, choisissez Afficher > Lecteur en plein écran.
4. Pour revenir à la taille originale, appuyez sur Échap ou F11.

Pour afficher la fenêtre Lecteur dans une fenêtre séparée.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Dans la barre de menu du lecteur d'enregistrement de session, choisissez Affichage > Lecteur dans une fenêtre séparée. Une nouvelle fenêtre s'affiche ; elle contient la fenêtre Lecteur. Vous pouvez faire glisser et redimensionner la fenêtre.
4. Pour incorporer la fenêtre Lecteur dans la fenêtre principale, choisissez Affichage > Lecteur dans une fenêtre séparée ou appuyez sur F10.

Pour mettre l'écran de lecture de session à l'échelle de la fenêtre Lecteur

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Dans la barre de menu du lecteur d'enregistrement de session, choisissez Lecture > Panorama et mise à l'échelle > Mise à l'échelle.
   - Mise à l'échelle (rendu rapide) rétrécit l'image tout en fournissant une bonne qualité graphique. Les images sont créées plus rapidement qu'avec l'option Haute qualité, mais les images et le texte ne sont pas aussi nets. Utilisez cette option si vous avez des problèmes de performances en utilisant le mode Haute qualité.
   - Mise à l'échelle (haute qualité) rétrécit l'image tout en fournissant une haute qualité de graphique et de texte. L'emploi de cette option peut se traduire par plus de lenteur dans la création des images qu'avec l'option Rendu rapide.

Pour réaliser un panorama de l'image

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Dans la barre de menu du lecteur d'enregistrement de session, choisissez Lecture > Panorama et mise à l'échelle > Panorama. Le pointeur se transforme en main et une représentation de l'écran en taille réduite s'affiche dans le coin supérieur droit de la fenêtre Lecteur.
4. Faites glisser l'image. La représentation en taille réduite indique votre position dans l'image.
5. Pour interrompre le panorama, choisissez l'une des options de mise à l'échelle.

Pour afficher une bordure rouge autour de l'enregistrement de session

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Dans la barre de menus du Lecteur d'enregistrement de session, choisissez Outils > Options > Lecteur.
4. Cochez la case Afficher le pourtour de l'enregistrement de la session.
   Conseil : si la case Afficher le pourtour de l'enregistrement de la session n'est pas cochée, vous pouvez afficher la bordure rouge temporairement en cliquant et en maintenant enfoncé le bouton gauche de la souris pendant que le pointeur se trouve dans la fenêtre Lecteur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mettre en cache des fichiers de session enregistrée

Jul 07, 2016

Chaque fois que vous ouvrez un fichier de session enregistrée, le lecteur d'enregistrement de session télécharge le fichier de l'emplacement de stockage des enregistrements. Si vous téléchargez les mêmes fichiers régulièrement, vous pouvez gagner du temps en mettant les fichiers en cache sur votre station de travail. Les fichiers mis en cache sont stockés sur votre station de travail dans ce dossier :

profilutilisateur\AppData\Local\Citrix\SessionRecording\Player\Cache

Vous pouvez spécifier la quantité d'espace disque utilisée pour le cache. Lorsque les enregistrements atteignent le volume d'espace disque spécifié, l'enregistrement de session supprime les enregistrements les plus anciens et les moins utilisés pour faire de la place aux nouveaux enregistrements. Vous pouvez vider le cache à tout moment pour libérer de l'espace disque.

Pour activer la mise en cache

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Dans la barre de menus du Lecteur d'enregistrement de session, choisissez Outils > Options > Cache.
4. Cochez la case Mettre en cache les fichiers téléchargés sur la machine locale.
5. Si vous souhaitez limiter le volume d'espace disque utilisé pour la mise en cache, cochez la case Limiter le volume d'espace disque utilisable et faites glisser le curseur ou entrez le nombre de mégaoctets à utiliser pour le cache.
6. Cliquez sur OK.

Pour purger le cache

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
3. Dans la barre de menus du Lecteur d'enregistrement de session, choisissez Outils > Options > Cache.
4. Cochez la case Mettre en cache les fichiers téléchargés sur la machine locale.
5. Dans le lecteur d'enregistrement de session, choisissez Outils > Options > Cache.
6. Cliquez sur Purger le cache, puis sur OK pour confirmer l'action.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dépannage de l'enregistrement de session

Jul 07, 2016

Les informations contenues dans ce chapitre contiennent des solutions à certains problèmes éventuels que vous pourriez rencontrer pendant et après l'installation des composants de l'enregistrement de session :

- échecs de connexion entre composants ;
- échecs d'enregistrement de sessions ;
- problèmes avec le lecteur d'enregistrement de session ou la console de stratégie d'enregistrement de session ;
- problèmes avec votre protocole de communication.

L'agent d'enregistrement de session ne peut pas se connecter

Lorsque l'agent d'enregistrement de session ne peut pas se connecter, le message d'événement Détection d'exception pendant l'envoi du message d'interrogation au broker d'enregistrement de session est journalisé, suivi du texte d'exception. Le texte d'exception donne la raison de l'échec de la connexion. Ces raisons sont les suivantes :

- La connexion sous-jacente a été fermée. Impossible d'établir une relation de confiance pour le canal sécurisé SSL/TLS. Cette exception signifie que le serveur d'enregistrement de session utilise un certificat signé par une autorité de certification (CA) à laquelle le serveur sur lequel l'agent d'enregistrement de session réside ne fait pas confiance, ou n'a pas de certificat CA. Le certificat peut aussi avoir expiré ou peut avoir été révoqué.

  Résolution : vérifiez que le certificat CA correct est installé sur le serveur hébergeant l'agent d'enregistrement de session ou utilisez une CA de confiance.

- Le serveur distant a retourné une erreur : (403) interdit. Il s'agit d'une erreur HTTPS standard qui se produit lorsque vous tentez de vous connecter en utilisant HTTP (protocole non sécurisé). L'ordinateur hébergeant le serveur d'enregistrement de session rejette la connexion car il n'accepte que les connexions sécurisées.

  Résolution : utilisez la fenêtre Propriétés de l'agent d'enregistrement de session pour changer le protocole du broker d'enregistrement de session pour HTTPS.

Le broker d'enregistrement de session a renvoyé une erreur inconnue lors de l'évaluation d'une requête de stratégie d'enregistrements. Code d'erreur 5 (Accès refusé). Veuillez consulter le journal des événements sur le serveur d'enregistrement de session pour plus de détails. Cette erreur se produit lorsque les sessions démarrent et qu'une requête pour une évaluation de stratégie d'enregistrement est faite. L'erreur est le résultat de la suppression du groupe Utilisateurs authentifiés (il s'agit du membre par défaut) du rôle Requête de stratégie de la console d'autorisation d'enregistrement de session.

Résolution : ajoutez à nouveau le groupe Utilisateurs authentifiés à ce rôle ou ajoutez chaque serveur hébergeant chaque agent d'enregistrement de session au rôle PolicyQuery.

La connexion sous-jacente a été fermée. Une connexion qui devait être maintenue active a été fermée par le serveur. Cette erreur signifie que le serveur d'enregistrement de session est en panne, ou qu'il est indisponible pour accepter les requêtes. IIS est peut-être déconnecté ou a redémarré, ou le serveur entier peut être déconnecté.

Résolution : vérifiez que le serveur d'enregistrement de session a démarré, que IIS est exécuté sur le serveur et que le serveur est connecté au réseau.

Échec de l'installation des composants du serveur d'enregistrement de session

© 1999-2017 Citrix Systems, Inc. All rights reserved.

L'installation des composants du serveur d'enregistrement de session échoue avec les codes d'erreur 2503 et 2502.
Résolution :
Vérifiez la liste de contrôle d'accès (ACL) du dossier C:\windows\Temp pour vous assurer que Utilisateurs et groupes locaux ont un accès en écriture à ce dossier. Si ce n'est pas le cas, ajoutez manuellement les autorisations en écriture.

Le serveur d'enregistrement de session ne peut pas se connecter à la base de données d'enregistrement de session

Lorsque le serveur d'enregistrement de session ne peut pas se connecter à la base de données d'enregistrement de session, il est possible qu'un message similaire aux suivants s'affiche :

Source de l'événement :

Une erreur liée au réseau ou spécifique à l'instance s'est produite lors de l'établissement d'une connexion à SQL Server. Cette erreur s'affiche avec l'ID 2047 dans le journal des événements Applications de l'observateur d'événements de l'ordinateur hébergeant le serveur d'enregistrement de session.

Description Gestionnaire de stockage d'enregistrement de session Citrix : Détection d'exception pendant l'établissement de connexion à la base de données. Cette erreur s'affiche dans le journal des événements Applications de l'observateur d'événements de l'ordinateur hébergeant le serveur d'enregistrement de session.

Impossible de se connecter au serveur d'enregistrement de session. Veuillez vérifier que le serveur d'enregistrement de session fonctionne. Ce message d'erreur s'affiche lorsque vous lancez la console de stratégie d'enregistrement de session.

Résolution :

- L'édition Express de Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012 ou Microsoft SQL Server 2014 est installée sur un serveur autonome et ne possède pas les services ou paramètres appropriés configurés pour l'enregistrement de session. Sur le serveur, le protocole TCP/IP doit être activé et le service SQL Server doit fonctionner. Veuillez consulter la documentation Microsoft pour des informations sur l'activation de ces paramètres.
- Lors de l'installation de l'enregistrement de session (option Administration), des informations incorrectes ont été fournies pour le serveur et la base de données. Désinstallez la base de données d'enregistrement de session et réinstallez-la, en fournissant les informations correctes.
- Le serveur de la base de données d'enregistrement de session est en panne. Vérifiez que le serveur est connecté.
- L'ordinateur hébergeant le serveur d'enregistrement de session ou celui hébergeant le serveur de la base de données d'enregistrement de session ne peut pas résoudre le nom de domaine complet ou le nom NetBIOS de l'autre. Utilisez la commande ping pour vérifier que les noms peuvent être résolus.
- Vérifiez la configuration du pare-feu sur la base de données d'enregistrement de session pour vous assurer que les connexions du serveur SQL Server sont autorisées. Reportez-vous à l'article Microsoft : https://msdn.microsoft.com/en-us/library/cc646023.aspx.

L'ouverture de session a échoué pour l'utilisateur 'NT_AUTHORITY\ANONYMOUS LOGON'. Ce message d'erreur signifie que les services sont journalisés incorrectement en tant que .\administrator.

Résolution : redémarrez les services en tant qu'utilisateur système local et redémarrez les services SQL.

Les sessions ne sont pas enregistrées

Si l'enregistrement de vos sessions applicatives échoue, commencez par vérifier le journal d'application dans l'observateur d'événements de la machine avec OS de serveur exécutant l'agent d'enregistrement de session et le serveur

© 1999-2017 Citrix Systems, Inc. All rights reserved.

d'enregistrement de session. Il peut vous fournir des informations de diagnostic importantes.

Si les sessions ne sont pas enregistrées, les problèmes suivants peuvent en être la cause :

- **Connectivité des composants et certificats**. Si les composants d'enregistrement de session ne peuvent pas communiquer entre eux, cela peut entraîner l'échec des enregistrements de sessions. Pour résoudre les problèmes d'enregistrement, vérifiez que tous les composants sont configurés correctement de manière à pointer vers les ordinateurs corrects et que tous les certificats sont valides et installés correctement.
- **Environnements de domaine autres que Active Directory**. L'enregistrement de session est conçu pour être exécuté dans un environnement de domaine Microsoft Active Directory. Si vous n'évoluez pas dans un environnement Active Directory, vous pouvez avoir des difficultés d'enregistrement. Veillez à ce que tous les composants d'enregistrement de session sont exécutés sur des ordinateurs membres d'un domaine Active Directory.
- **Le partage de session entre en conflit avec la stratégie active.** L'enregistrement de session fait correspondre la stratégie active à la première application publiée qu'un utilisateur ouvre. Toute application suivante ouverte au cours de la même session continue d'observer la stratégie en vigueur pour la première application. Pour empêcher le partage de session d'entrer en conflit avec la stratégie active, publiez les applications en conflit sur des machines avec OS de serveur distinctes.
- **L'enregistrement n'est pas activé.** Par défaut, l'installation de l'agent d'enregistrement de session sur une machine avec OS de serveur permet d'activer le serveur pour la fonction d'enregistrement. L'enregistrement n'aura pas lieu avant qu'une stratégie d'enregistrement active soit configurée pour le permettre.
- **La stratégie d'enregistrement active n'autorise pas l'enregistrement.** Pour qu'une session soit enregistrée, la stratégie d'enregistrement active doit permettre l'enregistrement des sessions pour l'utilisateur, du serveur ou de l'application publiée.
- **Les services d'enregistrement de session ne sont pas exécutés.** Pour que les sessions soient enregistrées, le service de l'agent d'enregistrement de session doit être exécuté sur la machine avec OS de serveur et le service Gestionnaire de stockage d'enregistrement de session doit s'exécuter sur l'ordinateur hébergeant le serveur d'enregistrement de session.
- **MSMQ n'est pas configuré.** Si MSMQ n'est pas configuré correctement sur le serveur exécutant l'agent d'enregistrement de session et sur le serveur d'enregistrement de session, des problèmes d'enregistrement peuvent se produire.

Impossible d'afficher la lecture de session active

Si vous rencontrez des difficultés lors de l'affichage d'enregistrements avec le lecteur d'enregistrement de session, le message d'erreur suivant peut s'afficher à l'écran :

Échec du téléchargement du fichier de la session enregistrée. La lecture de session active n'est pas autorisée. Le serveur est configuré de manière à interdire cette fonctionnalité. Cette erreur indique que le serveur est configuré pour interdire l'action.

Résolution : dans la boîte de dialogue Propriétés du serveur d'enregistrement de session, choisissez l'onglet Lecture et cochez la case Autoriser la lecture d'une session active.

Les enregistrements sont endommagés ou incomplets

Lorsque les enregistrements sont endommagés ou incomplets lors de leur affichage à l'aide du lecteur d'enregistrement de session, vous pouvez également voir des avertissements dans les journaux d'événements de l'agent d'enregistrement de session.

Source de l'événement : Gestionnaire de stockage d'enregistrement de session Citrix

Description : perte de données lors de l'enregistrement du fichier < nom du fichier icl >

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cela se produit généralement lorsque Machine Creation Services (MCS) ou Provisioning Services est utilisé pour créer les VDA avec une image principale configurée et que Microsoft Message Queuing (MSMQ) est installé. Dans ce cas, les VDA ont les mêmes QMId pour MSMQ.

Résolution : créer une QMId unique pour chaque VDA. Une solution est présentée dans la section Problèmes connus.

Le test de connexion de l'instance de base de données a échoué lors de l'installation du composant Base de données d'enregistrement de session ou Serveur d'enregistrement de session

Lorsque vous installez la base de données d'enregistrement de session ou le serveur d'enregistrement de session, le test de la connexion échoue avec le message d'erreur **Échec du test de la connexion à la base de données. Corrigez le nom de l'instance de base de données**, et ce, même si le nom de l'instance de base de données est correct.

Résolution : vérifiez que l'utilisateur actuel dispose de l'autorisation de rôle SQL Server public pour éviter l'échec pour cause d'autorisation insuffisante.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Vérifier les connexions des composants

Jul 07, 2016

Pendant l'installation de l'enregistrement de session, il se peut que les composants ne se connectent pas à d'autres. Tous les composants communiquent avec le serveur d'enregistrement de session (broker). Par défaut, le broker (un composant IIS) est sécurisé à l'aide du certificat du site Web IIS par défaut. Si un composant ne peut pas se connecter au serveur d'enregistrement de session, il est possible que les tentatives de connexion des autres composants échouent également.

L'agent d'enregistrement de session et le serveur d'enregistrement de session (gestionnaire de stockage et broker) journalisent les erreurs de connexion dans le journal des événements des applications, dans l'observateur d'événements de l'ordinateur hébergeant le serveur d'enregistrement de session, alors que la console de stratégie d'enregistrement de session et le lecteur d'enregistrement de session affichent des messages d'erreur de connexion à l'écran lorsque les connexions échouent.

Vérifier que l'agent d'enregistrement de session est connecté

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. À partir du menu Démarrer, choisissez Propriétés de l'agent d'enregistrement de session.
3. Dans la boîte de dialogue Propriétés du serveur d'enregistrement de session, cliquez sur Connexion.
4. Vérifiez que la valeur Serveur d'enregistrement de session est le nom de serveur correct de l'ordinateur hébergeant le serveur d'enregistrement de session.
5. Vérifiez que le serveur choisi pour la valeur Serveur d'enregistrement de session peut être contacté par la machine avec OS de serveur.

Remarque : vérifiez les erreurs et avertissements éventuels dans le journal Applications.

Vérifier que le serveur d'enregistrement de session est connecté

Avertissement : l'utilisation de l'Éditeur du Registre peut entraîner de sérieux problèmes et nécessiter la réinstallation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques.

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. Ouvrez l'éditeur de registre.
3. Naviguez vers le dossier HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.
4. Vérifiez que la valeur de SmAudDatabaseInstance réfère correctement à la base de données d'enregistrement de session que vous avez installée dans votre instance SQL Server.

Vérifier que la base de données d'enregistrement de session est connectée

1. À l'aide d'un outil SQL Management, ouvrez votre instance SQL contenant la base de données d'enregistrement de session que vous avez installée.
2. Ouvrez les autorisations de sécurité de la base de données d'enregistrement de session.
3. Vérifiez que le compte d'ordinateur d'enregistrement de session a accès à la base de données. Par exemple, si l'ordinateur hébergeant le serveur d'enregistrement de session a pour nom **SsRecSrv** dans le domaine MIS, le compte d'ordinateur de votre base de données doit être configuré ainsi : MIS\SsRecSrv$. Cette valeur est configurée au cours de l'installation de la base de données d'enregistrement de session.

Tester la connectivité IIS

Tester les connexions au site IIS du serveur d'enregistrement de session avec un navigateur Web pour accéder à la page

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Web du broker d'enregistrement de session peut vous aider à déterminer si les problèmes de communication éventuels entre les composants de l'enregistrement de session proviennent d'une mauvaise configuration de protocole, de problèmes de certification ou de problèmes au niveau du broker d'enregistrement de session.

Pour vérifier la connectivité IIS avec l'agent d'enregistrement de session

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. Lancez un navigateur Web et entrez l'adresse suivante :
   - Pour HTTPS : **https://nomserveur/SessionRecordingBroker/RecordPolicy.rem?wsdl**, *nomserveur* correspondant au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
   - Pour HTTP : **http://nomserveur/SessionRecordingBroker/RecordPolicy.rem?wsdl**, *nomserveur* correspondant au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
3. Si vous êtes invité à fournir une authentification NTLM (NT LAN Manager), ouvrez une session avec un compte d'administrateur de domaine.

Si votre navigateur affiche un document au format XML, cela permet de vérifier que l'ordinateur exécutant l'agent d'enregistrement de session s'est connecté au serveur d'enregistrement de session à l'aide du protocole de configuration.

Pour vérifier la connectivité IIS avec le lecteur d'enregistrement de session

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Lancez un navigateur Web et entrez l'adresse suivante :
   - Pour HTTPS : **https://nomserveur/SessionRecordingBroker/Player.rem?wsdl**, *nomserveur* correspondant au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
   - Pour HTTP : **http://nomserveur/SessionRecordingBroker/Player.rem?wsdl**, *nomserveur* correspondant au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
3. Si vous êtes invité à fournir une authentification NTLM (NT LAN Manager), ouvrez une session avec un compte d'administrateur de domaine.

Si votre navigateur affiche un document au format XML, cela permet de vérifier que l'ordinateur exécutant le lecteur d'enregistrement de session s'est connecté au serveur d'enregistrement de session à l'aide du protocole de configuration.

Pour vérifier la connectivité IIS avec la console de stratégie d'enregistrement de session

1. Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Lancez un navigateur Web et entrez l'adresse suivante :
   - Pour HTTPS : **https://nomserveur/SessionRecordingBroker/PolicyAdministration.rem?wsdl**, *nomserveur* correspondant au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
   - Pour HTTP : **http://nomserveur/SessionRecordingBroker/PolicyAdministration.rem?wsdl**, *nomserveur* correspondant au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
3. Si vous êtes invité à fournir une authentification NTLM (NT LAN Manager), ouvrez une session avec un compte d'administrateur de domaine.

Si votre navigateur affiche un document au format XML, cela permet de vérifier que l'ordinateur exécutant la console de stratégie d'enregistrement de session s'est connecté au serveur d'enregistrement de session à l'aide du protocole de configuration.

Dépanner les problèmes de certificat

Si le protocole de communication que vous utilisez est HTTPS, l'ordinateur hébergeant le serveur d'enregistrement de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

session doit être configuré avec un certificat de serveur. Toutes les connexions de composant au serveur d'enregistrement de session doivent posséder un certificat racine d'autorité de certification (CA). Sans cela, les tentatives de connexion entre les différents composants échoueront.

Vous pouvez tester vos certificats en accédant à la page Web du broker d'enregistrement de session, de la même manière que vous le feriez pour tester la connectivité IIS. Si vous pouvez accéder à la page XML de chaque composant, cela signifie que les certificats sont configurés correctement.

Voici quelques situations courantes pour lesquelles les émissions de certificats perturbent les connexions :

- **Certificats invalides ou manquants.** Si le serveur exécutant l'agent d'enregistrement de session n'a pas de certificat racine pouvant faire confiance au certificat de serveur, il n'est pas en mesure de faire confiance et de se connecter au serveur d'enregistrement de session sur le protocole HTTPS, ce qui entraîne l'échec de la connectivité. Veuillez vérifier que tous les composants font confiance au certificat du serveur d'enregistrement de session.
- **Incohérences de noms.** Si le certificat de serveur attribué à l'ordinateur hébergeant le serveur d'enregistrement de session est créé avec un nom de domaine complet (FQDN), alors tous les composants de connexion doivent utiliser le nom complet en se connectant au serveur d'enregistrement de session. Si un nom NetBIOS est utilisé, configurez les composants avec un nom NetBIOS pour le serveur d'enregistrement de session.
- **Certificats expirés.** Si un certificat de serveur est expiré, la connectivité au serveur d'enregistrement de session via le protocole HTTPS échoue. Veuillez vérifier que le certificat de serveur attribué à l'ordinateur hébergeant le serveur d'enregistrement de session est valide et qu'il n'est pas arrivé à expiration. Si le même certificat est utilisé pour la signature numérique des enregistrements de session, le journal des événements de l'ordinateur hébergeant le serveur d'enregistrement de session produira des messages d'erreur indiquant que le certificat a expiré ou des messages d'avertissement lorsqu'il arrive à expiration.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Rechercher des enregistrements en cas d'échec du lecteur d'enregistrement de session

Jul 07, 2016

Si vous rencontrez des difficultés lors de la recherche d'enregistrements avec le lecteur d'enregistrement de session, les messages d'erreur suivants peuvent s'afficher à l'écran :

- Échec de la recherche des fichiers de session enregistrée. Le nom de serveur distant n'a pas pu être résolu : nomserveur. nomserveur étant le nom du serveur auquel le lecteur d'enregistrement de session tente de se connecter. Le lecteur d'enregistrement de session ne peut pas contacter le serveur d'enregistrement de session. Il existe deux raisons possibles : un nom de serveur tapé incorrectement ou le DNS ne peut pas résoudre le nom du serveur.
  Résolution : dans la barre de menu du lecteur, choisissez Outils > Options > Connexions et vérifiez que le nom du serveur dans la liste Serveurs d'enregistrement de session est correct. S'il est correct, exécutez la commande ping dans une invite de commande afin de vérifier s'il est possible de résoudre le nom. Lorsque le serveur d'enregistrement de session est en panne ou déconnecté, l'erreur de recherche des fichiers de session enregistrée est Impossible de contacter le serveur distant.

- Impossible de contacter le serveur distant. Cette erreur se produit lorsque le serveur d'enregistrement de session est en panne ou déconnecté.
  Résolution : vérifiez que le serveur d'enregistrement de session est connecté.

- Erreur d'accès refusé. Une erreur d'accès refusé se produit si l'utilisateur n'a pas obtenu d'autorisation de recherche et de téléchargement de fichiers de session enregistrée.
  Résolution : attribuez le rôle Lecteur à l'utilisateur à l'aide de la console d'autorisation d'enregistrement de session.

- Échec de la recherche des fichiers de session enregistrée. La connexion sous-jacente a été fermée. Impossible d'établir une relation de confiance pour le canal sécurisé SSL/TLS. Cette exception est causée par le serveur d'enregistrement de session, qui utilise un certificat signé par une CA auquel la machine cliente ne fait pas confiance ou pour lequel elle n'a pas de certificat CA.
  Résolution : installez le certificat CA correct ou de confiance sur la station de travail sur laquelle le lecteur d'enregistrement de session est installé.

- Le serveur distant a retourné une erreur : (403) interdit. Il s'agit d'une erreur HTTPS standard qui se produit lorsque vous tentez de vous connecter en utilisant HTTP (protocole non sécurisé). Le serveur rejette la connexion parce qu'il est configuré par défaut pour n'accepter que les connexions sécurisées.
  Résolution : dans la barre de menus du lecteur d'enregistrement de session, choisissez Outils > Options > Connexions. Sélectionnez le serveur dans la liste Serveurs d'enregistrement de session, puis cliquez sur Modifier. Changez le protocole de HTTP à HTTPS.

Résolution des problèmes d'MSMQ

Si vos utilisateurs peuvent voir le message de notification mais si l'utilisateur l'affichant ne peut pas trouver les enregistrements après avoir effectué une recherche dans le lecteur d'enregistrement de session, il se peut que MSMQ ait un problème. Vérifiez que la file d'attente est connectée au serveur d'enregistrement de session (gestionnaire de stockage) et qu'elle utilise un navigateur Web pour tester les connexions afin d'identifier des erreurs de connexion éventuelles (si vous utilisez HTTP ou HTTPS pour votre protocole de communication MSMQ).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour vérifier que la file d'attente est connectée :

1. Ouvrez une session sur le serveur hébergeant l'agent d'enregistrement de session et afficher les files d'attente sortantes.
2. Vérifiez que la file d'attente de l'ordinateur hébergeant le serveur d'enregistrement de session indique un état connecté.
   - Si l'état indiqué est **En attente de connexion**, un certain nombre de messages se trouvent dans la file d'attente et le protocole est HTTP ou HTTPS (selon le protocole sélectionné dans l'onglet Connexions de la boîte de dialogue Propriétés de dialogue de l'agent d'enregistrement de session), effectuez les opérations de l'étape 3.
   - Si l'état indique **connecté** et qu'aucun message ne se trouve dans la file d'attente, il peut y avoir un problème sur le serveur hébergeant le serveur d'enregistrement de session. Ignorez l'étape 3 et effectuez l'étape 4.
3. Si un certain nombre de messages se trouvent dans la file d'attente, lancez un navigateur Web et entrez l'adresse suivante :
   - Pour HTTPS : **https://nomserveur/msmq/private$/CitrixSmAudData**,*nomserveur* correspondant au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
   - Pour HTTP : **http://nomserveur/msmq/private$/CitrixSmAudData**,*nomserveur* correspondant au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.

   Si la page renvoie une erreur telle que Le serveur n'accepte que les connexions sécurisées, changez le protocole MSMQ figurant dans la liste de la boîte de dialogue Propriétés de l'agent d'enregistrement de session pour HTTPS. Autrement, si la page fait état d'un problème avec le certificat de sécurité du site Web, il se peut qu'il y ait un problème avec une relation d'approbation pour le canal sécurisé TLS. Dans ce cas, installez le certificat CA correct, ou utilisez une CA de confiance.
4. Si la file d'attente ne contient pas de message, ouvrez une session sur l'ordinateur hébergeant le serveur d'enregistrement de session et affichez les files d'attente privées. Sélectionnez citrixsmauddata. Si un certain nombre de messages se trouvent dans la file d'attente (colonne Nombre de messages), vérifiez que le service StorageManager de l'enregistrement de session a démarré. S'il ne l'est pas, redémarrez le service.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Modifier le protocole de communication

Jul 07, 2016

Pour des raisons de sécurité, Citrix déconseille d'utiliser HTTP comme protocole de communication. L'installation de l'enregistrement de session est configurée pour utiliser le mode HTTPS. Si vous souhaitez utiliser HTTP au lieu de HTTPS, vous devez modifier plusieurs paramètres.

Pour utiliser HTTP comme protocole de communication

1. Ouvrez une session sur l'ordinateur hébergeant le serveur d'enregistrement de session et désactivez les connexions sécurisées pour le broker d'enregistrement de session dans IIS.
2. Changez le paramètre du protocole de HTTPS à HTTP dans chaque boîte de dialogue Propriétés de l'agent d'enregistrement de session :
    1. ouvrez une session sur chaque serveur sur lequel l'agent d'enregistrement de session est installé.
    2. À partir du menu Démarrer, choisissez Propriétés de l'agent d'enregistrement de session.
    3. Dans la boîte de dialogue Propriétés de l'agent d'enregistrement de session, choisissez l'onglet Connexions.
    4. Dans la zone Broker d'enregistrement de session, sélectionnez HTTP dans la liste déroulante Protocole et choisissez OK pour accepter la modification. Si vous êtes invité à redémarrer le service, choisissez Oui.
3. Modifiez le paramètre du protocole de HTTPS à HTTP dans les paramètres du lecteur d'enregistrement de session :
    1. ouvrez une session sur chaque poste de travail sur lequel le lecteur d'enregistrement de session est installé.
    2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
    3. Dans la barre de menu Lecteur d'enregistrement de session, choisissez Outils > Options > Connexions, sélectionnez le serveur et choisissez Modifier.
    4. Sélectionnez HTTP dans la liste déroulante Protocole et cliquez sur OK deux fois pour accepter la modification et quitter la boîte de dialogue.
4. Modifiez le paramètre du protocole de HTTPS à HTTP dans la console de stratégie d'enregistrement de session :
    1. Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
    2. À partir du menu Démarrer, choisissez Console de stratégie d'enregistrement de session.
    3. Choisissez HTTP dans la liste déroulante Protocole et choisissez OK pour vous connecter. Si la connexion est établie, ce paramètre est mémorisé lorsque vous lancez la console de stratégie d'enregistrement de session la fois suivante.

Pour rétablir HTTPS en tant que protocole de communication

1. Ouvrez une session sur l'ordinateur hébergeant le serveur d'enregistrement de session et activez les connexions sécurisées pour le broker d'enregistrement de session dans IIS.
2. Changez le paramètre du protocole de HTTP à HTTPS dans chaque boîte de dialogue Propriétés de l'agent d'enregistrement de session :
    1. ouvrez une session sur chaque serveur sur lequel l'agent d'enregistrement de session est installé.
    2. À partir du menu Démarrer, choisissez Propriétés de l'agent d'enregistrement de session.
    3. Dans la boîte de dialogue **Propriétés de l'agent d'enregistrement de session**, choisissez l'onglet Connexions.
    4. dans la zone Broker d'enregistrement de session, sélectionnez HTTPS dans la liste déroulante Protocole et choisissez OK pour accepter la modification. Si vous êtes invité à redémarrer le service, choisissez Oui.
3. Modifiez le paramètre du protocole de HTTP à HTTPS dans les paramètres du lecteur d'enregistrement de session :
    1. ouvrez une session sur chaque poste de travail sur lequel le lecteur d'enregistrement de session est installé.
    2. À partir du menu Démarrer, choisissez Lecteur d'enregistrement de session.
    3. Dans la barre de menu Lecteur d'enregistrement de session, choisissez Outils > Options > Connexions, sélectionnez le serveur et choisissez Modifier.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. Sélectionnez HTTPS dans la liste déroulante Protocole et cliquez sur OK deux fois pour accepter la modification et quitter la boîte de dialogue.

4. Modifiez le paramètre du protocole de HTTP à HTTPS dans la console de stratégie d'enregistrement de session :
    1. Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
    2. À partir du menu Démarrer, choisissez Console de stratégie d'enregistrement de session.
    3. Choisissez HTTPS dans la liste déroulante Protocole et choisissez OK pour vous connecter. Si la connexion est établie, ce paramètre est mémorisé lorsque vous lancez la console de stratégie d'enregistrement de session la fois suivante.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Référence : gérer vos enregistrements de base de données

Jul 07, 2016

L'utilitaire de base de données de journalisation ICA (ICLDB) est un utilitaire de ligne de commande pour base de données utilisé pour la manipulation des éléments de base de données constitués d'enregistrements de sessions. Cet utilitaire est installé en même temps que l'enregistrement de session dans le répertoire du lecteur:\Program Files\Citrix\SessionRecording\Server\Bin du serveur hébergeant le logiciel Serveur d'enregistrement de session.

Tableau de référence rapide

Le tableau suivant contient la liste des commandes et des options disponibles avec l'utilitaire ICLDB. Tapez les commandes en utilisant le format suivant :

icldb [version | locate | dormant | import | archive | remove | removeall] command-options [/l] [/f] [/s] [/?]

Remarque : des instructions plus approfondies se trouvent dans l'aide de l'utilitaire. Pour y accéder à partir d'une ligne de commande, tapez **icldb /?** dans le répertoire drive:**\Program Files\Citrix\SessionRecording\Server\Bin** . Pour accéder à l'aide de commandes spécifiques, tapez **icldb** ***command*** **/?**.

Commande	Description
archive	Permet d'archiver les fichiers d'enregistrement de session plus anciens que la période de rétention spécifiée. Utilisez cette commande pour archiver les fichiers.
dormant	Cette commande permet d'afficher ou de compter les fichiers d'enregistrement de session considérés comme dormants. Les fichiers dormants sont des enregistrements de session incomplets en raison d'une perte de données. Utilisez cette commande pour vérifier si vous suspectez une perte de données. Vous pouvez vérifier si les fichiers d'enregistrement de session deviennent dormants pour l'intégralité de la base de données ou si s'il ne s'agit que des enregistrements effectués pendant un certain nombre de jours, d'heures ou de minutes.
import	Permet d'importer les fichiers d'enregistrement de session dans la base de données d'enregistrement de session. Utilisez la commande pour reconstituer la base de données si vous perdez les enregistrements de la base de données. Vous pouvez également utiliser la commande pour fusionner des bases de données (si vous avez deux bases de données, vous pouvez importer les fichiers de l'une des bases de données).
locate	Permet de localiser et d'afficher le chemin complet vers un fichier d'enregistrement de session en utilisant l'identificateur de fichier comme critère.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Commande	Description
	Utilisez cette commande lorsque vous cherchez l'emplacement d'un fichier d'enregistrement de session. Il s'agit aussi d'une manière de vérifier si la base de données est à jour par rapport à un fichier spécifique.
remove	Permet de supprimer les références à des fichiers d'enregistrement de session de la base de données. Utilisez cette commande (prudemment) pour nettoyer la base de données. Spécifiez la période de rétention à utiliser comme critères. Vous pouvez également supprimer le fichier physique associé.
removeall	Cette commande supprime toutes les références aux fichiers d'enregistrement de session de la base de données d'enregistrement de session et rétablit l'état d'origine de la base de données. Les fichiers physiques ne sont pas supprimés ; il est toutefois impossible de les rechercher dans le lecteur d'enregistrement de session. Utilisez cette commande (prudemment) pour nettoyer la base de données. Les références supprimées ne peuvent être rétablies qu'en effectuant une restauration à partir des fichiers de sauvegarde.
version	Cette commande permet d'afficher la version du schéma de la base de données d'enregistrement de session.
/l	Cette commande enregistre les résultats et les erreurs dans le journal des événements Windows.
/f	Cette commande force l'exécution de la commande sans invites.
/s	Cette commande supprime le message de copyright.
/?	Cette commande affiche l'aide des commandes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Avis de tiers

Jul 07, 2016

L'enregistrement de session peut inclure des composants de logiciel tiers fournis sous licence selon les conditions suivantes. Cette liste a été générée à l'aide d'un logiciel tiers à la date indiquée dans la liste. Cette liste peut changer en fonction des versions du produit et ne peut ne pas être complète ; elle est fournie « telle quelle ». DANS LA LIMITE AUTORISÉE PAR LA LOI APPLICABLE, CITRIX ET SES FOURNISSEURS N'OFFRENT AUCUNE REPRÉSENTATION OU GARANTIE, EXPRESSE OU TACITE, LÉGALE OU AUTRE, CONCERNANT LA LISTE, SA PRÉCISION OU SON EXHAUSTIVITÉ, OU CONCERNANT TOUT RÉSULTAT DÉCOULANT DE L'UTILISATION OU DE LA DISTRIBUTION DE LA LISTE. EN UTILISANT OU DISTRIBUANT LA LISTE, VOUS CONVENEZ QU'EN AUCUN CAS CITRIX NE POURRA ÊTRE TENU RESPONSABLE DE TOUT DOMMAGE SPÉCIAL, DIRECT, INDIRECT OU ACCESSOIRE OU TOUT AUTRE DOMMAGE RÉSULTANT DE L'UTILISATION OU DE LA DISTRIBUTION DE CETTE LISTE.

Bibliothèque MMC .NET

Sous licence selon les termes de la Common Public License, version 1.0

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Journalisation de la configuration

Jul 07, 2016

La journalisation de la configuration capture les modifications apportées à la configuration du site et les activités administratives effectuées sur la base de données. Vous pouvez utiliser le contenu consigné pour :

- diagnostiquer et résoudre les problèmes après que des modifications sont apportées à la configuration ; le journal fournit une arborescence hiérarchique ;
- assister la gestion des modifications et suivre les configurations ;
- signaler les activités administratives.

Vous définissez les préférences de journalisation de la configuration, afficher les journaux de configuration et générer des rapports HTML et CSV à partir de Citrix Studio. Vous pouvez filtrer les affichages des journaux de configuration par plages de dates et selon les résultats de recherche en texte intégral. La journalisation obligatoire, lorsqu'elle est activée, empêche les modifications de la configuration à moins qu'elles puissent être journalisées. Avec des autorisations appropriées, vous pouvez supprimer des entrées dans le journal de configuration. Vous ne pouvez pas utiliser la fonction de journalisation de la configuration pour modifier le contenu du journal.

La journalisation de la configuration utilise un SDK PowerShell 2.0 et le service de journalisation de la configuration. Le service de journalisation de la configuration s'exécute sur chaque Controller dans le site ; si un Controller échoue, le service sur un autre Controller traite automatiquement les demandes de journalisation.

Par défaut, la fonction de journalisation de la configuration est activée, et utilise la base de données qui est créée lorsque vous créez le site (la base de données de configuration de site). Citrix vous recommande de modifier l'emplacement de la base de données utilisée pour la journalisation de la configuration dès que possible après la création d'un site. La base de données de journalisation de la configuration prend en charge les mêmes fonctions haute disponibilité que la base de données de configuration de site.

L'accès à la journalisation de la configuration est contrôlé via l'administration déléguée, avec les autorisations Modifier les préférences de journalisation et Afficher les journaux de configuration.

Les journaux de configuration sont localisés lorsqu'ils sont créés. Par exemple, un journal créé en anglais sera lue en anglais, quels que soient les paramètres régionaux du lecteur.

Qu'est-ce qui est journalisé ?

Les modifications de configuration et les activités administratives initiées depuis Studio, Director et des scripts PowerShell sont journalisées. Les exemples de modifications apportées à la configuration journalisées comprennent l'utilisation de (création, modification, suppression des affectations) :

- Catalogues de machines
- Groupes de mise à disposition (y compris la modification des paramètres de gestion de la puissance)
- Rôles et étendues de l'administrateur
- Ressources et connexions de l'hôte
- Stratégies Citrix au travers de Studio

Exemples de modifications administratives journalisées :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Gestion de la puissance d'une machine virtuelle ou d'un bureau utilisateur
- Envoi d'un message à un utilisateur par Studio ou Director

Les opérations suivantes ne sont pas enregistrées :

- Opérations autonomes telles que la mise sous tension de la gestion du pool de machines virtuelles.
- Actions de stratégie implémentées au travers de la console de gestion des stratégies de groupe (GPMC) ; utilisez les outils Microsoft pour afficher des journaux de ces actions.
- Les modifications effectuées via le Registre, accès direct à la base de données, ou à partir de sources autres que Studio, Director ou PowerShell.
- Lorsque le déploiement est initialisé, la journalisation de la configuration est disponible lorsque la première instance du service de journalisation de la configuration s'enregistre auprès du service de configuration. Par conséquent, les premières étapes de configuration ne sont pas journalisées (par exemple, lorsque le schéma de base de données est obtenu et appliqué, lors de l'initialisation d'un hyperviseur).

Gérer la journalisation de la configuration

Par défaut, la journalisation de la configuration utilise la base de données qui est créée lorsque vous créez un site (également connu sous le nom de base de données de configuration de site). Citrix vous recommande d'utiliser un autre emplacement pour la base de données de journalisation de configuration (et la base de données de surveillance) pour les raisons suivantes :

- La stratégie de sauvegarde de la base de données de journalisation de la configuration est susceptible d'être différente de celle de la stratégie de sauvegarde de la base de données de configuration de site.
- Le volume de données collectées pour la journalisation de la configuration (et le service de surveillance) peut avoir un impact négatif sur l'espace disponible pour la base de données de configuration de site.
- Elle partage le point de défaillance unique pour les trois des bases de données.

Remarque : les éditions de produit qui ne prennent pas en charge la journalisation de la configuration ne disposent pas d'un nœud Journalisation dans Studio.

Activer/désactiver la journalisation de la configuration et la journalisation obligatoire

Par défaut, la journalisation de la configuration est activée et la journalisation obligatoire est désactivée.

1. Sélectionnez **Journalisation** dans le volet de navigation Studio.
2. Sélectionnez **Préférences** dans le volet Actions. La boîte de dialogue Journalisation de la configuration contient des informations de base de données et indique si la journalisation de la configuration et la journalisation obligatoire sont activées ou désactivées.
3. Sélectionnez l'action souhaitée :

   Pour activer la journalisation de la configuration, sélectionnez le bouton radio **Activer la journalisation**. C'est le réglage par défaut. S'il est impossible d'écrire sur la base de données, les informations de journalisation sont ignorées, mais l'opération se poursuit.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour désactiver la journalisation de la configuration, sélectionnez le bouton radio **Désactiver la journalisation**. Si la journalisation était préalablement activée, les journaux existants restent lisibles avec le SDK PowerShell.

Pour activer la journalisation obligatoire, décochez la case **Autoriser les modifications lorsque la base de données est déconnectée**. Aucune modification de la configuration ou activité administrative ne sera enregistrée (contrairement à la normale) à moins qu'elle puisse être écrite dans la base de données de journalisation de la configuration. Vous pouvez activer la journalisation obligatoire uniquement lorsque la journalisation de la configuration est activée, c'est-à-dire lorsque le bouton radio **Activer la journalisation de la configuration** est sélectionné. Si le service de journalisation de la configuration échoue, et que la haute disponibilité n'est pas utilisée, la journalisation obligatoire est utilisée. Dans de tels cas, les opérations qui seraient normalement enregistrées ne le sont pas.

Pour désactiver la journalisation obligatoire, cochez la case **Autoriser les modifications lorsque la base de données est déconnectée**. Les modifications de configuration et les activités administratives sont autorisées, même si la base de données utilisée pour la journalisation de la configuration est inaccessible. C'est le réglage par défaut.

Pour modifier l'emplacement de la base de données de journalisation de la configuration

Remarque : vous ne pouvez pas modifier l'emplacement de la base de données lorsque la journalisation obligatoire est activée, car la modification de l'emplacement inclut un bref intervalle qui ne peut pas être enregistré.

1. Créez un serveur de base de données, à l'aide d'une version SQL Server prise en charge.
2. Sélectionnez **Journalisation** dans le volet de navigation Studio.
3. Sélectionnez **Préférences** dans le volet Actions.
4. Dans la boîte de dialogue Préférences de journalisation, sélectionnez **Modifier la base de données de journalisation**.
5. Dans la boîte de dialogue Changer la base de données de journalisation, spécifiez l'emplacement du serveur contenant le nouveau serveur de base de données. Les formats valides sont répertoriés dans l'article Bases de données.
6. Pour autoriser Studio pour créer la base de données, cliquez sur **OK**. Lorsque vous y êtes invité, cliquez sur **OK** et la base de données sera créée automatiquement. Studio tente d'accéder à la base de données à l'aide des informations d'identification de l'utilisateur de Studio ; si la tentative échoue, vous êtes invité à entrer les informations d'identification de l'utilisateur de la base de données. Studio télécharge ensuite le schéma de base de données vers la base de données. (Les informations d'identification ne sont conservées que lors de la création de la base de données.)
7. Pour créer la base de données manuellement, cliquez sur **Générer script de base de données**. Le script généré comprend des instructions pour la création manuelle de la base de données. Assurez-vous que la base de données est vide et qu'au moins un utilisateur est autorisé à accéder et modifier la base de données avant le chargement du schéma.

Les données journalisation de la configuration ne sont pas importées vers la nouvelle base de données. Les journaux ne peuvent pas être regroupés pour les deux bases de données lors de la récupération des journaux. La première entrée du journal dans la nouvelle base de données de journalisation de la configuration indique qu'une modification a été apportée dans une base de données, mais elle n'identifie pas la base de données précédente.

Afficher le contenu du journal de configuration

Lorsque vous effectuez des modifications de configuration et des activités administratives, les opérations de haut niveau créées par Studio et Director sont affichées dans la partie supérieure du panneau central dans Studio. Une opération

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de haut niveau se traduit par un ou plusieurs appels de service et de SDK, qui sont des opérations de bas niveau. Lorsque vous sélectionnez une opération de haut niveau dans le panneau supérieur du milieu, le panneau inférieur central affiche les opérations de bas niveau.

Si une opération échoue avant la fin de l'opération, l'opération de journalisation peut ne pas être effectuée dans la base de données ; par exemple, un enregistrement de début n'aura pas d'enregistrement de fin correspondant. Dans de tels cas, le journal indique qu'il manque des informations. Lorsque vous affichez les journaux basés en fonction de plages de temps, les journaux incomplets sont affichés si les données dans les journaux correspondent aux critères. Par exemple, si tous les journaux des cinq derniers jours sont demandés et qu'un journal existe avec une heure de début dans les cinq derniers jours, mais sans date de fin, il est inclus.

Lors de l'utilisation d'un script pour appeler des applets de commande PowerShell, si vous créez une opération de bas niveau sans spécifier une opération de haut niveau parente, la journalisation de la configuration va créer une opération de haut niveau de substitution.

Pour afficher le contenu du journal de configuration, sélectionnez **Journalisation** dans le panneau de navigation. Par défaut, l'affichage dans le panneau central affiche le contenu du journal par ordre chronologique (la plus récente des entrées en premier), en les séparant par date.

Pour filtrer l'affichage par	Effectuez cette action
Résultats de la recherche	Entrez le texte dans la zone Rechercher en haut du panneau central. L'affichage filtré inclut le nombre de résultats de la recherche. Pour revenir à l'affichage de la journalisation standard, désactivez le texte dans la zone Rechercher.
En-tête de la colonne	Cliquez sur un en-tête de colonne pour trier l'affichage par ce champ.
Une plage de dates	Sélectionnez un intervalle dans la zone de liste déroulante en regard de la zone Rechercher en haut du panneau central.

Générer des rapports

Vous pouvez générer des rapports au format CSV et HTML contenant les données du journal de la configuration.

- Le rapport CSV contient toutes les données de journalisation à partir d'un intervalle de temps spécifié. La hiérarchie des données dans la base de données est aplatie dans un seul tableau CSV. Aucun aspect des données n'a la priorité dans le fichier. Aucune mise en forme n'est utilisée, les données sont donc inintelligibles. Le fichier (appelé sur MyReport) contient les données dans un format lisible. Les fichiers CSV sont souvent utilisés pour l'archivage des données ou en tant que source de données pour un outil de création de rapports ou de manipulation de données tel que Microsoft Excel.
- Le rapport HTML fournit un formulaire lisible des données de journalisation pour un intervalle de temps spécifié. Il fournit une vue structurée et navigable pour la vérification des modifications. Un rapport HTML se compose de deux fichiers appelés Résumé et Détails. Le fichier Résumé répertorie les opérations de haut niveau : moment auquel chaque opération se produit, personne qui réalise l'opération et le résultat. Si vous cliquez sur un lien Détails en regard de chaque

© 1999-2017 Citrix Systems, Inc. All rights reserved.

opération, vous êtes amené aux opérations de bas niveau dans le fichier Détails, qui fournit des informations supplémentaires.

Pour générer un rapport du journal de configuration, sélectionnez **Journalisation** dans le panneau de navigation de Studio, puis sélectionnez **Créer un rapport personnalisé** dans le volet Actions.

- Sélectionnez la plage de dates pour le rapport.
- Sélectionnez le format du rapport : CSV, HTML ou les deux.
- Naviguez jusqu'à l'emplacement où le rapport doit être enregistré.

Supprimer le contenu du journal de configuration

Pour supprimer le journal de configuration, vous devez posséder certaines permissions d'administration déléguée et de base de données SQL Server.

- **Administration déléguée** : vous devez disposer d'un rôle Administration déléguée qui permet la lecture de la configuration du déploiement. Le rôle d'administrateur complet intégré dispose de cette autorisation. Les options En lecture seule ou Gérer doivent être sélectionnées dans la catégorie Autres permissions pour un rôle personnalisé.
  Pour créer une copie de sauvegarde des données de journalisation de la configuration avant de les supprimer, les options En lecture seule ou Gérer doivent également être sélectionnées dans la catégorie Permissions de journalisation pour le rôle personnalisé.

- **Base de données SQL Server** : vous devez disposer d'une connexion au serveur SQL avec la permission de supprimer des enregistrements de la base de données. Il existe deux façons de procéder :
  - Utiliser une connexion à une base de données SQL Server avec un rôle de serveur sysadmin, ce qui vous permet d'effectuer toute activité sur le serveur de base de données. Les rôles de serveur serveradmin ou setupadmin vous permettent d'effectuer des opérations de suppression.
  - Si votre déploiement requiert une sécurité supplémentaire, utilisez une connexion de base de données non-sysadmin mappée sur un utilisateur de base de données qui est autorisé à supprimer des enregistrements de la base de données.
    1. Dans SQL Server Management Studio, créez une connexion SQL Server avec un rôle de serveur autre que « sysadmin ».
    2. Mappez la connexion sur un utilisateur dans la base de données ; SQL Server crée automatiquement un utilisateur dans la base de données avec le même nom que la connexion.
    3. Dans l'appartenance au rôle de base de données, spécifiez au moins un des membres de rôle pour la base de données utilisateur : ConfigurationLoggingSchema_ROLE ou dbowner.

    Pour de plus amples informations, consultez la documentation de SQL Server Management Studio.

Pour supprimer les journaux de configuration :

1. Sélectionnez **Journalisation** dans le volet de navigation Studio.
2. Sélectionnez **Supprimer les journaux** dans le volet Actions.
3. Vous êtes invité à indiquer si vous voulez créer une sauvegarde des journaux avant de les supprimer. Si vous choisissez de créer une copie de sauvegarde, naviguez jusqu'à l'emplacement où l'archive de sauvegarde doit être enregistrée. La sauvegarde va être créée en tant que fichier CSV.

Une fois les journaux de configuration effacés, la suppression du journal est la première activité consignée dans le journal vide. Cette entrée fournit des informations sur la personne qui a supprimé les journaux et la date à laquelle ils ont été supprimés.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Surveiller les Personal vDisks

Jul 07, 2016

Vous pouvez utiliser un outil de diagnostic pour surveiller les modifications effectuées par les utilisateurs pour les deux parties de leurs Personal vDisks (les données de l'utilisateur et l'application). Ces modifications incluent les applications que les utilisateurs ont installé et les fichiers qu'ils ont modifié. Les modifications sont stockées dans un ensemble de rapports.

1. Sur la machine que vous voulez surveiller, exécutez **C:\Program Files\Citrix\personal vDisk\bin\CtxPvdDiag.exe**.
2. Recherchez un emplacement où vous souhaitez stocker les rapports et les journaux, sélectionnez les rapports à générer, et cliquez sur **OK.** Les rapports disponibles sont répertoriés ci-dessous.

Rapport de la ruche de logiciels : ce rapport génère deux fichiers : Software.Dat.Report.txt et Software.Dat.delta.txt. Le fichier Software.Dat.Report.txt enregistre les modifications effectuées par l'utilisateur dans la ruche HKEY_LOCAL_MACHINE\Software. Il contient les sections suivantes :

- Liste des applications installées sur la base : les applications qui ont été installées dans Layer 0.
- Liste des logiciels installés par l'utilisateur : les applications installées par l'utilisateur sur la partie de l'application du vDisk personnel.
- Liste de logiciels désinstallés par l'utilisateur : les applications supprimées par l'utilisateur qui étaient présentes à l'origine dans Layer 0.

Voir le rapport delta de la ruche pour de plus amples informations sur Software.Dat.delta.txt.

Rapport de la ruche système : le fichier SYSTEM.CurrentControlSet.DAT.Report.txt généré enregistre les modifications apportées à la ruche HKEY_LOCAL_MACHINE\System par l'utilisateur. Il contient les sections suivantes :

- Liste des services installés par l'utilisateur : les services et les pilotes installés par l'utilisateur.
- Le démarrage des services suivants a été modifié : les services et les pilotes dont le type de démarrage a été modifié par l'utilisateur.

Rapport de la ruche de sécurité : le fichier SECURITY.DAT.Report.txt généré surveille toutes les modifications que l'utilisateur effectue dans la ruche HKEY_LOCAL_MACHINE\Security.

Rapport de ruche du gestionnaire de comptes de sécurité (SAM) : le fichier SAM.DAT.Report.txt généré surveille toutes les modifications que l'utilisateur effectue dans la ruche HKEY_LOCAL_MACHINE\SAM.

Rapport delta de la ruche : le fichier Software.Dat.delta.txt généré enregistre toutes les clés de Registre et les valeurs ajoutées ou supprimées, et toutes les valeurs modifiées par l'utilisateur dans la ruche HKEY_LOCAL_MACHINE\Software.

Journal Personal vDisk : les fichiers journaux Pud-IvmSupervisor.log, PvDActivation.log, PvDSvc.log, PvDWMI.log, SysVol-IvmSupervisor.log et vDeskService-<#>.log sont générés par défaut dans P:\Users\\AppData\Local\Temp\PVDLOGS, mais sont déplacés vers l'emplacement sélectionné.

Journaux du système d'exploitation Windows

- EvtLog_App.xml et EvtLog_System.xml sont les journaux d'événements application et système au format XML du format Personal vDisk.
- Setupapi.app.log et setuperr.log contiennent des messages de journal de msiexec.exe qui était exécuté pendant l'installation de Personal vDisk.
- Setupapi.dev.log contient des messages de journal d'installation du périphérique.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Msinfo.txt contient la sortie de msinfo32.exe. Pour de plus amples informations, veuillez consulter la documentation Microsoft.

Rapport du système de fichiers : le fichier FileSystemReport.txt généré enregistre les modifications effectuées par l'utilisateur pour le système de fichiers dans les sections suivantes :

- Fichiers déplacés : les fichiers dans Layer 0 qui ont été déplacés par l'utilisateur vers le vDisk. Les fichiers Layer 0 sont hérités de l'image principale par la machine à laquelle le Personal vDisk est connecté.
- Fichiers supprimés : les fichiers dans Layer 0 qui ont été masqués par une action de l'utilisateur (par exemple, la suppression d'une application).
- Fichiers ajoutés (MOF, INF, SYS) : les fichiers qui possèdent des extensions .mof, .inf ou .sys que l'utilisateur a ajouté au Personal vDisk (par exemple, lorsqu'ils installé une application telle que Visual Studio 2010 qui enregistre un fichier .mof pour la récupération automatique).
- Fichiers ajoutés (autres) : autres fichiers que l'utilisateur a ajouté au vDisk (par exemple, lors de l'installation d'une application).
- Fichiers de base modifiés mais pas déplacés : les fichiers dans Layer 0 que l'utilisateur a modifié mais que les pilotes Personal vDisk en mode Kernel n'ont pas capturé dans le vDisk.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Director

Aug 22, 2016

Dans cet article :

À propos de Director

Déployer et configurer Director

Installer Director

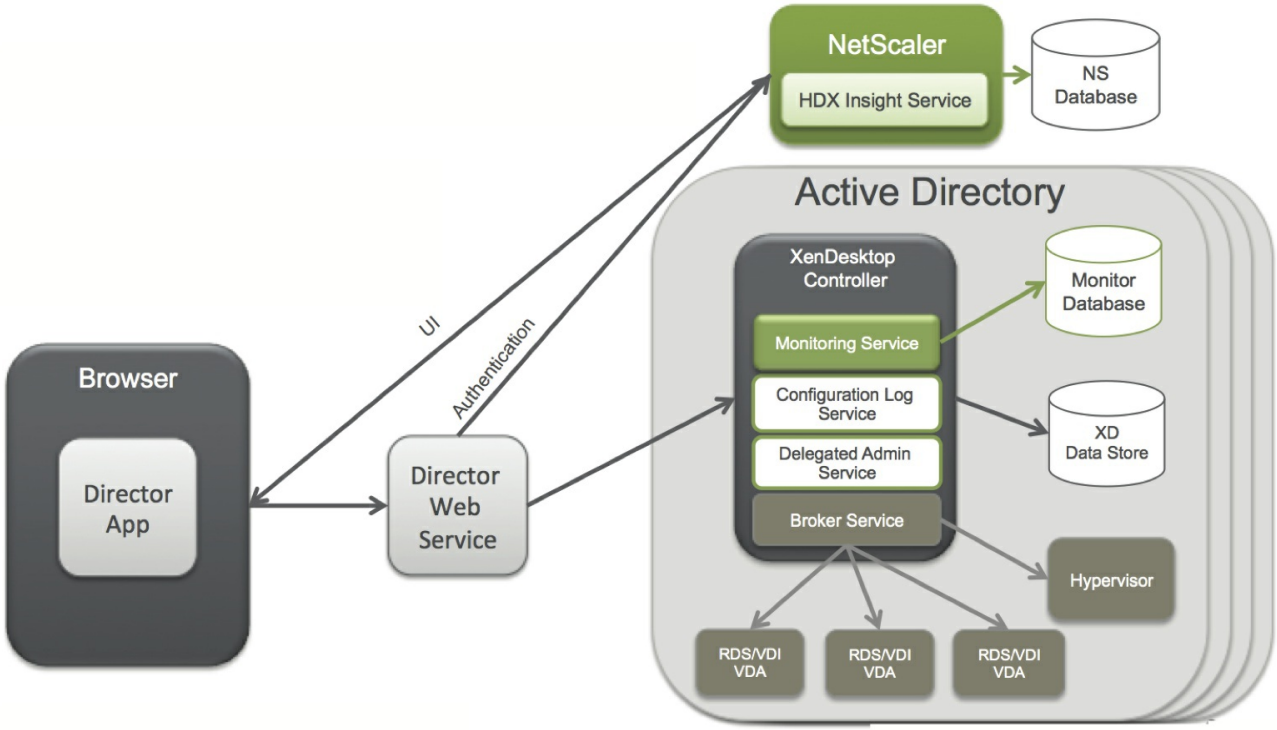
Installer Director pour XenApp 6.5

Ouvrir une session sur Director

Utiliser Director avec l'authentification Windows intégrée

À propos de Director

Director est un outil Web en temps réel qui permet aux administrateurs d'effectuer la surveillance et la résolution des problèmes, et de réaliser des tâches d'assistance pour les utilisateurs finaux.



Director peut accéder :

- Aux données en temps réel à partir de l'agent Broker à l'aide d'une console unifiée, intégrée à Analytics, Performance Manager et Network Inspector.
  - Analytics comprend la gestion des performances pour l'assurance de l'intégrité et de la capacité et les tendances historiques et l'analyse réseau, optimisées par NetScaler HDX Insight, pour identifier les goulots d'étranglement dus au réseau dans votre environnement XenApp ou XenDesktop.
- Aux données d'historiques stockées dans la base de données Monitor pour accéder à la base de données de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

journalisation de la configuration.

- Aux données ICA provenant de NetScaler Gateway à l'aide de HDX Insight.
  - À la visibilité du gain dans l'expérience des utilisateurs pour les applications et les bureaux virtuels, et les utilisateurs pour XenApp ou XenDesktop.
  - Effectuez une corrélation des données réseau avec les données d'application et les mesures en temps réel pour une résolution des problèmes effective.
  - Intégration à l'outil d'analyse XenDesktop 7 Director.
- Les données Personal vDisk qui offrent une surveillance au moment de l'exécution des données affichent une allocation de base et donnent au bureau d'assistance la possibilité de réinitialiser le Personal vDisk (pour n'être utilisé qu'en dernier recours).
  - L'outil de ligne de commande de CtxPvdDiag.exe est utilisé pour collecter les informations de journalisation dans un fichier pour la résolution des problèmes.

Director utilise un tableau de bord de résolution des problèmes qui offre un contrôle d'intégrité en temps réel du site XenApp ou XenDesktop. Cette fonctionnalité permet aux administrateurs d'afficher des erreurs en temps réel, offrant ainsi une meilleure idée de ce dont l'utilisateur fait l'expérience.

Vues de l'interface

Director offre différentes vues de l'interface adaptées aux administrateurs particuliers. Les permissions du produit déterminent ce qui est affiché et les commandes disponibles.

Par exemple, les administrateurs du bureau d'assistance voient une interface adaptée aux tâches du personnel d'assistance technique. Director permet aux administrateurs du bureau d'assistance de rechercher l'utilisateur signalant un problème et afficher les activités associées à cet utilisateur, tels que l'état des applications et des processus de l'utilisateur. Ils peuvent résoudre des problèmes rapidement en effectuant des actions telles que la fermeture d'une application ou d'un processus qui ne répond pas, l'observation d'opérations sur la machine de l'utilisateur, le redémarrage de la machine ou la réinitialisation du profil utilisateur.

Inversement, les administrateurs complets peuvent voir et gérer l'ensemble du site et peuvent réaliser des commandes pour plusieurs utilisateurs et machines. Le tableau de bord fournit une vue d'ensemble des aspects clés d'un déploiement, tel que l'état des sessions, les ouvertures de session des utilisateurs et l'infrastructure d'un site. Les informations sont mises à jour toutes les minutes. Si des problèmes surviennent, des détails apparaissent automatiquement sur le nombre et le type d'échec.

Déployer et configurer Director

Director est installé par défaut en tant que site Web sur le Delivery Controller. Pour les composants pré-requis et d'autres détails, consultez la documentation relative à la configuration système requise pour cette version.

Cette version de Director n'est pas compatible avec les déploiements XenApp antérieurs à la version 6.5 ou les déploiements XenDesktop antérieurs à la version 7.

Lorsque Director est utilisé dans un environnement contenant plus d'un site, assurez-vous de synchroniser les horloges du système sur tous les serveurs sur lesquels les Controller, Director et autres composants principaux sont installés. Sinon, il se peut que les sites ne s'affichent pas correctement dans Director.

Conseil : si vous souhaitez surveiller les sites XenApp 6.5 en plus des sites XenApp 7.5 ou XenDesktop 7.x, Citrix vous recommande d'installer Director sur un autre serveur depuis la console Director qui est utilisée pour surveiller les sites XenApp 6.5.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Important : pour protéger la sécurité des noms d'utilisateur et des mots de passe envoyés en texte brut via le réseau, Citrix recommande vivement d'autoriser les connexions Director utilisant uniquement HTTPS, et non pas HTTP. Certains des outils destinés à lire le texte brut des noms d'utilisateur et des mots de passe dans des paquets réseau HTTP (non cryptés), ce qui crée un risque de sécurité pour les utilisateurs.

Pour configurer des permissions

Pour ouvrir une session sur Director, les administrateurs disposant de permissions pour Director doivent être des utilisateurs de domaine Active Directory et disposer des droits suivants :

- Droits de lecture dans toutes les forêts Active Directory à parcourir (voir Configuration avancée).
- Les rôles d'administrateur délégué configuré (voir Administration déléguée et Director).
- Pour observer les utilisateurs, les administrateurs doivent être configurés à l'aide d'une stratégie de groupe Microsoft pour l'Assistance à distance Windows. De plus :
  - Lors de l'installation de VDA, assurez-vous que la fonction Assistance à distance de Windows est activée sur toutes les machines utilisateur (sélectionnée par défaut).
  - Lorsque vous installez Director sur un serveur, assurez-vous que l'Assistance à distance est installée (sélectionnée par défaut). Toutefois, elle est désactivée sur le serveur par défaut. La fonction ne doit pas être activée pour Director pour obtenir de l'aide auprès des utilisateurs. Citrix vous recommande de laisser la fonctionnalité désactivée pour améliorer la sécurité sur le serveur.
  - Pour permettre aux administrateurs d'initier l'assistance à distance Windows, vous devez leur attribuer les permissions nécessaires à l'aide des paramètres de stratégie de groupe Microsoft correspondants pour l'assistance à distance. Pour plus d'informations, reportez-vous à l'article CTX127388 : Comment activer l'assistance à distance pour Desktop Director (How to Enable Remote Assistance for Desktop Director).
- Pour les machines utilisateur avec VDA antérieure à 7, une configuration supplémentaire est requise. Voir Configurer les permissions pour VDA antérieurs à XenDesktop 7.

Installer Director

Installez Director à l'aide du programme d'installation du produit complet pour XenApp et Desktop, qui vérifie la présence de composants pré-requis, installe les composants manquants, configure le site Web Director et effectue la configuration de base. La configuration par défaut fournie par le programme d'installation convient aux déploiements classiques. Si Director n'a pas été inclus au cours de l'installation, utilisez le programme d'installation pour ajouter Director. Pour ajouter des composants supplémentaires, réexécutez le programme d'installation et sélectionnez les composants à installer. Pour de plus amples informations sur l'utilisation du programme d'installation, consultez la section Installer à l'aide de l'interface graphique dans la documentation relative à l'installation. Citrix vous recommande d'effectuer l'installation à l'aide du programme d'installation du produit uniquement, et non pas le fichier MSI.

Lorsque Director est installé sur le Controller, il est automatiquement configuré avec localhost comme adresse de serveur, et Director communique avec le Controller local par défaut.

Pour installer Director sur un serveur dédié qui est distant par rapport à un Controller, vous êtes invité à entrer l'adresse FQDN ou IP d'un Controller. Par défaut, Director communique avec ce Controller spécifié. Spécifiez une seule adresse de Controller pour chaque site que vous allez surveiller. Director découvre automatiquement tous les autres Controller du même site et retourne vers ces Controller en cas d'échec du Controller spécifié.

Remarque : Director n'équilibre pas les charges entre les Controller.

Pour sécuriser les communications entre le navigateur et le serveur Web, Citrix recommande de mettre en œuvre TLS sur le site Web IIS qui héberge Director. Pour plus d'informations, reportez-vous à la documentation de Microsoft IIS. La

© 1999-2017 Citrix Systems, Inc. All rights reserved.

configuration Director n'est pas requise pour activer TLS.

Installer Director pour XenApp 6.5

Pour installer Director pour XenApp 6.5, procédez comme suit : En général, Desktop Director est installé sur un ordinateur autre que celui utilisé pour les Controller XenApp.

1. Installez Director à partir du support d'installation de XenApp. Si Director est déjà installé pour XenDesktop, ignorez cette étape et passez à l'étape suivante.
2. Utilisez la console Gestionnaire des services Internet (IIS) sur chaque serveur Director pour mettre à jour la liste des adresses de serveur XenApp dans les paramètres de l'application comme indiqué dans la section « Pour ajouter des sites à Director » dans Configuration avancée.
   Vous devez fournir l'adresse de serveur d'un Controller par site XenApp : les autres Controller du site XenApp sont alors utilisés automatiquement en cas de basculement. Director n'équilibre pas les charges entre les Controller.

   Important : pour les adresses XenApp, pensez à bien utiliser le paramètre Service.AutoDiscoveryAddressesXA, et non le paramètre par défaut Service.AutoDiscoveryAddresses.
3. Le programme d'installation du fournisseur WMI de Director se trouve dans le dossier **Support\DirectorWMIProvider** sur le DVD. Installez-le sur tous les serveurs XenApp appropriés (contrôleurs et travailleurs sur lesquels les sessions sont en cours d'exécution).
   Si **winrm** n'est pas configuré, exécutez la commande **winrm qc**.
4. Configurez chaque serveur de tâches XenApp pour accepter les requêtes WinRM comme indiqué dans la rubrique Configurer les permissions.
5. Configurez une exception de pare-feu pour le port 2513, utilisé pour la communication entre Director et XenApp.
6. Pour sécuriser les communications entre le navigateur et le serveur Web, Citrix recommande de mettre en œuvre TLS sur le site Web IIS qui héberge Director.
   Pour plus d'informations, reportez-vous à la documentation de Microsoft IIS. Pour activer TLS, aucune configuration n'est requise dans Director.

> **Remarque**
>
> Pour autoriser Director à localiser toutes les tâches XenApp dans la batterie, vous devez ajouter une zone DNS inversée pour les sous-réseaux dans lesquels les serveurs XenApp résident sur les serveurs DNS utilisés par la batterie de serveurs.

Ouvrir une session sur Director

Le site Web Director se trouve à l'adresse https ou http:///Director.

Si l'un des sites d'un déploiement multisite est arrêté, l'ouverture de session pour Director nécessite un peu plus de temps lorsqu'il tente de se connecter au site qui est arrêté.

Utiliser Director avec l'authentification Windows intégrée

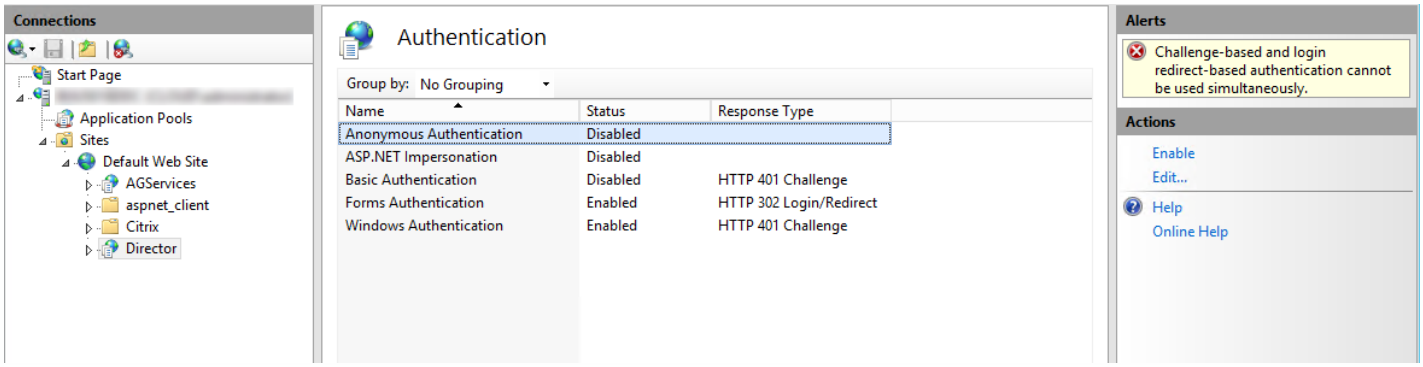
Avec l'authentification Windows intégrée, les utilisateurs appartenant à un domaine disposent d'un accès direct à Director sans avoir à saisir de nouveau leurs informations d'identification dans la page d'ouverture de session Director. Configuration requise pour l'utilisation de l'authentification Windows intégrée et de Director :

- Activez l'authentification Windows intégrée sur le site Web IIS qui héberge Director. Lorsque vous installez Director, l'authentification anonyme et l'authentification par formulaire sont activées. Pour utiliser l'authentification Windows

© 1999-2017 Citrix Systems, Inc. All rights reserved.

intégrée et Director, désactivez l'authentification anonyme et activez l'authentification Windows. L'authentification par formulaire doit rester activée pour l'authentification des utilisateurs sans domaine.

1. Démarrez le gestionnaire IIS.
2. Accédez à **Sites** > **Site Web par défaut** > **Director**.
3. Sélectionnez **Authentification**.
4. Cliquez avec le bouton droit sur **Authentification anonyme** et sélectionnez **Désactiver**.
5. Cliquez avec le bouton droit sur **Authentification Windows** et sélectionnez **Activer**.



- Configurez l'autorisation de délégation Active Directory pour la machine Director. Cette étape est requise uniquement si Director et le Delivery Controller sont installés sur des machines distinctes.
  1. Sur la machine Active Directory, ouvrez la console de gestion Active Directory.
  2. Une fois que la console de gestion Active Directory est ouverte, accédez à **Nom de domaine** > **Ordinateurs** et sélectionnez la machine Director à laquelle attribuer l'autorisation de délégation.
  3. Cliquez avec le bouton droit et sélectionnez **Propriétés**.
  4. Dans Propriétés, sélectionnez l'onglet **Délégation**.
  5. Sélectionnez l'option **Approuver cet ordinateur pour la délégation à tous les services (Kerberos uniquement)**.

- Le navigateur qui est utilisé pour accéder à Director doit prendre en charge l'authentification Windows intégrée. Cela peut nécessiter des étapes de configuration supplémentaires dans Firefox et Chrome. Pour plus d'informations, reportez-vous à la documentation relative au navigateur.
- Le service de surveillance Monitoring Service doit exécuter Microsoft .NET Framework 4.5.1 ou une version ultérieure prise en charge répertoriée dans la section Configuration système requise pour Director. Pour plus d'informations, veuillez consulter la section Configuration requise.

Lorsqu'un utilisateur ferme sa session sur Director ou à l'expiration de la session, la page d'ouverture de session s'affiche. À partir de la page d'ouverture de session, l'utilisateur peut définir le type d'authentification sur **Ouverture de session automatique** ou **Informations d'identification utilisateur**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration avancée

Jul 07, 2016

Dans cet article :

Pour prendre en charge des utilisateurs sur plusieurs domaines et forêts Active Directory

Ajouter des sites à Director

Désactiver la visibilité des applications en cours d'exécution dans le Gestionnaire d'activités

Certains paramètres de configuration avancés de Director, tels que la prise en charge de plusieurs sites ou de plusieurs forêts Active Directory, sont contrôlés au travers des paramètres du Gestionnaire des services Internet (IIS).
Important : lorsque vous modifiez un paramètre dans les services IIS, le service Director redémarre automatiquement et ferme la session des utilisateurs.
Pour configurer les paramètres avancés à l'aide des services IIS :

1. Ouvrez la console du Gestionnaire des services Internet Information Services (IIS).
2. Accédez au site Web Director sous le site Web par défaut.
3. Cliquez deux fois sur **Paramètres d'application**.
4. Cliquez deux fois sur un paramètre pour le modifier.

Par défaut, les licences Platinum conservent les données pendant 90 jours. Pour de plus amples informations sur les configurations, consultez la section Granularité de données et rétention.

Pour prendre en charge des utilisateurs sur plusieurs domaines et forêts Active Directory

Director utilise Active Directory pour rechercher des utilisateurs et accéder à des informations supplémentaires sur ces utilisateurs ou leur machine. Par défaut, Director recherche le domaine ou la forêt dans lequel ou laquelle :

- le compte d'administrateur est membre ;
- le serveur Web Director est membre (si différent).

Director tente d'effectuer des recherches au niveau de la forêt à l'aide du catalogue global Active Directory. Si l'administrateur ne dispose pas de permissions lui permettant d'effectuer des recherches au niveau de la forêt, la recherche porte uniquement sur le domaine.

Pour rechercher des données dans un domaine ou une forêt Active Directory distincts, vous devez spécifier explicitement les domaines ou les forêts à parcourir. Configurez le paramètre suivant :
`Connector.ActiveDirectory.Domains = (user),(server)`
La valeur des attributs utilisateur et serveur représentent les domaines de l'utilisateur Director (l'administrateur) et du serveur Director respectivement.

Pour autoriser les recherches dans un autre domaine ou une autre forêt, ajoutez le nom du domaine à la liste comme indiqué dans l'exemple suivant :

`Connector.ActiveDirectory.Domains = (user),(server),,`
Pour chaque domaine de la liste, Director tente d'effectuer des recherches au niveau de la forêt. Si l'administrateur ne dispose pas de permissions lui permettant d'effectuer des recherches au niveau de la forêt, la recherche porte uniquement sur le domaine.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **Remarque**
>
> Dans un environnement comportant plusieurs forêts, Director n'affiche pas les détails de sessions des utilisateurs d'autres forêts qui ont été attribués au groupe de mise à disposition XenDesktop à l'aide du groupe local de domaine.

Ajouter des sites à Director

Si Director est déjà installé, configurez-le pour qu'il fonctionne avec plusieurs sites. Pour ce faire, utilisez la console Gestionnaire des services Internet (IIS) sur chaque serveur Director pour mettre à jour la liste des adresses de serveurs dans les paramètres de l'application.

Ajoutez l'adresse d'un Controller pour chaque site au paramètre suivant :
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
où SiteAController et SiteBController correspondent aux adresses Delivery Controller de deux sites différents.

Pour les sites XenApp 6.5, ajoutez l'adresse d'un Controller pour chaque batterie XenApp au paramètre suivant :
Service.AutoDiscoveryAddressesXA = FarmAController,FarmBController
où FarmAController et FarmBController correspondent aux adresses des Controller XenApp de deux batteries différentes.

Pour les sites XenApp 6.5, il existe une autre méthode pour ajouter un Controller à une batterie XenApp :
DirectorConfig.exe /xenapp FarmControllerName

Désactiver la visibilité des applications en cours d'exécution dans le Gestionnaire d'activités

Par défaut, le Gestionnaire d'activité de Director affiche une liste de toutes les applications en cours d'exécution pour la session de l'utilisateur. Ces informations peuvent être consultées par les administrateurs qui ont accès à la fonctionnalité Gestionnaire d'activité de Director. Pour les rôles d'administrateur délégué, ceci comprend l'administrateur complet, l'administrateur du groupe de mise à disposition et l'administrateur du bureau d'assistance.

Pour protéger la confidentialité des utilisateurs et les applications qu'ils sont en cours d'exécution, vous pouvez désactiver l'onglet Applications afin qu'il arrête de répertorier les applications en cours d'exécution.

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

1. Sur le VDA, modifiez la clé de registre située à l'adresse HKLM\Software\Citrix\Director\TaskManagerDataDisplayed. Par défaut, la clé est définie sur 1. Modifiez la valeur sur 0, ce qui signifie que les informations ne seront pas affichées dans le Gestionnaire d'activités.
2. Sur le serveur sur lequel Director est installé, modifiez le paramètre qui contrôle la visibilité des applications en cours d'exécution. Par défaut, la valeur est true, ce qui offre la visibilité des applications en cours d'exécution dans l'onglet Applications. Modifiez la valeur sur false, ce qui désactive cette visibilité. Cette option affecte uniquement le gestionnaire d'activité dans Director et non le VDA.
   Modifiez la valeur du paramètre suivant :
   UI.TaskManager.EnableApplications = false

Important : pour désactiver l'affichage des applications en cours d'exécution, Citrix vous recommande d'effectuer ces modifications pour vous assurer que les données ne sont pas affichées dans le Gestionnaire d'activités.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Surveiller les déploiements

Jul 13, 2016

Dans cet article :

Surveiller les sites

Contrôler des sessions

Filtrer les données pour résoudre les échecs

Contrôler les tendances historiques sur un site

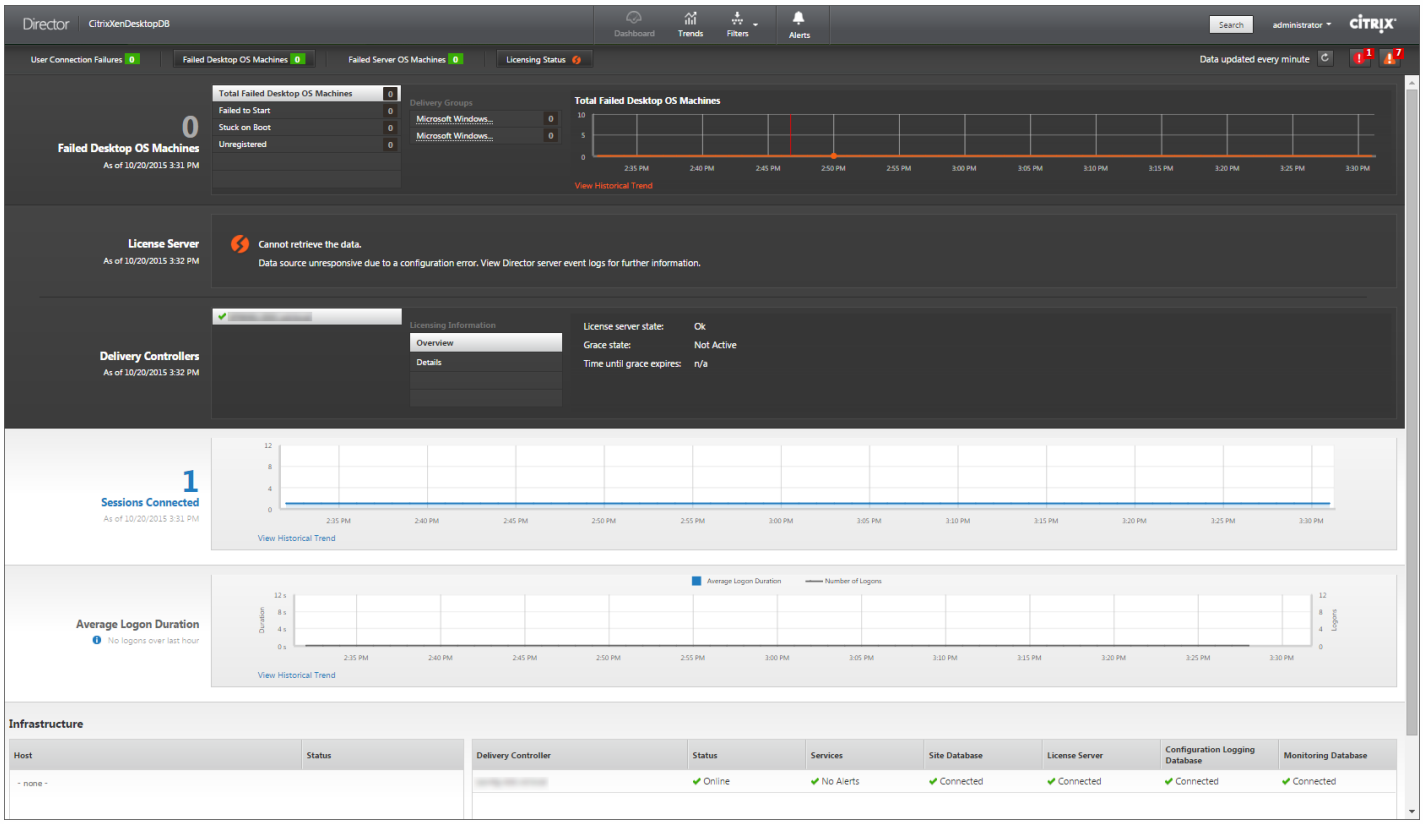
Contrôler les corrections à chaud

Contrôler les états d'alimentation de la machine utilisateur

Empêcher les connexions aux machines

Surveiller les sites

Avec des permissions d'administrateur complet, lorsque vous ouvrez Director, le Tableau de bord fournit un emplacement centralisé permettant de surveiller l'intégrité et l'utilisation d'un site.



S'il n'existe actuellement aucune erreur et qu'aucune erreur ne s'est produite au cours des dernières 60 minutes, les panneaux ne s'affichent pas. Lorsqu'il existe des erreurs, le panneau d'échec spécifique s'affiche automatiquement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Remarque : en fonction des licences de votre organisation et des privilèges de l'administrateur, certaines options ou fonctionnalités risquent de ne pas être disponibles.

Panneau	Description
Échecs de connexion utilisateur	Échecs de connexion lors des dernières 60 minutes. Cliquez sur les catégories situées en regard du nombre total pour afficher les métriques pour ce type d'échec. Dans la table suivante, ce nombre est réparti par groupe de mise à disposition. Échecs de connexion inclut les erreurs causées par les limites d'application qui sont atteintes. Pour de plus amples informations sur les limites d'application, consultez la section Applications.
Machines avec OS de bureau en échec ou Machines avec OS de serveur en échec	Nombre total d'échecs dans les dernières 60 minutes réparties par groupes de mise à disposition. Échecs répartis par types, y compris les échecs de démarrage, bloqués au démarrage, et non enregistrés. Pour les machines avec OS de serveur, les erreurs comprennent également le moment où les machines atteignent une charge maximale.
Statut de la licence	• Les alertes du serveur de licences sont envoyées par le serveur de licences et affichent également les actions requises pour la résolution de l'alerte. • Les alertes Delivery Controller affichent les détails de l'état des licences comme elles sont vues par le contrôleur et sont envoyées par le Delivery Controller. Vous pouvez définir le seuil des alertes dans Studio. Les alertes du serveur de licences et/ou Delivery Controller ne s'affichent pas si la version de votre serveur de licences est antérieure à 11.12.1 et/ou de votre Delivery Controller est antérieur à XenApp 7.6 ou XenDesktop 7.6.
Session(s) connectée(s)	Sessions connectées sur tous les groupes de mise à disposition pour les dernières 60 minutes.
Durée moyenne de l'ouverture de session	Données d'ouverture de session pour les dernières 60 minutes. Le nombre important sur la gauche est la durée moyenne d'ouverture de session sur l'heure en cours. Les données d'ouverture de session pour les VDA antérieurs à XenDesktop 7.0 ne sont pas incluses dans cette moyenne. Pour de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion utilisateur.
Infrastructure.	État d'intégrité des hôtes, Controller et infrastructure de votre site. Permet d'afficher les alertes de performances. Pour les hôtes, l'état de la connexion et l'intégrité de l'UC, de la mémoire, de la bande passante (utilisation du réseau) et du stockage (utilisation du disque) sont suivis à l'aide des informations fournies par XenServer ou VMware. Par exemple, vous pouvez configurer XenCenter pour générer des alertes de performances lorsque l'utilisation de l'UC, E/S réseau ou E/S disque dépasse un seuil spécifié sur un serveur ou une machine virtuelle géré(e). Par défaut, l'intervalle de répétition d'alerte est de 60 minutes, mais vous pouvez le

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Panneau	Description
	configurer. Pour plus de détails, dans la documentation XenServer, consultez la section Configuration des alertes de performances.

Remarque : l'absence d'icône pour une mesure donnée indique que cette mesure n'est pas prise en charge par le type de l'hôte utilisé. Par exemple, aucune information d'intégrité n'est disponible pour les hôtes System Center Virtual Machine Manager (SCVMM), AWS et CloudStack.
Continuez à résoudre les problèmes à l'aide de ces options (qui sont répertoriées ci-dessous) :

- Contrôler l'alimentation de la machine utilisateur
- Empêcher les connexions aux machines

Contrôler des sessions

Si une session devient déconnectée, elle reste active et ses applications continuent d'être exécutées, mais la machine cliente ne communique plus avec le serveur.

Action	Description
Afficher la machine ou la session actuellement connectée de l'utilisateur	À partir des vues Gestionnaire d'activités et Détails de l'utilisateur, affichez la machine ou la session actuellement connectée de l'utilisateur et une liste de toutes les machines et des sessions auxquelles cet utilisateur a accès. Pour accéder à cette liste, cliquez sur l'icône de sélection de session dans la barre de titre utilisateur. Voir Restaurer les sessions.
Afficher le nombre total de sessions déconnectées sur tous les groupes de mise à disposition	Depuis le Tableau de bord, dans le panneau Sessions connectées, affichez le nombre total de sessions connectées sur les groupes de mise à disposition pour les dernières 60 minutes. Puis cliquez sur le nombre total, qui ouvre la vue Filtres, où vous pouvez afficher les données de session graphiques basées sur les groupes de mise à disposition sélectionnés et les plages et l'utilisation au travers des groupes de mise à disposition.
Afficher les données sur une période plus longue	Dans la vue Tendances, sélectionnez l'onglet Sessions pour affiner les données d'utilisation de manière plus spécifique pour les sessions connectées et déconnectées sur une période de temps plus longue (c'est-à-dire, les totaux de session antérieurs aux dernières 60 minutes). Pour afficher ces informations, cliquez sur Afficher les tendances historiques.

Remarque : si la machine utilisateur exécute un Virtual Delivery Agent (VDA) d'ancienne génération, telle qu'un VDA antérieur à la version 7 ou un Linux VDA, Director ne peut pas afficher d'informations complètes sur la session. Un message s'affiche indiquant que les informations ne sont pas disponibles.

Filtrer les données pour résoudre les échecs

Lorsque vous cliquez sur des nombres sur le tableau de bord ou que vous sélectionnez un filtre pré défini depuis le menu Filtres, la vue Filtres s'ouvre pour afficher les données basées sur la machine sélectionnée ou le type d'échec.

Les filtres pré définis ne peuvent être modifiés, mais vous pouvez enregistrer un filtre pré défini en tant que filtre personnalisé puis le modifier. De plus, vous pouvez créer des vues de filtres personnalisés de machines, de connexions et de sessions sur tous les groupes de mise à disposition.

1. Sélectionner une vue :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Machines**. Sélectionnez des machines avec OS de bureau ou des machines avec OS de serveur. Ces vues illustrent le nombre de machines configurées. L'onglet Machines avec OS de serveur comprend également l'index de calculateur de charge, qui indique la distribution des compteurs de performances et les info-bulles du nombre de sessions si vous survolez le lien avec la souris.
- **Sessions**. Vous pouvez également afficher le nombre de sessions depuis la vue Machines.
- **Connexions**. Filtrez les connexions par différentes périodes de temps, y compris les 60 dernières minutes, les dernières 24 heures ou les derniers 7 jours.

2. Pour localiser le moment auquel les erreurs se sont produites, sélectionnez le critère.
3. Utilisez les onglets supplémentaires pour chaque vue, selon vos besoins, pour terminer le filtre.
4. Sélectionnez des colonnes supplémentaires, selon vos besoins, pour résoudre plus de problèmes.
5. Enregistrez votre filtre et attribuez-lui un nom.
   Pour ouvrir le filtre plus tard, depuis le menu Filtres, sélectionnez le type d'erreur (Machines, Sessions ou Connexions), puis sélectionnez le filtre enregistré.
6. Si nécessaire, pour les vues de machines ou de connexions, utilisez les commandes de puissance pour toutes les machines que vous sélectionnez dans la liste filtrée. Pour la vue Sessions, utilisez les commandes ou l'option de session pour envoyer des messages.

Continuez à résoudre les problèmes à l'aide de ces options (qui sont répertoriées ci-dessous) :

- Contrôler l'alimentation de la machine utilisateur
- Empêcher les connexions aux machines

Contrôler les tendances historiques sur un site

La vue Tendances accède aux informations de tendances d'historique pour les sessions, les échecs de connexion, les échecs de machines, les performances d'ouverture de session et l'évaluation de charge pour chaque site. Pour situer ces informations, dans la vue Tableau de bord ou Filtres, cliquez sur Tendances.

Cette fonctionnalité d'exploration vous permet de naviguer au travers des diagrammes de tendances en effectuant un zoom avant sur une période de temps (en cliquant sur un point de données dans le diagramme) et en effectuant un éclatement pour afficher les détails associés avec la tendance. Elle vous permet de mieux comprendre les détails des personnes ou éléments affecté(e)s par les tendances affichées.

Pour modifier l'étendue par défaut de chaque graphique, appliquez un filtre différent aux données.

Action	Description
Exporter les données du graphique	Sélectionnez l'onglet contenant les données à exporter. Cliquez sur Exporter et sélectionnez le format de fichier : .PDF, Excel ou .CSV.
Afficher les tendances des sessions	Dans l'onglet Sessions, sélectionnez le groupe de mise à disposition et la période de temps pour afficher des informations plus détaillées sur le nombre de sessions simultanées.
Afficher les tendances pour les échecs de connexion	Depuis l'onglet Échecs de connexion, sélectionnez le type de machine, le type d'échec, le groupe de mise à disposition et la période de temps pour afficher un

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	graphique contenant des informations plus détaillées sur les échecs de connexion utilisateur sur votre site.
Afficher les tendances des échecs de machine	Depuis l'onglet Machines avec OS de bureau défectueuses ou Machines avec OS serveur, sélectionnez le type de défaillance, le groupe de mise à disposition et la période de temps pour afficher un graphique contenant des informations plus détaillées sur les échecs de machine sur votre site.
Afficher les tendances pour les performances d'ouverture de session	Dans l'onglet Performances d'ouverture de session, sélectionnez le groupe de mise à disposition et la période de temps pour afficher un graphique contenant des informations plus détaillées sur la durée d'ouverture de session de l'utilisateur sur votre site et si le nombre d'ouvertures de session affecte les performances. Cette vue affiche également la durée moyenne des phases d'ouverture de session, telles que la durée de la négociation, la durée de démarrage de la machine virtuelle, etc. Ces données sont spécifiques aux ouvertures de session des utilisateurs et ne comprennent pas les utilisateurs essayant de se reconnecter à des sessions déconnectées. Le tableau en dessous du diagramme affiche la Durée de connexion par session utilisateur. L'administrateur peut choisir les colonnes à afficher et trier le rapport en fonction de n'importe colonne. Pour de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion utilisateur.
Afficher les tendances pour l'évaluation de charge	Dans l'onglet Index de calculateur de charge, affichez un graphique contenant des informations plus détaillées sur la charge distribuée entre les machines avec OS de serveur. Les options de filtre de ce graphique incluent le groupe de mise à disposition ou la machine avec OS de serveur dans un groupe de mise à disposition, la machine avec OS de serveur (disponible uniquement si la machine avec OS de serveur d'un groupe de mise à disposition a été sélectionnée), et la plage.
Afficher l'utilisation des applications hébergées	La disponibilité de cette fonctionnalité dépend de la licence de votre organisation. À partir de l'onglet Gestion de la capacité, sélectionnez l'onglet Utilisation des applications hébergées, sélectionnez le groupe de mise à disposition et la période de temps pour visualiser un graphique affichant la période d'utilisation simultanée maximale et une table affichant l'utilisation de l'application. À partir de la table affichant l'utilisation de l'application, vous pouvez choisir une application spécifique pour voir les détails et une liste des utilisateurs qui utilisent, ou ont utilisé l'application.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Afficher l'utilisation des OS de bureau et de serveur	La vue Tendances affiche l'utilisation des OS de bureau par site et par groupe de mise à disposition. Lorsque vous sélectionnez Site, l'utilisation est indiquée par groupe de mise à disposition. Lorsque vous sélectionnez Groupe de mise à disposition, l'utilisation est indiquée par utilisateur. La vue Tendances affiche également l'utilisation des OS de serveur par site, par groupe de mise à disposition et par machine. Lorsque vous sélectionnez Site, l'utilisation est indiquée par groupe de mise à disposition. Lorsque vous sélectionnez Groupe de mise à disposition, l'utilisation est indiquée par machine et par utilisateur. Lorsque Machine est sélectionné, l'utilisation est indiquée par utilisateur.
Afficher l'utilisation de machine virtuelle	À partir de l'onglet Utilisation de machine, sélectionnez Machines avec OS de bureau ou Machines avec OS de serveur pour obtenir une vue en temps réel de votre utilisation des machines virtuelles, ce qui vous permet d'évaluer rapidement les besoins en capacité de votre site. Disponibilité d'OS de bureau : affiche l'état actuel des machines avec OS de bureau (VDI) par disponibilité pour la totalité du site ou un groupe de mise à disposition spécifique. Disponibilité d'OS de serveur : affiche l'état actuel des machines avec OS de serveur par disponibilité pour la totalité du site ou un groupe de mise à disposition spécifique.
Afficher les données d'analyse du réseau à l'aide de HDX Insight	La disponibilité de cette fonctionnalité dépend de la licence de votre organisation et vos permissions d'administrateur. Dans l'onglet Réseau, surveillez votre analyse réseau, qui fournit une vue contextuelle utilisateur, application et bureau du réseau. Avec cette fonctionnalité, Director offre une analyse avancée du trafic ICA dans votre déploiement.

Les icônes de drapeaux sur le graphique indiquent des actions ou événements significatifs pour cette période spécifique. Placez le pointeur sur un drapeau et cliquez pour obtenir la liste des événements ou actions.

Remarque : les données d'ouverture de session de la connexion HDX ne sont pas collectées pour les VDA antérieurs à la version 7. Pour les VDA antérieurs, les données du graphique sont affichées en tant que 0.

Continuez à résoudre les problèmes à l'aide de ces options (qui sont répertoriées ci-dessous) :

- Contrôler l'alimentation de la machine utilisateur
- Empêcher les connexions aux machines

Contrôler les corrections à chaud

Pour afficher les corrections à chaud installées sur un VDA de machine (physique ou VM) spécifique, choisissez la vue Détails

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de la machine.

Contrôler les états d'alimentation de la machine utilisateur

Pour contrôler l'état des machines que vous sélectionnez dans Director, utilisez les options de Contrôle de l'alimentation. Ces options sont disponibles pour les machines avec système d'exploitation de bureau, mais pas pour les machines avec système d'exploitation de serveur.

Remarque : cette fonctionnalité n'est pas disponible pour les machines physiques utilisant Remote PC Access.

Commande	Fonction
Redémarrer	Effectue une fermeture (en douceur) ordonnée de la VM, et tous les processus en cours d'exécution sont arrêtés individuellement avant le redémarrage de la VM. Par exemple, sélectionnez les machines qui s'affichent dans Director en tant que « n'a pas réussi à démarrer » et utilisez cette commande pour les redémarrer.
Forcer le redémarrage	Redémarre la VM sans tenter d'effectuer de procédure de fermeture. Cette commande ne fonctionne de la même manière que lorsque vous débranchez un serveur physique puis le rebranchez et le redémarrez à nouveau.
Fermeture	Effectue une fermeture (en douceur) ordonnée de la VM ; tous les processus en cours d'exécution sont arrêtés individuellement.
Forcer la fermeture	Arrête la VM sans effectuer tout d'abord une procédure de fermeture. Cette commande fonctionne de la même manière que lorsque vous débranchez un serveur physique. Il est possible que tous les processus en cours d'exécution ne soient pas arrêtés, et vous risquez de perdre des données si vous arrêtez la VM de cette manière.
Suspend	Permet de suspendre une VM en cours d'exécution dans son état actuel et stocke cet état dans un fichier sur le référentiel de stockage par défaut. Cette option vous permet de fermer le serveur hôte de la VM et plus tard, après le redémarrage, reprendre la VM, le retourner à son état d'origine en cours d'exécution.
Reprendre	Reprend une VM suspendue et restaure l'état en cours d'exécution d'origine.
Démarrer	Démarre une VM lorsqu'elle est désactivée (également appelé un démarrage à froid).

Si les actions du contrôle de l'alimentation échouent, placez le curseur de la souris sur l'alerte et un message contextuel s'affiche avec des détails sur l'échec.

Empêcher les connexions aux machines

Utiliser le mode maintenance pour empêcher de nouvelles connexions temporairement lorsque l'administrateur approprié effectue des tâches de maintenance sur l'image.

Lorsque vous activez le mode maintenance sur les machines, aucune nouvelle connexion n'est autorisée jusqu'à ce que vous la désactiviez. Si la session des utilisateurs est actuellement ouverte, le mode maintenance prend effet dès que les sessions de tous les utilisateurs sont fermées. Pour les utilisateurs qui ne ferment pas leur session, envoyez un message les informant que les machines vont être arrêtées à un certain moment, et utilisez les commandes d'alimentation pour forcer la fermeture

© 1999-2017 Citrix Systems, Inc. All rights reserved.

des machines.

1. Sélectionnez la machine dans la vue Détails de l'utilisateur ou un groupe de machines dans la vue Filtres.
2. Sélectionnez le mode Maintenance et activez l'option.

Si un utilisateur essaie de se connecter à un bureau affecté lors qu'il se trouve en mode maintenance, un message s'affiche indiquant que le bureau est actuellement non disponible. Aucune nouvelle connexion ne peut être effectuée tant que vous n'aurez pas désactivé le mode maintenance.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Alertes et notifications

Jul 20, 2016

Dans cet article :

Surveiller les alertes

Créer des stratégies d'alerte

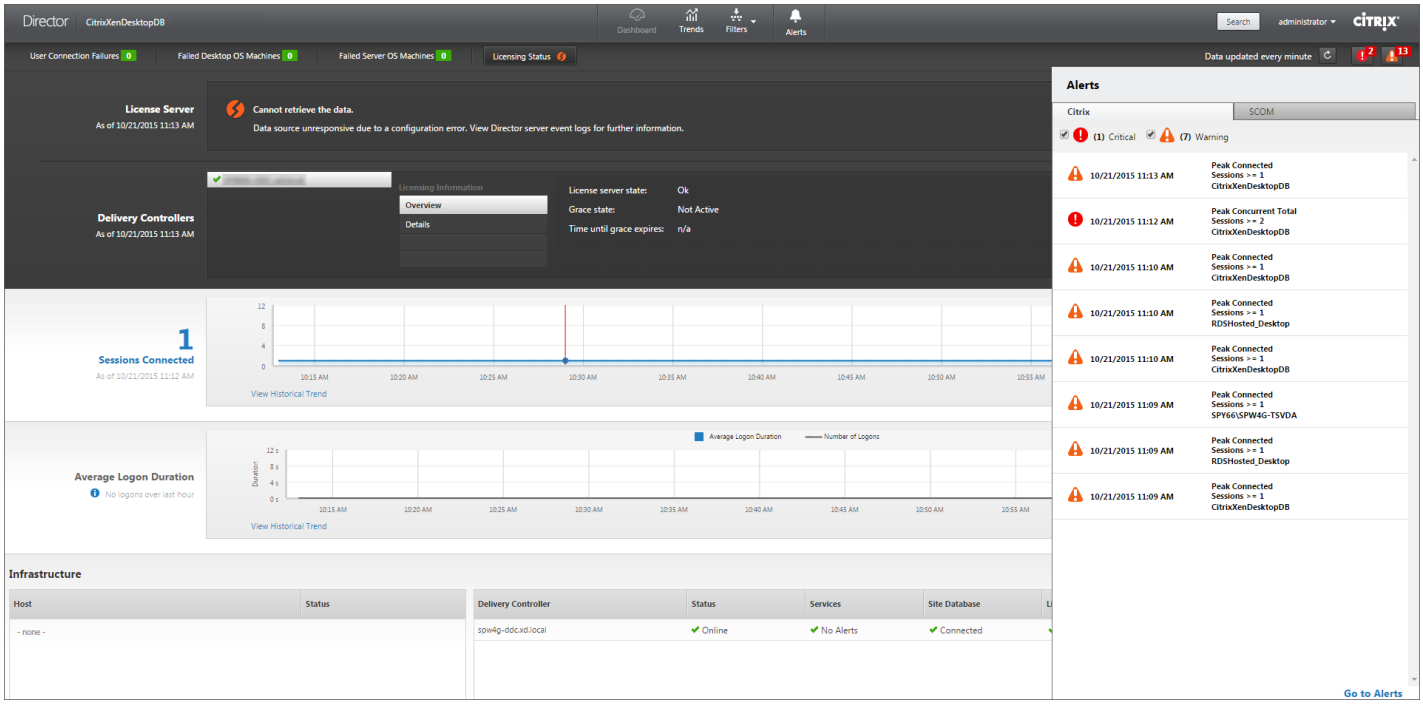
Conditions de stratégies d'alerte

Alertes SCOM

Configurer l'intégration de SCOM

Surveiller les alertes

Les alertes sont affichées dans Director sur le tableau de bord et dans d'autres vues de haut niveau avec des symboles d'avertissement et d'alerte critique. Les alertes sont mises à jour automatiquement toutes les minutes ; vous pouvez également mettre à jour les alertes à la demande.



Une alerte d'avertissement (triangle de couleur ambre) indique que le seuil minimal d'une condition a été atteint.

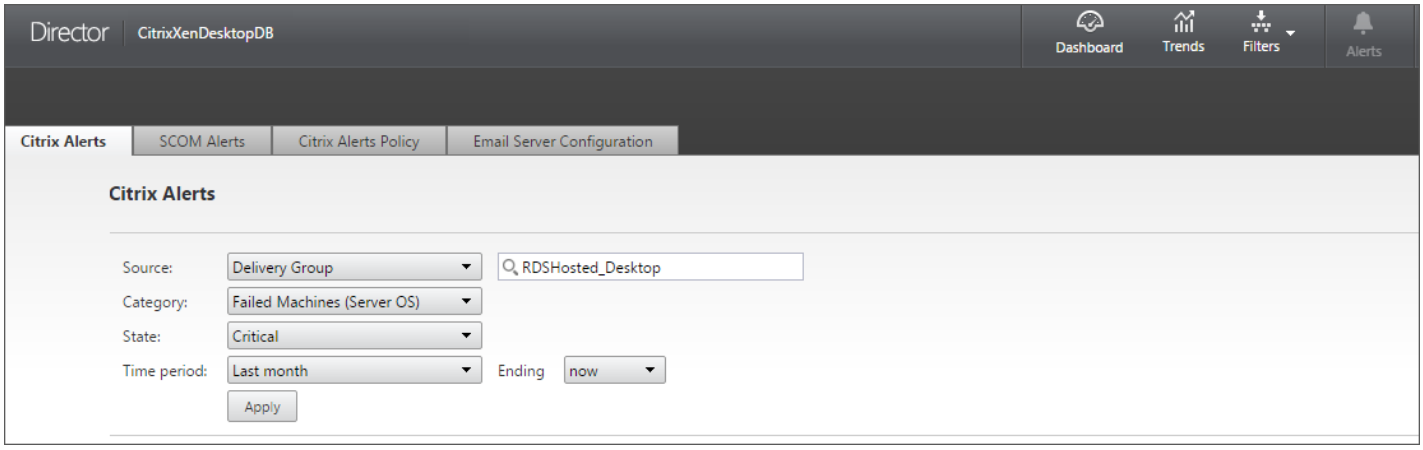
Une alerte critique (cercle rouge) indique que le seuil maximal d'une condition a été dépassé.

Vous pouvez afficher des informations plus détaillées sur les alertes en sélectionnant une alerte dans la barre latérale, en cliquant sur le lien **Aller aux alertes** dans le bas de la barre latérale ou en sélectionnant **Alertes** dans le haut de la page de Director.

Dans la vue Alertes, vous pouvez filtrer et exporter les alertes. Par exemple, les machines avec OS de serveur défectueuses

© 1999-2017 Citrix Systems, Inc. All rights reserved.

pour un groupe de mise à disposition spécifique sur le dernier mois.



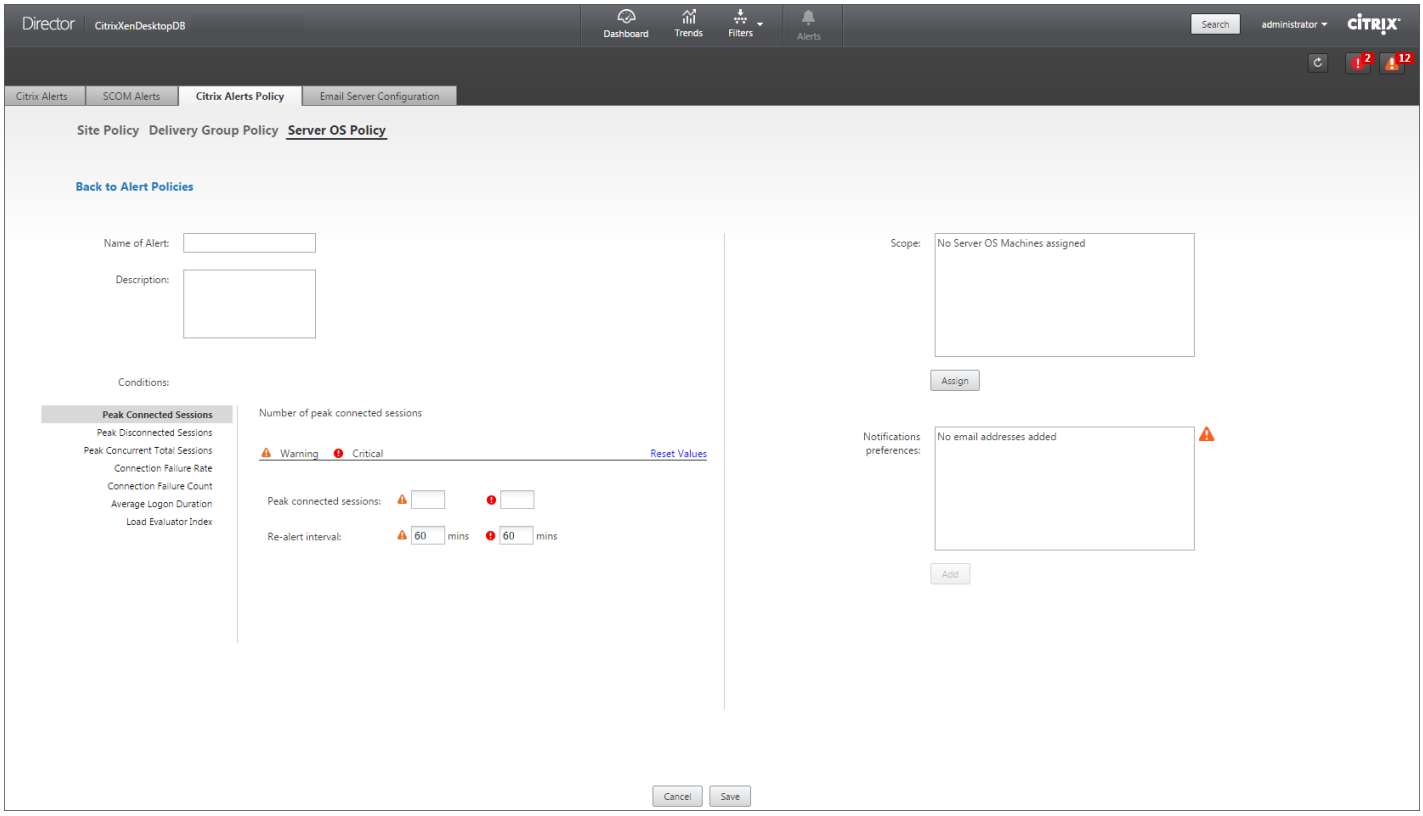
Alertes Citrix. Les alertes Citrix sont des alertes que vous pouvez surveiller dans Director provenant de composants Citrix. Vous pouvez configurer les stratégies d'alerte Citrix dans Director sous **Alertes** > **Stratégies d'alerte Citrix**. Dans le cadre de la configuration, vous pouvez définir l'envoi par e-mail de notifications à des individus et des groupes lorsque des alertes sont générées suite au franchissement du seuil d'une condition d'alerte. Pour de plus amples informations sur la configuration des alertes Citrix, consultez la section Créer des stratégies d'alerte.

Alertes SCOM. Les alertes SCOM affichent des informations provenant de Microsoft System Center 2012 Operations Manager (SCOM) pour fournir une indication plus complète de l'intégrité et des performances du centre de données de Director. Pour de plus amples informations, consultez les sections Alertes SCOM et Configurer l'intégration de SCOM.

Le nombre d'alertes affiché en regard des icônes d'alertes avant que vous développiez la barre latérale représente la somme totale des alertes Citrix et SCOM.

Créer des stratégies d'alerte

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Pour créer une nouvelle stratégie d'alerte, par exemple pour générer une alerte lorsqu'un ensemble spécifique de critères concernant le nombre de sessions est rempli :

1. Accédez à **Alertes** > **Stratégies d'alerte Citrix** et sélectionnez, par exemple, Stratégie d'OS de serveur.
2. Cliquez sur **Créer**.
3. Fournissez un nom et une description pour la stratégie, puis définissez les conditions qui doivent être remplies pour que l'alerte soit déclenchée. Par exemple, spécifiez le nombre d'alertes d'avertissement et d'alertes critiques pour Sessions connectées maximales, Sessions déconnectées maximales et Total des sessions simultanées maximales. La valeur définie pour les alertes d'avertissement ne doit pas être supérieure à la valeur des alertes critiques. Pour de plus amples informations, consultez les conditions des stratégies d'alertes.
4. Définissez le paramètre Intervalle de répétition d'alerte. Si les conditions pour l'alerte sont toujours présentes, l'alerte est de nouveau déclenchée à cet intervalle et, si elle est configurée dans la stratégie, une notification par e-mail est générée. Une alerte ignorée ne génère pas de notification par e-mail à l'intervalle de répétition d'alerte.
5. Définissez l'étendue. Par exemple, sélectionnez un groupe de mise à disposition spécifique.
6. Dans les préférences de notification, spécifiez les personnes qui doivent être notifiées par e-mail lorsque l'alerte est déclenchée. Vous devez spécifier un serveur de messagerie SMTP dans l'onglet **Configuration du serveur de messagerie** pour définir les préférences de notification par e-mail dans les stratégies d'alertes.
7. Cliquez sur **Enregistrer**.

La création d'une stratégie comprenant plus de 20 groupes de mise à disposition dans l'étendue peut prendre environ 30 secondes. Un compteur s'affiche durant cette période.

La création de plus de 50 stratégies par groupe de mise à disposition pour moins de 20 groupes de mise à disposition uniques (un total 1 000 cibles au maximum) peut entraîner une réponse plus rapide (environ 5 secondes).

Conditions de stratégies d'alerte

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Condition de stratégie d'alerte	Description et actions recommandées
Sessions connectées max.	Nombre de sessions connectées max. Actions recommandées lorsque l'alerte s'affiche : • Vérifier la vue Tendances de session dans Director pour les sessions connectées maximales. • S'assurer qu'il y a suffisamment de capacité pour gérer la charge de session. • Ajouter des machines si nécessaire.
Sessions déconnectées max.	Nombre de sessions déconnectées max. Actions recommandées lorsque l'alerte s'affiche : • Vérifier la vue Tendances de session dans Director pour les sessions déconnectées maximales. • S'assurer qu'il y a suffisamment de capacité pour gérer la charge de session. • Ajouter des machines si nécessaire. • Fermer les sessions déconnectées si nécessaire.
Total des sessions simultanées max.	Nombre de sessions simultanées max. Actions recommandées lorsque l'alerte s'affiche : • Vérifier la vue Tendances de session dans Director pour les sessions simultanées maximales. • S'assurer qu'il y a suffisamment de capacité pour gérer la charge de session. • Ajouter des machines si nécessaire. • Fermer les sessions déconnectées si nécessaire.
Taux d'échecs de connexion	Pourcentage d'échecs de connexion au cours de la dernière heure. Calculé en fonction du nombre total d'échecs de tentatives de connexions. • Vérifier la vue Tendance des défaillances dans Director pour les événements consignés dans le journal de configuration. • Déterminer si les applications ou bureaux sont accessibles.
Nombre d'échecs de connexion	Nombre d'échecs de connexion au cours de la dernière heure. Actions recommandées lorsque l'alerte s'affiche : • Vérifier la vue Tendance des défaillances dans Director pour les événements consignés dans le journal de configuration. • Déterminer si les applications ou bureaux sont accessibles.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Machines défectueuses (OS de bureau)	Nombre de machines défectueuses avec OS de bureau. Actions recommandées lorsque l'alerte s'affiche : • Les échecs peuvent se produire pour diverses raisons comme indiqué dans les vues Tableau de bord et Filtres de Director. Exécuter les diagnostics Citrix Scout pour déterminer la cause. Pour de plus amples informations, consultez la section Résoudre les problèmes utilisateur.
Machines défectueuses (OS de serveur)	Nombre de machines défectueuses avec OS de serveur. Actions recommandées lorsque l'alerte s'affiche : • Les échecs peuvent se produire pour diverses raisons comme indiqué dans les vues Tableau de bord et Filtres de Director. Exécuter les diagnostics Citrix Scout pour déterminer la cause.
Durée moyenne de l'ouverture de session	Durée moyenne des ouvertures de session au cours de la dernière heure. Actions recommandées lorsque l'alerte s'affiche : • Vérifier le tableau de bord Director pour obtenir des mesures à jour sur la durée des ouvertures de session. Les ouvertures de session peuvent prendre plus de temps si un grand nombre d'utilisateurs ouvrent une session pendant une courte période. • Vérifier la ligne de base et le détail des ouvertures de session pour déterminer la cause. Pour de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion utilisateur.
Index de calculateur de charge	Valeur de l'index de calculateur de charge pour les 5 dernières minutes. Actions recommandées lorsque l'alerte s'affiche : • Vérifier dans Director s'il existe des machines avec OS de serveur connaissant un pic de charge (charge max.). • Afficher le tableau de bord (échecs) et le rapport de tendances de l'index de calculateur de charge.

Alertes SCOM

L'intégration de SCOM avec Director vous permet de visualiser des alertes provenant de Microsoft System Center 2012 Operations Manager (SCOM) sur le tableau de bord et dans d'autres vues de haut niveau dans Director.

Les alertes SCOM s'affichent à l'écran, ainsi que les alertes Citrix. Vous pouvez accéder aux alertes SCOM et en afficher les détails depuis l'onglet SCOM dans la barre latérale.

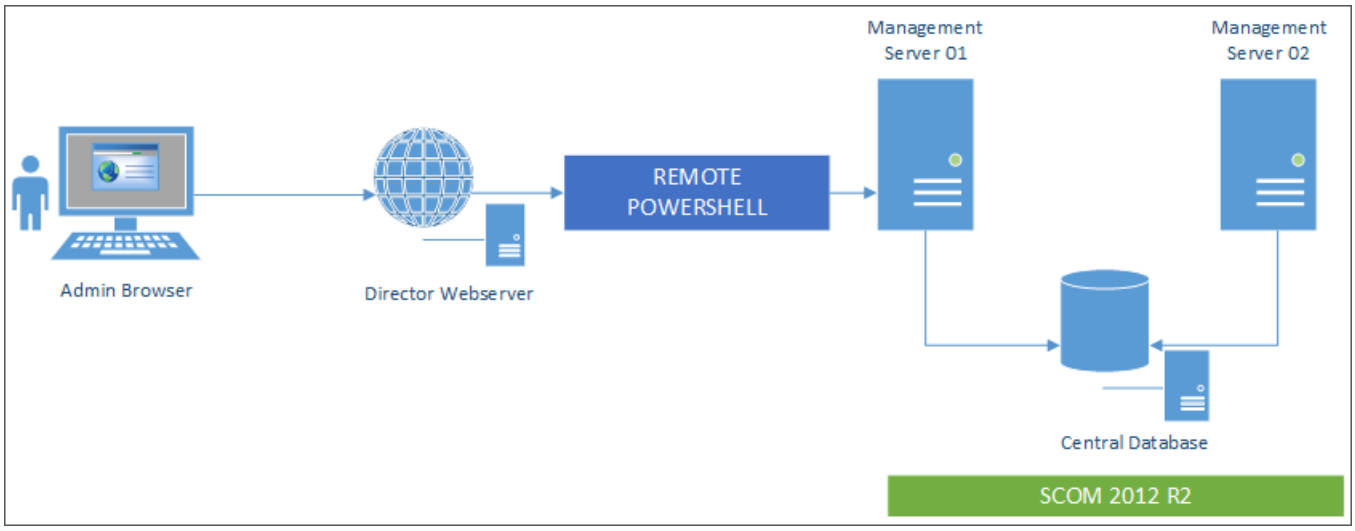
Vous pouvez afficher l'historique des alertes depuis un mois, trier, filtrer et exporter les informations filtrées dans des

© 1999-2017 Citrix Systems, Inc. All rights reserved.

rapports aux formats CSV, Excel et PDF.

Configurer l'intégration de SCOM

L'intégration de System Center Operations Manager (SCOM) utilise PowerShell 3.0 à distance ou une version plus récente pour interroger les données du serveur d'administration de System Center Operations Manager et maintient une connexion runspace permanente dans la session Director de l'utilisateur. Le serveur Director et le serveur SCOM doivent disposer de la même version de PowerShell.



La configuration requise pour l'intégration de SCOM est la suivante :

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0 ou version plus élevée (la version de PowerShell doit être la même dans le serveur Director et le serveur SCOM)
- UC quadruple cœur avec 16 Go de RAM (recommandé)
- Un serveur d'administration principal pour System Center Operations Manager doit être configuré dans le fichier web.config de Director. Vous pouvez le faire à l'aide de l'outil DirectorConfig.
- Citrix recommande que le compte d'administrateur de Director soit configuré en tant que rôle d'opérateur de SCOM de façon à ce qu'il puisse obtenir des informations d'alertes complètes dans Director. Si cela n'est pas possible, un compte d'administrateur SCOM peut être configuré dans le fichier web.config à l'aide de l'outil DirectorConfig, mais cette solution n'est pas recommandée.
- Citrix vous recommande de ne pas configurer plus de 10 administrateurs Director par serveur d'administration SCOM. C'est pour vous assurer que le serveur d'administration SCOM ne soit pas trop chargé et garantisse des performances optimales.

Sur le serveur Director :

1. Sur le serveur Director, tapez **Enable-PSRemoting** pour activer la communication à distance PowerShell.

2. Ajoutez le serveur d'administration SCOM à la liste TrustedHosts. Ouvrez une invite PowerShell élevée à partir d'une ligne de commande PowerShell élevée et exécutez les commandes suivantes :

    a. Obtenez la liste TrustedHosts.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

commande COPIER

```
Get-Item WSMAN:\localhost\Client\TrustedHosts
```

b. Ajoutez le nom de domaine complet du serveur d'administration SCOM à la liste TrustedHosts. représente l'ensemble existant d'entrées renvoyées depuis l'applet de commande Get-Item.

commande COPIER

```
Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "<FQDN SCOM Management Server>,<Old Values>"
```

3. Configurez SCOM à l'aide de l'outil DirectorConfig.

commande COPIER

```
C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom
```

Sur le serveur d'administration SCOM :

1. Attribuez les administrateurs Director à un rôle d'administrateur SCOM.

a. Ouvrez la console d'administration SCOM et accédez à **Administration** > **Sécurité** > **Rôles utilisateur**.

b. Dans Rôles utilisateur, vous pouvez créer un nouveau rôle utilisateur ou modifier un rôle existant. Il existe quatre catégories d'opérateurs SCOM. Ces rôles définissent la nature de l'accès aux données SCOM. Par exemple, un opérateur de SCOM en lecture seule ne peut pas afficher le panneau Administration et ne peut découvrir ou gérer les règles, comptes ou machines. Un rôle d'opérateur de SCOM est un rôle d'administrateur complet.

Remarque :

Si un administrateur de Director se voit attribuer un rôle non opérateur, il n'aura pas accès aux opérations suivantes.

i. Si plusieurs serveurs d'administration ont été configurés, au cas où le serveur d'administration principal n'est pas disponible, l'administrateur de Director ne sera pas en mesure de se connecter au serveur d'administration secondaire.
Le serveur d'administration principal est le serveur configuré dans le fichier web.config de Director, qui est le même serveur que celui spécifié à l'étape 3 ci-dessus à l'aide de l'outil DirectorConfig. Les serveurs d'administration secondaires sont des serveurs d'administration homologues du serveur principal.

ii. Lors du filtrage des alertes, l'administrateur de Director ne sera pas en mesure de rechercher l'origine de l'alerte.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cette opération requiert une autorisation de niveau opérateur.

c. Pour modifier un rôle utilisateur, cliquez avec le bouton droit sur le rôle, puis cliquez sur Propriétés.

d. Dans la boîte de dialogue Propriétés du rôle, vous pouvez ajouter ou supprimer des administrateurs Director pour ce rôle utilisateur.

2. Ajoutez les administrateurs Director au groupe Utilisateurs de gestion à distance sur le serveur d'administration SCOM. Ceci permet aux administrateurs Director d'établir une connexion PowerShell distante.

3. Tapez **Enable-PSRemoting** pour activer la communication à distance PowerShell.

4. Définissez les limites des propriétés WS-Management :

a. Modifiez MaxConcurrentUsers :

Dans l'interface de ligne de commande :

```
commande
```

COPIER

```
winrm set winrm/config/winrs @{MaxConcurrentUsers = "20"}
```

Dans PS :

```
commande
```

COPIER

```
Set-Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
```

b. Modifiez MaxShellsPerUser :

Dans l'interface de ligne de commande :

```
commande
```

COPIER

```
winrm set winrm/config/winrs @{MaxShellsPerUser="20"}
```

Dans PS :

```
commande
```

COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
```

c. Modifiez MaxMemoryPerShellMB :

Dans l'interface de ligne de commande :

commande COPIER

```
winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
```

Dans PS :

commande COPIER

```
Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024
```

5. Pour vous assurer que l'intégration de SCOM fonctionne dans les environnements de domaine mixtes, définissez l'entrée de registre suivante.

Chemin d'accès : HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Clé : LocalAccountTokenFilterPolicy

Type : DWord

Valeur : 1

> ## Avertissement
>
> La modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

Une fois que l'intégration de SCOM est configurée, il se peut que le message suivant s'affiche : « Impossible d'obtenir les dernières alertes de SCOM. Consultez les journaux d'événements du serveur Director pour plus d'informations. » Les journaux d'événements du serveur vous permettront d'identifier et de corriger le problème. Causes potentielles :

- Perte de connectivité réseau sur la machine Director ou SCOM.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Le service SCOM n'est pas disponible ou trop occupé pour répondre.
- Échec de l'autorisation en raison d'une modification des autorisations de l'utilisateur configuré.
- Une erreur dans Director lors du traitement des données SCOM.
- Version de PowerShell différente entre le serveur Director et le serveur SCOM.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administration déléguée et Director

Jul 07, 2016

L'administration déléguée utilise trois concepts : les administrateurs, les rôles et les étendues. Les permissions sont basées sur un rôle administrateur et l'étendue de ce rôle. Par exemple, un administrateur peut affecter un rôle d'administrateur du bureau d'assistance où l'étendue implique la responsabilité des utilisateurs à un site uniquement.

Pour de plus amples informations sur la création d'administrateurs délégués, veuillez consulter le document Administration déléguée.

Les permissions d'administration déterminent l'interface Director présentée aux administrateurs et les tâches à effectuer. Les permissions déterminent :

- Les vues auxquelles l'administrateur peut accéder, collectivement nommées vue.
- Les bureaux, les machines et les sessions que l'administrateur peut afficher et interagir avec.
- Les commandes de l'administrateur peut effectuer, telles que l'observation d'une session de l'utilisateur ou l'activation du mode maintenance.

Les rôles et les permissions intégrés déterminent également la manière d'utilisation de Director par les administrateurs :

Rôle Administrateur	**Permissions de Director**
Administrateur complet	Possède un accès complet à toutes les vues et peut effectuer toutes les commandes, y compris l'observation d'une session utilisateur, l'activation du mode maintenance et l'exportation des données des tendances.
Administrateur de groupe de mise à disposition	Possède un accès complet à toutes les vues et peut effectuer toutes les commandes, y compris l'observation d'une session utilisateur, l'activation du mode maintenance et l'exportation des données des tendances.
Administrateur en lecture seule	Peut accéder à toutes les vues et afficher tous les objets dans les étendues spécifiées ainsi que les informations globales. Peut télécharger des rapports à partir de canaux HDX et peut exporter les données de Tendances à l'aide de l'option Exporter dans la vue Tendances. Ne peut exécuter des commandes ou modifier quoi que ce soit dans les vues.
Administrateur du service d'assistance	Peut accéder uniquement aux vues Bureau d'assistance et Détails de l'utilisateur et peut afficher uniquement des objets que l'administrateur est autorisé à gérer. Peut observer une session utilisateur et exécuter des commandes pour cet utilisateur. Peut effectuer les opérations du mode maintenance. Peut utiliser les options de contrôle de l'alimentation pour les machines avec OS de bureau. Impossible d'accéder aux vues Tableau de bord, Tendances, Alertes ou Filtres. Ne peut utiliser les options de contrôle de l'alimentation pour les machines avec OS de serveur.
Administrateur du catalogue de machines	Aucun accès. Cet administrateur n'est pas pris en charge pour Director et ne peut pas afficher les données. Cet utilisateur peut accéder à la page Détails de machine (recherche machine).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Rôle	Permissions de Director
Administrateur d'hôte	Aucun accès. Cet administrateur n'est pas pris en charge pour Director et ne peut pas afficher les données.

Pour configurer les rôles personnalisés pour les administrateurs Director

Dans Studio, vous pouvez également configurer des rôles spécifiques à Director, personnalisés pour correspondre plus étroitement aux besoins de votre organisation et déléguer des permissions de manière plus flexible. Par exemple, vous pouvez limiter le rôle d'administrateur du Bureau d'assistance intégré afin que cet administrateur ne puisse pas fermer de sessions.

Si vous créez un rôle personnalisé avec les permissions Director, vous devez également donner à ce rôle d'autres permissions génériques :

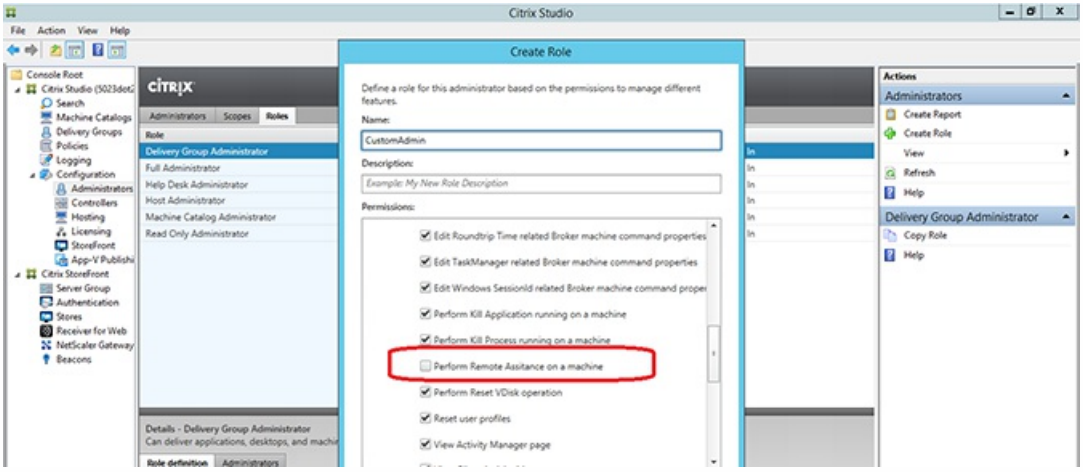
- permission Delivery Controller pour ouvrir une session sur Director.
- Permissions pour les groupes de mise à disposition pour afficher les données liées à ces groupes de mise à disposition dans Director.

Éventuellement, vous pouvez créer un rôle personnalisé en copiant un rôle existant et inclure des permissions supplémentaires pour différentes vues. Par exemple, vous pouvez copier le rôle du Bureau d'assistance et inclure des permissions pour afficher les pages Tableau de bord ou Filtres.

Sélectionnez les permissions de Director pour le rôle personnalisé, y compris :

- Arrêter l'application en cours d'exécution sur une machine
- Arrêter le processus en cours d'exécution sur une machine
- Effectuer une intervention à distance sur une machine
- Effectuer des réinitialisations d'opérations vDisk
- Réinitialiser les profils utilisateur
- Afficher la page Détails du client
- Afficher la page du tableau de bord
- Afficher la page Filtres
- Afficher la page Détails de la machine
- Afficher la page Tendances
- Afficher la page Détails de l'utilisateur

Dans cet exemple, l'observation (Effectuer une intervention à distance sur une machine) est désactivée.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

En outre, depuis la liste des permissions pour d'autres composants, prenez en compte ces permissions :

- Depuis les groupes de mise à disposition :
  - Activer/désactiver le mode de maintenance d'une machine via l'appartenance à un groupe de mise à disposition
  - Réaliser des opérations d'alimentation sur les machines de bureau Windows via l'appartenance à un groupe de mise à disposition
  - Réaliser la gestion de session sur les machines via l'appartenance à un groupe de mise à disposition

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sécuriser le déploiement de Director

Jul 07, 2016

Cet article dresse la liste des domaines susceptibles d'avoir un impact sur la sécurité du système lors du déploiement et de la configuration de Director.

Configurer Microsoft Internet Information Services (IIS)

Vous pouvez configurer Director avec une configuration IIS limitée. Veuillez noter qu'il ne s'agit pas de la configuration IIS par défaut.

Extensions de nom de fichier

Vous pouvez interdire les extensions de nom de fichier non répertoriées.

Director requiert ces extensions de nom de fichier dans le Filtrage des demandes :

- .aspx
- .css
- .html
- .js
- .png

Director requiert les verbes HTTP suivants dans le Filtrage des demandes : Vous pouvez interdire les verbes non répertoriés.

- GET
- POST
- HEAD

Director ne requiert pas ce qui suit :

- Filtres ISAPI
- Extensions ISAPI
- Programmes CGI
- Programmes FastCGI

Important

- Director requiert l'approbation Confiance totale. Ne définissez pas le niveau de confiance .NET global sur Élevé ou Moyen.
- Director gère un pool d'applications distinct. Pour modifier les paramètres de Director, sélectionnez le site Director et modifiez-le.

Configurer les droits des utilisateurs

Lorsque Director est installé, le droit d'ouverture de session Ouvrir une session en tant que service et les privilèges Ajuster les quotas de mémoire pour un processus, Générer des audits de sécurité et Remplacer un jeton de niveau processus sont accordés à ses pools d'applications. Il s'agit d'un comportement d'installation normal lorsque des pools d'applications sont créés.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Vous n’avez pas besoin de changer ces droits d’utilisateur. Ces privilèges ne sont pas utilisés par Director et sont automatiquement désactivés.

Certificats dans Director :

- Pour utiliser HTTPS, des certificats approuvés peuvent être configurés et utilisés.

Communications Director

Dans un environnement de production, Citrix vous recommande d'utiliser Internet Protocol Security (IPsec) ou le protocole HTTPS pour sécuriser le transfert des données entre Director et vos serveurs. IPsec est un ensemble d'extensions standard du protocole Internet qui garantit des communications authentifiées et cryptées avec intégrité des données et protection contre la relecture. IPsec étant un ensemble de protocoles de couches réseau, les protocoles d'un niveau plus élevé peuvent l'utiliser sans modification. HTTPS utilise les protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security) pour fournir un chiffrement fort des données.

Le Relais TLS peut être utilisé pour sécuriser le trafic de données entre Director et les serveurs XenApp/XenDesktop. Pour de plus amples informations, consultez l’article de blog Securing Citrix Director: OData Interface through TLS.

Citrix vous recommande de sécuriser les communications entre Director et les machines des utilisateurs à l'aide de NetScaler Gateway et du protocole HTTPS. Pour utiliser le protocole HTTPS, Director requiert que l'instance Microsoft Internet Information Services (IIS) hébergeant le service d'authentification soit configurée pour HTTPS. En l'absence de la configuration IIS appropriée, Director utilise le protocole HTTP pour les communications. Citrix vous recommande de ne pas autoriser les connexions utilisateur non sécurisées à Director dans un environnement de production.

Séparation de la sécurité de Director

Si vous déployez des applications Web dans le même domaine Web (nom de domaine et de port) que Director, tout risque ayant trait à la sécurité dans ces applications Web peut potentiellement réduire la sécurité de votre déploiement Director. Lorsqu'un degré plus important de séparation de la sécurité est nécessaire, Citrix recommande de déployer Director dans un domaine Web distinct.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurer les permissions pour VDA antérieurs à XenDesktop 7.

Jul 07, 2016

Si les utilisateurs possèdent des VDA antérieurs à XenDesktop 7 installés sur leurs machines, Director complète les informations sur le déploiement avec des données en temps réel sur l'état et des métriques via Windows Remote Management (WinRM).

En outre, utilisez cette procédure pour configurer WinRM pour une utilisation avec Remote PC dans XenDesktop 5.6 Feature Pack 1.

Par défaut, seuls les administrateurs locaux de la machine de bureau (c'est-à-dire, généralement, les administrateurs de domaine et autres utilisateurs privilégiés) disposent des permissions nécessaires pour afficher les données en temps réel.

Pour plus d'informations sur l'installation et la configuration de WinRM, veuillez consulter l'article CTX125243.

Pour autoriser d'autres utilisateurs à afficher les données en temps réel, vous devez leur accorder les permissions correspondantes. Par exemple, supposez qu'il existe plusieurs utilisateurs Director (HelpDeskUserA, HelpDeskUserB, etc) qui appartiennent au groupe de sécurité Active Directory appelé HelpDeskUsers. Le groupe a été attribué au rôle d'administrateur du bureau d'assistance dans Studio, leur offrant les permissions Delivery Controller requises. Toutefois, le groupe doit également pouvoir accéder aux informations de la machine de bureau.

Pour fournir l'accès nécessaire, vous pouvez configurer les permissions requises de l'une des façons suivantes :

- en définissant des permissions pour les utilisateurs Director (modèle d'usurpation d'identité) ;
- en définissant des permissions pour le service Director (modèle de sous-système autorisé).

Pour accorder des permissions relatives aux utilisateurs Director (modèle d'usurpation d'identité)

Par défaut, Director utilise le modèle d'usurpation d'identité : la connexion WinRM à la machine de bureau est établie en utilisant l'identité de l'utilisateur Director. C'est donc l'utilisateur qui doit disposer des permissions appropriées sur le bureau.

Vous pouvez configurer ces permissions de deux manières (décrites dans ce document) :

1. en ajoutant des utilisateurs au groupe d'administrateurs locaux sur la machine de bureau ;
2. en accordant aux utilisateurs les permissions spécifiques requises par Director. Cette option permet d'éviter de transmettre les permissions administratives de Director aux utilisateurs (par exemple, le groupe HelpDeskUsers) sur la machine.

Pour accorder des permissions au service Director (modèle de sous-système autorisé).

Au lieu d'accorder aux utilisateurs Director des permissions sur les machines de bureaux, vous pouvez configurer Director de sorte qu'il établisse les connexions WinRM à l'aide d'une identité de service et accorder à cette identité de service uniquement les permissions nécessaires.

Avec ce modèle, les utilisateurs Director ne sont pas autorisés à passer eux-mêmes des appels WinRM. Ils peuvent uniquement accéder aux données à l'aide de Director.

Le regroupement d'applications Director des services IIS est configuré pour être exécuté comme identité de service. Par défaut, il s'agit du compte virtuel APPPOOL\Director. Lorsque vous établissez des connexions à distance, ce compte

© 1999-2017 Citrix Systems, Inc. All rights reserved.

apparaît en tant que compte d'ordinateur Active Directory du serveur, par exemple MonDomaine\ServeurDirector$. Vous devez configurer ce compte avec les permissions nécessaires.

Si plusieurs sites Web Director sont déployés, vous devez placer chaque compte d'ordinateur du serveur Web dans un groupe de sécurité Active Directory configuré avec les permissions appropriées.

Pour configurer Director pour qu'il utilise l'identité du service pour WinRM au lieu de l'identité de l'utilisateur, configurez le paramètre suivant comme indiqué dans la rubrique Configuration avancée :

Service.Connector.WinRM.Identity = Service
Vous pouvez configurer ces permissions de l'une des façons suivantes :

1. en ajoutant le compte de service au groupe d'administrateurs locaux sur la machine de bureau ;
2. en accordant au compte de service les permissions spécifiques requises par Director (décrit ci-après). Cette option évite d'accorder au compte de service l'ensemble des permissions administratives sur la machine.

Pour attribuer des permissions à un utilisateur ou un groupe spécifique

Les permissions suivantes sont requises pour que Director puisse accéder aux informations relatives à la machine de bureau via WinRM :

- Permissions de lecture et d'exécution dans WinRM RootSDDL
- Permissions sur l'espace de nom WMI :
  - root/cimv2 - accès distant
  - root/citrix - accès distant
  - root/RSOP - accès distant et exécution
- Membre de ces groupes locaux :
  - Utilisateurs de type contrôle des performances
  - Lecteurs de journaux d'événements

L'outil ConfigRemoteMgmt.exe, utilisé pour accorder automatiquement des permissions, est disponible sur le support d'installation dans les dossiers x86\Virtual Desktop Agent et x64\Virtual Desktop Agent et sur le support d'installation dans le dossier tools. Vous devez accorder des permissions à tous les utilisateurs Director.

Pour accorder des permissions à un groupe de sécurité, utilisateur, compte d'ordinateur Active Directory, ou pour des actions telles que celles qui consistent à Mettre fin à l'application et Mettre fin au processus, exécutez l'outil avec les privilèges d'administration à partir d'une invite de commande qui utilise les arguments suivants :

ConfigRemoteMgmt.exe /configwinrmuser domain\name
où nom correspond au compte du groupe de sécurité, de l'utilisateur ou de l'ordinateur.

Pour accorder les permissions nécessaires à un groupe de sécurité d'utilisateur :

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers
Pour accorder les permissions à un compte d'ordinateur spécifique :

ConfigRemoteMgmt.exe /configwinrmuser domain\DirectorServer$
Pour les actions Mettre fin au processus, Mettre fin à l'application et Observer :

ConfigRemoteMgmt.exe /configwinrmuser domain\name /all
Pour accorder des permissions à un groupe d'utilisateurs :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers /all

Pour afficher l'aide de l'outil :

ConfigRemoteMgmt.exe

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurer HDX Insight

Jul 07, 2016

Remarque : la disponibilité de cette fonctionnalité dépend de la licence de votre organisation et vos permissions d'administrateur.

HDX Insight est l'intégration de l'analyse de réseau et de la gestion des performances avec Director :

- L'analyse de réseau tire parti de HDX Insight pour fournir une vue contextuelle de l'application et du bureau du réseau. Avec cette fonctionnalité, Director fournit une analyse avancée du trafic ICA dans leur déploiement.
- La gestion des performances fournit un archivage des données d'historique ainsi que des rapports de tendance. Avec la conservation de l'historique des données par rapport à l'évaluation en temps réel, vous pouvez créer des rapports de tendance, y compris des tendances de capacité et d'intégrité.

Après avoir activé cette fonctionnalité dans Director, HDX Insight fournit des informations supplémentaires à Director :

- La page Tendances affiche des effets de latence et de bande passante pour les applications, les bureaux et les utilisateurs sur l'ensemble du déploiement.
- La page Détails de l'utilisateur affiche des informations spécifiques à la latence et à la bande passante pour une session utilisateur particulière.

Limitations

- Durée des boucles de session ICA (RTT) affiche les données correctement pour Receiver pour Windows 3.4 ou version ultérieure et Receiver pour Mac 11.8 ou version ultérieure. Pour les versions antérieures de ces Receiver, les données ne s'affichent pas correctement.
- Dans la vue Tendances, les données d'ouverture de session de connexion HDX ne sont pas collectées pour les VDA antérieurs à la version 7. Pour les VDA antérieurs, les données du graphique sont affichées en tant que 0.

Pour configurer la fonctionnalité d'analyse de réseau sur Director

Director offre l'analyse réseau par le biais de NetScaler HDX Insight pour fournir aux administrateurs d'applications et de bureaux Citrix la possibilité de résoudre et de corréler les problèmes qui peuvent être attribués à une dégradation des performances réseau.

NetScaler Insight Center doit être installé et configuré dans Director pour activer l'analyse de réseau. Insight Center est une machine virtuelle (boîtier) téléchargée à partir de Citrix.com. À l'aide de l'analyse de réseau, Director communique et rassemble les informations relatives à votre déploiement. Cette information est exploitée depuis HDX Insight, qui offre une analyse robuste du protocole Citrix ICA entre le client et l'infrastructure Citrix principale.

1. Sur le serveur sur lequel Director est installé, situez l'outil de ligne de commande DirectorConfig dans C:\inetpub\wwwroot\Director\tools, et exécutez-le avec le paramètre /configNetScaler dans l'invite de la ligne de commande.
2. Lorsque vous y êtes invité, configurez le nom de domaine complet (FQDN ou l'adresse IP) de NetScaler Insight Center, le nom d'utilisateur, le mot de passe, et le type de connexion HTTP ou HTTPS.
3. Pour vérifier les modifications, fermez votre session et rouvrez-la.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Résoudre les problèmes utilisateur

Jul 07, 2016

Utilisez la vue **Assistance** de Director (page **Gestionnaire d'activités**) pour afficher des informations sur l'utilisateur :

- Vérifiez les détails sur l'ouverture de session de l'utilisateur, la connexion et les applications.
- Observez la machine de l'utilisateur.
- Résolvez le problème avec les actions recommandées dans le tableau suivant, et, si nécessaire, informez l'administrateur du problème.

Conseils de dépannage

Problème utilisateur	Consultez ces suggestions :
L'ouverture de session prend beaucoup de temps ou échoue par intermittence ou de manière répétée	Diagnostiquer les problèmes de connexion utilisateur
L'application est lente ou ne répond pas	Résoudre les défaillances d'application
La connexion a échoué	Restaurer les connexions de bureau
La session est lente ou ne répond pas	Restaurer les sessions
La vidéo est lente ou de qualité médiocre	Exécuter des rapports sur le système du canal HDX

Remarque : pour vous assurer que la machine n'est pas en mode de maintenance, à partir de la vue Détails de l'utilisateur, vérifiez le panneau Détails de la machine.

Astuces de recherche

Lorsque vous tapez le nom de l'utilisateur dans le champ Rechercher, Director recherche des utilisateurs dans Active Directory pour les utilisateurs de tous les sites configurés pour prendre en charge Director.

Lorsque vous entrez un nom de machine à plusieurs utilisateurs dans le champ Rechercher, Director affiche les Détails de la machine pour la machine spécifiée.

Lorsque vous entrez un nom de point de terminaison dans le champ Rechercher, Director utilise les sessions authentifiées (anonymes) et non authentifiées connectées à un point de terminaison spécifique, qui permet de résoudre des sessions non authentifiés. Assurez-vous que les noms de points de terminaison sont uniques pour activer la résolution des problèmes des sessions non authentifiées.

Les résultats de la recherche incluent également les utilisateurs qui ne sont pas connectés ou attribués à une machine.

- Les recherches ne sont pas sensibles à la casse.
- Les entrées partielles produisent une liste de correspondances possibles.
- Lorsque vous entrez les premières lettres d'un nom en deux parties (nom d'utilisateur, nom de famille et prénom ou nom d'affichage), en les séparant par un espace, les résultats comprennent les correspondances pour les deux chaînes. Si vous

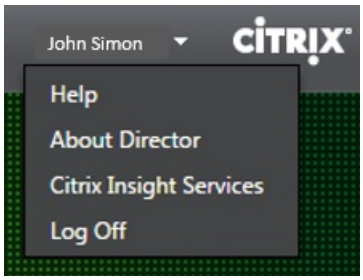
© 1999-2017 Citrix Systems, Inc. All rights reserved.

entrezjo rob, les résultats peuvent inclure des chaînes telles que « John Robertson » ou Robert, Jones.

Pour revenir à la page d'accueil, cliquez sur le logo Director.

Accéder à Citrix Insight Services

Vous pouvez accéder à Citrix Insight Services (CIS) à partir de la liste déroulante Utilisateur dans Director pour accéder à des informations de diagnostic supplémentaires. Les données disponibles dans CIS sont fournies à partir de sources telles que Call Home et Citrix Scout.



Charger les informations de dépannage auprès du support technique Citrix

Exécutez Citrix Scout à partir d'un Delivery Controller ou d'un VDA pour capturer les points de données clés et les traces Citrix Diagnostic Facility (CDF) pour dépanner les ordinateurs sélectionnés. Scout offre la possibilité de charger des données en toute sécurité vers la plate-forme Citrix Insight Services (CIS) pour aider l'assistance technique de Citrix à résoudre les problèmes. L'assistance technique de Citrix utilise la plate-forme CIS pour réduire la durée de résolution des problèmes signalés par les clients.

Scout est installé avec les composants XenApp ou XenDesktop. En fonction de la version de Windows, Scout s'affiche dans le menu Démarrer de Windows ou l'écran d'accueil lorsque vous installez ou mettez à niveau vers XenDesktop 7.1, XenDesktop 7.5, XenApp 7.5, XenDesktop 7.6, XenApp 7.6, XenDesktop 7.7 ou XenApp 7.7.

Pour démarrer Scout, à partir du menu Démarrer ou de l'écran d'accueil, sélectionnez Citrix > Citrix Scout.

Pour plus d'informations sur l'utilisation et la configuration Scout, et accéder aux questions fréquemment posées, consultez l'article CTX130147.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Observer les utilisateurs

Jul 07, 2016

À partir de Director, utilisez la fonctionnalité d'observation utilisateur pour afficher et travailler directement sur la machine virtuelle ou la session d'un utilisateur. L'utilisateur doit être connecté à la machine que vous souhaitez observer. Vérifiez ceci en vérifiant le nom de la machine dans la barre de titre utilisateur.

1. Dans la vue Détails de l'utilisateur, sélectionnez la session utilisateur.
2. Activez l'observation pour la session utilisateur sélectionnée :
   - Pour la surveillance de machine, dans la vue Gestionnaire d'activités, cliquez sur Observer.
   - Pour la surveillance de session, dans la vue Détails de l'utilisateur, situez le panneau Détails de la session et cliquez sur Observer.
3. Une fois que la connexion s'initialise, une boîte de dialogue vous invite à ouvrir ou enregistrer le fichier .msrcincident.
4. Ouvrez le fichier d'incident avec la Visionneuse de l'Assistance à distance, si elle n'est pas déjà sélectionnée par défaut. Une invite de confirmation s'affiche sur la machine utilisateur.
5. Demandez à l'utilisateur de cliquer sur Oui pour démarrer la machine ou le partage de session.

Pour un contrôle supplémentaire, demandez à l'utilisateur de partager le contrôle du clavier et de la souris.

Configurez votre navigateur Microsoft Internet Explorer pour ouvrir automatiquement le fichier Assistance à distance Microsoft téléchargé (.msra) à l'aide du le client Assistance à distance.

Pour ce faire, vous devez activer le paramètre Demander confirmation pour les téléchargements de fichiers dans l'éditeur de stratégie de groupe :

Configuration ordinateur > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Page Sécurité > Zone Internet > Demander confirmation pour les téléchargements de fichiers.

Cette option est activée par défaut pour les sites de la zone d'intranet locale. Si le site Director est en dehors de la zone intranet locale, vous pouvez ajouter manuellement le site à la zone.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Envoyer des messages aux utilisateurs

Jul 07, 2016

À partir de Director, envoyez un message à un utilisateur qui est connecté à une ou plusieurs machines. Par exemple, utilisez cette fonctionnalité pour envoyer des notifications immédiates sur des actions administratives telles que la maintenance de bureau imminente, les fermetures de session et les redémarrages de machine et les réinitialisations de profil.

1. Dans la vue Gestionnaire d'activités, sélectionnez l'utilisateur, puis cliquez sur Détails.
2. Dans la vue Détails de l'utilisateur, situez le panneau Détails de session, puis cliquez sur Envoyer un message.
3. Tapez votre message d'informations dans les champs Objet et Message, puis cliquez sur Envoyer.

Si le message n'est pas envoyé avec succès, un message de confirmation s'affiche dans Director. Si la machine de l'utilisateur est connectée, le message s'affiche.

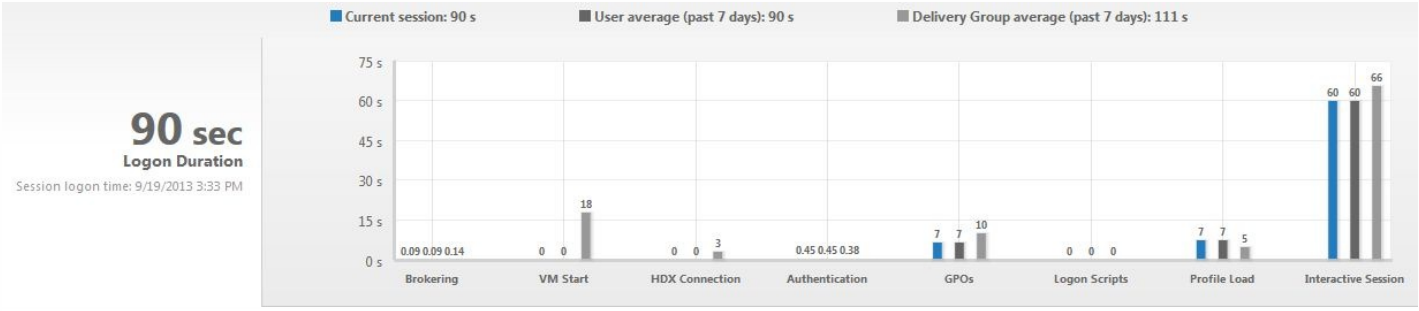
Si le message n'est pas envoyé avec succès, un message d'erreur s'affiche dans Director. Résoudre le problème en fonction du message d'erreur. Lorsque vous avez terminé, tapez le sujet et le texte du message et cliquez sur Réessayer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Diagnostiquer les problèmes de connexion utilisateur

Jul 13, 2016

Utilisez les données de durée d'ouverture de session pour résoudre les problèmes d'ouverture de session des utilisateurs. Dans la vue Détails de l'utilisateur, la durée est affichée sous forme de valeur sous laquelle s'affiche l'heure à laquelle l'ouverture de session s'est produite de même qu'un graphique des phases du processus d'ouverture de session.



Panneau Durée d'ouverture de session dans la vue Détails de l'utilisateur

Lorsque les utilisateurs ouvrent une session sur XenApp et XenDesktop, Monitor Service suit les phases du processus d'ouverture de session à partir du moment auquel l'utilisateur se connecte depuis Citrix Receiver jusqu'au moment où le bureau est prêt à être utilisé. Le nombre élevé sur la gauche représente la durée totale d'ouverture de session. Ce nombre est calculé en combinant la durée consacrée à l'établissement de la connexion et à l'obtention d'un bureau depuis le Delivery Controller avec la durée consacrée à l'authentification et à l'ouverture de session sur un bureau virtuel. Les informations de durée sont présentées en secondes (ou fractions de secondes) dans l'heure locale du navigateur Web de l'administrateur.

Utilisez ces étapes générales pour résoudre les problèmes d'ouverture de session :

1. Dans la vue **Détails de l'utilisateur**, résolvez l'état d'ouverture de session à l'aide du panneau Durée d'ouverture de session.
   - Si l'utilisateur ouvre une session, l'affichage indique le processus d'ouverture de session.
   - Si l'utilisateur est actuellement connecté, le panneau Durée d'ouverture de session affiche le temps qu'il a fallu à l'utilisateur pour se connecter à la session en cours.
2. Examinez les phases du processus d'ouverture de session.

Phases du processus d'ouverture de session	Description
Négociation des connexions	Durée requise pour décider quel bureau à attribuer à l'utilisateur.
Démarrage de VM	Si la session requiert le démarrage d'une machine, durée requise pour démarrer la machine virtuelle.
Connexion HDX	Durée requise pour effectuer les étapes permettant d'établir la connexion HDX du client vers la machine

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	virtuelle.
Authentification	Durée requise pour effectuer l'authentification sur la session distante.
GPO	Si des paramètres de stratégie de groupe sont activés sur les machines virtuelles, durée requise pour appliquer les objets de stratégie de groupe.
Scripts de connexion	Si des scripts de connexion sont configurés pour la session, durée requise pour l'exécution des scripts de connexion.
Chargement profil	Si des paramètres de profil sont configurés pour l'utilisateur ou la machine virtuelle, durée requise pour charger le profil utilisateur.
Session interactive	Durée requise pour transférer le contrôle du clavier et de la souris à l'utilisateur après chargement du profil utilisateur. De toutes les phases du processus d'ouverture de session, il s'agit généralement de la durée la plus longue. Elle est calculée comme suit : Durée de session interactive = heure à laquelle le bureau est prêt (EventId 1000 sur le VDA) - heure à laquelle le profil utilisateur est chargé (EventId 2 sur le VDA)

La durée totale d'ouverture de session n'est pas la somme exacte de ces phases. Par exemple, certaines phases se produisent en parallèle, et dans certaines phases, un traitement supplémentaire se produit pouvant entraîner une durée d'ouverture de session plus longue que la somme.

Remarque

Le graphique Durée d'ouverture de session affiche les phases d'ouverture de session en secondes. Toutes les valeurs de durée inférieures à une seconde sont affichées en tant que fraction de seconde. Les valeurs supérieures à une seconde sont arrondies à la demi-seconde la plus proche. Le graphique a été conçu pour afficher la valeur la plus élevée de l'axe Y en tant que 200 secondes. Toute valeur supérieure à 200 secondes est montrée avec la valeur réelle affichée au-dessus de la barre.

Pour identifier les valeurs inattendues ou inhabituelles dans le graphique, comparez la durée requise lors de chaque phase de la session en cours avec la durée moyenne pour cet utilisateur au cours des sept derniers jours, et avec la durée moyenne de tous les utilisateurs dans ce groupe de mise à disposition au cours des sept derniers jours.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Faites remonter le problème si nécessaire. Par exemple, si le démarrage de la machine virtuelle est lent, le problème peut provenir de l'hyperviseur, vous pouvez donc en informer l'administrateur de l'hyperviseur. Ou, si la durée de négociation est lente, vous pouvez adresser ce problème à l'administrateur de site pour vérifier l'équilibrage de charge sur le Delivery Controller.

Examinez les différences inhabituelles, notamment :

- Barres d'ouverture de session manquantes
- Écart important entre la durée actuelle et la durée moyenne de cet utilisateur. Causes potentielles :
  - Une nouvelle application a été installée.
  - Une mise à jour du système d'exploitation s'est produite.
  - Des modifications ont été apportées à la configuration.
  - La taille du profil utilisateur est élevée. Dans ce cas, le temps de chargement du profil sera élevé.
- Écart important entre le nombre d'ouvertures de session de l'utilisateur (actuel et durée moyenne) et la durée moyenne du groupe de mise à disposition.

Si nécessaire, cliquez sur **Redémarrer** pour observer le processus d'ouverture de session de l'utilisateur de manière à résoudre les problèmes, tels que le démarrage de VM ou la négociation de connexions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Résoudre les défaillances d’application

Jul 07, 2016

Dans la vue Gestionnaire d'activités, cliquez sur l'onglet Applications. Vous pouvez afficher toutes les applications sur toutes les machines auxquelles cet utilisateur a accès, y compris les applications locales et hébergées pour la machine actuellement connectée ainsi que l'état actuel de chaque.

Remarque : si l'onglet Applications est grisé, contactez un administrateur avec les permissions nécessaires à l'activation de l'onglet.

La liste contient uniquement ces applications qui ont été lancée dans la session.

Pour les machines avec OS de serveur et les machines avec OS de bureau, les applications sont répertoriées pour chaque session déconnectée. Si l'utilisateur n'est pas connecté, aucune application n'est affichée.

Action	Description
Arrêter l'application qui ne répond pas.	Choisissez l'application qui ne répond pas et cliquez sur Fermer l'application. Lorsque l'application est arrêtée, demandez à l'utilisateur de la démarrer à nouveau.
Arrêter les processus qui ne répondent pas.	Si vous avez les permissions requises, cliquez sur l'onglet Processus. Sélectionnez un processus lié à l'application ou qui utilise une quantité importante de ressources UC ou de mémoire, et cliquez sur Mettre fin au processus. Toutefois, si vous ne possédez pas les permissions nécessaires pour mettre fin au processus, une tentative d'arrêt d'un processus échouera.
Redémarrez la machine de l'utilisateur.	Pour les machines avec OS de bureau, pour la session sélectionnée, cliquez sur Redémarrer. Éventuellement, à partir de la vue de Détails de machine, utilisez la puissance des contrôles pour arrêter ou redémarrer la machine. Demandez aux utilisateurs de rouvrir une session afin que vous puissiez vérifier de nouveau l'application. Pour les machines avec OS de serveur, l'option de redémarrage n’est pas disponible. Au lieu de cela, fermez la session de l'utilisateur et laissez l'utilisateur rouvrir une session.
Placez la machine en mode de maintenance.	Si l'image de la machine nécessite une maintenance, telle que l'installation d'un correctif ou d'autres mises à jour, placez la machine en mode de maintenance et informez l’administrateur du problème. Cliquez sur la machine, et à partir de la vue Détails de machine, cliquez sur Détails et activez l'option du mode de maintenance. Informez l'administrateur du problème.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Restaurer les connexions de bureau

Jul 07, 2016

Dans Director, vérifiez le statut de connexion de l'utilisateur pour la machine courante dans la barre de titre utilisateur.

Si la connexion au bureau a échoué, l'erreur qui est la cause de l'échec est affichée et peut vous aider à résoudre le problème.

Action	Description
Assurez-vous que la machine n'est pas en mode de maintenance.	Sur la page Détails de l'utilisateur, assurez-vous que le mode maintenance est désactivé.
Redémarrez la machine de l'utilisateur.	Sélectionnez la machine et cliquez sur Redémarrer. Utilisez cette option si la machine de l'utilisateur ne répond pas ou ne parvient pas à se connecter, comme lorsque la machine utilise une quantité élevée de ressources UC, ce qui peut rendre le processeur inutilisable.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Restaurer les sessions

Jul 07, 2016

Si une session devient déconnectée, elle reste active et ses applications continuent d'être exécutées, mais la machine cliente ne communique plus avec le serveur.

Dans la vue Détails de l'utilisateur, résolvez les échecs de session dans le panneau Détails de la session. Vous pouvez afficher les détails de la session en cours, indiquée par l'ID de session.

Action	Description
Arrêtez les applications et les processus qui ne répondent pas.	Cliquez sur l'onglet Applications. Sélectionnez toute application qui ne répond pas et cliquez sur Fermer l'application. Sélectionnez également un processus correspondant qui ne répond pas et cliquez sur Arrêter le processus. Mettez également fin aux processus qui consomment une quantité de mémoire ou de ressources UC anormalement élevée, ce qui peut rendre le processeur inutilisable.
Déconnecter la session Windows.	Cliquez sur Contrôle de la session, puis sélectionnez Déconnecter. Cette option est uniquement disponible pour les machines avec OS de serveur avec broker. Pour les sessions sans broker, l'option est désactivée.
Fermez la session de l'utilisateur.	Cliquez sur Contrôle de la session, puis sélectionnez Fermer la session.

Pour tester la session, l'utilisateur peut essayer de la rouvrir. Vous pouvez également observer l'utilisateur pour surveiller plus étroitement cette session.

Remarque : si les machines utilisateur exécutent des Virtual Delivery Agent (VDA) antérieurs à la version 7, Director ne peut pas afficher d'informations complètes sur la session, et affiche à la place un message indiquant que les informations ne sont pas disponibles. Ces messages peuvent apparaître dans la page Détails de l'utilisateur et Gestionnaire d'activités.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Exécuter des rapports sur le système du canal HDX

Jul 07, 2016

Dans la vue Détails de l'utilisateur, vérifiez le statut des canaux HDX sur la machine de l'utilisateur dans le panneau HDX. Ce panneau est disponible uniquement si la machine utilisateur est connectée à l'aide de HDX.
Si un message s'affiche indiquant que les informations ne sont pas disponibles actuellement, patientez une minute afin que la page s'actualise, ou sélectionnez le bouton Actualiser. Les données HDX nécessitent un peu plus de temps pour être mises à jour que d'autres données.

Cliquez sur une icône d'erreur ou d'avertissement pour plus d'informations.

Conseil : vous pouvez afficher des informations sur les autres canaux dans la même boîte de dialogue en cliquant sur les flèches gauche situées dans le coin gauche de la barre de titre.
Les rapports du système de canal HDX sont principalement utilisés par le support technique Citrix pour résoudre davantage de problèmes.

1. Dans le panneau HDX, cliquez sur Télécharger le rapport système.
2. Vous pouvez afficher ou enregistrer le fichier de rapport .xml.
   - Pour afficher le fichier .xml, cliquez sur Ouvrir. Le fichier .xml s'affiche dans la même fenêtre que l'application Director.
   - Pour enregistrer le fichier .xml, cliquez sur Enregistrer. La fenêtre Enregistrer sous s'affiche, vous invitant à entrer un emplacement sur la machine Director dans lequel télécharger le fichier.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Réinitialiser Personal vDisk

Jul 07, 2016

Avertissement : lorsque vous réinitialisez le disque, les paramètres par défaut sont rétablis et toutes leurs données sont supprimées, y compris les applications. Les données de profil sont conservées, sauf si vous avez modifié le Personal vDisk par défaut (de redirection des profils depuis le lecteur C:), ou si vous ne disposez pas d'une solution de profil tierce.
Pour effectuer la réinitialisation, la machine possédant le Personal vDisk doit être en cours d'exécution ; cependant, l'utilisateur n'a pas besoin d'être connecté.

Cette option est uniquement disponible pour les machines avec OS de bureau ; elle est désactivée pour les machines avec OS de serveur.

1. Dans la vue Bureau d'assistance, choisissez la machine avec OS de bureau ciblée.
2. À partir de cette vue ou dans le panneau de personnalisation de la vue Détails de l'utilisateur, cliquez sur Réinitialiser Personal vDisk.
3. Cliquez sur Réinitialiser. Un message d'avertissement s'affiche indiquant à l'utilisateur que sa session va être fermée. La session de l'utilisateur est fermée (s'il en avait ouvert une) et la machine redémarre.

Si l'opération de réinitialisation est réussie, la valeur du champ Statut Personal vDisk dans le panneau de personnalisation de la vue Détails de l'utilisateur est En cours d'exécution. Si la réinitialisation échoue, un X rouge à droite de la valeur En cours d'exécution s'affiche. Lorsque vous pointez sur ce X, les informations relatives à l'erreur s'affichent.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Réinitialiser un profil utilisateur

Jul 07, 2016

Avertissement : si un profil est réinitialisé, bien que les dossiers et les fichiers de l'utilisateur sont enregistrés et copiés dans le nouveau profil, la plupart des données de profil utilisateur sont supprimées (par exemple, le Registre est réinitialisé et les paramètres d'application peuvent être supprimés).

1. À partir de Director, recherchez l'utilisateur dont vous voulez réinitialiser le profil et sélectionnez la session de cet utilisateur.
2. Cliquez sur **Réinitialiser le profil**.
3. Demandez à l'utilisateur de fermer toutes ses sessions.
4. Demandez à l'utilisateur d'ouvrir une session à nouveau. Les dossiers et fichiers qui ont été enregistrés depuis le profil de l'utilisateur sont copiés dans le nouveau profil.
   Important : si l'utilisateur possède des profils sur des plates-formes multiples (telles que Windows 8 et Windows 7), demandez à l'utilisateur de rouvrir une session tout d'abord sur le même bureau ou application que l'utilisateur a signalé comme un problème. Ceci garantit que le profil approprié est réinitialisé.
   Si le profil est un profil utilisateur Citrix, le profil est déjà réinitialisé lorsque le bureau de l'utilisateur s'affiche. Si le profil est un profil itinérant Microsoft, la restauration du dossier est peut-être toujours en cours d'exécution pendant un court instant. L'utilisateur doit rester connecté jusqu'à ce que la restauration soit terminée.

Remarque : les étapes précédentes supposent que vous utilisiez XenDesktop (VDA de bureau). Si vous utilisez XenApp (VDA de serveur), vous devez être connecté pour réinitialiser le profil. L'utilisateur doit ensuite se déconnecter et se reconnecter pour terminer la réinitialisation du profil.
Si le profil n'est pas correctement réinitialisé (par exemple, l'utilisateur ne peut pas correctement ouvrir une session à nouveau sur la machine ou certains fichiers sont manquants), vous devez manuellement restaurer le profil d'origine.
Les dossiers (et leurs fichiers) provenant du profil de l'utilisateur sont enregistrés et copiés vers le nouveau profil. Ils sont copiés dans l'ordre indiqué :

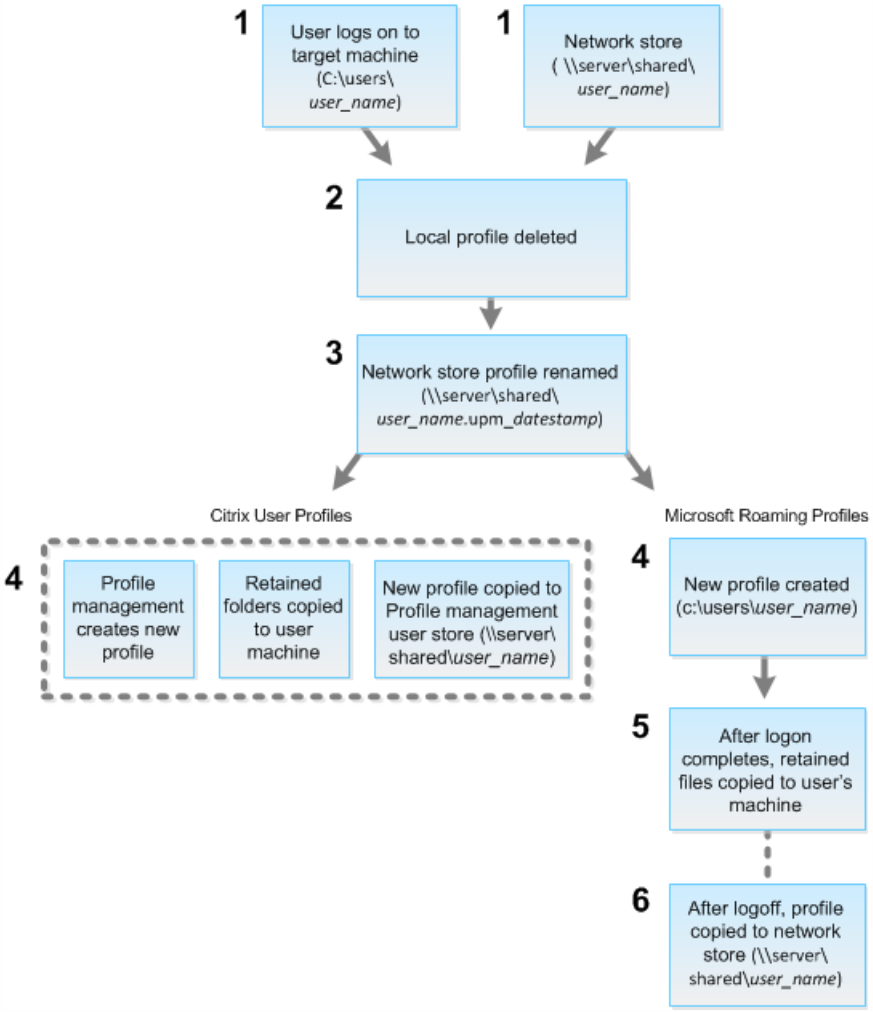
- Bureau
- Cookies
- Favoris
- Documents
- Images
- Musique
- Vidéos

Remarque : dans Windows 8 ou version ultérieure, les cookies ne sont pas copiés lorsque les profils sont réinitialisés.

Tout profil utilisateur Citrix ou profil itinérant Microsoft peut être réinitialisé. Lorsque l'utilisateur ferme sa session et que vous sélectionnez la commande de réinitialisation (dans Director ou en utilisant le kit de développement PowerShell), Director identifie d'abord le profil utilisateur en cours d'utilisation et délivre une commande de réinitialisation appropriée. Director reçoit les informations au travers de Profile Management, y compris les informations sur la taille, le type et la durée d'ouverture de session du profil.

La prochaine fois que l'utilisateur ouvre une session, ce diagramme illustre le traitement qui se produit.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. La commande de réinitialisation émise par Director spécifie le type de profil. Le service Profile Management, tente ensuite de réinitialiser un profil de ce type et recherche le partage réseau approprié (magasin de l'utilisateur). Si l'utilisateur est traité par Profile Management, mais reçoit une commande de profil itinérant, elle est rejetée (et vice versa).
2. Si un profil local est présent, il est supprimé.
3. Le profil réseau est renommé.
4. L'action suivante dépend du fait que le profil en cours de réinitialisation est un profil utilisateur Citrix ou un profil itinérant Microsoft.
   - Pour les profils utilisateur Citrix, le nouveau profil est créé à l'aide des règles d'importation de Profile Management, et les dossiers sont copiés dans le profil réseau, et l'utilisateur peut ouvrir une session normalement. Si un profil itinérant est utilisé pour la réinitialisation, tous les paramètres de registre du profil itinérant sont conservés dans le profil de réinitialisation.
     Remarque : vous pouvez configurer Profile Management de manière à ce qu'un profil modèle remplace le profil itinérant, si nécessaire.
   - Pour les profils itinérants Microsoft, un nouveau profil est créé par Windows, et lorsque l'utilisateur ouvre une session, les dossiers sont copiés vers la machine utilisateur. Lorsque l'utilisateur ferme une session, le profil est copié sur le magasin réseau.

1. Demandez à l'utilisateur de fermer toutes ses sessions.
2. Supprimez le profil local s'il existe.
3. Recherchez le dossier archivé sur le partage réseau contenant la date et l'heure ajoutées au nom du dossier, le dossier

© 1999-2017 Citrix Systems, Inc. All rights reserved.

avec une extension .upm_datestamp.

4. Supprimez le nom de profil courant ; c'est-à-dire, celui sans extension upm_datestamp.
5. Renommez le dossier d'archivage à l'aide du nom de profil original (c'est-à-dire, supprimez l'extension de date et d'heure). Vous avez retourné le profil à son état d'origine, pré-réinitialisation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Kits de développement (SDK) et API

Aug 22, 2016

Plusieurs kits de développement et API sont disponibles avec cette version.

SDK de XenApp et XenDesktop : le Kit de développement logiciel (SDK) de XenApp et XenDesktop est basé sur un certain nombre de composants logiciels enfichables Microsoft Windows PowerShell version 3.0 qui vous permettent d'effectuer les mêmes tâches que vous le feriez avec la console Studio Citrix, ainsi que les tâches que vous ne pouvez pas effectuer avec Studio uniquement.

Pour de plus amples informations, veuillez consulter Citrix Developer.

SDK de stratégie de groupe Citrix : le kit de développement de stratégie de groupe Citrix vous permet d'afficher et de configurer les paramètres et les filtres de stratégie de groupe. Il utilise un fournisseur PowerShell pour créer un lecteur virtuel qui correspond aux paramètres et filtres de la machine et de l'utilisateur. Le fournisseur apparaît sous forme d'extension de New-PSDrive. Pour utiliser le kit de développement de stratégie de groupe, soit Studio soit le kit de développement XenDesktop doit être installé. Consultez la section Kit de développement de stratégie de groupe ci-dessous pour de plus amples informations.

API Monitor Service OData : vous pouvez utiliser l'API Monitor Service OData pour :

- Analyser des tendances historiques pour la planification
- Effectuer une résolution des problèmes détaillées des échecs de connexion et de machine
- Extraire des informations afin de les envoyer dans d'autres outils et processus ; par exemple, à l'aide des tables PowerPivot de Microsoft Excel pour afficher les données de différentes manières
- Créer une interface utilisateur personnalisée en plus des données offertes par l'API

Pour de plus amples informations, consultez les articles sur l'API Monitor Service OData.

SDK XenApp et XenDesktop

À partir de la version 7.5.x, XenApp et XenDesktop partagent une architecture et une gestion unifiée : FlexCast Management Architecture. Cela signifie que XenApp offre de nombreuses fonctionnalités précédemment uniquement disponibles dans XenDesktop ; des éléments du Kit de développement logiciel (SDK) qui sont associés à des fonctionnalités communes qui s'appliquent également à XenApp et XenDesktop, même si les commandes font référence uniquement à XenDesktop.

Si vous avez de l'expérience avec le kit de développement XenDesktop 5, la liste suivante résume les différences des versions 7.x du kit de développement XenApp et XenDesktop.

- **Nouveau SDK de haut niveau** : XenDesktop 7 fournit un nouveau kit de développement de haut niveau qui vous permet de créer un script et d'automatiser la création de sites et d'effectuer une maintenance rapidement et facilement. Le kit de développement de haut niveau vous isole de la complexité des kits de développement de bas niveau, vous pouvez ainsi créer un nouveau site simplement en exécutant deux applets de commande.
- **Nouveau SDK de bas niveau** : les kits de développement de bas niveau individuels sont fournis pour les nouveaux services XenDesktop 7, y compris un SDK dédié et amélioré pour le service d'administration déléguée (DAS), qui faisait

© 1999-2017 Citrix Systems, Inc. All rights reserved.

précédemment partie du SDK Broker dans XenDesktop 5. Il existe également des kits de développement pour les nouvelles fonctionnalités, y compris le Monitor Service, Environnement de test et Journalisation de la configuration.

- **Catalogues de machine avec OS de serveur Windows et groupes de mise à disposition** : vous pouvez utiliser le kit de développement XenDesktop 7 pour mettre à disposition des applications et bureaux hébergés rentables sur des systèmes d'exploitation serveur.
- **Applications de machines avec OS de bureau** : les applications de machines avec OS de bureau ont beaucoup changé au niveau du SDK. Si vous disposez de scripts existants pour les applications en cours d'exécution sur des OS de bureau, vous devez mettre à jour ces scripts pour XenDesktop 7 comme il existe peu de compatibilité descendante.
- **Appliquer les paramètres aux machines des groupes de mise à disposition** : dans XenDesktop 7, à l'aide des emplacements de configuration, vous pouvez appliquer des paramètres à des machines dans un groupe de mise à disposition spécifique, plutôt qu'à toutes les machines d'un site. Cela vous permet de configurer, pour un groupe de mise à disposition donné, les paramètres qui s'appliquent à ce groupe. Un certain nombre d'emplacements de configuration prédéfinis sont fournis qui contiennent différents types de paramètres, tels que des paramètres pour les adresses StoreFront à utiliser avec les emplacements de serveur de publication Receiver ou App-V. Vous pouvez utiliser un ensemble de paramètres à partir d'un emplacement qui n'affectera qu'un groupe de mise à disposition particulier, et une autre collection de paramètres au même emplacement qui affectera un autre groupe de mise à disposition. Vous pouvez utiliser des noms approprié à votre déploiement particulier ; par exemple, « stratégie Service des ventes. »
- **Types de catalogue remplacés** : dans XenDesktop 7, les types de catalogues ont été remplacés par des catalogues avec des propriétés individuelles. Toutefois, pour des raisons de compatibilité, vous pouvez toujours utiliser les scripts existants qui emploient les types de catalogue, tel qu'une image unique (groupée) et clone léger (dédié), etc, mais en interne ceux-ci sont convertis en ensembles de propriétés.
  Attention : la rétrocompatibilité avec les types de catalogues XenDesktop 5 a été maintenue lorsque cela est possible et réalisable. Toutefois, lors de l'écriture de scripts, n'utilisez pas de types de catalogues ; au lieu de cela, spécifiez les catalogues avec des propriétés individuelles.

- **Objet Bureau remplacé** : dans XenDesktop 5, l'objet Bureau est l'un des types principaux d'objets du kit de développement logiciel (SDK) utilisé dans les scripts de SDK de broker. L'objet Bureau décrit la machine et la session sur la machine. Dans XenDesktop 7, cet objet est remplacé par l'objet Session et l'objet Machine, qui ont été développés pour effectuer le travail de l'objet Bureau. Toutefois, pour des raisons de rétrocompatibilité, vous pouvez toujours utiliser des scripts existants qui utilisent l'objet Bureau.
  Attention : la rétrocompatibilité avec XenDesktop 5 a été maintenue lorsque cela est possible et réalisable. Toutefois, lors de l'écriture de nouveaux scripts, n'utilisez pas l'objet Bureau ; au lieu de cela, spécifiez les objets Session et Machine.

Le kit de développement XenDesktop et la console Studio présentent des différences en termes de règles de stratégie. Les règles de stratégie d'attribution et d'affectation sont des entités indépendantes dans le kit de développement ; dans la console, ces entités ne sont pas visibles car elles sont fusionnées de manière transparente avec le groupe de mise à disposition. De plus, les règles de stratégie d'accès sont moins restrictives dans le kit de développement.

Le kit de développement logiciel comprend un certain nombre de composants logiciels enfichables PowerShell installés automatiquement par l'assistant d'installation lorsque vous installez les composants Delivery Controller ou Studio.

Autorisations : vous devez exécuter le shell ou le script avec une identité disposant de droits d'administration Citrix. Bien que les membres du groupe d'administrateurs locaux du Controller disposent automatiquement de privilèges d'administration complets pour permettre l'installation de XenApp ou XenDesktop, Citrix vous recommande, pour un fonctionnement normal, de créer des administrateurs Citrix avec les droits appropriés, plutôt que d'utiliser le compte des administrateurs locaux. Si

© 1999-2017 Citrix Systems, Inc. All rights reserved.

vous exécutez Windows Server 2008 R2, vous devez exécuter le shell ou le script en tant qu'administrateur Citrix, et non en tant que membre du groupe des administrateurs locaux.

Pour accéder aux applets de commande et les exécuter :

1. Démarrez un shell dans PowerShell 3.0 : ouvrez Studio, sélectionnez l'onglet **PowerShell** et cliquez sur **Lancer PowerShell**.
2. Pour utiliser les applets de commande du kit de développement dans des scripts, définissez la stratégie d'exécution dans PowerShell. Pour plus d'informations sur la stratégie d'exécution PowerShell, veuillez consulter votre documentation Microsoft.
3. Ajoutez les composants enfichables dont vous avez besoin à l'environnement PowerShell en utilisant l'applet de commande **Add -PSSnapin** dans la console Windows PowerShell.

    V1 et V2 indiquer la version du composant logiciel enfichable (les composants logiciels enfichables XenDesktop 5 sont à la version 1 ; les composants logiciels enfichables XenDesktop 7 sont à la version 2. Par exemple, pour installer les composants logiciels enfichables XenDesktop 7, tapez Add-PSSnapin Citrix.ADIdentity.Admin.V2). Pour importer tous les applets de commande, tapez : Add-PSSnapin Citrix.*.Admin.V*

Une fois que les composants logiciels enfichables ont été ajoutés, vous pouvez accéder aux applets de commande et à l'aide associée.

REMARQUE : pour consulter l'aide de l'applet de commande PowerShell XenApp et XenDesktop :

1. À partir de la console PowerShell, ajoutez les composants logiciels enfichables Citrix : Add – PSSnapin Citrix.*.Admin.V*.
2. Suivez les instructions fournies dans PowerShell (ISE).

Kit de développement de stratégie de groupe

Pour utiliser le kit de développement de stratégie de groupe, soit Studio soit le kit de développement XenDesktop doit être installé.

Pour ajouter le kit de développement de stratégie de groupe, tapez **Add-PSSnapin citrix.common.grouppolicy**. (Pour obtenir de l'aide, tapez : **help New-PSDrive -path localgpo:/**)

Pour créer un lecteur virtuel et le charger de paramètres, tapez : **New-PSDrive** <*Paramètres standard*> **[-PSProvider] CitrixGroupPolicy -Controller** <*chaîne*> où la chaîne de Controller correspond au nom de domaine complet d'un Controller du site auquel vous voulez vous connecter et à partir duquel vous voulez charger les paramètres.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

API Monitor Service OData

Jul 07, 2016

En plus d'utiliser la console Citrix Director pour afficher les données d'historique, vous pouvez interroger les données à l'aide de l'API de Monitor Service. Vous pouvez utiliser l'API pour :

- Analyser des tendances historiques pour la planification
- Effectuer une résolution des problèmes détaillées des échecs de connexion et de machine
- Extraire des informations afin de les envoyer dans d'autres outils et processus ; par exemple, à l'aide des tables PowerPivot de Microsoft Excel pour afficher les données de différentes manières
- Créer une interface utilisateur personnalisée en plus des données offertes par l'API

L'API de Monitor Service utilise le protocole OData (Open Data), qui est un protocole Web pour l'interrogation et la mise à jour des données, construit sur des technologies Web telles que HTTP. Pour de plus amples informations sur le protocole OData, consultez : http://www.odata.org.

Le service Moniteur de l'API est créé sur des bases de données SQL Server à l'aide de Windows Communication Foundation (WCF) Data Services qui sont remplis pendant le traitement et la consolidation. Deux points de terminaison sont exposés à l'aide de WCF avec wsHttpBinding. L'adresse de base est : http://{dc-host}/Citrix/Monitor/OData/v2. Vous pouvez également utiliser TLS pour sécuriser les points de terminaison ; voir Sécurisation de points de terminaison à l'aide de TLS pour plus d'informations.

1. Le point de terminaison des données expose l'accès en lecture seule directement vers les entités de la base de données et est accessible à l'aide du langage de requête OData. Ce point de terminaison permet un accès très assoupli en termes de filtrage et de sélection des colonnes. L'URI de l'API Data est : http://{dc-host}/Citrix/Monitor/OData/v2/Data. Pour de plus amples informations sur l'accès aux données du service Monitor, consultez la section Accès aux données à l'aide de l'API.
2. Le point de terminaison Methods expose les opérations de service qui sont utilisées par Citrix Director pour récupérer des données qui nécessitent un regroupement complexe et des performances élevées standards, telles que les requêtes sur les pages Tableau de bord et Tendances. L'URI de l'API Methods est : http://{dc-host}/Citrix/Monitor/OData/v2/Methods. Les méthodes sont uniquement utilisées dans Director lui-même et ne sont pas utilisées par la plupart des clients Citrix. Par conséquent, elles ne sont pas documentées ici.

La version de l'API incluse avec XenApp et XenDesktop 7.6 offre les nouvelles fonctionnalités suivantes :

- **Inventaire des corrections à chaud.** À l'aide de la vue Détails de l'utilisateur ou de la vue Machine dans Director, vous pouvez afficher une liste de toutes les corrections à chaud Citrix qui ont été installées sur une machine. Vous pouvez utiliser l'API pour extraire ces données et créer des rapports personnalisés (par exemple, l'état des correctifs installés sur un site entier) ou les extraire dans un moteur d'analyse. De nouvelles classes ont été introduites et la classe de Machine a été étendue pour prendre en charge le suivi des corrections Citrix installées sur le Controller et les VDA.
- **Résolution des problèmes de sessions anonymes.** Les sessions peuvent être exécutées comme un ensemble de comptes d'utilisateur local regroupés. L'API possède une nouvelle propriété IsAnonymous pour la classe Session (valeur par défaut FALSE).
- **Création de rapports d'utilisation des applications hébergées.** Director offre de nouveaux rapports de capacité qui affichent l'utilisation des applications hébergées dans le temps. L'API vous permet de créer des rapports sur les détails de chaque instance d'application en cours d'exécution dans une session utilisateur.

Toutes les mises à jour apportées aux données sont complètement documentées dans l'API de référence à l'adresse

© 1999-2017 Citrix Systems, Inc. All rights reserved.

http://support.citrix.com/help/monitorserviceapi/7.6/.

La méthode GetSessionSummary est obsolète dans cette version.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Accès aux données à l'aide de l'API

Jul 07, 2016

Les types de données suivants sont disponibles par le biais de l'API Monitor Service :

- des données liées à des échecs de connexion ;
- des machines dans un état d'échec ;
- l'utilisation de la session ;
- la durée d'ouverture de session ;
- les données d'équilibrage de charge ;
- les corrections à chaud appliquées à une machine ;
- l'utilisation de l'application hébergée.

Pour accéder à une description complète des objets de données, consultez la section http://blogs.citrix.com/2013/08/27/xendesktop-7-monitor-service-what-data-is-available/.

Pour utiliser l'API Monitor Service OData, vous devez être un administrateur XenApp ou XenDesktop. Pour appeler l'API vous avez besoin des privilèges en lecture seule ; toutefois, les données retournées sont déterminées par les rôles et les permissions de l'administrateur XenApp ou XenDesktop. Par exemple, les administrateurs du groupe de mise à disposition peuvent appeler l'API du service Monitor, mais les données qu'ils peuvent obtenir sont contrôlées par l'accès au groupe de mise à disposition configuré à l'aide de Citrix Studio. Pour plus d'informations sur les rôles et les permissions de l'administrateur XenApp ou XenDesktop, consultez la section Délégation de l'administration.

Requête des données

L'API du service Monitor de l'API du service est un API REST qui peut être accédé à l'aide d'un consommateur OData. Les consommateurs OData sont des applications qui consomment des données exposées à l'aide du protocole OData. Les consommateurs OData varient en sophistication, d'un simple navigateur Web à des applications personnalisées qui peuvent bénéficier de toutes les fonctionnalités du protocole OData. Pour de plus amples informations sur les consommateurs OData, consultez : http://www.odata.org/ecosystem#consumers.

Chaque partie du modèle de données du service service Monitor est accessible et peut être filtrée sur l'adresse URL. OData fournit un langage de requête au format de l'adresse URL que vous utilisez pour récupérer des entrées à partir d'un service. Pour de plus amples informations, veuillez consulter http://msdn.microsoft.com/en-us/library/ff478141.aspx.

La requête est traitée du côté serveur et peut être filtrée davantage en utilisant le protocole OData du côté client.

Les données modélisées peuvent être classées en trois catégories : les données agrégées (les tables de résumé), l'état actuel des objets (machines, sessions, etc.) et les données de journal, qui sont en fait des événements historiques (les connexions, par exemple).

Remarque : les énumérations ne sont pas prises en charge dans le protocole OData ; les entiers sont utilisés à la place. Pour déterminer les valeurs retournées par l'API Monitor Service OData, consultez la section http://support.citrix.com/help/monitorserviceapi/7.6/.

Agrégation des valeurs de données

Le service Monitor collecte les données, notamment l'utilisation de la session utilisateur, les détails des performances de l'ouverture de session utilisateur, les détails de l'équilibrage de charge de la session, et les informations de connexion et d'échec de machine. Les données sont agrégées différemment en fonction de leur catégorie. La compréhension de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

l'agrégation des valeurs de données présentées à l'aide de l'API OData Method est critique à l'interprétation des données. Par exemple :

- Des sessions connectées et des échecs de machine se produisent sur une certaine période de temps, par conséquent, elles sont exposées en tant que maximum sur une période de temps.
- LogOn Duration est une mesure de durée, par conséquent elle est exposée en tant que moyenne sur une période de temps.
- LogOn Count et Connection Failures représentent des nombres d'occurrences sur une période de temps, et par conséquent sont exposés en tant que sommes sur une période de temps.

Évaluation de données simultanées

Les sessions doivent se chevaucher pour être considérées comme simultanées. Toutefois, lorsque l'intervalle de temps est de 1 minute, toutes les sessions de cette minute (si elles se chevauchent ou non) sont considérées comme simultanées, la taille de l'intervalle est si petite que la surcharge de performances impliquée dans le calcul de la précision ne vaut pas la valeur ajoutée. Si les sessions se produisent dans la même heure, mais pas dans la même minute, elles ne sont pas considérées comme se chevauchant.

Corrélation des tables de synthèse avec des données brutes

Le modèle de données représente des métriques de deux manières différentes :
- Les tables de synthèse représentent des vues des mesures détaillées de l'agrégation par minute, heure et jour.
- Les données brutes représentent des événements individuels ou l'état actuel de l'objet suivi dans la session, la connexion, l'application et autres objets.

Lorsque vous tentez de corréler les données dans les appels API ou dans le modèle de données lui-même, il est important de bien comprendre les concepts et les limitations suivantes :

- **Aucune données de synthèse pour les intervalles partiels.** Des résumés de métriques sont conçus pour répondre aux besoins de tendances historiques sur de longues périodes. Les métriques sont agrégées dans la table de synthèse pour effectuer des intervalles. Il y aura pas de données de synthèse pour un intervalle partiel au début (les plus anciennes données disponibles) de la collection de données ni à la fin. Lorsque vous affichez les agrégations d'une journée (intervalle = 1 440), ceci signifie que la premier et le dernier jour incomplet ne possède pas de données. Bien que des données brutes puissent exister pour des intervalles partiels, elles ne seront jamais synthétisées. Vous pouvez déterminer le premier et le dernier intervalle d'agrégation pour une granularité de données particulière en extrayant les valeurs minimales et maximales de SummaryDate pour une table de synthèse particulière. La colonne SummaryDate représente le début de l'intervalle. La colonne Granularité représente la durée de l'intervalle pour les données agrégées.
- **Corrélation par heure.** Les métriques sont agrégées dans la table de synthèse pour terminer les intervalles comme décrit ci-dessus. Ils peuvent être utilisés pour les tendances historiques, mais les événements bruts peuvent être plus actifs dans l'état de ce qui a été résumé pour l'analyse de tendances. Toute comparaison temporelle de synthèse des données brutes doit prendre en compte le fait qu'aucune donnée de synthèse pour les intervalles partiels susceptibles de se produire ou pour le début et la fin de la période de temps.
- **Événements manqués et latents.** Les mesures qui sont agrégées dans la table de résumé peuvent être légèrement inexactes si les événements sont manqués ou latents pour la période d'agrégation. Bien que le service Monitor tente de conserver un état courant précis, il ne retourne pas dans le temps pour recalculer l'agrégation dans les tables de résumé pour les événements manqués ou latents.
- **Connexion haute disponibilité.** Lors de la haute disponibilité de connexion, il existera des espaces dans les données de synthèse du nombre de connexions actives, mais les instances de session seront toujours en cours d'exécution dans les données brutes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Périodes de rétention des données.** Les données des tables de synthèse sont conservées sur un autre programme de nettoyage différent de la planification des données brutes d'événement. Il se peut que les données soient manquantes, car elles ont été effacées depuis les tables de données de synthèse ou brutes. Les périodes de rétention peuvent également différer pour différents granularités de données de synthèse. Les données de granularité inférieures (en minutes) sont nettoyées plus rapidement que les données de granularité supérieures (en jours). Si des données sont manquantes dans une granularité à cause du nettoyage, elles peuvent être détectées dans une meilleure granularité. Étant donné que les appels API retournent uniquement la granularité demandée, l'absence de réception de données pour un niveau de granularité ne signifie pas que les données n'existent pas pour une meilleure granularité pour la même période.
- **Fuseaux horaires.** Les métriques sont stockées avec des horodatages UTC. Les tables de synthèse sont regroupées sur des limites de fuseau horaire. Pour les zones qui ne se trouvent pas dans les limites horaires, il se peut qu'il existe une différence pour laquelle les données sont agrégées.

Granularité de données et rétention

La granularité des données agrégées récupérées par Director est une fonction de la période de temps (T) demandée. Les règles sont les suivantes :

- 0 < T <= 1 heure utilise une granularité minute par minute
- 0 < T <= 30 jours utilise une granularité heure par heure
- T > 31 jours utilise une granularité jour par jour

Les données requises qui ne proviennent pas de données agrégées proviennent de la session brute et des informations de connexion. Ces données ont tendance à croître rapidement, et par conséquent, disposent de leur propre paramètre de nettoyage. Le nettoyage garantit que seules les données appropriées sont conservées à long terme. Cela garantit de meilleures performances tout en conservant la granularité nécessaire pour la création de rapports. Pour les clients qui ne possèdent pas de licence pour utiliser l'édition Platinum, le nettoyage commence le huitième jour, quel que soit le programme de rétention de nettoyage par défaut. Les clients Platinum peuvent modifier la rétention de nettoyage sur leur nombre de jours de rétention désirés, sinon, la valeur par défaut est utilisée.

Les paramètres suivants sont utilisés pour contrôler le nettoyage :

Nom du paramètre	Nettoyage affecté	Valeur par défaut (jours)	Accès à l'aide de
GroomSessionsRetentionDays	Enregistrements Session et SessionDetail	7 pour les utilisateurs non-Platinum, 90 pour Platinum	Applet de commande (set/get-monitorconfiguration)
GroomSummariesRetentionDays	Enregistrements DesktopGroupSummary, FailureLogSummary et LoadIndexSummary. Données agrégées : granularité quotidienne.	7 pour les utilisateurs non-Platinum, 90 pour Platinum	Applet de commande (set/get-monitorconfiguration)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom du paramètre	Nettoyage affecté	Valeur par défaut (jours)	Accès à l'aide de
GroomHourlyRetentionDays	Données agrégées : granularité horaire	32 jours	Monitor.Configuration Database Table. Voir la remarque ci-dessous.
GroomMinuteRetentionDays	Données agrégées : granularité par minute	3 jours	Monitor.Configuration Database Table. Voir la remarque ci-dessous.
GroomFailuresRetentionDays	Enregistrements MachineFailureLog et ConnectionFailureLog	7 pour les utilisateurs non-Platinum, 90 pour Platinum	Applet de commande (set/get-monitorconfiguration)
GroomLoadIndexesRetentionDays	Enregistrements LoadIndex	7 pour les utilisateurs non-Platinum, 90 pour Platinum	Applet de commande (set/get-monitorconfiguration)
GroomDeletedRetentionDays	Les entités Machine, Catalog, DesktopGroup et Hypervisor qui possèdent un LifecycleState « Supprimé ». Cette opération supprimera également tout enregistrement Session, SessionDetail, Summary, Failure ou LoadIndex.	7 pour les utilisateurs non-Platinum, 90 pour Platinum	Applet de commande (set/get-monitorconfiguration)
GroomMachineHotfixHistoryRetentionDays	Corrections à chaud appliquées aux machines VDA et Controller	90 pour les utilisateurs non-Platinum et Platinum	Applet de commande (set/get-monitorconfiguration)

Avertissement : la modification des valeurs de la base de données du service Monitor nécessite le redémarrage du service pour que les nouvelles valeurs prennent effet. Vous êtes invités à apporter des modifications à la base de données du service Monitor uniquement avec l'assistance de Citrix.

La conservation de données pendant de longues périodes aura les conséquences suivantes sur la taille des tables :

- **Données horaires.** Si les données horaires sont autorisées à rester dans la base de données pour un maximum de deux années, un site de 1 000 groupes de mise à disposition peut influencer la croissance de la base de données comme suit : 1 000 groupes de mise à disposition x 24 heures/jour x 365 jours/an x 2 ans = 17 520 000 lignes de données. L'impact sur les performances d'une telle quantité importante de données dans les tables d'agrégation est significatif. Étant donné

© 1999-2017 Citrix Systems, Inc. All rights reserved.

que les données du tableau de bord sont tirées de cette table, la configuration requise sur le serveur de base de données peut être importante. Il se peut que des quantités excessives de données aient un impact dramatique sur les performances.

- **Données de session et d'événement.** Ce sont les données collectées chaque fois qu'une session est démarrée et qu'une connexion/reconnexion est effectuée. Pour un site important (100 000 utilisateurs), ces données vont s'accroître très rapidement. Par exemple, l'équivalent de deux ans de tables rassemblerait plus d'un To de données nécessitant une base de données d'entreprise de haut au niveau.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sécurisation de points de terminaison à l'aide de TLS

Jul 07, 2016

Ce document explique comment utiliser TLS pour sécuriser les points de terminaison de l'API Monitor Service OData. Si vous choisissez d'utiliser TLS, vous devez configurer TLS sur tous les Delivery Controllers dans le site ; vous ne pouvez pas utiliser un mélange de TLS et non TLS.

Pour sécuriser les points de terminaison Monitor Service à l'aide de TLS, vous devez réaliser la configuration suivante. Des étapes doivent être effectuées une seule fois par site, d'autres doivent être exécutées à partir de chaque machine hébergeant Monitor Service dans le site. Les étapes sont décrites ci-dessous.

Partie 1 : enregistrement du certificat avec le système

1. Créez un certificat utilisant un gestionnaire de certificat approuvé. Le certificat doit être associé avec le port sur la machine que vous souhaitez utiliser pour OData TLS.
2. Configurez Monitor Service pour utiliser ce port pour la communication TLS. Les étapes dépendent de votre environnement et de la manière dont il fonctionne avec les certificats. L'exemple suivant illustre comment configurer le port 449 :

- Associez le certificat avec un port :
  netsh http add sslcert ipport=0.0.0.0:449 certhash=97bb629e50d556c80528f4991721ad4f28fb74e9 appid='{00000000-0000-0000-0000-000000000000}'
  Conseil : dans une fenêtre de commande PowerShell, assurez-vous de placer des guillemets simples autour du GUID du appID, comme illustré ci-dessus, ou la commande ne fonctionnera pas. Notez qu'un saut de ligne a été ajouté à cet exemple à des fins de lisibilité uniquement.

Partie 2 : modifier les paramètres de configuration de Monitor Service

1. À partir de n'importe quel Delivery Controller dans le site, exécutez les commandes PowerShell suivantes une seule fois. Ceci supprime l'enregistrement de Monitor Service par le service de configuration.
   asnp citrix.* $serviceGroup = get-configregisteredserviceinstance -servicetype Monitor | Select -First 1 ServiceGroupUid remove-configserviceGroup -ServiceGroupUid $serviceGroup.ServiceGroupU
2. Effectuez les opérations suivantes sur tous les contrôleurs du site :
   - À l'aide d'une invite cmd, accédez au répertoire Citrix Monitor installé (généralement dans C:\Program Files\Citrix\Monitor\Service). Dans ce répertoire, exécutez :
     Citrix.Monitor.Exe -CONFIGUREFIREWALL -ODataPort 449 -RequireODataSsl
   - Exécutez les commandes PowerShell suivantes :
   asnp citrix.* (if not already run within this window) get-MonitorServiceInstance | register-ConfigServiceInstance Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-MonitorServiceGro

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Exemples

Jul 07, 2016

Les exemples suivants expliquent comment exporter des données Monitor Service à l'aide de l'API OData.

Exemple 1 : données XML brutes

1. Placez l'adresse URL de chaque série de données dans un navigateur Web exécuté avec des permissions d'administration appropriées pour le site XenApp ou XenDesktop. Citrix vous recommande d'utiliser le navigateur Chrome avec le composant logiciel enfichable Advanced Rest Client.
2. Affichez la source.

Exemple 2 : PowerPivot avec Excel

Ces instructions supposent que vous avez déjà installé Microsoft Excel et PowerPivot.

Ouvrez Excel (exécuté avec les permissions d'administration appropriées pour le site XenApp ou XenDesktop).

Si vous utilisez Excel 2010 :

1. Cliquez sur l'onglet PowerPivot.
2. Cliquez sur la fenêtre PowerPivot.
3. Cliquez sur **À partir de flux de données** dans le ruban.
4. Choisissez un nom convivial de connexion (par exemple : XenDesktop Monitoring Data) et entrez l'adresse URL du flux de données : http://{dc-host}/Citrix/Monitor/OData/v2/Data (ou https: si vous utilisez TLS).
5. Cliquez sur **Next**.
6. Sélectionnez les tables que vous voulez importer dans Excel et cliquez sur **Terminer**. Les données sont récupérées.
7. Vous pouvez maintenant utiliser PowerPivot pour visualiser et analyser les données avec des tableaux croisés dynamiques et des graphiques croisés dynamiques. Pour de plus amples informations, consultez Learning Center : http://www.microsoft.com/fr-fr/2/LearningCenter.aspx

Si vous utilisez Excel 2013 :

1. Cliquez sur l'onglet Données.
2. Choisissez À partir d'autres sources > À partir de flux de données OData
3. Entrez l'adresse URL du flux de données : http://{dc-host}/Citrix/Monitor/OData/v1/Data (ou https: si vous utilisez TLS) et cliquez sur **Suivant**.
4. Sélectionnez les tables que vous voulez importer dans Excel et cliquez sur **Suivant**.
5. Acceptez les noms par défaut ou les noms personnalisés et cliquez sur **Terminer**.
6. Choisissez **Connexion uniquement** ou **Rapport du tableau croisé dynamique**. Les données sont récupérées.
7. Vous pouvez maintenant utiliser PowerPivot pour visualiser et analyser les données avec des tableaux croisés dynamiques et des graphiques croisés dynamiques. Pour de plus amples informations, consultez Learning Center : http://www.microsoft.com/fr-fr/2/LearningCenter.aspx

Exemple 3 : LINQPad

Ces instructions supposent que vous avez déjà installé LINQPad.

1. Exécutez LinqPad avec les permissions administratives appropriées pour le site XenApp ou XenDesktop.
   Conseil : la manière la plus facile est de le télécharger, l'installer et l'exécuter sur le Delivery Controller.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Cliquez sur Ajouter un lien de connexion.
3. Choisissez WCF Data Services 5.1 (OData 3) et cliquez sur **Suivant**.
4. Entrez l'adresse URL du flux de données : http://{dc-host}/Citrix/Monitor/OData/v2/Data (ou https: si vous utilisez TLS). Si nécessaire, entrez le nom d'utilisateur et un mot de passe pour accéder à Delivery Controller. Cliquez sur **OK**.
5. Vous pouvez maintenant exécuter des requêtes LINQ sur le flux de données et exporter les données requises selon vos besoins. Par exemple, cliquez avec le bouton droit de la souris sur les catalogues et choisissez **Catalogs.Take (100)**. Ceci retourne les 100 premiers catalogues dans la base de données. Choisissez Exporter > Exporter vers Excel tout en conservant votre formatage.

Pour obtenir des exemples supplémentaires de l'utilisation de l'API avec LINQPad, consultez la section http://blogs.citrix.com/2014/01/14/creating-director-custom-reports-for-monitoring-xendesktop/.

© 1999-2017 Citrix Systems, Inc. All rights reserved.