Interface Web 5.4

2015-05-07 20:30:26 UTC

Sommaire

Interface Web 5.4

Mise à jour : 2014-11-25

L'Interface Web permet aux utilisateurs d'accéder aux applications et contenus XenApp ainsi qu'aux bureaux virtuels XenDesktop. Les utilisateurs accèdent à leurs ressources via un navigateur Web standard ou par l'intermédiaire de Citrix Online Plug-in.

Dans cette section

Cette section de la bibliothèque propose des informations mises à jour sur l'installation, la configuration et l'administration de l'Interface Web, dont les rubriques suivantes :

Fichier Lisez-moi de l'Interface Web 5.4	Informations sur les mises à jour de dernière minute et problèmes connus.
Problèmes résolus dans l'Interface Web 5.4	Détails des problèmes corrigés par rapport à la dernière version de l'Interface Web.
Fonctionnalités de l'Interface Web	Présentation de l'Interface Web.
Nouveautés	Présentation des nouvelles fonctionnalités.
Composants de l'Interface Web	Description d'un déploiement Interface Web.
Configuration requise pour l'Interface Web	Conditions relatives aux logiciels, à la configuration, au serveur Web, aux utilisateurs et aux machines.
Installation de l'Interface Web	Installation de l'Interface Web et configuration de votre serveur Web.
Démarrage de l'Interface Web	Création et configuration des sites Interface Web.
Gestion des serveurs et des batteries	Configuration et gestion des paramètres de serveur et des communications avec les batteries de serveur.
Configuration de l'authentification pour l'Interface Web	Configuration de l'authentification entre l'Interface Web, les batteries de serveurs et les plug-ins Citrix.
Gestion des clients	Déploiement et utilisation des plug-ins Citrix avec l'Interface Web.
Gestion de l'accès sécurisé	Configuration et gestion de l'accès aux sites.
Modification des paramètres du proxy côté client	Configuration des clients Citrix et des serveurs exécutant XenApp ou XenDesktop via des serveurs proxy.
Personnalisation de l'affichage pour les utilisateurs	Personnaliser l'affichage de l'Interface Web pour les utilisateurs.
Gestion des préférences de session	Spécifier les paramètres que les utilisateurs peuvent régler.

Configuration du contrôle de l'espace de travail	Autoriser les utilisateurs à se déconnecter, se reconnecter et fermer la session de ressources rapidement.
Configuration de la sécurité de l'Interface Web	Sécuriser vos données dans un environnement Interface Web.
Configuration de sites à l'aide du fichier de configuration	Administrer les sites Interface Web à l'aide des fichiers de configuration.
Configuration de la prise en charge d'ADFS pour l'Interface Web	Créer et configurer des sites Interface Web intégrés Active Directory Federation Services (ADFS).

Fichier Lisez-moi de l'Interface Web 5.4

Version du fichier lisez-moi : 1.0

Table des matières

Documentation connexe

Pour obtenir une liste des problèmes liés aux clients susceptibles d'affecter les utilisateurs de l'Interface Web, consultez les fichiers Lisez-moi des clients Citrix actuellement déployés auprès de vos utilisateurs.

Pour obtenir une liste des problèmes résolus dans cette version, consultez l'article du centre de connaissances http://support.citrix.com/article/CTX124164.

Pour accéder à la documentation sur le système de licences, ouvrez la rubrique Obtenir une licence pour votre produit.

Assistance technique

Citrix fournit une assistance technique par le biais du réseau de partenaires Citrix Solutions Advisor. Contactez votre revendeur pour obtenir une assistance directe ou utilisez l'assistance technique en ligne de Citrix pour trouver le partenaire Citrix Solutions Advisor le plus proche.

Citrix offre des services d'assistance technique en ligne sur le site Web d'assistance de Citrix. La page Support comprend des liens vers les téléchargements, le centre de connaissances Citrix, les services de conseil Citrix et d'autres pages d'assistance utiles.

Problèmes connus dans cette version

La liste suivante contient les problèmes connus de cette version. **Veuillez lire ces informations attentivement avant d'installer ce produit.**

- Les icônes ne s'affichent pas correctement sur les machines qui exécutent WinCE 6.0 WFR3 et Internet Explorer 6
- Une erreur utilisateur peut se produire lorsque des bureaux publiés sont ajoutés aux favoris d'Internet Explorer

- Un message d'erreur s'affiche lorsqu'un utilisateur tente de se connecter à l'aide de clients obsolètes
- Citrix Online Plug-in ne peut pas être mis à jour sur les machines exécutant des systèmes d'exploitation Windows Embedded
- L'utilisation de Kerberos échoue lors de la configuration de la délégation sur des serveurs XenApp exécutant Windows Server 2008
- Impossible de démarrer le bureau virtuel lors de l'accès à l'Interface Web à partir de machines exécutant Windows Embedded CE 6.0
- Le contrôle de l'espace de travail et la mise à niveau du client ne sont pas disponibles pour les utilisateurs de Firefox 3.6
- Le contrôle de l'espace de travail n'est pas disponible sur certaines machines exécutant Windows Mobile 6.1
- Le contrôle de l'espace de travail est parfois indisponible sur certaines machines exécutant Windows Embedded CE 6.0 R2
- L'authentification unique avec carte à puce à partir d'Access Gateway ne peut pas être utilisée avec XenApp 6.0

Les icônes ne s'affichent pas correctement sur les machines qui exécutent WinCE 6.0 WFR3 et Internet Explorer 6

Les icônes au format .png ne s'affichent pas correctement lorsqu'elles apparaissent sur des machines exécutant Internet Explorer 6 avec WinCE 6.0 WFR3 (HotFix 3 build 664). Pour résoudre ce problème, utilisez Internet Explorer version 5 ou antérieure. Pour afficher des fichiers .png dans Internet Explorer 6, vous pouvez également consulter la solution décrite dans l'article Microsoft http://support.microsoft.com/kb/294714.

[#41839]

Les utilisateurs ne peuvent pas ajouter d'applications et de bureaux publiés aux favoris d'Internet Explorer

Les utilisateurs peuvent rencontrer des problèmes lors de l'ajout d'applications et de bureaux publiés aux favoris d'Internet Explorer. Dans certaines situations, le titre du lien vers le favori sera incorrect et ne fonctionnera pas. Pour ajouter des applications aux favoris, cliquez avec le bouton droit sur l'icône de l'application. Pour ajouter des bureaux, cliquez avec le bouton droit sur le texte de titre du bureau.

[#244446]

Un message d'erreur s'affiche lorsqu'un utilisateur tente de se connecter à l'aide de clients obsolètes

Cette version de l'Interface Web ne prend pas en charge l'utilisation de clients antérieurs à la version 7.0. Lorsque vous tentez de vous connecter à une application à distance à l'aide d'un client antérieur, il est possible que le message d'erreur suivant s'affiche : « 50 : la connexion au serveur a échoué. ». Pour éviter ce problème, il suffit de mettre à niveau vers la dernière version des clients. Si cela n'est pas possible, vous pouvez modifier les fichiers .ica modèles comme suit pour éviter que l'erreur ne se produise :

1. À l'aide d'un éditeur de texte tel que Notepad, ouvrez les fichiers suivants : default.ica, bandwidth_high.ica, bandwidth_low.ica, bandwidth_medium.ica et bandwidth_medium_high.ica. Ces fichiers se trouvent en général dans le répertoire C:\inetpub\wwwroot\Citrix*Nomdusite*\conf sous IIS et le répertoire WEB-INF du site Interface Web sous les serveurs d'application Java.

2. Localisez et supprimez les lignes suivantes dans chaque fichier :

   DoNotUseDefaultCSL=On
   BrowserProtocol=HTTPonTCP
   LocHttpBrowserAddress=!

[#163695]

Citrix Online Plug-in ne peut pas être mis à jour sur les machines exécutant des systèmes d'exploitation Windows Embedded

L'Interface Web propose d'installer ou de mettre à niveau Citrix Online Plug-in sur les machines exécutant des systèmes d'exploitation Windows Embedded, mais l'installation échoue. Vous pouvez éviter ce problème en installant manuellement la dernière version de Citrix Online Plug-in sur la machine intégrée. Si cela n'est pas possible, vous pouvez modifier les paramètres du site pour empêcher l'affichage de ces légendes d'installation :

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Déploiement du client. Pour les sites proposant uniquement des applications en ligne, sélectionnez la case Client natif et cliquez sur Propriétés.

4. Cliquez sur Détection de client.

5. Décochez la case Offrir des mises à niveau pour les clients et sélectionnez Uniquement lorsque l'accès aux ressources est impossible ou Jamais.

[#164709]

L'utilisation de Kerberos échoue lors de la configuration de la délégation sur des serveurs XenApp exécutant Windows Server 2008

En raison d'un problème avec Windows Server 2008, si vous configurez Active Directory afin d'utiliser uniquement Kerberos pour l'authentification lors de l'approbation de serveurs XenApp pour la délégation, l'authentification échoue. Ce problème se produit sur des serveurs XenApp exécutant Windows Server 2008 avec Service Pack 2, Windows Server 2008 x64 Editions avec Service Pack 2 et Windows Server 2008 R2. Pour activer l'intégration ADFS et l'authentification unique avec carte à puce à partir d'Access Gateway avec des serveurs XenApp exécutant Windows Server 2008, sélectionnez le paramètre Utiliser n'importe quel protocole d'authentification plutôt que le paramètre N'utiliser que Kerberos comme indiqué dans la documentation. [#169269]

Impossible de démarrer le bureau virtuel lors de l'accès à l'Interface Web à partir de machines exécutant Windows Embedded CE 6.0

Dans certains cas, les utilisateurs de clients légers WYSE V30LE qui exécutent Windows Embedded CE 6.0 et Internet Explorer 6.*x* ne peuvent pas démarrer le bureau lorsqu'ils se connectent à un site XenApp Web et qu'ils cliquent sur un lien de texte pour démarrer un bureau virtuel. Pour éviter ce problème, il suffit de cliquer sur l'icône adjacente au lien de texte pour démarrer le bureau. [#218317]

Le contrôle de l'espace de travail et la mise à niveau du client ne sont pas disponibles pour les utilisateurs de Firefox 3.6

En raison d'une modification apportée à Mozilla Firefox 3.6, le contrôle de l'espace de travail est automatiquement désactivé pour les utilisateurs qui accèdent à l'Interface Web avec ce navigateur. Par ailleurs, le processus de détection et de déploiement de client ne peut pas détecter les numéros de version des clients Citrix installés par les utilisateurs de Firefox 3.6, il lui est donc impossible de mettre les clients des utilisateurs à niveau. [#230068]

Le contrôle de l'espace de travail n'est pas disponible sur certaines machines exécutant Windows Mobile 6.1

Dans certains cas, les utilisateurs de périphériques portables HP iPAQ 910c exécutant Windows Mobile 6.1 Professional et Internet Explorer Mobile peuvent se rendre compte que le contrôle de l'espace de travail ne fonctionne pas correctement lorsqu'ils se connectent à un site XenApp Web. [#230580]

Le contrôle de l'espace de travail est parfois indisponible sur certaines machines exécutant Windows Embedded CE 6.0 R2

Dans certains cas, les utilisateurs de clients légers HP t5540 exécutant Windows Embedded CE 6.0 R2 et Internet Explorer 6.*x* peuvent se rendre compte, lorsqu'ils se connectent à un site XenApp Web, que le contrôle de l'espace de travail ne fonctionne pas correctement lorsqu'ils cliquent sur le bouton Se reconnecter. [#230654]

L'authentification unique avec carte à puce à partir d'Access Gateway ne peut pas être utilisée avec XenApp 6.0

À cause d'un problème avec XenApp 6.0, les utilisateurs de carte à puce ouvrant une session sur des sites intégrés Access Gateway ne sont pas capables d'accéder aux ressources lorsque la fonctionnalité Authentification unique avec carte à puce depuis Access Gateway est activée. Les utilisateurs qui cliquent sur un lien pour accéder à une ressource délivrée par XenApp 6.0 rencontrent le message d'erreur suivant : « Une erreur s’est produite lors de l'établissement de la connexion requise ». Vous pouvez éviter ce problème en configurant le site de manière à inviter les utilisateurs de cartes à puce à entrer leur code PIN chaque fois qu'ils accèdent à une ressource. [#230942]

http://www.citrix.com/

Administration de l'Interface Web

L'Interface Web permet aux utilisateurs d'accéder aux applications et contenus XenApp ainsi qu'aux bureaux virtuels XenDesktop. Les utilisateurs accèdent à leurs ressources via un navigateur Web standard ou par l'intermédiaire de Citrix Online Plug-in.

L'Interface Web utilise les technologies Java et .NET exécutées sur un serveur Web pour créer, de manière dynamique, une représentation HTML des batteries de serveurs pour les sites XenApp Web. Toutes les ressources publiées (applications, contenu et bureaux) dans la ou les batterie(s) que vous avez mis à disposition sont proposées aux utilisateurs. Vous pouvez créer des sites Web autonomes afin d'accéder aux ressources ou des sites Web intégrés au portail de votre entreprise. Par ailleurs, l'Interface Web vous permet de configurer des paramètres pour les utilisateurs qui accèdent aux ressources via Citrix Online Plug-in.

Vous pouvez créer et configurer des sites Interface Web sur Microsoft Internet Information Services (IIS) à l'aide de la console de gestion de l'Interface Web Citrix. La console est uniquement installée avec l'Interface Web pour Microsoft Internet Information Services. Pour plus d'informations sur l'utilisation de cet outil, veuillez consulter la section Configuration de sites à l'aide de la console de gestion de l'Interface Web Citrix.

Vous pouvez également modifier le fichier de configuration de site (WebInterface.conf) afin de gérer et administrer les sites Interface Web. Pour plus d'informations, veuillez consulter la section Configuration de sites à l'aide des fichiers de configuration.

En outre, vous pouvez personnaliser et développer les sites XenApp Web. La documentation relative au kit de développement de l'Interface Web explique comment configurer des sites à l'aide de ces méthodes.

Fonctionnalités de l'Interface Web

Les deux types de sites Interface Web permettent de fournir à vos utilisateurs différentes méthodes d'accès aux ressources, ce qui leur permet de choisir la méthode qui leur convient le mieux.

Sites XenApp Web. Vous pouvez fournir aux utilisateurs un site Web auquel ils peuvent se connecter à l'aide d'un navigateur Web. Une fois authentifiés, ils peuvent accéder aux ressources en mode connecté et aux applications en mode déconnecté à l'aide d'un client Citrix.

Sites XenApp Services. Vous pouvez utiliser Citrix Online Plug-in en conjonction avec l'Interface Web pour intégrer les ressources aux bureaux des utilisateurs. Les utilisateurs accèdent aux applications, bureaux virtuels et contenus en mode connecté en cliquant sur des icônes situées sur leur bureau, sur le menu Démarrer ou dans la zone de notification de leur bureau. Vous pouvez spécifier les options de configuration auxquelles les utilisateurs ont accès, de sorte qu'ils puissent modifier, par exemple, les paramètres audio, d'affichage ou d'ouverture de session.

Fonctions de gestion

Mise à jour : 2014-11-24

Prise en charge de plusieurs batteries de serveurs. Vous pouvez configurer plusieurs batteries de serveurs et permettre aux utilisateurs de visualiser les ressources mises à leur disposition à partir de toutes les batteries. Vous pouvez configurer chaque batterie de serveurs individuellement au moyen de la tâche Batteries de serveurs dans la console de gestion de l'Interface Web Citrix. Pour plus d'informations, veuillez consulter la section Configuration de sites à l'aide du fichier de configuration.

Récupération d'urgence. Vous pouvez spécifier des batteries de serveurs XenApp et XenDesktop à utiliser lorsque les utilisateurs ne peuvent pas accéder à leurs batteries de production, en raison d'une panne de courant ou d'un problème réseau. Cela vous permet de parer à toute interruption de l'accès aux serveurs de production de façon à ce que les applications ou bureaux métier ne soient jamais indisponibles.

Configuration de site partagée. L'Interface Web pour Microsoft Internet Information Services permet de spécifier un site « maître » dont le fichier de configuration est partagé sur le réseau. Ainsi, plutôt que d'utiliser la configuration d'un fichier local, d'autres sites peuvent être configurés à l'aide de la configuration du site maître.

Compatibilité avec les technologies Web les plus répandues. L'API de l'Interface Web est accessible à partir d'ASP.NET de Microsoft et de JavaServer Pages de Sun Microsystems. L'Interface Web pour les serveurs d'application Java est indépendante de la plate-forme, ce qui lui permet d'être installée sur des systèmes d'exploitation Windows sur lesquels Microsoft Internet Information Services (IIS) n'est pas utilisé en tant que serveur Web.

Fonctionnalités d'accès aux ressources

XenApp VM hosted apps. XenApp peut mettre à disposition des applications en mode connecté à partir de machines virtuelles. Cela vous permet de publier des applications incompatibles avec les services Bureau à distance ou qui n'ont pas encore été validées pour ces derniers, ou des applications dont l'installation n'est pas prise en charge sur les systèmes d'exploitation Windows Server.

Itinérance des utilisateurs. Vous pouvez associer des groupes d'utilisateurs avec des batteries de serveurs spécifiques pour offrir aux utilisateurs une expérience cohérente, quel que soit l'endroit où ils se trouvent où le serveur auquel ils sont connectés. Cela permet aux utilisateurs qui voyagent à l'étranger, d'ouvrir une session au serveur Interface Web local et de recevoir automatiquement des ressources dans leur langue maternelle à partir d'une batterie située dans leur pays d'origine.

Prise en charge des batteries UNIX. La prise en charge des batteries XenApp pour UNIX permet à l'Interface Web d'afficher et de proposer des applications s'exécutant sur des plates-formes UNIX, sur vos machines utilisateur.

Prise en charge d'Active Directory et des noms d'utilisateur principal. Tous les composants de l'Interface Web sont compatibles avec Microsoft Active Directory. Les utilisateurs qui visitent les sites XenApp Web peuvent ouvrir une session sur les batteries de serveurs faisant partie d'un déploiement Active Directory et accéder de manière transparente aux applications et au contenu. Les écrans d'ouverture de session sont compatibles avec l'utilisation des noms UPN par Active Directory.

Utilisateurs anonymes. L'Interface Web permet aux utilisateurs d'accéder aux applications XenApp en ouvrant une session aux sites XenApp Web à l'aide d'un compte anonyme.

Fonctions de sécurité

Prise en charge de SSL/TLS. L'Interface Web prend en charge le protocole SSL afin de garantir la sécurisation des communications entre le serveur de l'Interface Web et les batteries de serveurs. La mise en œuvre de SSL sur votre serveur Web avec des navigateurs Web prenant en charge SSL permet d'assurer la sécurité des flux de données sur votre réseau. L'Interface Web utilise Microsoft .NET Framework pour implémenter SSL et la cryptographie.

Prise en charge d'Access Gateway. Citrix Access Gateway est un boîtier VPN (virtual private network) SSL universel qui, lorsqu'il est utilisé avec l'Interface Web, garantit un accès unique et sécurisé à toute ressource d'informations (données et voix). Access Gateway regroupe les meilleures fonctionnalités d'Internet Protocol Security (IPSec) et du VPN SSL, en évitant la mise en œuvre et la gestion lourdes et coûteuses ; il fonctionne à travers tous les pare-feu et prend en charge toutes les ressources et tous les protocoles.

Prise en charge de Secure Gateway. Utilisé en conjonction avec l'Interface Web, Secure Gateway offre un point d'accès unique, sécurisé et crypté aux serveurs sur vos réseaux d'entreprise internes via Internet. Secure Gateway simplifie la gestion des certificats, un certificat de serveur étant uniquement requis sur le serveur Secure Gateway, plutôt que sur chaque serveur de la batterie.

Prise en charge des cartes à puce. L'Interface Web prend en charge l'utilisation de cartes à puce pour l'authentification utilisateur afin d'offrir un accès sécurisé aux applications, contenus et bureaux. L'utilisation de cartes à puce simplifie le processus d'authentification tout en améliorant la sécurité de l'ouverture de session.

Tickets. Cette fonctionnalité renforce la sécurité de l'authentification. L'Interface Web obtient des tickets qui authentifient les utilisateurs auprès des ressources. Les tickets possèdent une date d'expiration configurable et sont valides pour une seule ouverture de session. Après utilisation ou après expiration, un ticket n'est plus valide et ne peut pas être utilisé pour accéder à des ressources. L'utilisation des tickets élimine l'inclusion explicite des informations d'identification dans les fichiers .ica utilisés par l'Interface Web pour se connecter à des ressources.

Secure Ticket Authorities redondantes. Vous pouvez configurer de multiples Secure Ticket Authorities (STA) redondantes pour les utilisateurs qui accèdent à leurs ressources à l'aide d'Access Gateway. Cela permet de vous prémunir contre toute indisponibilité d'une STA au cours d'une session utilisateur, qui empêcherait la reconnexion à la session. Lorsque la redondance est activée, l'Interface tente d'obtenir et de délivrer à la passerelle deux tickets provenant de deux STA différentes. Si l'une des STA ne peut pas être contactée lors d'une session utilisateur, la session continue à l'aide de la deuxième STA sans aucune interruption.

Modification du mot de passe. Les utilisateurs qui ouvrent des sessions à l'Interface Web ou à Citrix Online Plug-in à l'aide d'informations d'identification de domaine explicites ont la possibilité de modifier leur mot de passe Windows quand ce dernier expire. Ils peuvent modifier leur mot de passe, que l'ordinateur appartienne ou non au domaine auprès duquel ils tentent de s'authentifier.

Libre-service de compte. L'intégration à la fonctionnalité de libre-service de compte disponible sur Citrix Password Manager permet aux utilisateurs de réinitialiser leur mot de passe réseau et de déverrouiller leur compte en répondant à une série de questions de sécurité.

Fonctions de déploiement de clients

Installation des clients par le Web. Lorsqu'un utilisateur visite un site XenApp Web, l'Interface Web détecte le type de machine et de navigateur Web, et invite l'utilisateur à installer un client Citrix approprié, à condition bien sûr qu'un client soit disponible. Les restrictions de sécurité renforcées mises en place dans les systèmes d'exploitation et navigateurs Web de dernière génération peuvent complexifier le téléchargement et le déploiement de clients Citrix. C'est la raison pour laquelle l'Interface Web dispose d'un processus de détection et de déploiement de client dont la tâche consiste à guider les utilisateurs tout au long de la procédure de déploiement, qui peut inclure le cas échéant, la reconfiguration de leur navigateur Web. Ce processus permet de garantir une expérience optimale pour les utilisateurs qui accèdent à des ressources et à du contenu, et ce, même à partir d'environnements ultra-sécurisés.

Prise en charge de Citrix Online Plug-in. Citrix Online Plug-in permet aux utilisateurs d'accéder aux ressources directement à partir de leurs bureaux, sans avoir recours à un navigateur Web. L'interface utilisateur de Citrix Online Plug-in peut également être « verrouillée » pour éviter toute erreur de configuration par l'utilisateur.

Prise en charge de Citrix Offline Plug-in. Citrix Offline Plug-in permet aux utilisateurs de livrer des applications XenApp en streaming sur leurs bureaux et de les ouvrir localement. Vous pouvez soit installer le plug-in avec Citrix Online Plug-in afin de fournir la totalité des fonctionnalités de virtualisation d'application côté client de Citrix, soit n'installer que le plug-in sur les bureaux des utilisateurs afin que ces derniers puissent accéder à des applications grâce à un navigateur Web utilisant un site XenApp Web.

Nouveautés

Mise à jour : 2014-12-02

L'Interface Web propose, dans cette version, les nouvelles fonctionnalités et améliorations suivantes :

Interface utilisateur mise à jour. La mise en page et le jeu de couleurs ont été mis à jour pour faciliter la navigation et la lisibilité.

Partage de session pour les applications hébergées sur des machines virtuelles. L'Interface Web prend désormais en charge le partage de session pour VM Hosted Apps. Cette fonctionnalité est uniquement disponible pour les applications déportées et les utilisateurs non anonymes.

Possibilité pour les utilisateurs d'accéder à de multiples bureaux. Dans les versions précédentes de l'Interface Web, les utilisateurs pouvaient uniquement accéder à une seule instance de bureau par groupe de bureaux. Les utilisateurs peuvent maintenant accéder à de multiples instances de bureaux dans les groupes de bureaux. Pour plus d'informations sur l'attribution de bureaux à des utilisateurs, consultez la documentation relative à XenDesktop 5.

Prise en charge de carte à puce améliorée pour Access Gateway. L'authentification par carte à puce à l'Interface Web est maintenant compatible avec plus d'environnements. L'Interface Web accepte désormais des noms UPN depuis Access Gateway ainsi que le nom d'utilisateur et le domaine. En outre, l'Interface Web a été mise à jour pour répondre aux exigences de sécurité FIPS. Cette nouvelle fonctionnalité peut uniquement être utilisée avec l'option authentification unique par carte à puce et vous devez ouvrir la session en tant qu'administateur. Pour de plus amples informations sur la configuration de la prise en charge des cartes à puce pour Access Gateway, consultez la documentation Access Gateway archivée.

Possibilité de définir des valeurs par défaut supplémentaires. Les administrateurs peuvent configurer des valeurs par défaut pour tous les paramètres liés à la bande passante, tels que la qualité audio, le nombre de couleurs, le profil de bande passante, le mappage d'imprimante et la taille de fenêtre.

Signature du fichier ICA. L'Interface Web signe numériquement les fichiers ICA générés, afin de permettre aux clients et plug-ins Citrix compatibles de vérifier que le fichier provient d'une source approuvée.

Composants de l'Interface Web

Un déploiement Interface Web implique l’interaction de trois composants réseau :

- une ou plusieurs batteries de serveurs ;
- un serveur Web ;
- une machine utilisateur avec un navigateur Web et un client Citrix.

Batteries de serveurs

Un groupe de serveurs gérés comme une seule entité et fonctionnant conjointement pour mettre des ressources à la disposition des utilisateurs est appelé une *batterie de serveurs*. Une batterie de serveurs se compose d'un certain nombre de serveurs, exécutant soit XenApp soit XenDesktop, mais jamais les deux à la fois.

La publication de ressources constitue l'une des tâches les plus importantes d'une batterie de serveurs. Ce processus permet aux administrateurs de mettre des ressources spécifiques délivrées par la batterie de serveurs à la disposition des utilisateurs (applications, contenu et bureaux). Lorsqu’un administrateur publie une ressource à l'intention d'un groupe d’utilisateurs, cette dernière devient un objet disponible auquel les clients Citrix peuvent se connecter et initier des sessions.

À l'aide de l'Interface Web, les utilisateurs peuvent ouvrir une session sur une batterie de serveurs et recevoir une liste personnalisée des ressources publiées associées à leur nom d'utilisateur. Cette liste de ressources est appelée série de ressources. Le serveur de l'Interface Web fonctionne comme un point d'accès pour la connexion à une ou plusieurs batteries de serveurs. Le serveur Interface Web interroge les batteries de serveurs pour obtenir les informations concernant les séries de ressources puis formate les résultats dans des pages HTML que les utilisateurs peuvent visualiser à l’aide de leur navigateur Web.

Pour obtenir des informations sur des batteries de serveurs, le serveur Interface Web communique avec le service XML Citrix, ce dernier étant exécuté sur un ou plusieurs serveurs de la batterie. Le service XML Citrix est un composant de XenApp et XenDesktop qui fournit des informations sur les ressources aux clients Citrix et aux serveurs Interface Web au moyen des protocoles TCP/IP et HTTP. Ce service constitue le point de contact entre la batterie de serveurs et le serveur Interface Web. Le service XML Citrix est installé avec XenApp et XenDesktop.

Serveur Web

Le serveur Web héberge l'Interface Web. L'Interface Web fournit les prestations suivantes :

- authentification des utilisateurs auprès d’une ou plusieurs batteries de serveurs ;
- récupération d'informations sur les ressources (y compris, une liste des ressources auxquelles les utilisateurs ont accès).

Machine utilisateur

Une *machine utilisateur* est un dispositif informatique capable d'exécuter un client Citrix et un navigateur Web. Une machine utilisateur peut être, entre autres choses, un PC de bureau, un ordinateur portable, un terminal ou un assistant personnel.

Sur une telle machine, le navigateur et le client Citrix servent respectivement de système de visualisation et de moteur. Le navigateur permet aux utilisateurs de visualiser des séries de ressources (créées par des scripts côté serveur sur le serveur Interface Web), tandis que le client agit comme le moteur permettant aux utilisateurs d'accéder aux ressources.

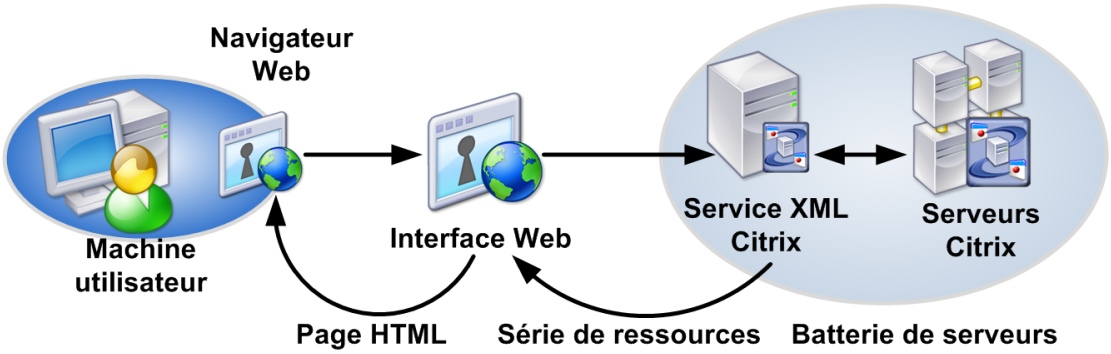
L'Interface Web offre une méthode permettant de *déployer des clients* Citrix à partir d'un site Web. Lorsqu'un utilisateur visite un site créé avec l'Interface Web, le processus Web de détection et de déploiement des clients détecte la machine et invite l'utilisateur à déployer le client Citrix approprié. Dans certains environnements, le processus de détection et de déploiement de client peut également détecter la présence ou l'absence de client et solliciter l'utilisateur le cas échéant. Pour plus d'informations, veuillez consulter la section Configuration du déploiement client et des légendes d'installation.

L'Interface Web prend en charge de nombreuses combinaisons de navigateurs et de clients Citrix. Pour obtenir la liste complète des combinaisons de navigateurs et de clients pris en charge, consultez la section Configuration requise par la machine utilisateur.

Fonctionnement de l'Interface Web

Les interactions typiques entre une batterie de serveurs, un serveur exécutant l'Interface Web et une machine utilisateur sont décrites ci-dessous.

Ce diagramme illustre un exemple d'interaction d'Interface Web typique. Le navigateur Web installé sur la machine utilisateur envoie des informations au serveur Web, lequel communique avec la batterie de serveurs afin de permettre aux utilisateurs d'accéder à leurs ressources.



- Les utilisateurs utilisent un navigateur Web pour s'authentifier à l'Interface Web.
- Le serveur Web lit les informations d'identification des utilisateurs et les communique au service XML Citrix sur les serveurs de la batterie de serveurs. Le serveur désigné sert d'intermédiaire entre le serveur Web et les autres serveurs de la batterie.
- Le service XML Citrix du serveur désigné récupère ensuite une liste de ressources auprès des serveurs auxquelles les utilisateurs peuvent accéder. Ces ressources forment la série de ressources de l'utilisateur. Le service XML Citrix récupère cette série de ressources à partir du système IMA (Independent Management Architecture).
- Dans une batterie XenApp pour UNIX, le service XML Citrix du serveur désigné utilise les informations rassemblées à partir de l'Explorateur ICA pour déterminer à quelles applications l'utilisateur peut accéder.
- Le service XML Citrix transmet alors les informations relatives à la série de ressources de l'utilisateur à l'Interface Web exécutées sur le serveur.
- L'utilisateur clique sur une icône représentant une ressource dans la page HTML.
- Le service XML Citrix est contacté pour localiser le serveur le moins occupé de la batterie. Il identifie l'adresse du serveur le moins occupé et renvoie son adresse à l'Interface Web.
- L'Interface Web communique avec le client Citrix (dans certains cas à l'aide du navigateur Web en tant qu'intermédiaire).
- Le client Citrix initie une session avec le serveur de la batterie conformément aux informations de connexion fournies par l'Interface Web.

Configuration requise pour l'Interface Web

Mise à jour : 2014-11-24

Pour pouvoir exécuter l'Interface Web, vos serveurs doivent exécuter un produit Citrix pris en charge.

L'Interface Web prend en charge les versions de produits suivantes :

- Citrix XenApp 7.6 et XenDesktop 7.6
- Citrix XenApp 7.5 et XenDesktop 7.5
- Citrix XenDesktop 7.1
- Citrix XenDesktop 7
- Citrix XenDesktop 5.6 Service Pack 1
- Citrix XenDesktop 5.6
- Citrix XenDesktop 5.5
- Citrix XenDesktop 5.0 Service Pack 1
- Citrix XenDesktop 5.0
- Citrix XenDesktop 4.0
- Citrix XenApp 6.5 pour Microsoft Windows Server 2008 R2
- Citrix XenApp 6.0 pour Microsoft Windows Server 2008 R2
- Citrix XenApp 5.0, avec Feature Pack 2, pour Microsoft Windows Server 2003 x64 Edition
- Citrix XenApp 5.0, avec Feature Pack 2, pour Microsoft Windows Server 2003
- Citrix XenApp 5.0, avec Feature Pack 1, pour Microsoft Windows Server 2008 x64 Edition
- Citrix XenApp 5.0, avec Feature Pack 1, pour Microsoft Windows Server 2008
- Citrix XenApp 5.0, avec Feature Pack 1, pour Microsoft Windows Server 2003 x64 Edition
- Citrix XenApp 5.0, avec Feature Pack 1, pour Microsoft Windows Server 2003
- Citrix XenApp 5.0 pour Microsoft Windows Server 2008 édition x64
- Citrix XenApp 5.0 pour Microsoft Windows Server 2008
- Citrix XenApp 5.0 pour Microsoft Windows Server 2003 édition x64

- Citrix XenApp 5.0 pour Microsoft Windows Server 2003
- Citrix XenApp 4.0 avec Feature Pack 1 pour systèmes d'exploitation UNIX
- Citrix Presentation Server 4.5 avec Feature Pack 1 pour Windows Server 2003 édition x64
- Citrix Presentation Server 4.5 avec Feature Pack 1 pour Windows Server 2003
- Citrix Presentation Server 4.5 pour Windows Server 2003 édition x64
- Citrix Presentation Server 4.5 pour Windows Server 2003

Important : pour assurer la compatibilité avec XenApp 4.0 Feature Pack 1, pour UNIX, vous devez effectuer une configuration supplémentaire pour le site. Pour plus d'informations, veuillez consulter la section Pour configurer la prise en charge de XenApp 4.0, avec Feature Pack 1, pour UNIX.

L'Interface Web fonctionne avec ces produits sur toutes les plates-formes prises en charge. Pour obtenir une liste des plates-formes prises en charge, consultez la documentation de votre serveur Citrix. Citrix vous recommande d'installer le dernier service pack pour le système d'exploitation sur vos serveurs.

Configuration générale requise

Les serveurs doivent appartenir à une batterie de serveurs. Les serveurs de la batterie doivent posséder des ressources (applications, contenu et/ou bureaux) publiées. Pour plus d'informations sur l'appartenance à une batterie de serveurs et sur la publication de ressources dans une batterie de serveurs, consultez la documentation de votre serveur Citrix.

XenApp pour serveurs UNIX doit également avoir des applications publiées. En outre, ces applications doivent être configurées en vue de leur utilisation avec l'Interface Web. Pour de plus amples informations sur l'installation du service XML Citrix pour UNIX et sur la configuration des applications en vue de leur utilisation avec l'Interface Web, consultez la documentation relative à XenApp pour UNIX.

Configuration logicielle minimum

Si la dernière version n'est pas installée, certaines nouvelles fonctionnalités ne sont pas disponibles. Par exemple, la migration transparente de batterie est uniquement disponible lors de la mise à niveau vers XenApp 6.0.

Le tableau suivant récapitule les configurations logicielles minimum requises pour les fonctionnalités clés de l'Interface Web.

Remarque : Pour confirmer la prise en charge de l'Interface Web 5.4 dans des versions spécifiques de produits Citrix, reportez-vous à la Configuration système requise pour ce produit.

Fonctionnalité de l'Interface Web	Configuration logicielle requise
Migration de batterie XenApp	Citrix XenApp 6.0
Itinérance des utilisateurs	Citrix XenDesktop 4.0 Citrix XenApp 6.0
XenApp VM hosted apps	Citrix XenApp 5.0 avec Feature Pack 2
Récupération d'urgence	Citrix XenDesktop 4.0 Citrix XenApp 5.0 avec Feature Pack 2
Secure Ticket Authorities redondantes	Citrix XenDesktop 4.0 Citrix XenApp 5.0 avec Feature Pack 2 Citrix Access Gateway 4.6, édition Standard
Prise en charge de Windows 7 et d'Internet Explorer 8.0	Citrix XenDesktop 4.0 Citrix XenApp 5.0 avec Feature Pack 2 Citrix Online Plug-in 11.2 Citrix Offline Plug-in 5.2
Redémarrage du bureau virtuel	Citrix XenDesktop 3.0 Citrix Desktop Receiver 11.1
Redirection vers les dossiers spéciaux	Citrix XenApp 5.0 Citrix XenApp Plugin pour applications hébergées 11.0 pour Windows
Lissage de polices	Citrix XenApp 5.0 Citrix XenApp Plugin pour applications hébergées 11.0 pour Windows

Prise en charge de XenDesktop	Citrix XenDesktop 2.0 Citrix Desktop Receiver Embedded Edition 10.250
Prise en charge de Windows Vista et Internet Explorer 7.0	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Clients Citrix Presentation Server 10.1 pour Windows
Prise en charge des applications en mode déconnecté	Citrix Presentation Server 4.5 Citrix Streaming Client 1.0 Agent Citrix Program Neighborhood 10.1
Prise en charge d'ADFS	Citrix Presentation Server 4.5
Prise en charge des stratégies de contrôle d'accès	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix Access Gateway 4.2 avec Advanced Access Control Clients Citrix MetaFrame Presentation Server pour Windows 32 bits, version 9.0
Libre-service de compte	Citrix Password Manager 4.0
Modification du mot de passe par l'utilisateur	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Agent Citrix Program Neighborhood 10.0
Fiabilité de session	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Clients Citrix MetaFrame Presentation Server pour Windows 32 bits, version 9.0
Contrôle de l'espace de travail	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Client Citrix MetaFrame Presentation Server pour Windows 32 bits, version 8.0
Prise en charge des cartes à puce	Citrix XenDesktop 3.0 Citrix Presentation Server 4.5 Citrix Desktop Receiver 11.1 Client Citrix ICA pour Windows 32 bits 7.0

Prise en charge de Secure Gateway	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0 avec Feature Pack 1 pour systèmes d'exploitation UNIX Client Citrix ICA pour Windows 32 bits 7.0
Authentification NDS	Citrix Presentation Server 4.5 Client Citrix ICA pour Windows 32 bits 7.0
Adressage DNS	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0 avec Feature Pack 1 pour systèmes d'exploitation UNIX Client Citrix ICA pour Windows 32 bits 7.0
Fonctions améliorées de publication de contenu	Citrix Presentation Server 4.5 Client Citrix ICA pour Windows 32 bits 7.0
Équilibrage de charge	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0 avec Feature Pack 1 pour systèmes d'exploitation UNIX
Prise en charge du pare-feu côté serveur	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0 avec Feature Pack 1 pour systèmes d'exploitation UNIX
Prise en charge du pare-feu côté client	Client Citrix ICA pour Windows 32 bits 7.0
Authentification unique	Citrix Presentation Server 4.5 Client Program Neighborhood pour Windows 32 bits Agent Citrix Program Neighborhood 7.0
Client Connexion Bureau à distance	Citrix XenDesktop 4.0 Citrix Presentation Server 4.5

Configuration requise pour le serveur Web

Mise à jour : 2014-09-24

Les clients Citrix doivent être présents sur votre serveur afin de pouvoir assurer le déploiement des clients par le Web. Pour de plus amples informations sur les versions des clients prises en charge, consultez la section Configuration requise par la machine utilisateur. Pour de plus amples informations sur la copie des clients sur le serveur Interface Web, consultez la section Copie des fichiers d'installation d'un client sur l'Interface Web.

Sur les plates-formes Windows

Vous pouvez installer l'Interface Web sur les plates-formes Windows suivantes :

Système d’exploitation	Serveur Web	Runtime/JDK	Moteur de servlet

Windows Server 2008 R2 x64 Windows Server 2008 R2 avec Service Pack 1	Internet Information Services 7.5	.NET Framework 3.5 avec Service Pack 1 Visual J#.NET 2.0 Second Edition ASP.NET 2.0	S.O.
Windows Server 2008 éditions x64 avec Service Pack 2 Windows Server 2008 x86 avec Service Pack 2	Internet Information Services 7.0		
Windows Server 2003 R2 x86 avec Service Pack 2 Windows Server 2003 Standard Edition x86 avec Service Pack 2 Windows Server 2003 Enterprise Edition x86 avec Service Pack 2 Windows Server 2003 R2 Standard Edition x86 avec Service Pack 2 Windows Server 2003 R2 Standard Edition x64 avec Service Pack 2	Internet Information Services 6.0		
Windows Server 2003 Standard Edition x86 avec Service Pack 2	Apache 2.2.*x*	Java 1.6.*x*	Apache Tomcat 6.0.*x*

Si vous voulez utiliser Microsoft Internet Information Services (IIS), vous devez configurer votre serveur afin d'ajouter le rôle de serveur approprié et installer IIS et ASP.NET (sous-composant d'IIS). Si IIS n'est pas installé lorsque vous installez .NET Framework, vous devez l'installer et réinstaller Framework, ou installer IIS et exécuter la commande aspnet_regiis.exe -i dans le répertoire C:\WINDOWS\Microsoft.NET\Framework*Version*. Les fichiers redistribuables .NET Framework et J# sont inclus dans le dossier \Support du support d'installation de XenApp et XenDesktop.

Configuration utilisateur requise

Mise à jour : 2014-05-23

Les combinaisons navigateur Web-système d'exploitation prises en charge qui permettent aux utilisateurs d'accéder aux sites Interface Web sont les suivantes :

Navigateur	Système d’exploitation
Internet Explorer 11	Windows 8.1 32 bits Windows 8.1 64 bits Windows 8 32 bits Windows 8 64 bits Windows 2012 64 bits Windows 2012 R2 64 bits Windows 7 32 bits avec Service Pack 1 (SP1) Windows 7 64 bits avec Service Pack 1 (SP1) Windows Server 2008 R2 avec Service Pack 1 (SP1) 64 bits avec Service Pack
Internet Explorer 10	Windows 7 32 bits avec Service Pack 1 (SP1) Windows 7 64 bits avec Service Pack 1 (SP1) Windows Server 2008 R2 avec Service Pack 1 (SP1) 64 bits avec Service Pack
Internet Explorer 9.*x* (mode 32 bits)	Windows Vista éditions 32 bits avec Service Pack 2 ou version supérieure Windows Vista éditions 64 bits avec Service Pack 2 ou version supérieure Windows 7 32 bits RTM ou supérieur Windows 7 64 bits RTM ou supérieur Windows Server 2008 32 bits avec Service Pack 2 ou version supérieure Windows Server 2008 64 bits avec Service Pack 2 ou version supérieure Windows Server 2008 R2 64 bits

Internet Explorer 8.*x* (mode 32 bits)	Windows 7 éditions 64 bits Windows 7 éditions 32 bits Windows XP Professionnel avec Service Pack 3 Windows XP Professionnel édition x64 avec Service Pack 2 Windows Vista éditions 32 bits avec Service Pack 2 Windows Vista éditions 64 bits avec Service Pack 2 Windows Server 2008 R2 Windows Server 2008 avec Service Pack 2 Windows Server 2003 avec Service Pack 2
Internet Explorer 7.*x* (mode 32 bits)	Windows Vista éditions 64 bits avec Service Pack 2 Windows Vista éditions 32 bits avec Service Pack 2 Windows Server 2008 avec Service Pack 2 Windows Server 2003 avec Service Pack 2
Safari 5.*x*	Mac OS X Snow Leopard 10.6
Safari 4.*x*	Mac OS X Leopard 10.5
Mozilla Firefox 4.*x* (mode 32 bits)	Windows 7 éditions 64 bits Windows 7 éditions 32 bits Windows XP Professionnel avec Service Pack 3 Windows XP Professionnel édition x64 avec Service Pack 2 Windows Vista éditions 32 bits avec Service Pack 2 Windows Vista éditions 64 bits avec Service Pack 2 Windows Server 2003 avec Service Pack 2
Mozilla Firefox 3.*x*	Mac OS X Snow Leopard 10.6 Mac OS X Leopard 10.5 Windows XP Professionnel édition x32 avec Service Pack 3 Windows Vista éditions 32 bits avec Service Pack 2 Windows 7 éditions 32 bits Red Hat Enterprise Linux 5.4 Desktop Windows Server 2003 avec Service Pack 2

Mozilla 1.7	Solaris 10

Remarque : l'Interface Web 5.4 est prise en charge uniquement avec les versions des logiciels répertoriées sur cette page. Bien qu'il est possible que les nouvelles versions fonctionnent, elles n'ont pas été testées et ne sont pas prises en charge.

Configuration requise pour accéder aux applications en mode déconnecté

Les combinaisons navigateur Web-système d'exploitation prises en charge qui permettent aux utilisateurs d'accéder à des applications en mode déconnecté sont les suivantes :

Navigateur	Système d’exploitation
Internet Explorer 8.*x* (mode 32 bits)	Windows 7 éditions 64 bits Windows 7 éditions 32 bits Windows Vista éditions 64 bits avec Service Pack 2 Windows Vista éditions 32 bits avec Service Pack 2 Windows XP Professionnel édition x64 avec Service Pack 2 Windows XP Professionnel avec Service Pack 3 Windows Server 2008 R2 Windows Server 2008 éditions x64 avec Service Pack 2 Windows Server 2008 avec Service Pack 2 Windows Server 2003 éditions x64 avec Service Pack 2 Windows Server 2003 avec Service Pack 2
Internet Explorer 7.*x* (mode 32 bits)	Windows Vista éditions 64 bits avec Service Pack 2 Windows Vista éditions 32 bits avec Service Pack 2 Windows XP Professionnel édition x64 avec Service Pack 2 Windows XP Professionnel avec Service Pack 3 Windows Server 2008 éditions x64 avec Service Pack 2 Windows Server 2008 avec Service Pack 2 Windows Server 2003 éditions x64 avec Service Pack 2 Windows Server 2003 avec Service Pack 2

Mozilla Firefox 3.*x*	Windows 7 éditions 64 bits Windows 7 éditions 32 bits Windows Vista éditions 64 bits avec Service Pack 2 Windows Vista éditions 32 bits avec Service Pack 2 Windows XP Professionnel édition x64 avec Service Pack 2 Windows XP Professionnel avec Service Pack 3 Windows Server 2003 avec Service Pack 2

Configuration requise pour les autres machines utilisateur

Les utilisateurs peuvent accéder à l'Interface Web avec les configurations de clients légers, périphériques portables et assistants personnels suivantes :

Appareil	Système d'exploitation	Navigateur
iPhone	S.O.	Safari 5.*x*
iPad	S.O.	Safari 5.*x*
HTC Touch2	Windows Mobile 6.5 Professional	Pocket/WinCE Internet Explorer Opera Mobile 10
HP GY227 WYSEV90	Windows XP Embedded avec Service Pack 2	Internet Explorer 6.*x*
HP T5730	Windows Embedded Standard 2009	Internet Explorer 7.*x*
HP T5540	Windows Embedded CE 6.0 R2	Internet Explorer 6.*x*
HP RK270 WYSEV30	Windows Embedded CE 6.0	Internet Explorer 6.*x*
HP GY231	Debian Linux 4.0	Debian Iceweasel 2.0
Symbian E61/E70	Symbian	Navigateur Symbian

Configuration requise par la machine utilisateur

Pour pouvoir fonctionner avec l'Interface Web, les machines utilisateur doivent disposer au moins d’un client Citrix ou d’un navigateur Web pris en charge avec l'environnement JRE. Tous les clients fournis sur le support d'installation de XenApp et XenDesktop sont compatibles avec l'Interface Web. Vous pouvez aussi les télécharger gratuitement à partir du site Web de Citrix.

Nous vous conseillons de mettre les derniers clients à la disposition de vos utilisateurs afin qu'ils puissent tirer parti des fonctionnalités les plus récentes. Chaque client offre des fonctionnalités différentes. Pour des informations complémentaires sur les fonctionnalités prises en charge, reportez-vous à la documentation correspondant au client.

Installation de l'Interface Web

Pour installer l'Interface Web, utilisez le support d'installation de XenApp ou XenDesktop.

Vous pouvez installer l'Interface Web sur les plates-formes suivantes :

- Un système d'exploitation Windows pris en charge exécutant :
    - Microsoft Internet Information Services (IIS)
    - Apache Tomcat
- Un système d'exploitation UNIX pris en charge exécutant :
    - Apache Tomcat
    - IBM WebSphere
    - Sun GlassFish Enterprise Server

Pour plus d'informations sur l'installation de la configuration requise du serveur Web, veuillez consulter la section Configuration requise pour le serveur Web.

Vous pouvez lancer des tâches de gestion de sites et d'installation sans surveillance grâce à des scripts de ligne de commande. Pour plus d'informations sur l'utilisation de la ligne de commande avec l'Interface Web, visitez le Centre de connaissances.

Pour plus d'informations sur l'installation de l'Interface Web, veuillez consulter les sections Pour installer l'Interface Web sur Microsoft Internet Information Services et Installation de l'Interface Web sur des serveurs d'application Java.

Considérations de sécurité

Si vous avez l'intention d'installer l'Interface Web sur un serveur Windows, Citrix vous conseille de suivre les instructions Microsoft standard concernant la configuration de votre serveur Windows. Pour les installations UNIX, suivez les recommandations du fabricant relatives à votre système d'exploitation.

Affichage du port utilisé par le service XML Citrix

Lors de la création du site Interface Web (IIS) ou de la génération du fichier .war (Java), vous êtes invité à indiquer le port utilisé par le service XML Citrix. Le service Citrix XML constitue le lien de communication entre la batterie de serveurs et le serveur Interface Web.

Sur les plates-formes Windows, le service XML Citrix peut être configuré pour partager le port TCP/IP d'Internet Information Services. Si c'est le cas, vous devez connaître le port utilisé par le service WWW d'Internet Information Services pour déterminer le port du service XML Citrix. Par défaut, le service d'administration utilise le port 80. Si un port dédié est requis pour le service XML Citrix, Citrix recommande d'utiliser le port 8080.

Pour obtenir la liste des ports utilisés sur les plates-formes Windows, entrez la commande netstat -a à l'invite de commandes. Sur XenApp pour serveurs UNIX, tapez ctxnfusesrv -l à l'invite de commandes pour afficher les informations sur le port.

Remarque : vous pouvez, si nécessaire, modifier le port utilisé par le service Citrix XML sur le serveur. Pour de plus amples informations, consultez la documentation accompagnant votre serveur Citrix.

Pour installer l'Interface Web sur Microsoft Internet Information Services

Avant d'installer l'Interface Web, vous devez configurer votre serveur pour ajouter le rôle de serveur Web et installer IIS et ASP.NET.

Pour utiliser IIS 7.*x* sur Windows Server 2008, installez le rôle Serveur Web (IIS) puis activez les services de rôle suivants :

- Serveur Web > Développement d'applications > ASP.NET
- Outils de gestion > Compatibilité avec la gestion IIS 6 > Compatibilité métabase IIS 6

Si vous prévoyez d'activer l'authentification unique, l'authentification unique avec carte à puce, et/ou l'authentification par carte à puce, vous devez également installer les services de rôle suivants :

- Pour l'authentification unique et l'authentification unique par carte à puce, activez Serveur Web > Sécurité > Authentification Windows.
- Pour l'authentification par carte à puce, activez Serveur Web > Sécurité > Authentification par mappage de certificat client.

Pour utiliser IIS 6.0 sur Windows Server 2003, ajoutez le rôle Serveur d'applications (IIS, ASP.NET) et activez ASP.NET.

Sur IIS, chaque site est assigné à un pool d'applications. La configuration du regroupement d'applications contient un paramètre déterminant le nombre maximal de processus d'exécution. Si vous changez la valeur par défaut de 1, il se peut que vous ne puissiez plus exécuter l'Interface Web.

Après avoir configuré votre rôle de serveur, assurez-vous que .NET Framework 3.5 avec Service Pack 1 et Visual J#.NET 2.0 Second Edition sont installés.

Si vous mettez à niveau une version précédente de l'Interface Web, version 4.5 minimum, le programme d'installation vous invite à sauvegarder vos sites existants avant de les mettre à niveau.

Important : les sites configurés de manière centralisée et Participant invité de Conferencing Manager ne sont plus pris en charge. Si vous mettez à niveau une version de l'Interface Web antérieure, le programme d'installation supprimera les sites Participant invité de Conferencing Manager existants de votre serveur Web. Les sites configurés de manière centralisée seront mis à niveau et convertis afin d'utiliser la configuration locale.

1. Ouvrez une session en tant qu'administrateur.

   Si vous installez l'Interface Web à partir du support d'installation de XenApp ou XenDesktop, insérez le disque dans le lecteur optique du serveur Web.

Si vous avez téléchargé l'Interface Web à partir du site Web de Citrix, copiez le fichier WebInterface.exe sur votre serveur Web.

2. Naviguez jusqu'au fichier WebInterface.exe et double-cliquez dessus.

3. Sélectionnez la langue de votre choix dans la liste. La langue du système d'exploitation que vous utilisez est détectée et affichée par défaut. Cliquez sur OK.

4. Dans la page Bienvenue, cliquez sur Suivant.

5. Dans la page Contrat de licence, sélectionnez J'accepte les termes du contrat de licence, puis cliquez sur Suivant.

6. Sur la page Emplacement d'installation, naviguez jusqu'à l'emplacement d'installation de l'Interface Web (emplacement par défaut : C:\Program Files (x86)\Citrix\Web Interface\). Cliquez sur Next.

7. Sur la page Emplacement des clients, sélectionnez Copier les clients sur cet ordinateur. Cliquez sur Parcourir pour rechercher les fichiers d'installation des clients Citrix sur le support d'installation ou votre réseau.

   Le programme d'installation copie le contenu du dossier \Citrix Receiver and Plug-ins du support d'installation ou d'un partage réseau vers le dossier Interface Web \Clients (C:\Program Files (x86)\Citrix\Web Interface*Version*\Clients). Tous les sites Web créés par le processus d'installation supposent que le serveur Web contient les fichiers des clients dans cette structure de répertoires.

   Si vous ne copiez pas les clients sur le serveur Web durant l'installation, sélectionnez Ignorer cette étape. Vous pouvez copier les clients sur le serveur ultérieurement.

8. Cliquez sur Suivant pour continuer, puis cliquez de nouveau sur Suivant pour confirmer votre intention de commencer l'installation.

9. Une fois l'installation terminée, cliquez sur Terminer.

10. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix pour accéder à la console de gestion de l'Interface Web Citrix, créer des sites et les configurer.

Compatibilité avec d'autres composants sur Windows Server 2003 édition x64

Sur les versions 64 bits de Windows Server 2003, l'installation de l'Interface Web pour Microsoft Internet Information Services permet la prise en charge de l'extension Web 32 bits dans IIS 6.0 et désactive la prise en charge de l'extension 64 bits. Si vous installez l'Interface Web pour Microsoft Internet Information Services sur la version 64 bits de Windows Server 2003, vous devez installer l'Interface Web avant tout autre logiciel Citrix, y compris XenApp, XenDesktop et la console License Management Console. Cet ordre d'installation doit être respecté car il permet aux produits de s'adapter à la prise en charge 32 bits dans IIS 6.0. Si vous installez ces produits dans un ordre incorrect, il est possible lors de l'accès au serveur Web que des messages d'erreur tels que « Service non disponible » s'affichent.

Lorsqu'elle est installée sur Windows Server 2003 x64 Editions, il est possible que l'Interface Web pour Microsoft Internet Information Services ne soit pas compatible avec des produits nécessitant des filtres ISAPI 64 bits, tels que le composant Windows Proxy RPC sur HTTP. Vous devez désinstaller Proxy RPC sur HTTP avant d'installer l'Interface Web.

Pour désinstaller Proxy RPC sur HTTP

1. À partir du menu Démarrer de Windows, cliquez sur Panneau de configuration > Ajout/suppression de programmes.
2. Sélectionnez Ajouter ou supprimer des composants Windows.
3. Sélectionnez Services de mise en réseau puis cliquez sur Détails.
4. Sélectionnez la case Proxy RPC sur HTTP et cliquez sur OK.
5. Cliquez sur Suivant pour désinstaller Proxy RPC sur HTTP, puis redémarrez votre serveur.

Installation de l'Interface Web sur des serveurs d'application Java

Remarque : si vous installez l'Interface Web sur IBM WebSphere, un message d'avertissement concernant la sécurité de l'application s'affiche, indiquant qu'un problème s'est produit avec le contenu du fichier was.policy. Il s'agit d'un fichier de stratégie créé par WebSphere lorsque vous sélectionnez Enforce Java 2 Security sous Security > Global Security. Modifiez le fichier was.policy conformément à la stratégie de sécurité de WebSphere Java 2, sinon il se peut que l'Interface Web ne fonctionne pas correctement. Ce fichier de stratégie est situé dans WEBSPHERE_HOME/AppServer/installedApps/*NodeName*/*WARFileName*.ear/META-INF.

L'Interface Web pour les serveurs d'application Java nécessite un moteur servlet pour fonctionner. Pour prendre en charge l'Interface Web, le serveur Web Apache exige un moteur de servlet supplémentaire, comme Tomcat (notez que Tomcat peut être utilisé comme serveur Web autonome ou comme moteur de servlet).

Pour installer l'Interface Web sur Tomcat

1. Copiez le fichier WebInterface.jar à partir du répertoire Interface Web du support d'installation sur un emplacement temporaire.
2. À partir d'une invite de commande, naviguez jusqu'au répertoire dans lequel le fichier d'installation a été téléchargé et exécutez le programme d'installation en tapant java -jar WebInterface.jar.
3. Appuyez sur Entrée pour lire le contrat de licence.
4. Entrez O pour accepter les termes du contrat de licence.
5. Sélectionnez un type de site dans la liste affichée.
6. Spécifiez la configuration initiale pour le site en répondant aux questions qui s'affichent à l'écran.
7. Un résumé des options sélectionnées s'affiche. Si les détails du site sont corrects, tapez O pour créer le fichier .war. Le fichier .war est créé et les clients Citrix sont copiés à partir du support d'installation, le cas échéant.
8. Suivez les instructions à l'écran afin de terminer l'installation du fichier .war.

Pour configurer la stratégie de sécurité sur Sun GlassFish Enterprise Server

Avant de pouvoir créer des sites XenApp Web configurés pour autoriser le libre-service de compte sur Sun GlassFish Enterprise Server, vous devez configurer manuellement la stratégie de sécurité du serveur.

1. Déployez le fichier .war du site sur le serveur.

2. Arrêtez le serveur Web.

3. Modifiez le fichier Server.policy qui se trouve dans le répertoire de configuration du domaine de déploiement. Par exemple, si Sun GlassFish Enterprise Serverr est installé sous *SunGlassFishEnterpriseServerRoot*/AppServer et que le site est déployé dans « domain1 », le fichier se trouve dans *SunGlassFishEnterpriseServerRoot*/AppServer/domains/domain1/config.

4. Ajoutez les entrées de configuration suivantes avant tout bloc générique :

   ```
   grant codeBase
   "file:${com.sun.aas.instanceRoot}/applications/
   j2ee-modules/WARFileName/-"{
   permission java.lang.RuntimePermission
   "getClassLoader";
   permission java.lang.RuntimePermission
   "createClassLoader";
   permission java.util.PropertyPermission
   "java.protocol.handler.pkgs", "read, write";
   };
   ```

   où *NomFichierWAR* est la première partie du nom de fichier du fichier .war de votre site, par exemple « XenApp ».

5. Modifiez le fichier .xml du dispositif de lancement dans *SunGlassFishEnterpriseServerRoot*/ApplicationServer/lib pour ajouter javax.wsdl à la liste des valeurs pour l'élément sysproperty key="com.sun.enterprise.overrideablejavaxpackages".

6. Démarrez le serveur Web.

Utilisation des packs de langue

Les packs de langue contiennent toutes les informations requises pour la localisation des sites dans une langue particulière (chinois {traditionnel et simplifié}, anglais, français, allemand, japonais, coréen, russe et espagnol), et notamment :

- les fichiers de ressources des sites ;
- l'aide utilisateur ;
- les images et icônes localisées.

Sur IIS, les packs de langue peuvent être ajoutés à l'installation de l'Interface Web en copiant l'arborescence ou en décompressant les fichiers dans le dossier \languages, qui se trouve généralement dans C:\Program Files (x86)\Citrix\Web Interface*Version*\languages. Pour personnaliser la langue d'un site particulier, vous pouvez copier le pack de langue sur l'emplacement du site et le modifier. Le site en question utilise ensuite le pack de langue ainsi modifié alors que les autres sites continuent à utiliser les valeurs par défaut.

Remarque : pour afficher les messages d'erreur Windows dans la langue appropriée sur IIS, vous devez installer le pack de langue approprié pour Microsoft .NET Framework.

Sur les serveurs d'application Java, il est possible d'installer des packs de langue supplémentaires ; pour ce faire, il vous faut les déplacer dans le répertoire approprié du site et extraire les fichiers.

Le pack de langue anglaise est utilisé par défaut ; il doit toujours être présent sur votre serveur. Les packs de langue sont spécifiques à la version de l'Interface Web avec laquelle ils ont été fournis, ils ne peuvent donc pas être utilisés avec des versions antérieures ou ultérieures. Pour plus d'informations sur l'utilisation des packs de langue, reportez-vous au kit de développement de l'Interface Web.

Suppression des packs de langue

Certains périphériques, tels que ceux exécutant Windows CE, ne peuvent pas afficher certaines langues (le japonais, par exemple). Dans ce cas, la liste de sélection de la langue figurant dans l'interface utilisateur affiche des carrés à la place des langues indisponibles. Pour éviter ce problème, vous pouvez supprimer une langue sur tous les sites ou uniquement sur certains d'entre eux.

Pour les sites sur IIS, supprimez *Codedelangue*.lang (par exemple, fr.lang) du dossier \languages, qui se trouve généralement dans C:\Program Files (x86)\Citrix\Web Interface*Version*\languages. Vous supprimerez ainsi la langue de tous les sites du serveur. Si vous souhaitez activer cette langue pour un site particulier, déplacez le fichier .lang vers le dossier \languages correspondant à ce site.

Pour les sites hébergés sur des serveurs d'application Java, après avoir créé un fichier .war, ouvrez ce dernier à l'aide d'un outil approprié, supprimez le fichier .lang et conditionnez-le à nouveau. Vous supprimez ainsi la langue des sites déployés à partir de ce fichier .war.

Mise à niveau d'une installation existante

Vous pouvez mettre à niveau la version 4.5 ou ultérieure de l'Interface Web vers la dernière version en installant l'Interface Web à partir du support d'installation de XenApp ou XenDesktop ou à partir des fichiers de téléchargement disponibles sur Internet.

Vous ne pouvez pas rétrograder vers une version antérieure de l'Interface Web.

Important : les sites configurés de manière centralisée et Participant invité de Conferencing Manager ne sont plus pris en charge. Si vous mettez à niveau une version de l'Interface Web antérieure, le programme d'installation supprimera les sites Participant invité de Conferencing Manager existants de votre serveur Web. Les sites configurés de manière centralisée seront mis à niveau et convertis afin d'utiliser la configuration locale.

La structure de répertoire du dossier \Clients, qui est utilisé pour déployer les clients auprès des utilisateurs via le Web, est différente dans la version 5.1 et les versions antérieures de l'Interface Web. Si vous mettez à niveau votre installation Interface Web à l'aide du support d'installation XenApp ou XenDesktop, copiez la structure de répertoire du support d'installation lorsque vous procédez à la mise à niveau de votre installation. Si vous procédez à la mise à niveau à l'aide d'un téléchargement Web, vous devez recréer manuellement la structure de répertoire requise pour votre installation Interface Web. Vous pouvez ensuite télécharger les clients nécessaires à partir du site Web de Citrix. Pour de plus amples informations sur la structure du répertoire \Clients, consultez la rubrique Copie des fichiers d'installation d'un client sur l'Interface Web.

Par défaut, l'Interface Web suppose que les noms de fichiers des fichiers d'installation de client sont les mêmes que ceux des fichiers fournis sur le support d'installation de XenApp ou XenDesktop. Si vous téléchargez des clients depuis le site Web Citrix ou que vous prévoyez de déployer des clients antérieurs, vérifiez que les noms des fichiers d'installation de client appropriés sont spécifiés pour les paramètres ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32, et ClientStreamingWin32 dans les fichiers de configuration pour vos sites XenApp Web. Pour de plus amples informations sur les paramètres des fichiers de configuration de l'Interface Web, consultez la section Paramètres WebInterface.conf.

Que faire après l'installation

Une fois l'Interface Web installée, vous devez permettre aux utilisateurs d'y accéder. Pour ce faire, vous devez créer et configurer des sites à l'aide de la console de gestion de l'Interface Web Citrix ou modifier le fichier de configuration WebInterface.conf directement.

Par ailleurs, vous devrez peut-être configurer l'Interface Web afin qu'elle puisse communiquer avec d'autres composants présents dans votre installation ; vous pouvez également la personnaliser ou étendre ses capacités.

- Pour plus d'informations sur la configuration de l'Interface Web à l'aide de la console ou du fichier WebInterface.conf, consultez la section Configuration de sites à l'aide de la console de gestion de l'Interface Web Citrix ou Configuration de sites à l'aide des fichiers de configuration.
- Pour plus d'informations sur la configuration de l'Interface Web pour Access Gateway ou Secure Gateway à l'aide de la console de gestion de l'Interface Web Citrix, veuillez consulter la section Pour configurer les paramètres de passerelle.
- Pour plus d'informations sur la configuration de l'Interface Web pour l'utilisation d'ADFS, veuillez consulter la section Configuration de la prise en charge d'ADFS pour l'Interface Web.
- Pour des informations complémentaires sur la sécurité, veuillez consulter la section Configuration de la sécurité de l'Interface Web.
- Pour de plus amples informations sur le développement et la personnalisation des fonctionnalités de l'Interface Web, reportez-vous au kit de développement de l'Interface Web.

Résolution des problèmes liés à l'installation de l'Interface Web

Sur les plates-formes Windows avec IIS, vous pouvez utiliser l'option Réparer pour résoudre les problèmes liés à l'installation de l'Interface Web. Si l'option Réparer ne permet pas de résoudre le problème, ou si cette option n'est pas disponible (par exemple, sur les installations de serveur d'application Java), essayez de désinstaller puis de réinstaller l'Interface Web. Pour plus d'informations, veuillez consulter la section Désinstallation de l'Interface Web. Vous devez reconstituer tous vos sites après la réinstallation de l'Interface Web.

Pour utiliser l'option Réparer

Si vous rencontrez des difficultés avec l'installation de votre Interface Web, essayez d'utiliser l'option Réparer pour résoudre le problème. L'option Réparer réinstalle les fichiers communs, mais elle ne répare ou ne remplace pas les sites existants.

Important : si votre installation Interface Web contient du code personnalisé et que vous sélectionnez l'option Réparer, le code personnalisé est supprimé. Citrix vous conseille de sauvegarder les fichiers que vous avez personnalisés avant d'utiliser cette option.

1. Cliquez deux fois sur le fichier WebInterface.exe.
2. Sélectionnez Réparer, puis cliquez sur Suivant.
3. Suivez les instructions à l'écran.

Désinstallation de l'Interface Web

Lorsque vous désinstallez l'Interface Web, tous les fichiers de l'Interface Web sont supprimés, y compris le dossier \Clients. Par conséquent, si vous souhaitez conserver des fichiers de l'Interface Web, copiez-les dans un autre emplacement avant de désinstaller l'Interface Web.

Dans certains cas, il est possible que la désinstallation de l'Interface Web échoue pour l'une des raisons suivantes :

- le programme de désinstallation dispose d'un accès insuffisant au Registre ;
- IIS a été supprimé du système après l'installation de l'Interface Web.

Pour désinstaller l'Interface Web sur Microsoft Internet Information Services

1. À partir du menu Démarrer de Windows, cliquez sur Panneau de configuration > Programmes et fonctionnalités.
2. Sélectionnez Interface Web Citrix et cliquez sur Désinstaller.
3. Suivez les instructions à l'écran.

Pour désinstaller l'Interface Web sur des serveurs d'application Java

Si votre serveur Web est doté d'un outil vous permettant de désinstaller des applications Web, suivez la procédure recommandée par le fabricant pour désinstaller l'Interface Web. Vous pouvez également désinstaller l'Interface Web manuellement.

1. À partir d'une invite de commande, naviguez jusqu'au répertoire dans lequel vous aviez copié le fichier .war.
2. Arrêtez le serveur Web et supprimez le fichier .war.

   Il peut également s'avérer nécessaire de supprimer le répertoire dans lequel le fichier .war a été développé. Le nom du répertoire est en principe identique au nom du fichier .war et se trouve dans le même répertoire. Par exemple, le contenu du fichier « mysite.war » est copié dans un répertoire appelé /mysite.

   Remarque : lorsque vous désinstallez l'Interface Web, certains fichiers peuvent rester sur le serveur. Pour de plus amples informations sur les fichiers restants, veuillez consulter le fichier Lisez-moi de Citrix XenApp.

Démarrage de l'Interface Web

Mise à jour : 2014-11-24

Choix de la méthode de configuration

Vous pouvez configurer et personnaliser l'Interface Web en utilisant soit la console de gestion de l'Interface Web Citrix soit les fichiers de configuration.

Utilisation de la console de gestion de l'Interface Web Citrix

La console de gestion de l'Interface Web Citrix est un composant logiciel enfichable MMC 3.0 (Microsoft Management Console) qui vous permet de créer et de configurer des sites XenApp Web et XenApp Services hébergés sur Microsoft Internet Information Services (IIS). Les types de sites Interface Web sont affichés dans le panneau de gauche. Le panneau de résultats central affiche les sites disponibles dans le conteneur de type de site sélectionné dans le panneau de gauche.

La console de gestion de l'Interface Web Citrix vous permet d'effectuer rapidement et facilement les tâches d'administration quotidiennes. Le panneau Actions dresse la liste des tâches actuellement disponibles. Les tâches associées aux éléments sélectionnés dans le panneau de gauche sont affichées dans la partie supérieure, et les actions associées aux éléments sélectionnés dans le panneau des résultats sont affichées en dessous.

Votre configuration devient effective lorsque vous effectuez des modifications à l'aide de la console. C'est la raison pour laquelle certains paramètres de l'Interface Web peuvent être désactivés si leur valeur ne s'applique pas à la configuration actuelle et si la valeur par défaut des paramètres correspondants est rétablie dans WebInterface.conf. Citrix recommande de sauvegarder régulièrement les fichiers WebInterface.conf et config.xml de vos sites.

La console de gestion de l'Interface Web Citrix est installée automatiquement lorsque vous installez l'Interface Web pour Microsoft Internet Information Services. Exécutez la console en cliquant sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

Remarque : assurez-vous que MMC 3.0 est présent sur le serveur sur lequel vous installez l'Interface Web car ce composant est requis pour l'installation de la console de gestion de l'Interface Web Citrix. MMC 3.0 est disponible par défaut sur toutes les plates-formes Windows qui prennent en charge l'hébergement de l'Interface Web.

Utilisation des fichiers de configuration

Vous pouvez modifier les fichiers de configuration suivants pour configurer les sites Interface Web :

- **Fichier de configuration de l'Interface Web.** Le fichier de configuration de l'Interface Web, WebInterface.conf, vous permet de modifier la plupart des propriétés de l'Interface Web ; il est disponible sur Microsoft Internet Information Services (IIS) et les serveurs d'application Java. Utilisez-le pour effectuer les tâches d'administration quotidiennes et personnaliser de nombreux autres paramètres. Modifiez les valeurs dans WebInterface.conf et sauvegardez le fichier mis à jour pour appliquer les modifications. Pour plus d'informations sur la configuration de l'Interface Web à l'aide du fichier WebInterface.conf, veuillez consulter la section Configuration de sites à l'aide du fichier de configuration.

- **Fichier de configuration de Citrix Online Plug-in.** Vous pouvez configurer Citrix Online Plug-in à l'aide du fichier config.xml situé sur le serveur Interface Web.

Création de sites sur des serveurs d'application Java

Sur les serveurs d'application Java, exécutez le programme d'installation de l'Interface Web pour créer de nouveaux sites. Le programme d'installation génère un fichier .war personnalisé pour le site, qu'il vous faut ensuite installer (en plaçant ce fichier dans l'emplacement approprié pour votre moteur de servlet). Vous pouvez modifier des sites en modifiant le contenu du fichier .war décompressé, ou en supprimer en effaçant le fichier .war.

Configuration de sites à l'aide de la console de gestion de l'Interface Web Citrix

La console de gestion de l'Interface Web Citrix est un composant logiciel enfichable MMC 3.0 (Microsoft Management Console) qui vous permet de créer et de configurer des sites XenApp Web et XenApp Services hébergés sur Microsoft Internet Information Services (IIS). Les types de sites Interface Web sont affichés dans le panneau de gauche. Le panneau de résultats central affiche les sites disponibles dans le conteneur de type de site sélectionné dans le panneau de gauche.

La console de gestion de l'Interface Web Citrix vous permet d'effectuer rapidement et facilement les tâches d'administration quotidiennes. Le panneau Actions dresse la liste des tâches actuellement disponibles. Les tâches associées aux éléments sélectionnés dans le panneau de gauche sont affichées dans la partie supérieure, et les actions associées aux éléments sélectionnés dans le panneau des résultats sont affichées en dessous.

Votre configuration devient effective lorsque vous effectuez des modifications à l'aide de la console. C'est la raison pour laquelle certains paramètres de l'Interface Web peuvent être désactivés si leur valeur ne s'applique pas à la configuration actuelle et si la valeur par défaut des paramètres correspondants est rétablie dans WebInterface.conf. Citrix recommande de sauvegarder régulièrement les fichiers WebInterface.conf et config.xml de vos sites.

La console de gestion de l'Interface Web Citrix est installée automatiquement lorsque vous installez l'Interface Web pour Microsoft Internet Information Services. Exécutez la console en cliquant sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

Remarque : assurez-vous que MMC 3.0 est présent sur le serveur sur lequel vous installez l'Interface Web car ce composant est requis pour l'installation de la console de gestion de l'Interface Web Citrix. MMC 3.0 est disponible par défaut sur toutes les plates-formes Windows qui prennent en charge l'hébergement de l'Interface Web.

Configuration de sites à l'aide des fichiers de configuration

Vous pouvez modifier les fichiers de configuration suivants pour configurer les sites Interface Web :

- **Fichier de configuration de l'Interface Web.** Le fichier de configuration de l'Interface Web, WebInterface.conf, vous permet de modifier la plupart des propriétés de l'Interface Web ; il est disponible sur Microsoft Internet Information Services (IIS) et les serveurs d'application Java. Utilisez-le pour effectuer les tâches d'administration quotidiennes et personnaliser de nombreux autres paramètres. Modifiez les valeurs dans WebInterface.conf et sauvegardez le fichier mis à jour pour appliquer les modifications. Pour plus d'informations sur la configuration de l'Interface Web à l'aide du fichier WebInterface.conf, veuillez consulter la section Configuration de sites à l'aide du fichier de configuration.
- **Fichier de configuration de Citrix Online Plug-in.** Vous pouvez configurer Citrix Online Plug-in à l'aide du fichier config.xml situé sur le serveur Interface Web.

Configuration partagée

Pour les sites hébergés sur IIS, vous pouvez spécifier qu'un site Interface Web obtienne sa configuration à partir d'un site « maître » que vous avez configuré pour partager ses fichiers de configuration sur le réseau. Une fois que vous avez défini les permissions de fichier appropriées, vous pouvez autoriser les autres sites à partager la configuration du site maître en spécifiant le chemin d'accès absolu au fichier de configuration de site maître (WebInterface.conf) dans le fichier bootstrap.conf du site local. Pour ce qui est des sites XenApp Services qui utilisent la configuration partagée, l'Interface Web essaye également de lire le fichier de configuration de Citrix Online Plug-in (config.xml) à partir du même répertoire que celui spécifié pour WebInterface.conf.

Lorsqu'un site a été modifié afin d'utiliser la configuration d'un fichier partagé, vous ne pouvez plus gérer sa configuration directement. Vous devez modifier la configuration du site maître à l'aide de la console ou en modifiant directement les fichiers de configuration sur le serveur Web hébergeant le site maître. Toute modification apportée à la configuration du site maître affecte tous les autres sites qui partagent le fichier de configuration du site maître. La configuration partagée n'est pas disponible pour les sites hébergés sur des serveurs d'application Java.

Pour partager des configurations de site

1. Configurez les permissions de partage de fichier appropriées pour autoriser l'accès via le réseau au dossier \conf (il se trouve généralement dans C:\inetpub\wwwroot\Citrix*nomdusite*\conf) du site maître et au fichier de configuration du site (WebInterface.conf), qui se trouve généralement dans le dossier \conf. Pour ce qui est des sites maîtres XenApp Services, les mêmes permissions doivent être configurées pour le fichier de configuration de Citrix Online Plug-in (config.xml), qui se trouve généralement dans le dossier \conf du site.

2. À l'aide d'un éditeur de texte, ouvrez le fichier bootstrap.conf (il se trouve généralement dans le dossier \conf) du site dont la configuration provient du fichier de configuration partagé.

3. Modifiez le réglage du paramètre ConfigurationLocation afin de spécifier le chemin d'accès au réseau absolu du fichier de configuration du site maître, comme par exemple :

   ConfigurationLocation=*ServerName**ShareName*\WebInterface.conf

Pour créer un site sur Microsoft Internet Information Services

Utilisez la tâche Créer un site dans la console de gestion de l'Interface Web Citrix pour créer l'un des sites suivants :

- **Sites XenApp Web.** Pour les utilisateurs qui accèdent aux ressources à l'aide d'un navigateur Web.
- **Sites XenApp Services.** Pour les utilisateurs qui accèdent aux ressources à l'aide de Citrix Online Plug-in.

Utilisez cette tâche pour indiquer l'emplacement d'IIS dans lequel le site est hébergé, l'adresse URL d'application des modifications et les paramètres d'authentification du site. Vous pouvez mettre à jour ces paramètres plus tard à l'aide des tâches Maintenance du site. Pour pouvoir créer des sites, vous devez être un administrateur local sur le serveur exécutant l'Interface Web.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.
2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Interface Web Citrix.
3. Dans le panneau Actions, cliquez sur Créer un site.
4. Sélectionnez le type de site à créer.
5. Spécifiez une adresse URL et un nom pour le site.
6. Suivez les instructions affichées à l'écran pour créer le site.

Hébergement de Microsoft Internet Information Services

Utilisez la tâche Gérer l'hébergement IIS sous Maintenance du site dans la console de gestion de l'Interface Web Citrix pour modifier l'emplacement de votre site Interface Web sur IIS.

Spécification du point d'authentification

Mise à jour : 2014-12-02

Lorsque vous créez un site XenApp Web à l'aide de la console de gestion de l'Interface Web Citrix, vous devez spécifier un *point d'authentification* ; ce dernier correspond à l'emplacement dans votre déploiement où s'effectue l'authentification utilisateur.

Authentification sur l'Interface Web

Vous pouvez autoriser les utilisateurs à s'authentifier à l'Interface Web à l'aide de plusieurs méthodes d'authentification intégrées, dont l'authentification explicite, l'authentification unique et l'authentification par carte à puce. Pour de plus amples informations sur les méthodes d'authentification à l'Interface Web, consultez la section Configuration de l'authentification pour l'Interface Web.

Authentification sur un compte de partenaire Active Directory Federation Services

Vous pouvez autoriser le partenaire de ressource d'un déploiement Active Directory Federation Services (ADFS) à accéder à des applications XenApp. Cela vous permet de fournir aux utilisateurs un accès aux applications sur le partenaire de compte.

Si vous envisagez de créer des sites ADFS incorporés, tenez compte de ce qui suit :

- XenDesktop ne prend pas en charge l'authentification ADFS.
- La prise en charge d'ADFS n'est pas disponible avec l'Interface Web pour les serveurs d'application Java.
- Le client pour Java et le logiciel Connexion au Bureau à distance ne prennent pas en charge l'accès aux sites intégrés ADFS.
- Les sites ADFS incorporés prennent en charge l'authentification à l'aide d'ADFS uniquement. Les autres méthodes d'authentification ne sont pas prises en charge.
- Après la création d'un site ADFS incorporé, vous ne pouvez pas configurer le site pour utiliser l'authentification incorporée ou l'authentification par Access Gateway à la place d'ADFS.

Pour plus d'informations, veuillez consulter la section Configuration de la prise en charge d'ADFS pour l'Interface Web.

Authentification sur Access Gateway

Vous pouvez activer l'authentification unique des informations d'identification des utilisateurs sur Access Gateway pour l'authentification explicite et par carte à puce. L'accès des utilisateurs aux ressources est contrôlé par l'utilisation de stratégies.

Si vos utilisateurs ouvrent une session à Access Gateway à l'aide d'informations d'identification explicites, l'authentification unique est activée par défaut. Les utilisateurs qui ouvrent une session à Access Gateway n'ont pas besoin de se réauthentifier à l'Interface Web pour accéder à leurs ressources. Pour renforcer la sécurité, vous pouvez désactiver l'authentification unique pour inviter les utilisateurs à entrer un mot de passe avant d'afficher les ressources.

Si vos utilisateurs ouvrent une session à Access Gateway à l'aide d'une carte à puce, ils n'ont pas besoin de se réauthentifier pour ouvrir une session à l'Interface Web. Par défaut, les utilisateurs sont toutefois invités à entrer un code PIN pour accéder à une ressource. Vous pouvez configurer le site pour autoriser les utilisateurs à accéder à leurs ressources XenApp sans avoir à entrer de code PIN. Cette fonctionnalité n'est pas prise en charge par XenDesktop.

Vous pouvez à tout moment mettre à jour ces paramètres à l'aide de la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix.

Authentification sur un tiers utilisant Kerberos

Vous pouvez utiliser un produit de fédération tierce ou d'authentification unique pour authentifier les utilisateurs et mapper leurs identités avec celles des comptes utilisateur Active Directory. Kerberos peut ensuite être utilisé pour l'authentification unique à l'Interface Web. Pour plus d'informations sur Kerberos, veuillez consulter la section Configuration de l'ouverture de session Kerberos.

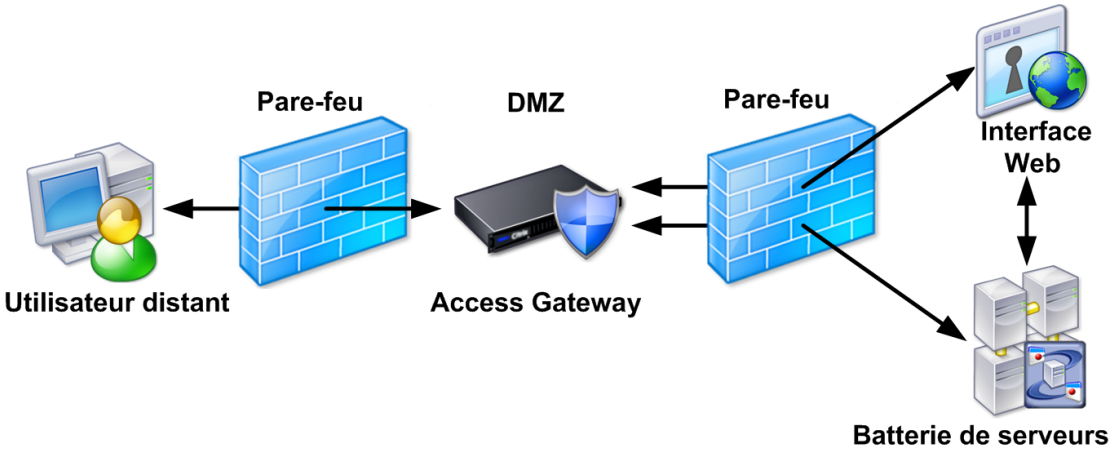
Authentification sur le serveur Web

Vous pouvez autoriser l'authentification des utilisateurs sur le serveur Web à l'aide de Kerberos. Pour plus d'informations concernant Kerberos, veuillez consulter la section Configuration de l'ouverture de session Kerberos.

Déploiement d'Access Gateway avec l'Interface Web

Lorsque vous déployez Access Gateway conjointement avec l'Interface Web, Citrix recommande d'installer XenApp/XenDesktop et l'Interface Web sur des serveurs du réseau interne, et le boîtier Access Gateway dans la zone démilitarisée (DMZ).

Ce graphique illustre la configuration recommandée pour le déploiement d'Access Gateway avec l'Interface Web.



Une DMZ est un sous-réseau compris entre le réseau interne sécurisé et Internet (ou tout réseau externe). Lorsqu'Access Gateway est déployé dans la DMZ, les utilisateurs y accèdent à l'aide de Citrix Secure Access Plug-in ou d'un client Citrix. Les utilisateurs ouvrent une session, sont authentifiés par Access Gateway et ensuite dirigés vers leurs ressources, en fonction des stratégies d'accès que vous avez configurées.

Mise à disposition des ressources auprès des utilisateurs

Grâce à Access Gateway, les utilisateurs ouvrent une session sur un domaine (pour Access Gateway édition Standard), point d'ouverture de session (pour Access Gateway édition Advanced et Access Gateway 5.0), ou serveur virtuel (pour Access Gateway édition Enterprise) pour accéder à leurs ressources. Pour rendre les ressources accessibles aux utilisateurs, configurez un domaine, point d'ouverture de session ou serveur virtuel pour fournir un accès à un site XenApp Web.

Access Gateway fournit plusieurs méthodes d'intégration des sites XenApp Web créés avec l'Interface Web, parmi lesquels :

- Site XenApp Web configuré comme page d'accueil par défaut pour un domaine, point d'ouverture de session ou serveur virtuel. Après avoir ouvert une session, le site XenApp Web est présenté aux utilisateurs.

- Site XenApp Web intégré à l'interface d'accès. Lorsque l'interface d'accès est sélectionnée comme page d'accueil par défaut, un site XenApp Web s'affiche à côté des partages de fichiers, des centres d'accès et des applications Web. Access Interface est uniquement disponible avec les éditions Advanced et Enterprise d'Access Gateway.

Intégration d'un site XenApp Web à Access Gateway

Mise à jour : 2014-10-30

Pour intégrer un site à Access Gateway, créez un site XenApp Web et configurez une ressource Web pour le site dans Access Gateway.

Pour créer un site intégré Access Gateway

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Interface Web Citrix.

3. Dans le panneau Actions, cliquez sur Créer un site.

4. Sélectionnez XenApp Web et cliquez sur Suivant.

5. Sur la page Spécifier l'emplacement IIS, spécifiez l'emplacement IIS, le chemin d'accès et le nom du site. Cliquez sur Next.

6. Sur la page Spécifier le point d'authentification, sélectionnez Sur Access Gateway et cliquez sur Suivant.

7. Sur la page Spécifiez les paramètres d'Access Gateway, tapez l'adresse URL du service d'authentification d'Access Gateway dans la case Adresse URL du service d'authentification.

8. Spécifiez la méthode utilisée par vos utilisateurs pour se connecter à Access Gateway et cliquez sur Suivant :

   - Si vos utilisateurs se connectent à Access Gateway à l'aide d'un nom d'utilisateur et d'un mot de passe, sélectionnez Explicite. Pour renforcer la sécurité en désactivant l'authentification unique des informations d'identification des utilisateurs de Access Gateway à l'Interface Web, sélectionnez la case Demander saisie d'un mot de passe avant d'afficher applications et bureaux.

   - Si vos utilisateurs se connectent à Access Gateway à l'aide d'une carte à puce, sélectionnez Carte à puce. Vous devez ouvrir la session en tant qu'administrateur du domaine avant d'activer l'authentification unique pour l'option de carte à puce.

   Important : les sites XenApp Web intégrés à Access Gateway peuvent prendre en charge soit l'authentification explicite, soit l'authentification par carte à puce, mais pas les deux. Si vos utilisateurs se connectent à Access Gateway à l'aide de l'authentification explicite et de l'authentification par carte à puce, vous devez créer et configurer des sites distincts pour chaque méthode d'authentification. Configurez ensuite Access Gateway de manière à diriger les utilisateurs vers le site approprié à leur méthode d'authentification.

9. Si vous configurez le site pour une authentification explicite, passez à l'étape 10. Si vous configurez l'authentification par carte à puce, sur la page Spécifier les paramètres de carte à puce, spécifiez si les utilisateurs sont invités à entrer un code PIN avant de pouvoir accéder à une ressource.

   - Si vous souhaitez que les utilisateurs entrent un code PIN chaque fois qu'ils accèdent à une ressource, sélectionnez Inviter les utilisateurs à entrer un code PIN. D'autres étapes de configuration sont requises pour activer cette fonctionnalité. Pour plus d'informations, veuillez consulter la section Pour autoriser les utilisateurs de cartes à puce à accéder à leurs ressources via Access Gateway en entrant un code PIN.

Remarque : vous pouvez faire en sorte que les utilisateurs Windows XP qui se connectent à leurs bureaux à l'aide de la même carte à puce que celle qu'ils utilisent pour se connecter à Access Gateway puissent accéder à leurs ressources sans avoir à entrer de code PIN. Pour plus d'informations, veuillez consulter la section Pour autoriser les utilisateurs de cartes à puce à accéder à leurs ressources via Access Gateway en entrant un code PIN.

- Si vous souhaitez que tous les utilisateurs puissent accéder à leurs ressources XenApp sans avoir à entrer de code PIN, sélectionnez Activer l'authentification unique par carte à puce. Cette fonctionnalité n'est pas prise en charge par XenDesktop et peut uniquement être utilisée lorsque le serveur Web se trouve dans le même domaine que vos utilisateurs. Vous devrez peut-être redémarrer le serveur Web pour activer l'authentification unique par carte à puce à partir du service Access Gateway. D'autres étapes de configuration sont requises pour activer cette fonctionnalité. Pour plus d'informations, veuillez consulter la section Pour autoriser les utilisateurs de cartes à puce à accéder à leurs ressources via Access Gateway sans entrer de code PIN.

  Remarque : par défaut, l'authentification unique par carte à puce à partir d'Access Gateway est activée pour tous les utilisateurs du domaine. Pour restreindre la liste des utilisateurs autorisés, modifiez les permissions utilisateur pour le fichier PTSAccess.txt. Ce dernier se trouve généralement dans le répertoire C:\Program Files (x86)\Citrix\DeliveryServices\ProtocolTransitionService\.

10. Confirmez les paramètres pour le nouveau site et cliquez sur Suivant pour le créer.

Pour fournir l'accès au site via Access Gateway

Ces étapes expliquent comment fournir l'accès au site via Access Gateway. Pour de plus amples informations, consultez la documentation relative à votre édition d'Access Gateway qui est archivée ici.

1. Configurez XenApp ou XenDesktop de façon à communiquer avec Access Gateway.
2. Configurez Access Gateway de manière à autoriser l'accès au site XenApp Web.

   Important : spécifiez le domaine au format *domaine* plutôt qu'au format *domaine.com*. L'authentification unique par carte à puce sur l'Interface Web à partir du service Access Gateway ne reconnaît pas les domaines au format *domaine.com*, par conséquent les utilisateurs ne peuvent pas se connecter si le domaine spécifié utilise ce format.
3. Assurez-vous que les paramètres de contrôle de l'espace de travail (pour Access Gateway édition Advanced uniquement) et d'expiration de session sont correctement configurés dans Access Gateway et l'Interface Web.

Pour autoriser les utilisateurs de cartes à puce à accéder à leurs ressources via Access Gateway sans entrer de code PIN

Si vous voulez que tous les utilisateurs puissent accéder à leurs ressources XenApp sans avoir à fournir de code PIN, vous devez activer Secure Sockets Layer (SSL) pour le site IIS hébergeant le site XenApp Web. Pour de plus amples informations, consultez la documentation Microsoft relative à IIS 7.*x* et IIS 6.0.

Après avoir activé SSL, assurez-vous que le serveur Web se trouve dans le même domaine que vos utilisateurs et configurez Active Directory pour autoriser la délégation contrainte.

Pour vérifier que le domaine est au niveau fonctionnel correct

Important : pour augmenter le niveau du domaine, tous les contrôleurs de domaine au sein du domaine doivent exécuter Windows Server 2008 ou Windows Server 2003. N'augmentez pas le niveau fonctionnel du domaine sur Windows Server 2008 si vous avez déjà ajouté ou que vous prévoyez d'ajouter des contrôleurs de domaine exécutant Windows Server 2003. Une fois le niveau fonctionnel augmenté, il ne peut plus être réduit.

1. Ouvrez une session au contrôleur de domaine en tant qu'administrateur du domaine et ouvrez le composant logiciel enfichable MMC Domaines et approbations Active Directory.

2. Dans le panneau de gauche, sélectionnez le nom de domaine et, dans le panneau Action, cliquez sur Propriétés.

3. Si le domaine n'est pas au niveau fonctionnel le plus élevé, sélectionnez le nom du domaine et, dans le panneau Action, cliquez sur Augmenter le niveau fonctionnel du domaine.

4. Pour augmenter le niveau fonctionnel du domaine, cliquez sur le niveau approprié puis sur Augmenter.

Pour approuver les serveurs exécutant l'Interface Web et le service XML Citrix pour la délégation

1. Ouvrez une session au contrôleur de domaine en tant qu'administrateur du domaine et ouvrez le composant logiciel enfichable MMC Utilisateurs et ordinateurs Active Directory.
2. Sur le menu Affichage, cliquez sur Fonctionnalités avancées.
3. Dans le panneau de gauche, cliquez sur le nœud Ordinateurs et sélectionnez le serveur Web.
4. Dans le panneau Actions, cliquez sur Propriétés.
5. Sur l'onglet Délégation, cliquez sur Approuver cet ordinateur pour la délégation vers les services spécifiés uniquement et Utiliser n'importe quel protocole d'authentification, puis cliquez sur Ajouter.
6. Dans la boîte de dialogue Ajouter des services, cliquez sur Utilisateurs ou ordinateurs.
7. Dans la boîte de dialogue Sélectionnez utilisateurs ou ordinateurs, tapez le nom du serveur exécutant le service XML Citrix dans la zone de texte Entrez le nom de l'objet à sélectionner, puis cliquez sur OK.
8. Sélectionnez le type de service http dans la liste et cliquez sur OK.
9. Sur l'onglet Délégation, vérifiez que le type de service http pour le serveur exécutant le service XML Citrix apparaît bien dans la liste Ce compte peut présenter des informations d'identification déléguées à ces services, puis cliquez sur OK.
10. Répétez les étapes 3 à 9 pour chaque serveur de la batterie exécutant le service XML Citrix que l'Interface Web doit contacter.
11. Dans le panneau de gauche, cliquez sur le nœud Ordinateurs et sélectionnez le serveur exécutant le service XML Citrix que l'Interface Web est configurée pour contacter.
12. Dans le panneau Actions, cliquez sur Propriétés.
13. Sur l'onglet Délégation, cliquez sur Approuver cet ordinateur pour la délégation vers les services spécifiés uniquement et Utiliser Kerberos uniquement, puis cliquez sur Ajouter.
14. Dans la boîte de dialogue Ajouter des services, cliquez sur Utilisateurs ou ordinateurs.
15. Dans la boîte de dialogue Sélectionnez utilisateurs ou ordinateurs, tapez le nom du serveur exécutant le service XML Citrix dans la zone de texte Entrez le nom de l'objet à sélectionner, puis cliquez sur OK.
16. Sélectionnez le type de service HOST dans la liste et cliquez sur OK.
17. Sur l'onglet Délégation, vérifiez que le type de service HOST pour le serveur exécutant le service XML Citrix apparaît bien dans la liste Ce compte peut présenter des informations d'identification déléguées à ces services, puis cliquez sur OK.

18. Répétez les étapes 11 à 17 pour chaque serveur de la batterie exécutant le service XML Citrix que l'Interface Web doit contacter.

19. Pour des raisons de sécurité, vous devez configurer tous les serveurs de la batterie pour la délégation contrainte. Pour fournir aux utilisateurs l'accès aux ressources sur ces serveurs, vous devez ajouter les services adéquats, tels que le service http pour un serveur Web, à la liste Ce compte peut présenter des informations d'identification déléguées à ces services.

    Pour des informations détaillées, reportez-vous au document technique *Service Principal Names and Delegation in Presentation Server* (CTX110784) disponible dans le centre de connaissances Citrix.

Pour déterminer quelles ressources sont accessibles depuis la batterie de serveurs

1. Ouvrez une session au contrôleur de domaine en tant qu'administrateur du domaine et ouvrez le composant logiciel enfichable MMC Utilisateurs et ordinateurs Active Directory.

2. Dans le panneau de gauche, cliquez sur le nœud Ordinateurs et sélectionnez un serveur dans la batterie.

3. Dans le panneau Actions, cliquez sur Propriétés.

4. Sur l'onglet Délégation, cliquez sur Approuver cet ordinateur pour la délégation vers les services spécifiés uniquement et Utiliser Kerberos uniquement, puis cliquez sur Ajouter.

5. Dans la boîte de dialogue Ajouter des services, cliquez sur Utilisateurs ou ordinateurs.

6. Dans la boîte de dialogue Sélectionnez utilisateurs ou ordinateurs, tapez le nom du serveur dans la case Entrez les noms des objets à sélectionner et cliquez sur OK.

7. Sélectionnez les types de service cifs et ldap dans la liste et cliquez sur OK.

    Remarque : si vous avez deux possibilités de service ldap, sélectionnez celui qui correspond au FQDN du contrôleur de domaine.

8. Sur l'onglet Délégation, vérifiez que les types de services cifs et ldap du contrôleur de domaine apparaissent dans la liste Ce compte peut présenter des informations d'identification déléguées à ces services, puis cliquez sur OK.

9. Répétez cette procédure pour chaque serveur de la batterie.

Pour configurer une durée limite d'accès aux ressources au niveau du domaine

Attention : une utilisation incorrecte de l'Éditeur de Registre peut entraîner de graves problèmes 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.

Par défaut, les utilisateurs ont accès aux ressources sur un réseau pendant 15 minutes. Vous pouvez augmenter cette durée en modifiant l'entrée de registre suivante sur le serveur exécutant le service XML Citrix :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
Kerberos\Parameters\S4UTicketLifetime

Cette valeur spécifie le nombre de minutes pendant lesquelles les utilisateurs ont accès aux ressources une fois une session ouverte.

La stratégie de sécurité de domaine régit la valeur maximale que vous pouvez définir pour S4ULifetime. Si vous définissez pour ce paramètre une valeur supérieure à celle spécifiée pour le paramètre au niveau du domaine, la valeur définie pour ce dernier est prioritaire.

1. Ouvrez une session au contrôleur de domaine en tant qu'administrateur du domaine et ouvrez le composant logiciel enfichable MMC Stratégie de sécurité du domaine.
2. Dans le panneau de gauche, sélectionnez Stratégies de compte > Stratégie Kerberos.
3. Dans le panneau des résultats, sélectionnez Durée de vie maximale du ticket de service.
4. Dans le panneau Actions, cliquez sur Propriétés.
5. Entrez la durée requise (en minutes) dans la case Le ticket expire dans.

Si vous ne souhaitez pas configurer de durée limite pour l'accès aux ressources, sélectionnez Utiliser tout protocole d'authentification lorsque vous spécifiez les ressources accessibles depuis la batterie de serveurs. Si vous sélectionnez cette option, la valeur spécifiée pour S4UTicketLifetime sera ignorée, quelle qu'elle soit. Pour de plus amples informations, visitez le site Web de Microsoft à l'adresse http://support.microsoft.com/.

Pour autoriser les utilisateurs de cartes à puce à accéder à leurs ressources via Access Gateway en entrant un code PIN

Mise à jour : 2014-07-04

Si vous souhaitez que les utilisateurs de cartes à puce entrent un code PIN chaque fois qu'ils accèdent à une ressource via Access Gateway, vous devez activer l'énumération des identificateurs de sécurité (SIDs) des utilisateurs sur le service XML Citrix.

Attention : une utilisation incorrecte de l'Éditeur de Registre peut entraîner de graves problèmes 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.

1. Si les comptes d'utilisateur existent dans un domaine différent de celui qui contient la batterie de serveurs, assurez-vous que le domaine partage une relation d'approbation bidirectionnelle.

2. Vérifiez que le service XML Citrix peut résoudre l'adresse IP et contacter le contrôleur de domaine du domaine du compte d'utilisateur. Les requêtes reçues par le service XML Citrix peuvent expirer si ce dernier ne peut pas communiquer avec les contrôleurs de domaine.

3. Accordez au compte Windows sous lequel le service XML Citrix est exécuté l'accès en lecture à l'attribut TGGAU dans Active Directory pour chaque domaine. Pour de plus amples informations sur l'attribut TGGAU, veuillez consulterl'article 331951 de la Base de connaissances Microsoft. Par défaut, le service XML Citrix est configuré pour être exécuté en tant que compte de service réseau. Les autorisations nécessaires peuvent être accordées en ajoutant ce compte aux groupes Active Directory intégrés suivants :

   - Accès compatible pré-Windows 2000

   - Accès d'autorisation Windows

4. Sur le serveur exécutant le service XML Citrix, accédez à HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\XMLService\ dans le registre système.

5. Sous le nœud XMLService, ajoutez une valeur DWORD appelée EnableSIDEnumeration et définissez la valeur sur 1.

   Remarque : Pour XenDesktop 5 et version supérieure, la clé de registre est : [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer] "EnableXmlServiceSidEnumeration"=REG_DWORD:1

6. Redémarrez IIS sur le serveur Web. Si vous souhaitez que les nouvelles autorisations soient prises en compte immédiatement, sans avoir à attendre l'expiration de la période de cache du ticket Kerberos, redémarrez le serveur exécutant le service XML Citrix.

7. Vous pouvez autoriser les utilisateurs Windows XP qui se connectent à leurs bureaux à l'aide de la même carte à puce que celle qu'ils utilisent pour se connecter à Access Gateway à accéder à leurs ressources sans avoir à entrer de code PIN en configurant l'authentification unique par carte à puce :

   a. installez Citrix Online Plug-in ou Citrix Desktop Viewer sur les machines de vos utilisateurs à l'aide d'un compte d'administrateur.

   b. Ajoutez le modèle de client à l'Éditeur d'objet de stratégie de groupe. Pour plus d'informations, veuillez consulter la section Étape 1 : installation du plug-in pour l'authentification par carte à puce.

   c. Activez l'authentification unique pour tous les clients Citrix utilisant la stratégie de groupe. Pour plus d'informations, veuillez consulter la section Étape 1 : installation du plug-in pour l'authentification par carte à puce.

Coordination des paramètres de l'Interface Web et Access Gateway

Certains paramètres de XenApp et XenDesktop peuvent être configurés dans l'Interface Web et Access Gateway. Cependant, étant donné qu'un site XenApp Web intégré à Access Gateway peut être référencé par plus d'un domaine (pour Access Gateway édition Standard), point d'ouverture de session(pour Access Gateway édition Advanced), ou serveur virtuel (pour Access Gateway édition Enterprise), il est possible qu'un domaine, point d'ouverture de session ou serveur virtuel intègre un site XenApp Web dans son interface d'accès alors qu'un autre domaine, point d'ouverture de session ou serveur virtuel affiche ce site comme sa page d'accueil par défaut. Cela peut provoquer des conflits avec certains paramètres de ressources.

Pour vous assurer que vos paramètres fonctionnent comme prévu, veuillez suivre les instructions ci-dessous :

- **Expiration de session.** Assurez-vous que tous les domaines, points d'ouverture de session ou serveurs virtuels utilisent les mêmes paramètres que le site XenApp Web.
- **Contrôle de l'espace de travail.** Pour Access Gateway édition Advanced, désactivez tous les paramètres de contrôle de l'espace de travail pour les points d'ouverture de session qui possèdent un site XenApp Web comme page d'accueil. Cela garantit l'utilisation des paramètres configurés dans l'Interface Web. Tous les autres points d'ouverture de session peuvent posséder un contrôle de l'espace de travail configuré de la manière souhaitée.

Définition des paramètres de configuration initiale d'un site

Après avoir créé un site avec la console, vous pouvez spécifier les paramètres de configuration initiale en sélectionnant la case Configurer ce site maintenant sur la dernière page de l'assistant Créer un site. Utilisez l'assistant Spécifier la configuration initiale pour configurer la communication avec un ou plusieurs serveurs et spécifier les types de ressources mises à la disposition des utilisateurs.

Spécification de batteries de serveurs

Lorsque vous configurez un nouveau site, vous devez entrer les détails des batteries de serveurs qui fourniront les ressources aux utilisateurs du site.

Vous pouvez à tout moment mettre à jour ces paramètres à l'aide de la tâche Batteries de serveurs dans la console de gestion de l'Interface Web Citrix. Pour plus d'informations sur la configuration de la communication avec les batteries de serveurs, consultez la section Gestion des serveurs et des batteries.

Important : pour assurer la compatibilité avec XenApp 4.0 Feature Pack 1, pour UNIX, vous devez effectuer une configuration supplémentaire pour le site. Pour plus d'informations, veuillez consulter la section Pour configurer la prise en charge de XenApp 4.0, avec Feature Pack 1, pour UNIX.

Spécification de méthodes d'authentification

Lorsque vous configurez un site XenApp Web créé avec le point d'authentification Sur l'Interface Web, vous pouvez spécifier la méthode utilisée par les utilisateurs pour ouvrir une session Interface Web.

Vous pouvez à tout moment mettre à jour ces paramètres à l'aide de la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix. Pour des informations complémentaires sur la configuration de l'authentification, consultez la section Configuration de l'authentification pour l'Interface Web.

Spécification de restrictions de domaine

Lorsque vous configurez un site XenApp Web créé avec le point d'authentification Sur l'Interface Web, vous pouvez restreindre l'accès des utilisateurs dans certains domaines.

Vous pouvez à tout moment mettre à jour ces paramètres à l'aide de la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix. Pour des informations complémentaires sur la configuration des restrictions de domaine, consultez la section Pour configurer les paramètres de restriction de domaine.

Spécification de l'apparence de l'écran Ouvrir une session

Lorsque vous configurez un nouveau site XenApp Web, vous pouvez spécifier le style de l'écran Ouvrir une session. Vous avez le choix entre une configuration simplifiée où seuls les champs d'ouverture de session appropriés s'affichent et une configuration comprenant la barre de navigation.

Vous pouvez mettre à jour ce paramètre à tout moment à l'aide de la tâche Apparence du site Web dans la console de gestion de l'Interface Web Citrix. Pour des informations complémentaires sur la personnalisation de l'apparence de l'interface utilisateur, consultez la section Personnalisation de l'affichage pour les utilisateurs.

Spécification des types de ressources mises à la disposition des utilisateurs

Lorsque vous configurez un nouveau site, vous devez spécifier les types de ressources que vous souhaitez rendre disponibles. L'Interface Web permet aux utilisateurs d'accéder aux ressources (applications, contenu et bureaux) grâce à un navigateur Web ou au Citrix Online Plug-in. L'intégration à la fonction d'application en mode déconnecté permet aux utilisateurs de livrer des applications en streaming sur leurs bureaux et de les lancer localement.

Vous pouvez autoriser les utilisateurs à accéder aux ressources comme suit :

- **Mode connecté.** Les utilisateurs accèdent aux applications, contenus et bureaux hébergés sur des serveurs distants. Les utilisateurs nécessitent une connexion réseau pour pouvoir travailler avec leurs ressources.

- **Mode déconnecté.** Les utilisateurs livrent en streaming des applications sur leurs bureaux pour les ouvrir localement. En ce qui concerne les sites XenApp Services, les utilisateurs peuvent, dès lors que les applications sont disponibles, les exécuter à tout moment sans être connectés au réseau. Pour les sites XenApp Web, les utilisateurs nécessitent des connexions réseau pour ouvrir une session au site et démarrer leurs applications. Une fois les applications exécutées, la connexion n'est plus nécessaire.

- **Mode double.** Les utilisateurs accèdent sur le même site aux applications, contenus et bureaux en mode connecté et déconnecté. Si aucune application en mode déconnecté n'est disponible, les versions en mode connecté sont utilisées, lorsque cela est possible.

Vous pouvez à tout moment mettre à jour ce paramètre à l'aide de la tâche Types de ressources dans la console de gestion de l'Interface Web Citrix. Pour des informations complémentaires sur les types de clients Citrix, consultez la section Gestion des clients.

Mise à niveau des sites existants

Si vous mettez à niveau une version antérieure de l'Interface Web (version 4.5 et supérieure), la mise à niveau des sites est prise en charge (à l'exception des sites Participant invité de Conferencing Manager).

Important : les sites Participant invité de Conferencing Manager ne sont plus pris en charge. Si vous mettez à niveau une version de l'Interface Web antérieure, le programme d'installation supprimera les sites Participant invité de Conferencing Manager existants de votre serveur Web.

Les sites Access Platform/XenApp Web et Services de l'Agent Program Neighborhood/XenApp Services existants sont traités comme suit :

- **Sites configurés localement.** Lors de l'installation, le processus d'installation de l'Interface Web met automatiquement à niveau la dernière version des sites configurés localement.

- **Sites groupés et configurés de manière centralisée.** Durant l'installation, le programme d'installation de l'Interface Web convertit automatiquement les sites groupés et configurés de manière centralisée afin d'utiliser la configuration locale. Les sites convertis sont ensuite mis à niveau vers la dernière version.

Par défaut, l'Interface Web suppose que les noms de fichiers des fichiers d'installation de client sont les mêmes que ceux des fichiers fournis sur le support d'installation de XenApp ou XenDesktop. Si vous téléchargez des clients depuis le site Web Citrix ou que vous prévoyez de déployer des clients antérieurs, vérifiez que les noms des fichiers d'installation de client appropriés sont spécifiés pour les paramètres ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32, et ClientStreamingWin32 dans les fichiers de configuration pour vos sites XenApp Web. Pour de plus amples informations sur les paramètres des fichiers de configuration de l'Interface Web, consultez la section Paramètres WebInterface.conf.

Utilisation des tâches de site

Pour configurer un site, sélectionnez le type de site dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur le site dans le panneau des résultats et sélectionnez une tâche dans la liste des tâches disponibles dans le panneau Actions ou dans le menu Action. Vous pouvez également cliquer avec le bouton droit de la souris sur le nom d'un site dans le panneau des résultats et sélectionner des tâches dans le menu contextuel.

Certaines tâches ne sont disponibles que pour certains types de sites et configurations. Le tableau ci-dessous dresse la liste des tâches disponibles pour chaque type de site.

Tâche	Sites XenApp Web		Sites XenApp Services		Site ADFS intégrés
	Mode connecté/double	Mode déconnecté uniquement	Mode connecté/double	Mode déconnecté uniquement	
Méthode d'authentification	*	*			
Méthodes d'authentification	*	*	*	*	*
Proxy côté client	*		*		*
Déploiement du client	*	*			*
Actualisation des ressources			*	*	
Types de ressources	*	*	*	*	*
Accès sécurisé	*		*		*
Batteries de serveurs	*	*	*	*	*
Paramètres du serveur			*	*	
Options de session			*		
Préférences de session	*	*			*
Raccourcis			*	*	
Maintenance du site	*	*	*	*	*
Apparence du site Web	*	*			*
Contrôle de l'espace de travail	*				*

Réparation et désinstallation de sites

Utilisez les tâches Réparer le site et Désinstaller le site sous Maintenance du site dans la console de gestion de l'Interface Web Citrix pour réparer et supprimer des sites. La désinstallation d'un site entraîne sa suppression complète du système ; vous n'êtes alors plus en mesure d'exécuter des tâches sur ce site.

Important : si vous exécutez la tâche Réparer le site alors que des images et des scripts personnalisés ont été créés pour le site, ces fichiers personnalisés sont supprimés. Ils sont également supprimés si vous utilisez la tâche Gérer l'hébergement IIS. Avant d'utiliser l'une de ces tâches, Citrix vous recommande donc de sauvegarder tous les fichiers que vous avez créés.

Mise à disposition de l'Interface Web auprès des utilisateurs

Une fois l'Interface Web installée et configurée, communiquez l'adresse URL de l'écran Ouvrir une session à vos utilisateurs. Si ces derniers souhaitent ajouter cette page aux Favoris de leurs navigateurs, Citrix conseille d'utiliser le signet http://*nomduserveur*/*chemindusite* sans indiquer de page particulière (telle que login.aspx).

Sur les serveurs d'application Java, le chemin d'accès au site (portion de l'adresse URL située après le nom d'hôte et le port) est déterminé par le moteur de servlet. Si vous installez le fichier .war dans le moteur de servlet, vous pouvez modifier ce chemin. Par défaut, ce chemin est */NomFichierWAR* où *NomFichierWAR* est la première partie du nom de fichier du fichier .war de votre site.

Accès direct à des sites

Si les utilisateurs accèdent aux sites XenApp Web directement ou par le biais d'Access Gateway édition Enterprise à l'aide de Citrix Secure Access Plug-in, vous pouvez activer la prise en charge des adresses URL des ressources. Cette fonctionnalité permet aux utilisateurs de créer des liens persistants vers les ressources accessibles par l'Interface Web.

Remarque : les adresses URL des ressources ne sont pas prises en charge pour les utilisateurs qui accèdent à des sites à l'aide d'Access Gateway édition Standard ou Advanced ou ceux qui accèdent à Access Gateway édition Enterprise sans client.

Les utilisateurs peuvent ajouter des liens persistants à leur liste de raccourcis ou à leur bureau. Pour activer la prise en charge des adresses URL des ressources à l'aide de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web dans le panneau de gauche, sélectionnez le site dans le panneau des résultats, cliquez sur Préférences de session dans le panneau Actions, cliquez sur Adresses URL persistantes et sélectionnez la case Autoriser l'accès aux ressources à l'aide des signets de navigateur.

Important : l'activation de cette fonctionnalité désactive la protection contre les attaques de type Cross-Site Request Forgery (CSRF).

Définition de l'écran Ouvrir une session comme page par défaut sur Microsoft Internet Information Services

Vous pouvez définir l'écran Ouvrir une session de l'Interface Web comme la page par défaut pour les utilisateurs du serveur Web, afin que l'URL soit http://*nomserveur*/. Pour ce faire, sélectionnez la case Définir comme page par défaut du site IIS lors de la création d'un site ou à n'importe quel moment dans la tâche Gérer l'hébergement IIS sous Maintenance du site dans la console de gestion de l'Interface Web Citrix.

Gestion des serveurs et des batteries

Mise à jour : 2014-11-24

Cette section décrit comment configurer l'Interface Web pour communiquer avec vos batteries de serveurs. Elle décrit également comment configurer et gérer les paramètres des serveurs et activer l'équilibrage de charge entre les serveurs exécutant le service XML Citrix.

Considérations sur le changement de mot de passe

S'il existe des différences parmi vos batteries de serveurs, des problèmes supplémentaires peuvent empêcher les utilisateurs de changer de mot de passe. Par exemple :

- La stratégie de domaine peut empêcher les utilisateurs de modifier leur mot de passe.
- Lorsque des batteries XenApp pour UNIX sont regroupées sur un site unique avec des batteries XenApp pour Windows et/ou XenDesktop, seul le mot de passe Windows peut être modifié.

Dans ces cas-là, Citrix vous conseille de désactiver le changement de mot de passe par l'utilisateur.

Si vous regroupez plusieurs batteries, assurez-vous que la première batterie répertoriée dans le fichier de configuration du site exécute Presentation Server 4.5 ou une version supérieure, ou XenDesktop.

Si nécessaire, vous pouvez activer le changement de mot de passe dans un déploiement mixte de batteries de serveurs. L'Interface Web contacte les batteries de serveurs dans l'ordre dans lequel elles sont définies, jusqu'à ce qu'une batterie de serveurs signale que le mot de passe a été modifié avec succès. Le processus est alors interrompu. Cela vous permet de spécifier la batterie de serveurs à laquelle la demande de changement de mot de passe est émise. Si la requête de changement de mot de passe échoue, la batterie de serveurs suivante dans la liste reçoit la requête de changement de mot de passe. Pour conserver la cohérence entre les mots de passe des utilisateurs, utilisez des mécanismes de réplication de mots de passe appropriés entre les batteries de serveurs.

Pour ajouter une batterie de serveur

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.
2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.
3. Dans le panneau Actions, cliquez sur Batteries de serveurs.
4. Cliquez sur Ajouter.
5. Entrez un nom pour la batterie de serveurs dans le champ Nom de batterie.
6. Dans la zone Paramètres de serveur, cliquez sur Ajouter pour spécifier un nom de serveur. Pour modifier un nom de serveur, sélectionnez le nom dans la liste, puis cliquez sur Modifier. Pour supprimer un nom de serveur, sélectionnez-le et cliquez sur Supprimer.
7. Si vous spécifiez plus d'un nom de batterie, sélectionnez un nom dans la liste et cliquez sur les boutons Monter ou Descendre pour le placer dans l'ordre de basculement approprié.

Important : pour assurer la compatibilité avec XenApp 4.0 Feature Pack 1, pour UNIX, vous devez effectuer une configuration supplémentaire pour le site. Pour plus d'informations, veuillez consulter la section Pour configurer la prise en charge de XenApp 4.0, avec Feature Pack 1, pour UNIX.

Pour configurer la tolérance aux défauts

L'Interface Web offre une tolérance de panne entre les serveurs exécutant le service XML Citrix. Utilisez la tâche Batteries de serveurs dans la console de gestion de l'Interface Web Citrix pour configurer la tolérance de panne. Si une erreur se produit lors d'une communication avec un serveur, l'Interface Web ne contacte pas ce serveur tant que le délai indiqué dans le champ Ignorer tout serveur en échec pour ne s'est pas écoulé et les communications se poursuivent avec les serveurs restants de la liste Serveurs.

Par défaut, tout serveur défectueux est ignoré pendant une heure. Si aucun des serveurs présents dans la liste ne répond, l'Interface Web tente de les recontacter toutes les 10 secondes.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Batteries de serveurs.

4. Cliquez sur Ajouter si vous ajoutez une batterie ou sélectionnez un nom dans la liste et cliquez sur Modifier pour configurer une batterie existante.

5. Dans la liste Serveurs, classez les serveurs par ordre de priorité. Sélectionnez un nom dans la liste et utilisez les boutons Monter et Descendre pour placer les serveurs dans l'ordre approprié.

6. Modifiez la période de temps pendant laquelle un serveur défectueux est ignoré dans la boîte de dialogue Ignorer tout serveur en échec pour.

Pour activer l'équilibrage de charge entre les serveurs

Mise à jour : 2014-11-25

Vous pouvez activer l'équilibrage de charge entre les serveurs exécutant le service XML Citrix. L'activation de l'équilibrage de charge vous permet de distribuer équitablement les connexions entre ces serveurs afin qu'aucun serveur ne soit surchargé. Par défaut, l'équilibrage de charge est désactivé.

Si une erreur se produit lors d'une communication avec un serveur, la charge de toute communication ultérieure est équilibrée parmi les serveurs restants dans la liste. Le serveur défectueux est ignoré pour une période de temps donnée (par défaut, une heure), mais vous pouvez modifier ce paramètre en utilisant la tâche Batteries de serveurs dans la console de gestion de l'Interface Web Citrix.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Batteries de serveurs.

4. Cliquez sur Ajouter si vous ajoutez une batterie ou sélectionnez un nom dans la liste et cliquez sur Modifier pour configurer une batterie existante.

5. Dans la liste Serveurs, ajoutez les serveurs que vous souhaitez utiliser pour l'équilibrage de charge.

6. Sélectionnez la case Utiliser la liste des serveurs pour l'équilibrage de charge.

7. Modifiez la période de temps pendant laquelle un serveur défectueux est ignoré dans la boîte de dialogue Ignorer tout serveur en échec pour.

Configuration des paramètres pour tous les serveurs d'une batterie

Vous pouvez utiliser la tâche Batteries de serveurs dans la console de gestion de l'Interface Web Citrix pour spécifier la méthode utilisée par le service Citrix XML pour transporter des données entre l'Interface Web et le serveur exécutant XenApp ou XenDesktop. Le service XML Citrix est un composant de XenApp et XenDesktop qui agit comme point de contact entre la batterie de serveurs et le serveur Interface Web. Par défaut, le numéro de port correspond à la valeur entrée lors de la création d'un site. Ce numéro de port doit correspondre au port utilisé par le service XML Citrix.

Par ailleurs, vous pouvez indiquer la durée d'expiration du ticket généré par le serveur. La fonctionnalité de ticket améliore la sécurité de l'authentification pour les ouvertures de session explicites en éliminant les informations d'identification de l'utilisateur des fichiers .ica envoyés depuis le serveur Web vers les machines utilisateur.

Par défaut, chaque ticket de l'Interface Web a une durée d'expiration de 200 secondes. Vous pouvez modifier la durée de vie du ticket si vous souhaitez, par exemple, adapter ce délai aux performances de votre réseau, car les tickets ayant expiré ne permettent pas d'authentifier des utilisateurs auprès de la batterie de serveurs. Si vous modifiez l’adresse ou les adresses IP d’un serveur exécutant le service XML Citrix, les tickets ne fonctionnent que si vous redémarrez le serveur. Après toute modification de ce type, veillez par conséquent à redémarrer le serveur.

Pour spécifier les paramètres pour tous les serveurs

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Batteries de serveurs.

4. Cliquez sur Ajouter si vous ajoutez une batterie ou sélectionnez un nom dans la liste et cliquez sur Modifier pour configurer une batterie existante.

5. Dans la zone Paramètres de communication, entrez le numéro de port dans le champ Port du service XML. Ce numéro de port doit correspondre au port utilisé par le service XML Citrix.

6. Sous Type de transport, sélectionnez l'une des options suivantes :

   - HTTP. Permet d'envoyer des données via une connexion HTTP standard. Utilisez cette option si vous avez prévu d'autres dispositions pour la sécurité de ce lien.

   - HTTPS. Permet d'envoyer des données via une connexion HTTP sécurisée à l'aide du protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security). Vous devez vous assurer que le service XML Citrix est défini pour partager son port avec IIS et qu'IIS a été configuré pour prendre HTTPS en charge.

   - Relais SSL. Permet de transmettre des données via une connexion sécurisée qui utilise le Relais SSL sur un serveur exécutant XenApp ou XenDesktop pour effectuer l'authentification de l'hôte et le cryptage de données.

7. Si vous utilisez le Relais SSL, spécifiez le port TCP du Relais SSL dans le champ Port du relais SSL (le port par défaut est le port 443). L'Interface Web utilise les certificats racine lors de l'authentification d'un serveur exécutant le Relais SSL. Assurez-vous que tous les serveurs exécutant le Relais SSL sont configurés pour utiliser le même numéro de port.

   Remarque : si vous utilisez le Relais SSL ou HTTPS, assurez-vous que les noms de serveur spécifiés correspondent (notamment la casse) aux noms du certificat du serveur exécutant XenApp ou XenDesktop.

8. Pour configurer la fonctionnalité de ticket, cliquez sur Paramètres de ticket.

9. Entrez la durée de vie des tickets pour les clients Citrix utilisant des ressources en mode connecté dans les champs Durée de vie de ticket ICA.

10. Entrez la durée de vie des tickets pour Citrix Offline Plug-in dans les champs Durée de vie du ticket de streaming.

Spécification des paramètres de serveur avancés

Mise à jour : 2014-12-02

À l'aide de la boîte de dialogue Paramètres avancés, vous pouvez activer le regroupement de sockets et la redirection du contenu, spécifier la durée d'expiration du service XML Citrix et spécifier le nombre de tentatives de connexion au service XML Citrix effectuées avant que la connexion ne soit considérée comme défectueuse.

Pour activer la mise en regroupement des sockets

Lorsque le regroupement de sockets est activé, l'Interface Web conserve un groupe de sockets, au lieu de créer une socket chaque fois qu'elle en a besoin et de la renvoyer au système d'exploitation dès que la connexion est fermée. L'activation de la mise en regroupement des sockets permet d'améliorer les performances, plus particulièrement pour les connexions SSL.

Le regroupement de sockets est uniquement disponible pour les sites créés avec les points d'authentification Sur l'Interface Web ou Sur Access Gateway. Il est activé par défaut. Le regroupement de sockets ne doit pas être utilisé lorsque l'Interface Web est configurée de manière à utiliser un ou plusieurs serveurs exécutant XenApp pour UNIX.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.
2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.
3. Dans le panneau Actions, cliquez sur Batteries de serveurs.
4. Cliquez sur Avancé.
5. Dans la zone Regroupement de sockets, sélectionnez la case à cocher Activer le regroupement de sockets.

Pour activer la redirection de contenu

Vous pouvez utiliser la tâche Batteries de serveurs dans la console de gestion de l'Interface Web Citrix pour activer et désactiver la redirection de contenu du plug-in vers le serveur pour les sites XenApp Services individuels. Ce paramètre annule tous les paramètres de redirection de contenu configurés pour XenApp.

Lorsque vous activez la redirection de contenu du plug-in vers le serveur, les utilisateurs exécutant Citrix Online Plug-in ouvrent le contenu en mode connecté et les fichiers locaux

avec des applications mise à disposition sur les serveurs. Par exemple, un utilisateur Citrix Online Plug-in qui reçoit une pièce jointe dans un logiciel de courrier électronique exécuté localement ouvre la pièce jointe dans une application en mode connecté. Lorsque vous désactivez la redirection de contenu, les utilisateurs ouvrent le contenu en mode connecté et les fichiers locaux avec des applications installées localement.

Par défaut, la redirection de contenu est activée du plug-in vers le serveur pour les sites XenApp Services.

La configuration de la redirection de contenu du plug-in vers le serveur s'effectue en associant les applications à des types de fichiers. Pour de plus amples informations sur l'association de type de fichier, consultez la section Pour associer des types de fichier à des applications publiées.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.
2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Services et sélectionnez votre site dans le panneau des résultats.
3. Dans le panneau Actions, cliquez sur Batteries de serveurs.
4. Cliquez sur Avancé.
5. Dans la zone Redirection du contenu, sélectionnez la case à cocher Activer la redirection du contenu.

Pour configurer les communications avec le service XML Citrix

Par défaut, la communication avec le service XML Citrix doit être établie en moins d'une minute et elle est considérée comme défectueuse au bout de deux tentatives infructueuses. Vous pouvez modifier ces paramètres par défaut à l'aide de la tâche Batteries de serveurs dans la console de gestion de l'Interface Web Citrix.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.
2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.
3. Dans le panneau Actions, cliquez sur Batteries de serveurs.
4. Cliquez sur Avancé.
5. Pour configurer la durée d'expiration de délai du service XML Citrix, saisissez les valeurs appropriées dans les boîtes de dialogue Expiration de délai de la socket.
6. Pour spécifier le nombre de tentatives de communication avec le service XML Citrix avant qu'elle ne soit considérée comme ayant échoué et qu'elle ne soit ignorée, entrez la valeur dans le champ Tentatives de communication avec le service XML.

Gestion des paramètres de serveur

Utilisez la tâche Paramètres du serveur dans la console de gestion de l'Interface Web Citrix pour configurer le mode de communication de Citrix Online Plug-in avec un site et spécifier si, en cas d'échec, les utilisateurs sont redirigés ou non vers des sites similaires.

Pour configurer les paramètres de communication avec le serveur

Utilisez les paramètres de communication avec le serveur pour :

- **Activer la communication SSL/TLS.** L'ouverture de session par carte à puce et les communications SSL/TLS sécurisées entre le plug-in et le serveur Interface Web ne sont pas activées par défaut. Vous pouvez activer la communication SSL/TLS à partir de cette boîte de dialogue ; les adresses URL devront alors appliquer automatiquement le protocole HTTPS. En outre, vous devez activer SSL sur le serveur exécutant XenApp ou XenDesktop.

- **Autoriser l'utilisateur à personnaliser l'adresse URL du serveur.** L'adresse URL du serveur dirige Citrix Online Plug-in vers le fichier de configuration approprié. Le chemin par défaut est déterminé par l'adresse du serveur entrée durant l'installation. Vous pouvez autoriser les utilisateurs à modifier l'adresse URL, ce qui active la case Adresse URL du serveur sur la page Options du serveur de la boîte de dialogue Options de Citrix Online Plug-in.

- **Configurer l'actualisation automatique.** Vous pouvez définir la fréquence à laquelle le plug-in doit actualiser ses paramètres de configuration.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Services et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Paramètres du serveur.

4. Pour sécuriser les communications entre Citrix Online Plug-in et un site, sélectionnez Utiliser SSL/TLS pour les communications entre les plug-ins et ce site.

5. Pour autoriser les utilisateurs à modifier l'adresse URL qui dirige Citrix online plug-in vers le fichier de configuration approprié, sélectionnez Autoriser les utilisateurs à personnaliser l'adresse URL du serveur.

6. Pour configurer la fréquence à laquelle Citrix online plug-in actualise ses paramètres de configuration, sélectionnez Programmer une actualisation automatique chaque et entrez la période d'actualisation en heures, jours, semaines ou années.

Pour spécifier des adresses URL de secours pour Citrix Online Plug-in

Vous pouvez spécifier des serveurs de secours à contacter pour Citrix Online Plug-in si le serveur de l'Interface Web principal n'est pas disponible. Utilisez la tâche Paramètres du serveur dans la console de gestion de l'Interface Web Citrix pour spécifier les adresses URL des serveurs de secours. Dans l'éventualité d'une défaillance du serveur, les utilisateurs sont automatiquement connectés au serveur de secours spécifié préalablement dans la liste Chemins de sites de secours. Si le serveur échoue, Citrix Online Plug-in tente de contacter le serveur suivant dans la liste.

Important : toutes les adresses URL de secours doivent pointer vers des sites qui sont hébergés sur le même type de serveur Web que le site principal. Par exemple, si le site principal est un site Interface Web pour Microsoft Internet Information Services, chaque site de secours doit également être un site Interface Web pour Microsoft Internet Information Services.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.
2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Services et sélectionnez votre site dans le panneau des résultats.
3. Dans le panneau Actions, cliquez sur Paramètres du serveur.
4. Cliquez sur Secours.
5. Cliquez sur Ajouter.
6. Entrez l'adresse URL du site auquel les utilisateurs sont connectés dans le champ Adresse URL de secours. Vous pouvez définir un maximum de cinq adresses URL de secours par site.
7. Cliquez sur OK.
8. Si vous spécifiez plusieurs adresses URL de secours, sélectionnez une adresse URL dans la liste, puis cliquez sur Monter ou Descendre pour les placer dans l'ordre approprié pour le basculement.

Pour configurer la redirection de site

Utilisez les paramètres de redirection pour définir le moment où les utilisateurs sont redirigés vers un site différent. Par exemple, vous créez un nouveau site pour votre DRH et souhaitez rediriger tous les utilisateurs de l'ancien site vers le nouveau site sans qu'ils aient à entrer l'adresse URL manuellement. Vous pouvez spécifier les détails du nouveau site à l'aide de la tâche Paramètres du serveur dans la console de gestion de l'Interface Web Citrix. Les utilisateurs sont redirigés vers le nouveau site immédiatement ou la prochaine fois qu'ils démarrent Citrix Online Plug-in.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Services et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Paramètres du serveur.

4. Cliquez sur Redirection.

5. Choisissez l'une des options suivantes :

   - Si vous ne voulez pas configurer la redirection du site, sélectionnez Ne pas rediriger.

   - Si vous voulez rediriger immédiatement les utilisateurs vers un site similaire, sélectionnez Rediriger lorsque la configuration de Citrix Online Plug-in est actualisée.

   - Si vous voulez rediriger les utilisateurs vers un site similaire lors du prochain lancement du plug-in, sélectionnez Rediriger au prochain démarrage de Citrix Online Plug-in.
6. Entrez l'adresse URL du site de remplacement dans le champ Adresse URL de redirection.

Configuration de l'authentification pour l'Interface Web

Mise à jour : 2014-11-25

Méthodes d'authentification

L'authentification s'effectue lorsqu'un utilisateur accède à des ressources (applications, contenu et bureaux). Si l'authentification réussit, la série de ressources de l'utilisateur s'affiche.

Vous pouvez configurer les méthodes d'authentification suivantes pour l'Interface Web :

- **Explicite (sites XenApp Web) ou invite (sites XenApp Services).** Pour ouvrir une session, les utilisateurs doivent fournir un nom d'utilisateur et un mot de passe. Le nom UPN (nom d'utilisateur principal), l'authentification de domaine Microsoft et NDS (Novell Directory Services) sont disponibles. Dans le cas des sites XenApp Web, l'authentification RSA SecurID et l'authentification SafeWord sont également disponibles.

  Remarque : l'authentification Novell est maintenant disponible avec l'Interface Web pour les serveurs d'application Java et elle n'est pas prise en charge par XenApp 6.0, XenApp 5.0 pour Windows Server 2008 ou XenDesktop. Toutefois, XenApp 6.0 est compatible avec Novell Domain Services pour Windows.

- **Authentification unique.** Les utilisateurs peuvent s'authentifier à l'aide des informations d'identification qu'ils ont fournies en ouvrant une session sur leur bureau Windows physique. Les utilisateurs n'ont pas à entrer ces informations à nouveau. De plus, leurs ressources s'affichent automatiquement. Vous pouvez également utiliser l'authentification Windows intégrée Kerberos pour la connexion aux batteries de serveurs. Si vous spécifiez l'option d'authentification Kerberos et qu'elle échoue, l'authentification unique échoue également et les utilisateurs ne peuvent pas ouvrir de session. Pour plus d'informations sur Kerberos, veuillez consulter la section Configuration de l'ouverture de session Kerberos.

- **Authentification unique avec carte à puce.** Les utilisateurs peuvent s'authentifier en insérant une carte à puce dans un lecteur de carte à puce connecté à la machine utilisateur. Si les utilisateurs ont installé Citrix Online Plug-in, ils sont invités à entrer le code secret de la carte à puce pour ouvrir une session sur la machine utilisateur. Une fois la session ouverte, les utilisateurs peuvent accéder à leurs ressources sans avoir à rouvrir de session. Les utilisateurs qui se connectent à des sites XenApp Web ne sont pas invités à entrer un code secret. Si vous configurez un site XenApp Services, vous pouvez utiliser l'authentification Windows Kerberos intégrée pour vous connecter à l'Interface Web et les cartes à puce pour l'authentification sur la batterie de serveurs. Si vous spécifiez l'option d'authentification Kerberos et qu'elle échoue, l'authentification unique échoue également et les utilisateurs ne peuvent pas ouvrir de session.

Remarque : en raison des améliorations de sécurité introduites dans Windows Vista, les utilisateurs de cartes à puce qui exécutent Vista ou Windows 7 doivent fournir leur code secret lorsqu'ils accèdent à une application, même si vous avez activé l'authentification unique par carte à puce.

- **Carte à puce.** Les utilisateurs peuvent s'authentifier au moyen d'une carte à puce. L'utilisateur est invité à entrer le code secret de la carte à puce.

  Remarque : les méthodes d'authentification unique, d'authentification unique avec carte à puce et d'authentification par carte à puce ne sont pas disponibles avec l'Interface Web pour les serveurs d'application Java.

- **Anonyme.** Les utilisateurs anonymes peuvent ouvrir une session sans fournir de nom d'utilisateur ni de mot de passe et accéder à des ressources publiées à leur intention.

  Important : les utilisateurs anonymes peuvent obtenir des tickets Secure Gateway, même s'ils n'ont pas été authentifiés par l'Interface Web. Or, Secure Gateway utilise l'Interface Web pour émettre des tickets uniquement pour les utilisateurs authentifiés, ce qui, en matière de sécurité, compromet l'un des avantages que constitue l'utilisation de Secure Gateway.

  Remarque : XenDesktop ne prend pas en charge les utilisateurs anonymes.

Recommandations relatives à l'authentification

Si vous prévoyez d'activer l'authentification unique, l'authentification unique avec carte à puce ou l'authentification par carte à puce, prenez ce qui suit en compte :

- Si les utilisateurs ouvrent des sessions sur leurs ordinateurs à l'aide de cartes à puce et que vous souhaitez activer l'authentification unique, sélectionnez l'option permettant d'utiliser l'authentification Kerberos.

- Si les utilisateurs ouvrent des sessions sur leurs ordinateurs à l'aide d'informations d'identification explicites, n'activez pas l'authentification par carte à puce ou l'authentification unique avec carte à puce pour les utilisateurs qui accèdent à l'Interface Web.

  Remarque : lorsque des utilisateurs ouvrent une session Windows à l'aide d'informations d'identification explicites puis accèdent à un site configuré pour une authentification unique par carte à puce, une boîte de dialogue Bienvenue à Windows s'affiche au moment où ils accèdent à des ressources. Pour annuler cette boîte de dialogue, les utilisateurs doivent appuyer sur ALT droit (ALT GR) + SUPPR. Citrix vous recommande de créer des sites distincts pour les utilisateurs utilisant des cartes à puce et ceux utilisant des informations d'identification explicites pour ouvrir des sessions.

Si vous modifiez les méthodes d'authentification à l'Interface Web, il est possible que les utilisateurs qui ont ouvert une session reçoivent des messages d'erreur. Si certains de ces utilisateurs accèdent à l'Interface Web à l'aide d'un navigateur Web, ils doivent fermer et redémarrer leur navigateur avant de rouvrir une session.

Configuration de l'authentification

Utilisez la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix pour configurer la méthode utilisée par les utilisateurs pour s'authentifier auprès de XenApp, XenDesktop et Citrix Online Plug-in.

Pour configurer les paramètres de restriction de domaine

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.
2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.
3. Dans le panneau Actions, cliquez sur Méthodes d'authentification et veillez à ce que l'authentification anonyme ne soit pas la seule méthode d'authentification activée pour les utilisateurs.
4. Cliquez sur Propriétés et sélectionnez Restriction de domaine.
5. Indiquez si vous souhaitez restreindre ou non l'accès des utilisateurs à des domaines sélectionnés. Choisissez parmi les modes suivants :
   - Si vous ne souhaitez pas restreindre l'accès en fonction des domaines, sélectionnez Autoriser tous les domaines.
   - Si vous souhaitez restreindre l'accès des utilisateurs à des domaines sélectionnés, sélectionnez Restreindre aux domaines suivants.
6. Cliquez sur Ajouter.
7. Entrez le nom des domaines que vous souhaitez ajouter à la liste de restriction de domaine dans la boîte de dialogue Domaine d'ouverture de session.

   Remarque : pour restreindre l'accès à des utilisateurs provenant de domaines spécifiques, vous devez entrer les mêmes noms de domaine dans les listes Domaine et Restriction UPN. Pour plus d'informations, veuillez consulter la section Pour utiliser l'authentification de domaine.

Pour configurer les paramètres d'ouverture de session automatique

Utilisez la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix pour configurer les paramètres d'ouverture de session automatique des utilisateurs qui utilisent l'authentification unique, l'authentification unique avec carte à puce ou l'authentification par carte à puce pour accéder à leurs ressources.

Si l'authentification anonyme est la seule méthode d'authentification que les utilisateurs sont autorisés à utiliser, une session est ouverte quels que soient les paramètres configurés par l'administrateur ou l'utilisateur.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Méthodes d'authentification et sélectionnez au moins une des cases suivantes : Authentification unique, Authentification unique avec carte à puce et Carte à puce.

4. Cliquez sur Propriétés et sélectionnez Ouverture de session automatique.

5. Spécifiez si les utilisateurs sont autorisés à ouvrir une session automatiquement et s'ils ont la possibilité d'activer ou de désactiver l'ouverture de session automatique sur l'écran Paramètres de compte.

Pour utiliser l'authentification de domaine

Si vous utilisez l'authentification explicite ou par invite, utilisez la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix pour indiquer si les utilisateurs doivent s'authentifier à l'aide de Windows ou de Novell Directory Services (NDS).

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Méthodes d'authentification et sélectionnez les cases Explicite, Invite et/ou Authentification unique selon vos besoins.

4. Cliquez sur Propriétés et sélectionnez Type d'authentification.

5. Sélectionnez Windows ou NIS (UNIX).

6. Indiquez le format des informations d'identification à utiliser pour l'ouverture des sessions utilisateur. Choisissez l'une des options suivantes :

   - Pour permettre aux utilisateurs d'entrer leurs informations d'ouverture de session, que ce soit sous la forme d'un nom UPN ou d'un nom d'utilisateur de domaine, sélectionnez Nom d'utilisateur de domaine et UPN.

   - Pour indiquer aux utilisateurs qu'ils doivent entrer leurs informations d'ouverture de session sous la forme d'un nom d'utilisateur de domaine uniquement, sélectionnez Nom d'utilisateur de domaine uniquement.

   - Pour indiquer aux utilisateurs qu'ils doivent entrer leurs informations d'ouverture de session sous la forme d'un nom UPN, sélectionnez UPN uniquement.
7. Cliquez sur Paramètres.

8. Dans la zone Affichage de domaines, configurez les paramètres suivants :

   - affichage ou masquage du champ Domaine sur l'écran d'ouverture de session ;

   - pré-remplissage du champ Domaine avec une liste de domaines dans laquelle les utilisateurs font un choix ou saisie manuelle d'une valeur par l'utilisateur dans le champ Domaine ;

     Remarque : si, lors d'une ouverture de session, un utilisateur reçoit un message d'erreur « Vous devez spécifier au moins un domaine », cela peut signifier qu'un champ de domaine est vide. Pour résoudre ce problème, sélectionnez Masquer la case de domaine. Si votre batterie contient uniquement des serveurs XenApp pour UNIX, sélectionnez Pré-rempli dans la liste déroulante Liste de domaines et ajoutez UNIX comme nom de domaine.

   - domaines que vous souhaitez voir apparaître dans la case Domaine sur l'écran Ouvrir une session.

9. Dans la zone Restriction UPN, configurez les paramètres suivants :

   - acceptation ou non de tous les suffixes UPN (Noms d'utilisateurs principaux). Par défaut, tous les suffixes UPN sont autorisés ;

   - sélection des suffixes UPN à accepter.

     Remarque : pour restreindre l'accès à des utilisateurs provenant de domaines spécifiques, vous devez entrer les mêmes noms de domaine dans les listes Domaine et Restriction UPN. Pour plus d'informations, veuillez consulter la section Configuration de l'authentification.

Pour utiliser l'authentification Novell Directory Services

Si vous utilisez l'authentification explicite ou par invite, utilisez la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix pour indiquer si les utilisateurs doivent s'authentifier à l'aide de Windows ou de Novell Directory Services (NDS).

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Méthodes d'authentification et sélectionnez les cases Explicite, Invite et/ou Authentification unique selon vos besoins.

4. Cliquez sur Propriétés et sélectionnez Type d'authentification.

5. Sélectionnez NDS.

6. Entrez un nom dans le champ Arborescence par défaut.

7. Cliquez sur Paramètres et configurez une restriction de contexte ou une authentification sans contexte.

   Remarque : par défaut, eDirectory ne fournit pas d'accès de connexion anonyme à l'attribut cn, nécessaire à l'ouverture de session sans contexte. Pour plus d'informations sur la reconfiguration de eDirectory, veuillez consulter le site http://developer.novell.com/wiki/index.php/Developer_Home.

8. Pour les sites XenApp Services, sélectionnez Utiliser les informations d'identification Windows si vous voulez que les utilisateurs de Citrix Online Plug-in (qui ont installé le client Novell) utilisent leurs informations d'identification Windows pour l'authentification unique.

Activation de l'authentification explicite

Si l'authentification explicite est activée, les utilisateurs doivent disposer d'un compte utilisateur et fournir les informations d'identification appropriées pour ouvrir une session.

Vous pouvez modifier les paramètres d'authentification explicite à l'aide de la console. Vous pouvez, par exemple, indiquer si les utilisateurs sont autorisés à modifier leur mot de passe dans une session.

L'authentification explicite est disponible pour les sites XenApp Web uniquement.

Pour activer l'authentification explicite

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Méthodes d'authentification et sélectionnez la case Explicite.

4. Cliquez sur Propriétés pour configurer d'autres paramètres d'authentification explicite.

Pour configurer les paramètres de mot de passe pour l'authentification explicite

Utilisez la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix pour configurer les options de changement de mot de passe et d'expiration du mot de passe des utilisateurs. certains paramètres de mot de passe sont affectés par d'autres paramètres d'authentification configurés pour un site :

- L'option À tout moment est désactivée si vous sélectionnez les options RSA SecurID et Utiliser l'intégration de mot de passe Windows dans la page Authentification à deux facteurs.

- Sélectionner l'option Utiliser les paramètres de rappel de la stratégie de groupe Active Directory peut signifier que les paramètres de rappel sont configurés selon votre stratégie Windows actuelle. Si aucune période de rappel n'a été définie pour votre stratégie Windows actuelle, les utilisateurs ne recevront aucun message les invitant à modifier leur mot de passe actuel avant que celui-ci n'expire.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Méthodes d'authentification et sélectionnez la case Explicite.

4. Cliquez sur Propriétés et sélectionnez Paramètres de mot de passe.

5. Si vous souhaitez que les utilisateurs puissent changer leur mot de passe au cours d'une session Interface Web, sélectionnez la case à cocher Autoriser les utilisateurs à changer de mot de passe.

6. Pour spécifier le moment où les utilisateurs peuvent changer de mot de passe, choisissez l'une des options suivantes.

   - Pour permettre aux utilisateurs de modifier leur mot de passe quand celui-ci expire, sélectionnez l'option Seulement lors de l'expiration. Avec cette option, si les utilisateurs ne parviennent pas à ouvrir une session sur l'Interface Web parce que leur mot de passe a expiré, ils sont redirigés vers la boîte de dialogue Modifier le mot de passe. Après avoir changé de mot de passe, les utilisateurs sont connectés automatiquement à l'aide du nouveau mot de passe.

   - Pour permettre aux utilisateurs de modifier leur mot de passe aussi souvent qu'ils le souhaitent, sélectionnez À tout moment. Lorsque vous sélectionnez cette option, le bouton Modifier le mot de passe apparaît sur l'écran Applications et Paramètres de compte des utilisateurs. Lorsque les utilisateurs cliquent sur ce dernier, une boîte de dialogue dans laquelle les utilisateurs peuvent saisir leur nouveau mot de passe apparaît.

7. Pour configurer un message de rappel informant les utilisateurs que leur mot de passe va bientôt expirer, choisissez l'une des options suivantes :

   - Si vous ne souhaitez pas notifier les utilisateurs avant que leur mot de passe expire, sélectionnez Ne pas effectuer de rappel.

   - Pour utiliser les paramètres de rappel de la stratégie Windows, sélectionnez Utiliser les paramètres de rappel de la stratégie de groupe Active Directory.

   - Pour rappeler aux utilisateurs que leur mot de passe va expirer dans un nombre défini de jours, sélectionnez l'option Utiliser un paramètre de rappel personnalisé. Spécifiez le nombre de jours, semaines ou années dans les boîtes de dialogue Rappeler aux utilisateurs avant expiration.

Pour activer l'authentification à deux facteurs

Utilisez la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix pour activer l'authentification à deux facteurs pour les utilisateurs, si nécessaire.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Méthodes d'authentification et sélectionnez la case Explicite.

4. Cliquez sur Propriétés et sélectionnez Authentification à deux facteurs.

5. Sélectionnez le type d'authentification à deux facteurs que vous souhaitez utiliser dans la liste Paramètre à deux facteurs et configurez les paramètres supplémentaires selon vos besoins.

Pour plus d'informations sur la configuration de l'authentification Aladdin SafeWord, RSA SecurID et RADIUS, consultez la section Configuration de l'authentification à deux facteurs.

Configuration du libre-service de compte

L'intégration à la fonctionnalité de libre-service de compte disponible sur Password Manager permet aux utilisateurs de réinitialiser leur mot de passe réseau et de déverrouiller leur compte en répondant à une série de questions de sécurité.

L'activation du libre-service de compte sur un site révèle des fonctions de sécurité sensibles à toute personne pouvant accéder à ce site. Si votre site est accessible depuis Internet, il n'existe aucune restriction sur les personnes pouvant avoir accès à ces fonctions. Si votre organisation possède une stratégie de sécurité qui restreint les fonctions de gestion de compte utilisateur à un usage interne uniquement, vous devez vous assurer que votre site n'est pas accessible en-dehors de votre réseau interne.

Important : lors de l'installation de Password Manager, vous indiquez quels utilisateurs sont autorisés à réinitialiser leur mot de passe et à déverrouiller leur compte. Si vous activez ces fonctionnalités pour l'Interface Web, il se peut que les utilisateurs ne soient pas autorisés à réaliser ces tâches en fonction des paramètres configurés dans Password Manager.

Seuls les utilisateurs qui accèdent à l'Interface Web à l'aide de connexions HTTPS peuvent utiliser le libre-service de compte. Si des utilisateurs tentent d'accéder à l'Interface Web à l'aide d'une connexion HTTP, le libre-service de compte ne sera pas disponible. Le libre-service de compte n'est pas disponible pour les sites intégrés Access Gateway.

Le libre-service de compte ne prend pas en charge l'ouverture de session à l'aide d'un nom UPN, tel que *nomd'utilisateur@domaine.com*.

Avant de configurer le libre-service de compte pour un site, vous devez vous assurer que :

- Le site est configuré pour utiliser une authentification explicite basée sur les systèmes d'exploitation Windows.
- Le site est configuré pour utiliser un seul service Password Manager. Si l'Interface Web est configurée pour utiliser de nombreuses batteries au sein d'un même domaine ou de plusieurs domaines de confiance, Password Manager doit être configuré pour accepter les informations d'identification de tous ces domaines.
- Le site est configuré pour permettre aux utilisateurs de changer leur mot de passe à n'importe quel moment, dans le cas où vous activez la fonctionnalité de réinitialisation du mot de passe.

Pour configurer le libre-service de compte

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Méthodes d'authentification et sélectionnez la case Explicite.

4. Cliquez sur Propriétés et sélectionnez Libre-service de compte.

5. Spécifiez si vous souhaitez ou non que les utilisateurs puissent réinitialiser leurs mots de passe ou déverrouiller leurs comptes.

6. Saisissez l'adresse URL de Password Manager dans la boîte de dialogue Adresse URL du service Password Manager.

Activation de l'authentification par invite

Mise à jour : 2014-11-24

Si l'authentification par invite est activée, les utilisateurs doivent disposer d'un compte utilisateur et fournir les informations d'identification appropriées pour ouvrir une session.

L'authentification explicite est disponible pour les sites XenApp Services uniquement.

Pour activer l'authentification par invite

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.
2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Services et sélectionnez votre site dans le panneau des résultats.
3. Dans le panneau Actions, cliquez sur Méthodes d'authentification et sélectionnez la case Invite.
4. Cliquez sur Propriétés pour configurer d'autres paramètres d'authentification par invite.

Pour configurer les paramètres de mot de passe pour l'authentification par invite

Utilisez la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix pour indiquer si les utilisateurs sont autorisés à enregistrer leur mot de passe et pour configurer les options de modification de mot de passe mises à la disposition des utilisateurs.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.
2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Services et sélectionnez votre site dans le panneau des résultats.
3. Dans le panneau Actions, cliquez sur Méthodes d'authentification et sélectionnez la case Invite.
4. Cliquez sur Propriétés et sélectionnez Paramètres de mot de passe.
5. Pour permettre aux utilisateurs d'enregistrer leur mot de passe, sélectionnez l'option Autoriser l'enregistrement des mots de passe.
6. Si vous souhaitez que les utilisateurs puissent changer leur mot de passe lorsque ce dernier expire, sélectionnez la case Autoriser les utilisateurs à changer les mots de passe expirés en contactant.

7. Spécifiez le chemin par lequel la demande de modification de mot de passe est acheminée en choisissant l'une des options suivantes :

   - Si vous souhaitez autoriser les utilisateurs de Citrix Online Plug-in à modifier leur mot de passe en se connectant directement au contrôleur de domaine, sélectionnez Contrôleur de domaine directement. Il s'agit de l'option la plus sécurisée, car la requête de modification du mot de passe, au lieu de passer par l'Interface Web et XenApp/XenDesktop, est acheminée directement depuis Citrix Online Plug-in vers le contrôleur de domaine.

   - Si vous préférez autoriser les utilisateurs de Citrix Online Plug-in à modifier leur mot de passe en se connectant directement au contrôleur de domaine, mais que vous souhaitez également autoriser les connexions via l'Interface Web et XenApp/XenDesktop lorsque la méthode de connexion préférée échoue, sélectionnez Contrôleur de domaine directement, avec retour vers la batterie de serveur.

   - Si vous souhaitez autoriser les utilisateurs de Citrix Online Plug-in à modifier leur mot de passe en se connectant au contrôleur de domaine par l'intermédiaire de l'Interface Web et XenApp/XenDesktop, sélectionnez Batterie de serveurs. Cette option garantit la mise à niveau des mots de passe de l'Interface Web et de XenApp et/ou XenDesktop lorsqu'ils sont modifiés par les utilisateurs. Toutefois, cette option est potentiellement moins sûre car le nouveau mot de passe est routé par un plus grand nombre de connexions réseau.

Activation de l'authentification unique

Mise à jour : 2013-02-21

Grâce à la console, vous pouvez activer l'authentification unique pour les utilisateurs qui ouvrent une session sur leur bureau physique à l'aide de leur nom d'utilisateur, de leur mot de passe et des informations d'identification de domaine. Cette fonction leur permet de s'authentifier à l'aide des informations d'identification qu'ils ont fournies en ouvrant une session sur leur bureau Windows physique. Les utilisateurs n'ont pas à entrer ces informations à nouveau. De plus, leurs ressources s'affichent automatiquement.

Configuration requise pour l'authentification unique

Pour utiliser la fonctionnalité d'authentification unique, l'Interface Web doit être exécutée sur IIS et les utilisateurs doivent exécuter des versions prises en charge d'Internet Explorer. Pour les sites XenApp Web, les utilisateurs doivent ajouter le site à la zone Sites de confiance Windows ou à la zone Intranet local à l'aide d'Internet Explorer.

Si vous utilisez Internet Explorer Version 7 ou version ultérieure :

1. Ajoutez le site aux sites de confiance Windows, cliquez sur Options Internet puis naviguez vers l'onglet Sécurité.

2. Mettez en surbrillance la zone Sites de confiance puis cliquez sur le niveau Personnalisé.

3. Naviguez jusqu'à la fin de la fenêtre Paramètres de sécurité jusqu'à Authentification utilisateur, cliquez sur Ouverture de session, puis définissez-la sur Ouverture de session automatique avec le nom d'utilisateur et le mot de passe courant.

Lorsqu'IIS 7.*x* est exécuté sur Windows Server 2008, assurez-vous que le service de rôle Serveur Web > Sécurité > Authentification Windows est activé pour le rôle Serveur Web (IIS).

Important : si vos serveurs exécutent des versions antérieures à Citrix MetaFrame XP Feature Release 2, les utilisateurs peuvent visualiser toutes les applications ainsi que le contenu lorsqu'ils utilisent l'authentification unique.

Si les utilisateurs utilisent des clients pour Windows antérieurs à la version 6.30 et que le cryptage ICA (SecureICA) est activé, l'authentification unique ne peut pas être utilisée. Pour activer ce type d'authentification avec le cryptage ICA, vos utilisateurs doivent installer les derniers clients Citrix. L'authentification unique n'est pas disponible avec l'Interface Web pour les serveurs d'application Java.

Important : lorsqu'un utilisateur accède à une ressource, un fichier est envoyé au client Citrix (dans certains cas à l'aide du navigateur Web en tant qu'intermédiaire). Ce fichier peut contenir un paramètre ordonnant au client d'envoyer les informations d'identification du poste de travail de l'utilisateur au serveur. Par défaut, le client ne reconnaît pas ce paramètre ; néanmoins, si la fonctionnalité d'authentification unique est activée sur Citrix Online Plug-in, il y a un risque qu'un agresseur envoie à l'utilisateur un

fichier entraînant le détournement des informations d'identification de l'utilisateur vers un faux serveur ou un serveur non autorisé. C'est pourquoi vous ne devez utiliser l'authentification unique que dans des environnements sécurisés et approuvés.

Étape 1 : installation du plug-in pour l'authentification unique

Mise à jour : 2014-12-02

Vous devez installer Citrix Online Plug-in ou Citrix Desktop Viewer sur les machines de vos utilisateurs à l'aide d'un compte d'administrateur. L'authentification unique est uniquement disponible avec ces plug-ins, qui sont disponibles sur le support d'installation de XenApp et XenDesktop. Pour des raisons de sécurité, Citrix Online Plug-in – Web ne contient pas cette fonctionnalité. Cela signifie que vous ne pouvez pas utiliser d'installation du client par le Web pour déployer des plug-ins Citrix contenant cette fonctionnalité auprès de vos utilisateurs.

Une fois l'installation terminée, vous devez activer l'authentification unique sur tous les clients Citrix utilisant la stratégie de groupe. Pour de plus amples informations, consultez l'article http://support.citrix.com/article/CTX122676 et la documentation Online Plug-in pour Windows archivée.

Étape 2 : activation de l'authentification unique pour les plug-ins

L'activation de l'authentification unique pour les clients se déroule en deux étapes. Vous ajoutez tout d'abord le modèle de client à l'Éditeur d'objet de stratégie de groupe. Ceci fait, utilisez ce modèle pour activer l'authentification unique sur tous les clients.

Pour ajouter le modèle de client à l'Éditeur d'objet de stratégie de groupe pour l'authentification unique

1. Ouvrez le composant logiciel enfichable MMC Éditeur d'objet Stratégie de groupe.
2. Sélectionnez l'objet de stratégie de groupe que vous souhaitez modifier.
3. Sélectionnez le nœud Modèles d'administration, et, dans le menu Action, cliquez sur Ajout/Suppression de modèles.
4. Cliquez sur Ajouter et recherchez le fichier modèle de client, icaclient.adm. Ce fichier est installé dans le dossier \Configuration pour les clients, généralement C:\Program Files (x86)\Citrix*Nomduclient*\Configuration.
5. Cliquez sur Ouvrir pour ajouter le modèle et cliquez sur Fermer.

Pour activer l'authentification unique pour tous les clients

1. Ouvrez le composant logiciel enfichable MMC Éditeur d'objet Stratégie de groupe.
2. Sélectionnez l'objet de stratégie de groupe que vous souhaitez modifier.
3. Dans le panneau de gauche, développez le nœud Modèles d'administration.
4. Sélectionnez Modèles d'administration classiques (ADM) > Citrix Components. Développez le nœud du client que vous avez installé et sélectionnez User authentication.
5. Dans le panneau des résultats, sélectionnez Local user name and password.
6. Dans le menu Action, cliquez sur Modifier.
7. Cliquez sur Activé et vérifiez que la case Enable pass-through authentication est sélectionnée.
8. Assurez-vous que toutes les étapes ci-dessus sont terminées pour l'utilisateur et l'ordinateur dans l'Éditeur d'objet de stratégie de groupe.
9. Fermez la session, puis ouvrez-en une nouvelle pour que les modifications que vous avez apportées à votre stratégie soient prises en compte.

Étape 3 : activation de l'authentification unique à l'aide de la console

Utilisez la console de gestion de l'Interface Web Citrix pour activer l'authentification unique. Lorsque cette fonction est activée, les utilisateurs n'ont pas besoin d'entrer à nouveau leurs informations d'identification et leurs ressources s'affichent automatiquement.

Par ailleurs, vous pouvez activer Kerberos avec l'authentification unique pour les sites XenApp Web et XenApp Services. Pour les sites XenApp Services, vous pouvez également spécifier Kerberos pour l'authentification unique avec carte à puce.

Pour activer l'authentification unique

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Méthodes d'authentification et sélectionnez la case Authentification unique.

4. Cliquez sur Propriétés et sélectionnez Authentification Kerberos.

5. Si vous souhaitez activer l'authentification Kerberos, sélectionnez la case Utiliser l'authentification Kerberos pour se connecter aux serveurs (pour les sites XenApp Web) ou la case N'utiliser que Kerberos (pour les sites XenApp Services).

Activation de l'authentification par carte à puce

Mise à jour : 2014-12-02

Pour utiliser l'authentification par carte à puce, l'Interface Web doit être exécutée sur IIS et les utilisateurs doivent exécuter des versions prises en charge d'Internet Explorer ou de Firefox. Pour l'authentification unique avec carte à puce, les utilisateurs doivent exécuter des versions prises en charge d'Internet Explorer ; Firefox n'est pas pris en charge.

Si vous planifiez d'activer l'authentification unique par carte à puce pour un site XenApp Web, les utilisateurs doivent ajouter le site à la zone Sites de confiance Windows ou à la zone Intranet local à l'aide d'Internet Explorer.

Lorsqu'IIS 7.*x* est exécuté Windows Server 2008, assurez-vous que le service de rôle Serveur Web > Sécurité > Authentification par mappage de certificat client est activé pour le rôle Serveur Web (IIS). Si vous planifiez d'activer l'authentification unique par carte à puce, assurez-vous que le service de rôle Serveur Web > Sécurité > Authentification Windows est également activé.

L'authentification par carte à puce n'est pas prise en charge par l'Interface Web pour les serveurs d'application Java.

SSL (Secure Sockets Layer) doit être activé sur le serveur Web car ce protocole de sécurité est utilisé pour protéger les communications entre le navigateur Web et le serveur. Pour de plus amples informations, consultez la documentation accompagnant votre serveur Web.

Pour activer l'authentification par carte à puce (avec ou sans autre méthode d'authentification), vous devez configurer l'écran Ouvrir une session pour qu'il soit uniquement accessible via des connexions HTTPS. Si le protocole HTTP standard est utilisé ou si le protocole HTTPS est mal configuré, les utilisateurs reçoivent un message d'erreur et ne peuvent pas ouvrir de session. Pour éviter ce problème, fournissez l'adresse URL HTTPS complète auprès de tous les utilisateurs ; par exemple, https://www.*Masociété.fr*:443/Citrix/XenApp.

Pour plus d'informations sur la configuration requise sur la machine cliente et la configuration requise sur le serveur pour l'authentification par carte à puce, veuillez consulter la section Utilisation de cartes à puce avec XenApp.

Étape 1 : installation du plug-in pour l'authentification par carte à puce

Pour utiliser l'authentification par carte à puce, les utilisateurs doivent installer Citrix Online Plug-in ou Citrix Desktop Viewer. Ils peuvent également utiliser l'installation des clients par le Web pour télécharger et installer Citrix Online Plug-in – Web à partir d'un site XenApp Web configuré à cet effet. Toutefois, pour utiliser l'authentification unique avec l'authentification par carte à puce, vous devez installer Citrix Online Plug-in ou Citrix Desktop Viewer sur les machines de vos utilisateurs à l'aide d'un compte d'administrateur. L'authentification unique est uniquement disponible avec ces plug-ins, qui sont disponibles sur le support d'installation de XenApp et XenDesktop. Pour des raisons de sécurité, Citrix Online Plug-in – Web ne contient pas cette fonctionnalité.

Si vous planifiez d'activer l'authentification unique par carte à puce, vous devez tout d'abord activer l'authentification unique pour tous les clients Citrix à l'aide d'une stratégie de groupe après avoir installé le plug-in. L'activation de l'authentification unique pour les clients se déroule en deux étapes. Vous ajoutez tout d'abord le modèle de client à l'Éditeur d'objet de stratégie de groupe. Ceci fait, utilisez ce modèle pour activer l'authentification unique sur tous les clients.

Pour ajouter le modèle de client à l'Éditeur d'objet de stratégie de groupe pour l'authentification unique

1. Ouvrez le composant logiciel enfichable MMC Éditeur d'objet Stratégie de groupe.
2. Sélectionnez l'objet de stratégie de groupe que vous souhaitez modifier.
3. Sélectionnez le nœud Modèles d'administration, et, dans le menu Action, cliquez sur Ajout/Suppression de modèles.
4. Cliquez sur Ajouter et recherchez le fichier modèle de client, icaclient.adm. Ce fichier est installé dans le dossier \Configuration pour les clients, généralement C:\Program Files (x86)\Citrix*Nomduclient*\Configuration.
5. Cliquez sur Ouvrir pour ajouter le modèle et cliquez sur Fermer.

Pour activer l'authentification unique par carte à puce pour tous les clients

1. Ouvrez le composant logiciel enfichable MMC Éditeur d'objet Stratégie de groupe.
2. Sélectionnez l'objet de stratégie de groupe que vous souhaitez modifier.
3. Dans le panneau de gauche, développez le nœud Modèles d'administration.
4. Sélectionnez Modèles d'administration classiques (ADM) > Citrix Components. Développez le nœud du client que vous avez installé et sélectionnez User authentication.
5. Dans le panneau des résultats, sélectionnez Smart card authentication.
6. Dans le menu Action, cliquez sur Modifier.
7. Cliquez sur Activé et sélectionnez les cases Allow smart card authentication et Use pass-through authentication for PIN.

Étape 2 : activation du mappeur du service d'annuaire Windows

Pour activer l’authentification par carte à puce, vous devez vous assurer que le mappeur du service d'annuaire Windows est activé sur le serveur Interface Web.

L'authentification pour l'Interface Web utilise des comptes de domaine Windows ; il s'agit, en d'autres termes, d'une identification par nom d'utilisateur et mot de passe. Les cartes à puce contiennent toutefois des certificats. Le mappeur du service d'annuaire utilise Windows Active Directory pour mapper un certificat avec un compte de domaine Windows.

Pour activer le mappeur du service d'annuaire Windows sur Microsoft Internet Information Services 7.x

1. Sur le serveur Interface Web, assurez-vous que le service de rôle Serveur Web > Sécurité > Authentification par mappage de certificat client IIS n'est *pas* installé pour le rôle Serveur Web (IIS).
2. Ouvrez le composant logiciel enfichable MMC Internet Information Services (IIS) Manager.
3. Sélectionnez votre serveur Web dans le panneau de gauche, et dans Affichage des fonctionnalités, cliquez deux fois sur Authentification.
4. Sur la page Authentification, activez la méthode Authentication du certificat client Active Directory.

Pour activer le mappeur du service d'annuaire Windows sur Microsoft Internet Information Services 6.0

1. Ouvrez le composant enfichable MMC Internet Information Services (IIS) Manager sur le serveur Interface Web.
2. Sélectionnez le nœud Sites Web situé sous le serveur Interface Web, et dans le panneau Action, cliquez sur Propriétés.
3. Dans la section Communications sécurisées de l'onglet Sécurité du répertoire, sélectionnez Activer le mappeur du service d'annuaire Windows.

Étape 3 : activation de l'authentification par carte à puce sur l'Interface Web

Vous devez configurer l'Interface Web pour activer l'authentification par carte à puce (afin que les utilisateurs puissent accéder à l'Interface Web et obtenir leurs séries de ressources) et l'authentification sur le serveur (afin que les utilisateurs puissent accéder à des ressources dans une session à l'aide de l'Interface Web).

Pour activer l’authentification par carte à puce pour les sites XenApp Web

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.
2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web et sélectionnez votre site dans le panneau des résultats.
3. Dans le panneau Actions, cliquez sur Méthodes d'authentification et sélectionnez la case Carte à puce ou Authentification unique avec carte à puce.
4. Cliquez sur Propriétés pour configurer d'autres paramètres pour l'authentification par carte à puce.

Pour activer l’authentification par carte à puce pour les sites XenApp Services

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Services et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Méthodes d'authentification et sélectionnez la case Carte à puce ou Authentification unique avec carte à puce.

4. Cliquez sur Propriétés et sélectionnez Itinérance.

5. Pour configurer le comportement de l'Interface Web lorsqu'une carte est retirée, sélectionnez Activer l'itinérance et choisissez l'une des options suivantes :

   - Pour déconnecter la session d'un utilisateur lorsque la carte à puce est retirée, sélectionnez Déconnecter les sessions lors du retrait d'une carte à puce.

   - Pour fermer la session d'un utilisateur lorsque la carte à puce est retirée, sélectionnez Fermer les sessions lors du retrait d'une carte à puce.
6. Si vous avez activé l'authentification unique par carte à puce et que vous souhaitez utiliser l'authentification Kerberos entre le plug-in et le site XenApp Services, cliquez sur Authentification Kerberos et sélectionnez la case Utiliser Kerberos pour l'authentification sur le site XenApp Services.

Exemple : activation de l'authentification par carte à puce pour les utilisateurs

Vous souhaitez activer l'authentification par carte à puce pour un utilisateur. L'utilisateur exécute Windows XP. Un lecteur de carte à puce est rattaché à l'ordinateur et la prise en charge des cartes à puce est configurée sur la batterie de serveurs. L'Interface Web est configurée pour une authentification explicite/par invite uniquement (nom utilisateur et mot de passe).

Pour activer l'authentification unique par carte à puce

1. Utilisez le support d'installation approprié pour installer Citrix Online Plug-in ou Citrix Desktop Viewer sur l'ordinateur de l'utilisateur. L'installation du plug-in est effectuée à l'aide d'un compte d'administrateur. Pour les sites XenApp Web, ajoutez le site à la zone Sites de confiance Windows ou à la zone Intranet local à l'aide d'Internet Explorer sur l'ordinateur de l'utilisateur.

2. Activez l'authentification unique pour tous les clients Citrix utilisant la stratégie de groupe. Pour plus d'informations, veuillez consulter la section Étape 1 : installation du plug-in pour l'authentification par carte à puce. Vous devez également vous assurer que l'authentification unique est activée sur la batterie. Pour de plus amples informations, consultez la documentation accompagnant votre serveur Citrix.

3. Assurez-vous que le mappeur du service d'annuaire Windows est activé. Pour plus d'informations, veuillez consulter la section Étape 2 : activation du mappeur du service d'annuaire Windows.

4. Utilisez la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix pour activer l'authentification par carte à puce. Pour des informations complémentaires, veuillez consulter la section Étape 3 : activation de l'authentification par carte à puce sur l'Interface Web. Les utilisateurs se connectent sur leurs bureaux Windows physiques à l'aide de leurs cartes à puce. Lorsqu'ils accèdent à leurs ressources, ils sont connectés automatiquement. Lorsque l'authentification par carte à puce est activée sans authentification unique, les utilisateurs doivent entrer à nouveau leur code PIN pour accéder à leurs ressources.

Configuration de l'authentification à deux facteurs

Vous pouvez configurer les méthodes d'authentification à deux facteurs suivantes pour les sites XenApp Web :

- **Aladdin SafeWord pour Citrix.** Méthode d'authentification qui utilise des codes alphanumériques générés par les jetons SafeWord et, facultativement, des codes PIN pour créer un passcode. Avant de pouvoir accéder aux applications du serveur, les utilisateurs doivent saisir les informations d'identification de leur domaine et leurs PASSCODES SafeWord dans l'écran Ouvrir une session.

- **RSA SecurID.** Méthode d’authentification qui utilise des nombres générés par les jetons RSA SecurID (*tokencodes*) et des codes PIN pour créer un *PASSCODE*. Avant de pouvoir accéder aux ressources sur le serveur, les utilisateurs doivent saisir leurs noms d’utilisateurs, leurs domaines, leurs mots de passe et leurs PASSCODES RSA SecurID dans l'écran Ouvrir une session. Lors de la création d’utilisateurs sur le serveur RSA ACE, les noms d'ouverture de session des utilisateurs doivent être les mêmes que leurs noms d’utilisateurs de domaine.

  Remarque : lors de l'utilisation de l'authentification RSA SecurID, le système peut générer et afficher un nouveau code secret pour l'utilisateur. Ce code secret s'affiche pendant 10secondes ou jusqu'à ce que l'utilisateur clique sur OK ou Annuler, ceci afin que le code secret ne puisse pas être vu par d'autres personnes. Cette fonctionnalité n'est pas disponible sur les ordinateurs de poche.

- **Serveur RADIUS.** Méthode d'authentification qui utilise le protocole d'authentification RADIUS (Remote Authentication Dial-in User Service) plutôt qu'un logiciel d'agent propriétaire. SafeWord et SecurID peuvent, tous deux, être installés et configurés pour être présentés en tant que serveur RADIUS. L'authentification RADIUS est la seule option d'authentification à deux facteurs disponible pour l'Interface Web pour les serveurs d'application Java.

Activation de l'authentification SafeWord sur Microsoft Internet Information Services

Cette section décrit l'activation de la prise en charge de RSA SecurID 6.0.

Configuration SafeWord requise

Pour utiliser l'authentification SafeWord avec l'Interface Web pour Microsoft Internet Information Services :

- Vous devez vous procurer la dernière version de l'agent SafeWord auprès de Aladdin Knowledge Systems. Si la prise en charge de l'authentification UPN est requise, appliquez les dernières mises à jour automatiques à l'agent SafeWord pour l'Interface Web et au serveur SafeWord.
- Vous devez vous assurer que l'Interface Web est installée avant d'installer l'agent SafeWord pour l'Interface Web.
- Vous devez vous assurer que l'agent SafeWord pour l'Interface Web est installé sur le serveur Interface Web.

Pour plus d'informations sur la configuration de votre produit SafeWord, veuillez consulter le site http://www.aladdin.com/safeword/default.aspx.

Activation de l'authentification RSA SecurID à l'aide de la console

Vous devez configurer l'Interface Web pour activer l'authentification RSA SecurID de sorte que les utilisateurs puissent avoir accès à leurs ressources et les afficher. Pour ce faire, utilisez la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix.

Activation de l'authentification RSA SecurID sur Microsoft Internet Information Services

Mise à jour : 2014-11-24

Cette section décrit l'activation de la prise en charge de RSA SecurID 7.0.

Configuration requise pour SecurID

Pour utiliser l'authentification SecurID avec l'Interface Web pour Microsoft Internet Information Services :

- L’Agent RSA ACE pour Windows 7.0 ou version ultérieure doit être installé sur le serveur Web.
- L'Interface Web doit être installée après l’Agent RSA ACE.
- L'Interface Web doit être hébergée sur Microsoft Internet Information Services 6.0.

Ajout du serveur Interface Web en tant qu'Agent Host

Vous devez créer un Agent Host pour le serveur Web dans la base de données du serveur RSA ACE, afin que ce dernier reconnaisse et accepte les requêtes d’authentification provenant du serveur Web. Lors de la création de l'Agent Host, configurez l'Interface Web en tant que NetOS Agent. Ce paramètre est utilisé par le serveur RSA ACE pour déterminer la méthode à utiliser pour communiquer avec l'Interface Web.

Copie du fichier sdconf.rec

Localisez le fichier sdconf.rec sur le serveur RSA ACE (ou si nécessaire, créez-le) et copiez-le dans le dossier \System32 sur le serveur Interface Web, qui se trouve généralement dans C:\Windows\System32. Ce fichier fournit à l'Interface Web toutes les informations nécessaires à la connexion au serveur RSA ACE.

Activation de l'authentification RSA SecurID à l'aide de la console

Vous devez configurer l'Interface Web pour activer l'authentification RSA SecurID de sorte que les utilisateurs puissent avoir accès à leurs ressources et les afficher. Pour ce faire, utilisez la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix.

Prise en charge de domaines multiples RSA SecurID

Si vous possédez des comptes utilisateurs qui partagent le même nom d'utilisateur, mais existent dans différents domaines Windows, vous devez les identifier dans la base de données du serveur RSA ACE à l'aide d'une ouverture de session par défaut sous la forme *DOMAINE\nomd'utilisateur* (plutôt qu'avec un nom d'utilisateur uniquement), et utiliser la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix pour configurer l'Interface Web afin qu'elle envoie le domaine et le nom d'utilisateur au serveur RSA ACE.

Activation de l'intégration de mots de passe Windows RSA SecurID

L'Interface Web prend en charge la fonctionnalité d'intégration de mot de passe Windows de RSA SecurID. Lorsque cette fonctionnalité est activée, les utilisateurs de l'Interface Web peuvent ouvrir une session et accéder à leurs ressources avec leur PASSCODE SecurID. Les utilisateurs doivent uniquement fournir un mot de passe Windows la première fois qu'ils ouvrent une session sur l'Interface Web ou lorsque leur mot de passe doit être changé.

Pour utiliser l'intégration de mot de passe Windows SecurID avec l'Interface Web pour Microsoft Internet Information Services :

- Le client d'authentification local RSA ACE/Agent pour Windows doit être installé sur le serveur Web (les administrateurs doivent ouvrir une session sur l'Interface Web à l'aide des informations d'identification de l'administrateur du serveur local).
- L'Interface Web doit être installée après l'Agent RSA ACE.
- Le service RSA Authentication Agent Offline Local doit être exécuté sur le serveur Web.
- L'Agent Host du serveur Web dans la base de données du serveur RSA ACE 6.0 doit être configuré pour activer la fonctionnalité d'intégration de mot de passe Windows.
- Les paramètres système de la base de données doivent être configurés pour activer la fonctionnalité d'intégration de mot de passe Windows au niveau du système.

Pour réinitialiser la clé de registre du nœud secret sur le serveur Web

Le nœud secret est utilisé pour assurer une communication sécurisée entre l'Interface Web et le serveur RSA ACE.

Le nœud secret peut ne plus être synchronisé entre ces deux serveurs dans les cas suivants :

- le serveur Interface Web est réinstallé ;
- le serveur RSA ACE est réinstallé ;
- l'enregistrement de l'Agent Host pour le serveur Web est supprimé, puis ajouté à nouveau ;
- la clé de registre NodeSecret est supprimée du serveur Web ;
- la case Node Secret Created n'est pas cochée dans la boîte de dialogue Edit Agent Host du serveur RSA ACE.

Si le nœud secret du serveur Interface Web et le serveur RSA ACE ne correspondent pas, SecurID échoue. Vous devez réinitialiser le nœud secret sur le serveur Interface Web et le serveur RSA ACE.

Attention : une utilisation incorrecte de l'Éditeur de Registre peut entraîner de graves problèmes 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.

1. Dans le Registre du système, recherchez :
   - HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT sur les serveurs 32 bits
   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SDTI\ACECLIENT sur les serveurs 64 bits
2. Supprimez la clé NodeSecret.

Remarque : la réinstallation de l'Interface Web ne supprime pas la clé NodeSecret. Si l'entrée Agent Host demeure inchangée sur le serveur RSA ACE, le nœud secret peut être réutilisé.

Activation de l'authentification RADIUS

Mise à jour : 2014-11-24

Cette section décrit comment installer et configurer Aladdin SafeWord et RSA SecurID pour être présentés en tant que serveur RADIUS. L'authentification RADIUS est la seule option d'authentification à deux facteurs disponible pour l'Interface Web pour les serveurs d'application Java.

Activation de RADIUS avec SafeWord

Lors de l'installation du logiciel serveur SafeWord, choisissez d'installer l'Agent IAS RADIUS.

Suivez les instructions à l'écran concernant l'installation du ou des client(s) RADIUS avec le composant logiciel enfichable Windows IAS (Internet Authentication Service) de la console MMC. Un nouveau client RADIUS doit être configuré pour chaque serveur Interface Web qui authentifie les utilisateurs sur le serveur SafeWord.

Chaque client RADIUS créé doit être fourni avec les éléments suivants :

- le nom de domaine complet ou l'adresse IP du serveur Interface Web à laquelle le client RADIUS est associé ;
- un secret, qui est disponible auprès du serveur associé Interface Web.
- le type de client doit être défini sur RADIUS standard ;
- afin de renforcer la sécurité, l'option Request must contain the Message Authenticator attribute doit être sélectionnée.

Activation de RADIUS avec RSA SecurID

RADIUS est activé sur RSA Authentication Manager à l'aide de l'outil SecurID Configuration Management. Pour de plus amples informations sur cet outil, reportez-vous à la documentation de RSA Authentication Manager.

Ajout de l'Interface Web et des serveurs RADIUS en tant qu'agents d'authentification

Si le logiciel RSA Authentication Manager qui authentifie les utilisateurs agit également comme serveur RADIUS, vous devez créer un enregistrement Authentication Agent pour le serveur RADIUS local dans la base de données de RSA Authentication Manager. Lors de la création de l'enregistrement Authentication Agent, indiquez le nom et l'adresse IP du serveur local et configurez ce serveur en tant que Net OS Authentication Agent. Le serveur local doit être assigné en tant que serveur intérimaire.

Par ailleurs, vous devez créer un enregistrement Authentication Agent pour chaque serveur Interface Web dans la base de données de RSA Authentication Manager de façon à ce que ce dernier puisse reconnaître et accepter les demandes d'authentification provenant de l'Interface Web via le serveur RADIUS. Lors de la création d'un enregistrement Authentication Agent, configurez l'Interface Web en tant que serveur de communication et définissez la clé de cryptage sur la valeur du secret partagé avec l'Interface Web.

Utilisation du mode RADIUS Challenge

Par défaut, un serveur RADIUS SecurID est en *mode RADIUS Challenge*. Dans ce mode :

- l'Interface Web affiche un écran de challenge générique comportant un message, une zone de mot de passe HTML, ainsi que les boutons OK et Annuler ;
- les messages de challenge ne sont pas localisés par l'Interface Web. Ils sont dans la même langue que les messages de challenge sur le serveur RADIUS SecurID.

Si les utilisateurs ne donnent pas de réponse (par exemple, s'ils cliquent sur Annuler), ils sont redirigés vers l'écran Ouvrir une session.

Citrix recommande que ce mode soit uniquement utilisé si des composants ou des produits logiciels autres que l'Interface Web utilisent également le serveur RADIUS pour l'authentification.

Utilisation de messages de challenge personnalisés

Vous pouvez configurer des messages de challenge personnalisés pour le serveur RADIUS SecurID. Lorsque vous utilisez des messages personnalisés reconnus par l'Interface Web, le serveur RADIUS peut présenter des pages d'interface identiques à celles affichées par l'Interface Web pour Microsoft Internet Information Services et ces pages sont traduites.

Cette fonctionnalité nécessite des modifications de la configuration du serveur RADIUS et doit être implantée uniquement si le serveur RADIUS est utilisé exclusivement pour authentifier les utilisateurs de l'Interface Web.

Vous pouvez modifier les messages de challenge en lançant l'utilitaire de configuration RADIUS RSA. Pour plus d'informations sur l'utilisation de cet outil, consultez la documentation accompagnant le logiciel SecurID. Pour afficher les mêmes messages à l'intention des utilisateurs qui accèdent à des sites sur IIS et sur des serveurs d'application Java, il est nécessaire de mettre à jour les challenges ci-dessous :

Teneur du message	Paquet	Valeur mise à jour
L'utilisateur veut-il un code secret système?	Challenge	CHANGE_PIN_EITHER
L'utilisateur est-il prêt à recevoir un code secret système ?	Challenge	SYSTEM_PIN_READY
L'utilisateur est-il satisfait du code secret système ?	Challenge	CHANGE_PIN_SYSTEM_[%s]
Nouveau code secret numérique de longueur fixe	Challenge	CHANGE_PIN_USER

Nouveau code secret alphanumérique de longueur fixe	Challenge	CHANGE_PIN_USER
Nouveau code secret numérique de longueur variable	Challenge	CHANGE_PIN_USER
Nouveau code secret alphanumérique de longueur variable	Challenge	CHANGE_PIN_USER
Nouveau code secret accepté	Challenge	RÉUSSITE
Entrer Oui ou Non	Challenge	ÉCHEC
Nouveau code d'authentifieur requis	Challenge	NEXT_TOKENCODE

Création d'un secret partagé pour RADIUS

Le protocole RADIUS nécessite l'utilisation d'un secret partagé, contenant des données connues uniquement du client RADIUS (c'est-à-dire de l'Interface Web) et du serveur RADIUS auprès duquel il s'authentifie. L'Interface Web stocke ce secret dans un fichier texte sur le système de fichiers local. L'emplacement de ce fichier est indiqué par la valeur de configuration RADIUS_SECRET_PATH dans le fichier web.config (pour les sites hébergés sur IIS) ou le fichier web.xml (pour les sites hébergés sur des serveurs d'application Java). L'emplacement indiqué est relatif au dossier \conf pour les sites hébergés sur IIS et relatif au répertoire /WEB_INF pour les sites hébergés sur des serveurs d'application Java.

Pour créer le secret partagé, créez un fichier texte nommé radius_secret.txt contenant une chaîne quelconque. Déplacez ce fichier vers l'emplacement indiqué dans le fichier de configuration approprié ; assurez-vous qu'il est verrouillé et qu'il ne peut être accessible qu'aux utilisateurs ou processus appropriés.

Spécification d'un identificateur de serveur d'accès réseau pour RADIUS

Le protocole RADIUS nécessite que les requêtes d'accès aux serveurs RADIUS comprennent l'adresse IP ou un autre type d'identificateur pour le client RADIUS (c'est-à-dire, l'Interface Web). Pour activer l'authentification RADIUS, vous devez fournir l'adresse IP du serveur Web ou spécifier une valeur pour l'attribut d'identificateur du serveur d'accès au réseau (NAS) RADIUS. Cette valeur peut être constituée d'une quelconque chaîne contenant au moins trois caractères. Bien qu'il ne soit pas nécessaire que cet attribut soit unique pour chaque client RADIUS, la définition d'un identificateur unique pour chaque client permet de faciliter le diagnostic des problèmes de communication RADIUS.

Pour fournir l'adresse IP du client RADIUS, entrez l'adresse IP du serveur Web en tant que valeur pour le paramètre de configuration RADIUS_IP_ADDRESS dans le fichier web.config (pour les sites hébergés sur IIS) ou le fichier web.xml (pour les sites hébergés sur des serveurs d'application Java). Pour définir l'identificateur NAS RADIUS, spécifiez une valeur pour RADIUS_NAS_IDENTIFIER dans web.config ou web.xml.

Activation de l'authentification RADIUS Two-Factor à l'aide de la console

Vous devez activer l'authentification à deux facteurs sur l'Interface Web de sorte que les utilisateurs puissent avoir accès à leur série de ressources et l'afficher. Pour ce faire, utilisez la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix. En plus d'activer l'authentification à deux facteurs, vous pouvez indiquer une ou plusieurs adresses de serveurs RADIUS (et facultativement des ports), l'équilibrage de charge ou le comportement du basculement des serveurs et le délai d'expiration de la réponse.

Important : lorsque vous activez l'authentification RADIUS, vous devez également fournir l'adresse IP du client RADIUS ou spécifier une valeur pour l'attribut d'identificateur du serveur d'accès au réseau RADIUS dans le fichier web.config (IIS) ou le fichier web.xml (serveurs d'application Java) pour le site.

Gestion des clients

Mise à jour : 2014-11-24

Cette section fournit des informations sur le déploiement et l'utilisation des clients Citrix à l'aide de l'Interface Web. Elle explique également comment créer un accès sécurisé.

Clients pour ressources en mode connecté

Les clients Citrix suivants peuvent être utilisés pour accéder à des ressources en mode connecté :

- **Client natif.** Les administrateurs installent le client natif approprié sur les machines des utilisateurs. Les utilisateurs ne disposant pas d'un client natif peuvent également télécharger et déployer Citrix Online Plug-in – Web à l'aide du processus de détection et de déploiement de client. Les fenêtres transparentes sont prises en charge ; les ressources sont présentées dans des fenêtres de bureau qu'il est possible de redimensionner. Si les utilisateurs accèdent aux ressources par le biais d'ordinateurs de poche, vous devez sélectionner le client natif.

- **Client pour Java.** Les utilisateurs exécutent le client pour Java lors de l'accès à la ressource. Ce client est généralement utilisé dans les situations suivantes : les utilisateurs ne disposent pas d'un client natif et sont dans l'incapacité de télécharger et déployer Citrix Online Plug-in – Web ou la configuration de la machine cliente ou du site Web XenApp les empêche de déployer ce client. Le client pour Java prend en charge les fenêtres transparentes ; les ressources sont présentées dans des fenêtres de bureau qu'il est possible de redimensionner.

- **Logiciel de connexion au Bureau à distance incorporé.** Les utilisateurs peuvent utiliser le logiciel Connexion au Bureau à distance installé par défaut avec le système d'exploitation Windows si vous avez activé cette option. Le processus de détection et de déploiement de client ne met pas le logiciel Connexion au Bureau à distance à disposition des utilisateurs qui ne l'ont pas installé. Les fenêtres transparentes ne sont pas prises en charge ; les ressources sont présentées dans des fenêtres de navigateur intégrées.

  Remarque : le client pour Java et le logiciel Connexion au Bureau à distance intégré ne sont pas pris en charge sur les périphériques exécutant Windows CE ou Windows Mobile. Le client pour Java et le logiciel Connexion au Bureau à distance intégré ne prennent pas en charge l'utilisation de sites intégrés ADFS.

Configuration de Citrix Online Plug-in

Citrix Online Plug-in permet aux utilisateurs d'accéder aux applications, contenus et bureaux virtuels directement depuis des bureaux Windows physiques sans avoir recours à un navigateur Web. Vous pouvez configurer à distance la création de liens vers les ressources sur le menu Démarrer, sur le bureau Windows ou dans la zone de notification de Windows. L'interface utilisateur de Citrix Online Plug-in peut également être « verrouillée » pour éviter toute erreur de configuration par l'utilisateur. Vous pouvez utiliser la console de gestion de l'Interface Web Citrix ou le fichier config.xml pour configurer Citrix Online Plug-in.

Utilisation de la console de gestion de l'Interface Web Citrix pour la configuration

Citrix Online Plug-in est par défaut configuré pour utiliser des options de présentation, des méthodes d'authentification et des options de connexion au serveur spécifiques. La console de gestion de l'Interface Web Citrix permet de changer les paramètres par défaut afin d'empêcher les utilisateurs de modifier certaines options.

Utilisation des fichiers de configuration

Vous pouvez également configurer Citrix Online Plug-in en utilisant les fichiers config.xml et InterfaceWeb.conf. Généralement, ces fichiers sont situés dans le répertoire C:\inetpub\wwwroot\Citrix\PNAgent\conf sur le serveur Interface Web.

Gestion des fichiers de configuration des plug-ins

Les options de Citrix Online Plug-in configurées dans la console sont stockées dans un fichier de configuration sur le serveur Interface Web. Ce fichier de configuration détermine la gamme des paramètres qui apparaissent sous la forme d'options dans la boîte de dialogue Options du Citrix Online Plug-in des utilisateurs. Les utilisateurs peuvent effectuer une sélection parmi les options disponibles afin de définir leurs préférences pour les sessions ICA, et notamment le mode d'ouverture de session, la taille de l'écran, la qualité audio et l'emplacement des liens vers les ressources.

Pour les nouveaux sites, un fichier de configuration standard (config.xml) contenant les paramètres par défaut est installé ; il est utilisable tel quel dans la plupart des environnements réseau. Le fichier config.xml est stocké dans le dossier \conf pour le site.

Copie des fichiers d'installation d'un client sur l'Interface Web

Mise à jour : 2014-11-24

Pour installer un client via le Web, les fichiers d'installation du client doivent être disponibles sur le serveur Interface Web.

Le programme d'installation de l'Interface Web vous invite à accéder au support d'installation de XenApp ou XenDesktop. Sur IIS, le programme d'installation copie le contenu du dossier \Citrix Receiver et Plug-ins du support d'installation vers un dossier appelé \Clients dans le répertoire racine (C:\Program Files (x86)\Citrix\Web Interface*Version*\Clients). Sur les serveurs d'application Java, le programme d'installation copie les clients Citrix du support d'installation et les conditionne dans le fichier .war.

Si vous n'avez pas copié les fichiers d’installation des clients sur le serveur Web lors de l'installation de l'Interface Web, assurez-vous de les copier sur le serveur Web avant d'installer des clients par le Web ; par exemple, copiez les fichiers du dossier Citrix Receiver and Plug-ins. Si le support d'installation de XenApp ou XenDesktop n'est pas disponible, vous devez recréer manuellement la structure de répertoire requise et télécharger les clients requis à partir du site Web de Citrix.

Par défaut, l'Interface Web suppose que les noms de fichiers des fichiers d'installation de client sont les mêmes que ceux des fichiers fournis sur le support d'installation de XenApp ou XenDesktop. Si vous téléchargez des clients depuis le site Web Citrix ou que vous prévoyez de déployer des clients antérieurs, vérifiez que les noms des fichiers d'installation de client appropriés sont spécifiés dans les fichiers de configuration pour vos sites XenApp Web.

Pour copier les fichiers clients sur l'Interface Web sur Microsoft Internet Information Services

1. Recherchez le dossier \Clients dans lequel l'Interface Web est installée ; par exemple, C:\Program Files (x86)\Citrix\Web Interface*Version*\Clients.

2. Insérez le support d'installation dans le lecteur optique du serveur Web ou parcourez le réseau pour rechercher une image partagée de ce support d'installation.

3. Accédez au dossier \Citrix Receiver and Plug-ins du support d'installation. Copiez le contenu du dossier sur le support d'installation vers le dossier \Clients sur le serveur Interface Web. Assurez-vous de copier uniquement le *contenu* du dossier et non le dossier \Citrix Receiver and Plug-ins lui-même.

   Si le support d'installation de XenApp ou XenDesktop n'est pas disponible, vous devez recréer manuellement la structure de répertoire ci-dessous et télécharger les clients requis à partir du site Web de Citrix.

   C:\Program Files (x86)\Citrix\Web Interface*Version*\Clients

   - \de
     - \Unix

       Placez les fichiers d'installation des clients pour UNIX (solaris.tar.Z, sol86.tar.Z) avec prise en charge de l'allemand dans ce dossier.
   - \en
     - \Unix

       Placez les fichiers d'installation des clients pour UNIX (solaris.tar.Z, sol86.tar.Z) avec prise en charge de l'anglais dans ce dossier.
   - \es
     - \Unix

       Placez les fichiers d'installation des clients pour UNIX (solaris.tar.Z, sol86.tar.Z) avec prise en charge de l'espagnol dans ce dossier.
   - \fr
     - \Unix

       Placez les fichiers d'installation des clients pour UNIX (solaris.tar.Z, sol86.tar.Z) avec prise en charge du français dans ce dossier.
   - \ja
     - \Unix

       Placez les fichiers d'installation des clients pour UNIX (solaris.tar.Z, sol86.tar.Z) avec prise en charge du japonais dans ce dossier.
   - \Java

     Placez les fichiers du client pour Java dans ce dossier.

- \Linux

  Placez le fichier d'installation de Citrix Receiver pour Linux (linuxx86-*Version*.tar.gz) dans ce dossier.

- \Mac

  - \Web Online Plug-in

    Placez le fichier d'installation de Citrix Online Web Plug-in pour Macintosh {Citrix online plug-in (web).dmg} dans ce dossier.

- \Windows

  - \Offline Plug-in

    Placez le fichier d'installation de Citrix Offline Plug-in (CitrixOfflinePlugin.exe) dans ce dossier.

  - \Online Plug-in

    Placez le fichier d'installation de Citrix Online Plug-in - Web (CitrixOnlinePluginWeb.exe) dans ce dossier.

Par défaut, l'Interface Web suppose que les noms de fichiers des fichiers d'installation de client sont les mêmes que ceux des fichiers fournis sur le support d'installation de XenApp ou XenDesktop. Si vous téléchargez des clients depuis le site Web Citrix ou que vous prévoyez de déployer des clients antérieurs, vérifiez que les noms des fichiers d'installation de client appropriés sont spécifiés pour les paramètres ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32, et ClientStreamingWin32 dans les fichiers de configuration pour vos sites XenApp Web.

Après avoir copié les fichiers d'installation de client dans la structure de répertoire ci-dessus, les sites XenApp Web qui sont configurés pour une installation des clients via le Web proposeront automatiquement les clients aux utilisateurs qui en ont besoin.

Pour copier les fichiers clients sur l'Interface Web sur des serveurs d'application Java

1. Dans le fichier .war développé pour le site, recherchez le répertoire /Clients.

2. Insérez le support d'installation dans le lecteur optique du serveur Web ou parcourez le réseau pour rechercher une image partagée de ce support d'installation.

3. Envoyez les répertoires vers le répertoire \Citrix Receiver and Plug-ins du support d'installation. Copiez le contenu du répertoire sur le support d'installation vers le répertoire /Clients sur le serveur Interface Web. Assurez-vous de copier uniquement le *contenu* du répertoire et non le répertoire \Citrix Receiver and Plug-ins lui-même.

   Si le support d'installation de XenApp ou XenDesktop n'est pas disponible, vous devez recréer manuellement la structure de répertoire ci-dessous et télécharger les clients requis à partir du site Web de Citrix.

   XenAppWebSiteRoot/Clients

   - /de
     - /Unix

       Placez les fichiers d'installation des clients pour UNIX (solaris.tar.Z, sol86.tar.Z) avec prise en charge de l'allemand dans ce répertoire.
   - /en
     - /Unix

       Placez les fichiers d'installation des clients pour UNIX (solaris.tar.Z, sol86.tar.Z) avec prise en charge de l'anglais dans ce répertoire.
   - /es
     - /Unix

       Placez les fichiers d'installation des clients pour UNIX (solaris.tar.Z, sol86.tar.Z) avec prise en charge de l'espagnol dans ce répertoire.
   - /fr
     - /Unix

       Placez les fichiers d'installation des clients pour UNIX (solaris.tar.Z, sol86.tar.Z) avec prise en charge du français dans ce répertoire.
   - /ja
     - /Unix

       Placez les fichiers d'installation des clients pour UNIX (solaris.tar.Z, sol86.tar.Z) avec prise en charge du japonais dans ce répertoire.
   - /Java

     Placez les fichiers du client pour Java dans ce répertoire.

   - /Linux

Placez le fichier d'installation de Citrix Receiver pour Linux (linuxx86-*Version*.tar.gz) dans ce répertoire.

- /Mac
  - /Web Online Plug-in

    Placez le fichier d'installation de Citrix Online Web Plug-in pour Macintosh {Citrix online plug-in (web).dmg} dans ce répertoire.
- /Windows
  - /Offline Plug-in

    Placez le fichier d'installation de Citrix Offline Plug-in (CitrixOfflinePlugin.exe) dans ce répertoire.

  - /Online Plug-in

    Placez le fichier d'installation de Citrix Online Plug-in - Web (CitrixOnlinePluginWeb.exe) dans ce répertoire.

Par défaut, l'Interface Web suppose que les noms de fichiers des fichiers d'installation de client sont les mêmes que ceux des fichiers fournis sur le support d'installation de XenApp ou XenDesktop. Si vous téléchargez des clients depuis le site Web Citrix ou que vous prévoyez de déployer des clients antérieurs, vérifiez que les noms des fichiers d'installation de client appropriés sont spécifiés pour les paramètres ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32, et ClientStreamingWin32 dans les fichiers de configuration pour vos sites XenApp Web.

4. Après avoir copié les fichiers d'installation de client dans la structure de répertoire ci-dessus, redémarrez le serveur Web.

   Si vous avez configuré le site XenApp Web pour une installation des clients par le web, ces derniers seront proposés aux utilisateurs qui en ont besoin.

Configuration du déploiement client et des légendes d'installation

Mise à jour : 2014-11-24

L'Interface Web dispose d'un processus de détection et de déploiement de client dont la tâche consiste à détecter les clients Citrix susceptibles d'être déployés dans l'environnement des utilisateurs puis à les guider au travers de la procédure de déploiement, qui peut inclure le cas échéant, la reconfiguration de leur navigateur Web.

Vous pouvez permettre aux utilisateurs de lancer le processus de détection et de déploiement de client de trois façons :

- Vous pouvez configurer l'exécution automatique du processus de détection et de déploiement de client lorsque les utilisateurs accèdent à un site XenApp Web. Le processus de détection et de déploiement de client démarre automatiquement, identifie le client Citrix approprié et le déploie de façon à ce que les utilisateurs puissent accéder à leurs ressources. Dans certains environnements, le processus de détection et de déploiement de client peut également détecter la présence ou l'absence de client et solliciter l'utilisateur le cas échéant.

- Vous pouvez permettre aux utilisateurs de spécifier le client qu'ils préfèrent utiliser pour accéder aux ressources en mode connecté. Cela ajoute le bouton Exécuter la détection de client à l'écran Paramètres, ce qui permet aux utilisateurs de lancer manuellement le processus de détection et de déploiement de client.

- Vous pouvez mettre des légendes d'installation à la disposition des utilisateurs. Il s'agit de liens qui sont présentés aux utilisateurs dans l'écran Messages. Il leur suffit de cliquer sur ces liens pour démarrer le processus de détection et de déploiement de client.

Lorsqu'un utilisateur accède à un site XenApp Web, le processus Web de détection et de déploiement de client tente de déterminer si le client Citrix préféré est installé sur l'ordinateur de l'utilisateur. Avant que l'utilisateur ouvre une session à un site XenApp Web configuré pour détecter et déployer automatiquement des clients, le processus démarre automatiquement et guide l'utilisateur au travers de la procédure d'identification et de déploiement d'un client Citrix adéquat lui permettant d'accéder à ses ressources. Le cas échéant, l'utilisateur peut également être invité à reconfigurer son navigateur Web.

Les liens qui s'affichent dans l'écran Messages permettent également aux utilisateurs d'accéder au processus de détection et de déploiement de client. Il leur suffit de cliquer sur ces liens pour démarrer le processus de détection et de déploiement de client. Ces liens sont appelés *légendes d'installation*.

Les légendes d'installation peuvent être mises à la disposition des utilisateurs qui ne disposent pas d'un client approprié ; elles peuvent également être utilisées pour leur permettre d'accéder au processus de détection et de déploiement de client afin de mettre leurs clients Citrix à niveau au profit d'une version plus récente ou d'un autre type de client offrant davantage de fonctionnalités.

Vous pouvez utiliser la tâche Déploiement du client dans la console de gestion de l'Interface Web Citrix afin de spécifier dans quelles conditions les utilisateurs peuvent accéder au processus de détection et de déploiement de client.

Pour configurer les légendes d'installation et de déploiement des clients

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Déploiement du client. Pour les sites proposant uniquement des applications en ligne, sélectionnez la case Client natif et cliquez sur Propriétés.

4. Cliquez sur Détection de client.

5. Si vous souhaitez que le processus de détection et de déploiement de client démarre automatiquement lorsque des utilisateurs qui ne disposent pas d'un client Citrix approprié accèdent à un site XenApp Web, sélectionnez la case Exécuter la détection de client à l'ouverture de session.

6. Pour inviter les utilisateurs à mettre leurs clients à niveau lorsque le processus de détection et de déploiement de client détecte de nouvelles versions téléchargeables sur le site Web XenApp, sélectionnez la case Offrir des mises à niveau pour les clients.

7. Indiquez quand les légendes d'installation sont présentées aux utilisateurs en choisissant l'une des options suivantes :

   - Pour informer l'utilisateur qu'aucun client approprié n'a été détecté ou qu'un client plus adéquat est disponible, sélectionnez Chaque fois qu'un client est requis. C'est le réglage par défaut.

   - Pour informer l'utilisateur uniquement lorsqu'aucun client approprié n'a été détecté, sélectionnez Uniquement lorsque l'accès aux ressources est impossible.

   - Si vous ne souhaitez pas afficher de légendes d'installation, sélectionnez Jamais.

Configuration de la signature de fichier ICA

Mise à jour : 2014-12-02

L'Interface Web peut signer numériquement les fichiers ICA générés avec un certificat choisi, ce qui permet aux clients et plug-ins Citrix compatibles de vérifier que le fichier provient de votre organisation.

Pour utiliser la signature de fichier ICA, les composants suivants sont requis :

- Interface Web version 5.4 ou supérieure
- Merchandising Server version 1.2 ou supérieure (pour les déploiements de stratégie de sécurité de clients non gérés)
- Objets de stratégie de groupe pour les déploiements de stratégie de sécurité de clients gérés
- Format de fichier de modèle d'administration pour Windows Server 2003 ou supérieur

Citrix recommande de procéder comme suit, par ordre de priorité :

- Achetez un certificat de signature de code ou certificat de signature SSL émanant d'une autorité de certification publique (telle que Verisign).
- Si votre entreprise dispose déjà d'une autorité de certification privée, créez un certificat de signature de code ou certificat de signature SSL à l'aide de l'autorité de certification privée.
- Utilisez un certificat SSL existant, tel que le certificat de l'Interface Web ou du serveur Dazzle.
- Créez un nouveau certificat d’autorité de certification racine et distribuez-le sur les clients à l'aide d'objets de stratégie de groupe.

Le certificat doit répondre aux conditions suivantes :

- Il doit inclure la clé privée.
- Il ne peut être expiré.
- L'une des affirmations suivantes doit être valide :
  - Le certificat ne dispose pas d'un champ d'utilisation de la clé ou d'utilisation améliorée de la clé.
  - Le champ d'utilisation de la clé permet à la clé d'être utilisée pour les signatures numériques.

- Le champ d'utilisation améliorée de la clé est défini sur Signature du code ou Authentification du serveur.

L'Interface Web signe les fichiers ICA à l'aide de l'algorithme de hachage SHA-1 ou SHA-256. L'algorithme de hachage SHA-256 est plus récent et plus sécurisé, toutefois, il est uniquement pris en charge sur les serveurs exécutant Windows 2008 ou version ultérieure et les clients exécutant Windows Vista ou version ultérieure. L'algorithme de hachage SHA-1 peut être utilisé sur tous les systèmes d'exploitation serveur et client pris en charge.

La signature de fichier ICA ne peut pas être utilisée avec le Client pour Java, le client RDP, le client Citrix Streaming client et avec les documents publiés téléchargés à partir de partages réseau.

Pour activer la signature de fichier ICA, le site doit être configuré pour utiliser le client natif et pour afficher les applications en mode connecté, et EnableLegacyIcaClientSupport doit être défini sur Off dans le fichier Webinterface.conf.

Pour de plus amples informations sur l'activation de la signature de fichier ICA pour Citrix Online Plug-in, consultez la documentation relative à Citrix Merchandising Server.

Pour activer la signature de fichier ICA dans la console de gestion de l'Interface Web Citrix

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Déploiement du client.

4. Cliquez sur Signature du fichier ICA.

5. Sélectionnez Activer la signature de fichier ICA et sélectionnez un certificat dans le menu déroulant. Si le certificat requis ne figure pas dans la liste, cliquez sur Importer pour importer un certificat dans le magasin de certificats personnels.

6. Si vous exécutez Windows 2008 ou une version ultérieure, vous pouvez sélectionner le type d'algorithme de hachage à utiliser. Autrement, SHA-1 sera utilisé. Après avoir configuré la signature de fichier ICA sur Windows 2003, vous devez redémarrer votre ordinateur.

Configuration du contrôle de la session de streaming

Vous pouvez utiliser la tâche Déploiement du client dans la console de gestion de l'Interface Web Citrix pour configurer l'Interface Web, afin de fournir les informations concernant les sessions utilisateur à l'administrateur Citrix. L'Interface Web fournit ces informations au moyen d'une adresse URL de session qui permet de communiquer avec Citrix Offline Plug-in. Dans la plupart des cas, cette adresse URL est détectée automatiquement. Cependant, il se peut qu'elle doive être définie manuellement (par exemple, si un proxy côté client est utilisé).

Vous pouvez utiliser la console Delivery Services Console pour visualiser les informations de session. Vous pouvez visualiser les informations de toutes les sessions utilisateur dans plusieurs batteries, des applications spécifiques, des sessions se connectant à un serveur spécifique ou les sessions et les applications d'un utilisateur spécifique.

Pour configurer le contrôle de la session de streaming

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Déploiement du client.

4. Cliquez sur Citrix Offline Plug-in.

5. Sélectionnez le mode de communication de l'Interface Web avec Citrix Offline Plug-in. Choisissez parmi les modes suivants :

   - Pour détecter automatiquement l'adresse URL de session utilisée pour communiquer avec le plug-in, sélectionnez Détecter automatiquement l'adresse URL de session.

   - Pour définir une adresse URL de session, sélectionnez Spécifier l'adresse URL de session et entrez les détails de l'adresse URL.

Déploiement du logiciel de connexion au Bureau à distance

La fonction de connexion au Bureau à distance est disponible sur les systèmes Windows 32 bits avec Internet Explorer. Les utilisateurs qui ont installé la version 6.0 (fournie avec Windows XP, Service Pack 3) ou supérieure du logiciel Connexion Bureau à distance peuvent l'utiliser pour accéder à leurs ressources. Si les utilisateurs ne peuvent pas utiliser d'autres clients, le processus de détection et de déploiement de client vérifie que le logiciel Connexion Bureau à distance est disponible et aide les utilisateurs à activer le contrôle ActiveX des services Terminal Server, le cas échéant. Seuls les sites offrant uniquement des applications en mode connecté ont la possibilité d'utiliser le logiciel Connexion Bureau à distance.

Remarque : si Internet Explorer ne place pas le site XenApp Web dans la zone Intranet local ou Sites de confiance, il affiche un message d'erreur. Le processus de détection et de déploiement de client de l'Interface Web fournit aux utilisateurs les instructions nécessaires à l'ajout du site à la zone de sécurité Windows appropriée.

Déploiement du client pour Java

Si vous déployez des clients Citrix sur un réseau à bande passante réduite ou si vous ne connaissez pas la plate-forme de vos utilisateurs, privilégiez l'utilisation du client pour Java. Le client pour Java est un applet multi-plateforme qui peut être déployé par le serveur Interface Web sur n'importe quel navigateur Web compatible Java.

De par le large éventail d'environnements utilisateur, de machines, de systèmes d'exploitation et de navigateurs Web pris en charge par le client pour java, il représente la solution idéale dans les situations dans lesquelles un client natif ne peut pas être utilisé. Vous pouvez configurer le processus de détection et de déploiement de client afin de proposer le client pour Java aux utilisateurs qui ne disposent pas d'un client natif ou qui sont dans l'incapacité de télécharger et déployer un client natif à partir du site Web de XenApp.

Vous devez vous assurer que le client pour Java est disponible dans le répertoire \Clients du site Web de XenApp pour pouvoir le déployer auprès de vos utilisateurs.

Pour configurer le retour au client pour Java

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Déploiement du client. Pour les sites proposant uniquement des applications en ligne, sélectionnez la case Client natif et cliquez sur Propriétés.

   Remarque : il n'est pas nécessaire de mettre le client pour java à la disposition des utilisateurs pour fournir la fonction de retour.

4. Cliquez sur Comportement de retour.

5. Spécifiez dans quels cas de figure le client pour Java est proposé aux utilisateurs ne disposant pas d'un client natif en choisissant l'une des options suivantes :

   - Si vous souhaitez que les utilisateurs ne disposant pas d'un client natif téléchargent et déploient un client Citrix approprié, sélectionnez Déployer un client natif. C'est le réglage par défaut.

   - Si vous souhaitez que le client pour Java soit proposé aux utilisateurs ne disposant pas d'un client natif et qu'ils ne soient invités à télécharger et déployer un client natif à la seule condition qu'ils ne puissent pas utiliser le client pour Java, sélectionnez Déployer un client natif et autoriser l'utilisateur à choisir entre ce dernier et le client pour Java.

   - Si vous souhaitez que les utilisateurs ne disposant pas d'un client natif soient invités à télécharger et déployer un client approprié en plus de se voir proposer le client pour Java, sélectionnez Automatiquement retourner au client pour Java.

Personnalisation du déploiement du client pour Java

Mise à jour : 2014-11-25

Vous pouvez configurer les composants compris dans le déploiement du Client pour Java.

La taille du client pour Java est déterminée par les packs que vous sélectionnez. Moins le nombre de packs sélectionné est important, plus la taille est réduite (jusqu'à 540 Ko). Pour limiter la taille du client pour Java pour les utilisateurs disposant de connexions à faible bande passante, vous pouvez déployer uniquement un ensemble minimal de composants. Vous pouvez également autoriser les utilisateurs à sélectionner les composants dont ils ont besoin. Pour plus d'informations sur le client pour Java et ses composants, veuillez consulter la documentation relative au Client pour Java.

Remarque : certains composants que vous rendez disponibles dans le Client pour Java peuvent exiger une configuration supplémentaire sur les machines des utilisateurs ou le serveur.

Le tableau suivant recense les options disponibles :

Pack	Description
Audio	Permet aux ressources exécutées sur le serveur de lire les sons par l'intermédiaire de dispositifs sonores installés sur les ordinateurs des utilisateurs. Pour contrôler la quantité de bande passante utilisée par le mappage audio du client sur le serveur, configurez les stratégies utilisateur Citrix.
Presse-papiers	Permet aux utilisateurs de copier du texte et des graphiques entre les ressources en mode connecté et les applications exécutées localement sur leurs machines.
Écho local du texte	Accélère l'affichage du texte saisi sur les machines des utilisateurs.
SSL/TLS	Assure la sécurité des communications à l'aide des protocoles SSL (Secure Socket Layer) et TLS (Transport Layer Security). SSL/TLS offre des fonctions d'authentification du serveur, de cryptage du flux de données et de vérification de l'intégrité des messages.
Chiffrement	Assure un cryptage élevé qui améliore la confidentialité des connexions aux clients Citrix.

Données du mappage des lecteurs clients	Permet aux utilisateurs d'accéder à leurs lecteurs locaux à partir d'une session. Lorsque les utilisateurs se connectent au serveur, leurs lecteurs clients (lecteurs de disquettes, réseau et optiques, par exemple) sont automatiquement montés. Les utilisateurs peuvent accéder à leurs fichiers stockés localement, s'en servir au cours de leurs sessions, puis les enregistrer de nouveau sur un lecteur local ou sur un lecteur du serveur. Pour activer ce paramètre, les utilisateurs doivent aussi configurer le mappage de lecteurs clients dans la boîte de dialogue Paramètres du client pour Java. Pour plus d'informations, reportez-vous à la documentation relative au Client pour Java.
Mappage d'imprimantes	Permet aux utilisateurs d'imprimer sur leurs imprimantes locales ou réseau à partir d'une session.
Interface utilisateur de configuration	Active la boîte de dialogue Paramètres du client pour Java. Cette boîte de dialogue permet aux utilisateurs de configurer le Client pour Java.

Utilisation de certificats racine privés avec le client pour Java, version 9.x

Si vous avez configuré Secure Gateway ou le service Relais SSL avec un certificat de serveur provenant d'une autorité de certification privée (si vous délivrez par exemple vos propres certificats à l'aide des Services de certificats Microsoft), vous devez importer le certificat racine dans le stock de clés Java de chaque machine utilisateur. Pour plus d'informations, reportez-vous à la documentation relative au Client pour Java.

Gestion de l'accès sécurisé

Tous les nouveaux sites Interface Web sont configurés par défaut pour un accès direct, ce qui signifie que l'adresse actuelle du serveur Citrix est communiquée à tous les clients Citrix. Toutefois, si vous utilisez Access Gateway, Secure Gateway ou un pare-feu dans votre déploiement, vous pouvez utiliser la tâche Accès sécurisé dans la console de gestion de l'Interface Web Citrix pour configurer l'Interface Web afin qu'elle comprenne les paramètres appropriés. Vous pouvez également configurer des méthodes d'accès différentes pour différents groupes d'utilisateurs. À titre d'exemple, les utilisateurs internes qui ouvrent une session via un réseau local d'entreprise peuvent être configurés pour un accès direct, tandis que les utilisateurs externes qui ouvrent une session via Internet accèdent à l'Interface Web par l'intermédiaire d'Access Gateway.

Cette section explique comment utiliser la tâche Accès sécurisé pour définir des paramètres d'accès, modifier les traductions d'adresse et configurer les réglages de passerelle.

Pour configurer des routes d'accès directes

Si vous souhaitez communiquer l'adresse actuelle du serveur Citrix à un groupe de clients Citrix donné, vous pouvez spécifier les adresses des machines utilisateur et les masques à l'aide de la tâche Accès sécurisé dans la console de gestion de l'Interface Web Citrix.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Accès sécurisé.

4. Sur la page Spécifier les méthodes d'accès, cliquez sur Ajouter pour ajouter une nouvelle route d'accès ou sélectionnez une entrée dans la liste et cliquez sur Modifier pour modifier une route existante.

5. Dans la liste Méthode d'accès, sélectionnez Directe.

6. Entrez l'adresse réseau et le masque de sous-réseau identifiant le réseau client.

7. Utilisez les boutons Monter et Descendre pour classer les routes d'accès par ordre de priorité dans le tableau Adresses des machines utilisateur.

Pour configurer des paramètres d'adresse secondaire

Si vous souhaitez communiquer l'adresse secondaire du serveur Citrix à un groupe de clients Citrix donné, vous pouvez spécifier les adresses des machines utilisateur et les masques à l'aide de la tâche Accès sécurisé dans la console console de gestion de l'Interface Web Citrix. Le serveur doit être configuré avec une adresse secondaire et le pare-feu doit être configuré pour une traduction d'adresse réseau.

Remarque : il est impossible d'accéder à des bureaux virtuels XenDesktop si des adresses secondaires sont utilisées.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.
2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.
3. Dans le panneau Actions, cliquez sur Accès sécurisé.
4. Sur la page Spécifier les méthodes d'accès, cliquez sur Ajouter pour ajouter une nouvelle route d'accès ou sélectionnez une entrée dans la liste et cliquez sur Modifier pour modifier une route existante.
5. Dans la liste Méthode d'accès, sélectionnez Secondaire.
6. Entrez l'adresse réseau et le masque de sous-réseau identifiant le réseau client.
7. Utilisez les boutons Monter et Descendre pour classer les routes d'accès par ordre de priorité dans le tableau Adresses des machines utilisateur.

Pour configurer la traduction d'adresse du pare-feu interne

Si vous utilisez un pare-feu dans votre déploiement, vous pouvez vous servir de l'Interface Web pour définir les mappages depuis les adresses internes vers les adresses externes et les ports. Par exemple, si votre serveur Citrix n'est pas configuré avec une adresse secondaire, vous pouvez configurer l'Interface Web pour qu'elle fournisse une adresse secondaire au client Citrix. Pour ce faire, utilisez la tâche Accès sécurisé dans la console de gestion de l'Interface Web Citrix.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Accès sécurisé.

4. Sur la page Spécifier les méthodes d'accès, cliquez sur Ajouter pour ajouter une nouvelle route d'accès ou sélectionnez une entrée dans la liste et cliquez sur Modifier pour modifier une route existante.

5. Dans la liste Méthode d'accès, sélectionnez Traduite.

6. Entrez l'adresse réseau et le masque de sous-réseau identifiant le réseau client. Utilisez les boutons Monter et Descendre pour classer les routes d'accès par ordre de priorité dans le tableau Adresses des machines utilisateur et cliquez sur Suivant.

7. Sur la page Spécifier les traductions d'adresse, cliquez sur Ajouter pour ajouter une nouvelle traduction d'adresse ou sélectionnez une entrée dans la liste et cliquez sur Modifier pour modifier une traduction existante.

8. Sous Type d'accès, sélectionnez l'une des options suivantes :

   - Si vous souhaitez que le client Citrix utilise l'adresse traduite pour se connecter au serveur Citrix, sélectionnez Traduction de route de machine utilisateur.

   - Si vous avez déjà configuré une route de passerelle traduite dans le tableau Adresses des machines utilisateur et que vous souhaitez que le client et le serveur passerelle utilisent l'adresse traduite pour se connecter au serveur Citrix, sélectionnez Traduction de route de machine utilisateur et de passerelle.

9. Entrez les ports et adresses internes et externes (traduits) pour le serveur Citrix. Les clients qui se connectent au serveur utilisent le numéro de port et l'adresse externes. Veillez à ce que les mappages que vous créez correspondent au type d'adressage utilisé par le serveur Citrix.

Pour configurer les paramètres de passerelle

Mise à jour : 2014-11-25

Si vous utilisez Access Gateway ou Secure Gateway dans votre déploiement, vous devez configurer l'Interface Web pour la prise en charge de passerelle. Pour ce faire, utilisez la tâche Accès sécurisé dans la console de gestion de l'Interface Web Citrix.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Accès sécurisé.

4. Sur la page Spécifier les méthodes d'accès, cliquez sur Ajouter pour ajouter une nouvelle route d'accès ou sélectionnez une entrée dans la liste et cliquez sur Modifier pour modifier une route existante.

5. Sous Méthode d'accès, sélectionnez l'une des options suivantes :

   - Si vous souhaitez communiquer l'adresse actuelle du serveur Citrix à la passerelle, sélectionnez Passerelle directe.

   - Si vous souhaitez communiquer l'adresse secondaire du serveur XenApp à la passerelle, sélectionnez Passerelle secondaire. Le serveur XenApp doit être configuré avec une adresse secondaire et le pare-feu doit être configuré pour une traduction d'adresse réseau.

     Remarque : il est impossible d'accéder à des bureaux virtuels XenDesktop si des adresses secondaires sont utilisées.

   - Si vous souhaitez que l'adresse communiquée à la passerelle soit déterminée par les mappages de traduction d'adresse définis dans l'Interface Web, sélectionnez Passerelle traduite.
6. Entrez l'adresse réseau et le masque de sous-réseau identifiant le réseau client. Utilisez les boutons Monter et Descendre pour classer les routes d'accès par ordre de priorité dans le tableau Adresses des machines utilisateur et cliquez sur Suivant.

7. Si vous n'utilisez pas de traduction d'adresse de passerelle, passez à l'étape 10. Si vous utilisez une traduction d'adresse de passerelle, cliquez sur Ajouter dans la page Spécifier les traductions d'adresse pour ajouter une nouvelle traduction d'adresse ou sélectionnez une entrée dans la liste et sélectionnez Modifier pour modifier une traduction d'adresse existante.

8. Sous Type d'accès, sélectionnez l'une des options suivantes :

- Si vous souhaitez que la passerelle utilise l'adresse traduite pour se connecter au serveur Citrix, sélectionnez Traduction de route de passerelle.

- Si vous avez déjà configuré une route de client traduite dans le tableau Adresses des machines utilisateur et que vous souhaitez que le client Citrix et la passerelle utilisent l'adresse traduite pour se connecter au serveur Citrix, sélectionnez Traduction de route de machine utilisateur et de passerelle.

9. Entrez les ports et adresses internes et externes (traduits) pour le serveur Citrix et cliquez sur OK. Lorsque la passerelle se connecte au serveur Citrix, elle utilise l'adresse et le numéro de port externes. Veillez à ce que les mappages que vous créez correspondent au type d'adressage utilisé par la batterie de serveurs. Cliquez sur Next.

10. Sur la page Spécifier les paramètres de passerelle, spécifiez le nom de domaine complet (FQDN) ainsi que le numéro de port de la passerelle que les clients doivent utiliser. Le FDQN doit correspondre au nom complet du certificat installé sur la passerelle.

11. Si vous souhaitez que le serveur Citrix laisse les sessions déconnectées ouvertes lorsque le client tente de se reconnecter automatiquement, sélectionnez la case Activer la fiabilité de session.

12. Si vous avez activé la fiabilité de session et que vous voulez utiliser les tickets de deux Secure Ticket Authorities (STA) simultanément, sélectionnez la case Demander des tickets de deux STA, si possible. Lorsque cette option est activée, l'Interface Web obtient des tickets de deux STA différentes de façon à ce que les sessions utilisateur ne soient pas interrompues si l'une des STA devenait indisponible au cours de la session. Si pour une raison quelconque, l'Interface Web ne parvient pas à contacter deux STA, elle utilise une seule STA. Cliquez sur Next.

    Remarque : vous devez déployer Access Gateway pour pouvoir utiliser cette fonctionnalité. Secure Gateway ne prend pas en charge plusieurs STA redondantes.

13. Sur la page Spécifier les paramètres Secure Ticket Authority, cliquez sur Ajouter pour spécifier l'adresse URL d'une STA que l'Interface Web peut utiliser ou sélectionnez une entrée dans la liste et cliquez sur Modifier pour modifier les détails des STA existantes. Les STA sont intégrées au service Citrix XML, par exemple, dans http[s]://*NomServeur.Domaine.com*/scripts/ctxsta.dll. Il est possible de spécifier plusieurs Secure Ticket Authority pour la tolérance aux pannes ; Citrix vous conseille toutefois de ne pas utiliser d'équilibreur de charge externe dans ce but. Utilisez les boutons Monter et Descendre pour classer les Secure Ticket Authority par ordre de priorité.

14. Choisissez si vous souhaitez ou non activer l'équilibrage de charge entre les Secure Ticket Authority à l'aide de l'option Utiliser pour l'équilibrage de charge. L'activation de l'équilibrage de charge vous permet de distribuer équitablement les connexions entre les serveurs afin qu'aucun serveur ne soit surchargé.

15. Spécifiez la durée pendant laquelle les STA qui ne sont pas contactables doivent être ignorées dans les cases Ignorer tout serveur en échec pour. L'Interface Web fournit une tolérance aux pannes sur les serveurs présents dans la liste Adresses URL Secure Ticket Authority de manière à ce qu'en cas d'erreur de communication, le serveur défectueux soit ignoré pour la période spécifiée.

Pour configurer les paramètres d'accès par défaut

L'ordre dans lequel les entrées s'affichent dans le tableau Adresses des machines utilisateur correspond à l'ordre dans lequel les règles sont appliquées. Si l'adresse de la machine utilisateur ne correspond à aucune règle définie explicitement pour l'accès, la règle par défaut est appliquée. Lorsque vous créez un site, la route par défaut est automatiquement configurée pour l'accès direct. Vous pouvez spécifier une méthode d'accès par défaut appropriée à votre déploiement grâce à la tâche Accès sécurisé dans la console de gestion de l'Interface Web Citrix.

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Accès sécurisé.

4. Sur la page Spécifier les méthodes d'accès, sélectionnez Valeur par défaut dans la liste et cliquez sur Modifier.

5. Sous Méthode d'accès, sélectionnez l'une des options suivantes :

   - Si vous souhaitez communiquer l'adresse actuelle du serveur Citrix au client Citrix, sélectionnez Directe.

   - Si vous souhaitez communiquer l'adresse secondaire du serveur XenApp au client, sélectionnez Secondaire. Le serveur XenApp doit être configuré avec une adresse secondaire et le pare-feu doit être configuré pour une traduction d'adresse réseau.

     Remarque : il est impossible d'accéder à des bureaux virtuels XenDesktop si des adresses secondaires sont utilisées.

   - Si vous souhaitez que l'adresse communiquée au client soit déterminée par les mappages de traduction d'adresse de l'Interface Web, sélectionnez Traduite.

   - Si vous souhaitez communiquer l'adresse actuelle du serveur Citrix à la passerelle, sélectionnez Passerelle directe.

   - Si vous souhaitez communiquer l'adresse secondaire du serveur XenApp à la passerelle, sélectionnez Passerelle secondaire. Le serveur XenApp doit être configuré avec une adresse secondaire et le pare-feu doit être configuré pour une traduction d'adresse réseau.

     Remarque : il est impossible d'accéder à des bureaux virtuels XenDesktop si des adresses secondaires sont utilisées.

- Si vous souhaitez que l'adresse communiquée à la passerelle soit déterminée par les mappages de traduction d'adresse définis dans l'Interface Web, sélectionnez Passerelle traduite.

6. Entrez l'adresse réseau et le masque de sous-réseau identifiant le réseau client. Utilisez les boutons Monter et Descendre pour classer les routes d'accès par ordre de priorité dans le tableau Adresses des machines utilisateur.

7. Si vous utilisez une traduction d'adresse ou une passerelle dans votre déploiement, cliquez sur Suivant et spécifiez les paramètres supplémentaires appropriés pour votre configuration par défaut. Pour plus d'informations, veuillez consulter les sections Pour configurer la traduction d'adresse du pare-feu interne et Pour configurer les paramètres de passerelle.

Modification des paramètres du proxy côté client

Si vous utilisez un serveur proxy du côté client de l'installation de l'Interface Web, vous pouvez choisir d'obliger ou non les clients Citrix à communiquer avec le serveur exécutant XenApp ou XenDesktop via le serveur proxy. Pour ce faire, utilisez la tâche Proxy côté client dans la console de gestion de l'Interface Web Citrix.

Un serveur proxy placé du côté client d'une installation Interface Web offre les avantages suivants en matière de sécurité :

- Masquage des informations, grâce auquel les noms système situés à l'intérieur du pare-feu ne sont pas divulgués en dehors du pare-feu par l'intermédiaire du DNS (Domain Name System)
- Multiplexage de différentes connexions TCP via une seule connexion

L'utilisation de la console de gestion de l'Interface Web Citrix vous permet de définir des règles proxy par défaut pour les clients Citrix. Cependant, vous pouvez aussi configurer des exceptions à ce comportement pour des machines utilisateur individuelles. Pour configurer des exceptions, associez l'adresse IP externe du serveur proxy à un paramètre proxy de l'Interface Web.

Vous pouvez aussi spécifier que le comportement du proxy doit être contrôlé par le client. Pour utiliser la fonction Secure Proxy dans XenApp et XenDesktop, par exemple, vous devez configurer l'Interface Web de façon à utiliser les paramètres proxy spécifiés sur le client et configurer le client pour utiliser un proxy sécurisé. Pour plus d'informations sur l'utilisation des clients Citrix pour contrôler le comportement du proxy, consultez la documentation accompagnant les clients.

Pour configurer les paramètres par défaut du proxy

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Proxy côté client.

4. Cliquez sur Ajouter pour créer un nouveau mappage ou sélectionnez une entrée dans la liste et cliquez sur Modifier pour modifier un mappage existant.

5. Entrez l'adresse externe du proxy et le masque de sous-réseau de la machine utilisateur dans les cases Adresse IP et Masque de sous-réseau.

6. Dans la liste Proxy, choisissez l'une des options suivantes :

   - Pour que le client Citrix détecte automatiquement le proxy Web en fonction de la configuration du navigateur de l'utilisateur, sélectionnez Réglage du navigateur de l'utilisateur.

   - Pour que le client détecte automatiquement le proxy Web à l'aide du protocole de découverte automatique du proxy Web (WPAD), sélectionnez Détection automatique du proxy Web.

   - Pour utiliser les paramètres clients configurés par l'utilisateur, sélectionnez Défini par le client.

   - Pour utiliser un serveur proxy SOCKS, sélectionnez SOCKS. Si vous choisissez cette option, vous devez entrer l'adresse et le numéro de port du serveur proxy. L'adresse proxy peut être une adresse IP ou un nom DNS.

   - Pour utiliser un serveur proxy sécurisé, sélectionnez Sécurisé (HTTPS). Si vous choisissez cette option, vous devez entrer l'adresse et le numéro de port du serveur proxy. L'adresse proxy peut être une adresse IP ou un nom DNS.

   - Si vous ne souhaitez pas utiliser de proxy, sélectionnez Aucun.
7. Si vous avez entré plusieurs mappages, utilisez les boutons Monter et Descendre pour classer les mappages par ordre de priorité dans le tableau.

Personnalisation de l'affichage pour les utilisateurs

Vous pouvez personnaliser l'affichage de l'interface utilisateur si vous souhaitez, par exemple, que le site reflète l'identité de l'entreprise.

Utilisez la tâche Apparence du site Web dans la console de gestion de l'Interface Web Citrix pour personnaliser :

- **Configuration.** Spécifiez les contrôles auxquels les utilisateurs ont accès ainsi que le format du site Web. Vous pouvez :
    - Sélectionnez la configuration d'écran du site XenApp Web. Vous avez le choix entre automatique, graphiques avancés ou graphiques simplifiés. L'interface utilisateur simplifiée est une version compacte conçue pour les utilisateurs qui utilisent des périphériques mobiles ou des connexions à des réseaux lents pour accéder à leurs ressources. L'option Automatique permet au système de choisir la configuration de site qui convient le mieux à la taille d'écran de chaque utilisateur.
    - Configurez les fonctionnalités et contrôles disponibles sur les écrans Applications des utilisateurs (y compris la fonction de recherche et les conseils) et spécifiez si les utilisateurs sont autorisés à personnaliser leurs propres écrans.
    - Définissez les styles d'affichage par défaut des ressources des utilisateurs dans les configurations d'écran graphiques avancés et graphiques simplifiés. Vous pouvez également spécifier les styles d'affichage que les utilisateurs sont autorisés à sélectionner.
    - Spécifiez comment les ressources sont groupées dans les écrans Applications des utilisateurs. Vous pouvez configurer des onglets séparés pour les applications, le contenu et les bureaux ou regrouper toutes les ressources sous un seul et même onglet.
- **Affichage.** Personnalisez l'interface utilisateur en affichant des images et des couleurs différentes sur le site. Vous pouvez :
    - Spécifiez le style des écrans d'ouverture de session des utilisateurs. Vous avez le choix entre une configuration simplifiée où seuls les champs d'ouverture de session appropriés s'affichent et une configuration comprenant la barre de navigation, ce qui permet aux utilisateurs d'accéder aux écrans Messages et Préférences.
    - Utilisez des images personnalisées pour les configurations graphiques avancés et graphiques simplifiés ; vous pouvez même ajouter des liens hypertexte aux images. Vous pouvez également modifier l'image d'arrière-plan qui s'affiche dans la zone d'en-tête du site ou simplement utiliser une autre couleur.
- **Contenu.** Définissez des messages personnalisés et spécifiez des versions traduites de ce texte pour les langues que vos utilisateurs utiliseront pour accéder au site. Vous pouvez personnaliser le texte et les messages qui apparaissent sur les écrans Ouverture de session et Applications ainsi que sur le bas de page de tous les écrans. En outre, vous pouvez configurer un message d'exclusion de responsabilité que les utilisateurs doivent accepter avant d'ouvrir une session.

Gestion des raccourcis et des options d'actualisation des ressources

Mise à jour : 2014-11-24

Vous pouvez utiliser la tâche Raccourcis dans la console de gestion de l'Interface Web Citrix pour indiquer la façon dont Citrix Online Plug-in affiche les raccourcis vers des ressources.

Vous pouvez créer les types de raccourcis ci-dessous.

- **Menu Démarrer.** Vous pouvez utiliser les paramètres figurant dans la tâche Raccourcis, les paramètres définis lors de la publication de ressources dans XenApp et XenDesktop ou les deux paramètres. Vous pouvez également indiquer si les raccourcis sont affichés dans le menu Démarrer et de quelle façon, et autoriser les utilisateurs à définir ce paramètre. Par ailleurs, vous pouvez créer des raccourcis dans le menu Tous les programmes, créer un sous-menu supplémentaire et/ou autoriser les utilisateurs à spécifier un nom de sous-menu.

- **Bureau.** Vous pouvez utiliser les paramètres figurant dans la tâche Raccourcis, les paramètres définis lors de la publication de ressources dans XenApp et XenDesktop ou les deux paramètres. Vous pouvez également indiquer si des raccourcis peuvent être affichés sur le bureau et de quelle façon, et autoriser les utilisateurs à définir ce paramètre. Par ailleurs, vous pouvez utiliser un nom de dossier personnalisé et/ou autoriser les utilisateurs à sélectionner un nom.

- **Zone de notification.** Vous pouvez afficher des ressources dans la zone de notification et/ou autoriser les utilisateurs à choisir le mode d'affichage de ces ressources.

La tâche Raccourcis vous permet également de supprimer des raccourcis. Vous pouvez indiquer le moment auquel les raccourcis sont supprimés (à la fermeture de Citrix Online Plug-in ou lorsque les utilisateurs ferment une session XenApp) et, pour les utilisateurs exécutant Windows CE ou Linux, si les raccourcis créés par l'utilisateur sont également supprimés en sus des raccourcis de Citrix Online Plug-in. Si vous sélectionnez les raccourcis de Citrix Online Plug-in et ceux créés par les utilisateurs, vous pouvez également limiter la profondeur de recherche dans les dossiers afin d'améliorer les performances.

Spécification des options d'actualisation des ressources

Utilisez la tâche Actualisation des ressources dans la console de gestion de l'Interface Web Citrix pour indiquer le moment auquel les listes des ressources des utilisateurs sont actualisées et si ces derniers peuvent personnaliser ces paramètres. Vous pouvez ainsi décider que l'actualisation doit avoir lieu au démarrage de Citrix Online Plug-in ou lorsque les utilisateurs accèdent aux ressources, et indiquer la fréquence d'actualisation de la liste.

Gestion des préférences de session

Utilisez la tâche Paramètres de session dans la console de gestion de l'Interface Web Citrix pour spécifier les paramètres que les utilisateurs peuvent modifier. Vous pouvez également utiliser cette tâche pour spécifier la durée après laquelle les sessions Interface Web des utilisateurs inactifs sont fermées et si l'Interface Web doit effacer le nom de la machine utilisateur dans le cas des clients pour ressources en mode connecté.

Pour les sites XenApp Web, vous pouvez configurer les paramètres suivants pour les sessions utilisateur :

- **Personnalisation des utilisateurs.** Activez ou désactivez le mode kiosque et spécifiez si le bouton Paramètres est affiché sur l'écran Applications des utilisateurs.
- **Sessions Web.** Spécifiez la durée pendant laquelle la session d'un utilisateur peut rester inactive avant d'être fermée.
- **Adresses URL persistantes.** Spécifiez si les utilisateurs peuvent utiliser des signets de navigateur pour accéder au site.
- **Performances de connexion.** Spécifiez les paramètres par défaut prédéfinis ou indiquez si les utilisateurs sont autorisés à personnaliser le contrôle de la bande passante, le nombre de couleurs, la qualité audio et les paramètres de mappage d'imprimantes.
- **Affichage.** Spécifiez si les utilisateurs sont autorisés à contrôler la taille de leur fenêtre dans les sessions en mode connecté et si l'Interface Web peut utiliser le lissage de polices ClearType. Il faut pour cela que les paramètres correspondants soient configurés sur les systèmes d'exploitation des utilisateurs, sur les clients Citrix et la batterie de serveurs.
- **Ressources locales.** Configurez les paramètres pour les combinaisons de touches Windows, la synchronisation des ordinateurs de poche et la redirection de dossiers spéciaux.
- **Noms des machines utilisateur.** Spécifiez si l'Interface Web doit remplacer le nom des machines utilisateurs pour les ressources en mode connecté.

  Important : si vous souhaitez utiliser la fonction de contrôle de l'espace de travail avec les versions 8.*x* et 9.*x* des clients pour Windows, vous devez activer le paramètre Remplacer le nom des machines utilisateur.

Pour les sites XenApp Services qui délivrent des ressources en mode connecté, vous pouvez utiliser la tâche Options de session dans la console de gestion de l'Interface Web Citrix pour configurer les paramètres suivants pour les sessions utilisateur :

- **Affichage.** Sélectionnez les tailles de fenêtre disponibles pour les sessions ICA et définissez des tailles personnalisées en pixels ou en pourcentage par rapport à la taille de l'écran. Par ailleurs, vous pouvez permettre à l'Interface Web d'utiliser le lissage de polices ClearType. Il faut pour cela que les paramètres correspondants soient configurés

sur les systèmes d'exploitation des utilisateurs, Citrix Online Plug-in et la batterie de serveurs.

- **Couleur et son.** Les options activées dans cette section peuvent être sélectionnées par les utilisateurs.

- **Ressources locales.** Activez les fonctions des combinaisons de touches Windows que les utilisateurs peuvent sélectionner. Les combinaisons de touches Windows n'affectent pas les connexions transparentes. Vous pouvez activer les fonctions suivantes :

  - **Bureau local.** Les combinaisons de touches ne s'appliquent qu'au bureau local physique ; elles ne sont pas transmises aux sessions ICA.

  - **Bureau distant.** Les combinaisons de touches s'appliquent au bureau virtuel dans la session ICA.

  - **Bureaux plein écran uniquement.** Les combinaisons de touches s'appliquent au bureau virtuel dans la session ICA uniquement lorsqu'il est en mode plein écran.

  Activez la redirection de dossiers spéciaux de façon à ce que lorsque les utilisateurs ouvrent, ferment ou enregistrent sur les dossiers \Documents ou \Bureau à partir de ressources en ligne, leurs actions sont redirigées vers les dossiers sur leurs ordinateurs locaux. Pour plus d'informations, veuillez consulter la section Redirection vers les dossiers spéciaux.

- **Contrôle de l'espace de travail.** Configurez le comportement de reconnexion et de fermeture de session. Pour plus d'informations, veuillez consulter la section Configuration du contrôle de l'espace de travail.

Contrôle de la bande passante

Le contrôle de la bande passante permet aux utilisateurs de sélectionner les paramètres de session en fonction de leur bande passante de connexion. Ces options apparaissent sur l'écran Paramètres, avant ou après l'ouverture de session. Le contrôle de la bande passante permet de régler le nombre de couleurs, la qualité audio et le mappage d'imprimantes. Vous pouvez également utiliser la console de gestion de l'Interface Web Citrix pour spécifier des paramètres par défaut ou personnalisés. Utilisez la tâche Gérer les paramètres de session pour personnaliser les paramètres de bande passante à l'aide des options Performances des connexions. Sélectionnez Personnalisée dans la liste déroulante Vitesse de connexion pour activer les options Qualité des couleurs, Son et Activer mappage d'imprimantes.

En cas d'utilisation du client pour Java, le contrôle de la bande passante détermine si des packs de mappage d'imprimantes et de mappage audio sont disponibles. En cas d'utilisation du logiciel de connexion au Bureau à distance, la qualité audio est activée ou désactivée et aucun contrôle de qualité ultérieur n'est fourni. Des paramètres de bande passante faible sont recommandés pour les connexions WAN sans fil.

Remarque : si le logiciel de connexion au Bureau à distance est utilisé avec le contrôle de la bande passante, l'Interface Web indique les paramètres appropriés à la bande passante sélectionnée. Toutefois, le comportement réel dépend de la version du logiciel de connexion au Bureau à distance utilisé, des serveurs Terminal Server et de la configuration des serveurs.

Par défaut, les utilisateurs peuvent régler la taille de la fenêtre des sessions.

Si vous empêchez les utilisateurs de régler un paramètre, celui-ci ne s'affiche pas dans l'interface utilisateur et les paramètres spécifiés sur le serveur pour la ressource sont utilisés.

Lissage de polices ClearType

ClearType est une technologie d'anticrénelage subpixellaire développée par Microsoft. Elle améliore le rendu de texte sur les écrans LCD en réduisant les défauts perceptibles visibles et en affichant des caractères plus « lisses ». Le lissage de polices ClearType est une fonctionnalité qui a été introduite dans Windows XP. Le lissage de polices est activé par défaut dans Windows 7 et Windows Vista, mais pas dans Windows XP.

L'Interface Web et Citrix Online Plug-in prennent en charge le lissage de polices ClearType durant les sessions ICA. Lorsqu'un utilisateur exécutant Windows XP se connecte au serveur, le plug-in détecte automatiquement le paramètre de lissage de polices sur l'ordinateur de l'utilisateur et l'envoie au serveur. Ce paramètre est utilisé pendant toute la durée de la session.

Le lissage de polices doit être activé sur les systèmes d'exploitation des utilisateurs, Citrix Online Plug-in, le site Interface Web et la batterie de serveurs. Utilisez la tâche Paramètres de session dans la console de gestion de l'Interface Web Citrix pour activer le lissage de polices pour les sites XenApp Web et la tâche Options de session pour les sites XenApp Services.

Le lissage de polices s'applique uniquement aux ressources en mode connecté. Cette fonctionnalité n'est pas disponible pour les applications en mode déconnecté.

Redirection vers les dossiers spéciaux

Mise à jour : 2014-11-24

La fonctionnalité de redirection de dossiers spéciaux permet aux utilisateurs de mapper des dossiers Windows spéciaux du serveur vers leur ordinateur local de façon à faciliter l'utilisation de ressources en mode connecté. Le terme *dossiers spéciaux* fait référence aux dossiers Windows standard, tels que \Documents et \Bureau, qui s'affichent toujours de la même façon quel que soit le système d'exploitation.

> **Remarque :** préalablement à Windows Vista, « Mon » apparaissait devant les noms de dossiers spéciaux, le dossier « Documents » était donc appelé « Mes documents » dans Windows XP.

Lorsque des utilisateurs ouvrent, ferment, ou enregistrent des fichiers dans une session dans laquelle la redirection de dossiers spéciaux n'est pas activée, les icônes Documents et Bureau qui apparaissent dans les boîtes de dialogue de navigation dans les ressources en mode connecté des utilisateurs représentent les dossiers Documents et Bureau des utilisateurs sur le serveur. La redirection de dossiers spéciaux permet de rediriger certaines actions, telles que l'ouverture ou l'enregistrement d'un fichier de façon à ce que lorsque les utilisateurs ouvrent ou enregistrent des fichiers dans leurs dossiers \Documents ou \Bureau, ils accèdent à ces mêmes dossiers sur leurs ordinateurs locaux. Pour l'instant, la redirection est uniquement prise en charge sur les dossiers \Documents et \Bureau.

La redirection de dossiers spéciaux s'applique uniquement aux ressources en mode connecté. Cette fonctionnalité n'est pas disponible pour les applications en mode déconnecté.

Activation de la redirection de dossiers spéciaux

La prise en charge de la redirection de dossiers spéciaux est désactivée par défaut pour les sites XenApp Web et XenApp Services. Si vous activez la redirection de dossiers spéciaux pour un site, vous devez vous assurer qu'aucune règle de stratégie dans votre batterie de serveurs n'empêche les utilisateurs d'accéder à leurs lecteurs locaux ou d'y effectuer des enregistrements.

Utilisez la tâche Paramètres de session dans la console de gestion de l'Interface Web Citrix pour activer la redirection de dossiers spéciaux pour les sites XenApp Web et la tâche Options de session pour les sites XenApp Services. Vous pouvez également permettre aux utilisateurs d'activer cette fonctionnalité sur l'écran Paramètres.

Lorsque la redirection de dossiers spéciaux est activée, les utilisateurs doivent s'assurer que les ressources disposent d'un accès en lecture et écriture total aux fichiers et dossiers locaux en sélectionnant Plein accès sur la boîte de dialogue Sécurité des fichiers clients dans le Centre de connexion Citrix. Les utilisateurs doivent fermer toutes les sessions actives avant de démarrer une nouvelle session sur une autre machine. Citrix recommande de ne pas activer la redirection de dossiers spéciaux pour les utilisateurs qui se connectent à la même session simultanément depuis plusieurs machines.

Configuration du contrôle de l'espace de travail

Utilisez la fonctionnalité de contrôle de l'espace de travail pour permettre aux utilisateurs de se déconnecter rapidement de toutes les ressources (applications, contenu et bureaux), de se reconnecter aux ressources déconnectées et de fermer la session de toutes les ressources. Ceci permet aux utilisateurs de passer d'une machine à une autre et d'avoir accès à toutes leurs ressources (déconnectées uniquement ou déconnectées et actives) soit lorsqu'ils ouvrent une session, soit manuellement à tout moment. Le personnel hospitalier peut, par exemple, avoir besoin de se déplacer entre plusieurs stations de travail et d'accéder à la même série de ressources à chaque ouverture de session.

Conditions requises par le contrôle de l'espace de travail

La configuration requise et les recommandations et fonctionnalités suivantes s'appliquent à la fonction de contrôle de l'espace de travail :

- Pour utiliser le contrôle de l'espace de travail avec les versions 8.*x* et 9.*x* des clients pour Windows ou Citrix Presentation Server 4.0, vous devez activer le paramètre Remplacer le nom des machines utilisateur dans la tâche Préférences de session de la console de gestion de l'Interface Web Citrix.

- Si l'Interface Web détecte une tentative d'accès depuis une session Citrix, la fonction de contrôle de l'espace de travail est désactivée.

- En fonction des paramètres de sécurité, Internet Explorer peut bloquer le téléchargement des fichiers si ce dernier n'est pas directement initié par l'utilisateur, c'est pourquoi les tentatives de reconnexion à des ressources à l'aide d'un client natif peuvent être bloquées. Dans les situations dans lesquelles la reconnexion est impossible, un message d'avertissement s'affiche et invite les utilisateurs à reconfigurer leurs paramètres de sécurité Internet Explorer.

- Le délai de chaque session Web expire après une période d'inactivité (généralement de 20 minutes). Lorsque la session HTTP expire, l'écran de fermeture de session s'affiche. Toutes les ressources ouvertes ou reconnectées au cours de cette session ne sont toutefois pas déconnectées. Les utilisateurs doivent se déconnecter manuellement, fermer la session ou ouvrir une nouvelle session Interface Web et utiliser le bouton Fermeture de session ou Déconnecter.

- Les ressources publiées en vue d'une utilisation anonyme sont fermées lorsque les utilisateurs anonymes et authentifiés se déconnectent, à condition que le service XML Citrix soit configuré de façon à approuver les informations d'identification de l'Interface Web. Les utilisateurs ne peuvent donc pas se reconnecter à des ressources anonymes après s'être déconnectés.

- Pour utiliser l'authentification unique, une carte à puce ou une carte à puce avec authentification unique, vous devez établir une relation d'approbation entre le serveur Interface Web et le Service XML Citrix. Pour plus d'informations, veuillez consulter la section Utilisation du contrôle de l'espace de travail avec des méthodes d'authentification intégrée pour les sites XenApp Web.

- Si les informations d'identification simplifiée ne sont pas activées pour les sites XenApp Services, les utilisateurs de carte à puce sont invités à entrer leur code secret pour chaque session Citrix (après reconnexion). Ce problème ne se pose pas avec l'authentification unique ou les cartes à puce avec authentification unique sur les sites XenApp Services car ces options permettent d'activer l'authentification unique des informations d'identification.

Limitations du contrôle de l'espace de travail

Si vous envisagez d'activer le contrôle de l'espace de travail, tenez compte de ce qui suit :

- Le contrôle de l'espace de travail n'est pas disponible pour les sites configurés pour mettre à disposition des applications en mode déconnecté. Si vous configurez un site pour une mise à disposition en mode double, le contrôle de l'espace de travail fonctionne uniquement avec les ressources en mode connecté.

- Vous ne pouvez pas utiliser le contrôle de l'espace de travail avec le client Windows 32 bits avant la version 8 ou avec le logiciel de connexion au Bureau à distance. En outre, cette fonctionnalité n'est disponible qu'avec des serveurs exécutant la version 4.5 de Presentation Server ou une version ultérieure.

- Le contrôle de l'espace de travail permet uniquement de se reconnecter à des bureaux virtuels XenDesktop déconnectés. Les utilisateurs ne peuvent pas se reconnecter à des bureaux virtuels suspendus.

Utilisation du contrôle de l'espace de travail avec des méthodes d'authentification intégrée pour les sites XenApp Web

La section suivante s'applique aux sites XenApp Web uniquement. Si les utilisateurs ouvrent une session à l'aide d'une authentification unique, d'une carte à puce ou d'une carte à puce à authentification unique, vous devez établir une relation d'approbation entre le serveur Interface Web et tout autre serveur exécutant le Service XML Citrix en contact avec l'Interface Web. Le Service Citrix XML communique des informations sur les ressources entre l'Interface Web et les serveurs exécutant XenApp et XenDesktop. Sans une telle relation, les boutons Se déconnecter, Se reconnecter et Fermeture de session ne fonctionnent pas pour les utilisateurs qui ouvrent une session à l'aide d'une carte à puce ou de l'authentification unique.

Vous n'avez pas à établir de relation d'approbation si vos utilisateurs sont authentifiés par la batterie de serveurs, c'est-à-dire s'ils n'ouvrent pas de session à l'aide des méthodes d'authentification unique ou d'une carte à puce.

Pour établir une relation d'approbation

Si vous configurez un serveur afin qu'il approuve les requêtes envoyées au service XML Citrix, vous devez prendre en compte les facteurs suivants.

- Lorsque vous établissez une relation d'approbation, vous dépendez du serveur de l'Interface Web pour l'authentification de l'utilisateur. Pour éviter tout risque relatif à la sécurité, utilisez IPSec, des pare-feu ou toute technologie garantissant que seuls les services approuvés communiquent avec le service XML Citrix. Si vous n'utilisez ni IPSec, ni pare-feu, ni une autre technologie de sécurité pour l'établissement de la relation d'approbation, n'importe quelle machine réseau peut provoquer la déconnexion ou la fermeture des sessions. La relation d'approbation n'est pas nécessaire si les sites sont configurés pour une authentification explicite uniquement.

- Activez la relation d'approbation uniquement sur les serveurs contactés directement par l'Interface Web. Les serveurs sont répertoriés dans la tâche Batteries de serveurs dans la console de gestion de l'Interface Web Citrix.

- Configurez la technologie que vous utilisez pour la sécurisation de l'environnement afin de limiter l'accès au service XML Citrix uniquement aux serveurs Interface Web. Si, par exemple, le service XML Citrix partage un port avec IIS (Internet Information Services) de Microsoft, vous pouvez utiliser la fonctionnalité de restriction des adresses IP d'IIS pour restreindre l'accès au service XML Citrix.

1. Ouvrez une session sur un serveur de la batterie et cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix Delivery Services Console.

2. Dans le panneau gauche de la console, accédez à Ressources Citrix > XenApp, développez le nœud pour votre batterie et cliquez sur Stratégies.

3. Dans le panneau de détails de la console, sélectionnez l'onglet Ordinateur et cliquez sur Nouveau.

4. Entrez un nom et une description (facultatif) pour votre nouvelle stratégie et cliquez sur Suivant.

5. Dans la liste Catégories, cliquez sur Service XML et, sous Paramètres, sélectionnez Approbation des requêtes XML et cliquez sur Ajouter.

6. Sélectionnez Activé et cliquez sur OK. Cliquez sur Next.

7. Le cas échéant, appliquez des filtres à votre stratégie pour déterminer les circonstances sous lesquelles elle s'applique et cliquez sur Suivant.

8. Assurez-vous que la case Activer cette stratégie est sélectionnée et cliquez sur Enregistrer.

Pour activer la reconnexion automatique à l'ouverture de session des utilisateurs

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, sélectionnez la tâche appropriée pour votre type de site :

   - Pour les sites XenApp Web, cliquez sur Contrôle de l'espace de travail.

   - Pour les sites XenApp Services, cliquez sur Options de session et sélectionnez Contrôle de l'espace de travail.
4. Sélectionnez l'option Reconnexion automatique aux sessions après ouverture de session par l'utilisateur.

5. Choisissez l'une des options suivantes :

   - Pour vous reconnecter automatiquement à la fois aux sessions déconnectées et aux sessions actives, sélectionnez Se reconnecter à toutes les sessions.

   - Pour vous reconnecter automatiquement aux sessions déconnectées uniquement, sélectionnez Se reconnecter uniquement aux sessions déconnectées.
6. Sélectionnez la case Autoriser les utilisateurs à personnaliser pour permettre aux utilisateurs de configurer ce paramètre par eux-mêmes. Les utilisateurs peuvent modifier ce paramètre sur l'écran Paramètres des sites XenApp Web ou dans la boîte de dialogue Options de Citrix Online Plug-in.

Pour activer le bouton Se reconnecter

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web ou Sites XenApp Services, et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, sélectionnez la tâche appropriée pour votre type de site :

   - Pour les sites XenApp Web, cliquez sur Contrôle de l'espace de travail.

   - Pour les sites XenApp Services, cliquez sur Options de session et sélectionnez Contrôle de l'espace de travail.
4. Sélectionnez l'option Activer le bouton Se reconnecter.

5. Choisissez l'une des options suivantes :

   - Pour configurer le bouton Se reconnecter afin de vous reconnecter à la fois aux sessions déconnectées et aux sessions actives, sélectionnez Se reconnecter à toutes les sessions.

   - Pour configurer le bouton Se reconnecter afin de vous reconnecter uniquement aux sessions déconnectées, sélectionnez Se reconnecter uniquement aux sessions déconnectées.
6. Sélectionnez la case Autoriser les utilisateurs à personnaliser pour permettre aux utilisateurs de configurer ce paramètre par eux-mêmes. Les utilisateurs peuvent modifier ce paramètre sur l'écran Paramètres des sites XenApp Web ou dans la boîte de dialogue Options de Citrix Online Plug-in pour les sites XenApp Services.

Pour configurer le comportement de fermeture de session

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.

2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web et sélectionnez votre site dans le panneau des résultats.

3. Dans le panneau Actions, cliquez sur Contrôle de l'espace de travail.

4. Sélectionnez la case Fermer toutes les sessions lorsque les utilisateurs ferment leur session du site pour fermer la session Interface Web des utilisateurs ainsi que toutes les sessions actives. Si vous ne sélectionnez pas cette case, les sessions des utilisateurs restent actives après leur fermeture.

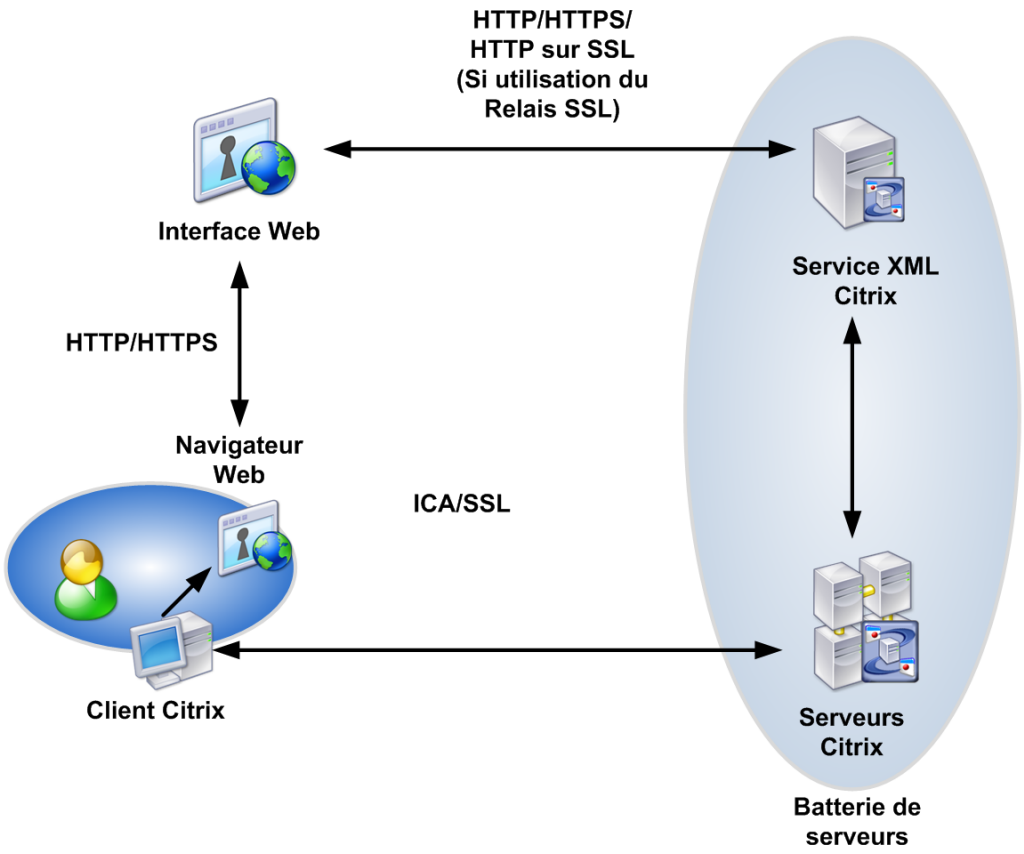
5. Sélectionnez la case Autoriser les utilisateurs à personnaliser pour permettre aux utilisateurs de configurer ce paramètre par eux-mêmes sur l'écran Paramètres du site.

Configuration de la sécurité de l'Interface Web

Un plan de sécurité exhaustif doit aborder la protection de vos données à chaque étape du processus de mise à disposition des publiées. Cette section décrit les problèmes et fournit des recommandations pour chacune des étapes suivantes de communication de l'Interface Web.

- **Communications entre machine utilisateur et Interface Web.** Explique les problèmes associés au transfert des données Interface Web entre les navigateurs Web et les serveurs, et suggère des stratégies pour la protection des données en transit et des données sauvegardées sur les machines utilisateur.
- **Communications entre l'Interface Web et le serveur Citrix.** Décrit comment sécuriser les informations d'authentification et les informations sur les ressources échangées entre le serveur Interface Web et la batterie de serveurs.
- **Communications entre la session utilisateur et le serveur.** Examine les problèmes associés à l'échange des informations de session entre les clients Citrix et les serveurs. Présente les implémentations des fonctionnalités de sécurité de l'Interface Web et de XenApp/XenDesktop qui protègent de telles données.

Ce diagramme illustre l'interaction entre les machines utilisateur, le serveur exécutant XenApp ou XenDesktop et le serveur Interface Web.



Considérations générales relatives à la sécurité

Pour la configuration du serveur, Citrix vous conseille de suivre les directives standard de Microsoft, comme avec tout autre serveur Windows.

Vérifiez toujours que tous les composants sont à jour avec tous les derniers correctifs logiciels. Pour obtenir plus d'informations et consulter les dernières recommandations de téléchargement, visitez le site Web de Microsoft à l'adresse : http://support.microsoft.com/.

SSL et TLS

Mise à jour : 2014-12-02

Le protocole SSL (Secure Socket Layer) offre la possibilité de sécuriser les communications de données sur les réseaux. SSL offre des fonctions d'authentification du serveur, de cryptage du flux de données et de vérification de l'intégrité des messages.

SSL utilise la cryptographie pour coder les messages, authentifier leur identité et garantir l'intégrité de leur contenu. Ces fonctions protègent des risques tels que l'écoute clandestine, les erreurs d'acheminement et la manipulation des données. SSL utilise des certificats de clé publique, émis par des autorités de certification, comme preuve d'identité. Pour de plus amples informations sur SSL, la cryptographie et les certificats, consultez les rubriques sous Sécurisation des batteries de serveurs et Sécuriser le réseau d'entreprise.

Transport Layer Security (TLS)

TLS (Transport Layer Security) est la dernière version normalisée du protocole SSL. L'IETF (Internet Engineering Taskforce) l'a renommé TLS en prenant en charge le développement du protocole SSL en tant que norme ouverte. Comme SSL, TLS offre des fonctions d'authentification du serveur, de cryptage du flux de données et de contrôle de l'intégrité des messages.

TLS version 1.0 est pris en charge par les versions de XenApp pour Windows et XenDesktop prises en charge. Les différences techniques entre SSL 3.0 et TLS 1.0 étant mineures, les certificats de serveur que vous utilisez pour SSL dans votre installation fonctionnent également pour TLS.

Certaines organisations, notamment des organisations gouvernementales américaines, requièrent l'utilisation du protocole TLS pour la sécurisation de leurs communications de données. Ces organisations peuvent également exiger l'utilisation d'une cryptographie éprouvée, telle que FIPS 140. FIPS (Federal Information Processing Standard) est une norme de cryptographie.

Remarque : la taille maximale de clé de certificat SSL/TLS prise en charge par l'Interface Web pour les serveurs d'application Java est de 2 048 bits.

Relais SSL

Le Relais SSL est un composant qui utilise SSL pour garantir la sécurité des communications entre les serveurs Interface Web et les batteries de serveurs. Le Relais SSL assure l'authentification des serveurs, le cryptage des données et l'intégrité des messages pour les connexions TCP/IP. Le Relais SSL est fourni par le service XTE Citrix.

Le Relais SSL sert d'intermédiaire dans les communications entre le serveur Interface Web et le Service XML Citrix. Lorsque vous utilisez le Relais SSL, le serveur Web contrôle d'abord son identité en vérifiant son certificat de serveur au moyen d'une liste d'autorités de

certification approuvées.

Après cette authentification, le serveur Web et le Relais SSL négocient une méthode de cryptage pour la session. Le serveur Web transmet ensuite toutes les requêtes d'information sous forme cryptée au Relais SSL. Le Relais SSL décrypte les requêtes et les transmet au Service XML Citrix. Lorsqu'il renvoie les informations au serveur Web, le service XML les transmet via le serveur exécutant le Relais SSL qui crypte les données et les transmet au serveur Web pour décryptage. L'intégrité des messages est contrôlée pour chaque communication afin de vérifier que les données n'ont pas été modifiées lors du transit.

Cryptage ICA

Le cryptage ICA permet de crypter les informations échangées entre un serveur et un client Citrix. Il est ainsi plus difficile pour les utilisateurs non autorisés d'interpréter une transmission cryptée.

Le cryptage ICA préserve la confidentialité des informations en cas d'écoute clandestine. Cependant, d'autres dangers menacent la sécurité, et l'utilisation du cryptage ne représente qu'un aspect d'une stratégie globale de sécurité. Contrairement à SSL/TLS, le cryptage ICA ne permet pas l'authentification du serveur. Par conséquent, les informations pourraient théoriquement être interceptées sur le réseau et redirigées vers un faux serveur. Par ailleurs, le cryptage ICA n'assure pas de contrôle de l'intégrité.

Le cryptage ICA n'est pas disponible pour XenApp pour serveurs UNIX.

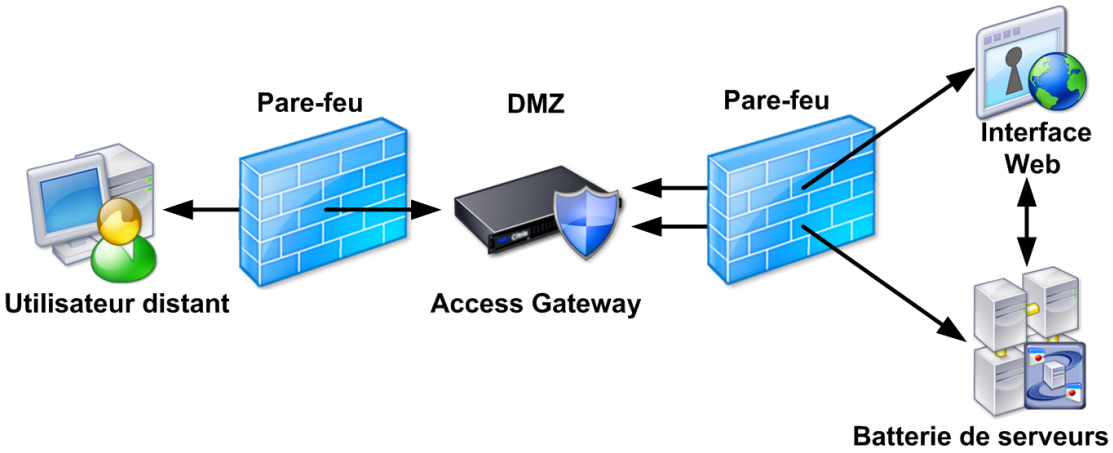
Access Gateway

Vous pouvez utiliser Access Gateway avec l'Interface Web et Secure Ticket Authority (STA) pour fournir l'authentification, l'autorisation et la redirection des ressources (applications, contenu et bureaux) mises à disposition à partir d'un serveur exécutant XenApp ou XenDesktop.

Access Gateway est un boîtier VPN (virtual private network) SSL universel qui garantit un accès unique et sécurisé à toute ressource d'informations (données et voix). Access Gateway crypte et prend en charge toutes les ressources et tous les protocoles.

Access Gateway fournit aux clients distants un accès sécurisé et transparent aux applications, contenus, bureaux et aux ressources réseau, leur permettant de travailler avec des fichiers sur des lecteurs réseau, des e-mails, des sites intranet et des ressources, comme s'ils travaillaient à l'intérieur du pare-feu de leur organisation.

Ce diagramme explique les méthodes utilisées par Access Gateway pour sécuriser les communications entre les clients Citrix compatibles SSL/TLS et les serveurs.



Pour plus d'informations sur Access Gateway, veuillez consulter la documentation relative à Access Gateway. Pour plus d'informations sur la configuration de l'Interface Web pour la prise en charge d'Access Gateway à l'aide de la console de gestion de l'Interface Web Citrix, veuillez consulter la section Pour configurer les paramètres de passerelle.

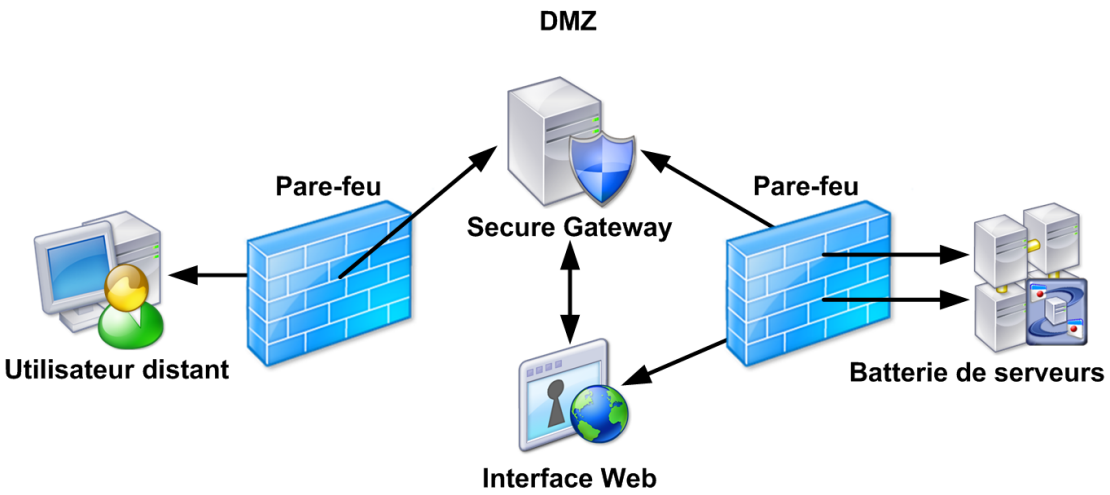
Secure Gateway

Mise à jour : 2014-11-25

Vous pouvez utiliser Secure Gateway avec l'Interface Web pour fournir un point d'accès Internet unique, sécurisé et crypté aux serveurs des réseaux d'entreprise internes.

En cryptant le trafic ICA, Secure Gateway joue le rôle d'une passerelle Internet sécurisée entre les clients Citrix compatibles SSL/TLS et les serveurs. La partie Internet du trafic entre les machines utilisateur et le serveur Secure Gateway est cryptée à l'aide du protocole SSL/TLS. Cela signifie que les utilisateurs peuvent accéder à des informations à distance sans compromettre la sécurité. Secure Gateway simplifie aussi la gestion des certificats, un certificat n'étant requis que sur le serveur Secure Gateway et non sur chaque serveur de la batterie.

Ce diagramme explique les méthodes utilisées par Secure Gateway pour sécuriser les communications entre les clients Citrix compatibles SSL/TLS et les serveurs.



Pour plus d'informations sur la configuration de l'Interface Web pour la prise en charge de Secure Gateway à l'aide de la console de gestion de l'Interface Web Citrix, veuillez consulter la section Pour configurer les paramètres de passerelle.

Sécurisation de Citrix Online Plug-in avec SSL

Pour utiliser SSL afin de sécuriser les communications entre Citrix Online Plug-in et le serveur Interface Web à l'aide de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Services dans le panneau de gauche, sélectionnez le site dans le panneau des résultats, cliquez sur Paramètres du serveur dans le panneau Actions, et sélectionnez la case Utiliser SSL/TLS pour les communications entre les plug-ins et ce site.

Assurez-vous, pour chaque application, que la case Activer les protocoles SSL et TLS est cochée dans la page Options du client de la boîte de dialogue Application propriétés dans la console Delivery Services Console.

Communications entre machine utilisateur et Interface Web

Les communications entre les clients Citrix et le serveur Interface Web consistent en un échange de différents types de données. Lorsque les utilisateurs procèdent à leur identification, parcourent les ressources et sélectionnent une ressource, le navigateur et le serveur Web se transmettent les informations d'identification des utilisateurs, les séries de ressources et les fichiers d'initialisation de session. Plus précisément, les données échangées incluent les éléments suivants.

- **Données de formulaire HTML.** Lorsque les utilisateurs ouvrent une session, les sites de l'Interface Web utilisent un formulaire HTML standard pour transmettre les informations d'identification des utilisateurs du navigateur Web au serveur Web. Le formulaire Interface Web transmet les noms d'utilisateur et les informations d'identification sous forme de texte clair.

- **Pages HTML et cookies de session.** Une fois entrées dans la page Ouvrir une session, les informations d'identification de l'utilisateur sont stockées sur le serveur Web et protégées par un cookie de session. Les pages HTML transmises du serveur Web au navigateur contiennent les séries de ressources. Ces pages dressent la liste des ressources mises à disposition de l'utilisateur.

- **Fichiers ICA.** Lorsqu'un utilisateur sélectionne une ressource, le serveur Web transmet un fichier .ica pour cette ressource au client Citrix (dans certains cas, le navigateur Web est utilisé comme intermédiaire). Le fichier .ica contient un ticket qui peut être utilisé pour ouvrir une session sur le serveur. les fichiers ICA ne comprennent pas de ticket pour l'authentification unique ou par carte à puce.

  Il arrive dans certains cas que le fichier .ica soit enregistré en tant que fichier texte sur le disque dur de l'utilisateur lorsqu'un client est lancé. Ceci n'empêche aucunement le client de se lancer et ne représente donc pas un problème.

  La signature de fichier ICA permet aux utilisateurs de vérifier qu'ils lancent des applications ou bureaux provenant d'un serveur Web approuvé. Pour des informations complémentaires, veuillez consulter la section Configuration de la signature de fichier ICA.

Problèmes de sécurité posés par les communications entre machine utilisateur et Interface Web

Des agresseurs peuvent exploiter les données de l'Interface Web alors qu'elles transitent sur le réseau entre le serveur Web et le navigateur, et lorsqu'elles sont écrites sur la machine utilisateur.

- Des agresseurs peuvent intercepter les données d'ouverture de session, le cookie de session et les pages HTML en transit entre le serveur Web et le navigateur.
- Bien que le cookie de session utilisé par l'Interface Web soit transitoire et disparaisse lorsque l'utilisateur ferme le navigateur Web, des agresseurs ayant accès au navigateur de l'utilisateur peuvent le récupérer et, le cas échéant, utiliser les informations d'identification.
- Bien que le fichier .ica ne contienne pas les informations d'identification de l'utilisateur, il comporte un ticket à usage unique, dont la validité expire, par défaut, au bout de 200 secondes. Il se peut que des agresseurs utilisent le fichier .ica intercepté pour se connecter au serveur avant que l'utilisateur autorisé n'utilise le ticket et établisse la connexion.
- Si les utilisateurs Internet Explorer qui se connectent à un serveur Web au moyen d'une connexion HTTPS ont sélectionné l'option empêchant la mise en cache des pages cryptées, le fichier .ica est enregistré en texte clair dans le dossier \Temporary Internet Files de Windows. Des agresseurs qui auraient accès au cache Internet Explorer d'un utilisateur pourraient récupérer le fichier .ica afin d'obtenir les informations réseau.
- Si l'authentification unique est activée sur le client Citrix, des agresseurs peuvent envoyer à l'utilisateur un fichier .ica qui provoque le détournement de ses informations d'identification vers un serveur non autorisé ou un faux serveur. Cela se produit lorsque le client capture les informations d'identification d'utilisateurs lors de l'ouverture de session sur leurs machines et les renvoie vers un serveur quelconque (si le fichier .ica contient le paramètre approprié).

Recommandations relatives à la protection des communications entre machine utilisateur et Interface Web

Les recommandations suivantes combinent des pratiques de sécurité standard de l'industrie et des méthodes Citrix pour la protection des données transitant entre les machines utilisateur et le serveur Web, et des données écrites sur les machines utilisateur.

Utilisation de serveurs Web et navigateurs SSL/TLS

La sécurisation des communications entre le serveur Web et le navigateur de l'Interface Web commence par la mise en place de serveurs Web et de navigateurs sécurisés. La sécurité de nombreux serveurs Web repose sur la technologie SSL/TLS.

Dans une transaction typique entre serveur Web et navigateur, le navigateur vérifie d'abord l'identité du serveur en comparant son certificat de serveur à une liste d'autorités de certification approuvées. Après vérification, le navigateur crypte les requêtes de page de l'utilisateur puis décrypte les documents renvoyés par le serveur Web. À la fin de chaque transaction, des contrôles d'intégrité de message TLS (Transport Layer Security) ou SSL (Secure Sockets Layer) vérifient que les données n'ont pas été modifiées lors du transit.

Dans un déploiement Interface Web, l'authentification SSL/TLS et le cryptage créent une connexion sécurisée permettant à l'utilisateur de transmettre les informations d'identification qu'il a entrées dans la page Ouvrir une session. Les données transmises à partir du serveur Web (cela comprend les informations d'identification, les cookies de session, les fichiers .ica et les pages HTML de série de ressources) sont toutes sécurisées.

Pour mettre en œuvre la technologie SSL/TLS sur votre réseau, vous devez posséder un serveur Web et un navigateur Web compatibles SSL/TLS. L'utilisation de ces produits s'effectue en toute transparence pour l'Interface Web. Il n'est pas nécessaire de configurer les serveurs Web et les navigateurs pour l'Interface Web. Pour plus de détails sur la configuration du serveur Web pour la prise en charge de la technologie SSL/TLS, veuillez consulter documentation de votre serveur Web.

Important : de nombreux serveurs Web compatibles SSL/TLS utilisent le port TCP/IP 443 pour les communications HTTP. Par défaut, le Relais SSL utilise également ce port. Si votre serveur Web exécute également le Relais SSL, assurez-vous que le serveur Web ou le Relais SSL est configuré pour utiliser un autre port.

N'activez pas l'authentification unique

Pour empêcher tout détournement des informations d'identification des utilisateurs vers un serveur non autorisé ou un faux serveur, n'activez pas l'authentification unique dans les installations sécurisées. N'utilisez cette fonction que dans les environnements réduits et approuvés.

Communications entre l'Interface Web et le serveur Citrix

Les communications entre l'Interface Web et le serveur exécutant XenApp ou XenDesktop impliquent le transfert des informations d'identification et des informations sur les séries de ressources de l'utilisateur entre l'Interface Web et le service XML Citrix sur la batterie de serveurs.

Dans une session standard, l'Interface Web transfère des informations d'identification au Service XML Citrix pour l'authentification de l'utilisateur et le Service XML Citrix renvoie des informations sur les séries de ressources. Le serveur et la batterie échangent les informations à l'aide d'une connexion TCP/IP et du protocole XML Citrix.

Problèmes de sécurité posés par les communications entre l'Interface Web et le serveur Citrix

À l'exception des mots de passe, qui sont transmis masqués, le protocole XML de l'Interface Web n'effectue aucun cryptage des données. Les données sont donc transmises en clair. Les communications sont vulnérables aux attaques suivantes :

- Des agresseurs peuvent intercepter le trafic XML et s'emparer des informations sur les séries de ressources et des tickets. Des agresseurs ayant la capacité de désactiver le masquage peuvent également obtenir les informations d'identification des utilisateurs.
- Des agresseurs peuvent se faire passer pour le serveur et intercepter les requêtes d'authentification.

Recommandations relatives à la protection des communications entre l'Interface Web et le serveur Citrix

Citrix recommande d'implémenter l'une des mesures de sécurité suivantes pour sécuriser le trafic XML entre le serveur Interface Web et la batterie de serveurs :

- Utilisez le Relais SSL comme intermédiaire de sécurité entre le serveur Interface Web et la batterie de serveurs. Le Relais SSL procède à l'authentification de l'hôte et au cryptage des données.
- Dans les déploiements ne prenant pas en charge le Relais SSL, installez l'Interface Web sur le serveur exécutant XenApp ou XenDesktop.
- Utilisez le protocole HTTPS pour envoyer les données de l'Interface Web via une connexion HTTP sécurisée à l'aide de SSL si Microsoft Internet Information Services (IIS) est installé sur le serveur exécutant XenApp ou XenDesktop.

Utilisation du Relais SSL

Mise à jour : 2014-12-02

Le Relais SSL est un composant par défaut de XenApp et XenDesktop.

Côté serveur, vous devez installer un certificat de serveur sur le serveur exécutant le Relais SSL et vérifier la configuration de ce dernier. Pour plus d'informations sur l'installation d'un certificat de serveur et la configuration du relais SSL sur les serveurs, consultez les rubriques sous Configuration de SSL/TLS entre les serveurs et les clients. Vous pouvez également consulter l'aide de l'Outil de configuration du Relais SSL. Pour XenApp pour serveurs UNIX, consultez la rubrique Relais SSL pour l'administration UNIX.

Lors de la configuration du Relais SSL, assurez-vous que le serveur exécutant le Relais SSL autorise la transmission des données SSL aux serveurs dont le service XML Citrix sera utilisé comme point de contact. Par défaut, le Relais SSL ne transmet les données qu'au serveur sur lequel il est installé. Vous pouvez toutefois le configurer pour diriger les données vers d'autres serveurs. Si votre Relais SSL est situé sur un serveur différent de celui sur lequel vous voulez envoyer les données Interface Web, assurez-vous que le serveur sur lequel vous voulez envoyer les données Interface Web figure dans la liste de serveurs du Relais SSL.

Vous pouvez configurer l'Interface Web pour qu'elle utilise le Relais SSL à l'aide de la console de gestion de l'Interface Web Citrix ou du fichier WebInterface.conf. Pour plus d'informations sur l'utilisation de la console pour configurer l'Interface Web afin d'utiliser le Relais SSL, consultez la rubrique Configuration des paramètres pour tous les serveurs d'une batterie.

Pour configurer l'Interface Web afin d'utiliser le Relais SSL à l'aide de WebInterface.conf

1. À l'aide d'un éditeur de texte, ouvrez le fichier WebInterface.conf.
2. Remplacez la valeur SSLRelayPort dans le paramètre **Farm<*n*>** par le numéro de port du Relais SSL sur le serveur.
3. Remplacez la valeur du réglage Transport dans le paramètre **Farm<*n*>** par SSL.

Pour ajouter un nouveau certificat racine au serveur Interface Web

Pour ajouter la prise en charge d'une autorité de certification, vous devez ajouter le certificat racine de l'autorité de certification au serveur Interface Web.

Copiez le certificat racine dans votre serveur Web.

- Sous IIS, le certificat est copié à l’aide du composant logiciel enfichable Gestionnaire de certificat de MMC (Microsoft Management Console).
- Sur les serveurs d'application Java, utilisez l'outil de ligne de commande keytool pour copier le certificat dans le répertoire de stockage de clés approprié pour votre plate-forme. Le certificat doit être ajouté au stock de clés associé à la machine virtuelle Java qui fournit les pages Web. Le stock de clés se trouve généralement dans les emplacements suivants :
  - {javax.net.ssl.trustStore}
  - {java.home}/lib/security/jssecacerts
  - {java.home}/lib/security/cacerts

Activation de l'Interface Web sur le serveur exécutant XenApp ou XenDesktop

Pour les déploiements ne permettant pas l’utilisation du Relais SSL, il est possible d’éliminer le risque d’une attaque réseau en exécutant un serveur Web sur le serveur qui fournit les données de l'Interface Web. L’hébergement des sites de l'Interface Web sur un tel serveur Web permet de diriger toutes les requêtes de l'Interface Web vers le service XML Citrix de l’hôte local et d’éliminer ainsi la transmission de données de l'Interface Web sur le réseau. Cependant, il convient de comparer les avantages de l’élimination de la transmission réseau aux risques d’exploitation du serveur Web.

Vous pouvez commencer par placer votre serveur Web et le serveur exécutant XenApp ou XenDesktop derrière un pare-feu afin de ne pas exposer les communications entre ces serveurs aux utilisateurs d’Internet. Dans ce scénario, les machines utilisateur doivent être capables de communiquer via le pare-feu avec le serveur Web et le serveur exécutant XenApp ou XenDesktop. Le pare-feu doit permettre le trafic HTTP (généralement via le port http 80 ou 443 si un serveur Web sécurisé est utilisé) pour les communications entre la machine utilisateur et le serveur Web. Pour les communications entre le client et le serveur, le pare-feu doit autoriser le trafic ICA entrant sur les ports1494 et 2598. Pour de plus amples informations sur l'utilisation du protocole ICA avec des pare-feu réseau, consultez la documentation du serveur Web. Pour plus de détails sur l'utilisation de l'Interface Web avec la traduction d'adresse réseau, reportez-vous au kit de développement de l'Interface Web.

Remarque : sur les systèmes exécutant XenApp, le programme d’installation vous permet de forcer le Service XML Citrix à partager le port TCP/IP d’Internet Information Services plutôt que d'utiliser un port dédié. Avec XenDesktop, le programme d'installation active le partage de port automatiquement. Lorsque le partage du port est activé, le service XML Citrix et le serveur Web utilisent le même port par défaut.

Utilisation du protocole HTTPS

Vous pouvez utiliser le protocole HTTPS pour sécuriser les données de l'Interface Web échangées entre le serveur Web et le serveur exécutant XenApp ou XenDesktop. HTTPS utilise le protocole SSL/TLS pour assurer un cryptage fort des données.

Le serveur Web établit une connexion HTTPS à IIS sur le serveur exécutant XenApp ou XenDesktop. Cette opération exige le partage du port IIS sur le serveur exécutant XenApp ou XenDesktop et l'activation du protocole SSL sur ce serveur. Le nom de serveur que vous spécifiez (à l'aide de la console ou dans le paramètre **Farm<*n*>** dans WebInterface.conf) doit être un nom DNS complet correspondant au nom du certificat de serveur SSL IIS.

Le service XML Citrix est disponible dans https://*nomserveur*/scripts/wpnbr.dll. Pour plus d'informations sur la configuration de l'Interface Web pour l'utilisation du protocole HTTPS à l'aide de la console de gestion de l'Interface Web Citrix, veuillez consulter la section Gestion de l'accès sécurisé.

Pour configurer l'Interface Web afin d'utiliser le protocole HTTPS à l'aide du fichier WebInterface.conf

1. À l'aide d'un éditeur de texte, ouvrez le fichier WebInterface.conf.
2. Remplacez la valeur du réglage Transport dans le paramètre **Farm<*n*>** par HTTPS.

Communications entre la session utilisateur et le serveur

Les communications de l'Interface Web entre les machines utilisateur et les serveurs impliquent la transmission de plusieurs types de données de session, notamment des requêtes d'initialisation et des informations de session.

- **Requêtes d'initialisation.** La première étape permettant d'établir une session, appelée *initialisation*, exige que le client Citrix fasse la requête d'une session et fournisse une liste de paramètres de configuration de session. Ces paramètres contrôlent divers aspects de la session, comme l'utilisateur devant ouvrir une session, la taille de la fenêtre à tracer et le programme à exécuter au cours de la session.

- **Informations de session.** Après l'initialisation de la session, les informations sont transmises entre le client Citrix et le serveur par un certain nombre de couches virtuelles ; par exemple les entrées souris (du client au serveur) et les mises à jour graphiques (du serveur au client).

Problèmes de sécurité posés par les communications entre la session utilisateur et le serveur

Pour capturer et interpréter les communications réseau entre le client et le serveur, des agresseurs doivent être capables de déchiffrer le protocole client binaire. Des agresseurs connaissant les détails du protocole client binaire peuvent :

- intercepter les informations de requête d'initialisation envoyées depuis le client Citrix, notamment les informations d'identification de l'utilisateur ;

- intercepter les informations de session, y compris le texte et les clics de souris entrés par les utilisateurs ainsi que les mises à jour d'affichage envoyées depuis le serveur.

Recommandations relatives à la protection des communications entre la session utilisateur et le serveur

Mise à jour : 2014-12-02

Citrix recommande de sécuriser les données transitant entre les machines utilisateur et les serveurs en cryptant le trafic ou en déployant Access Gateway.

Utilisation du protocole SSL/TLS ou du cryptage ICA

Citrix vous conseille d'utiliser SSL/TLS ou le cryptage ICA pour assurer la sécurité du trafic entre vos clients Citrix et vos serveurs. Les deux méthodes prennent en charge le cryptage 128 bits du flux de données entre le client et le serveur, mais SSL/TLS prend également en charge la vérification de l'identité du serveur.

Toutes les versions prises en charge de XenApp et XenDesktop prennent en charge SSL. SSL/TLS et le cryptage ICA sont pris en charge par les versions de XenApp pour Windows et XenDesktop prises en charge. Pour obtenir une liste des clients Citrix prenant en charge chaque méthode, consultez la documentation des clients ou le site de téléchargement Citrix. Pour plus d'informations sur le cryptage ICA, veuillez consulter la rubrique Administration XenApp.

Utilisation d'Access Gateway

Vous pouvez utiliser Access Gateway pour assurer la sécurité du trafic Internet entre vos clients Citrix et les serveurs. Access Gateway est un dispositif universel de réseau privé virtuel (VPN) SSL qui garantit un accès unique et sécurisé à toutes les ressources. Pour plus d'informations sur Access Gateway, veuillez consulter la documentation Access Gateway archivée. Pour plus d'informations sur la configuration de l'Interface Web pour la prise en charge d'Access Gateway à l'aide de la console de gestion de l'Interface Web Citrix, veuillez consulter la section Pour configurer les paramètres de passerelle.

Contrôle de la journalisation des diagnostics

Utilisez la tâche Journalisation des diagnostics sous Maintenance du site dans la console de gestion de l'Interface Web Citrix pour renforcer la sécurité du système en matière de journalisation des erreurs. Vous pouvez empêcher que les événements en double soient journalisés à plusieurs reprises et définir le nombre d'événements en double qui sont journalisés ainsi que la fréquence de leur journalisation.

Cette tâche vous permet également d'indiquer l'adresse URL de redirection des erreurs. Si vous spécifiez une adresse URL de page d'erreur personnalisée, vous devez gérer tous les identificateurs d'erreur avec cette adresse URL et envoyer des messages d'erreur à vos utilisateurs. En outre, cette adresse URL de page d'erreur remplacera l'écran de fermeture de session des utilisateurs même si ces derniers ont fermé leur session sans qu'aucune erreur ne se produise.

Configuration de sites à l'aide du fichier de configuration

Mise à jour : 2014-11-24

Fichiers de configuration de sites

Les sites Interface Web comprennent un fichier appelé WebInterface.conf contenant les données de configuration du site. Utilisez-le pour effectuer les tâches d'administration quotidiennes et personnaliser les paramètres d'un site. Vous pouvez par exemple spécifier les paramètres que les utilisateurs sont autorisés à modifier et configurer l'authentification à l'Interface Web.

Si vous entrez une valeur de paramètre incorrecte lors de la modification d'un fichier de configuration puis que vous utilisez la console de gestion de l'Interface Web Citrix, la console remplace cette valeur incorrecte par la valeur par défaut lorsque le fichier est enregistré.

Si la console de gestion de l'Interface Web Citrix est en cours d'exécution lorsque vous modifiez un fichier de configuration de site manuellement, toute modification que vous apportez à l'aide de la console entraînera l'écrasement de tous vos fichiers de configuration. Citrix vous conseille de fermer la console de gestion de l'Interface Web Citrix avant de modifier les fichiers de configuration de site. Si cela n'est pas possible, actualisez la console afin de valider les modifications manuelles que vous avez apportées au fichier de configuration avant de réaliser d'autres changements à l'aide de la console.

Le fichier WebInterface.conf est disponible dans le répertoire de configuration de site :

- Sur Microsoft Internet Information Services (IIS), ce fichier se trouve généralement dans C:\Inetpub\wwwroot\Citrix*nomdusite*\conf
- Sur les serveurs d'application Java tels que Apache Tomcat, cet emplacement est ./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF

Vous pouvez remplacer certaines valeurs de configuration dans WebInterface.conf (une page à la fois) dans vos scripts de serveur Web. Pour plus d'informations sur les scripts de serveur Web, reportez-vous au kit de développement de l'Interface Web.

Remarque : il est possible, sur les serveurs d'application Java, que vous ayez besoin d'arrêter et de redémarrer le serveur Web pour que les modifications apportées à WebInterface.conf soient prises en compte. De plus, assurez-vous que vous enregistrez vos modifications au format UTF-8.

Pour configurer les communications avec le serveur

Dans cet exemple, vous souhaitez définir le nom d'un serveur supplémentaire exécutant le service XML Citrix. Le service XML Citrix constitue le lien de communication entre la batterie de serveurs et le serveur Interface Web.

Les communications s'effectuent actuellement avec un serveur dénommé « rock », mais vous souhaitez ajouter le serveur « roll », en cas de défaillance de rock. Pour ce faire :

1. À l'aide d'un éditeur de texte, ouvrez le fichier WebInterface.conf et localisez la ligne suivante :

   Farm1=rock,Name:Farm1,XMLPort:80,Transport:HTTP, SSLRelayPort:443,…

2. Modifiez cette ligne pour inclure le serveur supplémentaire comme suit:

   Farm1=rock,roll,Name:Farm1,XMLPort:80,Transport:HTTP, SSLRelayPort:443,…

Pour configurer les communications du Relais SSL

Dans cet exemple, vous souhaitez sécuriser les communications entre le serveur Web et le serveur exécutant XenApp ou XenDesktop, par le biais du protocole SSL (Secure Socket Layer). Le Relais SSL est installé sur un serveur exécutant XenApp ou XenDesktop dont l'adresse est de type nom de domaine complet (blues.mycompany.com). Le Relais SSL est à l'écoute des connexions sur le port TCP 443.

Les communications s'effectuent actuellement avec un serveur « rhythm », mais vous souhaitez le remplacer par blues.mycompany.com. Pour ce faire :

1. À l'aide d'un éditeur de texte, ouvrez le fichier WebInterface.conf et localisez la ligne suivante :

   Farm1=rhythm,Name:Farm1,XMLPort:80,Transport:HTTP, SSLRelayPort:443

2. Définissez le transport sur SSL, comme indiqué ci-dessous:

   Farm1=blues.mycompany.com,Name:Farm1,XMLPort:80, Transport:SSL,SSLRelayPort:443

Remarque : le nom de serveur spécifié doit correspondre au nom figurant sur le certificat du serveur.

Pour configurer la prise en charge de Secure Gateway

Dans cet exemple, vous souhaitez définir un serveur Secure Gateway appelé « csg1.mycompany.com » sur lequel les clients Citrix utilisent le port 443, à l'aide des deux adresses Secure Ticket Authority suivantes :

- http://country.mycompany.com/scripts/ctxsta.dll
- http://western.mycompany.com/scripts/ctxsta.dll

Ajoutez les lignes suivantes dans le fichier WebInterface.conf :

AlternateAddress=Mapped

CSG_STA_URL1=http://country.mycompany.com/scripts/ctxsta.dll

CSG_STA_URL2=http://western.mycompany.com/scripts/ctxsta.dll

CSG_Server=csg1.mycompany.com

CSG_ServerPort=443

ClientAddressMap=*,SG

La dernière ligne permet d'activer Secure Gateway pour tous les utilisateurs.

Pour configurer des batteries de récupération d'urgence

Dans cet exemple, deux batteries de serveurs sont dédiées à la résolution des problèmes, tels qu'une panne de courant ou un problème réseau, susceptibles d'empêcher les utilisateurs d'accéder aux batteries de production.

Les serveurs exécutant le service XML Citrix dans les batteries s'appellent « jazz » et « fusion ». Vous voulez faire de ces deux batteries des batteries de récupération d'urgence. Pour ce faire, utilisez un éditeur de texte, ouvrez le fichier WebInterface.conf et ajoutez les lignes suivantes pour configurer les réglages de ce paramètre conformément à votre environnement :

RecoveryFarm1=jazz,Name:RecoveryFarm1,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60
RecoveryFarm2=fusion,Name:RecoveryFarm2,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:

Veuillez noter que la deuxième batterie est uniquement utilisée lorsque la première batterie de récupération d'urgence n'est pas accessible. Les ressources ne sont pas regroupées sur les deux batteries de récupération d'urgence car elles sont destinées aux batteries de production. Au lieu de cela, l'Interface Web contacte chaque batterie de récupération d'urgence l'une après l'autre et énumère les ressources de la première batterie avec laquelle elle parvient à communiquer.

Paramètres WebInterface.conf

Mise à jour : 2014-11-25

Le tableau ci-dessous indique les paramètres pouvant figurer dans WebInterface.conf (par ordre alphabétique). Les valeurs par défaut apparaissent en **gras**. Si un paramètre n'est pas spécifié dans WebInterface.conf, c'est sa valeur par défaut qui est utilisée.

AccountSelfServiceUrl

- Description : indique l'URL du service Password Manager.
- Valeur : adresse URL valide avec HTTPS
- Type de site : XenApp Web

AdditionalExplicitAuthentication

- Description : indique l'authentification explicite à deux facteurs que vous devez réaliser conjointement avec SAM (Secure Access Manager), ADS (Active Directory Services) ou NDS (Novell Directory Services).
- Valeur : None | SecurID | SafeWord | RADIUS
- Type de site : XenApp Web

AddressResolutionType

- Description : indique le type d'adresse à utiliser dans le fichier de lancement .ica.
- Valeur : dns-port | dns | ipv4-port | ipv4
- Type de site : XenApp Web et XenApp Services

AGAuthenticationMethod

- Description : indique les méthodes d'authentification autorisées pour les sites intégrés Access Gateway. Ce paramètre doit être défini sur Explicit si les utilisateurs se connectent à Access Gateway à l'aide d'un nom d'utilisateur et d'un mot de passe. Si les utilisateurs se connectent à Access Gateway avec une carte à puce, l'application du paramètre SmartCard indique que les utilisateurs doivent entrer un code PIN chaque fois qu'ils accèdent à une ressource. L'option SmartCardKerberos permet aux utilisateurs qui se connectent à Access Gateway avec une carte à puce d'accéder à leurs ressources sans entrer de code PIN.
- Valeur : Explicit | SmartCard | SmartCard Kerberos
- Type de site : XenApp Web

AGEPromptPassword

- Description : indique si les utilisateurs sont invités ou non à entrer de nouveau leurs mots de passe en ouvrant une session depuis la page d'ouverture de session d'Access Gateway.
- Valeur : Off | On
- Type de site : XenApp Web

AGEWebServiceURL

- Description : indique l'adresse URL du service d'authentification d'Access Gateway.
- Valeur : adresse URL valide
- Type de site : XenApp Web

AllowBandwidthSelection

- Description : indique si les utilisateurs peuvent ou non spécifier la vitesse de leur connexion réseau de façon à optimiser les paramètres ICA.
- Valeur : Off | On
- Type de site : XenApp Web

AllowCustomizeAudio

- Description : indique si les utilisateurs sont autorisés ou non à régler la qualité audio des sessions ICA.
- Valeur : Off | On
- Type de site : XenApp Web

AllowCustomizeAutoLogin

- Description : indique si les utilisateurs sont autorisés ou non à activer/désactiver l'ouverture de session automatique.
- Valeur : On | Off
- Type de site : XenApp Web

AllowCustomizeClientPrinterMapping

- Description : indique si les utilisateurs sont autorisés ou non à activer/désactiver le mappage d'imprimantes clientes.
- Valeur : Off | On
- Type de site : XenApp Web

AllowCustomizeJavaClientPackages

- Description : indique si les utilisateurs sont autorisés ou non à choisir les packs Client pour Java à utiliser.

- Valeur : Off | On
- Type de site : XenApp Web

AllowCustomizeLayout

- Description : indique si les utilisateurs sont autorisés ou non à choisir entre l'interface utilisateur avancée ou simplifiée.
- Valeur : Off | On
- Type de site : XenApp Web

AllowCustomizeLogoff

- Description : indique si les utilisateurs sont autorisés ou non à modifier le comportement du contrôle de l'espace de travail lorsqu'ils ferment la session du serveur.
- Valeur : On | Off
- Type de site : XenApp Web

AllowCustomizePersistFolderLocation

- Description : indique si les utilisateurs sont autorisés ou non à activer/désactiver la fonctionnalité leur permettant de revenir sur le dernier dossier visité sur l'écran Applications lorsqu'ils rouvrent une session.
- Valeur : Off | On
- Type de site : XenApp Web

AllowCustomizeReconnectAtLogin

- Description : indique si les utilisateurs sont autorisés ou non à ne pas tenir compte du comportement de la fonctionnalité de contrôle de l'espace de travail à l'ouverture d'une session.
- Valeur : On | Off
- Type de site : XenApp Web

AllowCustomizeReconnectButton

- Description : indique si les utilisateurs sont autorisés ou non à ne pas tenir compte du comportement de la fonctionnalité de contrôle de l'espace de travail lorsqu'ils utilisent le bouton Se reconnecter.
- Valeur : On | Off
- Type de site : XenApp Web

AllowCustomizeSettings

- Description : indique si les utilisateurs sont autorisés ou non à personnaliser leurs sessions Interface Web. Lorsque ce paramètre est réglé sur Off, le bouton Préférences ne s'affiche pas sur les écrans Ouvrir une session et Applications des utilisateurs.
- Valeur : On | Off
- Type de site : XenApp Web

AllowCustomizeShowHints

- Description : indique si les utilisateurs sont autorisés ou non à afficher/masquer les conseils sur l'écran Applications.
- Valeur : On | Off
- Type de site : XenApp Web

AllowCustomizeShowSearch

- Description : indique si les utilisateurs sont autorisés ou non à activer/désactiver la fonction de recherche sur l'écran Applications.
- Valeur : Off | On
- Type de site : XenApp Web

AllowCustomizeSpecialFolderRedirection

- Description : indique si les utilisateurs sont autorisés ou non à activer/désactiver la fonctionnalité de redirection de dossiers spéciaux.
- Valeur : Off | On
- Type de site : XenApp Web

AllowCustomizeTransparentKeyPassthrough

- Description : indique si les utilisateurs sont autorisés ou non à sélectionner l'authentification par combinaison de touches.
- Valeur : Off | On
- Type de site : XenApp Web

AllowCustomizeVirtualCOMPortEmulation

- Description : indique si les utilisateurs sont autorisés ou non à activer/désactiver la synchronisation des ordinateurs de poche.
- Valeur : Off | On
- Type de site : XenApp Web

AllowCustomizeWinColor

- Description : indique si les utilisateurs sont autorisés ou non à modifier la profondeur de couleurs des sessions ICA.
- Valeur : Off | On
- Type de site : XenApp Web

AllowCustomizeWinSize

- Description : indique si les utilisateurs sont autorisés ou non à modifier la taille de fenêtre des sessions ICA.
- Valeur : On | Off
- Type de site : XenApp Web

AllowDisplayInFrames

- Description : indique si les sites XenApp Web sont autorisés à être affichés au sein des cadres intégrés dans les pages Web tierces.
- Valeur : On | Off
- Type de site : XenApp Web

AllowFontSmoothing

- Description : indique si le lissage de polices est autorisé pour les sessions ICA.
- Valeur : On | Off
- Type de site : XenApp Web et XenApp Services

AllowUserAccountUnlock

- Description : indique si les utilisateurs sont autorisés ou non à déverrouiller leur compte à l'aide de l'option Libre-service de compte.
- Valeur : Off | On
- Type de site : XenApp Web

AllowUserPasswordChange

- Description : indique sous quelles conditions les utilisateurs peuvent modifier leur mot de passe.
- Valeur : Never | Expired-Only | Always (Sites XenApp Web uniquement)
- Type de site : XenApp Web et XenApp Services

AllowUserPasswordReset

- Description : indique si les utilisateurs sont autorisés ou non à réinitialiser leur mot de passe à l'aide de l'option Libre-service de compte.

- Valeur : Off | On
- Type de site : XenApp Web

AlternateAddress

- Description : indique si l'adresse secondaire de serveur doit ou ne doit pas être renvoyée dans le fichier .ica.
- Valeur : Off | Mapped | On
- Type de site : XenApp Web et XenApp Services

ApplicanceEmbeddedSmartCardSSO

- Description : indique si l'authentification avec carte à puce utilise le contrôle ActiveX pour l'authentification unique.
- Valeur : Off | On
- Type de site : Desktop Appliance Connector

ApplianceEmbeddedSmartCardSSOPinTimeout

- Description : nombre de secondes que l'écran de saisie du code PIN d'authentification avec carte à puce attend avant de retourner sur l'écran d'ouverture de session lorsqu'il ne détecte aucune activité.
- Valeur : 20
- Type de site : Desktop Appliance Connector

ApplianceMultiDesktop

- Description : spécifie si la liste des bureaux est affichée lorsque plusieurs bureaux sont attribués aux utilisateurs.
- Valeur : Off | On
- Type de site : Desktop Appliance Connector

ApplicationAccessMethods

- Description : indique si les utilisateurs sont autorisés à accéder à des applications à l'aide d'un client pour ressources en mode connecté, Citrix Offline Plug-in ou les deux.
- Valeur : Remote, Streaming
- Type de site : XenApp Web et XenApp Services

AppSysMessage _<*Codedelangue*>

- Description : indique le texte localisé qui s'affiche dans le bas de la zone de contenu principal de l'écran Applications. *Codedelangue* est en, fr, de, es, ja ou tout autre code de langue pris en charge.

- Valeur : None. Texte en clair plus un nombre quelconque de balises
 de nouvelle ligne HTML et de liens hypertexte
- Type de site : XenApp Web

AppTab<*n*>

- Description : indique les onglets qui s'affichent dans l'écran Applications. Plusieurs instances peuvent être utilisées pour définir des onglets multiples. Vous pouvez également définir un seul onglet qui contiendra toutes les ressources auxquelles l'utilisateur a accès à l'aide de la valeur AllResources.
- Valeur : Applications | Desktops | Content | AllResources
- Type de site : XenApp Web

AppWelcome Message _<*Codedelangue*>

- Description : indique le texte localisé qui s'affiche en haut de la zone de contenu principal de l'écran Applications. *Codedelangue* est en, fr, de, es, ja ou tout autre code de langue pris en charge.
- Valeur : None. Texte en clair plus un nombre quelconque de balises
 de nouvelle ligne HTML et de liens hypertexte
- Type de site : XenApp Web

AuthenticationPoint

- Description : indique l'emplacement où l'authentification a lieu.
- Valeur : WebInterface | ADFS | AccessGateway | 3rdParty | WebServer
- Type de site : XenApp Web

AutoLaunchDesktop

- Description : indique si l'accès automatique aux bureaux est activé. Lorsque ce paramètre est activé, l'Interface Web lancera automatiquement le bureau de l'utilisateur s'il s'agit de la seule ressource disponible dans toutes les batteries.
- Valeur : Off | On
- Type de site : XenApp Web

AutoLoginDefault

- Description : indique si les ouvertures de session automatiques sont activées par défaut pour les utilisateurs qui accèdent à leurs ressources à l'aide de l'authentification unique, de l'authentification unique avec carte à puce et de l'authentification par carte à puce.
- Valeur : On | Off
- Type de site : XenApp Web

BrandingColor

- Description : indique la couleur des zones d'en-tête et de bas de page.
- Valeur : nom ou nombre hexadécimal d'une couleur
- Type de site : XenApp Web

BrandingImage

- Description : indique l'adresse URL de l'image personnalisée pour les zones d'en-tête et de bas de page.
- Valeur : adresse URL valide
- Type de site : XenApp Web

BypassFailedRadiusServerDuration

- Description : indique le laps de temps s'écoulant avant qu'un serveur RADIUS défaillant puisse être réutilisé.
- Valeur : durée en minutes (60)
- Type de site : XenApp Web

BypassFailedSTADuration

- Description : indique le laps de temps s'écoulant avant qu'un serveur défaillant exécutant la Secure Ticket Authority pour une machine passerelle puisse être réutilisé.
- Valeur : durée en minutes (60)
- Type de site : XenApp Web

ClientAddressMap

- Description : indique les paires adresse cliente/type d'adresse pour la configuration du pare-feu du côté serveur. Le premier champ dans l'entrée est une adresse et un masque de sous-réseau, tandis que le deuxième peut avoir l'une des valeurs suivantes : Normal, Alternate, Translated, SG, SGAlternate et SGTranslated. L'utilisation d'un astérisque (*) à la place d'une adresse ou d'un sous-réseau indique la valeur par défaut de tous les clients Citrix non spécifiés.
- Valeur : <*AdresseSous-réseau*>/ <*MasqueSous-réseau*> |*, Normal | Alternate | Translated | SG | SGTranslated | SGAlternate, …
- Type de site : XenApp Web

ClientDefaultURL

- Description : indique l'adresse URL vers laquelle le processus de détection et de déploiement de client redirige les utilisateurs lorsque le client adéquat n'est pas disponible au téléchargement.
- Valeur : http://www. citrix.com/ download. Adresse URL valide

- Type de site : XenApp Web

ClientIcaLinuxX86

ClientIcaMac

ClientIcaSolarisSparc

ClientIcaSolarisX86

ClientIcaWin32

ClientStreamingWin32

- Description : configure le processus de détection et de déploiement de client pour la plate-forme spécifiée. Si le paramètre approprié n'a pas été configuré, les utilisateurs sont redirigés vers la page Web spécifiée par le paramètre ClientDefaultURL. Par défaut, ces paramètres sont configurés pour les clients natifs fournis sur le support d'installation de XenApp 5.6.

  Les deux premiers champs indiquent l'emplacement et le nom de fichier du programme d'installation du client. Si le fichier n'est pas trouvé, les utilisateurs sont redirigés vers la page Web spécifiée par le paramètre ClientDefaultURL.

  Le champ Mui indique si le client spécifié par les champs Directory et Filename assure la prise en charge multilingue. Si No est sélectionné, le processus de détection et de déploiement de client recherche le fichier spécifié dans le dossier <*Codedelangue*>\<*Nomdedossier*>.

  Le champ Version indique le numéro de version séparé par des virgules du client spécifié par les champs Directory et Filename. Si aucun numéro de version n'est spécifié, le processus de détection et de déploiement de client essaye de déterminer la version à partir du fichier spécifié.

  Le champ ShowEULA indique si les utilisateurs doivent accepter ou non le contrat de licence Citrix pour pouvoir installer le client spécifié.

  Le champ ClassID indique l'ID de classe des clients Windows. Ce paramètre est requis pour ces clients.

  Le champ Url indique la page Web vers laquelle les utilisateurs sont redirigés lorsqu'ils cliquent sur le bouton Télécharger et qu'aucun fichier de client n'a été spécifié à l'aide des champs Directory et Filename. Ce paramètre doit uniquement être utilisé lorsqu'aucun fichier client n'est disponible.

  Le champ Description permet de spécifier un message personnalisé à afficher au dessus du bouton Télécharger Veuillez noter que ce texte n'est pas traduit.

- Valeur : Directory: <*Nomdedossier*>, Filename:<*Nomdefichier*>, [Mui:Yes |No,] [Version: <*Numérodeversion*>,] [ShowEULA:Yes|No,] [ClassID: <*Valeur*>,] [Url: "<*URLvalide*>,] [Description: <*Légende*>]

- Type de site : XenApp Web

ClientProxy

- Description : indique les adresses et les masques de sous-réseau du client et les paramètres proxy associés pour un pare-feu du côté client. L'adresse du client dans le fichier ICA renvoyé est déterminée par ces paramètres. Chaque entrée comprend trois champs. Le premier est une adresse et un masque de sous-réseau. L'utilisation du signe (*) indique la valeur par défaut de tous les clients Citrix non spécifiés. Le deuxième champ est l'un des six types de proxy. La valeur du troisième champ (adresse du proxy) dans chaque série de trois est ignorée si le deuxième champ (type de proxy) ne contient pas un type de proxy explicite (SOCKS ou Secure), mais elle doit toujours être présente ; la valeur par défaut de ce champ est le signe moins (-).

- Valeur: <*AdresseSous-réseau*>/ <*MasqueSous-réseau*> |*, Auto | WpadAuto | Client | None | SOCKS | Secure, - | <*Adresse Proxy*> | <*AdresseProxy*>: <*PortProxy*>, …

- Type de site : XenApp Web et XenApp Services

CompactHeaderImage

- Description : indique l'adresse URL de l'image d'en-tête pour la version simplifiée de l'interface utilisateur.

- Valeur : adresse URL valide

- Type de site : XenApp Web

CompactViewStyles

- Description : indique les styles d'affichage mis à la disposition des utilisateurs sur l'écran Applications de la version simplifiée de l'interface utilisateur.

- Valeur : Icons, List

- Type de site : XenApp Web

CredentialFormat

- Description : indique les formats des informations d'identification pour les ouvertures de session explicites Windows et NIS.

- Valeur : All | UPN | DomainUsername

- Type de site : XenApp Web et XenApp Services

CSG_EnableSessionReliability

- Description : indique si la fiabilité de session doit être utilisée avec Secure Gateway ou Access Gateway.

- Valeur : On | Off

- Type de site : XenApp Web et XenApp Services

CSG_Server

- Description : indique l'adresse du boîtier Access Gateway ou du serveur Secure Gateway.

- Valeur : None. Adresse du serveur sous forme de nom de domaine complet
- Type de site : XenApp Web et XenApp Services

CSG_ServerPort

- Description : indique le port du boîtier Access Gateway ou du serveur Secure Gateway.
- Valeur : None. Port du serveur
- Type de site : XenApp Web et XenApp Services

CSG_STA_URL<*n*>

- Description : indique l'adresse URL du serveur exécutant la Secure Ticket Authority pour une machine passerelle.
- Valeur : None. Adresse URL d'une STA
- Type de site : XenApp Web et XenApp Services

CSG_UseTwoTickets

- Description : indique si l'Interface Web demande des tickets de deux Secure Ticket Authorities différentes lors de l'accès à une ressource via Access Gateway.
- Valeur : Off | On
- Type de site : XenApp Web et XenApp Services

DefaultAudioQuality

- Description : indique la qualité audio par défaut à utiliser avec les connexions ICA.
- Valeur : NoPreference | High | Medium | Low | Off
- Type de site : XenApp Web

DefaultBandwidthProfile

- Description : indique le profil de bande passante par défaut (c'est-à-dire l'ensemble des paramètres liés à la bande passante, tels que la qualité audio et le nombre de couleurs) à utiliser avec les connexions ICA.
- Valeur : Custom | High | Medium High | Medium | low
- Type de site : XenApp Web

DefaultColorDepth

- Description : indique le nombre de couleurs à utiliser avec les connexions ICA.
- Valeur : NoPreference | TrueColor | HighNoPreferenceColor
- Type de site : XenApp Web

DefaultCompactViewStyle

- Description : indique le style d'affichage par défaut sur l'écran Applications de la version simplifiée de l'interface utilisateur.
- Valeur : List | Icons
- Type de site : XenApp Web

DefaultCustomTextLocale

- Description : indique la langue par défaut à utiliser pour le texte personnalisé. La même langue doit être spécifiée dans tout autre paramètre de texte personnalisé (*_<*Codedelangue*>) défini.
- Valeur : None. en | de | es | fr | ja | tout autre identificateur de langue prise en charge
- Type de site : XenApp Web

DefaultPrinterMapping

- Description : indique si le mappage d'imprimante est activé par défaut pour les connexions ICA.
- Valeur : On | Off
- Type de site : XenApp Web

DefaultViewStyle

- Description : indique le style d'affichage par défaut sur l'écran Applications de la version avancée de l'interface utilisateur.
- Valeur : Icons | Details | Groups | List | Tree
- Type de site : XenApp Web

DefaultWindowSize

- Description : indique le mode de fenêtre par défaut à utiliser pour les sessions ICA. Cette valeur peut être spécifiée sous forme de pourcentage de la zone d'écran totale à l'aide du format X% ou sous forme de dimensions personnalisées fixes à l'aide du format XxY
- Valeur : FullScreen | Seamless | X% | XxY
- Type de site : XenApp Web

DisplayBrandingImage

- Description : indique si l'image personnalisée est affichée pour les zones d'en-tête et de bas de page.
- Valeur : On | Off

- Type de site : XenApp Web

DomainSelection

- Description : indique les noms de domaines répertoriés dans l'écran d'ouverture de session de l'authentification explicite.
- Valeur : liste des noms de domaines NetBIOS
- Type de site : XenApp Web et XenApp Services

DuplicateLogInterval

- Description : indique la période pendant laquelle les entrées de journal DuplicateLogLimit feront l'objet d'une surveillance.
- Valeur : durée en minutes (60)
- Type de site : XenApp Web et XenApp Services

DuplicateLogLimit

- Description : indique le nombre d'entrées de journal en double autorisées pour la période DuplicateLogInterval.
- Valeur : entier supérieur à 0 (10)
- Type de site : XenApp Web et XenApp Services

EnableFileTypeAssociation

- Description : indique si l'association de type de fichier est activée ou désactivée pour un site. Si la valeur est Off, la redirection du contenu n'est pas disponible pour le site.
- Valeur : On | Off
- Type de site : XenApp Web et XenApp Services

EnableKerberosToMPS

- Description : indique si l'authentification Kerberos est activée ou désactivée.
- Valeur : Off | On
- Type de site : XenApp Web et XenApp Services

EnableLegacyICAClientSupport

- Description : indique si les anciens clients Citrix ne pouvant pas lire les fichiers .ica UTF-8 sont pris en charge. Si vous réglez cette option sur off, le serveur produit des fichiers .ica encodés UTF-8.
- Valeur : Off | On
- Type de site : XenApp Web et XenApp Services

EnableLogoffApplications

- Description : indique si la fonction de contrôle de l'espace de travail se déconnecte des ressources actives lorsque les utilisateurs ferment leur session sur le serveur.
- Valeur : On | Off
- Type de site : XenApp Web

EnablePassthroughURLs

- Description : indique si les utilisateurs sont autorisés à créer des liens persistants vers les ressources accessibles en utilisant l'Interface Web.
- Valeur : Off | On
- Type de site : XenApp Web

EnableRadiusServerLoadBalancing

- Description : indique si la charge des sessions est équilibrée entre les serveurs RADIUS configurés. Le basculement entre les serveurs se produit dans tous les cas, quelle que soit la valeur de ce paramètre.
- Valeur : Off | On
- Type de site : XenApp Web

EnableSTALoadBalancing

- Description : indique si la charge des requêtes est équilibrée entre les serveurs Secure Ticket Authority configurés pour un périphérique de passerelle.
- Valeur : Off | On
- Type de site : XenApp Web et XenApp Services

EnableVirtualCOMPortEmulation

- Description : indique s'il faut activer ou pas la synchronisation des ordinateurs de poche via des connexions par câble USB.
- Valeur : Off | On
- Type de site : XenApp Web

EnableWizardAutoMode

- Description : indique si le processus de détection et de déploiement de client est exécuté en mode automatique ou non.
- Valeur : On | Off
- Type de site : XenApp Web

EnableWorkspaceControl

- Description : indique si les utilisateurs ont accès à la fonctionnalité de contrôle de l'espace de travail.
- Valeur : On | Off
- Type de site : XenApp Web

ErrorCallbackURL

- Description : indique l'adresse URL vers laquelle l'Interface Web doit se rediriger en cas d'erreur. La page Web à laquelle se rapporte l'adresse URL doit accepter et traiter quatre paramètres de chaîne de requête :

  CTX_MessageType

  CTX_MessageKey

  CTX_MessageArgs

  CTX_LogEventID
- Valeur : adresse URL valide
- Type de site : XenApp Web

Farm<*n*>

- Description : indique toutes les informations relatives à une batterie. Vous pouvez configurer un maximum de 512 batteries.
- Valeur : Citrix XML Service address [,Citrix XML Service address,] [,Name:<*Nom*>] [,XMLPort:<*Port*>] [,Transport:<HTTP | HTTPS | SSL>] [,SSLRelayPort:<*Port*>] [,BypassDuration:<*DuréeenMinutes* (60)>] [,LoadBalance:<on | off>] [,TicketTime ToLive:<*DuréeenSecondes* (200)>] [,RADETicket TimeToLive:<*DuréeenSecondes* (200)>]
- Type de site : XenApp Web et XenApp Services

Farm<*n*>Groups

- Description : indique les groupes Active Directory qui sont autorisés à énumérer les ressources à partir des batteries de serveurs. La saisie d'une valeur pour ce paramètre permet d'activer la fonctionnalité d'itinérance des utilisateurs. Un maximum de 512 groupes d'utilisateur peut être spécifié pour chaque batterie définie avec le paramètre Farm<*n*>.
- Valeur : None. *Domaine*\ *Grouped'utilisateurs*[,...]
- Type de site : XenApp Web, XenApp Services et XenDesktop

FooterText _<*Codedelangue*>

- Description : indique que le texte de bas de page localisé s'affiche dans la zone de bas de page de toutes les pages. *Codedelangue* est en, fr, de, es, ja ou tout autre code de langue pris en charge.

- Valeur : None. Texte en clair plus un nombre quelconque de balises
 de nouvelle ligne HTML et de liens hypertexte
- Type de site : XenApp Web

HeaderFontColor

- Description : indique la couleur de police pour la zone d'en-tête.
- Valeur : nom ou nombre hexadécimal d'une couleur
- Type de site : XenApp Web

HeadingHomePage

- Description : indique l'adresse URL de l'image à afficher comme en-tête de la page d'accueil.
- Valeur : adresse URL valide
- Type de site : XenApp Web

HeadingImage

- Description : indique l'adresse URL de l'image à afficher comme en-tête de l'Interface Web.
- Valeur : adresse URL valide
- Type de site : XenApp Web

HideDomainField

- Description : indique si le champ de domaine s'affiche sur l'écran d'ouverture de session.
- Valeur : Off | On
- Type de site : XenApp Web

IcaFileSigningCertificateThumbprint

- Description : empreinte numérique du certificat à utiliser pour la signature de fichier ICA.
- Valeur : None. Empreinte numérique qui peut contenir ou non des espaces
- Type de site : XenApp Web et Desktop Appliance Connector

IcaFileSigningEnabled

- Description : active ou désactive la fonctionnalité de signature de fichier ICA.
- Valeur : Off | On
- Type de site : XenApp Web et Desktop Appliance Connector

IcaFileSigningHashAlgorithm

- Description : algorithme de hachage à utiliser pour la signature de fichier ICA.
- Valeur : SHA1 | SHA256
- Type de site : XenApp Web et Desktop Appliance Connector

IgnoreClientProvidedClientAddress

- Description : indique si l'adresse fournie par le client Citrix est ignorée.
- Valeur : Off | On
- Type de site : XenApp Web et XenApp Services

InternalServerAddressMap

- Description : indique les paires d'adresses normales/traduites. L'adresse normale identifie le serveur avec lequel la passerelle communique et l'adresse traduite est renvoyée au client Citrix.
- Valeur : NormalAddress = Translated Address, …
- Type de site : XenApp Web et XenApp Services

JavaClientPackages

- Description : indique par défaut les packs Client pour Java à mettre à la disposition des utilisateurs.
- Valeur : ClipBoard, ConfigUI, PrinterMapping, SecureICA, SSL, Audio, ClientDriveMapping, ZeroLatency
- Type de site : XenApp Web

JavaFallbackMode

- Description : indique si le client pour Java est utilisé lorsque les utilisateurs ne disposent pas d'un client natif. Ce paramètre ne s'applique que lorsque la valeur Ica-Local est incluse dans le paramètre LaunchClients. Le paramètre Manual permet aux utilisateurs d'utiliser ou non le client pour Java.
- Valeur : None | Manual | Auto
- Type de site : XenApp Web

KioskMode

- Description : indique si les paramètres utilisateur doivent être persistants ou uniquement valables pendant toute la durée de la session. Lorsque le mode Kiosque est activé, les paramètres utilisateur ne persistent pas d'une session à l'autre.
- Valeur : Off | On
- Type de site : XenApp Web

LaunchClients

- Description : indique les clients Citrix que les utilisateurs sont autorisés à sélectionner. Ce paramètre est ignoré pour les sites en mode double, pour lesquels le paramètre par défaut est Ica-Local. Même si le paramètre Ica-Java est ignoré, le client pour Java peut toujours être proposé aux utilisateurs. Pour cela, vous devez régler le paramètre JavaFallbackMode sur None.
- Valeur : Ica-Local, Ica-Java, Rdp-Embedded
- Type de site : XenApp Web

LoginDomains

- Description : indique les noms de domaines utilisés pour la restriction d'accès.
- Valeur : liste des noms de domaines NetBIOS
- Type de site : XenApp Web et XenApp Services

LoginSys Message _<*Codedelangue*>

- Description : indique le texte localisé qui s'affiche dans le bas de la zone de contenu principal de l'écran d'ouverture de session. *Codedelangue* est en, fr, de, es, ja ou tout autre code de langue pris en charge.
- Valeur : None. Texte en clair plus un nombre quelconque de balises
 de nouvelle ligne HTML et de liens hypertexte
- Type de site : XenApp Web

LoginTitle _<*Codedelangue*>

- Description : indique le texte traduit qui s'affiche au dessus du message de bienvenue sur l'écran Ouvrir une session. *Codedelangue* est en, fr, de, es, ja ou tout autre code de langue pris en charge.
- Valeur : None. Texte en clair plus un nombre quelconque de balises
 de nouvelle ligne HTML et de liens hypertexte
- Type de site : XenApp Web

LoginType

- Description : indique le type d'écran d'ouverture de session mis à la disposition des utilisateurs. Cet écran peut être basé sur un domaine ou NDS.
- Valeur : Default | NDS
- Type de site : XenApp Web et XenApp Services

LogoffFederationService

- Description : indique si les sessions des utilisateurs sont toutes fermées ou fermées uniquement sur les sites XenApp Web à partir du service de fédération lorsque le bouton de fermeture de session est utilisé dans un site ADFS intégré.

- Valeur : On | Off
- Type de site : XenApp Web

MultiFarmAuthenticationMode

- Description : ce mode dispose de trois options permettant de spécifier la méthode d'authentification autorisée. L'option « All » est le paramètre par défaut dans lequel toutes les batteries sont authentifiées afin d'énumérer les applications. L'option « Any » permet d'énumérer les applications de n'importe quelle batterie pour l'utilisateur authentifié ; toutefois, si l'utilisateur entre des informations d'identification incorrectes, celles-ci sont présentées à chaque batterie pour l'authentification même si l'authentification a échoué sur l'une des batteries. Cela peut également verrouiller le compte. L'option « Primary » permet à l'utilisateur de s'authentifier auprès de la batterie principale (la première batterie dans la liste des batteries configurées pour l'Interface Web) avant de revenir sur le mode « Any » ; cette option empêche les comptes d'être verrouillés.
- Valeur : All | Any | Primary
- Type de site : XenApp Web

MultiLaunchTimeout

- Description : indique la durée pendant laquelle les icônes de ressource restent inactives après que l'utilisateur clique dessus pour lancer la ressource.
- Valeur : durée en minutes (2)
- Type de site : XenApp Web

NDSContextLookupLoadbalancing

- Description : indique si la charge des requêtes NDS est équilibrée entre les serveurs LDAP configurés. Le basculement entre les serveurs se produit dans tous les cas, quelle que soit la valeur de ce paramètre.
- Valeur : Off | On
- Type de site : XenApp Web

NDSContextLookupServers

- Description : indique les serveurs LDAP à utiliser. Si le port de serveur n'est pas indiqué, il est déduit du protocole : si ce paramètre est défini sur ldap, le port LDAP par défaut (389) est utilisé ; le port SSL LDAP par défaut (636) est utilisé si le paramètre est défini sur ldaps. Vous pouvez configurer un maximum de 512 serveurs LDAP.

  Si ce paramètre n'est pas défini ou alors absent, la fonctionnalité d'ouverture de session hors contexte est désactivée.
- Valeur : None. ldap://[:] | ldaps://[:],
- Type de site : XenApp Web

NDSTreeName

- Description : indique l’arborescence NDS à utiliser en cas d'authentification NDS.
- Valeur : None. Nom de l'arborescence NDS
- Type de site : XenApp Web et XenApp Services

OverlayAutologonCredsWithTicket

- Description : indique si un ticket d'ouverture de session doit être dupliqué dans une entrée de ticket d'ouverture de session ou placé dans une entrée de ticket de fichier de lancement .ica séparé. Lorsque le recouvrement des informations d'identification est activé, les tickets d'ouverture de session sont dupliqués.
- Valeur : On | Off
- Type de site : XenApp Web

OverrideIcaClientname

- Description : indique si un identificateur généré par l'Interface Web doit être transmis dans l'entrée de nom de client d'un fichier de lancement .ica.
- Valeur : Off | On
- Type de site : XenApp Web

PasswordExpiryWarningPeriod

- Description : indique la durée, en nombre de jours, pendant laquelle les utilisateurs seront invités à changer de mot de passe avant expiration de ce dernier.
- Valeur : entier entre 0 et 999 (14)
- Type de site : XenApp Web

PersistFolderLocation

- Description : indique si les utilisateurs sont renvoyés sur le dernier dossier visité de l'écran Applications lorsqu'ils rouvrent une session.
- Valeur : Off | On
- Type de site : XenApp Web

PNAChangePasswordMethod

- Description : indique comment Citrix Online Plug-in traite les requêtes de modification de mot de passe des utilisateurs. Si ce paramètre est défini sur Direct-Only, le plug-in modifie le mot de passe en communiquant directement avec le contrôleur de domaine. Direct-With-Fallback indique que le plug-in tente dans un premier temps de contacter le contrôleur de domaine, et en cas d'échec, utilise le site XenApp Services. L'option Proxy indique que le plug-in modifie les mots de passe en contactant le site XenApp Services.
- Valeur : Direct-Only | Direct-With- Fallback | Proxy

- Type de site : XenApp Services

PooledSockets

- Description : indique si le regroupement de sockets doit ou non être utilisé.
- Valeur : On | Off
- Type de site : XenApp Web et XenApp Services

PreLoginMessageButton _<*Codedelangue*>

- Description : indique un nom localisé pour le bouton de confirmation du message de pré-ouverture de session. *Codedelangue* est en, fr, de, es, ja ou tout autre code de langue pris en charge.
- Valeur : None. Texte en clair plus un nombre quelconque de balises
 de nouvelle ligne HTML et de liens hypertexte
- Type de site : XenApp Web

PreLoginMessageText _<*Codedelangue*>

- Description : indique le texte localisé qui s'affiche sur la page du message de pré-ouverture de session. *Codedelangue* est en, fr, de, es, ja ou tout autre code de langue pris en charge.
- Valeur : None. Texte en clair plus un nombre quelconque de balises
 de nouvelle ligne HTML et de liens hypertexte
- Type de site : XenApp Web

PreLoginMessageTitle _<*Codedelangue*>

- Description : indique un titre localisé pour la page du message de pré-ouverture de session. *Codedelangue* est en, fr, de, es, ja ou tout autre code de langue pris en charge.
- Valeur : None. Texte en clair plus un nombre quelconque de balises
 de nouvelle ligne HTML et de liens hypertexte
- Type de site : XenApp Web

RADERequestValidation

- Indique si la validation du texte doit être comparée aux requêtes entrantes provenant de Citrix Offline Plug-in.
- Valeur :
- Type de site : XenApp Web et XenApp Services

RADESessionURL

- Description : indique l'adresse URL d'une page de session RADE. Si ce paramètre est réglé sur auto, l'adresse URL est générée automatiquement.

- Valeur : Auto. Adresse URL valide
- Type de site : XenApp Web et XenApp Services

RadiusRequestTimeout

- Description : indique la valeur du délai d'attente à appliquer lorsqu'une réponse est attendue du serveur RADIUS de la session.
- Valeur : durée en minutes (30)
- Type de site : XenApp Web

RadiusServers

- Description : indique les serveurs RADIUS à utiliser, et le cas échéant, les ports d'écoute. Les serveurs peuvent être spécifiés à l'aide d'adresses IP ou de noms ; le serveur et le port de chaque élément sont séparés par le signe deux-points. Si le port n'est pas spécifié, le port RADIUS par défaut (1812) est utilisé. Vous pouvez configurer un maximum de 512 serveurs.
- Valeur : *Server* [:*Port*] [,…]
- Type de site : XenApp Web

ReconnectAtLogin

- Description : indique si le contrôle de l'espace de travail doit se reconnecter aux ressources lorsque les utilisateurs ouvrent des sessions et, si tel est le cas, s'il doit se reconnecter à toutes les ressources ou uniquement aux ressources déconnectées.
- Valeur : Disconnected AndActive | Disconnected | None
- Type de site : XenApp Web

ReconnectButton

- Description : indique si le contrôle de l'espace de travail doit se reconnecter aux applications lorsque les utilisateurs cliquent sur le bouton Reconnecter et, si tel est le cas, s'ils doivent se reconnecter à toutes les ressources ou uniquement aux ressources déconnectées.
- Valeur : Disconnected AndActive | Disconnected | None
- Type de site : XenApp Web

RecoveryFarm<*n*>

- Description : indique toutes les informations relatives à une batterie de récupération d'urgence. Vous pouvez configurer un maximum de 512 batteries.
- Valeur : Citrix XML Service address [,Citrix XML Service address,] [,Name:<*Nom*>] [,XMLPort:<*Port*>] [,Transport:<HTTP | HTTPS | SSL>] [,SSLRelayPort:<*Port*>] [,BypassDuration:<*DuréeenMinutes* (60)>] [,LoadBalance:<on | off>] [,TicketTime ToLive:<*DuréeenSecondes* (200)>] [,RADETicket TimeToLive:<*DuréeenSecondes* (200)>]

- Type de site : XenApp Web, XenApp Services et XenDesktop

RequestedHighColorIcons

- Description : indique si les icônes de couleurs 32 bits sont requises par le service XML Citrix, et si tel est le cas, dresse la liste des tailles d'icônes en pixels. Si ce paramètre est réglé sur None, seules les icônes 32 x 32 4 bits sont requises. Le réglage par défaut varie en fonction du type de site et de sa configuration.
- Valeur : 16, 32, 48 | None

  Pour les sites XenApp Services, le paramètre par défaut requiert toutes les icônes. Pour les sites XenApp Web, seules les tailles 16 x 16 et 32 x 32 sont requises par défaut.
- Type de site : XenApp Web et XenApp Services

RequestICAClientSecureChannel

- Description : indique les paramètres TLS.
- Valeur : Detect-Any Ciphers, TLS- GovCiphers, SSL-AnyCiphers
- Type de site : XenApp Web et XenApp Services

RequireLaunchReference

- Description : indique si l'utilisation de références de lancement est imposée. Des références de lancement sont requises pour l'authentification unique à XenApp VM hosted apps. Si la compatibilité avec XenApp 4.0, avec Feature Pack 1, pour UNIX est requise, ce paramètre doit être réglé sur Off.
- Valeur : On | Off
- Type de site : XenApp Web et XenApp Services

RestrictDomains

- Description : indique si le paramètre LoginDomains est utilisé afin de limiter l'accès de l'utilisateur.
- Valeur : Off | On
- Type de site : XenApp Web et XenApp Services

SearchContextList

- Description : indique des noms de contexte pour l'authentification NDS.
- Valeur : None. Liste de noms de contexte séparés par des virgules
- Type de site : XenApp Web et XenApp Services

ServerAddressMap

- Description : indique les paires d'adresses normales/traduites pour la configuration du pare-feu du côté serveur. L'adresse normale identifie le serveur et l'adresse traduite est

renvoyée au client Citrix.

- Valeur : NormalAddress, Translated Address, …
- Type de site : XenApp Web et XenApp Services

ServerCommunicationAttempts

- Description : indique le nombre de tentatives d'envoi de la requête au service XML Citrix avant que le service ne soit considéré comme défaillant.
- Valeur : entier supérieur à 0 (2)
- Type de site : XenApp Web et XenApp Services

ShowClientInstallCaption

- Description : indique comment et quand les légendes d'installation apparaissent. Si Auto est sélectionné, les légendes d'installation s'affichent si aucun client n'est installé ou qu'un client Citrix plus performant est disponible. Si ce paramètre est réglé sur Silencieux, les légendes d'installation sont affichées uniquement si les utilisateurs ne disposent pas de client. Le comportement de l'écran Ouvrir une session diffère légèrement dans le sens où les légendes sont affichées uniquement pour les clients pour ressources en mode connecté, et ce, à condition qu'aucun client ne soit détecté. C'est pourquoi il n'existe aucune différence entre les réglages Auto et Quiet de l'écran Ouvrir une session.
- Valeur : Auto | Quiet | Off
- Type de site : XenApp Web

ShowDesktopViewer

- Description : indique si la fenêtre Citrix Desktop Viewer et la barre d'outils sont activées par défaut lorsque les utilisateurs accèdent à leurs bureaux.
- Valeur : Off | On
- Type de site : XenApp Web et XenApp Services

ShowHints

- Description : indique si les conseils apparaissent ou non sur l'écran Applications.
- Valeur : On | Off
- Type de site : XenApp Web

ShowPasswordExpiryWarning

- Description : indique les conditions qui déclenchent l'affichage d'un avertissement d'expiration du mot de passe.
- Valeur : Never | Windows Policy | Custom
- Type de site : XenApp Web

ShowRefresh

- Description : indique si le bouton Actualiser est mis à la disposition des utilisateurs sur l'écran Applications.
- Valeur : Off | On
- Type de site : XenApp Web

ShowSearch

- Description : indique si la fonction de recherche est mise à la disposition des utilisateurs sur l'écran Applications.
- Valeur : On | Off
- Type de site : XenApp Web

SpecialFolderRedirection

- Description : indique si la fonctionnalité de redirection de dossiers spéciaux est activée. Si ce paramètre est réglé sur On, les ressources utilisent les dossiers \Documents et \Bureau se trouvant sur les ordinateurs locaux des utilisateurs. Si Off est sélectionné, les dossiers \Documents et \Bureau disponibles dans les applications seront ceux du serveur.
- Valeur : Off | On
- Type de site : XenApp Web et XenApp Services

SuppressDuplicateResources

- Description : indique si l'existence de ressources, dont les noms et emplacements de dossiers sont identiques, publiées sur différentes batteries est masquée aux yeux des utilisateurs.
- Valeur : Off | On
- Type de site : XenApp Web et XenApp Services

Timeout

- Description : indique la valeur du délai d'attente à appliquer lors des communications avec le service XML Citrix.
- Valeur : durée en minutes (60)
- Type de site : XenApp Web et XenApp Services

TransparentKeyPassthrough

- Description : indique le mode d'authentification unique par combinaisons de touches Windows.
- Valeur : FullScreen Only | Local | Remote

- Type de site : XenApp Web et XenApp Services

TwoFactorPasswordIntegration

- Description : indique si l'intégration du mot de passe doit être activée ou pas à l'aide de RSA SecurID 6.0.
- Valeur : Off | On
- Type de site : XenApp Web

TwoFactorUseFullyQualifiedUserNames

- Description : indique si les noms d'utilisateur entièrement qualifiés doivent être transmis ou non au serveur d'authentification lors de l'authentification à deux facteurs.
- Valeur : Off | On
- Type de site : XenApp Web

UpgradeClientsAtLogin

- Description : indique si le processus de détection et de déploiement de client s'exécute automatiquement lorsque des utilisateurs ouvrent une session et qu'une version plus récente du client natif approprié ou de Citrix Offline Plug-in est disponible. Ce paramètre ne s'applique que lorsque le paramètre EnableWizardAutoMode est réglé sur On.
- Valeur : Off | On
- Type de site : XenApp Web

UPNSuffixes

- Description : indique les suffixes permettant de restreindre l'authentification UPN pour l'authentification explicite.
- Valeur : liste de suffixes UPN
- Type de site : XenApp Web et XenApp Services

UserInterfaceBranding

- Description : indique si le site cible les utilisateurs qui accèdent à des applications ou ceux qui accèdent à des bureaux. Si vous réglez ce paramètre sur Desktops, les fonctionnalités du site sont modifiées afin d'améliorer l'expérience des utilisateurs de XenDesktop. Citrix conseille d'utiliser ce paramètre pour tout déploiement comprenant XenDesktop.
- Valeur : Applications | Desktops
- Type de site : XenApp Web

UserInterfaceLayout

- Description : indique s'il faut utiliser ou non l'interface utilisateur compacte.

- Valeur : Auto | Normal | Compact
- Type de site : XenApp Web

UserInterfaceMode

- Description : indique l'apparence de l'écran Ouvrir une session. Si ce paramètre est défini sur Simple, seuls les champs d'ouverture de session pour la méthode d'authentification sélectionnée sont affichés. Si Advanced est sélectionné, la barre de navigation s'affiche, ce qui permet d'accéder aux écrans Préférences et Messages de pré-ouverture de session.
- Valeur : Simple | Advanced
- Type de site : XenApp Web

ViewStyles

- Description : indique les styles d'affichage mis à la disposition des utilisateurs sur l'écran Applications de la version avancée de l'interface utilisateur.
- Valeur : Details | Groups | Icons | List | Tree
- Type de site : XenApp Web

WebSessionTimeout

- Description : indique la valeur du délai d'expiration des sessions inactives du navigateur Web.
- Valeur : durée en minutes (20)
- Type de site : XenApp Web

Welcome Message _<*Codedelangue*>

- Description : indique le texte de message de bienvenue traduit qui s'affiche dans la zone de bienvenue de l'écran Ouvrir une session. *Codedelangue* est en, fr, de, es, ja ou tout autre code de langue pris en charge.
- Valeur : None. Texte en clair plus un nombre quelconque de balises
 de nouvelle ligne HTML et de liens hypertexte
- Type de site : XenApp Web

WIAuthenticationMethods

- Description : indique les méthodes d'authentification autorisées pour les sites non intégrés à Access Gateway. Il s'agit d'une liste délimitée par des virgules, qui peut contenir n'importe lesquelles des valeurs spécifiées dans un ordre quelconque.
- Valeur : combinaison de : Explicit, Anonymous, Certificate SingleSignOn, Certificate, SingleSignOn
- Type de site : XenApp Web, XenApp Services et Desktop Appliance Connector

Contenu du fichier Config.xml

Mise à jour : 2014-12-02

Le fichier config.xml contient des paramètres répartis en catégories différentes. Vous pouvez modifier les paramètres des catégories suivantes :

- FolderDisplay. Indique l'emplacement d'affichage des icônes des ressources : dans le menu Démarrer, sur le bureau Windows ou dans la zone de notification. Un paramètre supplémentaire permet de spécifier un dossier particulier dans le menu Démarrer. Ces paramètres correspondent aux contrôles de la page Affichage d'application de la boîte de dialogue Options de Citrix Online Plug-in.
- DesktopIntegration. Indique s'il faut ajouter des raccourcis vers le menu Démarrer, le bureau ou les zones de notification.
- ConfigurationFile. Indique une adresse URL différente pour le fichier config.xml à utiliser ultérieurement pour le plug-in. Cela permet de déplacer plus facilement les utilisateurs vers un serveur Interface Web différent.
- Request. Indique l'emplacement où le plug-in doit demander les données relatives aux ressources et la fréquence d'actualisation des informations.
- Failover. Indique une liste d'adresses URL de serveur de sauvegarde à contacter si le serveur principal est indisponible.
- Ouverture de session. Indique la méthode d'ouverture de session à utiliser.
- ChangePassword. Indique sous quelles conditions les utilisateurs de Citrix Online Plug-in sont autorisés à changer leur mot de passe et le chemin par lequel la requête est routée.
- UserInterface. Indique si certains groupes d'options présentées aux utilisateurs dans le cadre de l'interface utilisateur de Citrix Online Plug-in doivent être affichés ou masqués.
- ReconnectOptions. Indique si les utilisateurs ont accès à la fonctionnalité de contrôle de l'espace de travail.
- FileCleanup. Indique si les raccourcis sont supprimés ou non lorsque des utilisateurs ferment une session Citrix Online Plug-in.
- ICA_Options. Indique les options d'affichage et de son pour les connexions aux plug-ins. Ceci correspond aux paramètres sur la page Options de session de la boîte de dialogue Options de Citrix Online Plug-in.
- AppAccess. Indique les types de ressources auxquelles les utilisateurs ont accès.

Pour plus d'informations sur l'utilisation du fichier config.xml, veuillez consulter la rubrique Online Plug-in pour Windows.

Considérations sur Citrix Online Plug-in

Les réglages de paramètres WebInterface.conf spécifiques affectent la validation des requêtes de Citrix Online Plug-in. Citrix vous conseille d'utiliser, dans WebInterface.conf, des paramètres en accord avec les paramètres du fichier config.xml pour Citrix Online Plug-in.

Réglages dans le fichier WebInterface.conf

Les paramètres de WebInterface.conf répertoriés dans le tableau suivant doivent être en accord avec ceux du fichier config.xml. Le tableau explique les paramètres affectant les réglages de Citrix Online Plug-in et les réglages recommandés.

Paramètre	Réglage recommandé
LoginType	Si NDS est sélectionné, l'authentification Novell doit également être activée dans config.xml.
NDSTreeName	DefaultTree dans la section Logon de config.xml doit contenir le même paramètre.
PNAChangePasswordMethod	Method dans la section ChangePassword de config.xml doit contenir le même paramètre.
WIAuthenticationMethods	Utilisez la même méthode d'authentification que celle configurée dans le fichier WebInterface.conf. L'authentification échouera si cette méthode n'est pas la même que dans le fichier config.xml.

Pour configurer l'Interface Web lors de l'utilisation de Citrix Online Plug-in

1. À l'aide d'un éditeur de texte, ouvrez le fichier WebInterface.conf.
2. Situez les paramètres suivants :
   - LoginType
   - NDSTreeName
   - PNAChangePasswordMethod
   - WIAuthenticationMethods
3. Modifiez les réglages pour ces paramètres comme décrit dans la section Contenu du fichier Config.xml.
4. Redémarrez le serveur Interface Web pour appliquer les modifications.

Pour plus d'informations sur les paramètres du fichier WebInterface.conf, veuillez consulter la section Paramètres WebInterface.conf.

Réglages dans le fichier bootstrap.conf

Les réglages présents dans le fichier bootstrap.conf sont répertoriés dans le tableau suivant.

Paramètre	Description	Valeurs	Types de sites
ConfigurationLocation	Indique le fichier à partir duquel le site Interface Web doit obtenir sa configuration. Il peut s'agir d'un fichier local, ou pour les sites hébergés sur IIS, d'un fichier distant partagé sur le réseau.	Chemin d'accès absolu à WebInterface.conf	XenApp Web XenApp Services
DefaultLocale	Indique la langue par défaut à utiliser si un navigateur Web demande une langue non prise en charge.	en | de | es | fr | ja | tout autre identificateur de langue prise en charge	XenApp Web XenApp Services
SiteName	Indique le nom du site qui apparaît dans la console de gestion de l'Interface Web Citrix Le réglage par défaut utilise l'adresse URL du site.	Chaîne valide	XenApp Web XenApp Services

Pour configurer la prise en charge de XenApp 4.0, avec Feature Pack 1, pour UNIX

Dans cet exemple, vous voulez configurer un site pour qu'il soit compatible avec XenApp 4.0, avec Feature Pack 1, pour UNIX. Les nouveaux sites Interface Web ne sont pas initialement compatibles avec ce produit ; vous devez les configurer manuellement.

1. À l'aide d'un éditeur de texte, ouvrez le fichier WebInterface.conf et localisez les lignes suivantes :

   OverrideIcaClientname=Off

   RequireLaunchReference=On

2. Modifiez les paramètres comme indiqué ci-dessous :

   OverrideIcaClientname=On

   RequireLaunchReference=Off

   Remarque : lorsque le paramètre RequireLaunchReference est défini sur Off, l'authentification unique est désactivée auprès de XenApp VM hosted apps. Les utilisateurs de ce site doivent entrer leurs informations d'identification chaque fois qu'ils accèdent à VM hosted app.

Pour configurer l'itinérance des utilisateurs

Dans cet exemple, vous voulez associer des groupes d'utilisateurs de votre filiale américaine à des batteries spécifiques de façon à ce que, lorsqu'ils se déplacent au Japon, ils puissent ouvrir une session sur un serveur Interface Web local et recevoir automatiquement des ressources en langue anglaise à partir d'une batterie située aux États-Unis.

Une batterie existante dont le service XML Citrix est exécuté sur le serveur « waltz » est déjà définie en tant que Farm1 dans le fichier de configuration. Cette dernière est disponible à tous les utilisateurs qui ouvrent une session au serveur Interface Web situé aux États-Unis. Les groupes d'utilisateurs « SalesMgrs » et « SalesTeam » se trouvent dans le domaine « ussales.mycompany.com » et le groupe d'utilisateurs « Accounts » dans le domaine « finance.mycompany.com ». Vous voulez associer les utilisateurs de ces groupes à des batteries dont les noms de serveurs exécutant le service XML Citrix sont « foxtrot » et « tango ». Procédez comme suit :

1. À l'aide d'un éditeur de texte, ouvrez le fichier WebInterface.conf sur le serveur Interface Web situé aux États-Unis et recherchez la ligne suivante :

   Farm1=waltz,Name:Farm1,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBalance

   Important : lorsque l'itinérance des utilisateurs est activée, la première batterie définie dans le fichier de configuration doit exécuter XenApp 6.0 ou version supérieure, ou XenDesktop 4.0 ou version supérieure. Si la première batterie répertoriée exécute une version antérieure, les utilisateurs n'auront accès à aucune ressource.

2. Définissez les nouvelles batteries en ajoutant les lignes suivantes :

   Farm2=foxtrot,Name:Farm2,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBalan
   Farm3=tango,Name:Farm3,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBalance

3. Attribuez des groupes d'utilisateurs aux nouvelles batteries en ajoutant les lignes suivantes :

   Farm2Groups=ussales.mycompany.com\SalesMgrs,ussales.mycompany.com\SalesTeam,finance.mycompar
   Farm3Groups=ussales.mycompany.com\SalesMgrs

   L'ajout du paramètre **Farm<*n*>Groups** à une batterie définie à l'aide de **Farm<*n*>** permet d'activer la fonctionnalité d'itinérance des utilisateurs. Cela signifie que vous devez attribuer des groupes d'utilisateurs à toutes vos batteries, et pas seulement aux batteries utilisées par les utilisateurs itinérants.

4. Veillez à ce que les utilisateurs puissent continuer à accéder à la batterie existante en ajoutant la ligne suivante :

   Farm1Groups=mycompany.com\DomainUsers

Pour permettre aux utilisateurs itinérants d'accéder à leurs ressources lorsqu'ils sont au Japon, vous devez répliquer ces paramètres dans le fichier de configuration du serveur Interface Web du Japon.

5. À l'aide d'un éditeur de texte, ouvrez le fichier WebInterface.conf sur le serveur Interface Web situé au Japon et insérez les lignes mentionnées aux étapes 2 et 3. Veillez également à attribuer des groupes d'utilisateurs à toutes les batteries japonaises existantes de façon à ce que les utilisateurs locaux puissent continuer à y accéder.

Messages de journal et ID d'événements

Mise à jour : 2014-11-25

L'Interface Web consigne des ID d'événements pour tous les types de sites et de plates-formes. Sur les systèmes d'exploitation Windows, les ID d'événements peuvent être visualisés à l'aide de l'Observateur d'événements et être utilisés par Citrix EdgeSight ou des outils de reporting et de suivi tiers. Sur les serveurs d'application Java, l'ID d'événement fait partie du message de journal consigné sur le fichier journal du serveur Web.

Le tableau suivant dresse la liste des ID d'événements de l'Interface Web et des messages qui leur sont associés. Il contient également une description succincte des problèmes ainsi que des suggestions permettant de les résoudre.

ID d'événement	Message	Severity	Description
10001	Une erreur d'analyse de configuration s'est produite : <*description de l'erreur*>.	Error	Un problème s'est produit avec le fichier de configuration du site. Vérifiez la présence d'erreurs dans le fichier WebInterface.conf.
10002	Une erreur de chargement de configuration s'est produite.	Error	Le fichier de configuration du site est manquant ou inaccessible. Vérifiez que le fichier WebInterface.conf n'a pas été supprimé et que les permissions appropriées ont été configurées pour autoriser la lecture de ce fichier.
10003	Impossible de récupérer la configuration de Citrix Online Plug-in.	Error	Le fichier de configuration de Online Plug-in est manquant ou inaccessible. Vérifiez que le fichier config.xml n'a pas été supprimé et que les permissions appropriées ont été configurées pour autoriser la lecture de ce fichier.
10004	Rechargement des données de configuration réussi.	Informations	Les modifications récentes apportées au fichier de configuration du site (WebInterface.conf) ou au fichier de configuration de Online Plug-in (config.xml) ont été validées et acceptées.
10005	La ou les clés suivantes sont dupliquées dans le fichier de configuration : <*nom de la clé*>.	Avertissement	Paramètre en double dans le fichier de configuration du site. Corrigez l'erreur dans WebInterface.conf.

10006	Point d'authentification inconnu : <*point d'authentification*>.	Error	Une valeur incorrecte a été spécifiée pour le paramètre Point d'authentification dans le fichier de configuration du site. Corrigez l'erreur dans WebInterface.conf.
10007	L'ouverture de session anonyme n'est pas autorisée lorsque les utilisateurs itinérants sont activés.	Error	XenDesktop ne prend pas en charge les utilisateurs anonymes. Pour utiliser la fonctionnalité d'itinérance des utilisateurs avec XenDesktop, désactivez l'authentification anonyme.
10008	La configuration n'est pas valide : l'authentification NDS n'est pas prise en charge dans cette version de l'Interface Web.	Error	Reconfigurez la méthode d'authentification pour le site et sélectionnez un nom UPN ou une authentification de domaine Microsoft.
10009	La configuration n'est pas valide : ni l'authentification par carte à puce, ni l'authentification unique ne sont prises en charge dans cette version de l'Interface Web.	Error	Cette erreur s'affiche lorsque vous utilisez la version UNIX/JSP de l'Interface Web, et que vous utilisez les points d'authentification Interface Web avec l'authentification unique, une carte à puce, ou l'authentification par carte à puce, ou les points d'authentification Access Gateway avec une carte à puce ou l'authentification avec carte à puce.
10010	Un problème est survenu lors de la configuration de l'authentification à deux facteurs.	Error	Vérifiez que l'authentification Aladdin SafeWord pour Citrix, RSA SecurID ou le serveur RADIUS ont été correctement configurés.
10011	Aucune méthode d'authentification n'est actuellement disponible.	Error	Vérifiez que le site est configuré correctement et qu'au moins une méthode d'authentification valide a été sélectionnée.
10101	Le service de transition de protocole n'est pas configuré correctement. Assurez-vous qu'un tokenManager est défini dans le fichier web.config, et qu'il définit un ou plusieurs services de jeton.	Error	Vérifiez que le fichier web.config du site XenApp Web spécifie au moins un émetteur de jeton. Ce dernier doit disposer de références de certificats qui peuvent être utilisées pour sécuriser la relation d'approbation avec l'authentification unique avec carte à puce à partir du service Access Gateway.

10201	La configuration n'est pas valide : la signature de fichier ICA n'est pas prise en charge dans cette version de l'Interface Web.	Error	Vous devez exécuter l'Interface Web 5.4 ou une version ultérieure pour utiliser la fonctionnalité de signature de fichier ICA.
10202	La signature de fichier ICA ne peut pas être utilisée lorsque la prise en charge des clients antérieurs est activée.	Error	Pour activer la signature de fichier ICA, le site doit être configuré pour utiliser le client natif et EnableLegacyIcaClientSupport doit être défini sur Off dans le fichier Webinterface.conf.
10203	La signature de fichier ICA ne peut pas être utilisée avec les applications en mode déconnecté.	Error	Vérifiez que le site est configuré pour afficher les applications en mode connecté ou en mode double.
10204	Vous devez autoriser les utilisateurs à choisir le client natif pour pouvoir utiliser la signature de fichier ICA.	Informations	Pour activer la signature de fichier ICA, le site doit être configuré pour utiliser le client natif.
10205	Une erreur s'est produite lors de la tentative de signature d'un fichier ICA : <*message d'erreur*>	Error	Reportez-vous aux informations contenues dans le message d'erreur pour obtenir des informations détaillées sur les actions à réaliser.
10206	Une erreur s'est produite lors de la tentative de signature d'un fichier ICA : <>. Redémarrez le serveur Web pour vous assurer que le service ICA File Signing est activé.	Error	Redémarrez le serveur Web et utilisez la console de gestion de l'Interface Web Citrix pour vous assurer que la signature de fichier ICA a été activée.
11001	Une URL de redirection non valide a été transmise au processus de détection et de téléchargement de client.	Error	L'adresse URL de redirection spécifie la page Web vers laquelle les utilisateurs sont redirigés lorsqu'ils exécutent le processus de détection et de déploiement de client. Cette erreur indique que l'adresse URL de redirection a été modifiée dans le code pour ce site.

11002	Le processus de détection et de déploiement de client n'a déployé aucun des clients activés. Vérifiez que le navigateur, le système d'exploitation et la méthode d'accès de l'utilisateur sont compatibles avec les clients activés. En outre, ces derniers doivent être disponibles dans le dossier \Clients du site XenApp Web.	Error	L'utilisateur n'a pas pu obtenir de client à partir du site. Vérifiez qu'un client approprié pour la machine de l'utilisateur, le système d'exploitation, le navigateur et la méthode d'accès est disponible sur le serveur et activé sur le site.
11003	Le processus de détection et de déploiement de client n'est pas pris en charge par le système d'exploitation de l'utilisateur.	Error	L'utilisateur n'a pas pu obtenir de client à partir du site car le processus de détection et de déploiement de client n'a pas réussi à identifier le système d'exploitation de la machine utilisateur.
11004	La requête provenant du navigateur exécuté sur la machine utilisateur <*adresse IP*> ne peut pas être traitée car l'en-tête HTTP de l'agent utilisateur, qui fournit les informations sur la plate-forme, est absent.	Error	L'utilisateur n'a pas pu accéder au site car la requête envoyée par le navigateur ne contenait pas d'en-tête HTTP de l'agent utilisateur, qui identifie le navigateur et la plate-forme de l'utilisateur. Vérifiez votre environnement réseau pour vous assurer que les en-têtes d'agent utilisateur ne sont pas supprimés des requêtes utilisateur.
12001	L'Interface Web a supprimé <*nombre*> tentatives de journalisation des messages avec cet ID de journal unique. Le taux de signalisation a diminué et l'Interface Web recommencera à journaliser ces messages.	Informations	Utilisez la tâche Journalisation des diagnostics sous Maintenance du site dans la console de gestion de l'Interface Web Citrix pour empêcher la journalisation répétée des événements en double et configurer le nombre maximal d'événements dupliqués journalisés ainsi que la fréquence de leur journalisation.

12002	Des tentatives supplémentaires de journalisation des messages avec cet ID de journal unique seront supprimées jusqu'à ce que le taux de signalisation diminue.	Informations	Utilisez la tâche Journalisation des diagnostics sous Maintenance du site dans la console de gestion de l'Interface Web Citrix pour empêcher la journalisation répétée des événements en double et configurer le nombre maximal d'événements dupliqués journalisés ainsi que la fréquence de leur journalisation.
12003	Le fichier d'ID d'événement n'a pas pu être chargé. Vérifiez dans le fichier <*nom du fichier*> que le chemin d'accès au fichier d'ID d'événement est correct.	Avertissement	Le fichier d'ID d'événement est manquant ou inaccessible. Vérifiez que le chemin d'accès indiqué dans le fichier web.config (pour les sites hébergés sur IIS) ou le fichier web.xml (pour les sites hébergés sur des serveurs d'application Java) est correct. Vérifiez que le fichier WebInterfaceEventIds.txt n'a pas été supprimé et que les permissions appropriées ont été configurées pour autoriser la lecture de ce fichier.
12004	La clé du message <*nom de la clé*> ne correspond pas à un ID d'événement valide. Vérifiez que le fichier d'ID d'événement a une entrée valide pour <*nom de la clé*>. L'ID d'événement doit être un nombre entier compris entre 1 et 65535.	Avertissement	L'ID d'événement spécifié est introuvable dans le fichier d'ID d'événement. Vérifiez que cet ID d'événement n'a pas été supprimé du fichier WebInterfaceEventIds.txt.
13001	Une connexion SSL n'a pas pu être établie avec le service Web sur <*adresse du serveur*> : <*port*>. Le message suivant a été généré par la plate-forme sous-jacente <*description de l'erreur*>.	Error	Une erreur SSL s'est produite ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez que l'Interface Web est configurée correctement pour s'intégrer avec Access Gateway ou Password Manager via SSL.

13002	Impossible d'obtenir d'identificateurs de sécurité pour au moins un groupe. Vérifiez que le service XML Citrix est accessible, qu'il prend en charge l'itinérance utilisateur et que les groupes dans le fichier de configuration sont corrects.	Error	Un problème s'est produit avec un ou plusieurs groupes d'utilisateurs configurés pour la fonctionnalité d'itinérance utilisateur. Vérifiez que tous les serveurs de la batterie exécutent une version de XenApp ou XenDesktop qui prend en charge cette fonctionnalité. Par ailleurs, vérifiez que les noms des groupes spécifiés sont valides et que la communication est possible avec les serveurs Citrix.
14001	Un problème s'est produit avec RSA SecurID ACE/Agent. Vérifiez que ACE/Agent est correctement installé et que le chemin d'accès au fichier aceclnt.dll a été ajouté à la variable d'environnement PATH.	Error	Pour utiliser l'authentification SecurID avec l'Interface Web pour Microsoft Internet Information Services, l'Interface Web doit être installée après le logiciel RSA Authentication Agent for Web for Internet Information Services.
14002	Un problème s'est produit avec RSA SecurID ACE/Agent. Vérifiez que la version correcte a été installée.	Error	Vérifiez qu'une version prise en charge du logiciel RSA Authentication Agent for Web for Internet Information Services est installée sur le serveur Web.
14003	Un problème s'est produit avec l'Agent Aladdin SafeWord. Vérifiez qu'il est correctement installé.	Error	Vérifiez que l'agent SafeWord pour l'Interface Web est installé sur le serveur Web. L'Interface Web doit être installée après l'Agent SafeWord.
14004	Impossible de mettre à jour le mot de passe mis en cache par RSA SecurID ACE/Agent. Vérifiez que les versions de RSA SecurID ACE/Agent et de ACE/Server sont compatibles et que ACE/Agent et ACE/Server sont configurés pour utiliser l'outil d'intégration des mots de passe Windows.	Error	Vérifiez que les versions de RSA Authentication Manager et RSA Authentication Agent for Web for Internet Information Services sont compatibles. Vérifiez également que les paramètres système de la base de données RSA Authentication Manager sont configurés pour activer l'intégration de mot de passe Windows au niveau du système.

14005	Impossible d'obtenir le mot de passe mis en cache par RSA SecurID ACE/Agent. Vérifiez que les versions de RSA SecurID ACE/Agent et de ACE/Server sont compatibles et que ACE/Agent et ACE/Server sont configurés pour utiliser l'outil d'intégration des mots de passe Windows.	Error	Vérifiez que les versions de RSA Authentication Manager et RSA Authentication Agent for Web for Internet Information Services sont compatibles. Vérifiez également que les paramètres système de la base de données RSA Authentication Manager sont configurés pour activer l'intégration de mot de passe Windows au niveau du système.
14006	Un problème s'est produit avec l'authentifieur SafeWord lors de l'authentification d'un utilisateur.	Error	Un problème s'est produit avec le serveur SafeWord. Pour de plus amples informations, consultez les fichiers journaux sur le serveur SafeWord.
14007	Un problème s'est produit avec RSA SecurID ACE/Agent. Vérifiez que le pool d'applications Interface Web est configuré pour les applications 32 bits ou 64 bits appropriées pour la version de ACE/Agent installée.	Error	Vérifiez la configuration requise pour l'application pour la version de ACE/Agent que vous exécutez.
15001	Un problème s'est produit lors de la lecture de la version du client à partir de <*chemin d'accès au fichier*>. Les utilisateurs ne seront pas invités à mettre leur client à niveau.	Error	Vérifiez que les permissions adéquates ont été configurées pour autoriser la lecture du fichier d'installation du client spécifié.
15002	Un problème s'est produit lors de la lecture du fichier de pack de langue <*nom du fichier*>. Vérifiez que le fichier est accessible et qu'il utilise le format approprié.	Error	Vérifiez que le fichier spécifié n'a pas été supprimé et que les permissions appropriées ont été configurées pour autoriser la lecture de ce fichier.
15003	Impossible d'accéder au répertoire <*nom du répertoire*>. Les clients contenus dans ce répertoire ne peuvent être pas mis à la disposition des utilisateurs. Assurez-vous que le compte Service réseau dispose des permissions d'accès au répertoire appropriées et redémarrez le serveur Web.	Error	Vérifiez que le répertoire spécifié n'a pas été supprimé et que les permissions appropriées ont été configurées pour autoriser la lecture de ce répertoire.

15004	Un problème s'est produit lors de la lecture du fichier de pack de langue <*nom du fichier*>. Une déclaration de version est manquante dans le fichier, le pack de langue ne sera donc pas utilisé.	Error	Le fichier de pack de langue ne contient aucun numéro de version. Corrigez l'erreur dans le fichier spécifié.
15005	Un problème s'est produit lors de la lecture du fichier de pack de langue <*nom du fichier*>. La version du pack de langue est <*numéro de version*>, or elle n'est pas compatible avec cette version de l'Interface Web.	Error	Les versions de l'Interface Web et du fichier de pack de langue ne correspondent pas. Les packs de langue sont spécifiques à la version de l'Interface Web avec laquelle ils ont été fournis, ils ne peuvent donc pas être utilisés avec des versions antérieures ou ultérieures. Mettez le fichier spécifié à niveau ou rétablissez la version précédente, le cas échéant
15006	Aucun pack de langue correspondant aux paramètres régionaux par défaut <*paramètres régionaux d'installation*> n'a été trouvé. Le pack de langue <*nom du fichier*> a été trouvé et sera utilisé par défaut.	Avertissement	Lorsque l'Interface Web ne parvient pas à trouver de pack de langue correspondant aux paramètres régionaux choisis durant l'installation, l'Interface Web utilise le premier pack de langue compatible qu'elle trouve.
16001	Impossible de lire le fichier secret RADIUS <*chemin d'accès au fichier*>.	Error	Le fichier secret RADIUS est manquant ou inaccessible. Vérifiez que le chemin d'accès indiqué dans le fichier web.config (pour les sites hébergés sur IIS) ou le fichier web.xml (pour les sites hébergés sur des serveurs d'application Java) est correct. Vérifiez que le fichier secret RADIUS n'a pas été supprimé et que les permissions appropriées ont été configurées pour autoriser la lecture de ce fichier.
16002	Le fichier secret RADIUS <*chemin d'accès au fichier*> est vide.	Error	Le protocole RADIUS nécessite l'utilisation d'un secret partagé, contenant des données connues uniquement du client RADIUS (l'Interface Web) et du serveur RADIUS auprès duquel il s'authentifie. Le fichier secret RADIUS peut contenir n'importe quelle chaîne, mais il ne doit pas être vide.

16003	Un problème s'est produit avec l'authentifieur RADIUS lors de l'authentification d'un utilisateur.	Error	Un problème s'est produit avec le serveur RADIUS. Pour de plus amples informations, consultez les fichiers journaux sur le serveur RADIUS.
16004	Les valeurs RADIUS_NAS_IDENTIFIER et/ou RADIUS_IP_ADDRESS doivent figurer dans le fichier de configuration du site Web. Les valeurs RADIUS_NAS_IDENTIFIER doivent contenir au moins 3 caractères. RADIUS_IP_ADDRESS doit être une adresse IP valide.	Error	Le protocole RADIUS nécessite que les requêtes d'accès aux serveurs RADIUS comprennent l'adresse IP ou un autre type d'identificateur pour le client RADIUS (l'Interface Web). Vérifiez que le fichier web.config (pour les sites hébergés sur IIS) ou le fichier web.xml (pour les sites hébergés sur des serveurs d'application Java) contient un identificateur NAS RADIUS ou une adresse IP valide.
17001	Échec de recherche du contexte sur le serveur <*adresse du serveur*> : <*exception*>. Ce serveur a été temporairement supprimé de la liste des serveurs actifs.	Error	Un problème s'est produit avec le serveur NDS spécifié. Ce serveur sera ignoré tant que le problème ne sera pas résolu. Pour de plus amples informations, consultez les fichiers journaux sur le serveur NDS.
17002	Tous les serveurs NDS ayant échoué, aucune recherche du contexte ne sera possible. Essayez d'ouvrir une session avec un nom d'utilisateur complet, tel que *.nomd'utilisat eur.masociété.com*.	Error	Aucun des serveurs NDS n'a pu être contacté. Essayez d'entrer des informations d'identification au format *.nom d'utilisateur.masc* Pour de plus amples informations, consultez les fichiers journaux sur les serveurs NDS.
18001	Une erreur de communication s'est produite lors de la tentative de contact avec le service d'authentification d'Advanced Access Control sur <*adresse URL*>. Vérifiez que le service d'authentification est en cours d'exécution. Le message suivant a été généré par la plate-forme sous-jacente <*description de l'erreur*>.	Error	Un problème s'est produit lors de la communication avec le service d'authentification d'Access Gateway ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le boîtier Access Gateway.

18002	Une erreur de communication s'est produite lors de la tentative de fermeture de la session à l'aide du service d'authentification d'Access Gateway sur <*URL*>. Vérifiez que le service d'authentification est en cours d'exécution. Le message suivant a été généré par la plate-forme sous-jacente <*description de l'erreur*>.	Error	Un problème s'est produit lors de la communication avec le service d'authentification d'Access Gateway ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le boîtier Access Gateway.
18003	Le service d'authentification d'Access Gateway n'a pas réussi à authentifier l'utilisateur. Le message signalé par le service était <*description de l'erreur*> [code d'état : <*numéro de code*>].	Error	Un problème s'est produit avec le service d'authentification d'Access Gateway ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le boîtier Access Gateway.
18004	Le service d'authentification d'Access Gateway n'a pas réussi à fermer la session. Le message signalé par le service était <*description de l'erreur*> [code d'état : <*numéro de code*>].	Error	Un problème s'est produit avec le service d'authentification d'Access Gateway ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le boîtier Access Gateway.
18005	Adresse URL fournie dans la configuration du site du service d'authentification d'Access Gateway non valide : <*adresse URL*>.	Error	Une adresse URL non valide a été spécifiée pour le paramètre AGEWebServiceURL dans le fichier de configuration du site. Corrigez l'erreur dans WebInterface.conf.
18006	L'utilisateur <*nom de l'utilisateurs*> n'a pas pu se connecter au site : <*nom du site*>. Redémarrez le serveur Web pour vous assurer que l'authentification unique avec carte à puce est activée à partir du service Access Gateway.	Error	L'utilisateur de la carte à puce n'a pas réussi à ouvrir de session au site intégré Access Gateway. Redémarrez le serveur Web et vérifiez que l'authentification unique avec carte à puce est exécutée à partir du service Access Gateway.

18007	Cette version d'Access Gateway ne prend pas en charge les demandes de modification de mot de passe de l'Interface Web. Pour permettre aux utilisateurs de modifier leur mot de passe, vous devez mettre à niveau vers une version d'Access Gateway prenant en charge cette fonctionnalité.	Error	Cette erreur s'affiche si la fonctionnalité de modification de mot de passe est activée sur votre site et que la version d'Access Gateway que vous utilisez ne prend pas en charge cette fonctionnalité. Désactivez la fonctionnalité de modification de mot de passe ou mettez à niveau vers une version d'Access Gateway qui prend en charge cette fonctionnalité.
19001	Une erreur s'est produite lors de la déconnexion des ressources d'un utilisateur. Le contrôle de l'espace de travail n'est pas activé, l'utilisateur est anonyme ou une erreur s'est produite lors de la récupération des informations d'identification de l'utilisateur ou du nom du client.	Error	Un problème s'est produit avec le contrôle de l'espace de travail. Vérifiez que le contrôle de l'espace de travail est activé pour le site et que l'utilisateur a ouvert une session à l'aide d'une méthode d'authentification autre que l'authentification anonyme.
19002	Une erreur s'est produite lors de la reconnexion des ressources d'un utilisateur. Le contrôle de l'espace de travail n'est pas activé, l'utilisateur est anonyme ou une erreur s'est produite lors de la récupération des informations d'identification de l'utilisateur ou du nom du client.	Error	Un problème s'est produit avec le contrôle de l'espace de travail. Vérifiez que le contrôle de l'espace de travail est activé pour le site et que l'utilisateur a ouvert une session à l'aide d'une méthode d'authentification autre que l'authentification anonyme.
20001	Une erreur de communication s'est produite lors de la tentative de contact avec le service Password Manager sur <*adresse URL*>. Vérifiez que le service est en cours d'exécution. Le message suivant a été généré par la plate-forme sous-jacente <*description de l'erreur*>.	Error	Un problème s'est produit lors de la communication avec le service Password Manager ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Password Manager.
20002	Adresse URL fournie dans la configuration du site du service Password Manager non valide : <*adresse URL*>.	Error	Une adresse URL non valide a été spécifiée pour le paramètre AccountSelfServiceUrl dans le fichier de configuration du site. Corrigez l'erreur dans WebInterface.conf.

21001	Une erreur critique de serveur s'est produite.	Error	Une exception Java s'est produite dans l'un des scripts exécuté sur la page Web. Essayez de recharger la page. Vous pouvez également utiliser la tâche Réparer le site sous Maintenance du site dans la console de gestion de l'Interface Web Citrix pour réinstaller les scripts pour le site.
21002	Erreur critique de serveur : <*description de l'erreur .NET*>.	Error	Une exception .NET s'est produite dans l'un des scripts exécuté sur la page Web. Essayez de recharger la page. Vous pouvez également utiliser la tâche Réparer le site sous Maintenance du site dans la console de gestion de l'Interface Web Citrix pour réinstaller les scripts pour le site.
21003	En raison d'une erreur, le file watcher n'a pas pu être créé sur le chemin <*répertoire de configuration du site*>.	Error	Vérifiez que le chemin d'accès au dossier de configuration du site est correct et que les permissions appropriées ont été configurées pour autoriser la lecture de ce répertoire. Vous pouvez également essayer de redémarrer IIS afin de mettre à jour le site avec les dernières modifications apportées à la configuration.
21004	Un utilisateur n'a pas pu accéder au site car le nom de domaine complet du serveur Web contient des traits de soulignement (_). Renommez le serveur Web et/ou le domaine pour supprimer les traits de soulignement. Si cela n'est pas possible, configurez une adresse secondaire pour le serveur Web ne contenant pas de traits de soulignement ou demandez aux utilisateurs d'accéder au site à l'aide de l'adresse IP du serveur Web.	Error	L'accès aux sites dont le nom contient des caractères non reconnus, tels que des traits de soulignement, est impossible. Vérifiez que le nom du serveur Web ne contient pas de trait de soulignement, et utilisez la la console de gestion de l'Interface Web Citrix pour changer le nom du serveur, le cas échéant.

21005	Le contrôle ActiveX Citrix Online Plug-in avec l'ID de classe <*numéro d'ID*> n'a pas pu être démarré. Vérifiez que l'ID de classe correct est spécifié dans le fichier de configuration du site.	Error	Vérifiez que l'ID de classe ActiveX correspond au numéro d'ID dans le fichier Webinterface.conf.
21006	Le contrôle ActiveX Citrix Online Plug-in avec l'ID de classe <*numéro d'ID*> n'a pas pu être démarré. Vérifiez que l'ID de classe correct est spécifié dans le fichier de configuration du site.	Error	Vérifiez que l'ID de classe ActiveX correspond au numéro d'ID dans le fichier Webinterface.conf.
22001	Les fichiers du client pour Java sont introuvables sur le serveur. Vérifiez que ces fichiers sont disponibles dans le dossier \Clients du site XenApp Web.	Error	Les packs du client pour Java sont manquants ou inaccessibles. Vérifiez que les fichiers n'ont pas été supprimés et que les permissions appropriées ont été configurées pour autoriser la lecture de ces fichiers.
23001	Une erreur ICA s'est produite lors de la tentative d'accès au bureau pour l'utilisateur <*nom d'utilisateur*>.	Error	Citrix Online Plug-in n'a pas pu accéder au bureau de l'utilisateur. Vérifiez que le bureau est exécuté et qu'il est accessible.
23002	Internet Explorer n'a pas pu fournir l'accès au bureau pour l'utilisateur <*nom d'utilisateur*>. Vérifiez que Citrix Desktop Appliance Lock est installé sur la machine de l'utilisateur et que Desktop Appliance Connector a été ajouté à une zone de sécurité Windows appropriée dans Internet Explorer.	Error	L'utilisateur du boîtier de bureau n'a pas pu accéder à un bureau en mode plein écran. Vérifiez que Citrix Online Plug-in a été installé et configuré correctement sur la machine utilisateur.
23003	L'accès à <*nombre*> bureau(x) a été accordé à l'utilisateur <*nom d'utilisateur*>. Les utilisateurs qui accèdent à un bureau en mode plein écran uniquement par le biais d'un Desktop Appliance Connector ne doivent être autorisés à accéder qu'à un seul bureau.	Avertissement	Plus d'un bureau a été mis à la disposition de l'utilisateur du boîtier de bureau. L'utilisateur peut accéder à un bureau. Toutefois, étant donné qu'il n'existe aucun moyen de sélectionner le bureau requis, il est possible que l'utilisateur ne soit pas connecté au même bureau la prochaine fois qu'il ouvre une session. Configurez le Desktop Appliance Connector de façon à ce que l'utilisateur soit uniquement autorisé à accéder à un seul bureau.

23004	La méthode d'authentification spécifiée n'est pas valide. Vous devez spécifier soit « Explicit », soit « Certificat », mais vous ne pouvez pas spécifier les deux méthodes.	Error	Les valeurs Explicit et Certificate ont été spécifiées pour le paramètre WIAuthenticationMethods dans le fichier de configuration du site. Vous ne pouvez pas activer l'authentification explicite et l'authentification avec carte à puce pour le même Desktop Appliance Connector. Corrigez l'erreur dans WebInterface.conf.
23005	La configuration de l'authentification SSO de la carte à puce intégrée n'est pas valide. La méthode d'authentification doit comprendre « Certificate ».	Error	La valeur Certificate doit être spécifiée pour le paramètre WIAuthenticationMethods dans le fichier de configuration du site pour Desktop Appliance Connector. Corrigez l'erreur dans WebInterface.conf.
23006	Les méthodes d'authentification spécifiées ne sont pas valides. La combinaison de méthodes d'authentification n'est pas prise en charge.	Error	Les méthodes d'authentification Desktop Appliance Connector spécifiées dans le paramètre WIAuthenticationMethods du fichier de configuration de site ne peuvent pas être utilisées conjointement. Corrigez l'erreur dans WebInterface.conf.
24001	Une tentative d'ouverture de session a été effectuée par un utilisateur non authentifié. Vérifiez que des comptes miroir ont été créés pour tous les utilisateurs appropriés du système. Si le problème persiste, essayez de réparer le site à l'aide de la console de gestion de l'Interface Web Citrix.	Error	Un problème s'est produit avec le site intégré ADFS. L'utilisateur n'a pas été authentifié. Vérifiez qu'un compte fantôme a été créé pour l'utilisateur dans le domaine du partenaire de ressource. Vous pouvez également utiliser la tâche Réparer le site sous Maintenance du site dans la console de gestion de l'Interface Web Citrix pour réinstaller le site.

24002	Une tentative d'ouverture de session a été effectuée par un utilisateur non authentifié. Si le problème persiste, essayez de réparer le site à l'aide de la console de gestion de l'Interface Web Citrix.	Error	Un problème s'est produit avec le site XenApp Web ou XenApp Services. L'utilisateur n'a pas été authentifié. Vérifiez qu'un compte utilisateur a été créé pour l'utilisateur dans le domaine. Vous pouvez également utiliser la tâche Réparer le site sous Maintenance du site dans la console de gestion de l'Interface Web Citrix pour réinstaller le site.
30001	Une erreur s'est produite lors de la tentative de lecture d'informations à partir des serveurs Citrix : <*nom de la batterie*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30002	Une erreur s'est produite lors de la tentative d'écriture d'informations sur les serveurs Citrix : <*nom de la batterie*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30003	Une erreur s'est produite lors de la tentative de connexion au serveur <*adresse du serveur*> sur le port <*port*>. Vérifiez que le service XML Citrix est en cours d'exécution et qu'il utilise le port approprié. Si le service XML est configuré pour partager les ports avec Microsoft Internet Information Services (IIS), vérifiez qu'IIS est en cours d'exécution. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez si le service XML a été configuré pour partager les ports TCP/IP avec IIS et, si c'est le cas, vérifiez qu'IIS est en cours d'exécution. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.

30004	Impossible de résoudre le nom du serveur <*adresse du serveur*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30005	Les serveurs Citrix ont envoyé une syntaxe HTTP incorrecte. Vérifiez que la version actuelle de l'Interface Web est compatible avec les serveurs utilisés. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez que la batterie de serveurs exécute XenDesktop ou Presentation Server 4.5 ou une version supérieure. Citrix recommande d'exécuter le même produit et la même version sur tous les serveurs de la batterie. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30006	Les serveurs Citrix ont envoyé une réponse incorrecte ou inattendue. Vérifiez que la version actuelle de l'Interface Web est compatible avec les serveurs utilisés. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez que la batterie de serveurs exécute XenDesktop ou Presentation Server 4.5 ou une version supérieure. Citrix recommande d'exécuter le même produit et la même version sur tous les serveurs de la batterie. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30008	Les serveurs Citrix ont fermé la connexion inopinément. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.

30009	Les serveurs Citrix ont envoyé des en-têtes HTTP indiquant qu'une erreur s'était produite : <*détails*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30010	Les serveurs Citrix ne peuvent traiter votre requête pour le moment. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30011	Une erreur s'est produite sur les serveurs Citrix lors de la tentative d'exécution de la requête : <*détails*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30012	Les serveurs Citrix ont signalé une erreur de disparité de version. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30013	Les serveurs Citrix ont reçu une requête incorrecte. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30014	Une erreur s'est produite sur les serveurs Citrix lors de l'analyse syntaxique de la requête. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.

30015	Le service XML Citrix à l'adresse <*chemin d'accès au fichier*> n'est pas capable de traiter de requêtes.	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30016	L'objet du service XML Citrix est introuvable : <*détails*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30017	La méthode du service XML Citrix n'est pas prise en charge : <*détails*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30018	La réponse du service XML Citrix n'est pas acceptable : <*détails*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30019	La longueur de requête du service XML Citrix est requise : <*détails*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30020	La requête du service XML Citrix est trop courte : <*détails*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.

30021	La requête du service XML Citrix a dépassé la taille maximale : <*détails*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30022	Le service XML Citrix ou les serveurs Citrix sont peut-être indisponibles ou temporairement surchargés : <*détails*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30023	Impossible de traiter le document XML envoyé par les serveurs Citrix. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30024	Il n'a pas été possible de traiter le document XML envoyé par les serveurs Citrix car il contient du code XML invalide. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30025	Une erreur s'est produite lors de la tentative de lecture d'informations à partir des serveurs Citrix : <*nom de la batterie*>. Il est possible que cette erreur résulte de la tentative de communication avec quelque chose d'autre que le Relais SSL. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour sécuriser les connexions à la batterie de serveurs grâce au cryptage SSL/TLS, vous devez utiliser le Relais SSL pour configurer la prise en charge sur chaque serveur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.

30026	Une erreur s'est produite lors de la tentative de connexion au Relais SSL : <*adresse du serveur*> : <*port*>. Vérifiez qu'un Relais SSL est en cours d'exécution, et qu'il est en écoute sur un port valide. Le nom contenu dans le certificat de serveur que le Relais SSL est configuré pour contacter doit correspondre exactement au nom du serveur sur lequel la connexion a été tentée. Ce message a été signalé depuis le service XML Citrix à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez que le Relais SSL est en cours d'exécution et à l'écoute sur le port approprié (généralement le port 443) et que le certificat de serveur du Relais SSL contient le nom de domaine complet du serveur (en respectant la casse) sur lequel la connexion a été tentée. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30027	La fonctionnalité de ticket n'est peut-être pas prise en charge par au moins un serveur Citrix. Pour utiliser cette fonctionnalité, vous devez mettre à niveau les serveurs exécutant le service XML ou désactiver la fonctionnalité de ticket. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez que tous les serveurs de la batterie exécutent XenDesktop ou MetaFrame XP 1.0 ou version supérieure. Citrix recommande d'exécuter le même produit et la même version sur tous les serveurs de la batterie. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30028	Impossible de résoudre le nom du Relais SSL <*adresse du serveur*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30029	Aucune connexion SSL n'a pu être établie : <*description de l'erreur SSL*>. Ce message a été signalé depuis le service XML Citrix à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.

30030	Aucune connexion de Relais SSL n'a pu être établie : <*description de l'erreur SSL*>. Ce message a été signalé depuis le service XML Citrix à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30031	Le service XML Citrix à l'adresse <*chemin d'accès au fichier*> ne prend pas en charge la capacité <*nom de la fonctionnalité*>.	Error	Vérifiez que tous les serveurs de la batterie exécutent une version de XenApp ou XenDesktop qui prend en charge la fonctionnalité spécifiée. Pour plus d'informations, veuillez consulter la section Configuration logicielle minimum.
30101	L'opération de modification du mot de passe était altérée.	Error	Pour des raisons de sécurité, l'utilisateur n'a pas pu changer le mot de passe Windows. Pour de plus amples informations, consultez les fichiers journaux sur les serveurs Citrix et/ou le contrôleur de domaine.
30102	Les serveurs Citrix ont signalé une erreur non spécifiée depuis le service XML à l'adresse <*chemin d'accès au fichier*>.	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30103	Les serveurs Citrix ont signalé que l'adresse secondaire est introuvable. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30104	Une erreur s'est produite lors de la connexion au serveur Citrix pour accéder à la ressource. Vérifiez que le serveur est en cours d'exécution et que le réseau fonctionne. Cette erreur a été signalée pour un service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez la présence de problèmes au niveau de la batterie et du réseau. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.

30105	Les serveurs Citrix ne font pas confiance au serveur. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Vérifiez qu'une relation d'approbation existe entre le serveur de l'Interface Web et le service XML Citrix. Pour plus d'informations, veuillez consulter la section Utilisation du contrôle de l'espace de travail avec des méthodes d'authentification intégrée pour les sites XenApp Web.
30106	Les serveurs Citrix ne possèdent pas de licence pour prendre en charge l'opération requise. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez que le serveur de licences Citrix est en cours d'exécution et accessible. Citrix recommande de mettre à jour le serveur de licences vers la version la plus récente pour garantir la compatibilité avec les derniers produits. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix et/ou le serveur de licences.
30107	Les serveurs Citrix ont signalé qu'ils sont trop occupés pour avoir accès à la ressource sélectionnée. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez que la batterie de serveurs n'est pas surchargée. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30108	La fonctionnalité de ticket est désactivée sur le serveur Citrix. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez que tous les serveurs de la batterie utilisent le même port pour communiquer avec le service XML. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.

30109	Le service XML à l'adresse <*chemin d'accès au fichier*> a signalé une erreur d'enregistrement. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30110	Une erreur de type <*type d'erreur*> avec un ID d'erreur <*ID d'erreur*> a été signalée par le service XML Citrix à l'adresse <*chemin d'accès au fichier*>. En fonction du serveur exécutant le service XML, de plus amples informations sont disponibles dans le journal des événements du serveur. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30111	Les serveurs Citrix ne prennent pas en charge le type d'adresse spécifiée. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30112	Aucune ressource n'a été trouvée pour l'utilisateur <*nom de l'utilisateur*> durant l'accès au groupe de bureaux <*nom du groupe*>. Ce message a été signalé depuis le service XML Citrix à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez que l'utilisateur a été affecté au groupe de bureaux spécifié et que des groupes non utilisés sont disponibles dans le groupe. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30113	Une requête émanant du serveur Citrix demandant la préparation d'une connexion a été rejetée lors du traitement de l'initialisation du groupe de bureaux <*nom du groupe*> pour l'utilisateur <*nom de l'utilisateur*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.

30114	Les serveurs Citrix n'ont pas reçu l'autorisation de récupérer des identificateurs de sécurité pour l'utilisateur. Accordez des permissions de lecture du service XML à l'attribut Token-Groups-Global-And-Universal dans Active Directory ou désactivez l'énumération d'identificateur de sécurité dans le service XML. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Si le service XML est configuré pour énumérer les identificateurs de sécurité des utilisateurs, vérifiez que les permissions appropriées ont été accordées dans Active Directory. Pour de plus amples informations, consultez l'article CTX117489 ainsi que les fichiers journaux sur le serveur Citrix.
30115	Les serveurs Citrix n'ont pas réussi à récupérer les identificateurs de sécurité pour l'utilisateur. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez l'article CTX117489 ainsi que les fichiers journaux sur le serveur Citrix.
30116	Connexion au bureau en mode de maintenance impossible pour l'utilisateur <*nom d'utilisateur*> lors de l'initialisation du groupe de bureaux <*nom du groupe*>. Ce message a été signalé depuis le service XML Citrix à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez que le bureau de l'utilisateur n'a pas été placé en mode de maintenance. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30117	Les serveurs Citrix ne prennent pas en charge l'opération de redémarrage du bureau. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez que la batterie de serveurs exécute XenDesktop 3.0 ou une version supérieure. Citrix recommande d'exécuter le même produit et la même version sur tous les serveurs de la batterie. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.

30118	Le délai d'inactivité des serveurs Citrix a expiré lors de l'attente de l'extinction d'une machine dans le groupe de bureaux <*nom du groupe*> pour l'utilisateur <*nom de l'utilisateur*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30119	Impossible d'éteindre une machine en mode de maintenance dans le groupe de bureaux <*nom du groupe*> pour l'utilisateur <*nom de l'utilisateur*>. Ce message a été signalé depuis le service XML Citrix à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez que le bureau de l'utilisateur n'a pas été placé en mode de maintenance. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30120	Impossible de trouver l'utilisateur <*nom de l'utilisateur*>. Ce message a été signalé depuis le service XML Citrix à l'adresse <*chemin d'accès au fichier*>. <*description de l'erreur*>	Error	Un problème s'est produit avec le service XML Citrix ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30201	Adresse Secure Ticket Authority non valide : <*adresse URL*>. <*description de l'erreur*>	Error	Une adresse URL non valide a été spécifiée pour le paramètre **CSG_STA_ URL<*n*>** dans le fichier de configuration du site. Corrigez l'erreur dans WebInterface.conf.
30202	La Secure Ticket Authority <*adresse URL*> ne prend pas en charge les requêtes de la version 4. Toutes les communications Secure Ticket Authority retourneront maintenant à la version 1. Les nouvelles connexions effectuées via Secure Gateway n'utiliseront pas la fiabilité de session.	Error	La version de Secure Gateway utilisée ne prend pas en charge la fonctionnalité de redondance de la Secure Ticket Authority. Par conséquent, cette fonctionnalité a été désactivée.

30203	La Secure Ticket Authority <*adresse URL*> a retourné un ticket dont l'autorité ou le type était inattendu(e) : <*type d'erreur*>, <*ID d'erreur*>, <*description de l'erreur SSL*>, <*détails*>. <*description de l'erreur*>	Error	Un problème s'est produit avec la Secure Ticket Authority ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30204	La Secure Ticket Authority spécifiée n'a pas pu être contactée et a été temporairement supprimée de la liste des services actifs.	Error	Un problème s'est produit avec la Secure Ticket Authority. Ce service sera ignoré tant que le problème ne sera pas résolu. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
30205	Aucune des Secure Ticket Authorities configurées n'a répondu à cette transaction XML.	Error	Aucune des Secure Ticket Authorities n'a pu être contactée. Essayez de redémarrer le serveur Web. Pour de plus amples informations, consultez les fichiers journaux sur les serveurs Citrix.
30301	La réponse HTTP indique que la connexion sous-jacente a été fermée.	Error	Vérifiez que la batterie de serveurs exécute XenDesktop ou Presentation Server 4.5 ou une version supérieure. Citrix recommande d'exécuter le même produit et la même version sur tous les serveurs de la batterie.
30401	Un socket a été détruit par la couche de transaction.	Error	Vérifiez la présence d'applications endommagées dans le magasin de données de la batterie. Pour obtenir davantage d'informations, veuillez consulter la section CTX114769.
31001	Le service XML Citrix spécifié n'a pas pu être contacté et a été temporairement supprimé de la liste des services actifs.	Error	Un problème s'est produit avec le service XML Citrix. Ce serveur sera ignoré tant que le problème ne sera pas résolu. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.

31002	La transaction de ce service XML a échoué, mais le service XML n'a pas été supprimé de la liste des services actifs.	Error	Bien que le service XML Citrix soit accessible, la requête ou instruction n'a pas abouti. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
31003	Aucun des services XML Citrix configurés pour la batterie <*nom de la batterie*> n'a répondu à cette transaction de service XML.	Error	Aucun des hôtes du service XML Citrix pour la batterie spécifiée n'a pu être contacté. Essayez de redémarrer le serveur Web. Pour de plus amples informations, consultez les fichiers journaux sur les serveurs Citrix.
31004	L'erreur de protocole XML <*ID d'erreur*> n'a pas pu être convertie en une erreur d'état d'accès.	Error	Vérifiez que l'utilisateur dispose de droits d'ouverture de session Active Directory aux serveurs Citrix.
31005	<*nombre*> ressources sur <*nombre*> ont été ignorées car elles ne sont pas valides.	Error	Le service XML Citrix n'a pas pu énumérer toutes les ressources disponibles. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
31006	L'ouverture de session de l'utilisateur <*nom de l'utilisateur*> a été rejetée car ce dernier ne détient pas de licence.	Error	L'utilisateur n'a pas pu ouvrir de session car aucune licence Citrix ou licence d’accès client aux services Bureau à distance Microsoft n'était disponible. Vérifiez que le serveur de licences Citrix est en cours d'exécution et accessible. Citrix recommande de mettre à jour le serveur de licences vers la version la plus récente pour garantir la compatibilité avec les derniers produits. Pour de plus amples informations, consultez les fichiers journaux sur les serveurs Citrix et/ou le serveur de licences.

31007	Les licences des serveurs Citrix ne leur permettent pas de prendre en charge le contrôle de l'espace de travail. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>.	Error	Vérifiez que les licences Citrix activent une édition de produit qui comprend la fonctionnalité de contrôle de l'espace de travail. Vérifiez également que le serveur de licences Citrix est en cours d'exécution et accessible. Citrix recommande de mettre à jour le serveur de licences vers la version la plus récente pour garantir la compatibilité avec les derniers produits. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix et/ou le serveur de licences.
31008	Les licences des serveurs Citrix ne leur permettent pas de lancer la ressource <*nom de la ressource*>. Ce message a été signalé depuis le service XML à l'adresse <*chemin d'accès au fichier*>.	Error	Vérifiez que les licences Citrix activent une édition de produit qui comprend ce type de ressource. Vérifiez également que le serveur de licences Citrix est en cours d'exécution et accessible. Citrix recommande de mettre à jour le serveur de licences vers la version la plus récente pour garantir la compatibilité avec les derniers produits. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix et/ou le serveur de licences.
31009	Impossible d'obtenir les données de compte du ou des comptes suivants : <*liste des noms de compte*> vérifiez que le nom est correctement orthographié. Ce message a été signalé depuis le service XML Citrix à l'adresse <*chemin d'accès au fichier*>.	Error	Le service XML Citrix ne peut pas accéder aux comptes spécifiés. Vérifiez que les comptes n'ont pas été supprimés et que les permissions appropriées ont été configurées pour autoriser leur lecture par le service XML. Vérifiez également que les noms de comptes ont été correctement saisis. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.

31101	L'utilisateur <*nom de l'utilisateur*> possède une session serveur, <*ID de session*>, mais n'a pas accès à la ressource <*nom de la ressource*>, qui a créé la session. L'utilisateur ne peut donc pas accéder à cette session.	Error	Les autorisations d'accès de l'utilisateur ont été modifiées alors que sa session était toujours active. Réinitialisez la session. Veuillez noter que cette opération entraînera une perte des données pour l'utilisateur. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
31201	La batterie <*nom de la batterie*> a été configurée pour utiliser les tickets, mais aucune balise de ticket n'a été reçue. Vérifiez que la batterie prend en charge les tickets.	Error	Vérifiez que tous les serveurs dans la batterie spécifiée exécutent XenDesktop ou MetaFrame XP 1.0 ou version supérieure. Citrix recommande d'exécuter le même produit et la même version sur tous les serveurs de la batterie. Pour de plus amples informations, consultez les fichiers journaux sur les serveurs Citrix.
31202	Un utilisateur a tenté de lancer la ressource désactivée <*nom de la ressource*>.	Error	Vérifiez que la ressource spécifiée est activée sur le serveur sur laquelle elle est hébergée.
31203	La batterie <*nom de la batterie*> a été configurée pour utiliser les références de lancement, mais aucune référence de lancement n'a été reçue du service XML Citrix. Vérifiez que la batterie prend en charge les références de lancement ou désactivez les requêtes de référence de lancement.	Error	Pour utiliser les références de lancement, tous les serveurs dans la batterie spécifiée doivent exécuter XenDesktop ou Presentation Server 4.5 ou version supérieure. Citrix recommande d'exécuter le même produit et la même version sur tous les serveurs de la batterie. Si la batterie exécute XenApp 4.0, avec Feature Pack 1, pour UNIX ou Presentation Server 4.0 et versions antérieures, assurez-vous que le paramètre RequireLaunchReference est défini sur Off et que OverrideIcaClientname est défini sur On dans le fichier de configuration du site XenApp Web, WebInterface.conf.
31301	La configuration de la batterie <*nom de la batterie*> n'est pas valide.	Error	Un problème s'est produit avec la batterie de serveurs spécifiée. Pour de plus amples informations, consultez les fichiers journaux sur les serveurs Citrix.

32001	La configuration ne contient aucune information sur les serveurs Citrix.	Error	Aucune batterie n'a été spécifiée pour le paramètre **Farm<*n*>** dans le fichier de configuration du site XenApp Services. Corrigez l'erreur dans WebInterface.conf.
32002	Impossible d'analyser la configuration de chaîne du fournisseur.	Error	Un problème s'est produit avec le site XenApp Services. Vérifiez la présence d'erreurs dans les fichiers de configuration du site.
32003	<*cause de l'erreur*> L'erreur système suivante s'est produite : <*description de l'erreur*>	Error	Un problème s'est produit avec le site XenApp Services ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez la présence d'erreurs dans les fichiers de configuration du site.
33001	Citrix Streaming Service : le service XML Citrix spécifié n'a pas pu être contacté et a été temporairement supprimé de la liste des services actifs.	Error	Citrix Offline Plug-in a rencontré un problème avec le service XML Citrix. Ce service sera ignoré tant que le problème ne sera pas résolu. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
33002	Citrix Streaming Service : la transaction de ce service XML Citrix a échoué, mais le service XML n'a pas été supprimé de la liste des services actifs.	Error	Bien que Citrix Offline Plug-in puisse accéder au service XML Citrix, la requête ou instruction n'a pas abouti. Pour de plus amples informations, consultez les fichiers journaux sur le serveur Citrix.
33003	Citrix Streaming Service : aucun des services XML Citrix configurés pour la batterie <*nom de la batterie*> n'a répondu à cette transaction de service XML.	Error	Aucun des hôtes du service XML Citrix pour la batterie spécifiée n'a pu être contacté par Citrix Offline Plug-in. Essayez de redémarrer le serveur Web. Pour de plus amples informations, consultez les fichiers journaux sur les serveurs Citrix.
33004	Citrix Streaming Service : la configuration de la batterie <*nom de la batterie*> n'est pas valide.	Error	Citrix Offline Plug-in a rencontré un problème avec la batterie de serveurs spécifiée. Pour de plus amples informations, consultez les fichiers journaux sur les serveurs Citrix.

33005	Citrix Streaming Service : la configuration ne contient aucune information sur les serveurs Citrix.	Error	Aucune batterie n'a été spécifiée pour le paramètre **Farm<*n*>** dans le fichier de configuration du site. Corrigez l'erreur dans WebInterface.conf.
33006	Le fichier de configuration RadeValidationRules.conf n'a pas pu être chargé. Vérifiez que le fichier est disponible dans le dossier de configuration du site.	Error	Le fichier de configuration RadeValidationRules.conf est manquant ou inaccessible. Vérifiez que le fichier n'a pas été supprimé et que les permissions appropriées ont été configurées pour autoriser la lecture de ce fichier.
33007	Le fichier de configuration RadeValidationRules.conf ne peut pas être utilisé car il contient des règles non valides. Vérifiez que toutes les règles utilisent une syntaxe d'expression régulière valide.	Error	Un problème s'est produit avec le fichier de configuration RadeValidationRules.conf. Toutes les règles dans ce fichier doivent être rédigées à l'aide d'une syntaxe d'expression régulière. Vérifiez la présence d'erreurs dans le fichier. Vous pouvez également utiliser la tâche Réparer le site sous Maintenance du site dans la console de gestion de l'Interface Web Citrix pour réinstaller le site. Toutes les modifications que vous apportez au fichier seront annulées.
34001	La configuration ne contient aucune information sur les serveurs Citrix.	Error	Aucune batterie n'a été spécifiée pour le paramètre **Farm<*n*>** dans Desktop Appliance Connector ou le fichier de configuration du site XenApp Web. Corrigez l'erreur dans WebInterface.conf.
34002	Impossible d'analyser la configuration de chaîne du fournisseur.	Error	Un problème s'est produit avec Desktop Appliance Connector ou le site XenApp Web. Vérifiez la présence d'erreurs dans le fichier WebInterface.conf.
34003	<*cause de l'erreur*> L'erreur système suivante s'est produite : <*description de l'erreur*>	Error	Un problème s'est produit avec le site XenApp Services ; des informations détaillées sont disponibles à la fin du message d'erreur. Vérifiez la présence d'erreurs dans le fichier WebInterface.conf.

40001	Une erreur s’est produite lors de l’énumération des ressources d’un utilisateur. Un message XML non reconnu a été reçu d'une machine utilisateur.	Error	Citrix Online Plug-in a rencontré un problème lors de la connexion aux serveurs Citrix. Vérifiez que Citrix Online Plug-in est correctement configuré sur la machine de l'utilisateur.
40002	Une erreur s’est produite lors de l’énumération des ressources d’un utilisateur. Un message XML non reconnu a été reçu d'une machine utilisateur.	Error	Citrix Online Plug-in a rencontré un problème lors de la connexion aux serveurs Citrix. Vérifiez que Citrix Online Plug-in est correctement configuré sur la machine de l'utilisateur.
40003	Une erreur s'est produite lors de la reconnexion des ressources d'un utilisateur. Un message XML non reconnu a été reçu d'une machine utilisateur.	Error	Citrix Online Plug-in a rencontré un problème lors de la reconnexion aux serveurs Citrix. Vérifiez que Citrix Online Plug-in est correctement configuré sur la machine de l'utilisateur.
40004	<*adresse IP*> a requis le fichier de configuration <*nom du fichier*> de Citrix Online Plug-in, or ce dernier n'existe pas.	Error	Vérifiez sur la machine de l'utilisateur que l'adresse URL du fichier de configuration a été saisie correctement dans la boîte de dialogue Options pour Citrix Online Plug-in.
40005	Une erreur s'est produite lors du lancement de la ressource d'un utilisateur : <*description de l'erreur*>	Error	Citrix Online Plug-in a rencontré un problème ; des informations détaillées sont disponibles à la fin du message d'erreur. Pour de plus amples informations, consultez les fichiers journaux sur les serveurs Citrix.
40006	Une erreur s'est produite lors d'une opération de contrôle de bureau. Un message XML non reconnu a été reçu d'une machine utilisateur.	Error	Citrix Online Plug-in a rencontré un problème lors du redémarrage du bureau de l'utilisateur. Vérifiez que Citrix Online Plug-in est correctement configuré sur la machine de l'utilisateur.

Désactivation des messages d'erreur

Sur IIS, vous pouvez désactiver les messages d'erreur fournis avec l'Interface Web et afficher l'erreur qui s'est produite. Pour ce faire, modifiez le fichier web.config qui se trouve dans le répertoire racine du site. Remplacez la ligne suivante :

<customErrors mode="On" defaultRedirect="~/html/serverError.html">

de la façon suivante :

<customErrors mode="Off" defaultRedirect="~/html/serverError.html">

Vous pouvez également afficher vos propres messages d'erreur personnalisés. Pour ce faire, modifiez la ligne comme suit :

<customErrors mode="On" defaultRedirect="~/html/*CustomErrorPage*">

où *CustomErrorPage* est le nom du fichier de votre page d'erreur personnalisée.

Configuration de la prise en charge d'ADFS pour l'Interface Web

Mise à jour : 2014-11-24

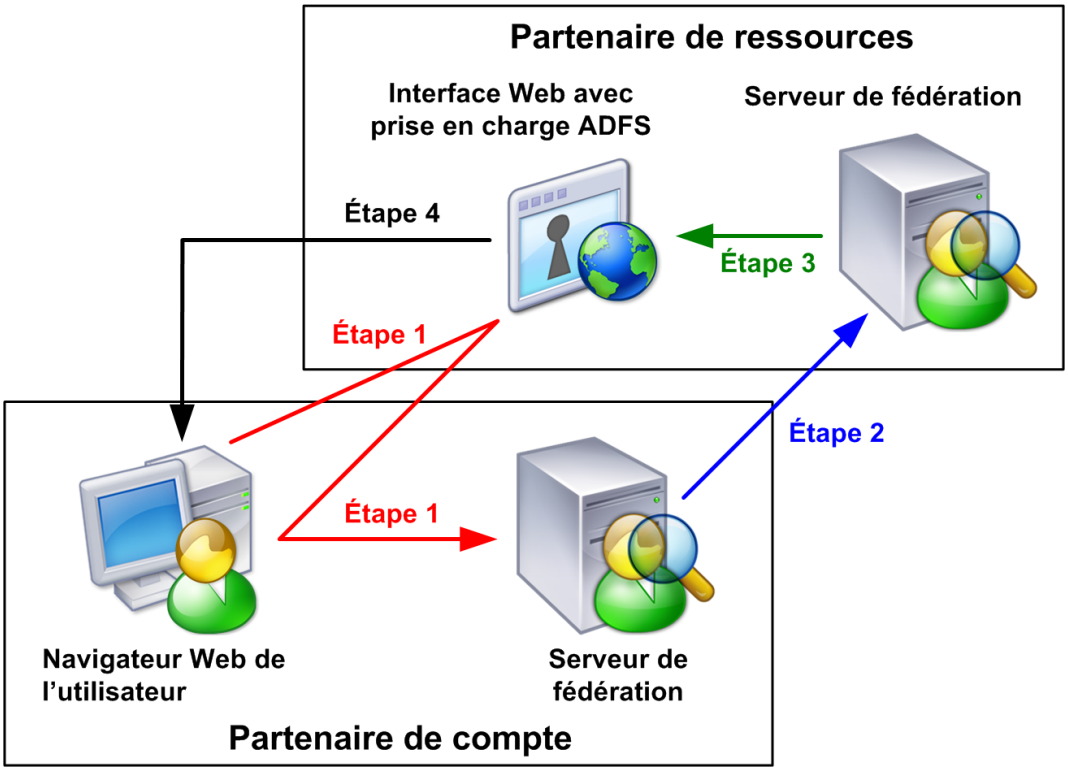
La prise en charge d'ADFS pour l'Interface Web permet au partenaire de ressource d'un déploiement ADFS d'utiliser XenApp. Les administrateurs peuvent créer des sites ADFS pour fournir aux utilisateurs un accès aux applications et au contenu sur le partenaire de ressource.

Important : ADFS exige que les communications entre le navigateur Web, le serveur Web et les serveurs de fédération soient sécurisées. Les utilisateurs de l'Interface Web doivent utiliser HTTPS/SSL pour accéder au site.

Fonctionnement des sites Active Directory Federation Services intégrés

Les événements suivants se produisent lorsqu'un utilisateur sur un partenaire de compte accède à une application sur un partenaire de ressource :

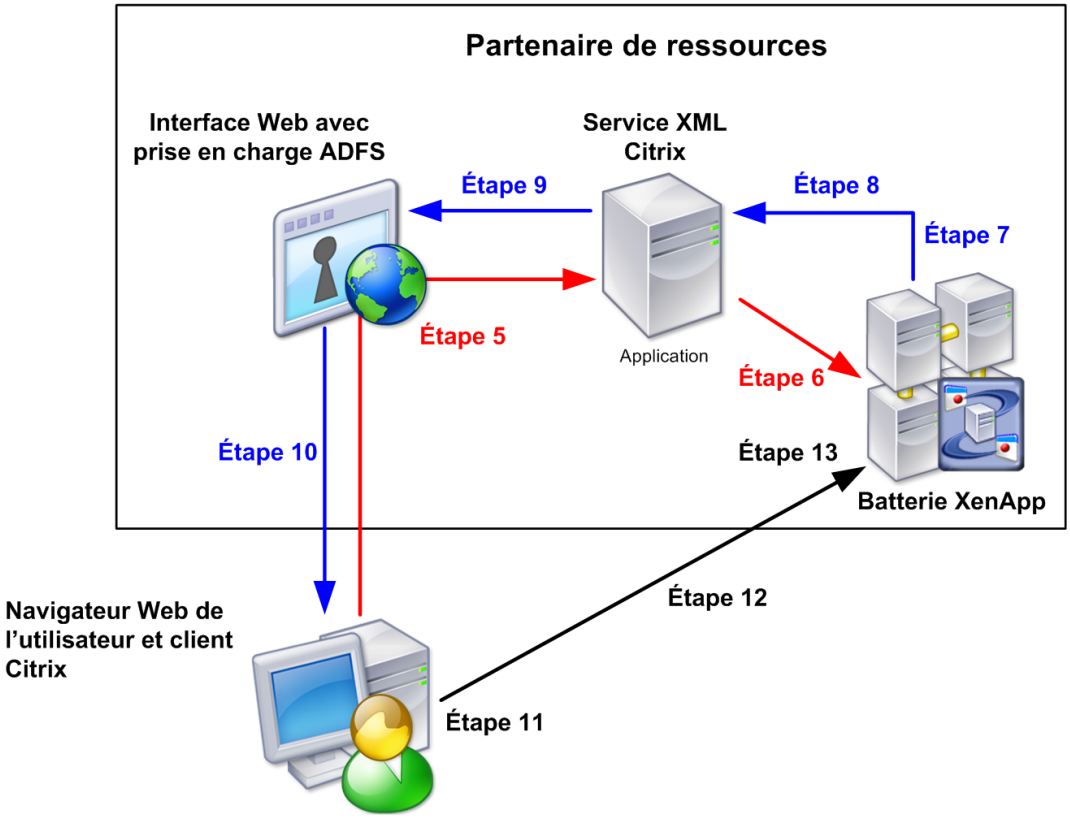
- **Étape 1.** Un utilisateur ouvrant la page d'accueil de l'Interface Web sur un partenaire de ressource est redirigé vers la page d'authentification du partenaire de compte.
- **Étape 2.** Le partenaire de compte authentifie l'utilisateur et renvoie un jeton de sécurité vers le partenaire de ressource.
- **Étape 3.** Sur le partenaire de ressource, ADFS valide le jeton de sécurité, le transforme en une identité Windows (représentant un compte fantôme) et redirige l'utilisateur vers l'écran Ouvrir une session de l'Interface Web.



Étape 4. L'Interface Web affiche la série d'applications mise à la disposition de l'utilisateur. Ce schéma illustre les différentes étapes qui se déroulent lorsque des utilisateurs appartenant au domaine du partenaire de compte ouvrent une session pour accéder à leur série d'applications.

- **Étape 5.** L'utilisateur accède à une application en cliquant sur un lien hypertexte sur la page. L'Interface Web contacte le Service XML Citrix pour demander l'accès.
- **Étape 6.** Le Service XML Citrix génère les données de l'interface SSPI (Security Support Provider Interface) et les transmet à un serveur XenApp.
- **Étape 7.** Le serveur utilise les données de l'interface SSPI pour authentifier l'utilisateur, puis stocke un jeton d'ouverture de session pour une authentification ultérieure.
- **Étape 8.** Le serveur génère un ticket de lancement pour représenter exclusivement le jeton d'ouverture de session stocké, puis transmet ce ticket au Service XML Citrix.
- **Étape 9.** Le Service XML Citrix renvoie le ticket de lancement vers l'Interface Web.
- **Étape 10.** L'Interface Web crée un fichier .ica contenant le ticket de lancement et le transmet au navigateur Web de l'utilisateur.
- **Étape 11.** La machine utilisateur ouvre le fichier .ica et tente d'établir une connexion ICA avec le serveur.
- **Étape 12.** Le client Citrix envoie le ticket de lancement au serveur XenApp.

.



Étape 13. Le serveur reçoit le ticket de lancement, le fait correspondre au jeton d'ouverture de session généré précédemment, puis utilise ce jeton d'ouverture de session pour connecter l'utilisateur à une session ICA sur le serveur. La session ICA s'exécute sous l'identité du compte fantôme.Ce schéma illustre les différentes étapes qui se déroulent lorsque des utilisateurs appartenant au domaine du partenaire de compte accèdent à des applications.

En fonction des paramètres configurés pour un site, lorsque des utilisateurs ferment une session, ils sont déconnectés de l'Interface Web ou de l'Interface Web et ADFS. S'ils ferment la session de l'Interface Web *et* ADFS, ils ferment la session de toutes les applications ADFS.

Avant la création de sites Active Directory Federation Services

Avant de créer un site ADFS, vous devez effectuer les opérations suivantes. Si vous oubliez l'une de ces opérations, vous ne pourrez peut-être pas créer de site.

- Synchronisez les horloges sur le serveur de fédération du partenaire de compte et le serveur de fédération du partenaire de ressource à cinq minutes près l'une par rapport à l'autre. Dans le cas contraire, les jetons de sécurité générés par le partenaire de compte peuvent ne pas être acceptés par le partenaire de ressource, les jetons pouvant apparaître comme ayant expiré. Afin d'éviter ce problème, les deux organisations doivent synchroniser leurs serveurs avec le même serveur de temps Internet. Pour plus d'informations, veuillez consulter la section Création des relations entre les domaines.

- Assurez-vous que le serveur Web et le serveur de fédération du partenaire de ressource ont accès aux Listes de Révocation de Certificats (LRC) de l'Autorité de Certification. ADFS pourrait échouer si les serveurs ne peuvent pas confirmer qu'un certificat n'est pas révoqué. Pour plus d'informations, veuillez consulter la section Création des relations entre les domaines.

- Veillez à ce que les serveurs de votre déploiement sont approuvés pour la délégation. Pour plus d'informations, veuillez consulter la section Configuration de la délégation pour les serveurs au sein de votre déploiement.

- Créez des comptes fantômes dans le domaine du partenaire de ressource pour chaque utilisateur externe pouvant s'authentifier sur l'Interface Web via ADFS. Pour plus d'informations, veuillez consulter la section Création de comptes fantômes.

- Installez XenApp, en vous assurant que le service XML Citrix est configuré pour partager son port avec IIS et qu'IIS est configuré pour prendre en charge HTTPS.

- Établissez une relation d'approbation entre le serveur Interface Web et tout autre serveur dans la batterie exécutant le service XML Citrix contacté par l'Interface Web. Pour plus d'informations, veuillez consulter la section Utilisation du contrôle de l'espace de travail avec des méthodes d'authentification intégrée pour les sites XenApp Web.

Important : cette section ne fournit aucune information sur l'installation d'ADFS. Avant d'essayer de créer un site ADFS, vérifiez qu'une installation ADFS est en état de fonctionnement, et qu'elle contient des utilisateurs de comptes externes capables d'accéder aux applications activées par ADFS dans un partenaire de ressource.

Configuration logicielle requise pour Active Directory Federation Services

Vous devez installer et configurer les logiciels suivants dans votre environnement :

- Windows Server 2008 ou Windows Server 2003 R2 pour les serveurs Web et les serveurs de fédération ; Dans le cas du serveur Web, seules les versions 32 bits de Windows Server 2008 et Windows Server 2003 R2 sont prises en charge.

- Active Directory Federation Services (ADFS) sur les partenaires de compte et de ressource. L'agent Web prenant en charge les revendications et l'agent Web basé sur les jetons Windows doivent tous deux être installés.

Création des relations entre les domaines

Le déploiement documenté ici est constitué de deux domaines (dans leurs propres forêts), l'une pour le partenaire de compte et l'autre pour le partenaire de ressource. Les composants requis ne doivent pas être sur des ordinateurs séparés.

Pour créer des relations entre les domaines

1. Assurez-vous d'être en possession des composants suivants. Le partenaire de compte requiert :

   - Contrôleur de domaines
   - Serveur de fédération
   - Machines utilisateur

   Le partenaire de ressource requiert :

   - Contrôleur de domaines
   - Serveur de fédération
   - Serveur Web
   - Un ou plusieurs serveurs pour une batterie XenApp

   Les serveurs de fédération doivent être hébergés sur des ordinateurs exécutant Windows Server 2008 ou Windows Server 2003 R2 et le rôle de serveur Active Directory Federation Services doit y être installé.

   Le serveur Web doit être hébergé sur un ordinateur exécutant une version 32 bits de Windows Server 2008 ou Windows Server 2003 R2. Les services de rôle Agent prenant en charge les revendications et Agent basé sur les jetons Windows doivent être installés, de même que *tous* les services de rôle pour le rôle de serveur Serveur Web (IIS).

2. Procurez-vous des certificats de serveur séparés pour le serveur Web et les deux serveurs de fédération.

   - Les certificats doivent être signés par une entité approuvée appelée Autorité de Certification.
   - Le certificat de serveur identifie un ordinateur spécifique ; vous devez donc connaître le nom de domaine complet (FQDN) de chaque serveur, par exemple, « xenappserver1.mydomain.com ».
   - Installez le certificat du serveur Web dans Microsoft Internet Information Services (IIS) afin d'activer le site Web IIS par défaut pour le trafic SSL.
   - Installez les certificats de serveur de fédération à l'aide du composant logiciel enfichable MMC (Microsoft Management Console) Certificates. Pour plus d'informations, veuillez consulter le guide *Step-by-Step Guide to the Microsoft Management Console* à l'adresse http://technet.microsoft.com/.

3. Afin de vous assurer que le serveur de fédération du partenaire de ressource approuve le serveur de fédération du partenaire de compte, installez le certificat de fédération du partenaire de compte dans le magasin Autorités de certification approuvées du serveur de fédération du partenaire de ressource.

4. Afin de vous assurer que le serveur Web approuve le serveur de fédération du partenaire de ressource, installez le certificat de fédération du partenaire de ressource dans le magasin Autorités de certification approuvées du serveur Web.

Important : le serveur Web et le serveur de fédération de ressource doivent avoir accès aux Listes de Révocation de Certificats (LRC) de l'Autorité de Certification (AC). Le serveur de fédération de ressource doit avoir accès à l'Autorité de Certification du partenaire de compte et le serveur Web doit avoir accès à l'Autorité de Certification du partenaire de ressource. ADFS pourrait échouer si les serveurs ne peuvent pas confirmer qu'un certificat n'est pas révoqué.

5. Sur le serveur de fédération du partenaire de ressource, ouvrez le composant logiciel enfichable MMC Services de fédération Active Directory.

6. Dans le panneau gauche, sélectionnez Service de fédération > Stratégie d'approbation > Organisations partenaires > Partenaires de compte, puis sélectionnez le nom du partenaire de compte.

7. Dans le panneau Actions, cliquez sur Propriétés.

8. Sur l'onglet Comptes ressource, sélectionnez Des comptes ressource existent pour tous les utilisateurs, puis cliquez sur OK.

9. À l'aide du même serveur de temps Internet, synchronisez les horloges sur le serveur de fédération du partenaire de compte et le serveur de fédération du partenaire de ressource à cinq minutes près l'une par rapport à l'autre. Dans le cas contraire, les jetons de sécurité générés par le partenaire de compte peuvent ne pas être acceptés par le partenaire de ressource, les jetons pouvant apparaître comme ayant expiré. Les partenaires de compte et de ressource peuvent être situés dans des fuseaux horaires différents, mais ils doivent être correctement synchronisés. Par exemple, le partenaire de compte est à New York et il est défini sur 16h00, heure de la côte est américaine (EST). Le partenaire de ressource en Californie doit être défini entre 12h55 et 13h05, heure normale du Pacifique (PST). (Il y a trois heures de différence entre les zones EST et PST).

10. Sur le serveur Web, ouvrez le composant enfichable MMC Internet Information Services (IIS).

11. Sélectionnez votre serveur Web dans le panneau de gauche, et dans Affichage des fonctionnalités, cliquez deux fois sur Adresse URL du service de fédération.

12. Sur la page Adresse URL du service de fédération, entrez l'adresse URL du serveur de fédération du partenaire de ressource et cliquez sur Appliquer dans le panneau Action.

Configuration de la délégation pour les serveurs au sein de votre déploiement

Mise à jour : 2014-11-24

Assurez-vous que tous les serveurs au sein de votre déploiement sont sécurisés pour la délégation. Pour ce faire, effectuez les tâches suivantes en tant qu'administrateur de domaine sur le contrôleur de domaine pour le domaine du partenaire de ressource.

Pour vérifier que le domaine du partenaire de ressource est au niveau fonctionnel correct

Important : pour augmenter le niveau du domaine, tous les contrôleurs de domaine au sein du domaine doivent exécuter Windows Server 2008 ou Windows Server 2003. N'augmentez pas le niveau fonctionnel du domaine sur Windows Server 2008 si vous avez déjà ajouté ou que vous prévoyez d'ajouter des contrôleurs de domaine exécutant Windows Server 2003. Une fois le niveau fonctionnel augmenté, il ne peut plus être réduit.

1. Sur le contrôleur de domaine du partenaire de ressource, ouvrez le composant logiciel enfichable MMC Domaines et approbations Active Directory.
2. Dans le panneau de gauche, sélectionnez le nom de domaine du partenaire de ressource et, dans le panneau Action, cliquez sur Propriétés.
3. Si le domaine n'est pas au niveau fonctionnel le plus élevé, sélectionnez le nom du domaine et, dans le panneau Action, cliquez sur Augmenter le niveau fonctionnel du domaine.
4. Pour augmenter le niveau fonctionnel du domaine, cliquez sur le niveau approprié puis sur Augmenter.

Pour approuver le serveur Interface Web pour la délégation

1. Sur le contrôleur de domaine du partenaire de ressource, ouvrez le composant logiciel enfichable MMC Utilisateurs et ordinateurs Active Directory.
2. Sur le menu Affichage, cliquez sur Fonctionnalités avancées.
3. Dans le panneau de gauche, cliquez sur le nœud Ordinateurs sous le nom de domaine du partenaire de ressource et sélectionnez le serveur Interface Web.
4. Dans le panneau Action, cliquez sur Propriétés. Dans le panneau Action, cliquez sur Propriétés.
5. Sur l'onglet Délégation, cliquez sur Approuver cet ordinateur pour la délégation vers les services spécifiés uniquement et Utiliser n'importe quel protocole d'authentification, puis cliquez sur Ajouter.
6. Dans la boîte de dialogue Ajouter des services, cliquez sur Utilisateurs ou ordinateurs.
7. Dans la boîte de dialogue Sélectionnez utilisateurs ou ordinateurs, tapez le nom du serveur exécutant le service XML Citrix dans la zone de texte Entrez le nom de l'objet à sélectionner, puis cliquez sur OK.
8. Sélectionnez le type de service http dans la liste et cliquez sur OK.
9. Sur l'onglet Délégation, vérifiez que le type de service http pour le serveur XenApp apparaît bien dans la liste Services pour lesquels ce compte peut présenter des informations d'identification déléguées et cliquez sur OK.
10. Répétez le processus pour chaque serveur de la batterie exécutant le service XML Citrix que l'Interface Web doit contacter.

Pour approuver le serveur exécutant le service XML Citrix pour la délégation

1. Sur le contrôleur de domaine du partenaire de ressource, ouvrez le composant logiciel enfichable MMC Utilisateurs et ordinateurs Active Directory.

2. Dans le panneau de gauche, cliquez sur le nœud Ordinateurs sous le nom de domaine du partenaire de ressource et sélectionnez le serveur exécutant le service XML Citrix XML que l'Interface Web est configurée pour contacter.

3. Dans le panneau Actions, cliquez sur Propriétés.

4. Sur l'onglet Délégation, cliquez sur Approuver cet ordinateur pour la délégation vers les services spécifiés uniquement et Utiliser Kerberos uniquement, puis cliquez sur Ajouter.

5. Dans la boîte de dialogue Ajouter des services, cliquez sur Utilisateurs ou ordinateurs.

6. Dans la boîte de dialogue Sélectionnez utilisateurs ou ordinateurs, tapez le nom du serveur exécutant le service XML Citrix dans la zone de texte Entrez le nom de l'objet à sélectionner, puis cliquez sur OK.

7. Sélectionnez le type de service HOST dans la liste et cliquez sur OK.

8. Sur l'onglet Délégation, vérifiez que le type de service HOST pour le serveur exécutant le service XML Citrix apparaît bien dans la liste Ce compte peut présenter des informations d'identification déléguées à ces services, puis cliquez sur OK.

9. Répétez le processus pour chaque serveur de la batterie exécutant le service XML Citrix que l'Interface Web doit contacter.

Pour déterminer quelles ressources sont accessibles depuis le serveur XenApp

1. Sur le contrôleur de domaine du partenaire de ressource, ouvrez le composant logiciel enfichable MMC Utilisateurs et ordinateurs Active Directory.
2. Dans le panneau de gauche, cliquez sur le nœud Ordinateurs sous le nom de domaine du partenaire de ressource et sélectionnez le serveur XenApp.
3. Dans le panneau Actions, cliquez sur Propriétés.
4. Sur l'onglet Délégation, cliquez sur Approuver cet ordinateur pour la délégation vers les services spécifiés uniquement et Utiliser Kerberos uniquement, puis cliquez sur Ajouter.
5. Dans la boîte de dialogue Ajouter des services, cliquez sur Utilisateurs ou ordinateurs.
6. Dans la boîte de dialogue Sélectionnez utilisateurs ou ordinateurs, tapez le nom des contrôleurs de domaine du partenaire de ressource dans la case Entrez le nom de l'objet à sélectionner et cliquez sur OK.
7. Sélectionnez les types de service cifs et ldap dans la liste et cliquez sur OK.

   Remarque : si vous avez deux possibilités de service ldap, sélectionnez celui qui correspond au FQDN du contrôleur de domaine.
8. Sur l'onglet Délégation, vérifiez que les types de services cifs et ldap du contrôleur de domaine du partenaire de ressource apparaissent dans la liste Services pour lesquels ce compte peut présenter des informations d'identification déléguées, puis cliquez sur OK.
9. Répétez le processus pour chaque serveur XenApp de la batterie.

Configuration des serveurs pour la délégation contrainte

Pour des raisons de sécurité, vous devez configurer tous les serveurs XenApp pour la délégation contrainte. Pour fournir aux utilisateurs l'accès aux ressources sur ces serveurs, vous devez ajouter les services correspondants à la liste Services pour lesquels ce compte peut présenter des informations d'identification déléguées à l'aide du composant enfichable MMC Utilisateurs et ordinateurs Active Directory. Par exemple, pour permettre aux utilisateurs de s'authentifier auprès d'un serveur Web sur l'hôte « peter », ajoutez le service http pour le serveur peter ; pour permettre aux utilisateurs de s'authentifier auprès d'un serveur SQL sur l'hôte « lois », ajoutez le service MSSQLSvc pour le serveur lois.

Pour des informations détaillées, reportez-vous au document technique *Service Principal Names and Delegation in Presentation Server* (CTX110784) disponible dans le centre de connaissances Citrix.

Configuration d'une durée limite d'accès aux ressources

Attention : une utilisation incorrecte de l'Éditeur de Registre peut entraîner de graves problèmes 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.

Par défaut, les utilisateurs ADFS ont accès aux ressources sur un réseau pendant 15minutes. Vous pouvez augmenter cette durée en modifiant l'entrée de registre suivante sur le serveur exécutant le service XML Citrix :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
Kerberos\Parameters\S4UTicketLifetime

Cette valeur spécifie le nombre de minutes pendant lesquelles les utilisateurs ont accès aux ressources une fois une session ouverte.

La stratégie de sécurité de domaine régit la valeur maximale que vous pouvez définir pour S4ULifetime. Si vous définissez pour ce paramètre une valeur supérieure à celle spécifiée pour le paramètre au niveau du domaine, la valeur définie pour ce dernier est prioritaire.

Pour configurer une durée limite d'accès aux ressources au niveau du domaine

1. Sur le contrôleur de domaine du partenaire de ressource, ouvrez le composant logiciel enfichable MMC Stratégie de sécurité de domaine.
2. Dans le panneau de gauche, sélectionnez Stratégies de compte > Stratégie Kerberos.
3. Dans le panneau des résultats, sélectionnez Durée de vie maximale du ticket de service.
4. Dans le panneau Actions, cliquez sur Propriétés.
5. Entrez la durée requise (en minutes) dans la case Le ticket expire dans.

Si vous ne souhaitez pas configurer de durée limite pour l'accès aux ressources, sélectionnez Utiliser tout protocole d'authentification lorsque vous spécifiez les ressources accessibles depuis le serveur XenApp. Si vous sélectionnez cette option, la valeur spécifiée pour S4UTicketLifetime sera ignorée, quelle qu'elle soit. Pour de plus amples informations, visitez le site Web de Microsoft à l'adresse http://support.microsoft.com/.

Création de comptes fantômes

Pour fournir l'accès aux applications, XenApp requiert des comptes Windows authentiques. C'est pourquoi vous devez créer manuellement un compte fantôme dans le domaine du partenaire de ressource pour chaque utilisateur externe qui s'authentifie auprès de l'Interface Web via ADFS.

Si vous disposez de plusieurs utilisateurs dans le domaine du partenaire de compte qui accèdent aux applications et contenus dans le domaine du partenaire de ressource, vous pouvez utilisez un produit tiers d'approvisionnement de compte afin de permettre une création rapide de comptes utilisateur fantômes dans Active Directory.

Pour ce faire, effectuez les tâches suivantes en tant qu'administrateur de domaine sur le contrôleur de domaine pour le domaine du partenaire de ressource.

Pour ajouter des suffixes de nom d'utilisateur principal

1. Sur le contrôleur de domaine du partenaire de ressource, ouvrez le composant logiciel enfichable MMC Domaines et approbations Active Directory.
2. Dans le panneau gauche, sélectionnez Domaines et approbations Active Directory.
3. Dans le panneau Actions, cliquez sur Propriétés.
4. Ajoutez un suffixe UPN pour chaque partenaire de compte externe. Par exemple, si le domaine Active Directory du partenaire de compte est « adomain.com », ajoutez adomain.com en tant que suffixe UPN.

Pour définir l'utilisateur du compte fantôme

1. Sur le contrôleur de domaine du partenaire de ressource, ouvrez le composant logiciel enfichable MMC Utilisateurs et ordinateurs Active Directory.
2. Dans le panneau gauche, sélectionnez le nom de domaine du partenaire de ressource.
3. Dans le panneau Action, cliquez sur Nouveau > Utilisateur.
4. Entrez le prénom de l'utilisateur, ses initiales ainsi que son nom dans les cases correspondantes.
5. Dans la case Nom de connexion de l'utilisateur, tapez le nom de compte. Assurez-vous que ce nom corresponde au nom sur le contrôleur de domaine du partenaire de compte.
6. Dans la liste, choisissez le suffixe UPN externe et cliquez sur Suivant.
7. Dans les cases Mot de passe et Confirmer le mot de passe, entrez un mot de passe qui corresponde à votre stratégie de mot de passe. Ce mot de passe n'est jamais utilisé car l'utilisateur s'authentifie via ADFS.
8. Décochez la case L'utilisateur doit changer de mot de passe à la prochaine ouverture de session.
9. Cochez les cases L'utilisateur ne peut pas changer de mot de passe et Pas de limite d'expiration du mot de passe.
10. Cliquez sur Suivant, puis cliquez sur Terminer.

Création de sites Active Directory Federation Services intégrés

Exécutez la tâche Créer un site dans la console de gestion Interface Web Citrix et configurez le site Interface Web afin d'utiliser l'authentification ADFS.

Remarque : la mise à disposition de bureaux virtuels XenDesktop dans un environnement ADFS n'est pas prise en charge. Par ailleurs, le client pour Java et le logiciel Connexion au Bureau à distance ne prennent pas en charge l'accès aux sites intégrés ADFS.

Pour créer un site Active Directory Federation Services intégré

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.
2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Interface Web Citrix.
3. Dans le panneau Actions, cliquez sur Créer un site.
4. Sélectionnez XenApp Web et cliquez sur Suivant.
5. Sur la page Spécifier l'emplacement IIS, spécifiez l'emplacement IIS, le chemin d'accès et le nom du site. Cliquez sur Next.
6. Sur la page Spécifier le point d'authentification, sélectionnez Sur le partenaire de compte Microsoft ADFS. Définissez l'adresse de retour de l'Interface Web et cliquez sur Suivant.
7. Confirmez les paramètres pour le nouveau site et cliquez sur Suivant pour le créer.

Configuration de votre site en tant qu'application Active Directory Federation Services

Après avoir créé votre site, vous devez le configurer en tant qu'application ADFS afin qu'il puisse être reconnu par le serveur de fédération.

Pour configurer votre site en tant qu'application Active Directory Federation Services

1. Sur le serveur de fédération du partenaire de ressource, ouvrez le composant logiciel enfichable MMC Services de fédération Active Directory.
2. Dans le panneau gauche, sélectionnez Service de fédération > Stratégie d'approbation > Mon organisation > Applications.
3. Dans le panneau Action, cliquez sur Nouveau > Application.
4. Cliquez sur Suivant, sélectionnez Application compatible avec les revendications et cliquez sur Suivant.
5. Entrez un nom pour le site dans la case Nom affiché de l'application.
6. Dans la case ApplicationURL, entrez l'adresse URL de votre site Interface Web *exactement* telle qu'elle apparaît dans la case Adresse URL de retour vers l'Interface Web lorsque vous avez créez le site et cliquez sur Suivant.

   Remarque : assurez-vous que vous utilisez HTTPS et le FQDN de votre serveur Web.
7. Cochez la case Nom d'utilisateur principal (UPN) et cliquez sur Suivant.
8. Assurez-vous que la case Activer cette application est sélectionnée et cliquez sur Suivant.
9. Cliquez sur Terminer pour ajouter votre site en tant qu'application AD FS.

Test de votre déploiement

Mise à jour : 2014-12-02

Après avoir configuré votre site en tant qu'application ADFS, testez votre déploiement afin de vous assurer que tout fonctionne correctement entre le partenaire de compte et le partenaire de ressource.

Pour tester le déploiement Active Directory Federation Services de l'Interface Web

1. Ouvrez une session sur votre machine utilisateur dans le domaine du partenaire de compte.
2. Ouvrez un navigateur Web et tapez l'URL FQDN du site Interface Web ADFS intégré que vous avez créé précédemment.

   Votre série d'applications apparaît.

   Remarque : si vous n'avez pas configuré ADFS pour l'authentification intégrée, vous pouvez être invité à entrer vos informations d'identification ou à insérer une carte à puce.
3. Si vous n'avez pas installé Citrix Online Plug-in, faites-le à présent. Pour de plus amples informations, consultez la documentation Online Plug-in pour Windows archivée.
4. Cliquez sur une application pour y accéder.

Déconnexion des sites Active Directory Federation Services intégrés

Utilisez la tâche Méthodes d'authentification dans la console de gestion de l'Interface Web Citrix pour indiquer si les utilisateurs cliquant sur les boutons Fermeture de session ou Se déconnecter du site Web se déconnectent de :

- L'Interface Web uniquement
- L'Interface Web et ADFS Federation Service

Si vous spécifiez que les utilisateurs se déconnectent de l'Interface Web uniquement, ils sont redirigés vers l'écran de fermeture de session de l'Interface Web. Si vous spécifiez que les utilisateurs se déconnectent de l'Interface Web et du service de fédération ADFS, ils sont redirigés vers la page de fermeture de session du service de fédération et ils sont déconnectés de toutes les applications ADFS.

Remarque : les utilisateurs qui s'authentifient à l'aide d'ADFS ne peuvent pas déverrouiller leur session XenApp car ils ne connaissent pas leur mot de passe. Pour déverrouiller des sessions, les utilisateurs doivent fermer leur session Interface Web, puis rouvrir une session à l'aide de l'authentification ADFS. Ils peuvent ensuite redémarrer leurs applications. Lorsqu'ils procèdent de la sorte, la session précédente se déverrouille et la nouvelle fenêtre se ferme.

Pour spécifier les services auxquels les utilisateurs se déconnectent

1. Dans le menu Démarrer de Windows, cliquez sur Tous les programmes > Citrix > Consoles de gestion > Gestion de l'Interface Web Citrix.
2. Dans le panneau gauche de la console de gestion de l'Interface Web Citrix, cliquez sur Sites XenApp Web et, dans le panneau des résultats, sélectionnez votre site intégré ADFS.
3. Dans le panneau Actions, cliquez sur Méthodes d'authentification.
4. Pour indiquer qu'un utilisateur se déconnecte à partir de l'Interface Web et du service de fédération ADFS, cochez la case Effectuer une déconnexion globale. Pour indiquer que les utilisateurs se déconnectent de l'Interface Web uniquement, décochez la case Effectuer une déconnexion globale.