Application Citrix Workspace pour Linux

Contents

À propos de cette version

May 21, 2021

Nouveautés dans la version 2104

Prise en charge de la protection des applications sur Red Hat Package Manager (RPM) fonctionnalité expérimentale

La protection des applications est désormais prise en charge sur la version RPM de l'application Citrix Workspace.

Pour de plus amples informations, consultez Protection des applications.

Améliorations apportées au protocole HDX Enlightened Data Transport (EDT)

Dans les versions antérieures, lorsque `HDXoverUDP` est défini sur `Preferred`, le transport de données via EDT est utilisé comme mode principal avec retour vers TCP.

Lorsque la fiabilité de session est activée, EDT et TCP sont tentés en parallèle lors de la connexion initiale, de la reconnexion de la fiabilité de session et de la reconnexion automatique des clients. Cette amélioration réduit le temps de connexion lorsque EDT est le protocole préféré, mais le transport UDP sous-jacent requis est indisponible et TCP doit être utilisé.

Par défaut, après le repli vers TCP, le transport adaptatif continue d'interroger EDT toutes les 5 minutes.

Optimisation Microsoft Teams

Dans cette version, la fonction d'annulation de l'écho est désactivée par défaut. Nous vous recommandons de ne pas utiliser vos haut-parleurs et votre microphone intégrés pour les appels. Utilisez plutôt un casque.

Ce correctif vise à résoudre les problèmes d'audio saccadé sur les clients légers.

Continuité du service (version Technical Preview)

> **Remarque :**
>
> Cette fonctionnalité est disponible en version Technical Preview. Citrix recommande d'utiliser cette fonctionnalité uniquement dans un environnement de non production. Pour vous inscrire,

> utilisez le formulaire Podio suivant : S'inscrire : Continuité du service (version Technical Preview) pour Citrix Workspace.

La fonction Continuité du service supprime ou réduit la dépendance à l'égard de la disponibilité des composants impliqués dans le processus de connexion. Les utilisateurs peuvent lancer leurs applications et bureaux virtuels quel que soit l'état d'intégrité des services cloud.

Pour plus d'informations, consultez la section Continuité du service dans la documentation de Citrix Workspace.

Nouveautés dans la version 2103

Épinglage de la disposition de plusieurs moniteurs

Avec cette version, vous pouvez enregistrer la sélection de la disposition d'écran multi-moniteurs. La disposition est la façon dont une session de bureau saffiche. L'épinglage permet de relancer une session avec la disposition sélectionnée, ce qui permet d'optimiser l'expérience utilisateur.

En tant que condition préalable, vous devez activer cette fonctionnalité dans le fichier `AuthManConfig.xml`. Accédez à `$ICAROOT/config/AuthManConfig.xml` et ajoutez les entrées suivantes pour activer la fonctionnalité d'épinglage de la disposition de l'écran :

```
1       <key>ScreenPinEnabled</key>
2       <value> true </value>
```

L'option **Disposition de l'écran** ne sera visible dans **l'indicateur d'application** qu'après l'ajout de la clé ci-dessus.

> **Remarque :**
>
> Cette fonctionnalité n'est pas disponible sur le lancement Web de l'application Citrix Workspace.

Pour de plus amples informations, consultez Épinglage de la disposition de plusieurs moniteurs.

Augmentation du nombre de canaux virtuels pris en charge

Dans les versions antérieures du client, les sessions prennaient en charge jusqu'à 32 canaux virtuels.

Avec cette version, vous pouvez utiliser jusqu'à 64 canaux virtuels dans une session.

Améliorations apportées à Microsoft Teams

Le codec vidéo VP9 est maintenant désactivé par défaut.

Nouveautés dans la version 2101

Amélioration du mappage des lecteurs clients

Avec cette version, l'accès aux lecteurs mappés est doté d'une fonctionnalité de sécurité supplémentaire.

Vous pouvez maintenant sélectionner le niveau d'accès pour le lecteur mappé pour chaque magasin d'une session.

Pour empêcher l'affichage de la boîte de dialogue de niveau d'accès à chaque fois, sélectionnez l'option **Ne plus me demander**. Le paramètre est appliqué sur ce magasin particulier.

Sinon, vous pouvez définir les niveaux d'accès chaque fois qu'une session est lancée.

Prise en charge de la protection des applications sur les packages Debian fonctionnalité expérimentale

La protection des applications est désormais prise en charge sur la version Debian de l'application Citrix Workspace.

Pour installer de façon silencieuse le composant de protection d'application, exécutez la commande suivante à partir du terminal avant d'installer l'application Citrix Workspace :

```
export DEBIAN_FRONTEND="noninteractive"
sudo debconf-set-selections <<< "icaclient app_protection/
   install_app_protection select no"
sudo debconf-show icaclient
* app_protection/install_app_protection: no
sudo apt install -f ./icaclient_<version>._amd64.deb
```

Améliorations apportées à Microsoft Teams

- Le programme d'installation de l'application Citrix Workspace est maintenant packagé avec les sonneries de Microsoft Teams.
- La sortie audio bascule automatiquement vers les périphériques audio nouvellement branchés, et un volume audio approprié est défini.
- Prise en charge du proxy HTTP pour l'authentification anonyme.

Nouveautés dans la version 2012

Amélioration du mappage des lecteurs clients

Auparavant, votre paramètre d'accès aux fichiers via CDM était appliqué à tous les magasins configurés.

À partir de cette version, l'application Citrix Workspace vous permet de configurer l'accès aux fichiers CDM par magasin.

> **Remarque :**
>
> Le paramètre d'accès aux fichiers n'est pas persistant sur toutes les sessions lors de l'utilisation de Workspace pour Web. L'option par défaut est **Ask me each time** (Me demander à chaque fois).

Pour de plus amples informations, consultez Mappage des lecteurs clients.

Protection des applications fonctionnalité expérimentale

> **Remarque :**
>
> - Cette fonctionnalité est prise en charge uniquement lorsque l'application Citrix Workspace est installée à l'aide du package Tarball. En outre, x64 et armhf sont les deux seuls packages pris en charge.
> - Cette fonctionnalité est prise en charge uniquement sur les déploiements locaux de Citrix Virtual Apps and Desktops.

La protection des applications est une fonctionnalité complémentaire qui offre une sécurité renforcée lors de l'utilisation de Citrix Virtual Apps and Desktops. Elle limite le risque d'être infecté par des programmes malveillants d'enregistrement de frappe et de capture d'écran. La protection des applications empêche l'exfiltration d'informations confidentielles telles que les informations d'identification de l'utilisateur et les informations sensibles affichées à l'écran. Cette fonctionnalité empêche les utilisateurs et les attaquants de prendre des captures d'écran et d'utiliser des enregistreurs de frappe pour récupérer et exploiter des informations sensibles.

Pour plus d'informations sur la configuration de la protection des applications sur Citrix Virtual Apps and Desktops, consultez la section Protection des applications de la documentation Citrix Virtual Apps and Desktops.

Pour plus d'informations sur la protection des applications dans l'application Citrix Workspace, consultez la section Protection des applications.

Amélioration de l'authentification fonctionnalité expérimentale

Nous présentons maintenant la boîte de dialogue d'authentification dans l'application Citrix Workspace et affichons les détails du magasin sur l'écran d'ouverture de session pour une meilleure

expérience utilisateur. Nous chiffrons et stockons les jetons d'authentification afin que vous n'ayez pas besoin de saisir de nouveau les informations d'identification lorsque votre système ou votre session redémarre.

> **Remarque :**
>
> - Cette amélioration de l'authentification ne s'applique qu'aux déploiements dans le cloud.
> - Cette amélioration de l'authentification n'est pas disponible sur la plateforme armhf.

Conditions préalables :

Vous devez installer la bibliothèque libsecret.

Cette fonction est désactivée par défaut.

Pour de plus amples informations, consultez Authentification.

Amélioration de la configuration audio

À partir de cette version, la valeur par défaut de l'attribut `VdcamVersion4Support` dans le fichier `module.ini` est définie sur `True`.

Pour de plus amples informations, consultez Audio.

Nouveautés dans la version 2010

Redirection audio améliorée

Auparavant, seul le périphérique audio par défaut était mappé dans une session même lorsque de nombreux périphériques étaient disponibles sur la machine. Le périphérique mappé apparaît généralement sous le nom de **Citrix HDX Audio**.

Avec cette version, l'application Citrix Workspace pour Linux affiche tous les périphériques audio locaux disponibles dans une session. Au lieu de **Citrix HDX Audio**, ils apparaissent désormais avec leurs noms de périphérique respectifs. Vous pouvez basculer dynamiquement vers n'importe quel périphérique disponible dans une session. Contrairement aux versions précédentes, vous n'avez plus besoin de sélectionner le périphérique audio par défaut avant de lancer la session. Les sessions sont mises à jour de manière dynamique lorsque vous branchez ou supprimez des périphériques audio.

Pour de plus amples informations, consultez Audio.

En outre, cette version résout certains problèmes pour améliorer la fonctionnalité Multi-Stream ICA.

Nouveautés dans la version 2009

Amélioration de la journalisation

Auparavant, les fichiers `debug.ini` et `module.ini` étaient utilisés pour configurer la journalisation.

À partir de la version 2009, vous pouvez configurer la journalisation à l'aide de l'une des méthodes suivantes :

- Interface de ligne de commande
- Interface graphique (GUI)

Également à partir de la version 2009, le fichier de configuration `debug.ini` est supprimé du programme d'installation de l'application Citrix Workspace.

La journalisation capture les détails du déploiement, les modifications de configuration et les activités administratives de l'application Citrix Workspace dans une base de données de journalisation. Un développeur tiers peut utiliser le SDK de journalisation, qui est fourni dans le cadre du SDK d'optimisation de la plate-forme de l'application Citrix Workspace.

Vous pouvez utiliser les informations de journalisation pour effectuer les opérations suivantes :

- Diagnostiquer et résoudre les problèmes qui se produisent après toute modification. Le journal fournit une arborescence hiérarchique.
- Assister la gestion des modifications et suivre les configurations.
- Signaler les activités administratives.

> **Remarque :**
>
> Ce mécanisme de journalisation est applicable uniquement sur la version commerciale.

Pour plus d'informations sur la journalisation, reportez-vous à la section Journalisation.

Nouveautés de la version 2006

Optimisation pour Microsoft Teams

Optimisation pour Microsoft Teams à l'aide de l'application Citrix Workspace et de Citrix Virtual Apps and Desktops. L'optimisation pour Microsoft Teams est similaire à l'optimisation HDX RealTime pour Microsoft Skype Entreprise. La différence est que nous regroupons tous les composants nécessaires à l'optimisation pour Microsoft Teams dans le VDA et l'application Citrix Workspace.

L'application Citrix Workspace pour Linux prend en charge les fonctionnalités audio, vidéo et de de partage d'écran avec l'optimisation Microsoft Teams.

> **Remarque :**
>
> L'optimisation Microsoft Teams est prise en charge uniquement sur les distributions Linux x64.

Pour plus d'informations sur l'activation de la journalisation, suivez les étapes mentionnées sous Journalisation pour Microsoft Teams.

Pour plus d'informations sur la configuration système requise, reportez-vous à la section Optimisation Microsoft Teams.

Pour plus d'informations, veuillez consulter Optimisation pour Microsoft Teams et Redirection Microsoft Teams.

Prise en charge du canal virtuel NetScaler App Experience (NSAP)

Auparavant disponible en tant que fonctionnalité expérimentale, la fonctionnalité de canal virtuel NetScaler App Experience (NSAP) est désormais entièrement opérationnelle. Le canal virtuel NSAP facilite l'approvisionnement des données HDX Insight, ce qui améliore la capacité à monter en charge et les performances. Le canal virtuel NSAP est activé par défaut. Pour le désactiver, désactivez l'indicateur NSAP `NSAP=Off` dans le fichier `module.ini`.

Pour plus d'informations, consultez HDX Insight dans la documentation de Linux Virtual Delivery Agent et HDX Insight dans la documentation de Citrix Application Delivery Management Service.

Mise à jour de Citrix Analytics Service

L'application Citrix Workspace est conçue pour transmettre des données à Citrix Analytics Service à partir de sessions ICA que vous lancez depuis un navigateur.

Pour plus d'informations sur la façon dont Citrix Analytics utilise ces informations, consultez Recherche en libre-service des performances et Recherche en libre-service pour Virtual Apps and Desktops.

Mise à jour de la version de TLS

Auparavant, la version minimale de TLS prise en charge était 1.0 et la version maximale de TLS prise en charge était 1.2.

À partir de cette version, la version minimale et maximale de TLS prise en charge est 1.2. Pour configurer une valeur différente pour `MinimumTLS`, consultez TLS.

Mise à jour de CryptoKit

CryptoKit version 14.2 est intégré à la version 1.1.1d d'OpenSSL.

Nouveautés dans la version 2004

Langues prises en charge

L'application Citrix Workspace pour Linux est désormais disponible en italien.

Amélioration des performances d'ouverture de session et d'énumération

Avec cette version, les comptes d'utilisateurs du cloud observent des temps d'ouverture de session et d'énumération des applications plus courts.

Optimisation audio pour Microsoft Teams fonctionnalité expérimentale

En tant que fonctionnalité expérimentale, l'application Citrix Workspace fournit une optimisation audio pour Microsoft Teams dans une session Citrix Virtual Desktop.

> **Remarque :**
>
> L'optimisation de l'audio Microsoft Teams est prise en charge uniquement sur les distributions Linux x64.

Pour de plus amples informations, consultez les sections Optimisation pour Microsoft Teams et Redirection Microsoft Teams dans la documentation de Citrix Virtual Apps and Desktops.

Prise en charge du canal virtuel NetScaler App Experience (NSAP) fonctionnalité expérimentale

En tant que fonctionnalité expérimentale, les données HDX Insight proviennent exclusivement du canal virtuel NSAP et sont envoyées non compressées, ce qui améliore la capacité à monter en charge et les performances. Le canal virtuel NSAP est activé par défaut. Pour le désactiver, désactivez l'indicateur NSAP `NSAP=Off` dans le fichier `module.ini`.

Pour plus d'informations, consultez HDX Insight dans la documentation de Linux Virtual Delivery Agent et HDX Insight dans la documentation de Citrix Application Delivery Management Service.

Nouveautés dans la version 1912

Amélioration de l'interface utilisateur transparente

La version 1910 a introduit la fonctionnalité d'interface utilisateur transparente (TUI, Transparent User Interface), y compris l'indicateur **VDTUI**. Cette fonctionnalité aide le système client à recevoir les paquets TUI envoyés par le serveur, et le client peut accéder aux composants associés à l'interface utilisateur. Cependant, si l'indicateur est défini sur **Désactivé**, la superposition de la boîte de dialogue « Démarrage de <Application> » s'affiche au-dessus des autres fenêtres d'application et masque l'invite de connexion.

L'indicateur **VDTUI**, situé dans le fichier `module.ini`, est désormais défini sur **Activé** par défaut. Par conséquent, la boîte de dialogue « Démarrage de <Application> » ne s'affiche plus lorsque vous lancez une application. Au lieu de cela, une boîte dialogue « Connexion de <Application> » s'affiche avec une barre de progression. La boîte de dialogue affiche également la progression du lancement de l'application.

Prise en charge de GStreamer 1.x fonctionnalité expérimentale

Dans les versions antérieures, GStreamer 0.10 était la version par défaut prise en charge pour la redirection multimédia. À partir de cette version, vous pouvez configurer GStreamer 1.x comme version par défaut.

Limitations :

- Lorsque vous lisez une vidéo, l'option de recherche en avant et en arrière peut ne pas fonctionner comme prévu.
- Lorsque vous lancez l'application Citrix Workspace sur des appareils ARMHF, GStreamer 1.x peut ne pas fonctionner comme prévu.

Pour de plus amples informations, consultez Activer GStreamer 1.x.

Chromium Embedded Framework (CEF) pour la redirection du contenu du navigateur fonctionnalité expérimentale

La redirection du contenu du navigateur permet de rediriger le contenu d'un navigateur Web vers une machine cliente et de créer un navigateur correspondant incorporé dans l'application Citrix Workspace.

Auparavant, la redirection du contenu du navigateur utilisait une superposition basée sur `WebkitGTK +` pour rendre le contenu. À partir de cette version, la redirection du contenu du navigateur utilise une superposition basée sur CEF pour une meilleure expérience utilisateur. Elle permet de décharger l'utilisation du réseau, le traitement des pages et le rendu graphique sur le point de terminaison.

Pour de plus amples informations, consultez : Activer la redirection du contenu du navigateur basée sur CEF

Pour de plus amples informations sur la redirection du contenu du navigateur, consultez la section Redirection du contenu du navigateur dans la documentation Citrix Virtual Apps and Desktops.

> **Remarques :**
>
> - Le fichier binaire **pacexec** est supprimé de la version x86 de l'application Citrix Workspace.
> - Citrix Files peut ne pas être compatible avec la fonctionnalité « Workspace Intelligence ».

Nouveautés dans la version 1910

Langues prises en charge

L'application Citrix Workspace pour Linux est désormais disponible en portugais brésilien.

Icône « appindicator »

L'icône appindicator démarre lorsque vous lancez l'application Citrix Workspace. Il s'agit d'une icône qui est présente dans la zone de notification. Avec l'introduction de l'icône appindicator, les performances d'ouverture de session de l'application Citrix Workspace pour Linux sont améliorées.

Vous pouvez observer une amélioration des performances lorsque vous :

- lancez l'application Citrix Workspace pour la première fois ;
- fermez et relancez l'application ;
- quittez et relancez l'application.

> **Remarque :**
>
> Le package `libappindicator` est requis pour que l'icône appindicator s'affiche. Installez le package `libappindicator` adapté à votre distribution Linux à partir du Web.

Interface utilisateur transparente

Le protocole ICA Citrix utilise le protocole Transparent User Interface Virtual Channel [TUI VC] pour transmettre des données entre les clients Citrix Virtual Apps and Desktops et les serveurs hôtes. Le protocole TUI transmet les messages des composants de l'interface utilisateur [Interface utilisateur] pour les connexions distantes.

Auparavant, l'application Citrix Workspace pour Linux ne prenait pas en charge la fonctionnalité TUI VC. Par conséquent, le système client ne pouvait pas gérer efficacement les données du composant de l'interface utilisateur du serveur. Ainsi, lorsque vous tentiez de lancer une application, la boîte de dialogue « Démarrage de <Application> » s'affichait au-dessus des autres fenêtres d'application.

Maintenant, l'application Citrix Workspace pour Linux prend en charge la fonctionnalité TUI VC. Cette fonctionnalité aide le client à recevoir les paquets TUI envoyés par le serveur, et le client peut accéder aux composants associés à l'interface utilisateur. Cette fonctionnalité vous permet de contrôler l'affichage de l'écran de superposition par défaut. Vous pouvez activer/désactiver l'indicateur `VDTUI` dans le fichier `module.ini` : `VDTUI - On/Off`.

Pour de plus amples informations sur les canaux virtuels, consultez Canaux virtuels ICA Citrix dans la documentation de Citrix Virtual Apps and Desktops.

Problèmes résolus

Problèmes résolus dans la version 2104

- Lors de l'utilisation de la redirection du contenu du navigateur, le focus clavier ne revient pas à la fenêtre parent même après une recherche dans la barre de recherche YouTube. [RFLNX-5349]
- Lors du partage d'un écran dans Microsoft Teams durant un appel pair à pair, l'audio peut être déformé. Le problème se produit avec les clients légers Dell Wyse 5070 et 5470. [RFLNX-6537]

- Lors de l'utilisation de Microsoft Teams dans l'application Citrix Workspace pour Linux, certains appels peuvent se déconnecter de façon inattendue. [RFLNX-6719]
- Cette version résout un certain nombre de problèmes afin d'améliorer la stabilité et les performances générales. [RFLNX-7006]
- Lors de l'utilisation du framework CEF, la redirection du contenu du navigateur peut entraîner une utilisation élevée du processeur. [RFLNX-7217]
- Lorsque vous basculez entre les applications publiées et locales, l'application publiée peut ne pas être mise à l'échelle correctement en mode plein écran. [CVADHELP-14812]
- Lorsque vous ouvrez Microsoft Excel via l'application Citrix Workspace pour Linux et accédez à **Données** > **Nouvelle requête**, le menu contextuel **Paramètres de la source de données** peut ne pas s'ouvrir comme prévu. [CVADHELP-16509]
- Les versions 2101 et 2102 de l'application Citrix Workspace pour Linux peuvent afficher une adresse IP client non valide dans Citrix Director [CVADHELP-16923]
- Le nom du périphérique audio peut être illisible. Le problème se produit sur les systèmes d'exploitation de langue chinoise. [CVADHELP-17290]

Problèmes résolus dans les versions précédentes

Problèmes résolus dans la version 2103

- Les tentatives d'établissement d'un appel vidéo non optimisé peuvent entraîner la perte du son. L'audio ne peut pas être récupéré tant que vous n'avez pas déconnecté et reconnecté la session. [CVADHELP-16846]
- Ce correctif définit la valeur par défaut pour AudioLatencyControlEnabled sur True, ce qui réduit la latence audio. [RFLNX-6620]
- La fonctionnalité de partage d'écran dans Microsoft Teams peut échouer en mode transparent. [RFLNX-6659]

Problèmes résolus dans la version 2101

- Lors de l'utilisation d'un proxy personnalisé, une invite d'authentification supplémentaire peut s'afficher. Le problème est causé par le Chromium Embedded Framework (CEF) utilisé par la redirection de contenu du navigateur. Pour résoudre le problème, configurez votre agent pour contourner l'invite supplémentaire. [CVADHELP-14804]
- Lorsque vous tentez de vous reconnecter à une session, la session peut cesser de répondre. Le problème se produit avec les sessions qui utilisent une carte à puce. Pour résoudre le problème, réinsérez la carte à puce. [CVADHELP-15028]
- Lorsque Microsoft Teams est en mode **optimisé**, la lecture vidéo peut cesser de répondre pendant les conférences téléphoniques. Le problème se produit lorsqu'un participant bascule entre une caméra intégrée et une caméra USB. [CVADHELP-16400]

- Lorsque Microsoft Teams est en mode **optimisé**, le processus `HdxRtcEngine.exe` peut se fermer de façon inattendue. [CVADHELP-16504]

Problèmes résolus dans la version 2012

- Lorsque vous tentez de lancer une page Web redirigée à l'aide de la redirection de contenu du navigateur, la page Web peut ne plus répondre. Le problème se produit lorsque vous cliquez sur un lien qui s'ouvre dans une nouvelle fenêtre ou un nouvel onglet. [RFLNX-5306]
- Lors de l'utilisation de la redirection de contenu du navigateur avec CEF, les microphones et les caméras ne sont pas redirigés. Pour activer la redirection, définissez l'attribut `CefEnableMediaDevices` sur `True` dans `All_Regions.ini`.[RFLNX-5337]
- Lorsque vous appuyez sur les touches **Alt+Ctrl**, elles peuvent rester bloquées. Le problème se produit lorsque l'option Disposition du clavier est définie sur Serveur par défaut. [RFLNX-5444]
- Les tentatives de sélection des options USB, Picture Transfer Protocol (PTP) et Media Transfer Protocol (MTP) sur un téléphone Android peuvent échouer. Pour résoudre ce problème avec les VDA Windows et Linux, ajoutez la règle d'autorisation suivante dans le fichier usb.conf :

  ALLOW: VID = (vid du périphérique) disableselectconfig=1

  [CVADHELP-15304]
- Citrix Director peut incorrectement indiquer 2009 comme numéro de version de l'application Citrix Workspace au lieu de 2010. [RFLNX-5743]
- Vous pouvez lancer l'application Citrix Workspace pour Linux avec succès lors de votre première tentative, mais les tentatives ultérieures risquent d'échouer. [RFLNX-5971]
- Lorsque vous tentez d'ajouter un magasin non authentifié (anonyme), deux messages d'erreur peuvent s'afficher. Le problème se produit avec l'application Citrix Workspace 2010 pour Linux. [RFLNX-5980]

Problèmes résolus dans la version 2010

- Lorsque vous exécutez un appel vidéo ou que vous partagez l'écran dans Microsoft Teams, l'écran peut clignoter. [RFLNX-4778]
- Les tentatives de personnalisation des fichiers webrpc.log et webrtc.log échouent. [RFLNX-5221]
- Les ressources sont énumérées pour le magasin même après avoir la suppression du magasin à l'aide de l'utilitaire storebrowse. [RFLNX-5499]
- Lorsque les paramètres régionaux Allemand ou Français sont installés sur la machine, l'optimisation Microsoft Teams peut ne pas fonctionner. [RFLNX-5599]

- Lorsque vous lancez une session à partir de l'application Citrix Workspace pour Linux, la session peut clignoter. Le problème se produit car la session se déconnecte et se reconnecte. Le problème se produit principalement avec les applications Microsoft. [CVADHELP-14194]
- Lorsque vous effectuez des opérations de Presse-papiers telles que le copier-coller de contenu entre différentes sessions, les opérations peuvent échouer par intermittence. [CVADHELP-15228]
- Lorsque vous démarrez une présentation de diaporama avec Microsoft PowerPoint lancée via l'application Citrix Workspace pour Linux version 1906 ou ultérieure, la présentation peut ne pas s'ouvrir en mode plein écran. [CVADHELP-15648]
- L'application Citrix Workspace pour Linux peut ne pas afficher de boîte de dialogue d'authentification pour les magasins qui utilisent le stockage local HTML5. Le problème se produit lorsque vous utilisez l'interface utilisateur en libre-service. [CVADHELP-15720]

Problèmes résolus dans la version 2009

- Parfois, la vue Réunion n'est pas rétablie pendant le multitâche dans Microsoft Teams. Le problème se produit lorsqu'une fenêtre locale chevauche la fenêtre distante. Par conséquent, la fenêtre distante ne reçoit pas les événements de la souris. Comme solution de contournement, sur l'écran réduit, survolez l'horloge numérique avec la souris et double-cliquez sur le nom de l'appelant. [RFLNX-4937]
- Dans une session exécutée sur des connexions UDP, les performances peuvent être lentes. [RFLNX-5135]
- Lorsque vous faites glisser la fenêtre d'une application publiée tierce transparente sur votre écran, la fenêtre peut automatiquement être réduite. [CVADHELP-13677]
- Un seul périphérique USB redirigé vers une session exécutée sur un appareil peut être redirigé de manière inattendue vers une session entrante exécutée sur le même appareil. [CVADHELP-13684]
- Dans un environnement multi-moniteurs, lorsque vous tentez de relancer une session plein écran sur un moniteur, la barre de connexion reste sur un autre moniteur. Le problème se produit même lorsque le curseur de la souris reste sur le même moniteur. [CVADHELP-14642]
- Lorsque vous tentez de vous reconnecter à une session, la session peut se déconnecter immédiatement après l'affichage du bureau. Le problème se produit avec les sessions qui nécessitent l'authentification par carte à puce. [CVADHELP-15036]

Problèmes résolus dans la version 2006

- Lors de l'utilisation de Microsoft Teams, l'option « Appel test » n'apparaît pas. [RFLNX-4234]
- Le lancement de session peut échouer sur les distributions Red Hat 8.2, CentOS 8.x, Fedora 29, 30 et 31. [RFLNX-3114] [RFLNX-4438] [RFLNX-4296]

- Avec l'ajout des binaires `wfica_for_plugins` au SDK d'optimisation de la plate-forme, une dépendance inutile introduite sur LIBS_GTK est maintenant supprimée. [RFLNX-4604]
- La récupération serveur et restitution sur le client de la redirection du contenu du navigateur basée sur CEF échoue. En conséquence, la redirection du contenu du navigateur échoue. [RFLNX-4459]
- Après avoir cliqué sur une application publiée dans Citrix StoreFront, une boîte de dialogue de connexion apparaît et reste là. Le problème se produit en mode non transparent. [CVADHELP-13896]
- Après avoir sélectionné l'option **Activer** pour activer l'application Citrix Workspace sur votre bureau, le fichier **receiverconfig.cr** est téléchargé. Les tentatives d'ajout du magasin à l'application Citrix Workspace en lançant ce fichier peuvent échouer. [CVADHELP-14389]
- Les tentatives de mappage de l'application Citrix Workspace pour Linux à un port série COM peuvent échouer, indiquant que le port ne peut pas être contacté. Le problème se produit lorsque les entrées COM précédentes ne sont pas renseignées [CVADHELP-14391]
- L'application Citrix Workspace pour Linux peut ne pas identifier certaines cartes à puce. Dans ce cas, les tentatives de lancement d'une session avec ces cartes échouent. [CVADHELP-14878]

Problèmes résolus dans la version 2004

- Si vous supprimez la section **Preferences** du fichier **All_Regions.ini**, le processus wfica échoue. Par conséquent, les sessions ne parviennent pas à se connecter. [RFLNX-3965]
- Le sous-menu **Préférences** > **Comptes** n'apparaît pas dans la fenêtre libre-service après avoir ajouté un magasin cloud pour la première fois. [RFLNX-3605]
- Le SDK d'optimisation de la plate-forme Linux ne fonctionne avec les versions 1908, 1910 et 1912 de l'application Citrix Workspace. Le problème se produit lorsque les binaires `wfica_for_plugins` sont supprimés du package d'installation de l'application Citrix Workspace. [RFLNX-4298]
- Lorsque vous ajoutez un magasin à l'aide de la commande **storebrowse**, celui-ci n'apparaît pas sur l'onglet **Préférences** > **Comptes**. Le problème se produit lorsque l'interface utilisateur en libre-service est en cours d'exécution sur le back-end. [RFLNX-3683]
- Dans une session, wfica peut se fermer de manière inattendue sur un site Web sur lequel la redirection de contenu du navigateur (BCR) est activée. Le problème se produit si vous définissez la valeur de **AllowMultiStream** sur **True**. [CVADHELP-13168]
- Dans une configuration à deux moniteurs, les tentatives de modification de l'affichage du bureau publié en mode plein écran peuvent échouer lorsque les moniteurs ont des résolutions différentes. [CVADHELP-13990]
- Vous pouvez rencontrer des problèmes d'affichage dans les sessions transparentes. Le problème se produit lorsque vous redimensionnez une fenêtre transparente ou basculez d'une fenêtre transparente à une autre. [CVADHELP-13458]
- Après avoir lancé une session de bureau à partir d'un magasin PNA, la fenêtre de la barre de

progression peut rester affichée, sauf si vous la fermez manuellement. [CVADHELP-14405]

Problèmes résolus dans la version 1912

- Sur Ubuntu 16.04 x64, l'icône de l'application Citrix Workspace peut apparaître de manière incorrecte dans la barre des tâches. [RFLNX-3582]
- Après avoir modifié le lien symbolique [symlink] de gst-play par gst-play1.0, les fichiers vidéo .mp4 peuvent être rendus avec un écran noir en arrière-plan et sans audio. [RFLNX-2429]
- Lorsque vous passez du mode économiseur d'écran au mode de session ICA plein écran, le clavier peut perdre le focus. Le problème se produit sur les appareils ArmHardFloat (armhf) qui s'exécutent sur le système d'exploitation Raspberry Pi. [RFLNX-3553]
- Lorsque vous utilisez l'interface utilisateur en libre-service, les options de la fenêtre **Préférences** peuvent ne pas fonctionner comme prévu. Le problème se produit lorsque le package libwebkit1 n'est pas disponible, comme c'est le cas avec les clients Debian 10 Buster. [RFLNX-3596]
- Lorsqu'un autre utilisateur système (et non le premier utilisateur) tente de lancer l'application Citrix Workspace, l'interface utilisateur en libre-service peut ne pas s'ouvrir et le message d'erreur suivant s'affiche :

  « Bind Error - address already in use. » (Erreur de liaison - Adresse déjà utilisée).

  [RFLNX-3601]
- Sur Ubuntu 18.04 et versions ultérieures, lorsque vous utilisez l'interface utilisateur en libre-service pour lancer des applications, l'application lancée est nommée « wfica_seamless », et non après l'application. Le problème se produit car l'environnement de bureau par défaut est GNOME. [RFLNX-3650]
- Lorsque vous vous déconnectez et que vous vous reconnectez avec un autre compte d'utilisateur, la page Accueil > Favoris affiche une liste incorrecte des applications préférées. [RFLNX-3458]
- Après avoir fermé l'interface utilisateur en libre-service, le message d'erreur suivant s'affiche :

  « free(): double free detected in tcache 2 Aborted. »

  Le problème se produit sur les appareils ArmHardFloat (armhf) qui s'exécutent sur le système d'exploitation Raspbian Buster. [RFLNX-3578]
- Lorsque la stratégie Expérience unifiée est désactivée, les applications désactivées peuvent toujours être énumérées dans l'application Citrix Workspace pour Linux. [CVADHELP-13742]
- Un lecteur USB amovible ne peut pas être mappé à un VDA sur le client CentOS 7.7. [CVADHELP-13422]

Problèmes résolus dans la version 1910

- L'application Citrix Workspace dépendait de libcurl3 pour l'installation. Avec ce correctif, la dépendance a été supprimée pour faciliter l'installation. [RFLNX-3487]
- Le rendu des données codées en H.264 avec le pack d'optimisation Video Decode and Presentation API for Unix (VDPAU) peut ne pas fonctionner comme prévu. [RFLNX-2892]
- Lorsque vous utilisez l'application Citrix Workspace pour Linux versions 1906 ou 1908, la page de connexion peut ne pas s'afficher lorsque des utilisateurs partagés se déconnectent de leur espace de travail. Au lieu de cela, l'invite de connexion suivante s'affiche : Connectez-vous pour accéder à votre Workspace. [RFLNX-3519]
- Lorsqu'une session de bureau s'étend sur plusieurs moniteurs, la barre d'outils peut disparaître. [RFLNX-3248]

Problèmes connus

Problèmes connus dans la version 2104

- Sur un VDA version 1912 LTSR CU2, les sessions peuvent être déconnectées. Le problème se produit lorsque vous activez la stratégie **Multistream** sur le Delivery Controller. Pour contourner le problème, mettez à niveau le VDA vers la version 2012 ou ultérieure. [RFLNX-6960]

Problèmes connus dans les versions précédentes

Problèmes connus dans la version 2103

- Lors d'un appel vidéo ou d'un partage d'écran, Microsoft Teams peut ne pas répondre et l'appel peut se terminer brusquement. [CVADHELP-16918]

Problèmes connus dans la version 2101

- Lors de la lecture de vidéos de longue durée, l'audio s'arrête mais la vidéo continue. Le problème se produit lorsque vous définissez `VdcamVersion4Support` sur `True`. Pour contourner le problème, désactivez l'option multi-audio en définissant `VdcamVersion4Support` sur `False`. [RFLNX-6472]
- Lors d'une réunion Microsoft Teams, l'audio peut être saccadé lorsqu'il est mis en mode muet. Le problème se produit sur les clients légers. [RFLNX-6537]
- Il peut arriver que l'application Citrix Workspace ne parvienne pas à lire les vidéos entrantes dans Microsoft Teams. [RFLNX-6662]
- Lorsque vous utilisez l'indicateur `cefenablemediadevices` avec Microsoft Teams, le microphone ne fonctionne pas comme prévu. Le problème se produit lors de l'utilisation de la fonctionnalité BCR basée sur CEF avec Microsoft Teams. [RFLNX-6689]

Problèmes connus dans la version 2012

- Lorsqu'une session est interrompue ou déconnectée brusquement, le processus `HdxRtcEngine.exe` peut se fermer de façon inattendue. [RFLNX-5885]
- Lorsque vous tentez de saisir du texte, le curseur s'affiche en blanc. Le problème se produit dans un scénario de double saut lorsque vous êtes connecté depuis une machine de point de terminaison Linux. Pour contourner le problème, consultez les articles CTX272423 et CTX131504 du centre de connaissances. [CVADHELP-16170]
- Lorsque vous établissez l'optimisation HDX pour un appel vidéo Microsoft Teams, la vidéo peut ne plus répondre et la lecture de l'audio s'interrompre. Le problème se produit lorsque vous déconnectez ou reconnectez un casque pendant l'appel. [CVADHELP-16186]

Problèmes connus dans la version 2010

- Impossible d'afficher les fichiers dans l'onglet **Fichiers**. Le problème se produit dans les déploiements cloud. [RFLNX-5596]
- Dans Microsoft Teams, vous devez sélectionner manuellement le périphérique audio. Le périphérique audio n'est pas défini automatiquement par défaut. [RFLNX-5652]
- Les tentatives d'utilisation du menu déroulant dans une session en mode plein écran peuvent échouer. Le problème se produit lorsque la redirection du contenu du navigateur est activée. [CVADHELP-13884]
- L'option de basculement vers TCP peut ne pas fonctionner même si `HDXoverUDP` est défini sur `Preferred`. Le problème se produit lorsque vous vous connectez à l'aide de Citrix Gateway. [CVADHELP-15526]

Problèmes connus dans la version 2009

- La fonctionnalité Multi-Stream ICA peut ne pas fonctionner correctement. [RFLNX-4286]
- Lorsque vous exécutez un appel vidéo ou que vous partagez l'écran dans Microsoft Teams, l'écran peut clignoter. [RFLNX-4778]
- Les tentatives de basculement entre les sessions de bureau peuvent échouer. [CVADHELP-15229]

Problèmes connus dans la version 2006

- Parfois, la vue **Réunion** n'est pas rétablie pendant le multitâche dans Microsoft Teams. Le problème se produit lorsqu'une fenêtre locale chevauche la fenêtre distante. Par conséquent, la fenêtre distante ne reçoit pas les événements de la souris. Comme solution de contournement, sur l'écran réduit, survolez l'horloge numérique avec la souris et double-cliquez sur le nom de l'appelant. [RFLNX-4937]

- Parfois, la reconnexion de session échoue. Le problème se produit lorsque vous configurez le protocole Multi-Stream ICA (MSI) avec un seul port sur TCP avec SD-WAN. [RFLNX-4782]

Problèmes connus dans la version 2004

- L'application Citrix Workspace pour Linux peut ne pas identifier certaines cartes à puce. Dans ce cas, les tentatives de lancement d'une session avec la carte échouent.
- Lorsque vous lancez une session après avoir activé le protocole ICA Multi-Stream (MSI) dans l'application Workspace et sur SD-WAN, la session se ferme de façon inattendue. Le message d'erreur suivant s'affiche :

  "La connexion au VDA a été perdue…"

  Le problème se produit car le MSI monoport n'est pas pris en charge. [RFLNX-4219]
- Le lancement de session peut échouer sur les distributions CentOS 8.x, Fedora 29, 30 et 31. Pour contourner le problème, consultez l'article CTX270926 du centre de connaissances. [RFLNX-3114]

Problèmes connus dans la version 1912

- Lors de l'utilisation de la redirection du contenu du navigateur basée sur CEF, le focus du clavier ne pointe pas vers la fenêtre principale si vous redirigez une URL. Pour contourner le problème, créez un onglet de navigateur et utilisez le bouton bascule pour accéder à l'onglet principal. [RFLNX-3871]
- Lors de l'utilisation de la redirection du contenu du navigateur basée sur CEF, vous pouvez observer une notification indiquant que le processus webcontainer s'est arrêté. Le problème se produit lorsque vous fermez l'instance du navigateur. [RFLNX-3872]
- Lorsque vous utilisez l'interface utilisateur en libre-service, les options de la fenêtre **Préférences** peuvent ne pas fonctionner comme prévu et l'application Workspace cesse temporairement de répondre. Le problème se produit sur la distribution Ubuntu 19.10. [RFLNX-3720]
- Les flux Workspace Intelligence ne sont pas pris en charge sur l'application Citrix Workspace version 1912.
- La redirection de webcam ne fonctionne pas avec Microsoft Teams. Il s'agit d'une limitation car Citrix ne prend pas en charge l'optimisation Microsoft Teams [MTOP] dans l'application Citrix Workspace pour Linux. [RFLNX-3674]

Problèmes connus dans la version 1910

- Lorsque vous utilisez l'interface utilisateur en libre-service, les options de la fenêtre **Préférences** peuvent ne pas fonctionner comme prévu. Le problème se produit lorsque

le package libwebkit1 n'est pas disponible, comme c'est le cas avec les clients Debian 10 Buster. Pour contourner la solution, supprimez la bibliothèque **UIdialoglibWebkit.so** située à l'intérieur du répertoire `install/path/lib`. [RFLNX-3596]

- En raison de modifications architecturales, vous ne pouvez plus vous connecter au magasin cloud [configuration de cloud]. Citrix vous recommande d'utiliser la dernière version de l'application Citrix Workspace.

Avis de tiers

L'application Citrix Workspace peut inclure un logiciel tiers distribué sous une licence selon les conditions définies dans le document suivant :

Avis de tiers de l'application Citrix Workspace pour Linux

Fonctionnalités expérimentales

À l'occasion, Citrix publie des fonctionnalités expérimentales afin de solliciter un commentaires des clients sur l'intérêt potentiel de nouvelles technologies ou fonctionnalités. Citrix n'offre pas de support pour les fonctionnalités expérimentales, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Citrix ne s'engage pas à intégrer de fonctionnalités expérimentales aux produits et peut les retirer pour quelque raison que ce soit à tout moment.

Conditions préalables à l'installation de l'application Citrix Workspace

June 10, 2021

Configuration système requise et compatibilité

Consultez la liste suivante pour connaître la configuration système requise :

Hardware	Requirements
Linux kernel	- Version 2.6.29 or later
Disk Space	- A minimum of 55 MB - Additional 110 MB if you expand/extract the installation package on the disk - A minimum of 1 GB RAM for system-on-a-chip (SoC) devices that use HDX MediaStream Flash Redirection
Color video display	- 256 color video display or higher

Libraries and Codec	Requirements
Libraries	- glibcxx 3.4.15 or later - glibc 2.11.3 or later - gtk 2.20.1 or later - libcap1 or libcap2 - libjson-c (for instrumentation) - GCC 4.8 for x64 * - GCC 4.9 for Armhf * - X11 or X.Org - udev support
Self-service user interface	- webkit2gtk 2.16.6 or later - libxml2 2.7.8 - libxerces-c 3.1
Codec libraries	- Advanced Linux Sound Architecture (ALSA) libasound2 - Speex - Vorbis codec libraries

Network	Requirements
Network protocol	- TCP/IP

Components	Requirements
H.264	For x86 devices: - A minimum processor speed of 1.6 GHz - Single-monitor sessions - Display resolutions for example, 1280 x 1024 pixels
	For the HDX 3D Pro feature: - A minimum processor speed of 2 GHz - A native hardware with accelerated graphics driver
	For ARM devices: - A hardware H.264 decoder is required for both general H.264 support and HDX 3D Pro **Note:** Performance improves after using faster processor clock speeds.
HDX MediaStream Flash Redirection	For all HDX MediaStream Flash Redirection requirements, see Knowledge Center article http://support.citrix.com/article/CTX134786. Citrix recommends testing with the latest plug-in before deploying a new version to take advantage of the latest functionality and security-related fixes.
Customer Experience Improvement Program (CEIP) integration	- zlib 1.2.3.3 - libtar 1.2 and later - libjson 7.6.1 or later

Components	Requirements
HDX RealTime Webcam Video Compression	- A Video4Linux compatible Webcam - GStreamer 0.10.25 (or a later 0.10.x version), including the distribution's "plugins-good" package Or GStreamer 1.0 (or a later 1.x version), including the distribution's “plugins-base,” “plugins-good,” “plugins-bad,” “plugins-ugly,” and “gstreamer-libav” packages
HDX MediaStream Windows Media Redirection	- GStreamer 0.10.25 (or a later 0.10.x version), including the distribution's "plugins-good" package. In general, version 0.10.15 or later is sufficient for HDX MediaStream Windows Media Redirection Or GStreamer 1.0 (or a later 1.x version), including the distribution's “plugins-base,” “plugins-good,” “plugins-bad,” “plugins-ugly,” and “gstreamer-libav” packages **Note:** If GStreamer is not included in your Linux distribution, you can download it from https://gstreamer.freedesktop.org/download/. Use of certain codes (for example, those in "plugins-ugly") might require a license from the manufacturer of that technology. Contact your system administrator for help.

Components	Requirements
Browser content redirection	- webkit2gtk version 2.16.6 - glibcxx 3.4.20 or later
Philips SpeechMike	- Visit the Philips web site to install the relevant drivers
Microsoft Teams Optimization	- Software o GStreamer 1.0 or later and Cairo 2 o libc++-9.0 or later o libgdk 3.22 or later o OpenSSL 1.1.1d o x64 Linux distribution - Hardware o Minimum 1.8 GHz dual-core CPU that can support 720p HD resolution during a peer-to-peer video conference call. o Dual or quad-core CPU with a base speed of 1.8 GHz and a high Intel Turbo Boost speed of at least 2.9 GHz.
Authentication enhancement	- Libsecret library

* À partir de la version 1910, l'application Citrix Workspace pour Linux peut ne pas fonctionner comme prévu sauf si le système d'exploitation répond aux critères de version de GCC suivants :

- Version GCC pour architecture x64 : 4.8 ou version ultérieure
- Version GCC pour architecture ARMHF : 4.9 ou version ultérieure

> **Remarque**
>
> À partir de la version 2101, l'application Citrix Workspace pour Linux peut ne pas fonctionner comme prévu, sauf si le système d'exploitation répond aux exigences suivantes :
>
> - GCC version 4.9 ou ultérieure
> - glibcxx 3.4.20 ou version ultérieure

Matrice de compatibilité

L'application Citrix Workspace pour Linux est compatible avec toutes les versions actuellement prises en charge des produits Citrix. Pour de plus amples informations sur le cycle de vie des produits Citrix et savoir quand Citrix arrête la prise en charge de versions spécifiques des produits, consultez le tableau du cycle de vie des produits Citrix.

Éléments requis sur les serveurs

StoreFront

- Vous pouvez utiliser toutes les versions de l'application Citrix Workspace prises en charge pour accéder aux magasins StoreFront à partir de connexions au réseau interne et via Citrix Gateway :
  - StoreFront 1811 et versions ultérieures.
  - StoreFront 3.12.
- Vous pouvez utiliser StoreFront configuré avec Workspace pour Web. Workspace pour Web permet d'accéder aux magasins StoreFront à partir d'un navigateur Web. Pour prendre connaissance des limitations de ce déploiement, consultez Remarques importantes dans la documentation StoreFront.

Connexions et Certificats

Connexions

L'application Citrix Workspace pour Linux prend en charge les connexions HTTPS et ICA-over-TLS par le biais des configurations suivantes.

- Pour les connexions LAN :
  - StoreFront avec StoreFront Services ou Workspace pour Web
- Pour les connexions sécurisées à distance ou locales :
  - Citrix Gateway 12.0
  - Netscaler Gateway 10.1 et versions ultérieures
  - Netscaler Access Gateway Enterprise Edition 10
  - Netscaler Access Gateway Enterprise Edition 9.x
  - Netscaler Access Gateway VPX

  Pour plus d'informations sur les versions de Citrix Gateway prises en charge par StoreFront, reportez-vous à la section Configuration système requise de StoreFront.

Certificats

Pour garantir la sécurité des transactions entre le serveur et le client, utilisez les certificats suivants :

Certificats privés (auto-signés)

Si un certificat privé est installé sur la passerelle distante, le certificat racine de l'autorité de certification doit être installé sur l'appareil de façon à pouvoir accéder aux ressources Citrix à l'aide de l'application Citrix Workspace.

> **Remarque :**
>
> Si le certificat de la passerelle distante ne peut pas être vérifié lors de la connexion (car le certificat racine n'est pas inclus dans le magasin de clés local), un avertissement relatif à un certificat non approuvé s'affiche. Si un utilisateur choisit d'ignorer l'avertissement, les applications s'affichent, mais ne démarrent pas. Le certificat racine doit être installé dans le magasin de certificats du client.

Certificats racines

Pour les ordinateurs appartenant à un domaine, vous pouvez utiliser le modèle d'administration d'objet de stratégie de groupe pour distribuer et approuver les certificats d'autorité de certification.

Pour les ordinateurs n'appartenant pas à un domaine, l'organisation peut créer un pack d'installation personnalisé pour distribuer et installer le certificat d'autorité de certification. Contactez votre administrateur système pour obtenir de l'aide.

Installer des certificats racine sur des machines utilisateur

Pour utiliser le protocole TLS, vous devez disposer d'un certificat racine sur la machine cliente permettant de vérifier la signature de l'autorité de certification apposée sur le certificat du serveur. Par défaut, l'application Citrix Workspace prend en charge les certificats suivants.

Certificat	Autorité émettrice
Class4PCA_G2_v2.pem	VeriSign Trust Network
Class3PCA_G2_v2.pem	VeriSign Trust Network
BTCTRoot.pem	Baltimore Cyber Trust Root
GTECTGlobalRoot.pem	GTE Cyber Trust Global Root
Pcs3ss_v4.pem	Class 3 Public Primary Certification Authority
GeoTrust_Global_CA.pem	GeoTrust
DigiCertGlobalRootCA.pem	DigiCert Global Root CA

Certificats génériques

Les certificats génériques remplacent les certificats de serveur individuel pour n'importe quel serveur situé dans le même domaine. L'application Citrix Workspace pour Linux prend en charge les certificats génériques, toutefois, ils doivent être uniquement utilisés conformément à la stratégie de sécurité de votre organisation. En pratique, des alternatives aux certificats génériques existent, par exem-

ple un certificat qui contient la liste des noms de serveurs dans l'extension SAN (Subject Alternative Name) peut être pris en compte. Ce type de certificat peut être émis par des autorités de certification publiques et privées.

Certificats intermédiaires et Citrix Gateway

Si votre chaîne de certificat contient un certificat intermédiaire, ce dernier doit être ajouté au certificat serveur de Citrix Gateway. Pour plus d'informations, reportez-vous à la section Configuration de certificats intermédiaires de la documentation Citrix Gateway.

Si votre serveur StoreFront ne peut pas fournir les certificats intermédiaires correspondant au certificat qu'il utilise, ou que vous installez des certificats intermédiaires pour prendre en charge des utilisateurs de cartes à puce, suivez ces étapes avant d'ajouter un magasin StoreFront :

1. Obtenez le ou les certificats intermédiaires séparément au format PEM.

   > **Conseil :**
   >
   > Si vous ne trouvez aucun certificat de format PEM, utilisez l'utilitaire openssl pour convertir un certificat au format CRT en un fichier .pem.

2. En tant qu'utilisateur, installez le package (généralement racine) :
   a) Copiez le ou les fichiers dans $ICAROOT/keystore/intcerts.
   b) Exécutez la commande suivante en tant qu'utilisateur qui a installé le package :

   ```
   $ICAROOT/util/ctx_rehash
   ```

Stratégie de validation des certificats de serveur

La stratégie de validation des certificats de serveur de l'application Citrix Workspace pour Linux est plus stricte.

> **Important :**
>
> Avant d'installer l'application Citrix Workspace pour Linux, vérifiez que les certificats sur le serveur ou la passerelle sont correctement configurés comme indiqué ci-dessous. Les connexions peuvent échouer si :
>
> - la configuration du serveur ou de la passerelle inclut un certificat racine incorrect ;
> - la configuration du serveur ou de la passerelle n'inclut pas tous les certificats intermédiaires ;
> - la configuration du serveur ou de la passerelle inclut un certificat intermédiaire expiré ou non valide ;

> - la configuration du serveur ou de la passerelle inclut un certificat intermédiaire avec signature croisée.

Lors de la validation d'un certificat de serveur, l'application Citrix Workspace pour Linux utilise maintenant **tous** les certificats fournis par le serveur (ou la passerelle). Comme dans les versions précédentes de l'application Citrix Workspace pour Linux, il vérifie également que les certificats sont approuvés. Si les certificats ne sont pas tous approuvés, la connexion échoue.

Cette stratégie est plus stricte que la stratégie de certificat des navigateurs web. De nombreux navigateurs Web comprennent un grand nombre de certificats racine auxquels ils font confiance.

Le serveur (ou la passerelle) doit être configuré avec le jeu correct de certificats. Un jeu incorrect de certificats peut entraîner l'échec de la connexion de l'application Citrix Workspace pour Linux.

Supposons qu'une passerelle soit configurée avec ces certificats valides. Cette configuration est recommandée pour les clients qui requièrent une validation stricte, en déterminant précisément quel certificat racine est utilisé par l'application Citrix Workspace pour Linux :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »
- « Certificat racine exemple »

L'application Citrix Workspace pour Linux vérifie ensuite que tous ces certificats sont valides. L'application Citrix Workspace pour Linux vérifie également qu'il fait déjà confiance à « Certificat racine exemple ». Si l'application Citrix Workspace pour Linux ne fait pas confiance à « Certificat racine exemple », la connexion échoue.

> **Important :**
>
> - Certaines autorités de certification disposent de plus d'un certificat racine. Si vous avez besoin de cette validation plus stricte, assurez-vous que votre configuration utilise le certificat racine approprié. Par exemple, il existe actuellement deux certificats (« DigiCert »/« GTE CyberTrust Global Root » et « DigiCert Baltimore Root »/« Baltimore CyberTrust Root ») qui peuvent valider les mêmes certificats de serveur. Sur certaines machines utilisateur, les deux certificats racine sont disponibles. Sur les autres machines, seul (« DigiCert Baltimore Root »/« Baltimore CyberTrust Root ») est disponible. Si vous configurez « GTE CyberTrust Global Root » sur la passerelle, les connexions de l'application Citrix Workspace pour Linux sur ces machines utilisateur échouent. Consultez la documentation de l'autorité de certification pour déterminer quel certificat racine doit être utilisé. Notez également que les certificats racine finissent par expirer, comme tous les certificats.
> - Certains serveurs et certaines passerelles n'envoient jamais le certificat racine, même si cela est configuré. Une validation plus stricte n'est par conséquent pas possible.

Supposons maintenant qu'une passerelle soit configurée avec ces certificats valides. Cette configuration, qui ignore le certificat racine, est généralement recommandée :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »

L'application Citrix Workspace pour Linux utilise ensuite ces deux certificats. Il recherche ensuite un certificat racine sur la machine utilisateur. Si elle en trouve un qui est validé et également approuvé (tel que « Certificat racine exemple »), la connexion réussit. Sinon, la connexion échoue. Cette configuration fournit le certificat intermédiaire dont l'application Citrix Workspace pour Linux a besoin, mais permet également à l'application Citrix Workspace pour Linux de choisir un quelconque certificat racine valide et approuvé.

Supposons maintenant qu'une passerelle soit configurée avec ces certificats :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »
- « Certificat racine incorrect »

Un navigateur Web peut ignorer le certificat racine incorrect. Toutefois, l'application Citrix Workspace pour Linux n'ignore pas le certificat racine incorrect et la connexion échoue.

Certaines autorités de certification disposent de plus d'un certificat intermédiaire. Dans ce cas, la passerelle est généralement configurée avec tous les certificats intermédiaires (mais pas le certificat racine) tels que :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple 1 »
- « Certificat intermédiaire exemple 2 »

> **Important :**
>
> - Certaines autorités de certification utilisent un certificat intermédiaire avec signature croisée. Ce cas de figure est destiné aux situations dans lesquelles il existe plus d'un certificat racine, et qu'un certificat racine antérieur est toujours en cours d'utilisation en même temps qu'un certificat racine plus récent. Dans ce cas, il y aura au moins deux certificats intermédiaires. Par exemple, le certificat racine antérieur « Class 3 Public Primary Certification Authority » et le certificat intermédiaire avec signature croisée « VeriSign Class 3 Public Primary Certification Authority - G5 » correspondant. Toutefois, un certificat racine antérieur « VeriSign Class 3 Public Primary Certification Authority - G5 » correspondant est également disponible, et il remplace « Class 3 Public Primary Certification Authority ». Le certificat racine antérieur n'utilise pas de certificat intermédiaire avec signature croisée.
> - Le certificat intermédiaire avec signature croisée et le certificat racine ont le même nom de sujet (Délivré à). Cependant le certificat intermédiaire avec signature croisée a un nom d'émetteur différent (Délivré par). Cela permet de différencier le certificat intermédiaire

> avec signature croisée d'un certificat intermédiaire ordinaire (tel « Certificat intermédiaire exemple 2 »).

Cette configuration, qui ignore le certificat racine et le certificat intermédiaire avec signature croisée, est généralement recommandée :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »

Évitez de configurer la passerelle de manière à utiliser le certificat intermédiaire avec signature croisée, car cela entraîne la sélection du certificat racine antérieur :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »
- « Certificat intermédiaire croisé exemple » [non recommandé]

Il n'est pas recommandé de configurer la passerelle avec le certificat de serveur uniquement :

- « Certificat de serveur exemple »

Dans ce cas, si l'application Citrix Workspace pour Linux ne peut pas trouver tous les certificats intermédiaires, la connexion échoue.

Hdxcheck

Citrix fournit un script, hdxcheck.sh, disponible dans le package d'installation de l'application Citrix Workspace. Le script vérifie que votre machine répond à toutes les exigences de configuration afin qu'elle puisse bénéficier de toutes les fonctionnalités de l'application Citrix Workspace pour Linux. Ce script se trouve dans le répertoire `Utilities` du pack d'installation.

Pour exécuter le script hdxcheck.sh

1. Ouvrez le terminal de votre machine Linux.
2. Tapez `cd $ICAROOT/util` et appuyez sur **Entrée** pour accéder au répertoire `Utilities` du pack d'installation.
3. Tapez `./hdxcheck.sh` pour exécuter le script.

Installer, désinstaller et mettre à niveau

May 4, 2021

Vous pouvez installer l'application Citrix Workspace en utilisant l'une des méthodes suivantes :

- Téléchargez l'application Citrix Workspace depuis Téléchargements de Citrix.
- Déployez l'application Citrix Workspace à l'aide de Workspace pour Web (configuration avec StoreFront).

Installation manuelle

Téléchargez les packages suivants à partir de la page Téléchargements de Citrix.

Packages Debian

Installez l'un des packages `Icaclient` ou l'un des packages `IcaclientWeb` en fonction de votre architecture d'OS.

Pour utiliser la redirection USB générique, installez l'un des packages `ctxusb` basés sur votre architecture d'OS.

Nom du package	Contenu
Packages Debian (Ubuntu, Debian, Linux Mint etc.)	
icaclient_20.06.0.15_amd64.deb	Prise en charge du libre-service, 64 bits x86_64
icaclient_20.06.0.15_i386.deb	Prise en charge du libre-service, 32 bits x86
icaclient_20.06.0.15_armhf.deb	Prise en charge du libre-service, ARM HF
icaclientWeb_20.06.0.15_amd64.deb	Receiver Web uniquement, 64 bits x86_64
icaclientWeb_20.06.0.15_i386.deb	Receiver Web uniquement, 32 bits x86
icaclientWeb_20.06.0.15_armhf.deb	Receiver Web uniquement, ARM HF
ctxusb_20.06.0.15_amd64.deb	Package USB, 64 bits x86_64
ctxusb_20.06.0.15_i386.deb	Package USB, 32 bits x86
ctxusb_20.06.0.15_armhf.deb	Package USB, ARM HF

Installer à l'aide d'un package Debian

Lorsque vous installez l'application Citrix Workspace à l'aide du package Debian sur Ubuntu, ouvrez les packages dans Ubuntu Software Centre.

Dans les instructions suivantes, remplacez
nomdupackage par le nom du package que vous installez.

Cette procédure utilise une ligne de commande et le gestionnaire de package natif pour Ubuntu/De-

bian/Mint. Vous pouvez également installer le package en cliquant deux fois sur le package .deb téléchargé dans un navigateur de fichiers. Cette opération démarre un gestionnaire de package qui télécharge tous les logiciels requis manquants. Si aucun gestionnaire de packages n'est disponible, Citrix vous recommande d'utiliser **gdebi**, un outil de ligne de commande.

> **Conditions préalables :**
>
> Vous devez installer le package `icaclient` ou le package `icaclientWeb`.

Pour installer le package à l'aide de la ligne de commande :

1. Ouvrez une session en tant qu'utilisateur (racine) privilégié.
2. Ouvrez une fenêtre de terminal.
3. Exécutez l'installation pour les trois packages suivants en tapant `gdebi packagename.deb`. Par exemple :
   - `gdebi icaclient\\_19.0.6.6\\_amd64.deb`
   - `gdebi icaclientWeb\\_19.0.6.6\\_i386.deb`
   - `gdebi ctxusb\\_2.7.6\\_amd64.deb`

   Pour utiliser `dpkg` dans les exemples ci-dessus, remplacez `gdebi` par `dpkg -i`.

   Si vous utilisez `dpkg`, installez toutes les dépendances manquantes en tapant `sudo apt-get -f install`..

   > **Remarque :**
   >
   > - Le package `ctxusb` est facultatif. Il permet de prendre en charge la redirection USB générique.
   > - À partir de la version 2101, une invite interactive vous demande d'installer la protection des applications.
4. Acceptez le EULA.

Installation du composant de protection des applications sur les packages Debian :

À partir de la version 2102, la protection des applications est prise en charge sur la version Debian de l'application Citrix Workspace.

Pour installer de façon silencieuse le composant de protection d'application, exécutez la commande suivante à partir du terminal avant d'installer l'application Citrix Workspace :

```
1 `export DEBIAN_FRONTEND="noninteractive"`
2
3 `sudo debconf-set-selections <<< "icaclient app_protection/
     install_app_protection select no"`
```



```
4
5 `sudo debconf-show icaclient`
6
7 `sudo apt install -f ./icaclient_<version>._amd64.deb`
```

Packages Red Hat

Installez l'un des packages `ICAClient` ou l'un des packages `ICAClientWeb` en fonction de votre architecture d'OS.

Pour utiliser la redirection USB générique, installez l'un des packages `ctxusb` basés sur votre architecture d'OS.

Nom du package	Contenu
Packages Redhat (Redhat, SUSE, Fedora etc.)	
ICAClient-rhel-20.06.0.15-0.x86_64.rpm	Prise en charge du libre-service, Red Hat (y compris VDA Linux), 64 bits x86_64
ICAClient-rhel-20.06.0.15-0.i386.rpm	Prise en charge du libre-service, Red Hat, 32 bits x86
ICAClientWeb-rhel-20.06.0.15-0.x86_64.rpm	Receiver pour Web uniquement, Red Hat, 64 bits x86_64
ICAClientWeb-rhel-20.06.0.15-0.i386.rpm	Receiver pour Web uniquement, Red Hat, 32 bits x86
ICAClient-suse-20.06.0.15-0.x86_64.rpm	Prise en charge du libre-service, SUSE, 64 bits x86_64
ICAClient-suse-20.06.0.15-0.i386.rpm	Prise en charge du libre-service, SUSE, 32 bits x86
ICAClientWeb-suse-20.06.0.15-0.x86_64.rpm	Receiver Web uniquement, SUSE, 64 bits x86_64
ICAClientWeb-suse-20.06.0.15-0.i386.rpm	Receiver Web uniquement, SUSE, 32 bits x86
ctxusb-20.06.0.15-1.x86_64.rpm	Package USB, 64 bits x86_64
ctxusb-20.06.0.15-1.i386.rpm	Package USB, 32 bits x86

> **Remarque :**
>
> Le *package RPM SuSE 11 SP3 Full Package (Self-Service Support)* est obsolète.

Installer à l'aide d'un package RPM

Si vous installez l'application Citrix Workspace à partir du package RPM sur SUSE, utilisez l'utilitaire YaST ou Zypper. L'utilitaire RPM installe le package .rpm. Une erreur se produit si les dépendances requises sont manquantes.

Pour définir le référentiel EPEL sur Red Hat

Téléchargez le package RPM source approprié depuis : https://fedoraproject.org/wiki/EPEL#Extra_Packages_for_Enterprise_Linux_.28EPEL.29.

Pour plus d'informations sur son utilisation, consultez https://fedoraproject.org/wiki/EPEL#How_can_I_use_these_extra_packages.3F

Par exemple, sur Red Hat Enterprise 7.x, vous pouvez installer le référentiel EPEL à l'aide de la commande :

```
1 `yum localinstall epel-release-latest-7.noarch.rpm`
```

> **Conseil :**
>
> RPM Package Manager n'installe pas les logiciels requis manquants. Pour télécharger et installer le logiciel, nous vous recommandons d'utiliser **zypper install <nom de fichier>** sur une ligne de commande sur OpenSUSE ou **yum localinstall <nom de fichier>** sur Fedora/Red Hat.

Pour installer à partir du package RPM

> **Conditions préalables :**
>
> Vous devez installer le package `icaclient` ou le package `icaclientWeb`.

1. Configurez le référentiel EPEL.
2. Ouvrez une session en tant qu'utilisateur (racine) privilégié.
3. Exécutez l'installation pour les trois packages suivants en tapant zypper dans .

   > **Remarque :**
   >
   > - `ctxusb` est un package facultatif. Installez le package pour prendre en charge la redirection USB générique.
   > - `ctxappprotection` est un package facultatif. Installez le package uniquement si vous souhaitez installer le composant de protection des applications.

4. Ouvrez une fenêtre de terminal.

   Pour les installations SUSE :

- `zypper in ICAClient-suse-19.12.0.19-0.x86_64.rpm`
- `zypper in ICAClient-suse-19.12.0.19-0.i386.rpm`
- `zypper in ctxusb-2.7.19-1.x86\\_64.rpm`
- `zypper in ctxappprotection-21.4.0.2-0.x86_64.rpm`

Pour les installations Red Hat :

- `yum localinstall ICAClient-rhel-19.12.0.19-0.i386.rpm`
- `yum localinstall ICAClientWeb-rhel-19.12.0.19-0.i386.rpm`
- `yum localinstall ctxusb-2.7.19-1.i386.rpm`
- `yum localinstall ctxappprotection-21.4.0.2-0.x86_64.rpm`

5. Acceptez le EULA.

Pour installer un package manquant

Sur une distribution basée sur Red Hat (RHEL, CentOS, Fedora, etc.), si le message d'erreur suivant s'affiche :

```
1  "… requires libwebkitgtk-1.0.so.0"
```

ajoutez un référentiel EPEL (les détails sont disponibles sur https://fedoraproject.org/wiki/EPEL).

Packages Tarball

Installez l'un des packages suivants en fonction de votre architecture d'OS.

Nom du package	Contenu
Tarballs (installation par script pour n'importe quelle distribution)	
linuxx64-20.06.0.15.tar.gz	Intel 64 bits
linuxx86-20.06.0.15.tar.gz	Intel 32 bits
linuxarmhf-20.06.0.15.tar.gz	ARM HF

La différence entre les packages qui offrent la prise en charge de l'application Workspace pour Web et ceux qui offrent la prise en charge du libre-service tient au fait que ces derniers comprennent des dépendances requises pour le libre-service en plus de celles requises pour l'application

Workspace pour Web. Les dépendances du libre-service sont un sur-ensemble de celles requises pour l'application Workspace pour Web, mais les fichiers installés sont identiques.

- Si vous n'avez besoin que de l'application Workspace pour Web, ou que votre distribution ne dispose pas des packages nécessaires pour prendre en charge le libre-service, installez uniquement le package de l'application Workspace pour Web.
- Sinon, installez l'application Citrix Workspace à partir du package Debian ou RPM. Ces fichiers sont plus faciles à utiliser, car ils installent automatiquement tout autre package requis.
- Si vous souhaitez personnaliser l'emplacement d'installation, installez l'application Citrix Workspace à l'aide du package tarball.

> **Remarque :**
>
> - N'utilisez pas les deux méthodes d'installation sur la même machine. Si vous le faites, vous risquez de voir des messages d'erreur et des comportements indésirables.

Installer à l'aide d'un package Tarball

> **Remarque :**
>
> Le package tarball ne vérifie pas les dépendances et n'installe pas non plus les dépendances. Toutes les dépendances système doivent être résolues indépendamment.

1. Ouvrez une fenêtre de terminal.
2. Décompressez le contenu du fichier `.tar.gz` dans un répertoire vide. Par exemple, tapez : `tar xvfz packagename.tar.gz`.
3. Tapez `./setupwfc` et appuyez sur Entrée pour exécuter le programme d'installation.
4. Acceptez la valeur par défaut de `1` (pour installer l'application Citrix Workspace) et appuyez sur **Entrée**.
5. Saisissez le chemin d'accès et le nom du répertoire d'installation requis et appuyez sur Entrée, ou appuyez sur Entrée pour installer l'application Citrix Workspace dans l'emplacement par défaut.

   Pour un utilisateur (racine) privilégié, le répertoire d'installation par défaut est `/opt/Citrix/ICAClient`.

   Pour un utilisateur non privilégié, le répertoire d'installation par défaut est `$HOME/ICAClient/platform`. La plate-forme est un identifiant généré par le système pour le système d'exploitation installé, par exemple `$HOME/ICAClient/linuxx86` pour la plate-forme Linux/x86.

   > **Remarque :**
   >
   > Si vous spécifiez un emplacement autre que celui par défaut, définissez-le dans $ICAROOT

> dans `$HOME/.profile` ou `$HOME/.bash\\_profile`.

6. Lorsque vous êtes invité à continuer, tapez `y` et appuyez sur Entrée.
7. Vous pouvez choisir d'intégrer ou non l'application Citrix Workspace à votre environnement de bureau. L'installation crée une option de menu à partir de laquelle les utilisateurs peuvent démarrer l'application Citrix Workspace. Tapez `y` lorsque vous y êtes invité pour activer l'intégration.
8. Si vous avez déjà installé GStreamer, vous pouvez choisir de l'intégrer à l'application Citrix Workspace, ce qui permet la prise en charge de l'accélération multimédia HDX MediaStream. Pour intégrer GStreamer à l'application Citrix Workspace, tapez `y` lorsque vous y êtes invité.

   > **Remarque :**
   >
   > Sur certaines plates-formes, l'installation du client à partir d'un package tarball peut entraîner le blocage du système après la demande d'intégration avec KDE et GNOME. Ce problème se produit lors de la première initialisation de gstreamer-0.10. Si vous rencontrez ce problème, mettez fin au processus d'installation (à l'aide de ctrl+c) et exécutez la commande `gst-inspect-0.10 -- gst-disable-registry-fork --version`. Après avoir exécuté la commande, vous pouvez réexécuter le package tarball sans rencontrer le problème.

9. Si vous avez ouvert une session en tant qu'utilisateur (racine) privilégié, choisissez d'installer la prise en charge USB pour les applications VDI publiées de Citrix Virtual Apps and Desktops. Tapez `y` lorsque vous y êtes invité pour installer la prise en charge USB.

   > **Remarque :**
   >
   > Si vous n'avez pas ouvert de session en tant qu'utilisateur (racine) privilégié, l'avertissement suivant s'affiche :
   >
   > "USB support cannot be installed by non-root users. Run the installer as root to access this install option."

10. Une fois l'installation terminée, le menu d'installation principal s'affiche à nouveau. Pour quitter le programme d'installation, tapez `3` et appuyez sur Entrée.

Désinstallation

Cette procédure a été testée avec le pack tarball. Supprimez les packages RPM et Debian à l'aide des outils standard de votre système d'exploitation.

La variable d'environnement ICAROOT doit être définie sur le répertoire d'installation du client. Pour un utilisateur non privilégié, le répertoire d'installation par défaut est `$HOME/ICAClient/platform`. La variable de plate-forme est un identifiant généré par le système pour le système d'exploitation

installé, par exemple `$HOME/ICAClient/linuxx86` pour la plate-forme Linux/x86. L'installation de l'utilisateur privilégié se fait par défaut sur `/opt/Citrix/ICAClient`.

> **Remarque :**
>
> Pour désinstaller l'application Citrix Workspace, vous devez être connecté avec les mêmes informations d'identification utilisateur que celles avec lesquelles vous avez réalisé l'installation.

Pour désinstaller le package tarball

1. Exécutez le programme d'installation en tapant `$ICAROOT/setupwfc` et appuyez sur Entrée.
2. Pour supprimer le client, tapez sur 2 puis appuyez sur **Entrée**.

Mise à niveau

Pour mettre à niveau Citrix Receiver vers l'application Citrix Workspace, téléchargez et installez la dernière application Citrix Workspace à partir de la page Téléchargements de Citrix.

Lorsque vous démarrez l'application pour la première fois, que vous effectuez une mise à niveau ou que vous désinstallez puis réinstallez l'application, la superposition d'écrans de **Citrix Workspace** s'affiche. Cliquez sur **OK** pour continuer à utiliser l'application Citrix Workspace, ou cliquez sur **En savoir plus** pour obtenir plus d'informations.

Mise en route

May 4, 2021

Configurer

Vous pouvez télécharger le package d'installation, personnaliser la configuration, puis installer l'application Citrix Workspace. Vous pouvez modifier le contenu du package de l'application Citrix Workspace, puis reconditionner les fichiers.

Personnaliser l'installation

1. Décompressez le fichier du package de l'application Citrix Workspace dans un répertoire vide. Le fichier du package est appelé platform.major.minor.release.build.tar.gz (par exemple, linuxx86.13.2.0.nnnnnn.tar.gz pour la plate-forme Linux/x86).
2. Apportez les modifications requises au package de l'application Citrix Workspace. À titre d'exemple, vous pouvez ajouter un certificat racine TLS pour utiliser un certificat à partir d'une

autorité de certification ne faisant pas partie de l'installation standard de l'application Citrix Workspace.

3. Ouvrez le fichier `PkgID`.
4. Ajoutez la ligne suivante pour indiquer que le pack a été modifié :

   MODIFIED=traceinfo

   où `traceinfo` est l'information indiquant la personne responsable de la modification et le moment où cette dernière a été réalisée.
5. Enregistrez, puis fermez le fichier.
6. Ouvrez la liste des fichiers de package, platform/platform.psf (par exemple, linuxx86/linuxx86.psf pour la plate-forme Linux/x86).
7. Actualisez la liste des fichiers du package pour refléter les modifications que vous avez apportées au package. Si la liste n'est pas actualisée, une erreur peut se produire lors de l'installation du nouveau package. Ces modifications peuvent inclure la mise à jour de la taille des fichiers que vous avez modifiés ou l'ajout de nouvelles lignes pour tous les fichiers ajoutés au package. Les colonnes de la liste des fichiers du package sont :
   - Type de fichier
   - Chemin d'accès relatif
   - Sous-package (qui doit toujours être défini sur `cor`)
   - Autorisations
   - Propriétaire
   - Groupe
   - Taille
8. Enregistrez, puis fermez le fichier.
9. Utilisez la commande tar pour reconstruire le fichier de package de l'application Citrix Workspace. Par exemple, `tar czf ../newpackage.tar.gz *`, où `newpackagez` est le nom du nouveau fichier de package de l'application Citrix Workspace.

Dernière prise en charge du webkit

L'application Citrix Workspace pour Linux requiert libwebkit2gtk (2.16.6+).

libwebkit2gtk présente les avantages suivants :

- Amélioration de l'expérience de l'interface utilisateur : webkit2gtk est compatible avec la fonctionnalité de redirection du contenu du navigateur. Utilisez webkit2gtk version 2.24 ou ultérieure pour bénéficier d'une expérience visuelle sur YouTube encore meilleure.
- Le webkit2gtk version 2.16.6 et versions ultérieures améliore l'expérience de connexion et le temps nécessaire pour se connecter.

- L'application fonctionne mieux avec les nouvelles distributions Linux et fournit les derniers correctifs de sécurité webkit.

> **Remarque :**
>
> webkit2gtk n'est pas disponible sur certaines distributions Linux. Pour contourner le problème, envisagez les options suivantes :
>
> - Créez webkit2gtk à partir de la source avant d'installer l'application Citrix Workspace 1906.
> - Téléchargez le package Web à partir de la page Téléchargements. Seuls les lancements Web sont pris en charge dans ce package.
> - Passez à une distribution Linux plus récente prenant en charge webkit2gtk 2.16.6 ou version ultérieure.

Launch

Vous pouvez démarrer l'application Citrix Workspace soit à l'invite du terminal soit à partir de l'un des environnements de bureau pris en charge.

Assurez-vous que la variable d'environnement `ICAROOT` est définie de manière à pointer vers le répertoire d'installation réel.

> **Conseil :**
>
> L'instruction suivante ne s'applique pas aux installations effectuées à partir de packages Web ou du package tarball mais dans les cas où les exigences Self-Service n'ont pas été respectées.

Invite de terminal

Pour démarrer l'application Citrix Workspace à l'invite du terminal, tapez :
`/opt/Citrix/ICAClient/selfservice`

et appuyez sur Entrée (où /opt/Citrix/ICAClient est le répertoire dans lequel vous avez installé l'application Citrix Workspace).

Bureau Linux

Vous pouvez démarrer l'application Citrix Workspace à partir d'un environnement de bureau à l'aide d'un gestionnaire de fichiers.

Sur certains bureaux, vous pouvez également démarrer l'application Citrix Workspace à partir d'un menu. L'application Citrix Workspace peut se trouver dans différents menus, en fonction de votre distribution Linux.

Préférences

Pour définir les préférences, cliquez sur **Préférences** dans le menu de l'application Citrix Workspace. Vous pouvez contrôler la façon dont les bureaux sont affichés, vous connecter à différentes applications et différents bureaux, et gérer l'accès aux périphériques et fichiers.

Gérer un compte

Pour accéder aux bureaux et applications, vous devez disposer d'un compte avec XenDesktop ou Citrix Virtual Apps. Votre service d'assistance informatique peut vous demander d'ajouter un compte à Citrix Workspace à cette fin. Il peut également vous demander d'utiliser un autre serveur Citrix Gateway ou Access Gateway pour un compte existant. Vous pouvez également supprimer des comptes à partir de Citrix Workspace.

1. Sur la page **Comptes** de la boîte de dialogue **Préférences**, effectuez l'une des opérations suivantes :
   - Pour ajouter un compte, cliquez sur **Ajouter**. Contactez votre administrateur système pour plus d'informations.
   - Pour modifier les détails d'un magasin utilisé par le compte, tels que la passerelle par défaut, cliquez sur **Modifier**.
   - Pour supprimer un compte, cliquez sur **Supprimer**.
2. Suivez les instructions à l'écran. Authentifiez-vous auprès du serveur lorsque vous y êtes invité.

Affichage de bureau

> **Remarque :**
>
> Cette fonctionnalité n'est pas disponible avec les sessions Citrix Virtual Apps pour UNIX.

Vous pouvez afficher des bureaux sur l'intégralité de l'écran de votre machine utilisateur (mode plein écran), qui est la valeur par défaut, ou dans une fenêtre distincte (mode fenêtre).

- Sur la page **Général** de la boîte de dialogue **Préférences**, sélectionnez un mode à l'aide de l'option **Afficher les bureaux en**.

Utilisez la fonctionnalité de la barre d'outils **Vous pouvez activer Desktop Viewer** pour modifier de manière dynamique la configuration de la fenêtre de votre session distante.

Desktop Viewer

Votre configuration requise pour la manière dont les utilisateurs accèdent aux bureaux virtuels peut varier d'un utilisateur à un autre et lorsque vos besoins sont en constante évolution.

Utilisez Desktop Viewer lorsque vos utilisateurs doivent interagir avec leur bureau virtuel. Le bureau virtuel de l'utilisateur peut être un bureau virtuel publié ou un bureau dédié ou partagé. Dans ce

scénario d'accès, la barre d'outils de Desktop Viewer permet à l'utilisateur de passer d'une session en mode fenêtre à une session en mode plein écran, et prend également en charge le multi-écrans pour les moniteurs d'intersection. Les utilisateurs peuvent basculer entre les sessions de bureau et travailler avec plusieurs bureaux à l'aide de connexions Citrix Virtual Apps and Desktops multiples sur la même machine utilisateur. Des boutons permettant de réduire toutes les sessions de bureau, d'envoyer la séquence Ctrl+Alt+Suppr, de se déconnecter et de fermer la session sont fournis afin de faciliter la gestion des sessions des utilisateurs.

Appuyez sur **Ctrl+Alt+Attn** pour afficher les boutons de la barre d'outils Desktop Viewer dans une fenêtre contextuelle.

Reconnexion automatique de session

L'application Citrix Workspace peut se reconnecter à des bureaux et applications desquels vous avez été déconnectés. Par exemple en cas de problèmes avec l'infrastructure réseau.

- Sur la page **Général** de la boîte de dialogue **Préférences**, sélectionnez une option dans **Reconnecter les applications et les bureaux**.

Accéder aux fichiers locaux

Une application ou un bureau virtuel peut avoir besoin d'accéder à des fichiers sur votre appareil. Vous pouvez configurer différentes options d'accès.

1. Sur la page **Accès au fichier** de la boîte de dialogue **Préférences**, sélectionnez un lecteur mappé, puis l'une des options suivantes :
   - **Lecture et écriture** : autorise le bureau ou l'application à réaliser des opérations d'écriture et de lecture sur les fichiers locaux.
   - **Lecture seule** : autorise le bureau ou l'application à lire les fichiers locaux mais pas à y accéder en écriture.
   - **Aucun accès** : n'autorise ni le bureau ni l'application à accéder aux fichiers locaux.
   - **Toujours me demander** : affiche une invite chaque fois que le bureau ou l'application requiert un accès aux fichiers locaux.
2. Cliquez sur **Ajouter**, spécifiez l'emplacement et sélectionnez un lecteur à mapper.

Microphone et webcam

Pour configurer un microphone ou une webcam, vous pouvez modifier la façon dont un bureau virtuel ou une application accède à votre microphone ou webcam :

Sur la page **Mic et webcam** de la boîte de dialogue **Préférences**, sélectionnez l'une des options suivantes :

- **Utiliser mon micro et ma webcam** : autorise le bureau ou l'application à utiliser le micro et la webcam.
- **Ne pas utiliser mon micro et ma webcam** : n'autorise ni le bureau ni l'application à utiliser le micro et la webcam.

Lecteur Flash

Vous pouvez choisir la manière dont le contenu Flash est affiché. Ce contenu est normalement affiché dans le **lecteur Flash** et inclut les animations, vidéos et applications :

Sur la page **Flash** de la boîte de dialogue **Préférences**, sélectionnez l'une des options suivantes :

- **Optimiser le contenu** : améliore la qualité de lecture, mais peut compromettre la sécurité.
- **Ne pas optimiser le contenu** : offre une qualité de lecture standard et une sécurité élevée.
- **Toujours me demander** : demande à l'utilisateur chaque fois qu'un contenu Flash est affiché.

Connexion

L'application Citrix Workspace permet aux utilisateurs d'accéder en libre-service et en toute sécurité à des applications et bureaux virtuels, et d'accéder à la demande à des applications Windows, Web et SaaS (Logiciel en tant que service). L'accès utilisateur est géré par Citrix StoreFront ou les pages Web créées avec l'Interface Web.

Pour se connecter à des ressources à l'aide de l'interface utilisateur Citrix Workspace

La page d'accueil de l'application Citrix Workspace affiche les applications et les bureaux virtuels mis à la disposition des utilisateurs en fonction de leurs paramètres de compte (c'est-à-dire, le serveur auquel ils se connectent à) et les paramètres configurés par les administrateurs Citrix Virtual Apps and Desktops. À l'aide de la page **Préférences** > **Comptes**, vous pouvez configurer l'URL d'un serveur StoreFront ou, si la découverte de compte par e-mail est configurée, en entrant votre adresse e-mail.

> **Conseil :**
>
> Si vous utilisez le même nom pour plusieurs magasins sur le serveur StoreFront, vous évitez les duplications en ajoutant des nombres. Les noms de tels magasins dépendent de l'ordre dans lequel ils sont ajoutés. Pour l'application Citrix Workspace, l'URL du magasin est affichée et identifie de manière unique le magasin.

Après la connexion à un magasin, le mode libre-service affiche les onglets **FAVORIS**, **BUREAUX** et **APPLICATIONS**. Pour lancer une session, cliquez sur l'icône appropriée. Pour ajouter une icône aux **FAVORIS**, cliquez sur le lien **Détails** en regard de l'icône et sélectionnez **Ajouter aux Favoris**.

Configurer les paramètres de connexion

Vous pouvez configurer certains paramètres par défaut pour les connexions entre l'application Citrix Workspace et les serveurs Citrix Virtual Apps and Desktops. Le cas échéant, vous pouvez également modifier ces paramètres pour des connexions individuelles.

Bien que certaines tâches et responsabilités respectives des administrateurs et des utilisateurs puissent coïncider, le terme « utilisateur » est employé pour distinguer les tâches typiquement effectuées par les utilisateurs de celles réalisées par les administrateurs.

Se connecter aux ressources à partir d'une ligne de commande ou d'un navigateur

Vous créez les connexions aux serveurs lorsque vous cliquez sur une icône de bureau ou d'application sur la page d'accueil de l'application Citrix Workspace. En outre, vous pouvez ouvrir des connexions à partir d'une ligne de commande ou d'un navigateur Web.

Pour créer une connexion à un serveur Program Neighborhood ou StoreFront à l'aide d'une ligne de commande

Conditions préalables :

Assurez-vous que le magasin est reconnu par l'application Citrix Workspace. Ajoutez-le si nécessaire à l'aide de la commande suivante :

```
./util/storebrowse --addstore \<store URL\>
```

1. Obtenez l'ID unique de l'application ou du bureau auquel vous souhaitez vous connecter. Il s'agit de la première chaîne entre guillemets sur une ligne acquise dans l'une des commandes suivantes :
   - Liste de tous les bureaux et applications sur le serveur :

     ```
     ./util/storebrowse -E <store URL>
     ```

   - Liste des bureaux et applications auxquels vous êtes abonné :

     ```
     ./util/storebrowse -S <store URL>
     ```

2. Exécutez la commande suivante pour démarrer le bureau ou l'application :

   ```
   ./util/storebrowse -L <desktop or application ID> <store URL>
   ```

Si vous ne pouvez pas vous connecter à un serveur, votre administrateur devra peut-être modifier l'emplacement du serveur ou les détails du proxy SOCKS. Pour de plus amples informations, consultez serveur proxy.

Pour créer une connexion à partir d'un navigateur Web

La configuration du démarrage de sessions à partir d'un navigateur Web est généralement effectuée automatiquement durant l'installation. En raison du large éventail de navigateurs et de systèmes d'exploitation, il est possible qu'une configuration manuelle soit requise.

Si vous configurez manuellement les fichiers .mailcap et MIME pour Firefox, Mozilla ou Chrome, utilisez les modifications de fichier suivantes de manière à ce que les fichiers .ICA lancent l'exécutable de l'application Citrix Workspace, wfica. Pour utiliser d'autres navigateurs, modifiez la configuration du navigateur en conséquence.

1. Exécutez les commandes suivantes pour l'installation non administrateur de l'application Citrix Workspace. Les paramètres de ICAROOT sont susceptibles de changer s'ils sont installés sur un emplacement autre que l'emplacement par défaut. Vous pouvez tester le résultat avec la commande

   `xdg-mime query default application/x-ica` qui doit renvoyer « wfica.desktop ».

   ```
   setenv ICAROOT=/opt/Citrix/ICAClient

   xdg-icon-resource install --size 64

   $ICAROOT/icons/000\\_Receiver_64.png Citrix Workspace app

   xdg-mime default wfica.desktop application/x-ica

   xdg-mime default new\\_store.desktop application/vnd.citrix.receiver.
   configure
   ```

2. Créez ou étendez le fichier /etc/xdg/mimeapps.list (pour l'installation administrateur) ou `$HOME/.local/share/applications/mimeapps.list (mimeapps.list)`. Le fichier doit démarrer par [Default Applications], et être suivi de :

   ```
   application/x-ica=wfica.desktop;

   application/vnd.citrix.receiver.configure=new\\_store.desktop;
   ```

   Vous devrez peut-être configurer Firefox sur la page Préférences/Applications.

   Pour « Citrix ICA settings file content », sélectionnez :

   - « Citrix Workspace app Engine (default) » dans le menu déroulant

     ou

   - Ou sélectionnez « Use other … » et sélectionnez le fichier /usr/share/applications/wfica.desktop (pour une installation administrateur de l'application Citrix Workspace)

     ou

   - $HOME/.local/share/applications/wfica.desktop (pour une installation non-administrateur).

Centre de connexion

Les utilisateurs peuvent gérer leurs connexions actives à l'aide du Centre de connexion. Cette fonctionnalité est un outil de productivité très utile, qui permet aux utilisateurs et aux administrateurs de résoudre les problèmes liés aux connexions lentes ou complexes. Grâce au Centre de connexion, les utilisateurs peuvent gérer les connexions en :

- Fermant une application.
- Fermant une session. Cette étape met fin à la session et ferme toutes les applications ouvertes.
- Déconnectant une session. Cette étape interrompt la connexion sélectionnée au serveur sans fermer les applications ouvertes (sauf si le serveur est configuré pour fermer les applications au moment de la déconnexion).
- Affichant les statistiques de transport de connexion.

Gérer une connexion

Pour gérer une connexion à l'aide du **Centre de connexion** :

1. Dans le menu de l'application Citrix Workspace, cliquez sur **Centre de connexion**.

   Les serveurs utilisés s'affichent et chaque session active est répertoriée.

2. Procédez comme suit :

   - Sélectionnez un serveur, déconnectez-vous ou fermez la session, ou affichez ses propriétés.
   - Sélectionnez une application, fermez la fenêtre.

Configurer

May 4, 2021

Lors de l'utilisation de l'application Citrix Workspace pour Linux, les étapes de configuration suivantes permettent aux utilisateurs d'accéder à leurs applications et bureaux hébergés.

Paramètres

Fichiers de configuration

Pour modifier des paramètres avancés ou moins courants, vous pouvez modifier les fichiers de configuration de l'application Citrix Workspace. Ces fichiers de configuration sont lus chaque fois que `wfica` démarre. Vous pouvez modifier différents fichiers, en fonction de l'impact souhaité de ces modifications.

Si le partage de session est activé, une session existante peut être utilisée à la place d'une nouvelle session reconfigurée. Par conséquent, les modifications que vous avez apportées dans un fichier de configuration peuvent être ignorées dans la session.

Paramètres par défaut

Si vous souhaitez modifier la valeur par défaut pour tous les utilisateurs de application Citrix Workspace, modifiez le fichier de configuration `module.ini` dans le répertoire `$ICAROOT/config`.

> **Remarque :**
>
> Si une entrée dans `All\\_Regions.ini` est définie sur une valeur spécifique, la valeur de cette entrée dans `module.ini` n'est pas utilisée. La valeur définie dans `All\\_Regions.ini` a priorité sur la valeur définie dans `module.ini`.

Fichier modèle

Si le fichier `$HOME/.ICAClient/wfclient.ini` n'existe pas, `wfica` le crée en copiant `$ICAROOT/config/wfclient.template`. Lorsque vous apportez des modifications à ce fichier de modèle, celles-ci s'appliquent à tous les utilisateurs de l'application Citrix Workspace.

Paramètres utilisateur

Pour appliquer les modifications de configuration à un utilisateur, modifiez le fichier `wfclient.ini` dans le répertoire `$HOME/.ICAClient` de l'utilisateur. Les paramètres de ce fichier s'appliquent aux futures connexions pour cet utilisateur.

Valider les entrées du fichier de configuration

Pour restreindre les valeurs des entrées dans le fichier `wfclient.ini`, vous pouvez spécifier les options autorisées ou des plages d'options dans `All\\_Regions.ini`.

Si vous spécifiez une seule valeur possible, cette valeur est utilisée. `$HOME/.ICAClient/All\\_Regsions.ini` peut uniquement faire correspondre ou réduire les valeurs possibles définies par `$ICAROOT/config/All\\_Regions.ini` mais ne peut pas éliminer les restrictions.

> **Remarque :**
>
> La valeur définie dans `wfclient.ini` a priorité sur la valeur définie dans `module.ini`.

Paramètres

Les paramètres répertoriés dans chaque fichier sont regroupés en sections. Chaque section commence par un nom entre crochets indiquant les paramètres qui appartiennent au même groupe ; par exemple, `\[ClientDrive\]` pour les paramètres associés au mappage des lecteurs clients (CDM).

Les valeurs par défaut sont automatiquement fournies pour tout paramètre manquant, sauf indication contraire. Si un paramètre est présent mais qu'aucune valeur ne lui a été affectée, la valeur par défaut est automatiquement appliquée. Par exemple, si `InitialProgram` est suivi d'un signe égal (=) mais sans valeur, la valeur par défaut (Ne pas exécuter de programme après l'ouverture de session) est appliquée.

Priorité

`All\\_Regions.ini` spécifie quels paramètres peuvent être définis par d'autres fichiers. Vous pouvez restreindre les valeurs des paramètres ou les définir exactement.

Pour toute connexion donnée, les fichiers sont vérifiés dans l'ordre suivant :

1. `All\\_Regions.ini` - Les valeurs de ce fichier écrasent celles dans :
   - Le fichier .ICA des connexions
   - `wfclient.ini`
2. `module.ini` - Les valeurs dans ce fichier sont utilisées si elles n'ont pas été définies dans le fichier `All\\_Regions.ini`, le fichier .ica des connexions ou le fichier `wfclient.ini`, mais elles ne sont pas limitées par des entrées dans le fichier `All\\_Regions.ini`.

Si aucune valeur n'est trouvée dans l'un de ces fichiers, le paramètre par défaut dans le code de l'application Citrix Workspace est utilisé.

> **Remarque :**
>
> il existe des exceptions à cet ordre de priorité. Par exemple, pour des raisons de sécurité, le code lit certaines valeurs spécifiquement dans le fichier `wfclient.ini`.

Épinglage de la disposition de plusieurs moniteurs

À partir de la version 2103, vous pouvez enregistrer la sélection de la disposition d'écran multi-moniteurs. La disposition est la façon dont une session de bureau saffiche. L'épinglage permet de relancer une session avec la disposition sélectionnée, ce qui permet d'optimiser l'expérience utilisateur.

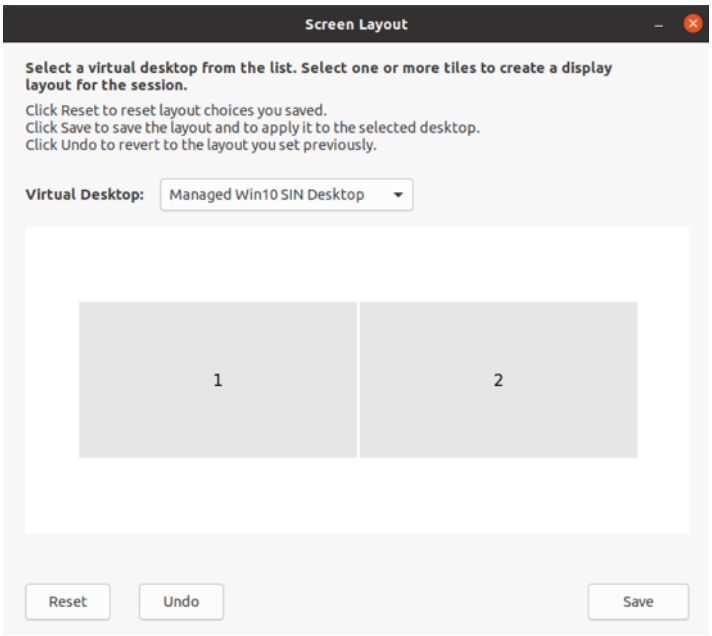
En tant que condition préalable, vous devez activer cette fonctionnalité dans le fichier `AuthManConfig.xml`. Accédez à `$ICAROOT/config/AuthManConfig.xml` et ajoutez les entrées suivantes :


```
<key>ScreenPinEnabled</key>
<value> true </value>
```

L'option **Disposition de l'écran** ne sera visible dans l'icône de l'indicateur d'application qu'après l'ajout de la clé ci-dessus. Pour plus d'informations sur l'icône d'indicateur d'application, consultez Icône « appindicator ».

Pour sélectionner la disposition de l'écran, cliquez sur l'icône de l'indicateur d'application dans la barre des tâches, puis sélectionnez **Disposition de l'écran**. La boîte de dialogue **Disposition de l'écran** s'affiche.

Alternativement, vous pouvez lancer la boîte de dialogue **Disposition de l'écran** en appuyant sur **Ctrl+m** lorsque vous êtes sur la fenêtre en libre-service.



Sélectionnez un bureau virtuel dans le menu déroulant. La sélection de la disposition s'applique uniquement au bureau que vous sélectionnez.

Sélectionnez une ou plusieurs tuiles pour former une sélection rectangulaire pour la disposition. La session apparaît alors selon la disposition sélectionnée.

Limitations :

- L'activation de l'épinglage de l'écran désactive la fonctionnalité d'enregistrement de la disposition dans une session.
- Cette fonctionnalité est applicable uniquement sur les bureaux marqués comme favoris.

Protection des applications fonctionnalité expérimentale

> **Remarque :**
>
> - Cette fonctionnalité est prise en charge uniquement lorsque l'application Citrix Workspace est installée à l'aide du package Tarball. En outre, x64 et armhf sont les deux seuls packages pris en charge.
> - Cette fonctionnalité est prise en charge uniquement sur les déploiements locaux de Citrix Virtual Apps and Desktops.

La protection des applications est une fonctionnalité complémentaire qui offre une sécurité renforcée lors de l'utilisation de Citrix Virtual Apps and Desktops. Elle limite le risque d'être infecté par des programmes malveillants d'enregistrement de frappe et de capture d'écran. La protection des applications empêche l'exfiltration d'informations confidentielles telles que les informations d'identification de l'utilisateur et les informations sensibles affichées à l'écran. Cette fonctionnalité empêche les utilisateurs et les attaquants de prendre des captures d'écran et d'utiliser des enregistreurs de frappe pour récupérer et exploiter des informations sensibles.

Conditions préalables :

Ubuntu 18.04 ou version ultérieure.

Installer le composant de protection des applications :

Lorsque vous installez l'application Citrix Workspace à l'aide du package Tarball, le message suivant s'affiche.

« Souhaitez-vous installer le composant de protection des applications ? Avertissement : vous ne pouvez pas désactiver cette fonctionnalité. Vous ne pouvez pas désactiver cette fonctionnalité. Pour la désactiver, vous devez désinstaller l'application Citrix Workspace. Pour plus d'informations, contactez votre administrateur système. [$INSTALLER_N par défaut] »

Entrez **Y** pour installer le composant de protection des applications.

Par défaut, le composant de protection des applications n'est pas installé.

Redémarrez votre machine pour que les modifications prennent effet. La protection des applications peut ne pas fonctionner comme prévu, sauf si vous redémarrez votre ordinateur.

Installation du composant de protection des applications sur les packages RPM :

À partir de la version 2104, la protection des applications est prise en charge sur la version RPM de l'application Citrix Workspace.

Pour installer la protection des applications, procédez comme suit :

1. Installez l'application Citrix Workspace.
2. Installez le package de protection des applications `ctxappprotection<version>.rpm` à partir du programme d'installation de l'application Citrix Workspace.
3. Redémarrez le système pour que les modifications prennent effet.

Installation du composant de protection des applications sur les packages Debian :

À partir de la version 2101, la protection des applications est prise en charge sur la version Debian de l'application Citrix Workspace.

Pour installer de façon silencieuse le composant de protection d'application, exécutez la commande suivante à partir du terminal avant d'installer l'application Citrix Workspace :

```
export DEBIAN_FRONTEND="noninteractive"
sudo debconf-set-selections <<< "icaclient app_protection/
   install_app_protection select no"

sudo debconf-show icaclient
* app_protection/install_app_protection: no

sudo apt install -f ./icaclient_<version>._amd64.deb
```

Problèmes connus :

- Lorsque vous réduisez un écran protégé, la protection des applications continue de s'exécuter en arrière-plan.

CEIP (programme d'amélioration de l'expérience du client)

Données collectées	Description	Usage que nous faisons de ces données
Données de configuration et d'utilisation	Le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) rassemble des données de configuration et d'utilisation à partir de l'application Citrix Workspace pour Linux et les envoie automatiquement à Google Analytics.	Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de l'application Citrix Workspace.

Informations supplémentaires

Citrix traite vos données conformément aux termes de votre contrat avec Citrix et les protège comme indiqué dans l'Annexe sur la sécurité des Services Citrix sur le Citrix Trust Center.

Citrix utilise également Google Analytics pour collecter certaines données à partir de l'application Citrix Workspace dans le cadre du programme CEIP. Veuillez contrôler la façon dont Google gère les données collectées pour Google Analytics.

Vous pouvez désactiver l'envoi de données via le programme CEIP à Citrix et Google Analytics (à l'exception des deux éléments de données collectés pour Google Analytics indiqués par un * dans le deuxième tableau ci-dessous) comme suit :

1. Accédant à la section `CEIP` dans le dossier `\<ICAROOT\>/config/module.ini`.
2. Sélectionnant l'entrée `EnableCeip` et en la définissant sur `Disable`.

> **Remarque :**
>
> Une fois la clé `EnableCeip` définie sur `Disable`, si vous souhaitez désactiver l'envoi des deux derniers éléments de données CEIP collectés par Google Analytics (c'est-à-dire la version du système d'exploitation et la version de l'application Workspace), accédez à la section suivante et définissez la valeur comme suggéré :

Emplacement : `<ICAROOT>/config/module.ini`

Section : `GoogleAnalytics`

Entrée : `DisableHeartBeat`

Valeur : `True`

Les données spécifiques à CEIP collectées par Google Analytics sont les suivantes :

Version du système d'exploitation*	Version de l'application Workspace*	Nom de l'application	ID client
Méthode de lancement de session	Version du compilateur	Plate-forme matérielle	

Icône « appindicator »

L'icône appindicator démarre lorsque vous lancez l'application Citrix Workspace. Il s'agit d'une icône qui est présente dans la zone de notification. Avec l'introduction de l'icône appindicator, les performances d'ouverture de session de l'application Citrix Workspace pour Linux sont améliorées.

Vous pouvez observer une amélioration des performances lorsque vous :

- lancez l'application Citrix Workspace pour la première fois ;
- fermez et relancez l'application ;

- quittez et relancez l'application.

> **Remarque :**
>
> Le package `libappindicator` est requis pour que l'icône appindicator s'affiche. Installez le package `libappindicator` adapté à votre distribution Linux à partir du Web.

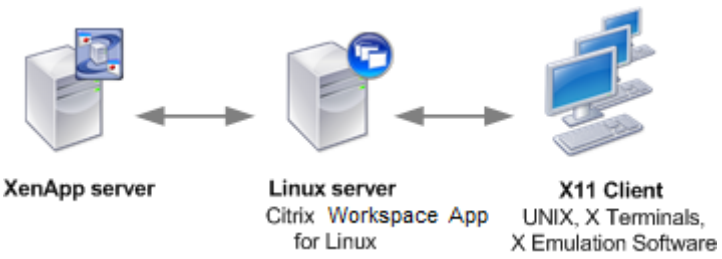
ICA vers proxy X

Vous pouvez utiliser une station de travail exécutant l'application Citrix Workspace en tant que serveur et rediriger la sortie vers une autre machine compatible X11. Cela peut être utile pour envoyer des applications Microsoft Windows à des terminaux X ou des stations de travail UNIX pour lesquels l'application Citrix Workspace n'est pas disponible.

> **Remarque :**
>
> L'application Citrix Workspace étant disponible pour de nombreuses machines X, son installation s'avère être la meilleure solution. L'exécution de l'application Citrix Workspace en tant que ICA vers proxy X, est également appelée ICA côté serveur.

Lorsque vous exécutez l'application Citrix Workspace, vous pouvez le considérer comme un convertisseur ICA vers X11, dirigeant la sortie X11 vers votre bureau Linux local. Toutefois, vous pouvez rediriger la sortie vers un autre affichage X11. Vous pouvez exécuter plusieurs copies de l'application Citrix Workspace simultanément sur un même système, chacune envoyant sa sortie sur une machine différente.

Ce graphique montre un système avec l'application Citrix Workspace pour Linux configuré en tant que ICA vers proxy X :



Pour configurer ce type de système, vous devez disposer d'un serveur Linux agissant en tant qu'ICA vers proxy X11 :

- Si vous disposez déjà de terminaux X, vous pouvez exécuter l'application Citrix Workspace sur le serveur Linux habituellement responsable de l'envoi d'applications X aux terminaux X.
- Si vous souhaitez déployer des stations de travail UNIX pour lesquelles l'application Citrix Workspace n'est pas disponible, vous avez besoin d'un serveur supplémentaire faisant office de proxy. Il peut s'agir d'un ordinateur sous Linux.

Les applications sont envoyées à la machine utilisateur finale à l'aide de X11, en utilisant les capacités du protocole ICA. Par défaut, vous pouvez utiliser le mappage de lecteur uniquement pour accéder aux lecteurs sur le proxy. Cela ne constitue pas un problème si vous utilisez des terminaux X (qui n'ont généralement pas de disques locaux). Si vous envoyez des applications à d'autres stations de travail UNIX, deux options s'offrent à vous :

- monter en NFS la station de travail UNIX locale sur la station de travail faisant office de proxy, puis pointer un mappage de lecteur client sur le point de montage NFS du proxy ;
- utiliser un proxy NFS vers SMB tel que SAMBA, ou un client NFS sur le serveur tel que Microsoft Services pour UNIX.

Certaines fonctions ne sont pas transmises à la machine finale :

- Redirection USB
- Redirection de carte à puce
- Redirection de port COM
- Les fonctionnalités audio ne sont pas envoyées à la machine X11, même si le serveur faisant office de proxy les prend en charge.
- Les imprimantes clientes ne sont pas transmises via la machine X11. Vous accédez à l'imprimante UNIX manuellement depuis le serveur à l'aide de l'impression LPD, ou utiliser une imprimante réseau.
- La redirection des entrées multimédia n'est pas censée fonctionner car elle nécessite une webcam sur l'ordinateur qui exécute l'application Citrix Workspace, qui est le serveur faisant office de proxy. Toutefois, la redirection des sorties multimédia fonctionne avec GStreamer lorsque ce dernier est installé sur le serveur faisant office de proxy (non testé).

Pour démarrer l'application Citrix Workspace avec ICA côté serveur à partir d'un terminal X ou d'une station de travail UNIX :

1. Utilisez ssh ou telnet pour vous connecter à la machine faisant office de proxy.
2. Dans un shell de la machine proxy, définissez la variable d'environnement **DISPLAY** sur la machine locale. Par exemple, dans un shell C, saisissez :

   ```
   setenv DISPLAY <local:0>
   ```

   > **Remarque :**
   >
   > Si vous utilisez la commande `ssh -X` pour vous connecter à la machine faisant office de proxy, vous n'avez pas besoin de définir la variable d'environnement **DISPLAY**.

3. À l'invite de commande sur la machine locale, saisissez xhost <nom serveur proxy>
4. Si l'application Citrix Workspace n'est pas installée dans le répertoire d'installation par défaut, assurez-vous que la variable d'environnement ICAROOT est définie de manière à pointer vers le répertoire d'installation réel.

5. Localisez le répertoire dans lequel l'application Citrix Workspace a été installée. À l'invite de commandes, tapez `selfservice &`.

Redirection de contenu du serveur vers le client

La redirection de contenu serveur vers client permet aux administrateurs d'ouvrir les adresses URL d'une application publiée à l'aide d'une application locale. À titre d'exemple, l'ouverture d'un lien vers une page Web à l'aide de Microsoft Outlook dans une session ouvre le fichier requis à l'aide du navigateur de la machine utilisateur. La redirection de contenu serveur vers client permet aux administrateurs d'allouer des ressources Citrix de manière plus efficace, offrant ainsi aux utilisateurs des performances optimisées.

Les types d'adresses URL suivantes peuvent être redirigées :

- HTTP
- HTTPS
- RTSP (Real Player) ;
- RTSPU (Real Player) ;
- PNM (Real Players plus anciens).

Si l'application Citrix Workspace pour Linux ne dispose pas d'une application appropriée ou ne peut accéder directement au contenu, l'adresse URL est ouverte au moyen de l'application serveur.

La redirection de contenu serveur vers client est configurée sur le serveur et activée par défaut dans l'application Citrix Workspace si le chemin inclut RealPlayer et au moins l'un des navigateurs suivants : Firefox, Mozilla ou Netscape.

Pour activer la redirection de contenu serveur vers client lorsque RealPlayer et au moins un navigateur sont absents du chemin

1. Ouvrez le fichier de configuration `wfclient.ini`.
2. Dans la section [Browser], modifiez les paramètres suivants :

   Path=path

   Command=command

   où path est le répertoire dans lequel se trouve l'exécutable du navigateur et où command est le nom de l'exécutable utilisé pour traiter les adresses URL du navigateur redirigées, ajoutées à l'adresse URL envoyée par le serveur. Par exemple :

`$ICAROOT/nslaunch` Netscape, firefox, mozilla

```
1 Ce paramétre entraîne les effets suivants :
2
```



```
3 - L'utilitaire `nslaunch` est exécuté pour transférer l'adresse URL
      dans une fenêtre de navigateur existante.
4 - Chaque navigateur de la liste est testé à tour de rôle, jusqu'à ce
      que le contenu soit affiché.
```

1. Dans la section [Player], modifiez les paramètres suivants :

   Path=path

   Command=command

   où path est le répertoire dans lequel se trouve l'exécutable de RealPlayer et où command est le nom de l'exécutable utilisé pour traiter les adresses URL multimédia redirigées, ajoutées à l'adresse URL envoyée par le serveur.

2. Enregistrez, puis fermez le fichier.

> **Remarque :**
>
> Dans les deux cas, pour le paramètre Path, vous devez uniquement indiquer le répertoire dans lequel se trouvent les exécutables du navigateur et de RealPlayer. Il n'est pas nécessaire de fournir le chemin d'accès complet aux exécutables. Par exemple, dans la section [Browser], Path peut être défini comme /usr/X11R6/bin plutôt que /usr/X11R6/bin/netscape. De plus, vous pouvez indiquer plusieurs noms de répertoire sous forme d'une liste de noms séparés par deux points. Si ces paramètres ne sont pas spécifiés, le $PATH utilisateur actuel est employé.

Pour désactiver la redirection de contenu serveur vers client à partir de Citrix Workspace :

1. Ouvrez le fichier de configuration module.ini.
2. Modifiez le paramètre CREnabled en lui attribuant la valeur Off.
3. Enregistrez, puis fermez le fichier.

Connexion

Configurer les connexions

Sur les machines disposant d'une puissance de processeur limitée ou pour lesquelles la bande passante disponible est restreinte, il convient d'équilibrer les performances et les fonctionnalités. Les utilisateurs et administrateurs peuvent choisir une combinaison équilibrée en termes de fonctionnalités et de performances. Vous pouvez réduire la bande passante requise par votre connexion et améliorer les performances en apportant une ou plusieurs des modifications suivantes sur le serveur et non sur la machine utilisateur :

- **Activer la réduction de latence SpeedScreen** : la réduction de latence SpeedScreen améliore les performances des connexions à latence élevée en fournissant un retour visuel immédiat en réponse aux entrées de données et aux clics de souris de l'utilisateur. Utilisez le Gestionnaire

de Réduction de latence SpeedScreen pour activer cette fonctionnalité sur le serveur. Par défaut, dans l'application Citrix Workspace, cette fonctionnalité est désactivée pour le clavier et uniquement activée pour la souris sur les connexions à latence élevée. Consultez le Guide de référence OEM de l'application Citrix Workspace pour Linux.

- **Activer la compression de données** : la compression des données réduit le volume des données transférées via la connexion. Ce processus requiert des ressources processeur supplémentaires pour compresser et décompresser les données, mais permet d'améliorer les performances des connexions à faible bande passante. Utilisez les paramètres de stratégie **Citrix Qualité audio et Compression d'image** pour activer cette fonctionnalité.
- **Réduire la taille de la fenêtre** : modifiez la taille de fenêtre jusqu'à ce que vous atteigniez une taille de lecture confortable. Sur la batterie, définissez les options de session.
- **Réduire le nombre de couleurs** : réduit le nombre de couleurs à 256. Sur le site Citrix Virtual Apps and Desktops, définissez les options de session.
- **Réduire la qualité sonore** : si le mappage audio est activé, réduisez la qualité sonore au réglage minimum à l'aide du paramètre de stratégie Citrix Qualité audio.

Police

Lissage des polices ClearType

Le lissage de polices ClearType (également appelé rendu de police subpixellaire) améliore la qualité des polices affichées au-delà de celle disponible au moyen des techniques traditionnelles de lissage de polices ou d'anticrénelage. Vous pouvez activer ou désactiver cette fonctionnalité. Vous pouvez également spécifier le type de lissage en modifiant le paramètre suivant dans la section [WFClient] du fichier de configuration approprié :

FontSmoothingType = nombre

Où nombre peut prendre l'une des valeurs suivantes :

Valeur	Comportement
0	La préférence locale de la machine est utilisée. Cette valeur est définie par le paramètre FontSmoothingTypePref.
1	Aucun lissage
2	Lissage standard
3	Lissage ClearType (subpixellaire horizontal)

Les lissages standard et ClearType peuvent augmenter de manière significative les besoins en bande

passante de l'application Citrix Workspace.

> **Important :**
>
> Le serveur peut configurer FontSmoothingType via le fichier ICA. Cela prévaut sur la valeur définie dans la section [WFClient].

Si le serveur définit la valeur sur 0, la préférence locale est déterminée par un autre paramètre dans la section [WFClient] :
FontSmoothingTypePref = nombre

Où un nombre peut prendre l'une des valeurs suivantes :

Valeur	Comportement
0	Aucun lissage
1	Aucun lissage
2	Lissage standard
3	Lissage ClearType (subpixellaire horizontal) (comportement par défaut)

Dossier

Configurer la redirection de dossiers spéciaux

Dans ce contexte, il n'existe que deux dossiers spéciaux pour chaque utilisateur :

- le dossier Desktop de l'utilisateur ;
- le dossier Documents de l'utilisateur (Mes documents sous Windows XP).

La redirection de dossiers spéciaux vous permet d'indiquer les emplacements des dossiers spéciaux d'un utilisateur afin que ceux-ci demeurent à un emplacement fixe sur les différents types de serveur et configurations de batteries de serveurs. Ceci est important si, par exemple, un utilisateur mobile a besoin d'ouvrir une session sur des serveurs de différentes batteries. Pour les stations de travail statiques, à partir desquelles l'utilisateur peut ouvrir une session sur des serveurs résidant dans une seule batterie, la redirection de dossiers spéciaux est rarement nécessaire.

Pour configurer la redirection de dossiers spéciaux :

Une procédure en deux parties se présente comme suit. Dans un premier temps, vous devez activer la redirection de dossiers spéciaux en saisissant une entrée dans le fichier module.ini. Dans un second temps, indiquez l'emplacement des dossiers dans la section [WFClient], comme décrit ci-dessous :

1. Ajoutez le texte suivant dans le fichier module.ini (par exemple $ICAROOT/config/module.ini) :

   [ClientDrive]

SFRAllowed = True

2. Ajoutez le texte suivant à la section [WFClient] (par exemple $HOME/.ICAClient/wfclient.ini) :

   DocumentsFolder = documents

   DesktopFolder = desktop

   où documents et desktop sont des noms de fichiers UNIX, comprenant les chemins complets des répertoires à utiliser respectivement pour les dossiers utilisateur Documents et Desktop. Par exemple :

   DesktopFolder = $HOME/.ICAClient/desktop

   - Vous pouvez indiquer n'importe quel composant du chemin sous forme de variable d'environnement, par exemple $HOME.
   - Indiquez des valeurs pour ces deux paramètres.
   - Les répertoires que vous spécifiez doivent être disponibles via le mappage de machine cliente. En d'autres termes, le répertoire doit être situé dans la sous-arborescence d'une machine cliente mappée.
   - Utilisez les lettres de lecteur C ou suivantes.

Mappage des lecteurs clients

Le mappage des lecteurs clients permet d'affecter des lettres de lecteur du serveur Citrix Virtual Apps ou Citrix Virtual Desktops aux répertoires existants sur la machine utilisateur locale. Par exemple, dans une session utilisateur Citrix, le lecteur H peut être mappé à un répertoire de la machine locale qui exécute l'application Workspace.

Le mappage de lecteurs clients permet de rendre disponible auprès des utilisateurs un répertoire monté sur la machine utilisateur locale, comprenant un CD-ROM, DVD ou une clé USB de mémoire, et ce le temps d'une session, à condition que l'utilisateur local soit autorisé à y accéder. Lorsqu'un serveur est configuré pour permettre le mappage de lecteur client, les utilisateurs peuvent accéder à leurs fichiers stockés localement, travailler sur ceux-ci lors de leur session, puis les enregistrer à nouveau sur un lecteur local ou sur un lecteur du serveur.

L'application Citrix Workspace prend en charge le mappage des machines clientes pour les connexions aux serveurs Citrix Virtual Apps and Desktops. Le mappage des machines clientes permet à une application distante exécutée sur un serveur d'accéder aux périphériques connectés à la machine utilisateur locale. Les applications et les ressources système sont affichées auprès de l'utilisateur sur la machine utilisateur de la même façon que pour une exécution locale. Avant d'utiliser ces fonctionnalités, assurez-vous que le mappage des machines clientes est pris en charge par le serveur.

> **Remarque :**
>
> Le modèle de sécurité Security-Enhanced Linux (SELinux) peut affecter le fonctionnement du mappage de lecteurs clients et les fonctionnalités de redirection USB (sur Citrix Virtual Apps and Desktops). Si vous avez besoin d'une ou de ces deux fonctionnalités, désactivez SELinux avant de les configurer sur le serveur.

Deux types de mappage de lecteur sont disponibles :

- Mappage de lecteur client statique : cette méthode permet aux administrateurs de mapper n'importe quelle partie d'un système de fichiers sur une machine utilisateur à une lettre de lecteur spécifiée sur le serveur à l'ouverture de session. Ce type de mappage peut être utilisé, par exemple, pour mapper tout ou partie du répertoire de base d'un utilisateur ou du répertoire /tmp, ainsi que les points de montage de périphériques matériels tels que des CD-ROM, DVD ou clés USB.
- Mappage de lecteur client dynamique : cette méthode contrôle les répertoires dans lesquels les périphériques matériels tels que les CD-ROM, DVD et clés USB sont généralement montés sur la machine utilisateur. Tous les nouveaux répertoires apparaissant au cours d'une session sont automatiquement mappés à la prochaine lettre de lecteur sur le serveur.

Lorsque l'application Citrix Workspace se connecte à Citrix Virtual Apps ou Citrix Virtual Desktops, les mappages de lecteur client sont rétablis, sauf si le mappage des périphériques clients est désactivé. Vous pouvez utiliser des règles vous permettant d'avoir un contrôle accru sur la manière dont le mappage des périphériques clients s'applique. Pour de plus amples informations, consultez la documentation de Citrix Virtual Apps and Desktops.

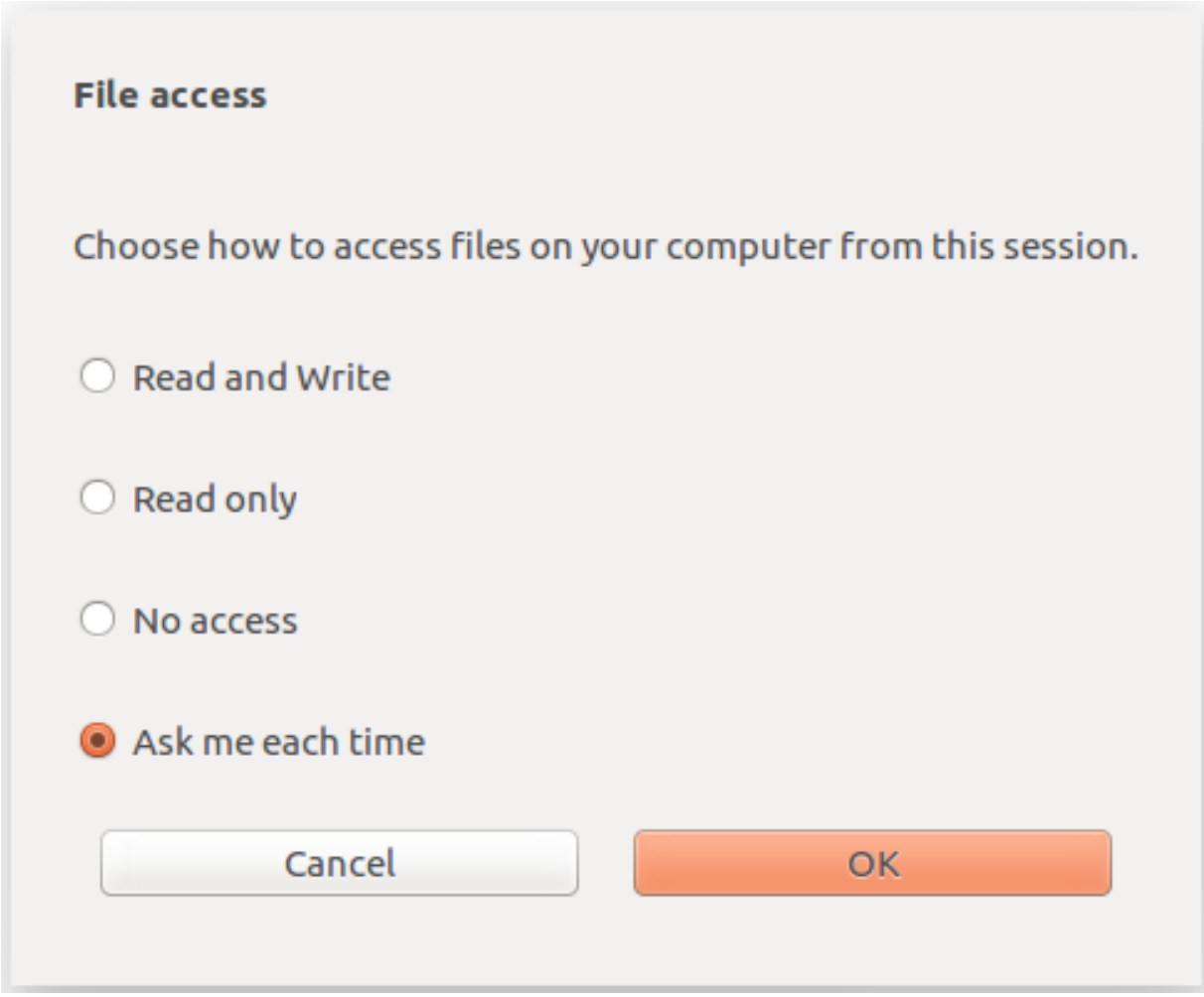
Les utilisateurs peuvent mapper les lecteurs à l'aide de la boîte de dialogue Préférences.

> **Remarque :**
>
> Par défaut, l'activation du mappage de lecteur client statique active également le mappage de lecteur client dynamique. Pour désactiver ce dernier mais activer le premier, définissez `DynamicCDM` sur `False` dans `wfclient.ini`.

Auparavant, votre paramètre d'accès aux fichiers via CDM était appliqué à tous les magasins configurés.

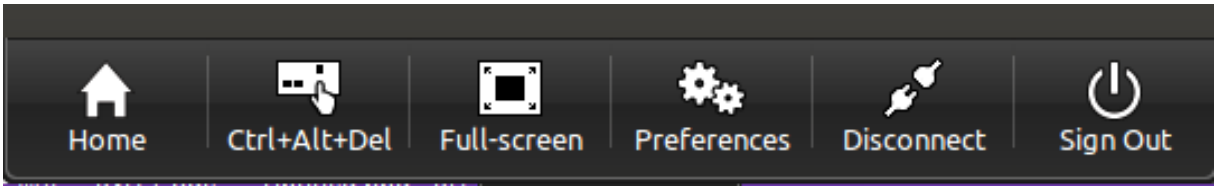
À partir de la version 2012, l'application Citrix Workspace vous permet de configurer l'accès aux fichiers CDM par magasin.

> **Remarque :**
>
> Le paramètre d'accès aux fichiers n'est pas persistant sur toutes les sessions lors de l'utilisation de Workspace pour Web. L'option par défaut est **Ask me each time** (Me demander à chaque fois).

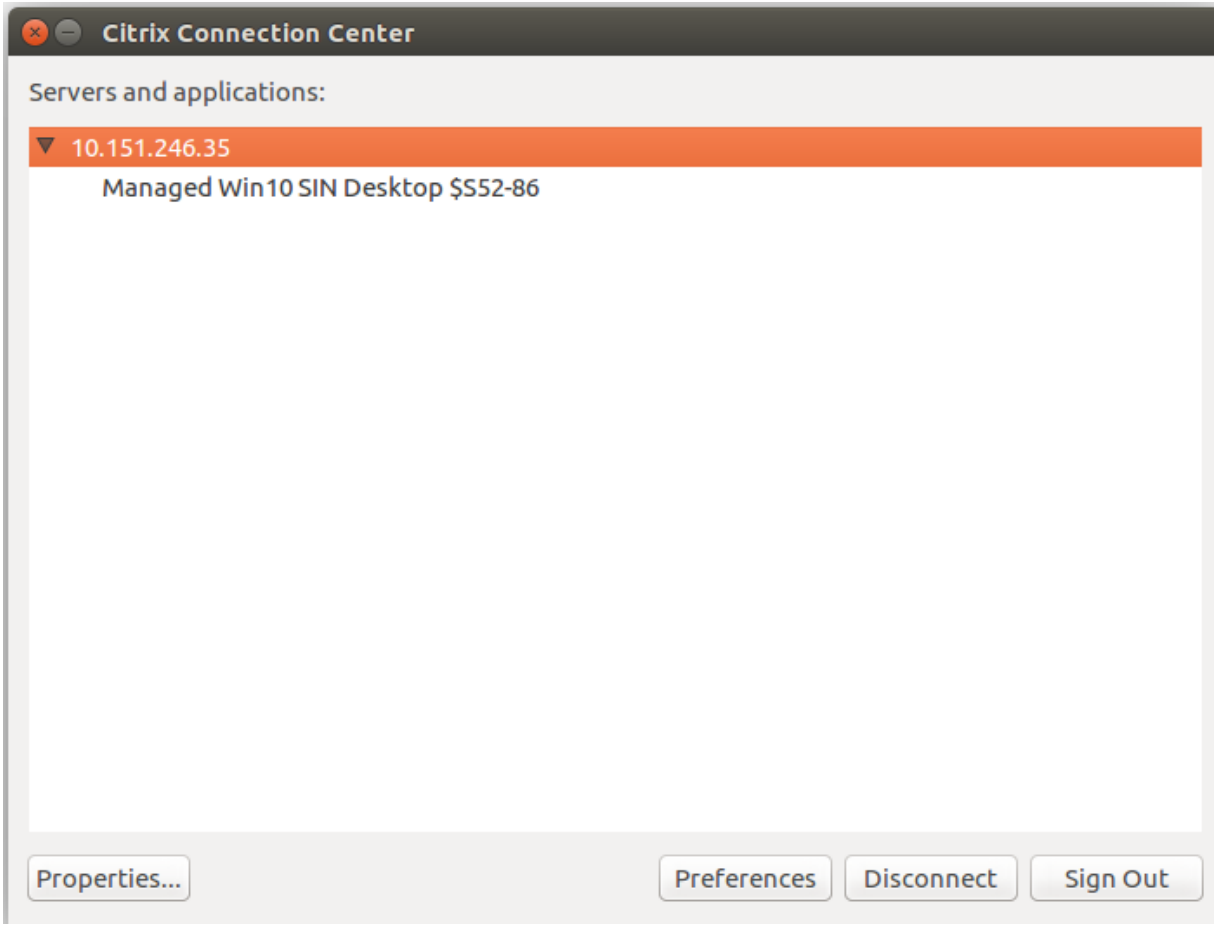


Vous pouvez utiliser le fichier `wfclient.ini` pour configurer les attributs de chemin d'accès et de nom de fichier mappés. Utilisez l'interface graphique pour définir un niveau d'accès aux fichiers comme indiqué dans la capture d'écran précédente.

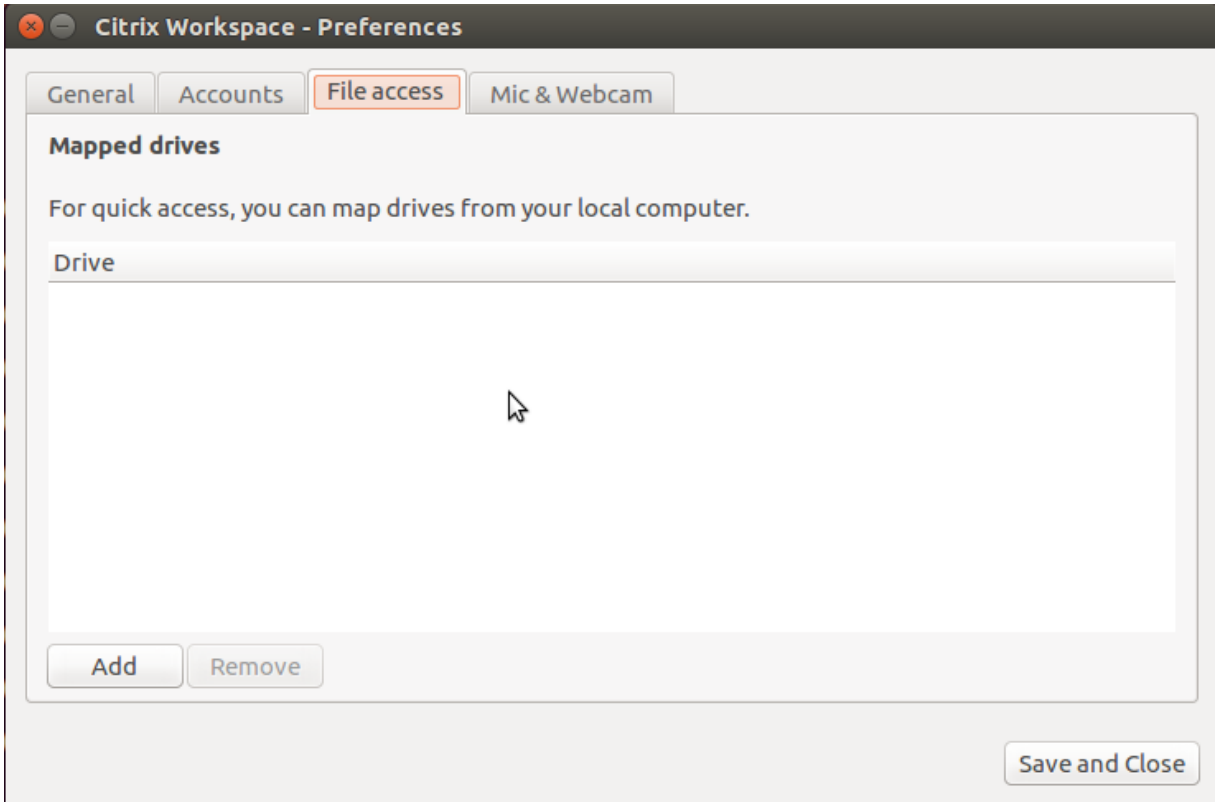
Dans une session de bureau, vous pouvez définir un niveau d'accès aux fichiers en accédant à la boîte de dialogue **Préférences** > **Accès aux fichiers** à partir de Desktop Viewer.



Dans une session d'application, vous pouvez définir un niveau d'accès aux fichiers en lançant la boîte de dialogue **Accès aux fichiers** à partir du **Centre de connexion Citrix**.



La boîte de dialogue **Accès aux fichiers** inclut le nom du dossier mappé et son chemin d'accès.



L'indicateur de niveau d'accès n'est plus pris en charge dans le fichier `wfclient.ini`.

Mapper imprimantes clientes

L'application Citrix Workspace prend en charge l'impression sur imprimantes réseau et sur imprimantes locales connectées aux machines utilisateur. Par défaut, sauf si vous créez des stratégies pour en modifier les paramètres, Citrix Virtual Apps permet aux utilisateurs d'effectuer les opérations suivantes :

- imprimer sur tous les périphériques d'impression accessibles à partir de la machine utilisateur ;
- ajouter des imprimantes.

Toutefois, ces paramètres peuvent ne pas être optimaux pour tous les environnements. Par exemple, le paramètre par défaut permettant aux utilisateurs d'imprimer sur toutes les imprimantes accessibles depuis la machine utilisateur est le plus facile à administrer initialement. Mais il peut occasionner des délais d'ouverture de session plus longs dans certains environnements. Dans ce cas, il peut s'avérer utile de limiter la liste des imprimantes configurées sur la machine utilisateur.

De même, les stratégies de sécurité de votre organisation peuvent vous amener à empêcher les utilisateurs de mapper les ports d'imprimantes locales. Pour ce faire, sur le serveur, configurez le paramètre de stratégie ICA Connecter automatiquement les ports COM du client sur Désactivé.

Pour limiter la liste des imprimantes configurées sur la machine utilisateur :

1. Ouvrez le fichier de configuration (intitulé wfclient.ini) à l'un des emplacements suivants :
    - répertoire $HOME/.ICAClient pour limiter les imprimantes pour un utilisateur unique ;
    - répertoire $ICAROOT/config pour limiter les imprimantes pour tous les utilisateurs de l'application Workspace. Tous les utilisateurs dans ce cas sont ceux qui utilisent d'abord le programme self-service après le changement.
2. dans la section [WFClient] du type de fichier :

    ClientPrinterList=imprimante1:imprimante2:imprimante3

    où imprimante1, imprimante2, etc. correspondent aux noms des imprimantes sélectionnées. Séparez les entrées de nom d'imprimante par deux-points (:).
3. Enregistrez, puis fermez le fichier.

Mapper les imprimantes clientes sous UNIX

Dans un environnement UNIX, les pilotes d'imprimante définis par l'application Citrix Workspace sont ignorés. Le système d'impression de la machine utilisateur doit être capable de gérer le format d'impression généré par l'application.

Avant que les utilisateurs puissent imprimer sur une imprimante cliente à partir de Citrix Virtual Apps pour UNIX, l'administrateur doit activer la fonction d'impression. Pour de plus amples informations, consultez la section Citrix Virtual Apps pour UNIX dans la documentation de Citrix Virtual Apps and Desktops.

Mapper une imprimante locale

L'application Citrix Workspace pour Linux prend en charge le pilote d'imprimante universel PS Citrix. C'est la raison pour laquelle, dans la plupart des cas, il est inutile de définir une configuration locale pour les utilisateurs souhaitant imprimer sur des imprimantes réseau ou sur des imprimantes locales connectées aux machines utilisateur. Il peut toutefois s'avérer nécessaire de mapper manuellement des imprimantes clientes sur Citrix Virtual Apps pour Windows si, par exemple, le logiciel d'impression de la machine utilisateur ne prend pas en charge le pilote d'imprimante universel.

Pour mapper une imprimante locale sur un serveur :

1. À partir de l'application Citrix Workspace, établissez une connexion avec le serveur et ouvrez une session sur un ordinateur exécutant Citrix Virtual Apps.
2. Dans le menu Démarrer, choisissez **Paramètres > Imprimantes**.
3. Dans le menu Fichier, choisissez **Ajouter l'imprimante**.

    L'assistant Ajout d'imprimante s'affiche.

4. Cet assistant permet d'ajouter une imprimante réseau à partir du réseau client, du domaine du client. Généralement, il s'agit d'un nom d'imprimante standard, similaire à ceux créés par les services Bureau à distance natifs, tels que « HPLaserJet 4 depuis nom_du_client dans la session 3 ».

   Pour plus d'informations concernant l'ajout d'imprimantes, veuillez consulter la documentation de votre système d'exploitation Windows.

Audio

Auparavant, seul le périphérique audio par défaut était mappé dans une session même lorsque de nombreux périphériques étaient disponibles sur la machine. Le périphérique mappé apparaît généralement sous le nom de **Citrix HDX Audio**.

À partir de la version 2010, l'application Citrix Workspace pour Linux affiche tous les périphériques audio locaux disponibles dans une session. Au lieu de **Citrix HDX Audio**, ils apparaissent désormais avec leurs noms de périphérique respectifs. Vous pouvez basculer dynamiquement vers n'importe quel périphérique disponible dans une session. Contrairement aux versions précédentes, vous n'avez plus besoin de sélectionner l'entrée ou la sortie audio par défaut avant de lancer la session. Les sessions sont mises à jour de manière dynamique lorsque vous branchez ou supprimez des périphériques audio.

À partir de la version 2012, la fonction de redirection audio améliorée est activée par défaut.

Pour désactiver cette fonctionnalité, procédez comme suit :

1. Accédez au dossier \<ICAROOT\>/config/ et ouvrez le fichier module.ini.
2. Accédez à la section clientaudio et ajoutez l'entrée suivante :

   VdcamVersion4Support=False

> **Remarque :**
>
> - Lorsque la fonction de redirection audio améliorée est désactivée, seul le périphérique audio par défaut portant le nom **Citrix HDX Audio** apparaît dans la session.
> - L'option **Mic et webcam** de la boîte de dialogue **Préférences** reste désactivée par défaut. Pour plus d'informations sur l'activation du micro et de la webcam, reportez-vous à la section Préférences.

Limitations connues :

- Sur un VDA s'exécutant sur Windows Server 2016, vous ne pouvez pas modifier la sélection du périphérique audio dans une session. La sélection est définie sur l'entrée et la sortie audio par défaut uniquement.
- La redirection de périphérique audio n'est pas prise en charge avec les périphériques audio Bluetooth.

- Vous pouvez modifier le périphérique audio par défaut uniquement sur les systèmes d'exploitation Windows 10, Windows 7 et Windows 8. Sur les systèmes d'exploitation Windows Server, tels que Windows Server 2012, 2016 et 2019, vous ne pouvez pas modifier le périphérique audio par défaut en raison d'une limitation dans les sessions Bureau à distance Microsoft.

Le périphérique audio par défaut est généralement le périphérique ALSA configuré par défaut pour votre système. Pour spécifier un périphérique différent, procédez comme suit :

1. Sélectionnez et ouvrez un fichier de configuration en fonction des utilisateurs que vous souhaitez voir affectés par vos modifications. Pour plus d'informations sur l'impact des mises à jour de fichiers de configuration particuliers sur différents utilisateurs, veuillez consulter la section paramètres par défaut.
2. Ajoutez l'option suivante, en créant la section si besoin est :

```
[ClientAudio]

AudioDevice = <device>
```

où l'information machine se situe dans le fichier de configuration ALSA de votre système d'exploitation.

> **Remarque :**
>
> L'emplacement de cette information peut varier en fonction des systèmes d'exploitation Linux. Pour plus de détails sur l'emplacement de cette information, Citrix vous recommande de consulter la documentation de votre système d'exploitation.

Mapper l'audio du client

Le mappage audio du client permet aux applications exécutées sur le serveur Citrix Virtual Apps ou Citrix Virtual Desktops de restituer les sons sur des périphériques audio installés sur la machine utilisateur. Vous pouvez définir la qualité audio individuellement pour chaque connexion sur le serveur, mais les utilisateurs peuvent également la configurer sur leur machine. Si les réglages de qualité audio de la machine utilisateur et du serveur diffèrent, le réglage le plus faible est utilisé.

Le mappage audio du client peut entraîner une charge excessive sur les serveurs et sur le réseau. La bande passante nécessaire au transfert des données audio croît avec la qualité audio. Une qualité audio supérieure sollicite en outre davantage les ressources système du serveur.

Vous pouvez configurer le mappage audio du client à l'aide de règles. Pour de plus amples informations, consultez la documentation de Citrix Virtual Apps and Desktops.

> **Remarque :**
>
> Le mappage audio du client n'est pas pris en charge pour les connexions à Citrix Virtual Apps sur UNIX.

Activation de l'audio UDP

L'audio UDP peut améliorer la qualité des appels téléphoniques effectués sur Internet. Il utilise le protocole UDP (User Datagram Protocol) à la place de TCP (Transmission Control Protocol).

Limitations :

- L'audio UDP n'est pas disponible dans les sessions cryptées (c'est-à-dire celles qui utilisent le cryptage TLS ou ICA). Dans de telles sessions, la transmission audio utilise TCP.
- La priorité du canal ICA peut affecter l'audio UDP.

1. Définissez les options suivantes dans la section ClientAudio du fichier module.ini :
   - Définissez EnableUDPAudio sur True. Par défaut, cette option est définie sur False, ce qui désactive l'audio UDP.
   - Spécifiez les numéros de port minimum et maximum pour le trafic audio UDP à l'aide de UDPAudioPortLow et UDPAudioPortHigh. Les ports 16500 à 16509 sont utilisés par défaut.
2. Définissez les paramètres audio client et serveur comme suit de façon à ce que l'audio soit de qualité moyenne (c'est-à-dire ni élevée ni faible).

		Qualité audio sur le client	Qualité audio sur le client	Qualité audio sur le client
		High	Moyen	Low
Qualité audio sur le serveur	High	High	Moyen	Low
Qualité audio sur le serveur	Moyen	Moyen	Moyen	Low
Qualité audio sur le serveur	Low	Low	Low	Low

UDP sur le client

Dans le fichier `$ICAROOT/config/module.ini`, ajoutez ce qui suit :

Dans la section [ClientAudio] :

EnableUDPAudio=True
UDPAudioPortLow=int

UDPAudioPortHigh=int

Dans le fichier $HOME/.ICAClient/wfclient.ini, ajoutez ce qui suit :

Dans la section [WFClient] :

AllowAudioInput=True
EnableAudioInput=true
AudioBandWidthLimit=1

> **Remarque :**
>
> Si le dossier .ICAClient n'est pas trouvé (se produit uniquement lors de la première installation et du premier lancement) lancez l'application Citrix Workspace et fermez. Cette action créé le dossier .ICAClient.

Ajoutez ce qui suit sous wfclient.ini.* Définissez la stratégie sur le DDC :

Définissez "Redirection Windows Media" sur "Interdit"
Définissez "Audio sur UDP" sur "Autorisé"
Définissez "Transport en temps réel audio via UDP" sur "Activé"
Définissez "Qualité audio" sur "Moyenne"

Modifier l'utilisation de l'application Citrix Workspace

La technologie ICA se caractérise par de faibles besoins en bande passante et en ressources de traitement. Toutefois, si vous utilisez une connexion à très faible bande passante, tenez compte des points suivants pour maintenir le niveau de performance :

- **Évitez d'accéder à des fichiers de taille importante à l'aide du mappage de lecteur client**. Lorsque vous accédez à un fichier volumineux à l'aide du mappage de lecteur client, le fichier est transféré via la connexion serveur. Si la connexion est lente, ce transfert risque de durer longtemps.
- **Évitez d'imprimer des documents volumineux sur les imprimantes locales**. Lorsque vous imprimez un document sur une imprimante locale, le fichier est transféré sur une connexion serveur. Si la connexion est lente, ce transfert risque de durer longtemps.
- **Évitez de lire du contenu multimédia**. La lecture d'un contenu multimédia requiert un volume élevé de bande passante et peut entraîner une baisse des performances.

USB

La prise en charge USB permet aux utilisateurs d'interagir avec une large gamme de périphériques USB connectés au bureau virtuel. Les utilisateurs peuvent brancher des périphériques USB sur leurs ordinateurs et les périphériques sont redirigés sur leurs bureaux virtuels. Les périphériques USB suiv-

ants sont pris en charge : lecteurs flash, smartphones, ordinateurs de poche, imprimantes, scanners, lecteurs MP3, périphériques de sécurité et tablettes.

La redirection USB nécessite Citrix Virtual Apps 7.6 (ou version ultérieure) ou Citrix Virtual Desktops. Citrix Virtual Apps ne prend pas en charge la redirection USB des périphériques de stockage de masse et requiert une configuration spéciale pour prendre en charge des périphériques audio. Pour plus d'informations, consultez la section documentation de Citrix Virtual Apps 7.6.

Les fonctionnalités isochrones des périphériques USB tels que les webcams, les micros, les haut-parleurs et les micro-casques sont prises en charge dans des environnements LAN (réseaux locaux) à faible latence et à haut débit. Mais généralement, la redirection audio ou webcam standard est plus appropriée.

Les types de périphériques suivants sont pris en charge directement dans une session Citrix Virtual Apps and Desktops ; ils n'utilisent donc pas la prise en charge USB :

- Claviers
- Souris
- Cartes à puce
- Casques
- Webcams

> **Remarque :**
>
> Les périphériques USB spécialisés (par exemple, claviers et souris 3D Bloomberg) peuvent être configurés pour utiliser la prise en charge USB. Pour plus d'informations sur la configuration des règles de stratégie pour d'autres périphériques USB spécialisés, consultez CTX119722.

Par défaut, certains types de périphériques USB ne sont pas pris en charge pour l'accès à distance via Citrix Virtual Apps and Desktops. Par exemple, une carte d'interface réseau peut être reliée à la carte système par une connexion USB interne. Il n'est pas conseillé de configurer un accès distant dans ce cas. Les types de périphériques USB suivants ne sont pas pris en charge par défaut dans une session Citrix Virtual Apps and Desktops :

- Dongles Bluetooth
- Cartes réseau intégrées
- Concentrateurs USB

Pour mettre à jour la liste par défaut des périphériques USB disponibles pour l'accès à distance, modifiez le fichier usb.conf, situé dans le répertoire $ICAROOT/. Pour de plus amples informations, consultez la section Mettre à jour la liste des périphériques USB disponibles pour l'accès à distance.

Pour permettre l'envoi des périphériques USB sur les bureaux virtuels, activez la règle de stratégie USB. Pour de plus amples informations, consultez la documentation de Citrix Virtual Apps and Desktops.

Fonctionnement de la prise en charge USB

Lorsqu'un utilisateur branche un périphérique USB, ce dernier est comparé à la stratégie USB, et s'il est autorisé, il est redirigé sur le bureau virtuel. Si la stratégie par défaut refuse le périphérique, il n'est disponible que sur le bureau local.

Pour les bureaux auxquels les utilisateurs accèdent via le mode d'appliance de bureau, lorsqu'un utilisateur branche un périphérique USB, ce périphérique est automatiquement redirigé sur le bureau virtuel. Le bureau virtuel est responsable du contrôle du périphérique USB et de son affichage dans l'interface utilisateur.

Pour que la redirection fonctionne, la fenêtre de session doit avoir le focus lorsque l'utilisateur branche le périphérique USB, sauf si le mode Desktop Appliance est utilisé.

Périphériques de stockage de masse

Si un utilisateur se déconnecte d'un bureau virtuel alors qu'un périphérique de stockage de masse USB est encore branché sur le bureau local, ce périphérique n'est pas redirigé sur le bureau virtuel lorsque l'utilisateur se reconnecte. Pour s'assurer que le périphérique de stockage de masse est effectivement redirigé sur le bureau virtuel, l'utilisateur doit retirer puis réinsérer le périphérique après la reconnexion.

> **Remarque :**
>
> Si vous connectez un périphérique de stockage de masse à un poste de travail Linux configuré pour refuser la prise en charge à distance de ce type d'équipement USB, le périphérique n'est pas accepté par le logiciel de l'application Workspace. Et un navigateur de fichiers Linux distinct peut s'ouvrir. Par conséquent, Citrix vous recommande de préconfigurer les machines utilisateur en désélectionnant par défaut l'option **Browse removable media when inserted**. Sur les périphériques Debian, utilisez la barre de menu Debian en sélectionnant **Desktop > Preferences > Removable Drives and Media**. Et sous l'onglet **Storage**, sous **Removable Storage**, désactivez la case à cocher **Browse removable media when inserted**.

Pour la redirection de périphérique USB client, tenez compte de qui suit.

> **Remarque :**
>
> - Si la stratégie de serveur Redirection du périphérique USB client est activée, les périphériques de stockage de masse sont toujours redirigés en tant que périphériques USB même si le mappage du lecteur client est activé.
> - L'application ne prend pas en charge la redirection de périphérique composite pour les périphériques USB.

Classes USB

Les classes de périphériques USB suivantes sont autorisées par les règles de stratégie USB par défaut :

- Audio (Classe 01)

  Inclut les microphones, haut-parleurs, casques et contrôleurs MIDI.

- Interface physique (Classe 05)

  Ces périphériques sont similaires aux périphériques d'interface utilisateur (HID), mais ils fournissent en général des données en temps réel et comprennent des manettes de retour de force, des plates-formes mouvantes et des exosquelettes de retour de force.

- Acquisition d'images fixes (Classe 06)

  Comprend scanners et appareils photo numériques. Les appareils photo numériques prennent généralement en charge la classe d'acquisition d'images fixes qui utilise le protocole PTP (Picture Transfer Protocol) ou MTP (Media Transfer Protocol) pour transférer des images sur un ordinateur ou un autre périphérique. Les appareils photo peuvent également apparaître en tant que périphériques de stockage de masse. Il est également possible de configurer un appareil photo pour utiliser les deux classes, par le biais des menus fournis par l'appareil photo.

  Si un appareil photo apparaît en tant que périphérique de stockage de masse, le mappage des lecteurs clients est utilisé et la prise en charge USB n'est pas requise.

- Imprimantes (Classe 07)

  En général, la plupart des imprimantes appartiennent à cette classe, à l'exception de certaines qui utilisent des protocoles spécifiques au fabricant (classe ff). Les imprimantes multifonctions peuvent disposer d'un concentrateur interne ou être des périphériques composites. Dans les deux cas, l'élément d'impression utilise généralement la classe Imprimantes et l'élément de fax ou de numérisation utilise une autre classe ; par exemple, acquisition d'images fixes.

  Les imprimantes fonctionnent correctement sans prise en charge USB.

- Stockage de masse (Classe 08)

  Les périphériques de stockage de masse les plus courants sont les lecteurs flash USB ; les disques dur USB, lecteurs CD/DVD et lecteurs de cartes SD/MMC sont également des périphériques de stockage de masse. Les périphériques disposant d'un espace de stockage interne dotés d'une interface de stockage de masse sont également nombreux ; sont compris dans cette catégorie les lecteurs multimédias, les appareils photos numériques et les téléphones portables. Sous-classes connues :

- 01 Périphériques flash limités
- 02 Lecteurs de CD/DVD (ATAPI/MMC-2)

- 03 Lecteurs de bandes (QIC-157)
- 04 Lecteurs de disquettes (UFI)
- 05 Lecteurs de disquettes (SFF-8070i)
- 06 La plupart des périphériques de stockage de masse utilisent cette variante de SCSI.

  Étant donné que le mappage des lecteurs clients peut être utilisé pour accéder à la plupart des périphériques au travers du mappage de lecteur client, la prise en charge USB n'est pas requise.

  Important : certains virus sont connus pour se propager activement à l'aide de tous les types de stockage de masse. Posez-vous la question de savoir si les besoins de votre entreprise justifient l'utilisation de périphériques de stockage de masse, soit via le mappage de lecteurs clients, soit via la prise en charge USB. Pour réduire le risque, le serveur peut être configuré pour empêcher l'exécution des fichiers via le mappage de lecteurs clients.
- Sécurité du contenu (Classe 0d)

  Les périphériques de sécurité du contenu assurent la protection du contenu, en général pour la gestion des licences ou des droits numériques. Cette classe comprend les dongles.
- Santé personnelle (Classe 0f)

  Ces appareils comprennent des capteurs de pression artérielle, des moniteurs de pouls, des podomètres, des piluliers et des spiromètres.
- Spécifique au fabricant et à l'application (Classes fe et ff)

  De nombreux périphériques utilisent des protocoles spécifiques au fabricant ou des protocoles qui n'ont pas été adoptés par le consortium USB, et ces derniers apparaissent en général en tant que spécifique au fabricant (classe ff).

Classes de périphériques USB

Les classes de périphériques USB suivantes sont refusées par les règles de stratégie USB par défaut :

- Communications et contrôle CDC (Classes 02 et 0a)

  Comprend modems, cartes RNIS, cartes réseau ainsi que certains téléphones et télécopieurs.

  La stratégie USB par défaut n'autorise pas ces périphériques, car l'un d'entre eux peut fournir la connexion au bureau virtuel.
- Périphériques d'interface utilisateur (Classe 03)

  Comprend un large éventail de périphériques d'entrée et de sortie. Les périphériques d'interface utilisateur (HID) sont composés de claviers, souris, dispositifs de pointage, tablettes graphiques, capteurs, contrôleurs de jeu, boutons et fonctions de contrôle.

La sous-classe 01 est appelée classe « boot interface » ; elle est utilisée pour les claviers et les souris.

La stratégie USB par défaut n'autorise ni les claviers USB (classe 03, sous-classe 01, protocole 1), ni les souris USB (classe 03, sous-classe 01, protocole 2). En effet, la majorité des claviers et des souris sont correctement gérés sans prise en charge USB. Il est normalement nécessaire d'utiliser ces périphériques localement ainsi qu'à distance lors de la connexion à un bureau virtuel.

- Concentrateurs USB (Classe 09)

  Les concentrateurs USB permettent de connecter des périphériques supplémentaires à l'ordinateur local. Il n'est pas nécessaire d'accéder à ces périphériques à distance.

- Cartes à puce (Classe 0b)

  Les lecteurs de carte à puce comprennent des lecteurs de carte à puce avec ou sans contact, ainsi que des jetons USB dotés d'une puce équivalente à une carte à puce.

  L'accès distant par carte à puce est utilisé pour accéder aux lecteurs de carte à puce et la prise en charge USB n'est pas nécessaire.

- Vidéo (Classe 0e)

  La classe vidéo couvre les périphériques utilisés pour manipuler les vidéos, tels que les web-cams, les caméscopes numériques, les convertisseurs vidéo analogique, certains tuner TV et certains appareils photo numériques qui prennent en charge le streaming vidéo.

  De manière générale, la compression vidéo de caméra Web HDX RealTime offre des performances optimales.

- Contrôleurs sans fil (Classe e0)

  Comprend une large gamme de contrôleurs sans fil, tels que les contrôleurs de bande ultra large et Bluetooth.

  Certains de ces appareils peuvent fournir un accès réseau critique ou connecter des périphériques critiques tels que des claviers ou des souris Bluetooth.

  La stratégie USB par défaut n'autorise pas ces appareils. Toutefois, il peut être utile pour certains appareils de fournir l'accès à l'aide de la prise en charge USB.

Liste des périphériques USB

Vous pouvez mettre à jour la gamme de périphériques USB disponibles pour l'accès à distance depuis des bureaux en modifiant la liste des règles par défaut figurant dans le fichier usb.conf sur la machine utilisateur dans le répertoire $ICAROOT/.

Pour mettre à jour la liste, ajoutez de nouvelles règles de stratégie afin d'autoriser ou de refuser des périphériques USB non compris dans la gamme par défaut. Les règles créées de cette manière par un administrateur contrôlent les périphériques qui sont offerts au serveur. Les règles sur le serveur contrôlent ensuite les périphériques qui sont acceptés.

La configuration des stratégies par défaut relative aux périphériques non autorisés est la suivante :

DENY: class=09 # Hub devices

DENY: class=03 subclass=01 # HID Boot device (keyboards and mice)

DENY: class=0b # Smartcard

DENY: class=e0 # Wireless Controllers

DENY: class=02 # Communications and CDC Control

DENY: class=03 # UVC (webcam)

DENY: class=0a # CDC Data

ALLOW: # Ultimate fallback: allow everything else

Règles de stratégie USB

Conseil : lorsque vous créez des règles de stratégie, reportez-vous aux codes de catégories USB, disponibles sur le site Web USB à l'adresse http://www.usb.org/. Les règles de stratégie figurant dans le fichier usb.conf de la machine utilisateur prennent le format {ALLOW:|DENY:} suivi d'un ensemble d'expressions reposant sur les valeurs des balises suivantes :

Balise	Description
VID	ID fournisseur du descripteur de périphérique
REL	ID de version du descripteur de périphérique
PID	ID de produit du descripteur de périphérique
Classe	Classe du descripteur de périphérique ou d'un descripteur d'interface
Sous-classe	Sous-classe du descripteur de périphérique ou d'un descripteur d'interface
Prot	Protocole à partir du descripteur de périphérique ou d'un descripteur d'interface

Lors de la création de règles de stratégies, prenez en compte les points suivants :

- Les règles ne sont pas sensibles à la casse.
- Les règles peuvent éventuellement comporter un commentaire, introduit par #, à la fin. Aucun délimiteur n'est requis et le commentaire est ignoré en cas de correspondance.
- Les espaces vides et les lignes de commentaires pures sont ignorés.
- L'espace utilisé comme séparateur est ignoré, mais il ne peut pas figurer au milieu d'un nombre ou d'un identificateur. Par exemple, Deny: Class = 08 SubClass=05 est une règle valide, mais Deny: Class=0 8 Sub Class=05 ne l'est pas.
- Les balises doivent utiliser l'opérateur de correspondance =. Par exemple, VID=1230.

Exemple

L'exemple suivant illustre une section du fichier usb.conf stocké sur une machine utilisateur. Pour que ces règles soient implémentées, le même ensemble de règles doit figurer sur le serveur.

ALLOW: VID=1230 PID=0007 # ANOther Industries, ANOther Flash Drive

DENY: Class=08 SubClass=05 # Mass Storage Devices

DENY: Class=0D # All Security Devices

Modes de démarrage

À l'aide du mode d'appliance de bureau, vous pouvez modifier la façon dont un bureau virtuel traite les périphériques USB préalablement connectés. Dans la section WfClient du fichier $ICAROOT/config/module.ini sur chaque machine utilisateur, définissez DesktopApplianceMode = Boolean comme suit.

VRAI	Les périphériques USB déjà branchés démarrent, à condition qu'ils ne soient pas bloqués au moyen d'une règle de type Deny dans les stratégies USB définies sur le serveur (dans une entrée de registre) ou sur la machine utilisateur (dans le fichier de configuration des règles de stratégie).
FAUX	Aucun périphérique USB ne démarre.

Webcams

De manière générale, la compression vidéo de caméra Web HDX RealTime offre des performances optimales. Toutefois, dans certaines circonstances, vous pouvez demander aux utilisateurs de connecter

leur caméra Web à l'aide d'un port USB. Pour ce faire, vous devez désactiver la compression vidéo de webcam HDX RealTime.

Redirection de webcam

Voici quelques indications sur la redirection de la webcam :

- La redirection de la webcam fonctionne avec et sans RTME.
- La redirection de webcam fonctionne avec les applications 32 bits. Par exemple, Skype, GoToMeeting. Utilisez un navigateur 32 bits pour vérifier la redirection de la webcam en ligne. Par exemple, www.webcamtests.com
- L'utilisation de la webcam est exclusive aux applications. Par exemple, lorsque Skype est exécuté avec une webcam et que vous lancez GoToMeeting, quittez Skype pour utiliser la webcam avec GoToMeeting.

Xcapture

Le package de l'application Citrix Workspace permet d'assister les utilisateurs dans l'échange de données graphiques entre le presse-papiers du serveur et les applications X Windows non conformes aux spécifications ICCCM sur le bureau X. Les utilisateurs peuvent utiliser xcapture pour :

- sélectionner des boîtes de dialogue ou des zones d'écran et les copier entre le bureau de la machine utilisateur (y compris les applications non conformes aux spécifications ICCCM) et une application exécutée dans une fenêtre de connexion ;
- copier des graphiques entre une fenêtre de connexion et les utilitaires de manipulation de graphiques X xmag ou xv.

Pour lancer xcapture à partir de la ligne de commande :

À partir de l'invite de commande, tapez `/opt/Citrix/ICAClient/util/xcapture` et appuyez sur ENTRÉE (où /opt/Citrix/ICAClient est le répertoire dans lequel vous avez installé l'application Citrix Workspace).

Pour copier à partir du bureau de la machine utilisateur :

1. Dans la boîte de dialogue xcapture, cliquez sur **From screen**. Le curseur prend la forme d'une croix.
2. Choisissez l'une des tâches suivantes :
    - Select a window. Placez le curseur sur la fenêtre à copier, puis cliquez sur le bouton central de la souris.
    - Select a region. Maintenez le bouton gauche de la souris enfoncé et faites glisser le curseur pour sélectionner la zone à copier.

- Cancel the selection. Cliquez avec le bouton droit de la souris. Lors du cliquer-déplacer, vous pouvez annuler la sélection en cliquant sur le bouton droit de la souris avant de relâcher le bouton central ou gauche.

3. Dans la boîte de dialogue xcapture, cliquez sur **To ICA**. Le bouton xcapture change de couleur pour indiquer que l'information est en cours de traitement.
4. Une fois le transfert terminé, utilisez la commande de collage appropriée dans l'application lancée à partir de la fenêtre de connexion.

Pour copier depuis xv vers une application située dans une fenêtre de connexion :

1. Copiez les informations à partir de xv.
2. Dans la boîte de dialogue xcapture, cliquez sur From XV et To ICA. Le bouton xcapture change de couleur pour indiquer que l'information est en cours de traitement.
3. Une fois le transfert terminé, utilisez la commande de collage appropriée dans l'application lancée à partir de la fenêtre de connexion.

Pour copier depuis une application située dans la fenêtre de connexion vers xv :

1. Copiez les informations à partir de l'application située dans la fenêtre de connexion.
2. Dans la boîte de dialogue xcapture, cliquez sur From ICA et To XV. Le bouton xcapture change de couleur pour indiquer que l'information est en cours de traitement.
3. Une fois le transfert terminé, collez les informations dans xv.

Souris

Souris relative

La prise en charge d'une souris relative fournit une option qui permet d'interpréter la position de la souris de manière relative plutôt qu'absolue. Cette capacité est requise par les applications qui exigent des entrées de souris relatives plutôt qu'absolues.

> **Remarque :**
>
> Cette fonctionnalité est uniquement disponible dans les sessions exécutées sur Citrix Virtual Apps ou Citrix Virtual Desktops 7.8 (ou version ultérieure). Elle est désactivée par défaut.

Pour activer la fonctionnalité :

Dans le fichier `$HOME/.ICAClient/wfclient.ini`, dans la section [WFClient], ajoutez l'entrée RelativeMouse=1.

Cette étape met la fonctionnalité en service tout en la gardant inactive jusqu'à ce que vous l'activiez.

> **Conseil :**

> Pour plus d'informations sur la mise en service des fonctionnalités de souris relative, reportez-vous à la section Valeurs de souris relative alternatives.

Pour activer la fonctionnalité :

Tapez Ctrl/F12.

Une fois la fonction activée, tapez Ctrl/F12 à nouveau pour synchroniser la position du pointeur du serveur avec le client. Les positions du pointeur du serveur et du client ne sont pas synchronisées lors de l'utilisation de Relative Mouse.

Pour désactiver la fonctionnalité :

Tapez Ctrl-Maj/F12.

La fonctionnalité est également désactivée lorsqu'une fenêtre de session perd le focus.

Valeurs de souris relative alternatives

Vous pouvez également utiliser les valeurs suivantes pour RelativeMouse :

- RelativeMouse=2 Met la fonctionnalité en service et l'active chaque fois qu'une fenêtre de session obtient le focus.
- RelativeMouse=3 Met en service, active et maintient la fonctionnalité activée à tout moment.
- RelativeMouse=4 Active ou désactive la fonctionnalité lorsque le pointeur de la souris côté client est masqué ou affiché. Ce mode convient pour l'activation ou la désactivation automatique de la souris relative pour les interfaces applicatives de jeux à la troisième personne.

Pour changer les commandes de clavier, ajoutez des paramètres tels que :

- RelativemouseOnChar=F11
- RelativeMouseOnShift=Maj
- RelativemouseOffChar=F11
- RelativeMouseOffShift=Maj

Les valeurs prises en charge par Citrix pour **RelativemouseOnChar** et **RelativemouseOffChar** sont répertoriées sous [Hotkey Keys] dans le fichier config/module.ini de l'arborescence d'installation de l'application Citrix Workspace. Les valeurs pour **RelativeMouseOnShift** et **RelativeMouseOffShift** définissent les touches de modification à utiliser et sont répertoriées sous l'en-tête [Hotkey Shift States].

Clavier

Comportement du clavier

Pour générer une combinaison de touches Ctrl+Alt+Suppr à distance :

1. Décidez quelle combinaison de touches la combinaison Ctrl+Alt+Suppr va créer sur le bureau virtuel distant.
2. Dans la section WFClient du fichier de configuration approprié, configurez UseCtrlAltEnd en conséquence :
    - True signifie que Ctrl+Alt+Fin transmet la combinaison Ctrl+Alt+Suppr au bureau distant.
    - False (valeur par défaut) signifie que Ctrl+Alt+Entrée transmet la combinaison Ctrl+Alt+Suppr au bureau distant.

Redirection générique

Configuration du clavier Bloomberg v4 via la redirection USB générique côté client :

La stratégie doit être activé au préalable dans un Domain Delivery Controller (DDC).

1. Recherchez les valeurs vid et pid du clavier Bloomberg. Par exemple, dans Debian et Ubuntu, exécutez la commande suivante :

    ```
    lsusb
    ```

2. Accédez à $ICAROOT et modifiez le fichier usb.conf.
3. Ajoutez l'entrée suivante dans le fichier usb.conf file pour permettre le redirection USB du clavier Bloomberg, puis enregistrez le fichier.

    ALLOW: vid=1188 pid=9545

4. Redémarrez le démon ctxusbd sur le client. Par exemple, dans Debian et Ubuntu, exécutez la commande suivante :

    ```
    systemctl restart ctxusbd
    ```

5. Lancez une session client. Assurez-vous que la session a le focus lorsque vous branchez le clavier Bloomberg v4 pour le rediriger.

Redirection sélective

Cette fonctionnalité permet d'utiliser l'interface du clavier Bloomberg v4 sur plusieurs sessions. Cette fonctionnalité offre davantage de flexibilité pour utiliser le clavier sur toutes les sessions distantes, à l'exception de l'empreinte digitale et des interfaces audio. L'empreinte digitale et les interfaces audio sont redirigées vers des sessions uniques comme auparavant.

Vous pouvez effectuer la redirection du clavier Bloomberg comme suit :

- via la redirection USB générique
- via la redirection USB générique et avec la prise en charge de la redirection sélective

> **Remarque :**
>
> Cette fonctionnalité est activée par défaut sur les plates-formes x86 et x64 mais désactivée sur les plates-formes ARMHF.

Pour activer la fonctionnalité :

1. Modifiez la section BloombergRedirection comme suit dans le fichier config/All_Regions.ini.

   ```
   BloombergRedirection=true
   ```

2. Effectuez toutes les étapes mentionnées dans Redirection générique.

Pour désactiver la fonctionnalité :

1. Modifiez la section BloombergRedirection dans le fichier config/All_Regions.ini.
2. Définissez la valeur BloombergRedirection sur false.

   ```
   BloombergRedirection=false
   ```

3. Effectuez toutes les étapes mentionnées dans Redirection générique.

> **Remarque :**
>
> En définissant la valeur sur false, la fonctionnalité retourne au comportement qu'elle adoptait dans les versions précédentes du client, où toutes les interfaces sont redirigées vers une session unique.

Redirection du contenu du navigateur

Chromium Embedded Framework (CEF) pour la redirection du contenu du navigateur [Fonction expérimentale]

Dans les versions antérieures à la version 1912, la redirection du contenu du navigateur utilisait une superposition basée sur WebkitGTK+ pour rendre le contenu. Cependant, des problèmes de performance ont été constatés sur les clients légers. À partir de la version 1912, la redirection du contenu du navigateur utilise une superposition basée sur CEF. Cette fonctionnalité enrichit l'expérience utilisateur en matière de redirection du contenu du navigateur. Elle permet de décharger l'utilisation du réseau, le traitement des pages et le rendu graphique sur le point de terminaison.

Activer la redirection du contenu du navigateur basée sur CEF

Pour activer la redirection du contenu du navigateur basée sur CEF, procédez comme suit :

1. Modifiez le fichier situé dans :
   `$ICAROOT/config/All_Regions.ini`
   où $ICAROOT est le répertoire d'installation par défaut de l'application Citrix Workspace.

2. Ajoutez l'entrée suivante dans la section [Client Engine\WebPageRedirection] :

```
UseCefBrowser=true
```

Problème connu :

- Lorsque vous définissez l'option `UseCefBrowser` sur **`true`** dans ~/`.ICAClient/All_Regions.ini`, l'éditeur IME japonais, chinois et coréen peut ne pas fonctionner dans les champs de saisie. L'application Citrix Workspace pour Linux ne prend pas en charge l'éditeur IME japonais, chinois et coréen lors de l'utilisation du SaaS sécurisé avec le navigateur Citrix intégré.

Pour de plus amples informations sur la redirection du contenu du navigateur, consultez la section Redirection du contenu du navigateur dans la documentation Citrix Virtual Apps and Desktops.

Reconnexion automatique

Cette rubrique décrit la fonction HDX Broadcast - Reconnexion automatique des clients. Citrix recommande d'utiliser cette dernière avec la fonctionnalité de fiabilité de session HDX Broadcast.

Les utilisateurs peuvent être déconnectés de leurs sessions en raison d'un manque de fiabilité réseau, de temps d'attente réseau très variables ou de limites des terminaux sans fil. Avec la fonction Reconnexion automatique des clients, l'application Citrix Workspace pour Linux peut détecter les déconnexions de session involontaires et reconnecter automatiquement les utilisateurs à leurs sessions.

Lorsque cette fonctionnalité est activée sur le serveur, les utilisateurs n'ont pas besoin de se reconnecter manuellement pour continuer à travailler. Citrix Workspace essaie de se reconnecter à la session (un nombre de fois défini) jusqu'à ce que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion. Si l'authentification utilisateur est requise, une boîte de dialogue invitant l'utilisateur à entrer ses informations d'identification s'affiche lors des reconnexions automatiques. Aucune reconnexion automatique n'a lieu lorsqu'un utilisateur quitte une application sans fermer la session. Les utilisateurs ne peuvent se reconnecter qu'à des sessions déconnectées.

Par défaut, l'application Citrix Workspace pour Linux attend 30 secondes avant de retenter une reconnexion à une session déconnectée et tente de se reconnecter à cette session trois fois.

Lors de la connexion via AccessGateway, ACR n'est pas disponible. Pour vous protéger contre les pannes réseau, assurez-vous que la fiabilité de session est activée sur le serveur et le client, et qu'elle est également configurée sur AccessGateway.

Pour accéder à des instructions sur la configuration de la fonctionnalité de reconnexion automatique des clients HDX Broadcast, consultez la documentation de Citrix Virtual Apps and Desktops.

Fiabilité de session

Cette rubrique décrit la fonctionnalité de fiabilité de session HDX Broadcast, qui est activée par défaut.

Grâce à la fonctionnalité de fiabilité de session HDX Broadcast, la fenêtre d'une application publiée est toujours affichée même si la connexion à l'application subit des interruptions. Par exemple, les utilisateurs dotés de connexions sans fil entrant dans un tunnel peuvent perdre leur connexion à l'entrée d'un tunnel, pour la reprendre à la sortie. Durant l'interruption, les données de l'utilisateur, les touches sur lesquelles ils appuient et d'autres interactions sont toutes stockées, et l'application semble figée. Lorsque la connexion est rétablie, ces interactions sont réappliquées dans l'application.

Lorsque la reconnexion automatique des clients et la fiabilité de session sont configurées, la fiabilité de session a priorité s'il y a un problème de connexion. La fiabilité de session essaye de rétablir une connexion à la session existante. La détection d'un problème de connexion peut prendre jusqu'à 25 secondes, en plus d'une période configurable (la valeur par défaut est de 180 secondes) pour la tentative de reconnexion. Si la fiabilité de session ne parvient pas à se reconnecter, la reconnexion automatique des clients tente de se reconnecter.

si la fiabilité de session HDX Broadcast est activée, le port par défaut utilisé pour les communications passe de 1494 à 2598.

Les utilisateurs de Citrix Workspace ne peuvent pas remplacer les réglages du serveur.

> **Important :**
>
> La fiabilité de session HDX Broadcast requiert qu'une autre fonctionnalité, Common Gateway Protocol, soit activée (à l'aide de paramètres de stratégie) sur le serveur. La désactivation de Common Gateway Protocol désactive également la fiabilité de session HDX Broadcast.

Performances multimédias

L'application Citrix Workspace intègre une large gamme de technologies offrant une expérience utilisateur haute définition dans les environnements utilisateur riches en multimédia. Ces dernières améliorent l'expérience utilisateur lors de la connexion aux applications et bureaux hébergés comme suit :

- Redirection Windows Media HDX Mediastream
- Redirection HDX MediaStream Flash
- Compression vidéo pour caméra Web HDX RealTime
- H.264

> **Remarque :**
>
> Citrix prend en charge la coexistence RTOP avec l'application Citrix Workspace pour Linux version 1901 et versions ultérieures avec GStreamer 0.1.

Redirection Windows Media HDX Mediastream

La redirection HDX Mediastream Windows Media évite les besoins excessifs en bande passante pour la capture et la lecture multimédia sur des bureaux Windows virtuels auxquels les utilisateurs accèdent depuis des machines utilisateur Linux. La redirection Windows Media offre un mécanisme de lecture des fichiers d'exécution multimédia sur la machine utilisateur plutôt que sur le serveur. Ainsi, les besoins en bande passante pour la lecture de fichiers multimédia sont limités.

La redirection Windows Media améliore les performances du lecteur Windows Media et les lecteurs compatibles exécutés sur des bureaux virtuels Windows. Un large éventail de formats de fichiers est pris en charge, notamment :

- Advanced Systems Format (ASF) ;
- Motion Picture Experts Group (MPEG) ;
- Audio-Video Interleaved (AVI) ;
- MPEG Audio Layer-3 (MP3) ;
- fichiers son WAV.

L'application Citrix Workspace comprend un tableau de traduction texte configurable, MediaStreamingConfig.tbl, pour la traduction des GUID des formats multimédia spécifiques à Windows en types MIME utilisables par GStreamer. Vous pouvez mettre à jour le tableau de traduction en effectuant les opérations suivantes :

- Ajoutez des formats de filtres/fichiers multimédia précédemment inconnus ou non pris en charge au tableau de traduction.
- Bloquez les GUID problématiques pour obliger le retour à la restitution côté serveur.
- Ajoutez des paramètres supplémentaires aux chaînes MIME existantes pour permettre la résolution des problèmes des formats problématiques en modifiant les paramètres GStreamer d'un flux.
- Gérez puis déployez les configurations personnalisées dépendant des types de fichiers multimédia pris en charge par GStreamer sur une machine utilisateur.

Avec la récupération côté client, vous pouvez également autoriser la machine utilisateur à streamer du multimédia directement depuis des adresses URL au format http://, <mms://> ou <rtsp://> plutôt que via un serveur Citrix. Le serveur est chargé de diriger la machine utilisateur vers le multimédia et d'envoyer les commandes de contrôle (y compris Lecture, Pause, Stop, Volume, Recherche). Cependant il ne traite aucune donnée multimédia. Cette fonctionnalité nécessite des bibliothèques multimédias GStreamer sur le périphérique.

Pour implémenter la redirection HDX Mediastream Windows Media :

1. Installez GStreamer 0.10, une infrastructure multimédia open-source, sur chaque machine utilisateur sur laquelle il est requis. En général, vous installez GStreamer avant d'installer l'application Citrix Workspace afin de permettre au processus d'installation de configurer l'application Citrix Workspace pour l'utiliser.

La plupart des distributions Linux incluent GStreamer. Vous pouvez également télécharger GStreamer à l'adresse http://gstreamer.freedesktop.org.

2. Pour activer la récupération côté client, installez les *plug-ins* de source de protocole GStreamer requis pour les types de fichiers que les utilisateurs lisent sur la machine. Vous pouvez vérifier qu'un plug-in est installé et opérationnel à l'aide de l'utilitaire gst-launch. Si gst-launch peut lire l'URL, le plug-in requis est opérationnel. Par exemple, exécutez `gst-launch-0.10 playbin2 uri=<http://example-source/file.wmv>` et vérifiez que la vidéo est lue correctement.
3. Lors de l'installation de l'application Citrix Workspace sur la machine, sélectionnez l'option GStreamer si vous utilisez le script tarball (ceci est réalisé automatiquement pour les packages .deb et .rpm).

Tenez compte de ce qui suit à propos de la fonctionnalité de récupération côté client :

- Cette fonctionnalité est activée par défaut. Vous pouvez la désactiver à l'aide de l'option SpeedScreenMMACSFEnabled dans la section Multimedia du fichier All-Regions.ini. Lorsque cette option est définie sur False, la redirection Windows Media est utilisée pour le traitement multimédia.
- Par défaut, toutes les fonctionnalités MediaStream utilisent le protocole GStreamer playbin2. Vous pouvez utiliser le protocole playbin antérieur pour toutes les fonctionnalités MediaStream à l'exception de la récupération côté client, qui continue à utiliser playbin2, à l'aide de l'option SpeedScreenMMAEnablePlaybin2 dans la section Multimedia du fichier All-Regions.ini.
- L'application Citrix Workspace ne reconnaît pas les fichiers de playlist ou les fichiers d'informations de configuration de flux tels que les fichiers .asx ou .nsc. Si possible, les utilisateurs doivent spécifier une adresse URL standard qui ne fait pas référence à ces types de fichiers. Utilisez gst-launch pour vérifier la validité de l'URL.

Note à propos de GStreamer 1.0 :

- Par défaut, GStreamer 0.10 est utilisé pour la redirection HDX MediaStream Windows Media. GStreamer 1.0 est utilisé uniquement lorsque GStreamer 0.10 n'est pas disponible.
- Si vous souhaitez utiliser GStreamer 1.0, suivez les instructions ci-dessous :

1. Localisez le répertoire d'installation des plug-ins GStreamer. En fonction de votre distribution, de l'architecture du système d'exploitation et de la manière dont vous installez GStreamer, l'emplacement d'installation des plug-ins varie. Le chemin d'accès de l'installation par défaut est /usr/lib/x86_64-linux-gnu/gstreamer-1.0 ou $HOME /.local/share/gstreamer-1.0.
2. Localisez le répertoire d'installation de l'application Citrix Workspace pour Linux. Pour un utilisateur (racine) privilégié, le répertoire d'installation par défaut est /opt/Citrix/ICAClient. Pour un utilisateur non privilégié, le répertoire d'installation par défaut est $HOME/ICAClient/plateforme (où la plate-forme peut être linuxx64, par exemple). Pour de plus amples informations, consultez Installer et configurer.
3. Installez libgstflatstm1.0.so en créant un lien symbolique dans le répertoire des plug-ins

GStreamer : dans -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so. Cette étape peut nécessiter des autorisations élevées, par exemple avec sudo.

4. Utilisez gst_play1.0 en tant que lecteur : dans -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play. Cette étape peut nécessiter des autorisations élevées, par exemple avec sudo.

- Si vous souhaitez utiliser GStreamer 1.0 dans la Compression vidéo de Webcam HDX RealTime, utilisez gst_read1.0 en tant que lecteur : dans -sf $ICACLIENT_DIR/util/gst_read1.0 $ICACLIENT_DIR/util/gst_read.

Activer GStreamer 1.x

Dans les versions antérieures à 1912, GStreamer 0.10 était la version par défaut prise en charge pour la redirection multimédia. À partir de la version 1912, vous pouvez configurer GStreamer 1.x comme version par défaut.

Limitations :

- Lorsque vous lisez une vidéo, la recherche en avant et en arrière peut ne pas fonctionner comme prévu.
- Lorsque vous lancez l'application Citrix Workspace sur des appareils ARMHF, GStreamer 1.x peut ne pas fonctionner comme prévu.

Installer GStreamer 1.x

Installez l'infrastructure GStreamer 1.x et les plug-ins suivants à partir de https://gstreamer.freedesktop.org/documentation/installing/on-linux.html :

- Gstreamer-plugins-base
- Gstreamer-plugins-bad
- Gstreamer-plugins-good
- Gstreamer-plugins-ugly
- Gstreamer-libav

Créer des fichiers binaires localement

Sur certaines distributions de systèmes d'exploitation Linux, par exemple SUSE et openSUSE, le système peut ne pas trouver les packages GStreamer dans la liste des sources par défaut. Dans ce cas, téléchargez le code source et créez tous les fichiers binaires localement :

1. Téléchargez le code source à partir de https://gstreamer.freedesktop.org/src/.
2. Extrayez le contenu.
3. Accédez au répertoire où le package décompressé est disponible.

4. Exécutez les commandes suivantes :

```
$sudo ./configure
$sudo make
$sudo make install
```

Par défaut, les fichiers binaires générés sont disponibles dans */usr/local/lib/gstreamer-1.0/*.

Pour plus d'informations sur la résolution des problèmes, consultez l'article CTX224988 du centre de connaissances.

Configurer GStreamer 1.x

Pour configurer GStreamer 1.x à utiliser avec l'application Citrix Workspace, appliquez la configuration suivante à l'aide de l'invite de shell :

- $ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so.
- $ln -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play

Où,

- ICACLIENT_DIR est le chemin d'installation de l'application Citrix Workspace pour Linux.
- GST_PLUGINS_PATH est le chemin du plug-in de GStreamer. Par exemple, sur une machine Debian 64 bits, il s'agit de */usr/lib/x86_64-linux-gnu/gstreamer-1.0/*.

Limitations :

- Lors de l'utilisation de GStreamer version 1.15.1 ou ultérieure, la redirection de webcam peut échouer et la session peut être déconnectée.

Redirection HDX MediaStream Flash

La redirection HDX Mediastream pour Flash permet de lire du contenu Adobe Flash sur des machines utilisateur, offrant ainsi une lecture audio et vidéo haute définition, sans augmenter les besoins en bande passante.

1. Assurez-vous que votre machine utilisateur dispose des fonctionnalités requises. Pour de plus amples informations, consultez Configuration système requise.
2. Ajoutez les paramètres suivants à la section [WFClient] du fichier wfclient.ini (pour toutes les connexions effectuées par un utilisateur spécifique) ou à la section [Client Engine\Application Launching] du fichier All_Regions.ini (pour tous les utilisateurs de votre environnement) :
    - **HDXFlashUseFlashRemoting=Ask**: **Never**; **Always**

Active HDX MediaStream pour Flash sur la machine utilisateur. Par défaut, la valeur définie est **Never** et une boîte de dialogue demande aux utilisateurs s'ils souhaitent optimiser le contenu Flash lorsqu'ils se connectent à des pages Web présentant ce contenu.

- **HDXFlashEnableServerSideContentFetching=Disabled**; **Enabled**

  Active ou désactive la récupération de contenu côté serveur pour l'application Citrix Workspace. Par défaut, la valeur définie est **Disabled**.

- **HDXFlashUseServerHttpCookie=Disabled**; **Enabled**

  Active ou désactive la redirection des cookies HTTP. Par défaut, cette option est définie sur **Disabled**.

- **HDXFlashEnableClientSideCaching=Disabled**; **Enabled**

  Active ou désactive la mise en cache côté client du contenu Web récupéré par l'application Citrix Workspace. Par défaut, la valeur définie est **Enabled**.

- **HDXFlashClientCacheSize= [25-250]**

  Définit la taille du cache côté client, en Mo. Cette taille peut être comprise entre 25 et 250 Mo. Lorsque la taille limite est atteinte, le contenu existant dans le cache est supprimé pour permettre le stockage de nouveau contenu. Par défaut, cette option est définie sur **100**.

- **HDXFlashServerSideContentCacheType=Persistent**: **Temporary**; **NoCaching**

  Définit le type de mise en cache utilisé par l'application Citrix Workspace pour le contenu récupéré côté serveur. Par défaut, cette option est définie sur **Persistent**.

  Remarque : ce paramètre est requis seulement lorsque **HDXFlashEnableServerSideContentFetching**est défini sur la valeur **Enabled**.

3. La redirection Flash est désactivée par défaut. Dans /config/module.ini, changez FlashV2=Off sur FlashV2=On pour activer cette fonctionnalité.

Compression vidéo pour caméra Web HDX RealTime

HDX RealTime inclut une option de compression vidéo de caméra Web permettant d'améliorer l'efficacité de la bande passante au cours de conférences vidéo. Ainsi, les utilisateurs bénéficient de performances optimales lorsqu'ils se servent d'applications telles que GoToMeeting avec HD Faces ou Skype Entreprise.

1. Assurez-vous que votre machine utilisateur dispose des fonctionnalités requises.

2. Assurez-vous que le canal virtuel `Multimedia` est activé. Pour cela, ouvrez le fichier de configuration module.ini situé dans le répertoire $ICAROOT/config et assurez-vous que `MultiMedia` est défini sur la valeur « On » à la section [ICA3.0].
3. Activez l'entrée audio en cliquant sur Utiliser mon micro et ma webcam sur la page Mic et webcam de la boîte de dialogue Préférences.

Désactiver la compression vidéo de caméra Web HDX RealTime

De manière générale, la compression vidéo de caméra Web HDX RealTime offre des performances optimales. Toutefois, dans certaines circonstances, vous pouvez demander aux utilisateurs de connecter leur caméra Web à l'aide d'un port USB. Pour ce faire, vous devez effectuer les tâches suivantes :

- Désactiver la compression vidéo de webcam HDX RealTime
- Activer la prise en charge USB pour les webcams

1. Ajoutez le paramètre suivant à la section [WFClient] du fichier .ini approprié :

   HDXWebCamEnabled=Off

   Pour de plus amples informations, consultez paramètres par défaut.
2. Ouvrez le fichier usb.conf, généralement situé sous $ICAROOT/usb.conf.
3. Supprimez ou ajoutez en commentaire la ligne suivante :

   > DENY: class=0e # UVC (valeur par défaut via la compression vidéo pour webcam HDX RealTime)
4. Enregistrez, puis fermez le fichier.

SaaS sécurisé avec navigateur Citrix intégré fonctionnalité expérimentale

L'accès sécurisé aux applications SaaS assure une expérience utilisateur unifiée qui met des applications SaaS publiées à la disposition des utilisateurs. Les applications SaaS sont disponibles avec Single Sign-on. Les administrateurs peuvent à présent protéger le réseau de l'organisation et les machines des utilisateurs finaux contre les logiciels malveillants et les fuites de données en filtrant l'accès à des sites Web et des catégories de sites Web spécifiques.

L'application Citrix Workspace pour Linux prend en charge l'utilisation d'applications SaaS avec le service de contrôle d'accès. Le service permet aux administrateurs d'offrir une expérience homogène, intégrant Single Sign-on, et l'inspection du contenu.

Conditions préalables :

Assurez-vous que le package `libgtkglext1` est disponible.

La mise à disposition d'applications SaaS depuis le cloud présente les avantages suivants :

- Configuration simple : simplicité d'exploitation, de mise à jour et d'utilisation.
- Single Sign-on : ouverture de session sans problème avec Single Sign-on.
- Modèle standard pour différentes applications : configuration d'applications populaires basée sur un modèle.

> **Remarque :**
>
> SaaS avec Citrix Browser Engine est pris en charge uniquement sur les plates-formes x64 et x86 et non sur le matériel ArmHardFloatPort (armhf).

Pour plus d'informations sur la configuration d'applications SaaS à l'aide des services de contrôle d'accès, reportez-vous à la documentation sur le Contrôle d'accès.

Pour plus d'informations sur les applications SaaS avec l'application Citrix Workspace, consultez la section Configuration de l'espace de travail dans la documentation e l'application Citrix Workspace pour Windows.

H.264

L'application Citrix Workspace prend en charge l'affichage des graphiques H.264, y compris les graphiques HDX 3D Pro, qui sont traités par Citrix Virtual Apps and Desktops 7. Cette prise en charge utilise le codec de compression profonde, qui est activé par défaut. Comparativement au codec JPEG existant, cette fonctionnalité offre de meilleures performances pour les applications graphiques professionnelles sur les réseaux WAN.

Suivez les instructions fournies dans cette rubrique pour désactiver cette fonctionnalité (et traiter les graphiques à l'aide du codec JPEG). Vous pouvez également désactiver le suivi du texte tout en bénéficiant toujours de la prise en charge du codec de compression profonde. Cela permet de réduire les coûts UC lors du traitement de graphiques qui incluent des images complexes mais très peu de texte ou du texte non critique.

> **Important :**
>
> Pour configurer cette fonctionnalité, n'utilisez pas de paramètre sans perte dans la stratégie Qualité visuelle de Citrix Virtual Apps and Desktops. Si vous utilisez un paramètre avec perte, le codage H.264 est désactivé sur le serveur et ne fonctionne pas dans l'application Citrix Workspace.

Pour désactiver la prise en charge du codec de compression profonde :

Dans le fichier wfclient.ini, définissez **H264Enabled** sur False. Cela désactive également le suivi de texte.

Pour désactiver le suivi de texte uniquement

Avec la prise en charge du codec de compression profonde activée, dans le fichier wfclient.ini, définissez **TextTrackingEnabled** sur False.

Mosaïques d'écran

Vous pouvez améliorer la façon dont les mosaïques d'écran encodées en JPEG sont traitées à l'aide des fonctionnalités décodage de bitmaps directement sur l'écran, décodage des mosaïques par lots et XSync différée.

1. Assurez-vous que votre bibliothèque JPEG prend en charge ces fonctionnalités.
2. Dans la section Thinwire3.0 du fichier wfclient.ini, définissez DirectDecode et BatchDecode sur True.

   Remarque : l'activation du décodage des mosaïques par lots active également la XSync différée.

Journalisation

Dans les versions antérieures, les fichiers `debug.ini` et `module.ini` étaient utilisés pour configurer la journalisation.

À partir de la version 2009, vous pouvez configurer la journalisation à l'aide de l'une des méthodes suivantes :

- Interface de ligne de commande
- Interface utilisateur graphique (GUI)

Également à partir de la version 2009, le fichier de configuration `debug.ini` est supprimé du package d'installation de l'application Citrix Workspace.

La journalisation capture les détails du déploiement de l'application Citrix Workspace, les modifications de configuration et les activités administratives dans une base de données de journalisation. Un développeur tiers peut tirer parti de ce mécanisme de journalisation à l'aide du SDK de journalisation, qui est fourni dans le cadre du SDK d'optimisation de la plate-forme de l'application Citrix Workspace.

Vous pouvez utiliser les informations de journalisation pour effectuer les opérations suivantes :

- Diagnostiquer et résoudre les problèmes qui se produisent après toute modification. Le journal fournit une arborescence hiérarchique.
- Assister la gestion des modifications et suivre les configurations.
- Signaler les activités administratives.

Si l'application Citrix Workspace est installée avec des privilèges utilisateur racine, les journaux sont stockés dans `/var/log/ICAClient.log`. Sinon, les journaux sont stockés dans `${ HOME } /.ICAClient/logs/ICAClient.log`.

Interface de ligne de commande

1. À l'invite de commandes, accédez au chemin d'accès `/opt/Citrix/ICAClient/util`.

2. Exécutez la commande suivante pour définir les préférences du journal.

```
./setlog help
```

Toutes les commandes disponibles sont affichées.

Le tableau suivant répertorie divers modules et leurs valeurs de classe de trace correspondantes. Utilisez le tableau suivant pour obtenir un ensemble spécifique de valeurs de journal de ligne de commande :

Module	Classe de journal
Assertions	LOG_ASSERT
Moniteur audio	TC_CM
Redirection du contenu du navigateur (BCR) avec CEF	TC_CEFBCR
Mappage audio du client	TC_CAM
Centre de connexion	TC_CONNCENTER
Port de communication client	TC_CCM
Mappage des lecteurs clients	TC_CDM
Clip	TC_CLIP
Mappage d'imprimante client	TC_CPM
Mappage d'imprimante client	TC_CPM
Police	TC_FONT
Trame	TC_FRAME
Abstraction graphique	TC_GA
Éditeur de méthode d'entrée	TC_IME
IPC	TC_IPC
Mappage de clavier	TC_KEY
Pilote de licence	TC_VDLIC
Multimédia	TC_MMVD
Mapping de souris	TC_MOU
MS Teams	TC_MTOP
Autres bibliothèques	TC_LIB
Pilote de protocole	TC_PD
Magasin PNA	TC_PN

Module	Classe de journal
Journaux d'événements standard	LOG_CLASS
SRCC	TC_SRCC
Connexion SSPI	TC_CSM
Carte à puce	TC_SCARDVD
Libre-service	TC_SS
Extension libre-service	TC_SSEXT
Bibliothèque StoreFront	TC_STF
Pilote de transport	TC_TD
Thinwire	TC_TW
Interface utilisateur transparente	TC_TUI
Canal virtuel	TC_VD
PAL	TC_VP
Interface utilisateur	TC_UI
UIDialogLibWebKit3	TC_UIDW3
UIDialogLibWebKit3_ext	TC_UIDW3E
Démon USB	TC_CTXUSB
Pilote de trames vidéo	TC_VFM
Kit Web	TC_WEBKIT
Pilote WinStation	TC_WD
WfICA	TC_NCS
Moteur Wfica	TC_WENG
Wfica Shell	TC_WFSHELL
Aide Web	TC_WH
Aucune latence	TC_ZLC

GUI

Accédez à **Menu** > **Préférences**. La boîte de dialogue **Préférences de Citrix Workspace** s'affiche.

Les valeurs suivantes sont disponibles, chacune offrant des niveaux de traçage croissants :

- Désactivé
- Uniquement les erreurs
- Normal
- Détaillé

Par défaut, l'option **Journalisation** est définie sur **Normal**.

Compte tenu du volume important de données qui peut être généré, le suivi peut affecter de manière considérable les performances de l'application Citrix Workspace. Le niveau **Détaillé** n'est pas recommandé, à moins que cela ne soit nécessaire à des fins de dépannage.

Cliquez sur **Enregistrer et fermer** après avoir sélectionné le niveau de journalisation souhaité. Les modifications sont appliquées dynamiquement dans la session.

Cliquez sur l'icône des paramètres en regard du menu déroulant de l'option **Journalisation**. La boîte de dialogue **Préférences du journal Citrix** s'affiche.

> **Remarque :**
>
> Si vous supprimez le fichier `ICAClient.log`, vous devez redémarrer le service de journalisation `ctxlogd`.
>
> Par exemple, si vous utilisez une installation compatible avec systemd, exécutez la commande suivante :

`systemctl restart ctxlogd`.

Activer la journalisation sur les versions 2006 et antérieures :

Si vous utilisez les versions 2006 et antérieures, activez la journalisation à l'aide de la procédure suivante :

1. Téléchargez et installez l'application Citrix Workspace sur votre machine Linux.
2. Définissez la variable d'environnement `ICAROOT` sur l'emplacement d'installation.

   Par exemple, `/opt/Citrix/ICAClient`.

   Par défaut, la classe de trace `TC_ALL` est activée pour fournir toutes les traces.
3. Pour collecter des journaux pour un module particulier, ouvrez le fichier `debug.ini` sur `$ICAROOT` et ajoutez les
   paramètres de traçage requis à la section [wfica].

   Ajoutez les classes de trace avec un symbole « + ». Par exemple, +TC_LIB

   Vous pouvez ajouter plusieurs classes séparées par le symbole de barre verticale.
   Par exemple, +TC_LIB|+TC_MMVD.

Le tableau suivant répertorie divers modules et leurs valeurs de classe de trace correspondantes :

Dépannage :

Si `ctxlogd` ne répond plus, les journaux sont suivis dans syslog.

Pour plus d'informations sur l'obtention de nouveaux journaux et de journaux actualisés lors des lancements ultérieurs, reportez-vous à la section Configuration Syslog.

Configuration Syslog

Par défaut, tous les journaux syslog sont enregistrés dans /var/log/syslog. Vous pouvez configurer le nom et le chemin du fichier journal en modifiant la ligne suivante sous la section [RULES] dans le fichier `/etc/rsyslog.conf`. Par exemple,

```
1 user.* -/var/log/logfile_name.log
```

Enregistrez vos modifications et redémarrez le service syslog à l'aide de la commande :

```
sudo service rsyslog restart
```

Points à retenir :

- Pour vous assurer qu'un nouveau serveur syslog est disponible, supprimez syslog et exécutez la commande : `sudo service rsyslog restart`.
- Pour éviter les messages en double, ajoutez **$RepeatedMsgReduction on** au début du fichier `rsyslog.conf`.
- Pour recevoir les journaux, assurez-vous que la ligne **$ModLoad imuxsock.so** ne contient pas de commentaires au début du fichier `rsyslog.conf`.

Journalisation à distance

Pour activer la journalisation à distance sur :

- **Configuration côté serveur :** supprimez les commentaires des lignes suivantes dans le fichier rsyslog.conf du serveur syslog :

  ```
  $ModLoad imtcp

  $InputTCPServerRun 10514
  ```

- **Configuration côté client :** ajoutez la ligne suivante en remplaçant localhost par l'adresse IP du serveur distant :

  ```
  *.* @@localhost:10514
  ```


Optimisation pour Microsoft Teams

Optimisation pour Microsoft Teams à l'aide de l'application Citrix Workspace et de Citrix Virtual Apps and Desktops. L'optimisation pour Microsoft Teams est similaire à l'optimisation HDX RealTime pour Microsoft Skype Entreprise. La différence est que nous regroupons tous les composants nécessaires à l'optimisation pour Microsoft Teams dans le VDA et l'application Workspace pour Linux.

L'application Citrix Workspace pour Linux prend en charge les fonctionnalités audio, vidéo et de de partage d'écran avec l'optimisation Microsoft Teams.

> **Remarque :**
>
> - L'optimisation Microsoft Teams est prise en charge uniquement sur les distributions Linux x64.

Pour plus d'informations sur l'activation de la journalisation, suivez les étapes mentionnées sous Journalisation pour Microsoft Teams.

Pour plus d'informations sur la configuration système requise, reportez-vous à la section Optimisation Microsoft Teams.

Pour plus d'informations, veuillez consulter Optimisation pour Microsoft Teams et Redirection Microsoft Teams.

Journalisation pour Microsoft Teams

Pour activer la journalisation pour Microsoft Teams :

1. Accédez au fichier `/opt/Citrix/ICAClient/debug.ini`.
2. Modifiez la section [HDXTeams] comme suit :

```
[HDXTeams]
; Retail logging for HDXTeams 0/1 = disabled/enabled
HDXTeamsLogSwitch = 1
; Debug logging; , It is in decreasing order
; LS_NONE = 4, LS_ERROR = 3, LS_WARNING = 2, LS_INFO = 1,
   LS_VERBOSE = 0
WebrtcLogLevel = 0
; None = 5, Info = 4, Warning = 3, Error = 2, Debug = 1, Trace = 0
WebrpcLogLevel = 0
```


Prise en charge du canal virtuel NetScaler App Experience (NSAP)

Auparavant disponible en tant que fonctionnalité expérimentale, la fonctionnalité de canal virtuel NetScaler App Experience (NSAP) est désormais entièrement prise en charge. Toutes les données HDX Insight proviennent exclusivement du canal virtuel NSAP et sont envoyées non compressées. Cette approche améliore la scalabilité et les performances des sessions. Le canal virtuel NSAP est activé par défaut. Pour la désactiver, désactivez l'indicateur VDNSAP `VDNSAP=Off` dans le fichier module.ini.

Pour plus d'informations, consultez HDX Insight dans la documentation de Linux Virtual Delivery Agent et HDX Insight dans la documentation de Citrix Application Delivery Management Service.

Persistance de disposition de plusieurs moniteurs

Cette fonctionnalité conserve les informations de disposition du moniteur de la session sur les points de terminaison. La session apparaît sur le ou les mêmes moniteurs selon la configuration.

Conditions préalables :

Cette fonctionnalité nécessite les éléments suivants :

- StoreFront v3.15 ou version ultérieure
- Si .ICAClient est déjà présent dans le dossier de base de l'utilisateur actuel :

  Supprimez le fichier All_Regions.ini

  ou

  Pour conserver le fichier AllRegions.ini, ajoutez les lignes suivantes à la fin de la section [Client Engine\Application Launching] :

  SubscriptionUrl=

  PreferredWindowsBounds=

  PreferredMonitors=

  PreferredWindowState=

  SaveMultiMonitorPref=

Si le dossier .ICAClient n'est pas présent, cela indique une nouvelle installation de l'application Citrix Workspace. Dans ce cas, le paramètre par défaut des fonctionnalités est conservé.

Cas d'utilisation

- Lancez une session sur un moniteur en mode fenêtré et enregistrez le paramètre.
  Lorsque vous relancez la session, elle apparaît dans le même mode, sur le même moniteur et dans la même position.

- Lancez une session sur un moniteur en mode plein écran et enregistrez le paramètre. Lorsque vous relancez la session, elle apparaît en mode plein écran sur le même moniteur.
- Étirez et répartissez une session en mode fenêtré sur plusieurs moniteurs, puis passez en mode plein écran. La session continue en plein écran sur tous les moniteurs. Lorsque vous relancez la session, elle apparaît en mode plein écran et couvre tous les moniteurs.

> **Remarque :**
>
> La disposition est écrasée à chaque enregistrement. La disposition est enregistrée uniquement sur StoreFront actif.
>
> Si vous lancez plusieurs sessions de bureau à partir du même StoreFront sur différents moniteurs, l'enregistrement de la disposition dans une session enregistre les informations de disposition de toutes les sessions.

Enregistrer mise en page

Pour activer la fonctionnalité d'enregistrement de la disposition :

1. Installez StoreFront 3.15 ou une version ultérieure (égale ou supérieure à v3.15.0.12) sur un Delivery Controller (DDC) compatible.
2. Téléchargez la build de l'application Citrix Workspace 1808 pour Linux ou version supérieure à partir de la page Téléchargements, puis installez-la sur votre machine Linux.
3. Définissez la variable d'environnement ICAROOT sur l'emplacement d'installation.
4. Vérifiez si le fichier **All_Regions.ini** est présent dans le dossier **.ICAClient**. Si c'est le cas, supprimez-le.
5. Dans le fichier **$ICAROOT/config/All_Regions.ini** recherchez le champ **SaveMultiMonitorPref**. Par défaut, la valeur de ce champ est définie sur true (ce qui signifie que cette fonctionnalité est activée). Pour désactiver cette fonctionnalité, définissez ce champ sur false.
   Si vous apportez des modifications à la valeur **SaveMultiMonitorPref**, vous devez supprimer le fichier **All_Regions.ini** présent dans le dossier **.ICAClient** pour éviter les incompatibilités de valeurs et un verrouillage de profil possible. Définissez ou annulez l'indicateur **SaveMultiMonitorPref** avant de lancer des sessions.
6. Lancez une nouvelle session de bureau.
7. Cliquez sur **Enregistrer la disposition** dans la barre d'outils de Desktop Viewer pour enregistrer la disposition de la session en cours. Une notification apparaît en bas à droite de l'écran indiquant la réussite de l'opération.
   Lorsque vous cliquez sur Enregistrer la disposition, l'icône devient grise. Ceci indique que l'enregistrement est en cours. Lorsque la disposition est enregistrée, l'icône s'affiche normalement.
   Toutefois, si l'icône est grisée depuis longtemps, consultez l'article CTX235895 du centre de connaissances pour obtenir des informations de dépannage.

8. Déconnectez-vous ou fermez la session.
   Relancez la session. La session apparaît dans le même mode, sur le même moniteur et dans la même position.

Limitations et scénarios non pris en charge :

- L'enregistrement d'une disposition pour une session en mode fenêtré sur plusieurs moniteurs n'est pas pris en charge en raison des limitations du gestionnaire d'affichage Linux.
- L'enregistrement des informations de session sur des moniteurs avec une résolution variée n'est pas pris en charge dans cette version et peut entraîner un comportement imprévisible.
- Les déploiements client avec plusieurs StoreFront ne sont pas pris en charge.

Utiliser Citrix Virtual Desktops sur deux moniteurs

1. Sélectionnez Desktop Viewer et cliquez sur la flèche vers le bas.
2. Sélectionnez **Fenêtre**.
3. Faites glisser l'écran Citrix Virtual Desktops entre les deux moniteurs. Assurez-vous qu'environ la moitié de l'écran est présent dans chaque moniteur.
4. Dans la barre d'outils de Citrix Virtual Desktops, sélectionnez **Plein écran**.

   L'écran s'étend aux deux moniteurs.

Workspace Launcher

Citrix propose désormais Workspace Launcher (WebHelper), qui permet de lancer des bureaux et des applications publiés.

Auparavant, le plug-in de navigateur fourni avec l'application Citrix Workspace pour Linux qui permettait aux utilisateurs de lancer des bureaux et des applications publiés était basé sur NPAPI.

En guise de solution, Citrix a introduit le lanceur Workspace (WebHelper). Pour activer cette fonctionnalité, configurez StoreFront pour envoyer des demandes au lanceur Workspace afin de détecter l'installation de l'application Citrix Workspace.

À partir de la version 1901, le lanceur Citrix Workspace fonctionne avec des connexions directes à StoreFront et à Citrix Gateway. Cette fonctionnalité permet de lancer automatiquement le fichier ICA et de détecter l'installation de l'application Citrix Workspace.

En guise de solution, Citrix a introduit le lanceur Workspace (WebHelper). Pour activer cette fonctionnalité, configurez StoreFront pour envoyer des demandes au lanceur Workspace afin de détecter l'installation de l'application Citrix Workspace.

Pour plus d'informations sur la configuration de StoreFront, voir **Solution - 2** > **a) Administrator configuration** dans l'article CTX237727 du Centre de connaissances.

> **Remarque :**
>
> Le lanceur Citrix Workspace ne fonctionne actuellement qu'avec des connexions directes à StoreFront. Il n'est pas pris en charge dans d'autres cas, tels que les connexions via Citrix Gateway.

Désactivation du nouveau mode d'interface utilisateur Web de l'espace de travail

Lorsque vous lancez l'application Citrix Workspace pour Linux en utilisant un fichier exécutable provenant de fournisseurs de clients légers tiers, l'application peut ne plus répondre en raison de l'utilisation à 100 % du processeur.

Pour contourner le problème, revenez à l'ancien mode d'interface utilisateur :

1. Supprimez les fichiers en cache en utilisant la commande :
   `rm -r ~/.ICAClient`
2. Accédez au dossier `$ICAROOT/config/AuthManconfig.xml`.
3. Changez la valeur de la clé `CWACapableEnabled` sur false.
4. Lancez l'application Citrix Workspace pour Linux. Assurez-vous que le fichier exécutable charge l'ancienne interface utilisateur.

Synchronisation de la disposition du clavier

La synchronisation de la disposition du clavier entre le client et le VDA vous permet de basculer entre les dispositions de clavier préférées sur la machine cliente lors de l'utilisation d'un VDA Windows ou Linux. Cette fonction est désactivée par défaut.

Conditions préalables :

- Activez la fonctionnalité de mappage de disposition du clavier Unicode sur le VDA Windows. Pour plus d'informations, consultez l'article CTX226335 du centre de connaissances.
- Activez la fonctionnalité de synchronisation dynamique de la disposition du clavier sur le VDA Linux. Pour de plus amples informations, consultez Synchronisation dynamique de la disposition du clavier
- La synchronisation de la disposition du clavier dépend de XKB lib, qui permet la synchronisation automatique de la disposition du clavier entre le VDA et l'appareil client.
- Lorsque vous utilisez un Windows Server 2016 ou Windows Server 2019, accédez au chemin d'accès suivant dans l'Éditeur du Registre `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme` et ajoutez une nouvelle valeur DWORD avec le nom de la clé `DisableKeyboardSync` et définissez la valeur sur `0`.

Pour activer cette fonctionnalité, ajoutez les lignes suivantes au fichier module.ini :

> [ICA 3.0]
>
> KeyboardSync=On
>
> [KeyboardSync]
>
> DriverName = VDIME.DLL

Lorsque vous définissez **KeyboardSync=On** dans le fichier module.ini et que vous définissez **KeyboardLayout=(Profil utilisateur)** dans le fichier **wfclient.ini**, le pilote virtuel vdime détecte la disposition du clavier sur le client et envoie les informations au VDA. Lorsque la disposition du clavier change dans une session cliente, le vdime en est conscient et envoie immédiatement la nouvelle disposition au VDA.

Pour désactiver cette fonctionnalité , définissez **KeyboardSync=Off** dans le fichier module.ini pour revenir au comportement antérieur. Dans le comportement antérieur, la disposition du clavier est lue à partir du fichier **$HOME/ .icaclient/WFClient .ini** et envoyée au VDA avec d'autres informations clientes lorsque la session démarre.

Utilisation

Lorsque cette fonctionnalité est activée, si la disposition du clavier change sur la machine cliente pendant une session, la disposition du clavier de la session change en conséquence.

Prise en charge de la disposition du clavier pour VDA Windows et VDA Linux

> **Remarque :**
>
> Les paramètres régionaux du clavier Linux de toutes les références listées dans le tableau suivant sont un trait d'union.

Disposition du clavier Linux	Disposition du clavier Linux/VDA Linux	Paramètres régionaux Windows	ID du clavier Windows	Disposition du VDA Linux
ara	-	ar-SA	00000401	ara
ara	azerty	ar-DZ	00020401	ara
at	-	de-AT	00000407	at
be	iso-alternate	fr-BE	0000080c	be
be	-	nl-BE	00000813	be
bg	-	bg-BG	00030402	bg
bg	phonetic	bg-BG	00040402	bg

Disposition du clavier Linux	Disposition du clavier Linux/VDA Linux	Paramètres régionaux Windows	ID du clavier Windows	Disposition du VDA Linux
bg	bas_phonetic	bg-BG	00020402	bg
br	-	pt-BR	00000416	br
by	-	be-BY	00000423	by
ca	eng	en-CA	00000409	ca
ca	multix	fr-CA	00011009	ca
ca	fr-legacy	fr-CA	00000c0c	ca
ca	-	fr-CA	00001009	ca
ch	fr	fr-CH	0000100c	ch
ch	-	de-CH	00000807	ch
cn	-	en-US	00000409	us
cz	-	cs-CZ	00000405	cz
cz	qwerty	cs-CZ	00010405	cz
de	-	de-DE	00000407	de
de	mac	de-DE	00000407	de
dk	-	da-DK	00000406	dk
ee	-	et-EE	00000425	ee
es	-	es-ES	0000040a	es
es	mac	es-ES	0000040a	es
fi	-	fi-FI	0000040b	fi
fr	-	fr-FR	0000040c	fr
fr	mac	fr-FR	0000040c	fr
gb	-	en-GB	00000809	gb
gb	mac	en-GB	00000809	gb
gb	extd	en-GB	00000452	gb
gr	-	el-GR	00000408	gr
hr	-	hr-HR	0000041a	hr
hu	-	hu-HU	0000040e	hu

Disposition du clavier Linux	Disposition du clavier Linux/VDA Linux	Paramètres régionaux Windows	ID du clavier Windows	Disposition du VDA Linux
ie	-	en-IE	00001809	ie
il	-	he-IL	0002040d	il
in	eng	en-IN	00004009	in
iq	-	ar-IQ	00000401	iq
is	-	is-IS	0000040f	is
it	-	it-IT	00000410	it
jp	-	en-US	00000409	us
jp	mac	en-US	00000409	us
kr	-	en-US	00000409	us
latam	-	es-MX	0000080a	latam
lt	-	lt-LT	00010427	lt
lt	ibm	lt-LT	00000427	lt
lt	std	lt-LT	00020427	lt
lv	-	lv-LV	00020426	lv
non	-	nb-NO	00000414	non
pl	-	pl-PL	00000415	pl
pl	qwertz	pl-PL	00010415	pl
pt	-	pt-PT	00000816	pt
pt	mac	pt-PT	00000816	pt
ro	std	ro-RO	00010418	ro
rs	-	sr-Cyrl-RS	00000c1a	rs
rs	latin	sr-Latn-RS	0000081a	rs
ru	-	ru-RU	00000419	ru
ru	typewriter	ru-RU	00010419	ru
ru	mac	ru-RU	00000419	ru
se	-	sv-SE	0000041d	se
se	mac	sv-SE	0000041d	se

Disposition du clavier Linux	Disposition du clavier Linux/VDA Linux	Paramètres régionaux Windows	ID du clavier Windows	Disposition du VDA Linux
si	-	sl-SI	00000424	si
sk	-	sk-SK	0000041b	sk
sk	qwerty	sk-SK	0001041b	sk
th	-	th-TH	0000041e	th
th	pat	th-TH	0001041e	th
tj	-	tg-Cyrl-TJ	00000428	tj
tr	-	tr-TR	0000041f	tr
tr	f	tr-TR	0001041f	tr
tw	-	en-US	00000409	us
ua	-	uk-UA	00000422	ua
us	-	en-US	00000409	us
us	mac	en-US	00000409	us
us	dvorak	en-US	00010409	us
us	dvorak-l	en-US	00030409	us
us	dvorak-r	en-US	00040409	us
us	intl	nl-NL	00020409	us
vn	-	vi-VN	0000042a	vn

Disposition du clavier VDA

La fonctionnalité de disposition du clavier VDA vous permet d'utiliser la disposition du clavier VDA quels que soient les paramètres de disposition du clavier du client. Elle prend en charge les types de claviers suivants : PC/XT 101, 102, 104, 105, 106.

Pour utiliser la disposition du clavier côté serveur, procédez comme suit :

1. Lancez le fichier wfclient.ini.
2. Modifiez la valeur de l'attribut `KeyboardLayout` comme suit :

   ```
   KeyboardLayout=(Server Default)
   ```

   La valeur par défaut de l'attribut `KeyboardLayout` est (User Profile).

3. Redémarrez la session pour que les modifications prennent effet.

Association de type de fichier

Citrix Virtual Apps Services peut également publier un fichier plutôt qu'une application ou un bureau. Ce processus s'appelle la publication de contenu, et permet à pnabrowse d'ouvrir le fichier publié.

Il existe toutefois une restriction concernant les types de fichiers reconnus par l'application Citrix Workspace pour Linux. Pour que le système puisse reconnaître le type de fichier du contenu publié et pour que les utilisateurs puissent le visualiser dans l'application Citrix Workspace, une application publiée doit être associée au type de fichier du fichier publié. À titre d'exemple, pour visualiser un fichier Adobe PDF à l'aide de l'application Citrix Workspace, une application telle qu'Adobe PDF Viewer doit être publiée. Les utilisateurs ne peuvent pas visualiser le contenu publié si aucune application appropriée n'a été publiée.

Pour activer la FTA côté client :

1. Assurez-vous que l'application que vous souhaitez associer est une application préférée ou à laquelle vous êtes abonné.
2. Pour obtenir la liste des applications publiées et l'URL du serveur, exécutez les commandes :

```
./util/storebrowse -l

./util/storebrowse -S <StoreFront URL>
```

3. Exécutez la commande ./util/ctx_app_bind avec la syntaxe suivante :

   ```
   ./util/ctx_app_bind [-p] example_file|MIME-type published-application [server|server-URI]
   ```

   par exemple,

   ```
   ./util/ctx_app_bind a.txt BVT_DB.Notepad_AWTSVDA-0001 https://awddc1.bvt.local/citrix/store/discovery
   ```

4. Assurez-vous que le mappage de lecteur client (CDM) est activé sur le fichier que vous essayez d'ouvrir.
5. Double-cliquez sur le fichier pour l'ouvrir à l'aide de l'application associée.

Association d'une application publiée à des types de fichiers

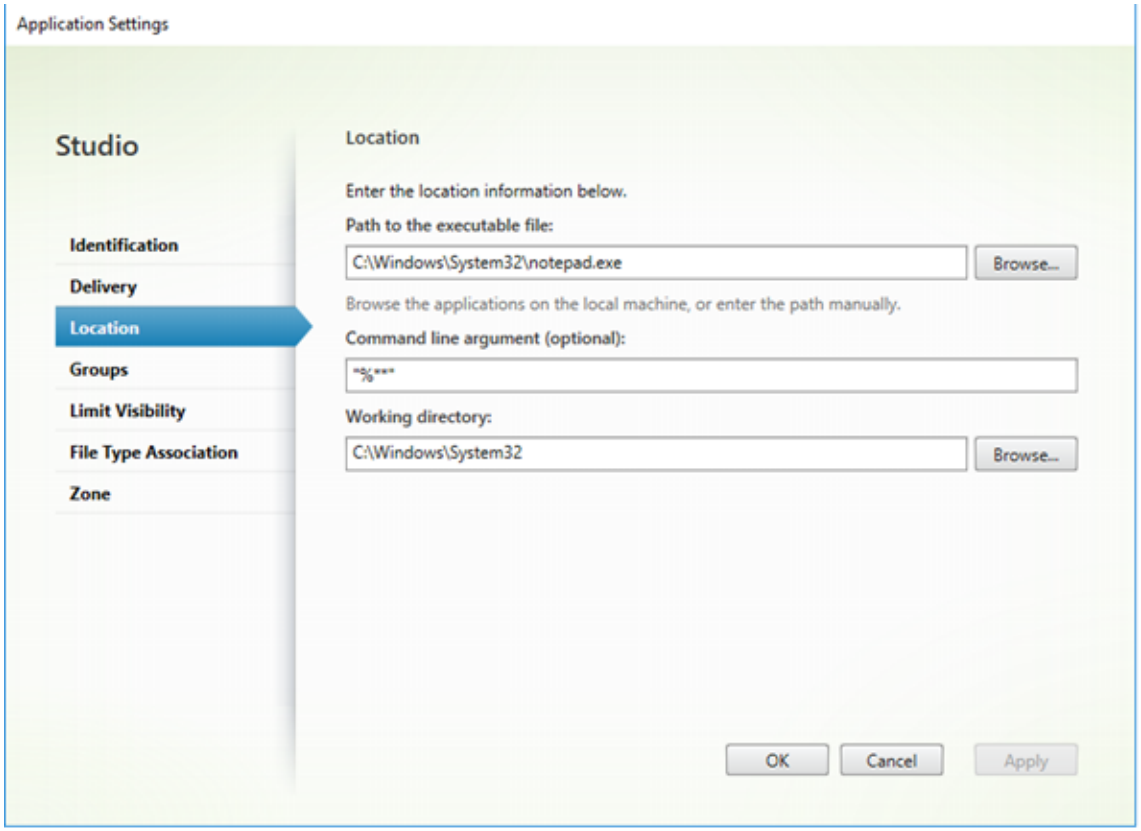
L'application Citrix Workspace lit et applique les paramètres configurés par les administrateurs dans Citrix Studio.

Conditions préalables :

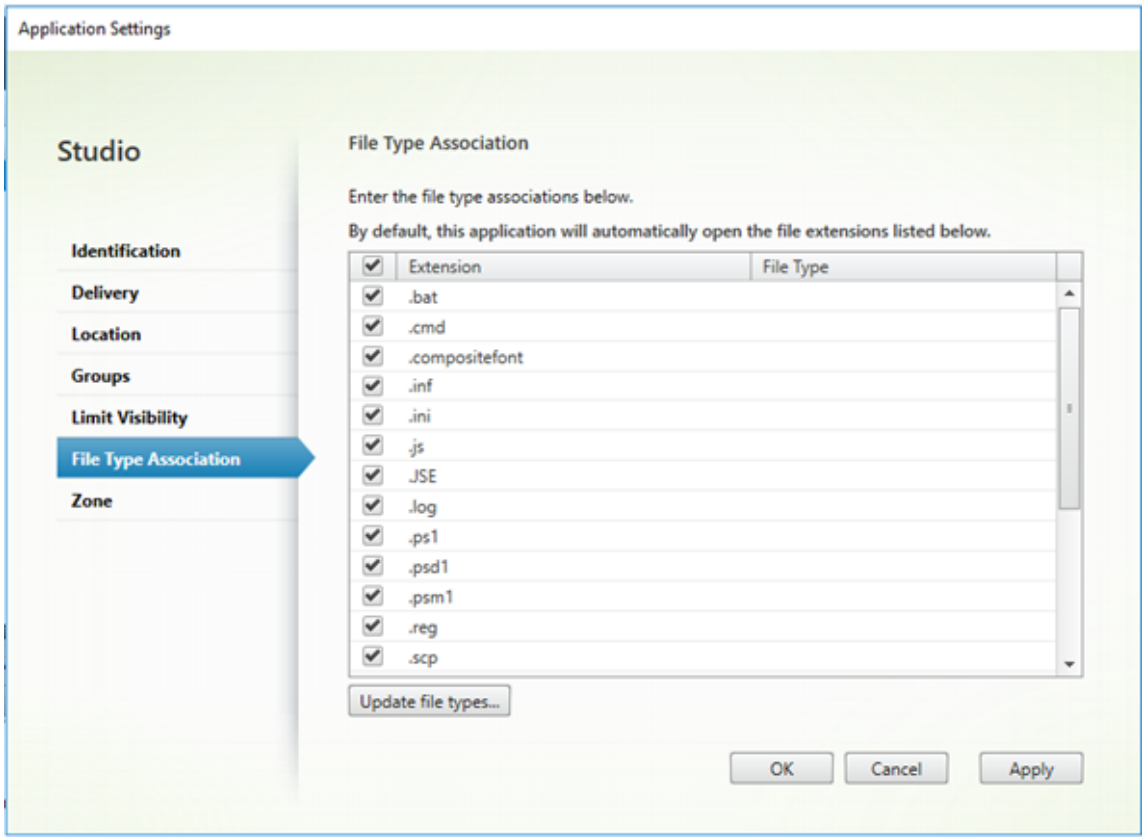
Assurez-vous de vous connecter au serveur Store sur lequel la FTA est configurée.

Pour lier une extension de nom de fichier à une application Citrix Workspace pour Linux :

1. Publiez l'application.
2. Connectez-vous à Citrix Studio.
3. Cliquez avec le bouton droit de la souris sur l'application et sélectionnez **Propriétés.**
4. Sélectionnez **Emplacement.**
5. Ajoutez "%**" dans le champ Argument de ligne de commande (facultatif) pour contourner la validation de ligne de commande, puis cliquez sur OK.



6. Cliquez avec le bouton droit de la souris sur l'application et sélectionnez **Propriétés**.
7. Sélectionnez **Association de type de fichier**.
8. Sélectionnez les extensions que l'application Citrix Workspace doit associer à l'application.



9. Cliquez sur **Appliquer** et **mettez à jour les types de fichiers**.
10. Suivez les étapes mentionnées dans Association de type de fichier pour activer la FTA côté client.

> **Remarque :**
>
> Assurez-vous que l'association de type de fichier StoreFront est activée (ON). Par défaut, l'association de type de fichier est activée.

Prise en charge de Citrix Analytics

L'application Citrix Workspace pour Linux est instrumentée pour transmettre en toute sécurité les journaux à Citrix Analytics lorsque certains événements sont déclenchés par l'application. Les journaux sont analysés et stockés sur les serveurs Citrix Analytics lorsqu'ils sont activés. Pour plus d'informations sur Citrix Analytics, consultez Citrix Analytics.

Interface utilisateur transparente

Le protocole ICA Citrix utilise le protocole Transparent User Interface Virtual Channel [TUI VC] pour transmettre des données entre les clients Citrix Virtual Apps and Desktops et les serveurs hôtes. Le

protocole TUI transmet les messages des composants de l'interface utilisateur [Interface utilisateur] pour les connexions distantes.

L'application Citrix Workspace pour Linux prend en charge la fonctionnalité TUI VC. Cette fonctionnalité aide le client à recevoir les paquets TUI envoyés par le serveur, et le client peut accéder aux composants associés à l'interface utilisateur. Cette fonctionnalité vous permet de contrôler l'affichage de l'écran de superposition par défaut. Vous pouvez activer/désactiver l'indicateur `VDTUI` dans le fichier `module.ini` : `VDTUI - On/Off`.

Pour de plus amples informations sur les canaux virtuels, consultez Canaux virtuels ICA Citrix dans la documentation de Citrix Virtual Apps and Desktops.

Authentification

March 23, 2021

Pour offrir une meilleure expérience, à compter de l'application Citrix Workspace 2012, nous présentons la boîte de dialogue d'authentification dans l'application Citrix Workspace et affichons les détails du magasin sur l'écran d'ouverture de session. Nous chiffrons et stockons les jetons d'authentification afin que vous n'ayez pas besoin de saisir de nouveau les informations d'identification lorsque votre système ou votre session redémarre.

> **Remarque :**
>
> cette amélioration de l'authentification ne s'applique qu'aux déploiements dans le cloud.

Conditions préalables :

Vous devez installer la bibliothèque libsecret.

Cette fonction est désactivée par défaut.

Pour activer cette amélioration :

1. Recherchez le fichier de configuration : `$ICAROOT/config/AuthManConfig.xml`.
2. Définissez la valeur de `AuthManLiteEnabled` sur **`true`**.

Carte à puce

Pour configurer la prise en charge de carte à puce dans l'application Citrix Workspace pour Linux, vous devez configurer le serveur StoreFront dans la console StoreFront.

L'application Citrix Workspace prend en charge les lecteurs de cartes à puce compatibles avec les pilotes PCSC-Lite et PKCS#11. Par défaut, l'application Citrix Workspace place désormais `opensc-pkcs11.so` dans l'un des emplacements standards.

L'application Citrix Workspace peut trouver `opensc-pkcs11.so` dans un emplacement non standard ou un autre pilote `PKCS\##11`. Vous pouvez stocker l'emplacement respectif en suivant la procédure ci-dessous :

1. Recherchez le fichier de configuration : `$ICAROOT/config/AuthManConfig.xml`.
2. Localisez la ligne <key>PKCS11module</key> et ajoutez l'emplacement du pilote à l'élément <value> qui suit immédiatement la line.

> **Remarque :**
>
> Si vous entrez un nom de fichier, l'application Citrix Workspace accède à ce fichier dans le répertoire `$ICAROOT/PKCS\ ##11`. Vous pouvez également utiliser un chemin d'accès absolu commençant par « / ».

Après avoir supprimé une carte à puce, configurez le comportement de l'application Citrix Workspace en mettant à jour `SmartCardRemovalAction` dans le fichier de configuration en procédant comme suit :

1. Recherchez le fichier de configuration : `$ICAROOT/config/AuthManConfig.xml`.
2. Localisez la ligne <key>SmartCardRemovalAction</key> et ajoutez `noaction` ou `forcelogoff` à l'élément <value> qui suit immédiatement la ligne.

Le comportement par défaut est `noaction`. Aucune action n'est effectuée pour effacer les informations d'identification stockées et les jetons générés lors du retrait de la carte à puce.

L'action `forcelogoff` efface toutes les informations d'identification et tous les jetons stockés dans StoreFront lors du retrait de la carte à puce.

Activation de la prise en charge des cartes à puce

L'application Citrix Workspace prend en charge divers lecteurs de cartes à puce si la carte à puce est activée à la fois sur le serveur et sur l'application Citrix Workspace.

Vous pouvez utiliser des cartes à puce aux fins suivantes :

- Authentification d'ouverture de session par carte à puce : vous authentifie auprès des serveurs Citrix Virtual Apps
- Prise en charge des applications recourant à une carte à puce : permet aux applications publiées recourant à une carte à puce d'accéder aux lecteurs de carte à puce locaux.

Les données de carte à puce sont sensibles en matière de sécurité et doivent être transmises au moyen d'un canal authentifié sécurisé (TLS, par exemple).

Pré-requis de la prise en charge des cartes à puce :

- Les lecteurs de carte à puce et les applications publiées doivent être conformes aux normes PC/SC de l'industrie.

- Installez le pilote approprié au lecteur de carte à puce.
- Installez le package PC/SC Lite.
- Installez et exécutez le démon `pcscd`, qui fournit le middleware permettant d'accéder à la carte à puce à l'aide de PC/SC.
- Sur un système 64 bits, les versions 64 bits et 32 bits du package « libpscslite1 » doivent être présentes.

> **Important :**
>
> Si vous utilisez le terminal SunRay avec le logiciel serveur SunRay version 2.0 ou ultérieure, installez le package de contournement SRCOM PC/SC, disponible au téléchargement à l'adresse http://www.sun.com/.

Pour plus d'informations sur la configuration de la prise en charge des cartes à puce sur vos serveurs, veuillez consulter Cartes à puce dans la documentation de Citrix Virtual Apps and Desktops.

Prise en charge de l'authentification multifacteur (nFactor)

L'authentification multifacteur améliore la sécurité d'une application en exigeant des utilisateurs qu'ils fournissent plusieurs preuves d'identification pour y accéder. L'authentification multifacteur rend les étapes d'authentification et les formulaires de collecte d'informations d'identification associés configurables par l'administrateur.

L'application Citrix Workspace native prend en charge ce protocole en s'appuyant sur le support de formulaires de connexion déjà mis en œuvre pour StoreFront. Les pages de connexion Web pour les serveurs virtuels Citrix Gateway et Traffic Manager utilisent également ce protocole.

Pour de plus amples informations, veuillez consulter Authentification SAML et Authentification multifacteur (nFactor) dans la documentation de Citrix ADC.

Sécuriser

April 16, 2021

Pour sécuriser les communications entre votre site et l'application Citrix Workspace, vous pouvez intégrer vos connexions via l'application Citrix Workspace à l'aide de technologies sécurisées telles que Citrix Gateway :

> **Remarque :**
>
> Citrix recommande d'utiliser Citrix Gateway entre les serveurs StoreFront et les machines utilisateur.

- Un pare-feu : les pare-feu de réseau peuvent autoriser ou empêcher le passage des paquets de données en fonction de l'adresse et du port de destination. Si vous utilisez l'application Citrix Workspace avec un pare-feu de réseau qui mappe l'adresse IP interne du serveur sur une adresse Internet externe (c'est-à-dire, la traduction d'adresse de réseau, ou NAT), configurez l'adresse externe.
- Serveur approuvé.
- Pour les déploiements de Citrix Virtual Apps uniquement (non applicable à XenDesktop 7) : un serveur proxy SOCKS ou serveur proxy sécurisé (également appelé serveur proxy de sécurité, serveur proxy HTTPS ou serveur proxy de tunneling TLS). Vous pouvez utiliser des serveurs proxy pour limiter l'accès à l'intérieur et à l'extérieur de votre réseau, et pour gérer les connexions entre l'application Citrix Workspace et les serveurs. L'application Citrix Workspace prend en charge les protocoles de proxy SOCKS et de proxy sécurisé.
- Pour les déploiements Citrix Virtual Apps : Citrix Secure Web Gateway ou solutions de relais SSL avec protocoles TLS. Les versions TLS 1.0 à 1.2 sont prises en charge.

Citrix Gateway

Citrix Gateway (anciennement Access Gateway) sécurise les connexions aux magasins StoreFront, et permet aux administrateurs de contrôler, de façon détaillée, l'accès utilisateur aux bureaux et applications.

Pour se connecter à des bureaux et des applications via Citrix Gateway :

1. Spécifiez l'URL de Citrix Gateway qui vous a été fournie par votre administrateur. Vous pouvez effectuer cette opération de l'une des manières suivantes :

   - La première fois que vous utilisez l'interface utilisateur en libre-service, vous êtes invité à entrer l'adresse URL dans la boîte de dialogue Ajouter compte.
   - Lorsque vous utilisez l'interface utilisateur en libre-service ultérieurement, entrez l'URL en cliquant sur Préférences > Comptes > Ajouter.
   - Si vous établissez une connexion avec la commande storebrowse, entrez l'adresse URL sur la ligne de commande.

   L'URL spécifie la passerelle et, éventuellement, un magasin spécifique :

   - Pour vous connecter au premier magasin détecté par l'application Citrix Workspace, utilisez une URL au format suivant par exemple : https://gateway.company.com.
   - Pour vous connecter à un magasin spécifique, utilisez une URL au format https://gateway.company.com?<nommagasin> par exemple. Le format de cette URL dynamique n'est pas un format standard ; n'incluez pas le signe égal = dans l'URL. Si vous établissez une connexion à un magasin spécifique avec storebrowse, vous devrez peut-être utiliser des guillemets autour de l'URL dans la commande storebrowse.

2. Lorsque vous y êtes invité, connectez-vous au magasin (via la passerelle) à l'aide de votre nom d'utilisateur, mot de passe et de jeton de sécurité. Pour de plus amples informations sur cette étape, consultez la documentation de Citrix Gateway.

   Lorsque l'authentification est terminée, vos bureaux et applications sont affichés.

Serveur proxy

Les serveurs proxy permettent de limiter l'accès à l'intérieur comme à l'extérieur du réseau, et de gérer les connexions établies entre l'application Citrix Workspace et votre déploiement Citrix Virtual Apps and Desktops. L'application Citrix Workspace prend en charge le protocole SOCKS, de même que Citrix Secure Web Gateway et le Relais SSL Citrix, le protocole proxy sécurisé et l'authentification Stimulation/Réponse Windows NT (NTLM).

La liste des types de proxy pris en charge est limitée aux types Auto, None et Wpad par le contenu des fichiers Trusted_Regions.ini et Untrusted_Regions.ini. Si vous utilisez les types SOCKS, Secure ou Script, modifiez ces fichiers pour ajouter les types supplémentaires à la liste des types autorisés.

> **Remarque :**
>
> Pour garantir l'établissement d'une connexion sécurisée, activez le protocole TLS.

Serveur proxy sécurisé

La configuration de connexions utilisant le protocole de proxy sécurisé assure également la prise en charge de l'authentification Stimulation/Réponse Windows NT (NTLM). Si ce protocole est disponible, il est détecté et utilisé au moment de l'exécution sans nécessiter de configuration supplémentaire.

> **Important :**
>
> La prise en charge de NTLM nécessite les bibliothèques OpenSSL 1.1.1d et libcrypto.so. Installez les bibliothèques sur la machine utilisateur. Ces bibliothèques sont souvent incluses dans les distributions Linux. Vous pouvez également les télécharger depuis http://www.openssl.org/.

Secure Web Gateway et SSL

Vous pouvez intégrer l'application Citrix Workspace avec Citrix Secure Web Gateway ou le service Relais SSL (Secure Sockets Layer) Citrix. L'application Citrix Workspace prend en charge le protocole TLS. TLS (Transport Layer Security) est la dernière version normalisée du protocole SSL. Le groupe de travail Internet Engineering Taskforce (IETF) l'a rebaptisé TLS lorsqu'il est devenu responsable du développement de SSL sous la forme d'une norme ouverte. TLS garantit la sécurité des communications de données grâce à l'authentification des serveurs, au cryptage du flux de données et aux

contrôles d'intégrité des messages. Certaines organisations, notamment des organisations gouvernementales américaines, requièrent l'utilisation du protocole TLS pour la sécurisation de leurs communications de données. Ces organisations peuvent nécessiter l'utilisation d'une cryptographie validée, comme la norme FIPS 140 (Federal Information Processing Standard). La norme FIPS 140 est une norme de cryptographie.

Secure Web Gateway

Vous pouvez utiliser Citrix Secure Web Gateway en mode Normal ou en mode Relais afin de fournir un canal de communication sécurisé entre l'application Citrix Workspace et le serveur. Il n'est pas nécessaire de configurer l'application Citrix Workspace si vous utilisez Citrix Secure Web Gateway en mode Normal.

Si Citrix Secure Web Gateway Proxy est installé sur un serveur dans le réseau sécurisé, vous pouvez l'utiliser en mode Relais. Pour de plus amples informations, consultez la documentation de Citrix Virtual Apps (Citrix Secure Web Gateway).

Si vous utilisez le mode Relais, le serveur Citrix Secure Web Gateway fonctionne comme un serveur proxy. Dans ce cas, vous devez configurer l'application Citrix Workspace pour qu'elle utilise :

- le nom de domaine complet du serveur Citrix Secure Web Gateway ;
- le numéro de port du serveur Citrix Secure Web Gateway. Le mode Relais n'est pas pris en charge par Citrix Secure Web Gateway, version 2.0.

Le nom de domaine complet (FQDN) doit contenir, dans l'ordre, les trois composants suivants :

- Nom d'hôte
- Domaine intermédiaire
- Domaine de tête

Par exemple : mon_ordinateur.mon_entreprise.com est un nom de domaine complet car il liste dans l'ordre un nom d'hôte (mon_ordinateur), un domaine intermédiaire (mon_entreprise) et un domaine de tête (com). La combinaison du domaine intermédiaire et du domaine de tête (mon_entreprise.com) est appelée nom de domaine.

Relais SSL

Par défaut, le Relais SSL Citrix utilise le port TCP 443 sur le serveur Citrix Virtual Apps pour les communications sécurisées TLS. Lorsque le Relais SSL reçoit une connexion TLS, il décrypte les données avant de les rediriger sur le serveur.

Si vous configurez le Relais SSL Citrix pour l'écoute sur un port autre que le port 443, vous devez spécifier le numéro du port d'écoute non standard dans l'application Citrix Workspace.

Le Relais SSL Citrix vous permet de sécuriser les communications suivantes.

- Entre une machine utilisateur et un serveur sur lesquels TLS est activé.

Pour obtenir des informations sur la configuration et l'utilisation du Relais SSL en vue de sécuriser l'installation, veuillez consulter la documentation de Citrix Virtual Apps.

TLS

Vous pouvez contrôler les versions du protocole TLS qui peuvent être négociées en ajoutant les options de configuration suivantes dans la section [WFClient]:

- MinimumTLS=1.2
- MaximumTLS=1.2

Il s'agit des valeurs par défaut, qui sont implémentées en code. Modifiez-les comme bon vous semble.

> **Remarque :**
>
> - Ces valeurs sont lues chaque fois qu'un programme démarre. Si vous les modifiez après le démarrage de self-service ou storebrowse, tapez : **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**.
> - L'application Citrix Workspace pour Linux n'autorise pas l'utilisation du protocole SSLv3.

Pour sélectionner la suite de chiffrement, ajoutez l'option de configuration suivante dans la section [WFClient] :

- SSLCiphers=GOV

Il s'agit de la valeur par défaut. Les autres valeurs reconnues sont COM et ALL.

> **Remarque :**
>
> Tout comme avec la configuration de la version TLS, si vous changez cette valeur après le démarrage de self-service ou storebrowse, vous devez taper :
> **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**

Mise à jour cryptographique

Cette fonctionnalité est un changement important au protocole de communication sécurisé. Les suites de chiffrement avec le préfixe TLS_RSA_ ne proposent pas la fonctionnalité Forward Secrecy et sont considérées comme faibles.

Les suites de chiffrement TLS_RSA_ ont été entièrement supprimées. Au lieu de cela, les suites de chiffrement TLS_ECDHE_RSA_ avancées sont prises en charge. Si votre environnement n'est pas configuré avec les suites de chiffrement TLS_ECDHE_RSA_, les lancements de clients ne sont pas pris en charge en raison de la faiblesse du chiffrement. Pour l'authentification client, les clés RSA 1536 bits sont prises en charge.

Les suites de chiffrement avancées suivantes sont prises en charge :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

DTLS v1.0 prend en charge les suites de chiffrement suivantes :

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

DTLS v1.2 prend en charge les suites de chiffrement suivantes :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

> **Remarque :**
>
> À partir des versions 1903 et ultérieures, DTLS est pris en charge à partir de Citrix Gateway 12.1 et versions ultérieures. Pour plus d'informations sur les suites de chiffrement prises en charge par DTLS pour Citrix Gateway, consultez Prise en charge du protocole DTLS

Suites de chiffrement

Pour activer différentes suites de chiffrement, modifiez la valeur du paramètre `SSLCiphers` sur `ALL`, `COM` ou `GOV`. Par défaut, l'option est définie sur `ALL` dans le fichier `All_Regions.ini` du répertoire `$ICAROOT/config`.

Les ensembles suivants de suites de chiffrement sont fournis respectivement par ALL, GOV et COM :

- ALL
  - les 3 chiffrements sont pris en charge.
- GOV
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- COM
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Pour plus d'informations sur le dépannage, reportez-vous à la section Suites de chiffrement.

Les suites de chiffrement avec le préfixe TLS_RSA_ ne proposent pas la fonctionnalité Forward Secrecy De manière générale, ces suites de chiffrement sont maintenant obsolètes dans le secteur. Toutefois, pour prendre en charge la rétrocompatibilité avec les anciennes versions de Citrix Virtual Apps and Desktops, l'application Citrix Workspace pour Linux peut utiliser ces suites de chiffrement.

Pour une meilleure sécurité, définissez l'indicateur `Enable\\_TLS\\_RSA\\_` sur `False`.

Voici une liste des suites de chiffrement obsolètes :

- TLS_RSA_AES256_GCM_SHA384
- TLS_RSA_AES128_GCM_SHA256
- TLS_RSA_AES256_CBC_SHA256
- TLS_RSA_AES256_CBC_SHA
- TLS_RSA_AES128_CBC_SHA
- TLS_RSA_3DES_CBC_EDE_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

> **Remarque :**
>
> Les deux dernières suites de chiffrement utilisent l'algorithme RC4 et sont obsolètes parce qu'elles ne sont pas sécurisées. Vous pouvez également considérer la suite de chiffrement TLS_RSA_3DES_CBC_EDE_SHA comme étant obsolète. Vous pouvez utiliser ces indicateurs pour appliquer toutes ces suites obsolètes.

Pour de plus amples informations sur la configuration de DTLS v1.2, consultez la section Transport adaptatif dans la documentation de Citrix Virtual Apps and Desktops.

Conditions préalables :

Si vous utilisez les versions 1901 et antérieures, suivez les étapes suivantes :

Si .ICAClient est déjà présent dans le répertoire de base de l'utilisateur actuel :

- Supprimez le fichier `All\\_Regions.ini`

Ou

- Pour conserver le fichier `AllRegions.ini`, ajoutez les lignes suivantes à la fin de la section [Network\SSL] :
  - Enable_RC4-MD5=
  - Enable_RC4_128_SHA=
  - Enable_TLS_RSA_=

Si le dossier .ICAClient n'existe pas dans le dossier de base de l'utilisateur actuel, cela indique une nouvelle installation de l'application Citrix Workspace. Dans ce cas, le paramètre par défaut des fonctionnalités est conservé.

Le tableau suivant répertorie les suites de chiffrement compris dans chaque ensemble :
Tableau 1 - Matrice de prise en charge de la suite de chiffrement

Ciphersuite	Native Cyrpto Kit mode and cipher set								
	Open			FIPS			SP800-52		
	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y		Y	Y		Y	Y	
TLS_RSA_WITH_AES_256_GCM_SHA384 (1) (2)	X								
TLS_RSA_WITH_AES_128_GCM_SHA256 (1) (2)	X	X							
TLS_RSA_WITH_AES_256_CBC_SHA256 (1) (2)	X								
TLS_RSA_WITH_AES_256_CBC_SHA (2)	X								
TLS_RSA_WITH_AES_128_CBC_SHA (2)	X	X							
TLS_RSA_WITH_RC4_128_SHA (2) (3)	X	X							
TLS_RSA_WITH_RC4_128_MD5 (2) (3)	X	X							
TLS_RSA_WITH_3DES_EDE_CBC_SHA (2)	X								
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	Y	Y	Y	Y	Y	Y	Y	Y	Y
Notes									
(1) Ciphersuites that require TLS1.2/DTLS 1.2									
(2) Ciphersuites disabled by default									
(3) Ciphersuites not available for DTLS protocol									
Y - Supported ciphersuites									
X-Deprecated ciphersuites									

> **Remarque :**
>
> Toutes les suites de chiffrement ci-dessus sont conformes aux normes FIPS et SP800-52. Les deux premières sont autorisées uniquement pour les connexions (D) TLS1.2. Consultez **Tableau 1 - Matrice de prise en charge de la suite de chiffrement** pour une représentation complète de la prise en charge de la suite de chiffrement.

Storebrowse

July 6, 2020

Storebrowse est un utilitaire de ligne de commande léger qui permet l'interaction entre le client et le serveur. Grâce à l'utilitaire storebrowse, les administrateurs peuvent automatiser les opérations quotidiennes suivantes :

- Ajouter un magasin
- Répertorier les applications et les bureaux publiés à partir d'un magasin configuré.
- Abonner et désabonner les applications et les bureaux d'un magasin configuré.
- Activer et désactiver les raccourcis pour des applications et des bureaux publiés.
- Lancer des applications publiées.
- Reconnecter les sessions déconnectées.

Généralement, l'utilitaire storebrowse est disponible dans le dossier `/util`. Vous pouvez le trouver sous l'emplacement d'installation. Par exemple, `/opt/Citrix/ICAClient/util`.

Conditions préalables

L'utilitaire storebrowse nécessite le package de bibliothèque **libxml2**.

Lancer des applications et des bureaux publiés

Il existe deux façons de lancer une ressource :

- Vous pouvez utiliser la ligne de commande et les commandes storebrowse.
- Vous pouvez utiliser l'interface utilisateur pour lancer une ressource.

Cet article traite des commandes storebrowse.

Utilisation des commandes

La section suivante détaille les commandes storebrowse que vous pouvez utiliser à partir de l'utilitaire storebrowse.

-a –addstore

Description :

Ajoute un nouveau magasin avec les détails de la passerelle et des balises ainsi que le processus de démon ServiceRecord. Cette commande renvoie l'URL complète du magasin. Une erreur apparaît si l'ajout d'un magasin échoue.

Exemple de commande sur StoreFront :

Commande :

```
./storebrowse –a *URL of StoreFront or a PNAStore*
```

Exemple :

```
./storebrowse -a https://my.firstexamplestore.net
```

> **Remarque :**
>
> Vous pouvez ajouter plusieurs magasins à l'aide de l'utilitaire storebrowse.

-?, -h, –help

Description :

Fournit des détails sur l'utilisation de l'utilitaire storebrowse.

-l –liststore

Description :

Répertorie les magasins que vous avez ajoutés.

Exemple de commande sur StoreFront :


```
./storebrowse -l
```

-E –enumerate

Description :

Répertorie les ressources disponibles. Par défaut, les valeurs suivantes apparaissent :

- Nom de la ressource
- Nom d'affichage
- Dossier de la ressource

Pour afficher plus d'informations, ajoutez la commande **-M** (–details) à la commande **-E**.

> **Remarque :**
>
> Lorsque vous exécutez la commande **-E**, une fenêtre d'authentification s'affiche si vous n'avez pas fourni vos informations d'identification précédemment.

Entrez l'URL entière du magasin telle qu'indiquée par la commande **—liststore**.

Exemple de commande sur StoreFront :

- `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -E -M https://my.firstexamplestore.net/Citrix/Store/discovery`

-S –subscribed

Description :

Dresse la liste des ressources auxquelles vous avez souscrit. Par défaut, les valeurs suivantes apparaissent :

- Nom de la ressource
- Nom d'affichage
- Dossier de la ressource

Pour afficher plus d'informations, ajoutez la commande **-M** (–details) à la commande **-E**.

Exemple de commande sur StoreFront :

- `./storebrowse.exe -S https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -S -M https://my.firstexamplestore.net/Citrix/Store/discovery`

-M –details

Description :

Cette commande renvoie plusieurs attributs pour les applications publiées. Généralement, cette commande est utilisée avec les commandes **—E** et **-S**. Cette commande prend un argument qui est la somme des nombres correspondant aux détails requis :

- Publisher(0x1)
- VideoType(0x2)
- SoundType(0x4)
- AppInStartMenu(0x8)
- AppOnDesktop(0x10)
- AppIsDesktop(0x20)
- AppIsDisabled(0x40)
- WindowType(0x80)
- WindowScale(0x100)
- DisplayName(0x200)
- AppIsMandatory(0x10000)
- CreateShortCuts (0x100000)
- RemoveShortCuts (0x200000)

> **Remarques :**
>
> - Pour créer pour les applications auxquelles des utilisateurs ont souscrit, utilisez l'argument CreateShortcuts (0x100000) avec les commandes **-S**, **-s** et **-u**.
> - Pour supprimer toutes les entrées de menu, utilisez RemoveShortcuts (0x200000) avec la commande **-S**.

Exemple de commande sur StoreFront :

```
./storebrowse.exe -S -M 0x264 https://my.firstexamplestore.net/Citrix/Store/discovery
```

où 0x264 est la combinaison de DisplayName (0x200), AppIsDisabled (0x40), AppIsDesktop (0x20) et SoundType (0x4). Le résultat répertorie les ressources avec abonnement ainsi que les détails.

Vous pouvez utiliser la commande **—M** pour répertorier les ressources avec les détails requis :

```
./storebrowse.exe -E -M 0x264 https://my.firstexamplestore.net/Citrix/Store/discovery
```

> **Remarques :**
>
> - Vous pouvez exprimer les valeurs au format décimal ou hexadécimal. Par exemple, 512 pour 0x200.

> - Lorsque certains détails ne sont pas disponibles via storebrowse, la valeur du résultat est nulle.

-s –subscribe

Description :

Abonne la ressource spécifiée à partir d'un magasin donné.

Exemple de commande sur StoreFront :

```
./storebrowse -s <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

-u –unsubscribe

Description :

Annule l'abonnement de la ressource spécifiée dans un magasin donné.

Exemple de commande sur StoreFront :

```
./storebrowse -u <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

-L –launch

Description :

Lance une connexion à une ressource publiée. L'utilitaire se ferme automatiquement, et la session reste connectée.

Exemple de commande sur StoreFront :

```
./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

-i –icons

Description :

Cette commande récupère les icônes de bureau et d'application au format PNG. Cette commande est utilisée avec la commande **-E** ou **-S**.

Pour récupérer les icônes dans les tailles et profondeurs requises, utilisez la méthode de l'argument best ou de l'argument size.

Argument best

En utilisant la méthode de l'argument best, vous pouvez récupérer les icônes avec les meilleures tailles disponibles sur le serveur. Vous pouvez ensuite convertir les icônes vers les tailles requises. La méthode l'argument best est la façon la plus efficace de stocker, d'appliquer la bande passante et de simplifier les scripts. Les fichiers sont enregistrés au format <resource name>.png.

Argument size

Pour récupérer les icônes dans les tailles et profondeurs spécifiées, utilisez la méthode de l'argument size. Une erreur apparaît si le serveur ne peut pas récupérer les icônes d'une taille ou d'une profondeur donnée.

L'argument size est au format wxB, où :

- **W** est la largeur des icônes. Toutes les icônes sont carrées, donc une seule valeur est nécessaire pour spécifier la taille.
- **B** est la profondeur de couleur. Autrement dit, le nombre de bits par pixel.

> **Remarque :**
>
> La valeur **W** est obligatoire. La valeur **B** est facultative.

Si vous ne spécifiez pas les valeurs, des icônes de toutes les profondeurs d'image disponibles apparaissent. Les fichiers sont enregistrés au format <resource name> _WxWxB.png.

Les deux méthodes enregistrent des icônes au format **.png**, pour chaque ressource renvoyée par la commande **—E**ou **—S**.

Les icônes sont stockées dans le dossier **.icaclient/cache/icons**.

Exemple de commande sur StoreFront :

- `./storebrowse -E -i best https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -S -i 16x16 https://my.firstexamplestore.net/Citrix/Store/discovery`

-W [r|R] –reconnect [r|R]

Description :

Reconnecte les sessions déconnectées mais actives du magasin spécifié. L'option [r] reconnecte toutes les sessions déconnectées. L'option [r] reconnecte toutes les sessions déconnectées et actives.

Exemple de commande sur StoreFront :

- `./storebrowse -Wr https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -WR https://my.firstexamplestore.net/Citrix/Store/discovery`

-WD –disconnect

Description :

Déconnecte toutes les sessions du magasin spécifié.

Exemple de commande sur StoreFront :

```
./storebrowse -WD https://my.firstexamplestore.net/Citrix/Store/discovery
```

-WT –logoff

Description :

Met fin à toutes les sessions du magasin spécifié.

Exemple de commande sur StoreFront :

```
./storebrowse -WT https://my.firstexamplestore.net/Citrix/Store/discovery
```

-v –version

Description :

Affiche la version de l'utilitaire storebrowse.

Exemple de commande sur StoreFront :

```
./storebrowse -v
```

-r –icaroot

Description :

Spécifie le répertoire racine dans lequel l'application Citrix Workspace pour Linux est installée. S'il n'est pas spécifié, le répertoire racine est déterminé au moment de l'exécution.

Exemple de commande sur StoreFront :

```
./storebrowse -r /opt/Citrix/ICAClient
```


-U –username, -P –password, -D domain

Description :

Transmet le nom d'utilisateur, le mot de passe et les détails du domaine au serveur. Cette méthode fonctionne uniquement avec un magasin PNA. Les magasins StoreFront ignorent cette commande. Les détails ne sont pas mis en cache. Vous devez entrer les détails avec chaque commande.

Exemple de commande sur StoreFront :

```
./storebrowse -E https://my.firstexamplestore.net/Citrix/Store/discovery -U
user1 -P password -D domain-name
```

-d –deletestore

Description :

Annule l'enregistrement d'un magasin auprès du démon ServiceRecord.

Exemple de commande sur StoreFront :

```
./storebrowse -d https://my.firstexamplestore.net/Citrix/Store/discovery
```

-c –configselfservice

Description :

Obtient et configure les paramètres de l'interface utilisateur en libre-service qui sont stockés dans StoreCache.ctx. Prend un argument au format <entry[=value]>. Si seule l'entrée est présente, la valeur actuelle du paramètre est imprimée. Toutefois, si une valeur est présente, elle est utilisée pour configurer le paramètre.

Exemple de commande sur StoreFront :

```
./storebrowse -c SharedUserMode=True
```

-C –addCR

Description :

Lit le fichier Citrix Receiver (CR) fourni et vous invite à ajouter chaque magasin. La sortie est la même que la commande **-a**, mais contient plusieurs magasins, séparés par de nouvelles lignes.

Exemple de commande sur StoreFront :

```
./storebrowse -C <path to CR file>
```


-K –killdaemon

Description :

Arrête le processus de démon storebrowse. Toutes les informations d'identification et tous les jetons sont alors effacés.

Exemple de commande sur StoreFront :

```
./storebrowse -K
```

-e –listerrorcodes

Description :

Répertorie les codes d'erreur enregistrés.

Exemple de commande sur StoreFront :

```
./storebrowse -e
```

-g –storegateway

Description :

Définit la passerelle par défaut pour un magasin qui est déjà enregistré auprès du démon ServiceRecord.

Exemple de commande sur StoreFront :

```
./storebrowse -g "<unique gateway name>" https://my.firstexamplestore.net/
Citrix/Store/discovery
```

> **Remarque :**
>
> Le nom unique de la passerelle doit figurer dans la liste des passerelles pour le magasin spécifié.

-q, –quicklaunch

Description :

Lance une application à l'aide de l'URL directe. Cette commande fonctionne uniquement pour les magasins StoreFront.

Exemple de commande sur StoreFront :

```
.\storebrowse.exe -q <https://my.firstexamplestore.net/Citrix/Store/resources
/v2/Q2hJkOlmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix
/Store/discovery>
```


-n –nosingleshot

Description :

Exécute toujours le démon pour le processus storebrowse.

Exemple de commande sur StoreFront :

```
./storebrowse -n
```

-F –fileparam

Description :

Lance un fichier avec le chemin d'accès du fichier et la ressource spécifiés.

Exemple de commande sur StoreFront :

```
./storebrowse -F "<path to file>" -L <Resource Name> <https://my.firstexamplestore
.net/Citrix/Store/discovery>
```

Workflow

Cet article illustre un workflow simple sur la façon de lancer une application à l'aide des commandes storebrowse :

1. `./storebrowse -a https://my.firstexamplestore.net`

   Ajoute un magasin et fournit l'URL complète du magasin. Notez l'URL complète car elle est utilisée dans les commandes ultérieures.

2. `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`

   Répertorie toutes les applications et tous les bureaux publiés. Entrez vos informations d'identification à l'aide de la fenêtre contextuelle qui s'affiche pour le magasin enregistré.

3. `./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery`

   Lance la ressource. Prenez Resource_Name à partir du résultat de la commande précédente.

4. `./storebrowse -K`

   Cette commande purge les informations d'identification entrées précédemment et met fin au démon storebrowse. Si vous ne mentionnez pas explicitement cette commande, le processus storebrowse se ferme au bout d'une heure.

Dépannage

March 23, 2021

Cet article contient des informations destinées à aider les administrateurs à résoudre tous les problèmes rencontrés avec l'application Citrix Workspace pour Linux.

Connexion

Vous pouvez rencontrer les problèmes de connexion suivants.

Lancement d'ICA sur Fedora 29/30

Le lancement d'ICA peut échouer sur Fedora 29/30. Pour contourner le problème, procédez comme suit :

1. Installez openssl10 à l'aide de la commande

```
`sudo yum install compat-openssl10.x86_64`
```

1. Définissez la variable d'environnement dans ~/.bashrc à charger pour chaque session. Cette action pointe vers l'ancienne bibliothèque libcrypto.

```
`export LD_PRELOAD=/lib64/libcrypto.so.1.0.2o`

> **Remarque :**
>
> L'application fonctionne bien dans le serveur X.Org par rapport au
   compositeur Wayland. Pour les distributions utilisant Wayland comme
   protocole graphique par défaut, supprimez les marques de
   commentaires pour l'un des éléments suivants :
 >
> `WylandEnable=false in /etc/gdm/custom.conf` or
 > `/et/gdm3/custome.conf`. Déconnectez-vous et connectez-vous pour
    pointer vers le serveur X.Org.
```

Session de ressource ou de bureau publié(e)

Si, lors de l'établissement d'une connexion à un serveur Windows, une boîte de dialogue présente le message « Connexion au serveur… » sans qu'aucune fenêtre de connexion ne s'affiche ensuite, vous

devrez peut-être configurer le serveur au moyen d'une licence d'accès client (CAL, Client Access License). Pour plus d'informations sur le système de licences, consultez la section Système de licences.

Reconnexion de session

Il peut arriver que la reconnexion à une session avec un nombre de couleurs plus élevé que celui exigé par l'application Citrix Workspace entraîne l'échec de la connexion. Cette défaillance est dûe à un manque de mémoire disponible sur le serveur. En cas d'échec de la reconnexion, l'application Citrix Workspace tente d'utiliser le nombre de couleurs initial. Sinon, le serveur tente de démarrer une nouvelle session avec le nombre de couleurs requis, en laissant la session initiale dans l'état déconnecté. La deuxième connexion peut toutefois échouer si la mémoire disponible sur le serveur est toujours insuffisante.

Nom Internet complet

Citrix vous recommande de configurer le DNS (Domain Name Server) sur votre réseau afin de pouvoir résoudre le nom des serveurs auxquels vous souhaitez vous connecter. Si le DNS n'est pas configuré, vous ne pourrez peut-être pas résoudre le nom du serveur en adresse IP. Vous pouvez également spécifier le serveur avec son adresse IP plutôt qu'avec son nom. Les connexions TLS requièrent un nom de domaine complet, et non une adresse IP.

Échec de la détection du proxy

Si votre connexion est configurée de manière à utiliser la détection automatique des serveurs proxy et qu'un message d'erreur de type « Échec de détection du proxy : erreur JavaScript » s'affiche lorsque vous tentez de vous connecter, copiez le fichier `wpad.dat` dans le répertoire `$ICAROOT/util`. Exécutez la commande suivante, où NomHôte désigne le nom d'hôte du serveur auquel vous tentez de vous connecter :

```
cat wpad.dat | ./pacexec pac.js FindProxyForURL <http://hostname>
hostname 2\>&1 | grep "undeclared variable"
```

Si aucune sortie n'est générée, cela signifie que le fichier `wpad.dat` du serveur ne présente pas de problème grave devant faire l'objet d'investigations. Cependant, si la commande génère un message de type « assignment to undeclared variable … », corrigez le problème. Ouvrez le fichier `pac.js` et, pour chaque variable répertoriée dans la sortie, ajoutez une ligne en haut du fichier en respectant le format suivant, où « … » correspond au nom de la variable.

```
var ...;
```


Sessions lentes

Si une session ne démarre pas tant que vous ne déplacez pas la souris, il existe peut-être avec un problème avec la génération de nombres aléatoires dans le noyau Linux. Pour résoudre le problème, exécutez un démon entropy-generating tel que `rngd` (basé sur le matériel) ou `haveged` (de Magic Software).

Suites de chiffrement

Si votre connexion échoue avec les nouvelles suites de chiffrement prises en charge :

1. Vous pouvez utiliser différents outils pour vérifier les suites de chiffrement prises en charge par votre serveur, notamment :
   - `Ssllabs.com` (nécessite que le serveur ait accès à Internet)
   - `sslyze` (`https://github.com/nabla-c0d3/sslyze`)
2. Dans le client Linux WireShark, recherchez le paquet (Client Hello, Server Hello) avec le filtre (ip.addr = = vdaipAddress) pour trouver la section SSL. Les suites de chiffrement sont ensuite envoyées par le client et acceptées par le serveur.

Citrix Optimization SDK incorrect

Le package Citrix Optimization SDK contient une version incorrecte du fichier UIDialogLibWebKit.so. Pour contourner le problème, procédez comme suit :

1. Téléchargez le package Citrix Optimization SDK version 18.10 à partir de la page Téléchargements.
   a) Accédez au chemin CitrixPluginSDK/UIDialogLib/GTK :
   ```
   cd CitrixPluginSDK/UIDialogLib/GTK
   ```
   b) Supprimez tous les fichiers objet :
   ```
   rm -rf *.o
   ```
   c) Accédez au dossier WebKit :
   ```
   cd ../WebKit
   ```
   d) Supprimez le UIDialogLibWebKit.so existant :
   ```
   rm -rf UIDialogLibWebKit.so
   ```
   e) Utilisez la commande suivante dans le répertoire WebKit :
   ```
   make all
   ```
   Le nouveau UIDialogLibWebKit.so est généré.
   f) Copiez la nouvelle bibliothèque dans le répertoire **$ICAROOT/lib**.

Suites de chiffrement à faible complexité pour les connexions SSL

Lors de l'établissement d'une connexion TLS, l'application Citrix Workspace pour Linux offre une suite de chiffrement par défaut plus moderne et plus restreinte. Si vous vous connectez à un serveur qui requiert une suite de chiffrement plus ancienne, vous devez définir l'option de configuration SSLCiphers=ALL dans la section [WFClient] d'un fichier de configuration.

Les suites de chiffrement avancées suivantes sont prises en charge :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030), ALL, GOV
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028), ALL, GOV
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013), ALL, COM

Perte de connexion

Lorsque vous utilisez le protocole UDT, le message d'erreur : « La connexion à "…" a été perdue » peut s'afficher. Ce problème peut survenir lorsque la connexion transite via un routeur avec une unité de transmission maximale pour UDT qui est inférieure à la valeur par défaut de 1 500 octets. Procédez comme suit :

- Définissez les `edtMSS=1000` dans un fichier de configuration.

Erreurs de connexion

Des erreurs de connexion peuvent entraîner l'affichage d'un grand nombre de boîtes de dialogue d'erreur différentes. Exemples :

- Erreur de connexion : « Une erreur de protocole s'est produite lors de la communication avec le service d'authentification ».
- Impossible de contacter le service d'authentification.
- Votre compte ne peut pas être ajouté à l'aide de cette adresse de serveur

Un certain nombre de problèmes peuvent entraîner de telles erreurs :

- L'ordinateur local et l'ordinateur distant ne peuvent pas négocier un protocole TLS commun. Pour de plus amples informations, consultez la section TLS.
- Lorsque l'ordinateur distant requiert une suite de chiffrement plus ancienne pour une connexion TLS. Dans ce cas, vous pouvez définir l'option de configuration `SSLCiphers=ALL` dans la section `\[WFClient\]` d'un fichier de configuration et exécuter `killall AuthManagerDaemon ServiceRecord selfservice storebrowse` avant de redémarrer la connexion.
- L'ordinateur distant demande un certificat client inapproprié. IIS ne doit **accepter** ou **demander** de certificats que pour Citrix, l'authentication ou un certificat.
- Autres problèmes.

Connexions à faible bande passante

Citrix recommande d'utiliser la version la plus récente de Citrix Virtual Apps and Desktops sur le serveur et de l'application Citrix Workspace sur la machine utilisateur.

Si vous utilisez une connexion à faible bande passante, vous pouvez améliorer les performances de cette connexion en modifiant la configuration de l'application Citrix Workspace et la façon dont vous utilisez cette dernière.

- **Configurez la connexion de votre application Citrix Workspace** : la configuration des connexions de votre application Citrix Workspace peut réduire la bande passante requise par ICA et améliorer les performances.
- **Modifiez la façon dont l'application Citrix Workspace est utilisée** : modifier la façon dont l'application Citrix Workspace est utilisée permet également de réduire la bande passante requise pour une connexion ultra-performante.
- **Activez l'audio UDP** : cette fonctionnalité peut garantir une latence constante sur les réseaux surchargés dans les connexions VoIP (Voice-over-IP)
- **Utilisez les dernières versions de Citrix Virtual Apps et de l'application Citrix Workspace pour Linux** : Citrix améliore les performances à chaque nouvelle version ; de ce fait, de nombreuses fonctions nécessitent la dernière version de l'application Citrix Workspace et du logiciel serveur.

Afficher

Screen Tearing

Le screen tearing (déchirure d'écran) se produit lorsque deux images différentes (ou plus) apparaissent simultanément sur l'écran, en blocs horizontaux. Ce problème est plus fragrant dans les zones larges sur lesquelles du contenu est fréquemment modifié. Bien que les données soient capturées sur le VDA de manière à éviter le tearing, et qu'elles soient transmises au client de manière à ne pas introduire de tearing, X11 (le sous-système graphique de Linux/Unix) ne fournit pas de méthode cohérente permettant de dessiner sur l'écran de manière à éviter le tearing.

Pour éviter le screen tearing, Citrix préconise l'approche standard qui consiste à synchroniser le dessin de l'application avec le dessin de l'écran. En d'autres termes, attendre `vsvnc` pour initier le dessin de l'image suivante. Il existe un certain nombre d'options lors de l'utilisation de Linux ; elles dépendent du matériel graphique dont vous disposez sur le client et du gestionnaire de fenêtres que vous utilisez. Ces options sont divisées en deux groupes de solutions :

- Paramètres du processeur graphique X11
- Utilisation d'un gestionnaire de composition

Configuration du processeur graphique X11

Pour les processeurs Intel HD Graphics, créez un fichier dans xorg.conf.d appelé **20-intel.conf** avec le contenu suivant :

Section “Device”

```
1  Identifier    ”Intel Graphics”
2  Driver        ”intel”
3  Option        ”AccelMethod” ”sna”
4  Option        ”TearFree” ”true”
```

EndSection

Pour les processeurs NVIDIA Graphics, accédez au fichier dans le dossier xorg.conf.d qui contient l’option « MetaModes » pour votre configuration. Pour chaque MetaMode séparé par une virgule, ajoutez ce qui suit :

{ForceFullCompositionPipeline = On}

Par exemple :

Option “MetaModes” “DFP-0: 1920x1200 +0+0 {ForceFullCompositionPipeline = On}”

> **Remarque :**
>
> Différentes distributions Linux utilisent des chemins différents pour xorg.conf.d, par exemple, /etc/X11/xorg.conf.d, ou /user/share/X11/xorg.conf.d.

Gestionnaires de composition

Utilisez ce qui suit :

- Compiz (intégré à Ubuntu Unity). Installez « CompizConfig Settings Manager ».

  Exécutez « CompizConfig Settings Manager ».

  Sous « General > Composition » décochez la case « Undirect Fullscreen Windows ».

> **Remarque :**
>
> Utilisez « CompizConfig Settings Manager » avec précaution, car toute valeur modifiée de façon incorrecte peut empêcher le système de se lancer.

- Compton (composant additionnel). Reportez-vous à la page/documentation principale de Compton pour de plus amples informations. Par exemple, exécutez la commande suivante :

  ```
  compton --vsync opengl --vsync -aggressive
  ```


Touches incorrectes

Si vous utilisez un clavier non anglais, l'affichage à l'écran peut ne pas correspondre à votre saisie au clavier. Dans ce cas, vous devez spécifier le type et la configuration de clavier utilisés. Pour plus d'informations sur la spécification des claviers, veuillez consulter la section Contrôler le comportement du clavier.

Actualisation excessive de l'affichage

Certains gestionnaires de fenêtres signalent constamment la nouvelle position de la fenêtre lors des déplacements de fenêtres transparentes, ce qui peut entraîner une actualisation excessive de l'affichage. Pour résoudre ce problème, basculez le gestionnaire de fenêtres dans un mode qui dessine uniquement les contours des fenêtres lors du déplacement d'une fenêtre.

Compatibilité des icônes

L'application Citrix Workspace pour Linux crée des icônes de fenêtre qui sont compatibles avec la plupart des gestionnaires de fenêtres, mais qui ne le sont pas complètement avec la convention de communication entre clients X.

Compatibilité totale des icônes

Pour garantir la compatibilité totale des icônes :

1. Ouvrez le fichier de configuration wfclient.ini.
2. Modifiez la ligne suivante dans la section [WFClient] : UseIconWindow=True
3. Enregistrez, puis fermez le fichier.

Couleur du curseur

Il est quelquefois difficile de voir le curseur s'il est de la même couleur ou presque que l'arrière-plan. Pour remédier à ce problème, forcez l'affichage des zones du curseur en noir ou en blanc.

Pour modifier la couleur du curseur

1. Ouvrez le fichier de configuration wfclient.ini.
2. Ajoutez l'une des lignes suivantes à la section [WFClient] :

   CursorStipple=ffff,ffff (pour afficher le curseur en noir)

   CursorStipple=0,0 (pour afficher le curseur en blanc)
3. Enregistrez, puis fermez le fichier.

Clignotement des couleurs

Lorsque vous déplacez le pointeur de la souris vers la fenêtre de connexion ou l'en sortez, les couleurs de la fenêtre qui n'est pas activée se mettent à clignoter. Il s'agit d'une limitation connue de l'utilisation du système X Windows avec les affichages PseudoColor. Dans la mesure du possible, choisissez un nombre de couleurs supérieur pour la connexion concernée.

Changements de couleur avec l'affichage TrueColor

Les utilisateurs ont la possibilité de choisir 256 couleurs lorsqu'ils se connectent à un serveur. Cette option suppose que le matériel vidéo prend en charge la palette de couleurs de manière à permettre aux applications de changer les couleurs de la palette pour produire des affichages animés.

Or, les affichages TrueColor ne permettent pas d'émuler la capacité à produire des animations par le changement rapide du contenu de la palette. L'émulation logicielle de cette fonctionnalité est coûteuse à la fois en termes de temps et de trafic réseau. Pour réduire ce coût, l'application Citrix Workspace place dans la mémoire tampon les changements de palette rapides et met seulement à jour la palette réelle au bout de quelques secondes.

Affichage incorrect

L'application Citrix Workspace utilise le codage de caractères EUC-JP ou UTF-8 pour le japonais tandis que le serveur applique le codage de caractères SJIS. L'application Citrix Workspace ne procède à aucune conversion entre ces jeux de caractères. Ce problème peut donc entraîner des problèmes d'affichage de fichiers enregistrés sur le serveur et ouverts localement ou inversement (des fichiers locaux visualisés à partir du serveur). Ce problème concerne également les caractères japonais contenus dans les paramètres utilisés dans le passage de paramètres étendu.

Extension des sessions

Par défaut, les sessions en plein écran couvrent tous les moniteurs, mais une option de ligne de commande de contrôle d'affichage multi-écran, -span, est également disponible. Elle permet aux sessions en plein écran de s'étendre sur plusieurs écrans.

La barre d'outils de Desktop Viewer vous permet de passer d'une session en mode fenêtre à une session en mode plein écran, et prend également en charge le multi-écrans pour les moniteurs d'intersection.

> **Important :**
>
> L'option -span est sans effet sur les sessions affichées dans des fenêtres transparentes ou normales (y compris dans des fenêtres agrandies).

L'option - span suit le format ci-dessous :
-span [h][o][a|mon1[,mon2[,mon3, mon4]]]

Si h est spécifié, une liste des écrans est imprimée sur `stdout`. Si h est la valeur complète de l'option, wfica se ferme.

Si o est spécifié, la fenêtre de la session prend l'attribut override-redirect.

> **Attention :**
>
> Il est déconseillé d'appliquer cette valeur d'option. Elle doit être spécifiée en dernier recours, pour être utilisée avec des gestionnaires de fenêtres non coopératifs. Dans ce cas, la fenêtre de la session n'est pas visible pour le gestionnaire de fenêtres, ne possède pas d'icône associée et ne peut pas être réempilée. Elle ne disparaît qu'une fois la session fermée.

Si a est spécifié, l'application Citrix Workspace tente de créer une session couvrant tous les moniteurs.

L'application Citrix Workspace suppose que le reste de la valeur de l'option -span est une liste de numéros d'écrans. Une valeur unique sélectionne un écran précis, deux valeurs définissent des écrans situés dans les coins supérieur gauche et inférieur droit de la zone requise, quatre spécifient des écrans situés sur les bords supérieur, inférieur, gauche et droit de la zone.

En supposant que le paramètre o n'a pas été spécifié, wfica utilise le message _NET_WM_FULLSCREEN_MONITORS pour demander une configuration de fenêtre appropriée au gestionnaire de fenêtres, si celui-ci est pris en charge. Sinon, il utilise les indicateurs de taille et de position pour demander la configuration souhaitée.

Vous pouvez exécuter la commande suivante pour tester la prise en charge du gestionnaire de fenêtres :

```
xprop -root | grep \\_NET\\_WM\\_FULLSCREEN\\_MONITORS
```

Si la commande ne génère aucune sortie, cela signifie que le gestionnaire n'est pas pris en charge. Dans ce cas, vous devrez peut-être utiliser une fenêtre de type override-redirect. Vous pouvez configurer une fenêtre de type override-redirect à l'aide de `-span o`.

Pour créer une session couvrant plusieurs écrans à partir de la ligne de commande :

1. À l'invite de commandes, entrez la commande suivante :

   ```
   /opt/Citrix/ICAClient/wfica -span h
   ```

   La liste des numéros des écrans connectés à la machine utilisateur est imprimée dans stdout et wfica se ferme.

2. Prenez note de ces numéros d'écrans.
3. À l'invite de commandes, entrez la commande suivante :

   ```
   /opt/Citrix/ICAClient/wfica -span \[w\[,x\[,y,z\]\]\]
   ```


où w, x, y et z correspondent aux numéros des écrans obtenus à l'étape 1 ci-dessus et où la valeur unique w indique un écran unique, deux valeurs w et x définissent des écrans situés dans les coins supérieur gauche et inférieur droit de la zone requise et quatre valeurs w, x, y et z spécifient des écrans situés sur les bords supérieur, inférieur, gauche et droit de la zone.

> **Important :**
>
> Définissez la variable WFICA_OPTS avant de démarrer le libre-service via un navigateur. Pour ce faire, modifiez le fichier de profil, qui se trouve généralement dans $HOME/.bash_profile ou $HOME/.profile, en y insérant une ligne définissant la variable WFICA_OPTS. Par exemple :

```
export WFICA_OPTS="-span a"
```

Cette modification s'applique à la fois aux sessions Citrix Virtual Apps et Citrix Virtual Desktops.

Si vous avez déjà démarré self-service ou storebrowse, supprimez les processus qu'ils ont démarrés pour que la nouvelle variable d'environnement prenne effet. Supprimez-les avec :

killall AuthManagerDaemon ServiceRecord storebrowse

Applications locales

Vous ne pouvez pas sortir d'une session plein écran pour utiliser des applications locales ou une autre session, car l'interface utilisateur du système côté client est masquée et la fonctionnalité Transparence du clavier désactive la commande clavier habituelle, Alt+Tab par exemple, envoyant la commande au serveur à la place.

Pour résoudre ce problème, utilisez CTRL+F2 pour désactiver temporairement la fonctionnalité Transparence du clavier jusqu'à ce que le focus revienne à la fenêtre de session. Vous pouvez également définir TransparentKeyPassthrough sur No dans $ICAROOT/config/module.ini. Cela désactive la fonctionnalité Transparence du clavier. Toutefois vous devrez peut-être remplacer le fichier ICA en ajoutant ce paramètre dans le fichier All_regions.ini.

Navigateur

Navigateur local

Lors de l'activation d'un lien dans une session Windows, le contenu s'affiche dans un navigateur local La redirection de contenu serveur vers client est activée dans le fichier wfclient.ini. Cette situation entraîne l'exécution d'une application locale. Pour désactiver la redirection de contenu serveur vers client, consultez la section redirection de contenu du serveur vers le client.

Accéder aux ressources publiées

Lorsque vous accédez aux ressources publiées, votre navigateur vous invite à enregistrer un fichier. Il est quelque fois nécessaire de configurer des navigateurs autres que Firefox et Chrome avant d'établir une connexion à une ressource publiée. Cependant, lorsque vous tentez d'accéder à une ressource en cliquant sur une icône de la page, le navigateur vous invite à enregistrer le fichier ICA.

Navigateur particulier

Si vous rencontrez des problèmes lors de l'utilisation d'un navigateur Web particulier, définissez la variable d'environnement BROWSER de manière à spécifier le chemin d'accès local et le nom du navigateur requis avant d'exécuter setupwfc.

Navigateur Firefox

Lorsque vous lancez des bureaux ou des applications dans Firefox, si la page ne répond pas, essayez d'activer le plug-in ICA.

Plug-in ICA dans Firefox

Lorsque le plug-in ICA est activé dans Firefox, les sessions de bureau et d'application peuvent ne pas démarrer. Dans ce cas, essayez de désactiver le plug-in ICA.

Erreurs de configuration

Ces erreurs peuvent se produire suite à une entrée de connexion mal configurée.

E_MISSING_INI_SECTION - vérifiez le fichier de configuration « … ». La section « … » est manquante dans le fichier de configuration.

Le fichier de configuration a été modifié de manière incorrecte ou est endommagé.

E_MISSING_INI_ENTRY - vérifiez le fichier de configuration « … ». La section « … » doit contenir une entrée « … ».

Le fichier de configuration a été modifié de manière incorrecte ou est endommagé.

E_INI_VENDOR_RANGE - vérifiez le fichier de configuration « … ». La gamme de fournisseurs de serveurs X « … » du fichier de configuration n'est pas valide.

Les informations du fournisseur de serveurs X du fichier de configuration sont endommagées. Contactez Citrix.

Erreurs de configuration dans le fichier wfclient.ini

Ces erreurs peuvent se produire suite à une modification incorrecte du fichier wfclient.ini.

E_CANNOT_WRITE_FILE - impossible d'écrire dans le fichier : « … ».

Un problème s'est produit lors de l'enregistrement de la base de données de connexions ; par exemple, l'espace disque était insuffisant.

E_CANNOT_CREATE_FILE - impossible de créer le fichier : « … ».

Un problème s'est produit lors de la création d'une base de données de connexions.

E_PNAGENT_FILE_UNREADABLE - impossible de lire le fichier Citrix Virtual Apps « … » : aucun fichier ou répertoire de ce nom n'existe.

— Ou —

Impossible de lire le fichier Citrix Virtual Apps « … » : Permission refusée.

Vous tentez d'accéder à une ressource via un menu ou un élément de bureau, mais le fichier Citrix Virtual Apps lié à la ressource n'est pas disponible. Actualisez la liste des ressources publiées en sélectionnant Application Refresh dans le menu View, puis tentez d'accéder à nouveau à la ressource. Si l'erreur persiste, vérifiez les propriétés de l'icône de bureau ou de l'élément de menu, ainsi que le fichier Citrix Virtual Apps auquel l'icône ou l'élément fait référence.

Erreurs de fichiers PAC

Ces erreurs peuvent se produire si votre déploiement utilise des fichiers PAC (autoconfiguration de proxy) pour spécifier des configurations de proxy.

Échec de détection du proxy : adresse URL de configuration automatique incorrecte.

L'adresse indiquée dans le navigateur possède un type d'adresse URL non valide. Les types valides sont http:// et https:// ; les autres types ne sont pas pris en charge. Rectifiez l'adresse afin d'utiliser un type d'adresse URL valide, puis réessayez.

Échec de détection du proxy : échec du téléchargement HTTP du script .PAC : échec de la connexion.

Vérifiez si une adresse ou un nom incorrect a été entré. Si tel est le cas, corrigez l'adresse, puis recommencez. Sinon, il se peut que le serveur soit hors service. Réessayez plus tard.

Échec de détection du proxy : échec de téléchargement HTTP du script .PAC : chemin introuvable.

Le fichier PAC demandé ne se trouve pas sur le serveur. Soit vous corrigez cette erreur sur le serveur, soit vous reconfigurez le navigateur.

Échec de détection du proxy : échec de téléchargement HTTP du script .PAC.

La connexion a échoué pendant le téléchargement du fichier PAC. Rétablissez la connexion, puis réessayez.

Échec de détection du proxy : script de configuration automatique vide.

Le fichier PAC est vide. Soit vous corrigez cette erreur sur le serveur, soit vous reconfigurez le navigateur.

Échec de détection du proxy : aucune prise en charge JavaScript.

Le fichier exécutable PAC ou le fichier texte pac.js est manquant. Réinstallez l'application Citrix Workspace.

Échec de détection du proxy : erreur JavaScript.

Le fichier PAC contient du code JavaScript non valide. Corrigez le fichier PAC situé sur le serveur. Voir aussi Connexion.

Échec de détection du proxy : résultats erronés provenant du script de configuration automatique vide.

Une réponse mal formulée a été envoyée par le serveur. Soit vous corrigez cette erreur sur le serveur, soit vous reconfigurez le navigateur.

Certificats

Lorsque vous utilisez un magasin avec l'authentification SAML (à l'aide du protocole Authv3), le message d'erreur suivant s'affiche : « Certificat TLS inacceptable ».

Ce problème se produit lorsque vous utilisez la version 1906 ou des versions ultérieures de l'application Citrix Workspace pour Linux. Pour obtenir des instructions de dépannage, consultez l'article CTX260336 du Centre de connaissances.

Si votre serveur StoreFront ne peut pas fournir les certificats intermédiaires correspondant au certificat qu'il utilise, ou que vous installez des certificats intermédiaires pour prendre en charge des utilisateurs de cartes à puce, suivez ces étapes avant d'ajouter un magasin StoreFront :

1. Obtenez le ou les certificats intermédiaires séparément au format PEM.

   > **Conseil :**
   >
   > Si vous ne trouvez aucun certificat de format PEM, utilisez l'utilitaire openssl pour convertir un certificat au format CRT en un fichier .pem.

2. En tant qu'utilisateur, installez le package (généralement racine) :

   a) Copiez le ou les fichiers dans $ICAROOT/keystore/intcerts.

   b) Exécutez la commande suivante en tant qu'utilisateur qui a installé le package :

   ```
   $ICAROOT/util/ctx_rehash
   ```


Si vous authentifiez un certificat de serveur qui a été émis par une autorité de certification et qui n'a pas encore été approuvé par la machine utilisateur, suivez les instructions suivantes avant d'ajouter un magasin StoreFront :

1. Obtenez le certificat racine au format PEM.
   Conseil : si vous ne trouvez aucun certificat de ce format, utilisez l'utilitaire openssl pour convertir un certificat au format CRT en un fichier .pem.
2. En tant qu'utilisateur qui a installé le package (généralement racine) :
   a) Copiez le fichier dans $ICAROOT/keystore/cacerts.
   b) Exécutez la commande suivante :
   `$ICAROOT/util/ctx_rehash`

Autres

Problèmes de connexion

Vous pouvez également rencontrer les problèmes de connexion suivants.

Fermer une session

Si vous voulez savoir si le serveur a demandé à l'application Citrix Workspace de fermer une session, vous pouvez utiliser le programme *wfica* pour consigner les réceptions de commande demandant à mettre fin à la session à partir du serveur.

Pour enregistrer ces informations via le système syslog, ajoutez *SyslogThreshold* avec la valeur 6 à la section [WFClient] du fichier de configuration. Cela permet la journalisation des messages qui ont la priorité LOG_INFO ou une priorité plus élevée. La valeur par défaut pour *SyslogThreshold* est de 4 (=LOG_WARNING).

De même, pour que *wfica* envoie les informations en tant qu'erreur standard, ajoutez *PrintLogThreshold* avec la valeur 6 à la section [WFClient]. La valeur par défaut pour *PrintLogThreshold* est de 0 (=LOG_EMERG).

Pour de plus amples informations sur la journalisation, consultez Journalisation et pour plus d'informations sur la configuration de syslog, consultez configuration syslog.

Paramètres du fichier de configuration

Pour que ces paramètres entrent en vigueur, il est nécessaire qu'à chaque entrée figurant dans le fichier wfclient.ini corresponde une entrée équivalente dans le fichier All_Regions.ini. De plus, chaque entrée figurant dans les sections [Thinwire3.0], [ClientDrive] et [TCP/IP] du fichier wfclient.ini doit disposer d'une entrée correspondante dans le fichier canonicalization.ini. Pour plus d'informations, consultez les fichiers All_Regions.ini et canonicalization.ini situés dans le répertoire $ICAROOT/config.

Applications publiées

Si vous avez des problèmes avec l'exécution d'applications publiées accédant à un port série, elle peut échouer (sans nécessairement générer de message d'erreur) si le port est verrouillé par une autre application. Dans ce genre de situation, vérifiez qu'aucune application n'a temporairement verrouillé le port série ou ne l'a verrouillé sans le libérer avant sa fermeture.

Pour résoudre ce problème, arrêtez l'application qui bloque le port en série. Dans le cas de verrouillages de style UUCP, il se peut qu'un fichier de verrouillage reste en place après fermeture de l'application. L'emplacement de ces fichiers de verrouillage dépend du système d'exploitation utilisé.

Démarrage de l'application Citrix Workspace

Si l'application Citrix Workspace ne démarre pas, le message d'erreur « Application default file could not be found or is out of date » s'affiche. Cela peut s'expliquer par le fait que la variable d'environnement ICAROOT est mal définie. Il est indispensable de définir cette variable si vous avez installé l'application Citrix Workspace à un emplacement autre que le répertoire par défaut. Pour résoudre ce problème, Citrix vous recommande d'effectuer l'une des opérations suivantes :

- Définissez ICAROOT comme répertoire d'installation.

  Pour vérifier si la variable d'environnement ICAROOT est définie correctement, essayez de lancer l'application Citrix Workspace à partir d'une session de terminal. Si le message d'erreur s'affiche encore, cela signifie très probablement que la variable d'environnement ICAROOT est mal définie.

- Dans ce cas, réinstallez l'application Citrix Workspace à l'emplacement par défaut. Pour plus d'informations sur l'installation de l'application Citrix Workspace, consultez la section Installer et configurer.

  Si l'application Citrix Workspace était installée à l'emplacement par défaut, supprimez le répertoire `/opt/Citrix/ICAClient` où `$HOME/ICAClient/` avant de procéder à la réinstallation.

Citrix CryptoKit (anciennement SSLSDK)

Pour rechercher le numéro de version de Citrix CryptoKit (anciennement SSLSDK) ou OpenSSL que vous exécutez, vous pouvez utiliser la commande suivante :

```
strings libctxssl.so | grep "Citrix SSLSDK"
```

Vous pouvez également exécuter cette commande sur AuthManagerDaemon ou PrimaryAuthManager

Raccourcis clavier

Si votre gestionnaire de fenêtres utilise les mêmes combinaisons de touches pour fournir la fonctionnalité native, votre combinaison de touches risque de ne pas fonctionner correctement. Par ex-

emple, le gestionnaire de fenêtres KDE utilise les combinaisons de touches CTRL+MAJ+F1 jusqu'à CTRL+MAJ+F4 pour basculer entre les bureaux 13 à 16. Si vous rencontrez ce problème, essayez l'une des solutions suivantes :

- Le mode Translated sur le clavier mappe un ensemble de combinaisons de touches locales à des combinaisons de touches du côté serveur. Par exemple, par défaut en mode Translated, CTRL+MAJ+F1 correspond à la combinaison de touches ALT+F1 du côté serveur. Pour reconfigurer ce mappage sur une autre combinaison de touches locales, mettez à jour l'entrée suivante dans la section [WFClient] de $HOME/.ICAClient/wfclient.ini. Cela mappe la combinaison de touches locales Alt+Ctrl+F1 sur Alt+F1 :
  - Modifiez Hotkey1Shift=Ctrl+Maj sur Hotkey1Shift=Alt+Ctrl.
- Le mode Direct sur le clavier envoie toutes les combinaisons de touches directement vers le serveur. Elles ne sont pas traitées localement. Pour configurer le mode Direct, dans la section [WFClient] de $HOME/.ICAClient/wfclient.ini, définissez TransparentKeyPassthrough sur Remote.
- Reconfigurez le gestionnaire de fenêtres afin qu'il supprime les combinaisons de touches par défaut.

Clavier croate distant

Cette procédure garantit que les caractères ASCII sont envoyés correctement aux bureaux virtuels distants avec des configurations de clavier croate.

1. Dans la section WFClient du fichier de configuration approprié, définissez UseEUKSforASCII sur True.
2. Définissez UseEUKS sur 2.

Clavier japonais

Pour configurer l'utilisation d'un clavier japonais, mettez à jour l'entrée suivante dans le fichier de configuration wfclient.ini :

KeyboardLayout=Japanese (JIS)

Clavier ABNT2

Pour configurer l'utilisation d'un clavier ABNT2, mettez à jour l'entrée suivante dans le fichier de configuration wfclient.ini :

KeyboardLayout=Brazilian (ABNT2)

Clavier local

Si certaines touches du clavier local ne se comportent pas comme prévu, choisissez la configuration de serveur qui correspond le mieux dans la liste de $ICAROOT/config/module.ini.

Lecteur Windows Media

L'application Citrix Workspace ne dispose peut-être pas des plug-ins GStreamer requis pour traiter un format demandé. Lorsque cela se produit, le serveur demande généralement un format différent. Il arrive parfois que la vérification de la présence d'un plug-in approprié indique à tort qu'un tel plug-in est effectivement présent. Cela est généralement détecté et entraîne l'affichage d'une boîte de dialogue d'erreur sur le serveur indiquant que le Lecteur Windows Media a rencontré un problème lors de la lecture d'un fichier. Il suffit généralement de lire de nouveau le fichier dans la session car cela entraîne le rejet du format par l'application Citrix Workspace, et en conséquence, le serveur demande un autre format ou restitue le média lui-même.

Dans quelques situations, l'absence d'un plug-in approprié n'est pas détectée et le fichier n'est pas lu correctement, bien que l'indicateur de progression avance comme prévu dans le Lecteur Windows Media.

Pour éviter l'affichage de cette boîte de dialogue d'erreur ou l'échec de la lecture dans les sessions futures :

1. Ajoutez de façon temporaire l'option de configuration « SpeedScreenMMAVerbose=On » à la section [WFClient] de $Home/.ICAClient/wfclient.ini, par exemple.
2. Redémarrez WFICA à partir d'un libre-service qui a été démarré à partir d'un terminal.
3. Lisez une vidéo qui génère cette erreur.
4. Notez (dans la sortie de traçage) le type mime associé à la trace du plug-in manquant, ou le type mime qui devrait être pris en charge mais dont la lecture échoue (par exemple, "video/x-h264..").
5. Modifiez $ICAROOT/config/MediaStreamingConfig.tbl. Sur la ligne sur laquelle figure le type mime, insérez un '?' entre ':' et le type mime. Cela désactive le format.
6. Répétez les étapes 2 à 5 (ci-dessus) pour tout autre format multimédia qui génère cette erreur.
7. Distribuez ce MediaStreamingConfig.tbl modifié aux autres machines qui disposent du même ensemble de plug-ins GStreamer.

> **Remarque :**
>
> Éventuellement, après avoir identifié le type mime, il est possible d'installer un plug-in GStreamer pour le décoder.

Configuration de port série

Pour configurer un port série unique, ajoutez les entrées suivantes dans le fichier de configuration $ICAROOT/config/module.ini :

LastComPortNum=1

ComPort1=device

Pour configurer deux ports série ou plus, ajoutez les entrées suivantes dans le fichier de configuration $ICAROOT/config/module.ini :

LastComPortNum=2

ComPort1=device1

ComPort2=device2

Erreurs

Cette rubrique dresse la liste d'autres messages d'erreur courants pouvant s'afficher lors de l'utilisation de l'application Citrix Workspace.

Une erreur s'est produite. Le code d'erreur est 11 (E_MISSING_INI_SECTION). Reportez-vous à la documentation. Fin de la session.

Lors de l'exécution de l'application Citrix Workspace à partir de la ligne de commande, ce message signifie généralement que la description fournie sur la ligne de commande est introuvable dans le fichier appsrv.ini.

E_BAD_OPTION - l'option « … » n'est pas valide.

Argument manquant pour l'option « … ».

E_BAD_ARG - l'option « … » comporte un argument non valide : « … ».

Argument non valide spécifié pour l'option « … ».

E_INI_KEY_SYNTAX - la clé « … » du fichier de configuration « … » n'est pas valide.

Les informations du fournisseur de serveurs X du fichier de configuration sont endommagées. Créez un fichier de configuration.

E_INI_VALUE_SYNTAX - la valeur « … » du fichier de configuration « … » n'est pas valide.

Les informations du fournisseur de serveurs X du fichier de configuration sont endommagées. Créez un fichier de configuration.

E_SERVER_NAMELOOKUP_FAILURE - la connexion au serveur « … » a échoué.

Impossible de résoudre le nom du serveur.

Impossible d'écrire sur un ou plusieurs fichiers : « … ». Corrigez les éventuels problèmes de disques saturés ou d'autorisations, puis réessayez.

Recherchez des problèmes de disques saturés ou d'autorisations insuffisantes. Si un problème est détecté puis résolu, réessayez l'opération ayant généré le message d'erreur.

La connexion au serveur a été perdue. Rétablissez la connexion, puis réessayez. Ces fichiers peuvent comporter des données manquantes : « … ».

Rétablissez la connexion, puis réessayez l'opération ayant généré l'erreur.

Informations de diagnostic

Si vous rencontrez des problèmes liés à l'utilisation de l'application Citrix Workspace, le centre d'assistance technique peut être amené à vous demander de lui transmettre des informations de diagnostic. Ces informations leur permettront de tenter de poser un diagnostic et de vous aider à corriger le problème.

Pour obtenir les informations de diagnostic relatives à l'application Citrix Workspace

1. Dans le répertoire d'installation, tapez util/lurdump. Il est recommandé de procéder de la sorte lorsqu'une session est ouverte, et si possible, alors que le problème est présent.

   Un fichier rassemblant des informations de diagnostic détaillées est généré, comprenant les détails de version, le contenu des fichiers de configuration de l'application Citrix Workspace et les valeurs de différentes variables système.

2. Avant d'envoyer ce fichier au centre d'assistance, vérifiez qu'il ne contient pas d'informations confidentielles.

Résoudre les problèmes de connexion aux ressources

Les utilisateurs peuvent gérer leurs connexions actives à l'aide du Centre de connexion. Cette fonctionnalité est un outil de productivité très utile, qui permet aux utilisateurs et aux administrateurs de résoudre les problèmes liés aux connexions lentes ou complexes. Grâce au Centre de connexion, les utilisateurs peuvent gérer les connexions en :

- Fermant une application.
- Fermant une session. Cette étape met fin à la session et ferme toutes les applications ouvertes.
- Déconnectant une session. Cette étape interrompt la connexion sélectionnée au serveur sans fermer les applications ouvertes (sauf si le serveur est configuré pour fermer les applications au moment de la déconnexion).
- Affichant les statistiques de transport de connexion.

SDK et API

July 6, 2020

SDK du canal virtuel Citrix

Le SDK du canal virtuel Citrix prend en charge l'écriture de pilotes du côté serveur et du côté client afin de fournir des canaux virtuels supplémentaires à l'aide du protocole ICA. Les applications de canal virtuel côté serveur se trouvent sur des serveurs Citrix Virtual Apps and Desktops. Si vous souhaitez écrire des pilotes virtuels pour d'autres plates-formes clientes, contactez le support technique Citrix.

Le SDK du canal virtuel offre ce qui suit :

- L'interface Citrix Virtual Driver Application Programming Interface (VDAPI) utilisée avec les fonctions de canal virtuel dans le SDK de l'API Citrix Server (WFAPI SDK) pour créer de nouveaux canaux virtuels. La prise en charge de canal virtuel fournie par VDAPI est conçue pour faciliter l'écriture de vos propres canaux virtuels.
- Un code source opérationnel pour plusieurs exemples de programmes de canal virtuel qui illustrent les techniques de programmation.
- Le SDK de canal virtuel requiert le SDK WFAPI pour écrire sur le côté serveur du canal virtuel.

Pour de plus amples informations, consultez SDK du canal virtuel Citrix pour l'application Citrix Workspace pour Linux.

Référence de ligne de commande

Pour plus d'informations sur les paramètres et références de ligne de commande, veuillez consulter Référence des commandes de l'application Citrix Workspace pour Linux.

SDK d'optimisation de la plate-forme

Dans le cadre de l'initiative HDX SoC pour l'application Citrix Workspace pour Linux, nous avons développé le « SDK d'optimisation de la plate-forme » afin d'offrir un écosystème d'appareils à faible coût, faible consommation et très performants dans des formats innovants.

Le SDK d'optimisation de la plate-forme peut être utilisé par les développeurs désireux d'améliorer les performances des appareils Linux en leur permettant de créer des extensions de plug-in pour le composant de moteur ICA (wfica) de l'application Citrix Workspace pour Linux. Les plug-ins sont intégrés en tant que bibliothèques partageables qui sont chargées dynamiquement par wfica. Ces plug-ins peuvent vous aider à optimiser les performances de vos appareils Linux en activant les fonctions suivantes :

- Décodage accéléré des données JPEG et H.264 utilisées pour afficher l'image de la session
- Contrôle de l'allocation de mémoire utilisée pour afficher l'image de la session
- Amélioration des performances en prenant le contrôle de l'affichage de bas niveau de l'image de la session
- Services de sortie graphique et d'entrée utilisateur pour les environnements de système d'exploitation qui ne prennent pas en charge X11

Pour de plus amples informations, consultez la section Application Citrix Workspace pour Linux - SDK d'optimisation de la plate-forme.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States