Application Citrix Workspace pour Linux

Contents

À propos de cette version

October 10, 2022

Nouveautés dans la version 2209

Prise en charge de l'authentification à l'aide de FIDO2 [Technical Preview]

Avec cette version, vous pouvez vous authentifier auprès d'applications ou de bureaux virtuels à l'aide de clés de sécurité FIDO2. Les clés de sécurité FIDO2 permettent aux employés de l'entreprise de s'authentifier auprès d'applications ou de bureaux prenant en charge FIDO2 sans entrer de nom d'utilisateur ou de mot de passe. Pour plus d'informations sur FIDO2, consultez Authentification FIDO2.

> **Remarque :**
>
> Si vous utilisez le périphérique FIDO2 via la redirection USB, supprimez la règle de redirection USB de votre appareil FIDO2 du `usb.conf` fichier du `$ICAROOT/` dossier. Cette mise à jour vous permet de passer au canal virtuel FIDO2.

Par défaut, l'authentification FIDO2 est désactivée. Pour activer l'authentification FIDO2, procédez comme suit :

1. Accédez au fichier `<ICAROOT>/config/module.ini`.
2. Accédez à la section ICA 3.0.
3. Définissez `FIDO2= On`.

Cette fonctionnalité prend actuellement en charge les authentificateurs itinérants (USB uniquement) avec code PIN et fonctionnalités tactiles. Vous pouvez configurer l'authentification basée sur les clés de sécurité FIDO2. Pour plus d'informations sur les conditions préalables et l'utilisation de cette fonctionnalité, consultez Autorisation locale et authentification virtuelle à l'aide de FIDO2.

Lorsque vous accédez à une application ou à un site Web prenant en charge FIDO2, une invite s'affiche demandant l'accès à la clé de sécurité. Si vous avez préalablement enregistré votre clé de sécurité avec un code PIN (un minimum de 4 et un maximum de 64 caractères), vous devez saisir le code PIN lors de la connexion.

Si vous avez préalablement enregistré votre clé de sécurité sans code PIN, il vous suffit de toucher la clé de sécurité pour vous connecter.

Limitation :

Vous risquez de ne pas enregistrer le second appareil sur un même compte à l'aide de l'authentification FIDO2.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

Améliorations apportées au mode de saisie du clavier [version Technical Preview]

Auparavant, vous pouviez activer différents modes de saisie du clavier uniquement en mettant à jour la valeur de `KeyboardEventMode` dans le fichier de configuration. Aucune option d'interface utilisateur n'existait pour sélectionner le mode de saisie du clavier.

À partir de l'application Citrix Workspace 2209, vous pouvez configurer différents modes de saisie du clavier à partir de la nouvelle section **Paramètres du mode de saisie du clavier**. Vous pouvez sélectionner **Scancode** ou **Unicode** comme mode de saisie du clavier.

Pour plus d'informations, consultez **Améliorations apportées au mode de saisie du clavier** dans la documentation sur la synchronisation de la disposition du clavier.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

Prise en charge des dispositions de clavier étendues [version Technical Preview]

À partir de la version 2209 de l'application Citrix Workspace, le mode de saisie du clavier Scancode prend en charge les dispositions de clavier étendues suivantes :

- Clavier japonais 106
- Claviers portugais ABNT/ABNT2
- Claviers multimédia

Le mode de saisie du clavier Scancode prend en charge les dispositions de clavier étendues, ainsi que tous les modes de synchronisation de la disposition du clavier.

Cette prise en charge est activée par défaut.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

Améliorations apportées à Microsoft Teams

- **Activation du partage d'applications :** à partir de l'application Citrix Workspace 2209 pour Linux et Citrix Virtual Apps and Desktops 2109, vous pouvez partager une application à l'aide de la fonctionnalité Partage d'écran de Microsoft Teams.
- **Améliorations apportées à la prise en charge de la fonction DPI élevé :** lorsque la fonction « DPI élevé » est activée et que vous utilisez des moniteurs 4K, les superpositions vidéo de Microsoft Teams se trouvent à la position et à la taille souhaitées. Quels que soient vos paramètres d'affichage, tels que la disposition sur un ou plusieurs écrans, les superpositions s'affichent toujours correctement et ne sont pas redimensionnées ou apparaissent dans une position indésirable. Pour activer cette amélioration, assurez-vous que le paramètre `DPIMatchingEnabled` du fichier `wfclient.ini` de configuration est défini sur **True**. Pour plus d'informations, consultez Prise en charge de la correspondance DPI.
- **Mise à niveau du SDK WebRTC :** la version du SDK WebRTC utilisée pour Microsoft Teams optimisé a été mise à niveau vers la version M98.

Version améliorée des bibliothèques de compatibilité

À partir de cette version, l'application Citrix Workspace pour Linux est compatible avec les bibliothèques suivantes :

- glibc 2.27 ou version ultérieure
- glibcxx 3.4.25 ou version ultérieure

Mise à jour du composant Protection des applications

> **Remarque :**
>
> Le composant Protection des applications n'est pas pris en charge sur Ubuntu 22.04. Par conséquent, si vous installez le module Protection des applications sur Ubuntu 22.04, vous ne pourrez peut-être pas démarrer des applications et des bureaux virtuels dans l'application Citrix Workspace. Pour plus d'informations sur la fonction Protection des applications, consultez la

> section Protection des applications.

Problèmes résolus dans la version 2209

- Lorsque la fonctionnalité Protection des applications est activée, la fonctionnalité de protection contre l'enregistrement de frappe peut ne pas fonctionner pour l'interface Authentication Manager qui charge la page Web dans une fenêtre séparée. [RFLNX-9004]
- Après la mise à niveau vers l'application Citrix Workspace 2007 pour Linux, l'ajout d'un magasin à l'aide de Storebrowse peut prendre beaucoup de temps, car le magasin tente de contacter le service de configuration de l'application qui est inaccessible. [CVADHELP-20618]
- Lorsque vous vous connectez à un magasin cloud à partir de l'interface utilisateur en libre-service, une roue tournante peut apparaître sur la page de connexion. [CVADHELP-20039]
- Lorsque vous démarrez deux applications à partir de deux groupes de mise à disposition différents, le démarrage de la deuxième application peut être retardé. [CVADHELP-18198]

Problèmes connus dans la version 2209

- Lorsque vous démarrez une session dans l'application Microsoft Edge, l'icône Microsoft Edge s'affiche de manière aléatoire à différentes échelles. Cette erreur se produit si vous avez appliqué les paramètres suivants :
  - La valeur `DPIMatchingEnabled` est définie sur **True**.
  - L'échelle du client affichée à l'écran n'est pas réglée sur 100 %.

  [HDX-39764]
- Les tentatives de démarrage d'une session VDA de serveur à l'aide de l'authentification par carte à puce peuvent échouer pour les cartes à puce comportant plusieurs utilisateurs. Pour résoudre le problème, réinsérez la carte à puce. [HDX-44255]
- Le VDA peut se bloquer après avoir redirigé l'interface du périphérique. Ce problème se produit lorsque vous activez la stratégie « Redirection de périphérique USB client » sur DDC et que vous connectez des périphériques USB composites au point de terminaison, tels qu'un casque USB. Ajoutez la valeur d'entrée dans le fichier usb.conf sous la forme `vid=** pid=** split=01 and intf=00,01`. Démarrez ensuite la session à partir de l'application Citrix Workspace et définissez la redirection de l'interface du périphérique. [HDX-44117]
- Le lancement de la session peut échouer sur le système d'exploitation Raspberry Pi ARMHF basé sur Debian 11. Citrix vous recommande d'utiliser le système d'exploitation Raspberry Pi ARM64 basé sur Debian 11 ou un système d'exploitation Raspberry Pi ARMHF plus ancien basé sur Debian 10. [HDX-41729]
- Lorsque vous supprimez un compte principal, il se peut que les informations d'identification de connexion ne soient pas supprimées du cache de Selfservice. Par conséquent, vous pourrez

peut-être vous connecter au magasin sans fournir d'informations d'identification. Pour contourner ce problème, fermez Selfservice pour supprimer les informations d'identification. [RFLNX-9051]

- Une fois que vous avez fourni les informations d'identification et que vous avez démarré Selfservice, un écran blanc peut apparaître. Pour contourner ce problème, fermez Selfservice et redémarrez-le. [RFLNX-8951]
- Dans OpenSUSE SLES 15, il se peut que vous obteniez une roue tournante lorsque vous vous connectez à un magasin cloud. [RFLNX—9109]
- Il se peut que vous ne parveniez pas à démarrer Selfservice sur RHEL9 et Fedora 36. [RFLNX-9128]

> **Remarque :**
>
> Pour obtenir la liste complète des problèmes des versions précédentes, consultez la section Problèmes connus.

Versions précédentes

Cette section fournit des informations sur les nouvelles fonctionnalités et les problèmes résolus dans les versions précédentes que nous prenons en charge conformément aux étapes du cycle de vie de l'application Citrix Workspace.

2207

Nouveautés

Amélioration de la qualité audio

Auparavant, la valeur maximale de mise en mémoire tampon de sortie pour lire l'audio de manière fluide était de 200 ms dans l'application Citrix Workspace. Par conséquent, une latence de 200 ms a été ajoutée dans le scénario de lecture. Cette valeur maximale de mise en mémoire tampon de sortie avait également un impact sur les applications audio interactives.

Grâce à cette amélioration, la valeur maximale de mise en mémoire tampon de sortie est réduite à 50 ms dans l'application Citrix Workspace. En conséquence, l'expérience utilisateur avec l'application audio interactive est améliorée. De plus, la durée des boucles (RTT) est réduite de 150 ms.

À partir de cette version, vous pouvez sélectionner le seuil de lecture et le pré-tampon audio pulsé appropriés pour améliorer la qualité audio. Pour cette amélioration, les paramètres suivants ont été ajoutés dans la section [ClientAudio] du fichier `module.ini` :

- `PlaybackDelayThreshV4` — Pour spécifier le niveau initial de mise en mémoire tampon de sortie en millisecondes. L'application Citrix Workspace essaie de maintenir ce niveau de

mise en mémoire tampon pendant toute la durée d'une session. La valeur par défaut de `PlaybackDelayThreshV4` est 50 ms. Ce paramètre n'est valide que si `AudioRedirectionV4` est défini sur **True**.

- `AudioTempLatencyBoostV4` — Lorsque le débit audio connaît un pic soudain ou n'est pas suffisant pour un réseau instable, cette valeur augmente la valeur de mise en mémoire tampon de sortie. Cette augmentation de la valeur de mise en mémoire tampon de sortie fournit un son fluide. Cependant, l'audio peut être légèrement retardé. La valeur par défaut de `AudioTempLatencyBoostV4` est définie sur 100 ms. Ce paramètre n'est valide que si `AudioRedirectionV4` est défini sur **True** et `AudioLatencyControlEnabled` est défini sur **True**. Par défaut, la valeur de `AudioLatencyControlEnabled` est définie sur True.

Pour savoir comment activer cette amélioration, consultez la section **Amélioration de la qualité audio** de la documentation Audio.

Prise en charge de la correspondance DPI [Tech Preview]

À partir de cette version, les valeurs de résolution d'affichage et d'échelle DPI définies dans l'application Citrix Workspace correspondent aux valeurs de la session des applications et des bureaux virtuels. Vous pouvez définir la valeur d'échelle requise dans le client Linux, et la mise à l'échelle de la session VDA est mise à jour automatiquement.

La mise à l'échelle DPI est principalement utilisée avec les écrans de grande taille et à haute résolution. Cette fonctionnalité permet d'afficher les éléments suivants dans une taille qui peut être visualisée confortablement :

- Applications
- Texte
- Images
- Autres éléments graphiques

Limitation :

Actuellement, la fonction de correspondance DPI ne prend pas en charge la mise à l'échelle fractionnelle côté client. Si la valeur d'échelle DPI est élevée, l'optimisation Microsoft Teams peut ne pas être prise en charge comme prévu.

Pour savoit comment activer cette fonctionnalité, voir Prise en charge de la correspondance DPI.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonc-

> tion de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

Redirection de périphérique USB composite

À partir de cette version, l'application Citrix Workspace permet de diviser les périphériques USB composites. Un périphérique USB composite peut effectuer plusieurs fonctions. Chacune de ces fonctions est présentée dans une interface différente. Des exemples de périphériques USB composites incluent les périphériques HID composés d'une entrée et d'une sortie audio et vidéo.

Actuellement, la redirection de périphérique USB composite n'est disponible que dans les sessions de bureau. Les appareils divisés apparaissent dans Desktop Viewer.

Auparavant, lorsqu'un périphérique était débranché et rebranché pendant une session, il était redirigé automatiquement. Par conséquent, le périphérique était automatiquement connecté au VDA. Avec cette version, vous devez activer la redirection automatique manuellement via les paramètres du fichier de configuration. La redirection automatique des périphériques USB composites est désactivée par défaut.

Pour plus d'informations sur la configuration de la redirection de périphériques USB composites, consultez la section **Redirection de périphérique USB composite** dans la documentation USB.

Prise en charge améliorée de l'annulation de l'écho audio [Tech Preview]

À partir de cette version, l'application Citrix Workspace prend en charge l'annulation de l'écho. Cette fonctionnalité est conçue pour les cas d'utilisation audio en temps réel et améliore l'expérience utilisateur. La fonction d'annulation de l'écho prend en charge l'audio de qualité moyenne, l'audio de faible qualité et l'audio adaptatif. Citrix recommande d'utiliser l'audio adaptatif pour de meilleures performances.

Par défaut, la fonction d'annulation de l'écho est désactivée. Dans les cas d'utilisation en temps réel, il est recommandé d'activer l'annulation de l'écho si le haut-parleur est utilisé à la place du casque.

Limitation :

La fonction d'annulation de l'écho est désactivée pour un son de haute qualité.

Pour plus d'informations, consultez la section **Prise en charge améliorée de l'annulation de l'écho audio** dans la documentation Audio.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonc-

> tion de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

Prise en charge de la sonnerie secondaire

Vous pouvez utiliser la fonction de sonnerie secondaire pour sélectionner un appareil secondaire sur lequel vous souhaitez recevoir la notification d'appel entrant lorsque Microsoft Teams est optimisé (Citrix HDX optimisé dans À propos/Version). Par exemple, imaginez que vous avez défini un haut-parleur comme sonnerie secondaire et que votre point de terminaison est connecté à un casque. Dans ce cas, Microsoft Teams envoie le signal d'appel entrant au haut-parleur même si votre casque est le périphérique principal pour l'appel audio lui-même. Vous ne pouvez pas définir de sonnerie secondaire dans les cas suivants :

- Lorsque vous n'êtes pas connecté à plusieurs périphériques audio
- Lorsque le périphérique n'est pas disponible (par exemple, un casque Bluetooth)

> **Remarque :**
>
> Cette fonctionnalité est disponible uniquement après le déploiement d'une future mise à jour de Microsoft Teams. Pour savoir quand la mise à jour sera déployée par Microsoft, consultez la feuille de route Microsoft 365. Vous pouvez également consulter l'article CTX253754 pour la mise à jour de la documentation et l'annonce.

Problèmes résolus

- Lorsque vous lancez un bureau en mode plein écran à l'aide de Lightweight X11 Desktop Environment (LXDE) et que vous vous déconnectez du réseau, un message d'erreur **Connection to <XXX> has been lost** s'affiche avec une option **Quit** dans la boîte de dialogue. Le message s'affiche si la stratégie de reconnexion automatique des clients (ACR) ou de fiabilité de session (SR) a expiré. Lorsque vous cliquez sur **Quit**, le bureau de l'utilisateur disparaît. Toutefois, si vous cliquez n'importe où ailleurs sur l'écran, il se peut que le bouton **Quit** ne s'affiche jamais dans la boîte de dialogue. Vous devez quitter manuellement le bureau de l'utilisateur en appuyant sur la touche **Echap** ou **Entrée**. [CVADHELP-17478]
- L'application Citrix Workspace pour Linux peut interpréter les URL contenant la chaîne **cloud** (par exemple <*xxx-yyy-cloud.com*>) comme des URL de domaine cloud, même si elles représentent des URL locales. [CVADHELP-19480]
- La session peut se déconnecter lorsque vous essayez d'utiliser la webcam HDX. Le problème se produit uniquement dans le VDA version 2203. [CVADHELP-20223]
- La copie et le collage de contenu entre des applications publiées, des sessions VDI ou une session VDI et une application publiée peuvent échouer. La session ou l'application peut ne plus répondre pendant un certain temps. [CVADHELP-19899]

- Lorsque vous prévisualisez une vidéo à l'aide de la webcam dans Skype, l'aperçu peut afficher un écran noir. [HDX-37860]
- La compression vidéo de la webcam HDX RealTime ne prend pas en charge les caméras au format vidéo MJPEG dans l'application Citrix Workspace. [HDX-40352]
- Lorsque vous partagez l'écran ou une application pendant un appel Microsoft Teams, votre interlocuteur peut voir des artefacts visuels. Ce problème se produit en raison de fréquences d'images instables, telles que la lecture vidéo incorrecte (images noires figées ou transitoires). Cette version inclut des fréquences d'images ou d'échantillonnage améliorées qui réduisent les artefacts visuels. [HDX-38032]
- La vidéo ou une image dans l'application Citrix Workspace peut ne pas s'afficher correctement. Ce problème se produit lorsque l'application Citrix Workspace est utilisée avec le VDA version 2109 ou ultérieure. [HDX-40287]
- Lorsque vous lancez wfica avec la commande `-span o`, la session peut ne pas se lancer et s'étendre sur tous les moniteurs disponibles. De même, lorsque vous lancez wfica avec la commande `-span h`, la liste des moniteurs actuellement connectés à la machine utilisateur peut ne pas s'imprimer. [HDX-32519]
- Lorsque vous lancez wfica avec la commande `-span o`, la session peut ne pas se lancer et s'étendre sur tous les moniteurs disponibles. De même, lorsque vous lancez wfica avec la commande `-span h`, la liste des moniteurs actuellement connectés à la machine utilisateur peut ne pas s'imprimer. Pour plus d'informations, consultez la section Référence des commandes. [HDX-32519]
- Lorsqu'une erreur SSL se produit sur un protocole pendant une tentative de connexion TCP et EDT/UDP, les deux connexions peuvent échouer en raison de la condition de concurrence. Cette erreur SSL peut se produire si la configuration TLS diffère entre les protocoles et que le client ne peut pas se connecter via un protocole. [RFLNX-8747]
- Lorsque vous essayez de vous connecter à distance à une machine sur laquelle l'application Citrix Workspace avec la fonction Protection des applications est installée, le serveur x11vnc se bloque et la connexion échoue. Par conséquent, il se peut que vous ne puissiez pas vous connecter à distance à la machine via le serveur x11vnc. [RFLNX-8933]
- Lorsque vous ajoutez un magasin avec les paramètres par défaut, l'énumération Storebrowse peut échouer. Ce problème se produit uniquement dans le système d'exploitation Debian 32 bits. [RFLNX-8743]
- Un message d'erreur peut s'afficher lorsque vous installez l'application Citrix Workspace avec la fonctionnalité Protection des applications activée sur des machines Linux 32 bits. [RFLNX-8809]
- Lorsque vous ajoutez un magasin à l'aide de la commande `storebrowse -a` et que vous l'énumérez à l'aide de la commande `storebrowse -E`, l'énumération Storebrowse peut échouer. Ce problème se produit uniquement dans le système d'exploitation Raspberry Pi. [RFLNX-8803]

2205

Nouveautés

Amélioration de l'authentification pour Storebrowse

> **Remarque :**
>
> Cette fonctionnalité est généralement disponible pour l'application Citrix Workspace.

À partir de cette version, la boîte de dialogue d'authentification est présente dans l'application Citrix Workspace et les détails du magasin s'affichent sur l'écran d'ouverture de session. Cette fonctionnalité offre une meilleure expérience utilisateur. Les jetons d'authentification sont chiffrés et stockés. Ainsi, vous n'avez pas besoin de saisir de nouveau les informations d'identification lorsque votre système ou votre session redémarre.

Vous pouvez également désactiver ou activer l'amélioration de l'authentification pour la fonctionnalité Storebrowse à l'aide de la clé `StorebrowseIPC` du fichier `AuthmanConfig.xml`. Par défaut, cette fonctionnalité est désactivée.

L'amélioration de l'authentification prend en charge storebrowse pour les opérations suivantes :

- Storebrowse -E : répertorie les ressources disponibles.
- Storebrowse -L : lance une connexion à une ressource publiée.
- Storebrowse -S : dresse la liste des ressources auxquelles vous avez souscrit.
- Storebrowse -T : met fin à toutes les sessions du magasin spécifié.
- Storebrowse -Wr : reconnecte les sessions déconnectées mais actives du magasin spécifié. L'option [r] reconnecte toutes les sessions déconnectées.
- Storebrowse -Wr : reconnecte les sessions déconnectées mais actives du magasin spécifié. L'option [R] reconnecte toutes les sessions déconnectées et actives.
- Storebrowse -s : abonne la ressource spécifiée à partir d'un magasin donné.
- Storebrowse -u : annule l'abonnement de la ressource spécifiée dans un magasin donné.
- Storebrowse -q : lance une application à l'aide de l'URL directe. Cette commande fonctionne uniquement pour les magasins StoreFront.

> **Remarque :**
>
> - Vous pouvez continuer à utiliser les commandes Storebrowse restantes comme précédemment (en utilisant AuthManagerDaemon).
> - L'amélioration de l'authentification s'applique uniquement aux déploiements dans le cloud.
> - Grâce à cette amélioration, la fonction de connexion permanente est prise en charge.

Pour plus d'informations, consultez Amélioration de l'authentification.

Connexion permanente [version Technical Preview]

La fonction de connexion permanente vous permet de rester connecté pendant la durée (2 à 365 jours) configurée par votre administrateur. Lorsque cette fonctionnalité est activée, vous n'avez pas besoin de fournir les informations d'identification de connexion pour l'application Citrix Workspace pendant la période configurée.

Grâce à cette fonctionnalité, les sessions SSO vers Citrix DaaS sont étendues jusqu'à une période de 365 jours. Cette extension est basée sur la durée de vie des jetons de longue durée. Vos informations d'identification sont mises en cache par défaut pendant 4 jours ou pendant la durée de vie du jeton selon la valeur la plus faible, puis étendues lorsque vous devenez actif pendant ces 4 jours (en vous connectant à l'application Citrix Workspace).

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

Pour plus d'informations, consultez la section Connexion permanente.

Découverte automatique du magasin basée sur l'adresse e-mail

> **Remarque :**
>
> Cette fonctionnalité est généralement disponible pour l'application Citrix Workspace.

Vous pouvez maintenant fournir votre adresse e-mail dans l'application Citrix Workspace pour détecter automatiquement le magasin associé à l'adresse e-mail. Si plusieurs magasins sont associés à un domaine, le premier magasin renvoyé par Global App Configuration Service est ajouté par défaut comme magasin de choix. Si nécessaire, les utilisateurs peuvent toujours basculer vers un autre magasin.

Pour plus d'informations, consultez la section **Découverte automatique du magasin basée sur l'adresse e-mail** dans la documentation de Ajouter l'URL du magasin à l'application Citrix Workspace.

Disposition pour désactiver le service LaunchDarkly

À partir de cette version, vous pouvez désactiver le service LaunchDarkly sur l'application Citrix Workspace.

Pour plus d'informations, consultez la section Gestion des feature flag.

Problèmes résolus

- Le serveur DNS d'un environnement client dont l'accès Internet est limité peut ne pas résoudre l'URL, `clientstream.launchdarkly.com`. Par conséquent, l'application Citrix Workspace envoie un grand nombre de requêtes DNS (> 1 000 en trois secondes par jour) à l'URL. [CVADHELP-19559]
- Lorsque la fonctionnalité Protection des applications est activée, il arrive que la fonctionnalité de protection contre les programmes d'enregistrement de frappe ne fonctionne pas sur l'interface Authentication Manager utilisant la bibliothèque `UIDialogLibWebKit3.so`. Ce problème est résolu dans l'environnement de bureau GNOME et KDE. [RFLNX-8027]
- Lorsque vous essayez d'imprimer à partir d'une session VDA exécutée sur le client ARMHF Raspberry Pi version 3 ou 4, la session peut cesser de répondre. [CVADHELP-18506]
- Lorsque vous lancez l'interface utilisateur en libre-service avec les paramètres par défaut, le message d'erreur suivant peut s'afficher :

  « La réponse à la demande de jeton secondaire n'est pas 200/400/404 42 »

  Ce problème se produit sur Fedora 35. [RFLNX-8603]

2203

Nouveautés

Prise en charge de IPv6 EDT

À compter de cette version, l'application Citrix Workspace prend en charge IPv6 EDT.

Prise en charge du protocole TLS version 1.3

À compter de cette version, l'application Citrix Workspace prend en charge le protocole TLS (Transport Layer Security Protocol) version 1.3.
Pour plus d'informations, veuillez consulter la section TLS.

Magasins Web personnalisés

À compter de la version 2203, cette fonctionnalité est généralement disponible pour l'application Citrix Workspace. Vous pouvez accéder au magasin Web personnalisé de votre organisation à partir de l'application Citrix Workspace.

> **Remarque :**

> La fonctionnalité d'épinglage de la disposition de plusieurs moniteurs n'est pas prise en charge dans le magasin Web personnalisé.

Pour de plus amples informations, consultez la section Magasins Web personnalisés.

Amélioration de l'authentification (fonctionnalité expérimentale)

À compter de cette version, les améliorations apportées à l'authentification prennent en charge Store-Browse pour les opérations suivantes :

- Storebrowse -E pour répertorier les ressources disponibles.
- Storebrowse -L pour lancer une connexion à une ressource publiée.
- Storebrowse -S pour répertorier les ressources auxquelles vous êtes abonné.

> **Remarque :**
>
> Vous pouvez continuer à utiliser les autres commandes Storebrowse dans `AuthMangerDaemon`. Elles seront prises en charge avec les améliorations de l'authentification apportées dans la prochaine version.

Pour plus d'informations, consultez la section Amélioration de l'authentification pour Storebrowse.

Amélioration apportée à la synchronisation de la disposition du clavier

La synchronisation de la disposition du clavier vous permet de basculer entre leurs dispositions de clavier préférées sur la machine cliente. Cette fonction est désactivée par défaut. Lorsqu'elle est activée, la disposition du clavier client se synchronise automatiquement avec la session Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service).

À compter de la version 2203, l'application Citrix Workspace prend en charge les trois modes de synchronisation de la disposition du clavier suivants :

- **Synchroniser une seule fois – lorsque la session est lancée** : basé sur la valeur `KeyboardLayout` du fichier `wfclient.ini`, la disposition du clavier du client est synchronisée avec le serveur lorsque la session est lancée. Si la valeur `KeyboardLayout` est définie sur `0`, le clavier système est synchronisé avec le VDA. Si la valeur `KeyboardLayout` est définie sur une langue spécifique, le clavier spécifique à la langue est synchronisé avec le VDA. Les modifications que vous apportez à la disposition du clavier du client pendant la session ne prennent pas effet immédiatement. Pour appliquer les modifications, déconnectez-vous et connectez-vous à l'application. Le mode **Synchroniser une seule fois - lorsque la session est lancée** est la disposition de clavier par défaut sélectionnée pour l'application Citrix Workspace.
- **Autoriser la synchronisation dynamique** : cette option synchronise la disposition du clavier client sur le serveur lorsque vous modifiez la disposition du clavier client.
- **Ne pas synchroniser** : indique que le client utilise la disposition du clavier présente sur le serveur.

Pour plus d'informations, consultez la section Synchronisation de la disposition du clavier.

Chat et réunions multi-fenêtre pour Microsoft Teams

Vous pouvez utiliser plusieurs fenêtres pour le chat et les réunions dans Microsoft Teams lorsqu'elles sont optimisées par HDX dans Citrix Virtual Apps and Desktops (version 2112 ou ultérieure). Vous pouvez ouvrir plusieurs fenêtres pour les conversations ou les réunions de différentes manières. Pour plus d'informations sur la fonctionnalité pop-out ou multi-fenêtre, consultez Teams Pop-Out Windows for Chats and Meetings.

Si vous exécutez une ancienne version de l'application Citrix Workspace ou du Virtual Delivery Agent (VDA), notez que Microsoft abandonnera le code de fenêtre unique à l'avenir. Toutefois, vous disposerez d'un minimum de neuf mois pour mettre à niveau vers une version du VDA ou de l'application Citrix Workspace prenant en charge le mode multi-fenêtre (version 2203 ou supérieure). Pour effectuer la mise à niveau vers une version supérieure, vous disposerez d'au moins neuf mois après la disponibilité générale de cette fonctionnalité.

> **Remarque :**
>
> Cette fonctionnalité est disponible uniquement après le déploiement d'une future mise à jour de Microsoft Teams. Lorsque la mise à jour sera déployée par Microsoft, vous pourrez consulter l'article CTX253754 pour la mise à jour de la documentation et l'annonce.

Amélioration de la redirection automatique des périphériques USB

Auparavant, lorsqu'un périphérique était débranché et rebranché pendant une session, il était redirigé automatiquement. Par conséquent, le périphérique était automatiquement connecté au VDA. Avec cette version, vous devez activer la redirection automatique manuellement via les paramètres du fichier de configuration. La redirection automatique des périphériques USB est désactivée par défaut. Pour plus d'informations, consultez la section USB.

Problèmes résolus

- Lorsque vous ajoutez un magasin et que vous l'authentifiez auprès de l'application Citrix Workspace, la fenêtre d'authentification est chargée une deuxième fois, même après une authentification réussie. Ce problème se produit lorsque vous vous connectez pour la première fois à l'application Citrix Workspace après avoir défini `AuthManLiteEnabled` sur **True**. [RFLNX-8694]
- Après avoir installé l'application Citrix Workspace avec la fonction Protection des applications activée sur le système d'exploitation utilisant `glibc 2.34`, le démarrage du système d'exploitation peut échouer lors du redémarrage du système. [RFLNX-8358]

- Lorsque vous utilisez Microsoft Teams pour passer un appel P2P ou pour assister à une réunion et que vous attendez un certain temps, la charge d'un cœur de processeur peut atteindre 100% en raison d'une erreur de socket. [HDX-38974]
- L'application Citrix Workspace ne prend pas en charge la nouvelle version du système d'exploitation Raspberry Pi basée sur Debian bullseye. [HDX-37000]
- Lorsque vous lancez une session avec le fichier ICA et que vous vous déconnectez de la session, la valeur renvoyée attendue que vous recevez de la ligne de commande `wfica` est 0. Toutefois, au lieu de la valeur attendue, la valeur que vous recevez est 2. Ce problème se produit dans l'application Citrix Workspace version 2106 ou ultérieure. [HDX-38916]
- Dans l'application Citrix Workspace, vous pouvez rencontrer des échecs intermittents lorsque vous répondez ou passez un appel Microsoft Teams. Le message d'erreur suivant s'affiche :

  « L'appel n'a pas pu être établi. »

  [HDX-38819]

2202

Nouveautés dans la version 2202

Audio UDP via Citrix Gateway

> **Remarque :**
>
> Cette amélioration est généralement disponible pour l'application Citrix Workspace.

Dans cette version, l'application Citrix Workspace prend en charge le protocole DTLS (Datagram Transport Layer Security) pour l'audio UDP. Par conséquent, vous pouvez accéder à l'audio UDP via Citrix Gateway.

Pour activer l'audio UDP via Citrix Gateway :

1. Accédez au dossier <`ICAROOT`>/`config` et ouvrez le fichier `module.ini`.
2. Accédez à la section [WFClient] et définissez l'entrée suivante :

   EnableUDPThroughGateway=True
3. Accédez à la section [ClientAudio] et définissez l'entrée suivante :

   EnableUDPAudio=True

Pour plus d'informations, consultez la section **Activation de l'audio UDP** dans la documentation Audio.

> **Remarque :**
>
> Si vous utilisez la configuration StoreFront default.ica, la valeur de `EnableUDPThroughGateway` définie dans la section [Application] est prioritaire sur la valeur définie dans le fichier `module.ini`. Toutefois, vous ne pouvez définir la valeur `EnableUDPAudio` dans la section [ClientAudio] uniquement à l'aide du fichier `module.ini`. En outre, cette valeur n'est pas prioritaire sur la valeur définie dans le fichier de configuration StoreFront default.ica.

Problèmes résolus

- Lorsque vous installez l'application Citrix Workspace, que vous ajoutez un magasin et lancez un bureau, la fenêtre de session peut ne pas s'afficher. Ce problème se produit si la bibliothèque `libpcscd` n'est pas installée sur Ubuntu 16.04. [HDX-36574]
- Dans l'application Citrix Workspace 2112, vous pouvez rencontrer une utilisation élevée du processeur sur le point de terminaison lorsqu'une webcam est activée dans un appel vidéo Microsoft Teams optimisé. [HDX-37168]
- Vous rencontrez des problèmes de performances car l'utilisation du processeur atteint 100%. [RFLNX-8200]
- Lors d'une session de bureau lancée à l'aide de l'interface graphique en libre-service, l'enregistrement de la disposition de session actuelle à l'aide du bouton **Enregistrer mise en page** de la barre d'outils **Desktop Viewer** peut échouer avec le message d'erreur suivant :

  « Impossible d'enregistrer la disposition de la session. »

  Toutefois, la disposition de la session peut être restaurée lors de la prochaine reconnexion de session.
  [CVADHELP-18971]
- La création de dossiers ou de fichiers sur des lecteurs mappés à l'aide du mappage des lecteurs clients peut échouer sur les VDA Windows exécutés sur des versions plus récentes de systèmes d'exploitation clients avec le message d'erreur suivant :

  « Vous devez disposer d'une autorisation pour effectuer cette action. »
  Les systèmes d'exploitation incluent Ubuntu 21.04 et Fedora 34 ou version ultérieure.
  [CVADHELP-18448]
- Le serveur DNS d'un environnement client dont l'accès Internet est limité peut ne pas résoudre l'URL, `clientstream.launchdarkly.com`. En conséquence, l'application Citrix Workspace pour Linux envoie constamment des requêtes DNS à l'URL. Cette action peut entraîner des millions de requêtes DNS pour quelques centaines de clients Linux en ligne, causant le crash du serveur DNS. [CVADHELP-19140]

> **Remarque :**
>
> Les requêtes DNS aux sites liés à LaunchDarkly peuvent être envoyées toutes les trois secondes par jour.

2112

Nouveautés dans la version 2112

Prise en charge de l'inversion de couleur du curseur

Auparavant, l'application Citrix Workspace affichait un curseur en pointillé de la même couleur que l'arrière-plan noir et blanc d'un texte. Par conséquent, il était difficile de localiser la position du curseur.

Dans cette version, la couleur du curseur s'inverse en fonction de la couleur d'arrière-plan d'un texte. Vous pouvez ainsi facilement localiser la position du curseur dans le texte. Cette fonctionnalité est désactivée par défaut.

Conditions préalables :

- 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 `All_Regions.ini`, ajoutez les lignes suivantes à la fin de la section [Virtual Channels\Thinwire Graphics] :

  InvertCursorEnabled=

  InvertCursorRefreshRate=

  InvertCursorMode=

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.

Pour activer cette fonctionnalité, procédez comme suit :

1. Accédez au fichier de configuration `$HOME/.ICAClient/wfclient.ini`.
2. Accédez à la section [Thinwire3.0] et définissez l'entrée suivante :

   InvertCursorEnabled=True

> **Remarque :**
>
> Le curseur ne s'inverse pas lorsque la valeur de la stratégie **Utiliser codec vidéo pour la compression** dans Citrix Studio est définie sur **Ne pas utiliser de codec vidéo**.

Mise à jour de l'audio adaptatif

L'audio adaptatif fonctionne désormais lors de l'utilisation de la mise à disposition de l'audio UDP (User Datagram Protocol). Pour plus d'informations, consultez la section Audio adaptatif.

> **Remarque :**
>
> Cette amélioration requiert la version 2112 ou ultérieure de VDA.

Pour plus d'informations sur la configuration audio UDP à l'aide de l'audio adaptatif sur l'application Citrix Workspace, consultez la section **Activation de l'audio UDP** dans la documentation Audio.

Prise en charge de plusieurs périphériques audio [version Technical Preview]

À partir de cette version, l'application Citrix Workspace affiche tous les périphériques audio locaux disponibles dans une session, ainsi que leur nom. En outre, une prise en charge Plug and Play pour les périphériques audio Bluetooth et HDMI est également fournie.

Cette fonction est désactivée par défaut. Pour activer cette fonctionnalité, définissez la valeur `AudioRedirectionV4` sur **True** dans le fichier module.ini.

Pour plus d'informations, consultez la section Audio.

> **Remarque :**
>
> À partir de cette version, l'attribut `VdcamVersion4Support` du fichier `module.ini` est renommé `AudioRedirectionV4`.

Audio UDP via Citrix Gateway [version Technical Preview]

Dans cette version, l'application Citrix Workspace prend en charge le protocole DTLS (Datagram Transport Layer Security) pour l'audio UDP. Par conséquent, vous pouvez accéder à l'audio UDP via Citrix Gateway.

Pour activer l'audio UDP via Citrix Gateway :

1. Accédez au dossier <`ICAROOT`>/`config` et ouvrez le fichier `module.ini`.
2. Accédez à la section [WFClient] et définissez l'entrée suivante :

   EnableUDPThroughGateway=True
3. Accédez à la section [ClientAudio] et définissez l'entrée suivante :

   EnableUDPAudio=True

Pour plus d'informations, consultez la section **Activation de l'audio UDP** dans la documentation Audio.

> **Remarque :**
>
> Si vous utilisez la configuration StoreFront default.ica, la valeur de `EnableUDPThroughGateway` définie dans la section [Application] est prioritaire sur la valeur définie dans le fichier `module.ini`. Toutefois, vous pouvez définir la valeur `EnableUDPAudio` dans la section [ClientAudio] uniquement à l'aide du fichier `module.ini` ; elle n'est pas prioritaire sur la valeur définie dans la configuration StoreFront default.ica.

Améliorations apportées à la prise en charge des cartes à puce

> **Remarque :**
>
> Cette amélioration est généralement disponible pour l'application Citrix Workspace.

À compter de cette version, l'application Citrix Workspace prend en charge la fonctionnalité Plug and Play pour le lecteur de carte à puce.

Lorsque vous insérez une carte à puce, le lecteur de carte à puce la détecte dans le serveur et le client. Vous pouvez utiliser la fonctionnalité Plug and Play sur plusieurs cartes en même temps, et elles seront toutes détectées.

Conditions préalables :

Installez la bibliothèque `libpcscd` sur le client Linux.

> **Remarque :**
>
> Cette bibliothèque peut être installée par défaut dans les versions récentes de la plupart des distributions Linux. Cependant, il se peut que vous deviez installer la bibliothèque `libpcscd` dans des versions antérieures de certaines distributions Linux, telles qu'Ubuntu 1604.

Pour désactiver cette amélioration :

1. Naviguez jusqu'au dossier `<ICAROOT>/config/module.ini`.
2. Accédez à la section `SmartCard`.
3. Définissez le `DriverName=VDSCARD.DLL`.

Amélioration apportées à l'optimisation de Microsoft Teams

> **Remarque :**
>
> Les fonctionnalités suivantes sont disponibles uniquement après le déploiement d'une future mise à jour de Microsoft Teams. Lorsque la mise à jour sera déployée par Microsoft, vous pourrez consulter l'article CTX253754 pour la mise à jour de la documentation et l'annonce.

- **Demander le contrôle dans Microsoft Teams**

Avec cette version, vous pouvez demander le contrôle lors d'un appel Microsoft Teams lorsqu'un participant partage l'écran. Une fois que vous avez le contrôle, vous pouvez effectuer des sélections ou des modifications sur l'écran partagé.

Pour prendre le contrôle lorsqu'un écran est partagé, cliquez sur **Demander le contrôle** en haut de l'écran Microsoft Teams. Le participant à la réunion qui partage l'écran peut accepter ou refuser votre demande.

Tant que vous avez le contrôle, vous pouvez effectuer des sélections, des modifications et d'autres activités sur l'écran partagé. Lorsque vous avez terminé, cliquez sur **Abandonner le contrôle**.

Limitations :

- Les utilisateurs d'un client Linux ne peuvent pas *donner* le contrôle à d'autres utilisateurs. En d'autres termes, une fois que l'utilisateur du client Linux commence à partager du contenu, l'option **Donner le contrôle** n'est pas présente dans la barre d'outils de partage. Ce problème est une limitation Microsoft.
- L'option **Demander le contrôle** n'est pas disponible lors de l'appel peer-to-peer entre les utilisateurs suivants :
  - Un utilisateur optimisé
  - Un utilisateur sur le client de bureau Microsoft Teams natif qui s'exécute sur le point de terminaison.

  Pour contourner le problème, les utilisateurs peuvent rejoindre une réunion pour obtenir l'option **Demander le contrôle**.
- **Prise en charge des appels d'urgence dynamiques**

Avec cette version, l'application Citrix Workspace prend en charge les appels d'urgence dynamiques. Lorsque cette fonction est utilisée avec les forfaits d'appel Microsoft, Operator Connect et Direct Routing, elle permet de :

- Configurer et acheminer les appels d'urgence
- Informer le personnel de sécurité

La notification est fournie en fonction de l'emplacement actuel de l'application Citrix Workspace exécutée sur le point de terminaison, au lieu du client Microsoft Teams exécuté sur le VDA.

La loi Ray Baum exige que l'emplacement de la personne effectuant l'appel d'urgence soit transmis au centre de réception des appels d'urgence approprié. À partir de l'application Citrix Workspace 2112 pour Linux, l'optimisation Microsoft Teams avec HDX est conforme à la loi Ray Baum. Pour prendre en charge cette fonctionnalité, la bibliothèque LLDP doit être incluse dans la distribution du système d'exploitation du client léger.

Problèmes résolus

- Lors de la lecture de vidéos de longue durée, l'audio s'arrête mais la vidéo continue. Le problème s'est produit lorsque vous avez défini `VdcamVersion4Support` (renommé `AudioRedirectionV4`) sur **True**. [RFLNX-6472]
- Pendant les appels audio pair à pair de Microsoft Teams, le son peut ne pas fonctionner pendant les 15 premières secondes de l'appel. [HDX-29526]
- Au cours de la session de partage d'écran, la bordure rouge indiquant l'écran partagé s'étend sur tous les écrans, lorsque Microsoft Teams s'exécute en mode transparent et en configuration multi-moniteur. [HDX-34978]
- Pendant l'appel vidéo Microsoft Teams, la caméra peut clignoter. [HDX-36345]
- La session à double saut (ou double-hop) ne prend pas en charge la fonctionnalité Plug and Play du lecteur de carte à puce. [HDX-34582]
- Les tentatives de lancement d'une session à l'aide de l'authentification par carte à puce peuvent échouer. Le problème se produit avec l'application Citrix Workspace pour Linux version 2104 et ultérieure. [CVADHELP-18402]
- La lecture audio au cours d'une session peut détériorer les facteurs de performance du réseau, tels que la durée des boucles et la fiabilité de la session. [CVADHELP-18723]
- L'application Citrix Workspace 2106 et versions ultérieures installées sur un client léger peut échouer lorsqu'elle est connectée à un bureau virtuel sur lequel le codec Opus (renommé audio adaptatif) est activé. Ce problème se produit parce que le fichier opus.dll créé dans le répertoire `ICAClient` comprend le fichier opus lib créé à partir d'un autre référentiel. Ce fichier opus lib comprend le jeu d'instructions AVX-512 qui ne prend pas en charge certains processeurs du client léger. [HDX-36440]
- Lorsque vous vous connectez à un magasin cloud à partir de l'interface utilisateur en libre-service, une roue tournante peut apparaître sur la page de connexion. [RFLNX-8486]
- Une fois que vous vous êtes connecté à l'interface utilisateur en libre-service, la tentative d'arrêt du processus en libre-service à l'aide de la commande `Killall selfservice` de la ligne de commande peut échouer. [RFLNX-8248]

2111

Nouveautés

Workspace Intelligence (version Technical Preview)

Cette version de l'application Citrix Workspace est optimisée pour profiter des fonctionnalités Workspace Intelligence au moment de leur publication. Pour plus d'informations, consultez Fonctionnalités de Workspace Intelligence - Micro-apps.

Indicateur d'état de la batterie

Auparavant, l'état de la batterie d'un appareil n'apparaissait pas dans la zone de notification pour les VDA de serveur.

Dans cette version, l'indicateur d'état de la batterie s'affiche pour les VDA de serveur.

Prise en charge des magasins Web personnalisés [version Technical Preview]

Avec cette version, vous pouvez accéder au magasin Web personnalisé de votre organisation à partir de l'application Citrix Workspace.

Pour utiliser cette fonctionnalité, l'administrateur doit ajouter le domaine ou le magasin Web personnalisé à la liste des URL autorisées dans Global App Configuration Service. Une fois cette opération effectuée, vous pouvez fournir l'URL du magasin Web personnalisé sur l'écran **Ajouter un compte** de l'application Citrix Workspace. Le magasin Web personnalisé s'ouvre dans la fenêtre de l'application Workspace native.

Pour plus d'informations sur la configuration des adresses URL des magasins Web pour les utilisateurs, consultez Global App Configuration Service.

Pour supprimer le magasin Web personnalisé, accédez à **Comptes** > **Ajouter ou supprimer des comptes**, sélectionnez l'URL du magasin Web personnalisé, puis cliquez sur **Supprimer**.

Avant de commencer, vous devez activer le magasin Web personnalisé dans le fichier `AuthManConfig.xml`. Pour de plus amples informations, consultez la section Magasins Web personnalisés.

> **Remarque :**
>
> Vous pouvez uniquement utiliser les URL répertoriées dans le fichier `AuthManConfig.xml` pour le magasin Web personnalisé. Vous pouvez ajouter différentes adresses URL dans le fichier `AuthManConfig.xml` que vous souhaitez prendre en compte pour le magasin Web personnalisé.

Redirection de webcam pour applications 64 bits [version Technical Preview]

Cette version améliore les performances globales et la stabilité de la webcam avec les applications 32 bits. Elle introduit également la prise en charge de la redirection de webcam pour les applications 64 bits. Pour de plus amples informations, consultez la section Webcams.

Améliorations apportées à la prise en charge des cartes à puce [version Technical Preview]

À compter de cette version, l'application Citrix Workspace prend en charge la fonctionnalité Plug and Play pour le lecteur de carte à puce.

Lorsque vous insérez une carte à puce, le lecteur de carte à puce la détecte dans le serveur et le client. Vous pouvez utiliser la fonctionnalité Plug and Play sur plusieurs cartes en même temps, et elles seront toutes détectées.

Pour configurer cette fonctionnalité, procédez comme suit :

1. Naviguez jusqu'au dossier <ICAROOT>/config/module.ini.
2. Accédez à la section SmartCard.
3. Définissez le DriverName=VDSCARDV2.DLL.

Améliorations apportées à Microsoft Teams

- Ajout d'une nouvelle dépendance pour llvm-12 : dans cette version, une nouvelle dépendance appelée libunwind-12 library est ajoutée pour llvm-12. Toutefois, par défaut, elle n'existe pas dans le référentiel d'origine. Installez libunwind-12 library manuellement dans le référentiel. Pour plus d'informations sur l'installation de libunwind-12 library, consultez Optimisation pour Microsoft Teams.
- Amélioration des configurations de l'annulation de l'écho, du contrôle automatique du gain et de la suppression du bruit : si Microsoft Teams configure les options de contrôle automatique du gain et de suppression du bruit, Microsoft Teams redirigé par Citrix respecte les valeurs configurées. Sinon, ces options sont activées par défaut. Toutefois, l'option d'annulation de l'écho est désactivée par défaut. Pour plus d'informations, consultez Optimisation pour Microsoft Teams.

Problèmes résolus

- Les tentatives de reconnexion à la session peuvent se produire une seule fois lors de la reconnexion automatique des clients. Par conséquent, la stratégie **Reconnexion automatique des clients** peut ne pas fonctionner comme prévu. [HDX-34114]
- Vous rencontrez des échecs d'appel lorsqu'un appel P2P est effectué depuis l'application Citrix Workspace pour Linux 2109 vers l'application Citrix Workspace pour Windows 2109 ou Citrix Workspace pour Mac 2109. [HDX-35223]

2109

Nouveautés

Amélioration de la fiabilité de session

Auparavant, grâce à la fonctionnalité de fiabilité de session HDX Broadcast, la fenêtre d'une application publiée était toujours affichée même si la connexion à l'application subissait des interruptions.

Avec cette version, l'écran change lorsque la fiabilité de session commence. La fenêtre de session est grisée et un minuteur affiche le temps qui reste avant la prochaine tentative de reconnexion.

> **Remarque :**
>
> Cette fonctionnalité est prise en charge uniquement pour Citrix Virtual Desktops.

Amélioration de la journalisation

Auparavant, aucun outil permettant de collecter les fichiers journaux dans l'application Citrix Workspace n'était disponible. Les fichiers journaux se trouvaient dans des dossiers différents. Vous deviez collecter manuellement les fichiers journaux à partir de ces dossiers différents.

À partir de cette version, l'application Citrix Workspace introduit l'outil collectlog.py pour collecter des fichiers journaux à partir de dossiers différents. Vous pouvez exécuter cet outil à l'aide de la ligne de commande. Les fichiers journaux sont générés sous forme de fichier journal compressé. Vous pouvez télécharger ce fichier journal compressé à partir du serveur local. Pour plus d'informations, consultez la section Journalisation.

Continuité du service

> **Remarque :**
>
> Cette fonctionnalité est généralement disponible pour l'application 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 sessions Citrix Virtual Apps and Desktops et Citrix DaaS quel que soit l'état d'intégrité des services cloud.

Pour plus d'informations sur les exigences requises pour prendre en charge la continuité du service sur l'application Citrix Workspace, consultez Configuration système requise.

Pour plus d'informations sur l'installation de la continuité des services avec l'application Citrix Workspace, consultez Installation de la continuité du service.

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

Prise en charge de la continuité du service avec l'extension Web de Citrix Workspace pour Google Chrome

La prise en charge de la continuité du service avec l'extension Web de Citrix Workspace pour Google Chrome est disponible en version Technical Preview publique. Vous pouvez utiliser l'extension Web de Workspace pour Google Chrome avec l'application Citrix Workspace pour Linux 2109. Cette extension est disponible sur le Google Chrome Web Store. L'application Workspace communique avec l'extension Web de Citrix Workspace à l'aide du protocole hôte de messagerie natif pour l'extension de navigateur. Ensemble, l'application Workspace et l'extension Web Workspace utilisent des locations de connexion Workspace pour permettre aux utilisateurs du navigateur d'accéder à leurs applications et bureaux pendant les pannes. Pour plus d'informations, consultez Continuité du service.

Audio adaptatif

Avec l'audio adaptatif, vous n'avez pas besoin de configurer manuellement les stratégies de qualité audio sur le VDA. L'audio adaptatif optimise les paramètres de votre environnement et remplace les formats de compression audio obsolètes pour offrir une excellente expérience utilisateur. L'audio adaptatif est activé par défaut. Pour plus d'informations, consultez la section Audio adaptatif.

> **Remarque :**
>
> Si la mise à disposition de l'audio UDP est requise pour les applications audio en temps réel, l'audio adaptatif doit être désactivé sur le VDA pour permettre le retour vers la mise à disposition de l'audio UDP.

Amélioration apportées à l'utilitaire Storebrowse pour la continuité du service

Auparavant, les fichiers de location de connexion Workspace étaient synchronisés avec les fichiers disponibles sur le serveur distant uniquement si vous étiez connecté à l'aide de Self-Service Plug-in. Par conséquent, la fonctionnalité de continuité du service n'était pas prise en charge lorsque vous lanciez des applications ou des sessions de bureau à l'aide de Storebrowse. La plupart des fournisseurs de clients légers tiers utilisent Storebrowse pour se connecter à la plate-forme Workspace ; cependant, la fonctionnalité de continuité du service n'était pas été activée pour ces fournisseurs.

À partir de cette version, les fichiers de location de connexion Workspace sont synchronisés avec les fichiers disponibles sur le serveur distant lorsque vous vous connectez également à l'aide de Storebrowse. Cette fonctionnalité aide les fournisseurs de clients légers tiers à accéder à Workspace même en mode hors connexion.

> **Remarque :**
>
> - Cette amélioration n'est disponible que lorsque la continuité du service est activée dans les déploiements cloud. Pour plus d'informations, consultez la section Configurer la continuité du service dans la documentation de Citrix Workspace.
> - Cette amélioration n'est pas disponible si vous avez défini la valeur `AuthManLiteEnabled` sur **True** dans le fichier `$ICAROOT/config/AuthManConfig.xml`. Par défaut, cette valeur est définie sur **False**.

Global App Config Service (version Technical Preview publique)

Le nouveau Global App Config Service pour Citrix Workspace permet à un administrateur Citrix de fournir les URL du service Workspace via un service géré de manière centralisée.

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 :

```
1       <key>AppConfigEnabled</key>
```



```
      <value> true </value>
<!--NeedCopy-->
```

Pour plus d'informations sur les paramètres d'URL du service Workspace, consultez la documentation Global App Configuration Service.

> **Remarque :**
>
> L'application Citrix Workspace pour Linux utilise Global App Configuration Service uniquement pour mettre à disposition les adresses URL du service Workspace.

Découverte MTU EDT (Enlightened Data Transport)

L'application Citrix Workspace prend désormais en charge la découverte MTU (unité de transmission maximale) dans Enlightened Data Transport (EDT). Cela augmente la fiabilité et la compatibilité du protocole EDT et optimise l'expérience utilisateur.
Pour de plus amples informations, consultez la section Découverte MTU EDT dans la documentation de Citrix Virtual Apps and Desktops.

Créer de chaînes utilisateur-agent personnalisées dans une demande réseau

Dans cette version, l'application Citrix Workspace introduit une option permettant d'ajouter les chaînes agent-utilisateur dans la demande réseau et d'identifier la source d'une demande réseau. En fonction de cette demande de chaînes agent-utilisateur, vous pouvez décider comment gérer votre demande réseau. Cette fonctionnalité vous permet d'accepter les demandes réseau uniquement à partir d'appareils approuvés.

> **Remarque :**
>
> Cette fonctionnalité est prise en charge sur les déploiements cloud de l'applications Citrix Workspace. En outre, x86, x64 et armhf sont les packages pris en charge.

Pour de plus amples informations, consultez la section Créer de chaînes utilisateur-agent personnalisées dans une demande réseau.

Gestion des feature flag

Si un problème survient avec l'application Citrix Workspace en production, nous pouvons désactiver dynamiquement une fonctionnalité affectée dans l'application Citrix Workspace même après la livraison de la fonctionnalité. Pour ce faire, nous utilisons des commutateurs de fonctionnalité et un service tiers appelé LaunchDarkly. Vous n'avez pas besoin d'effectuer des configurations pour activer le trafic vers LaunchDarkly, sauf si un pare-feu ou un proxy bloque le trafic sortant. Dans ce cas, vous activez le trafic vers LaunchDarkly via des URL ou adresses IP spécifiques, en fonction des exigences de votre stratégie.

Pour de plus amples informations, consultez la section Gestion des feature flag.

Problèmes résolus

- 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]
- Lors de l'utilisation du VDA version 2106, la fonctionnalité de partage d'écran dans Microsoft Teams en mode **Optimisé** peut échouer. [HDX-34002]
- Sur Ubuntu 20.04, l'interface utilisateur en libre-service peut ne pas fonctionner comme prévu lors de l'utilisation d'un magasin cloud. [RFLNX-8155]

2108

Nouveautés de la version 2108

Protection des applications

Le composant Protection de l'application est désormais entièrement fonctionnel.

La fonction Protection des applications nécessite l'installation d'une licence complémentaire sur votre serveur de licences. Une licence Citrix Virtual Desktops doit être également présente. Pour de plus amples informations sur les licences, consultez la section **Configurer** dans la documentation de Citrix Virtual Apps and Desktops.

La fonction Protection des applications prend en charge les applications et les sessions de bureau et est activée par défaut. Toutefois, vous devez configurer la fonctionnalité dans le fichier `AuthManConfig.xml` pour l'activer dans les interfaces Authentication Manager et Self-Service Plug-in.

Avec cette version, vous pouvez lancer des ressources protégées à partir de l'application Citrix Workspace pendant que Mozilla Firefox est en cours d'exécution.

Pour plus d'informations, consultez Protection des applications.

Amélioration de la configuration audio

Auparavant, la valeur par défaut de l'attribut `VdcamVersion4Support` dans le fichier `module.ini` était définie sur **True**. Avec cette version, la valeur par défaut est définie sur **False**. Par conséquent, seul le périphérique audio par défaut portant le nom **Citrix HDX Audio** apparaît dans la session. Cette amélioration vise à minimiser les problèmes audio qui se produisent lorsque l'attribut est défini sur **True**.

Pour activer 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=True
3. Redémarrez la session pour que les modifications prennent effet.

Problèmes résolus

- Il se peut que les tentatives de copier-coller du texte depuis l'appareil d'un utilisateur vers la session échouent. [CVADHELP-16828]
- La redirection du contenu du navigateur peut échouer lorsqu'une superposition basée sur WebkitGTK+ est utilisée pour afficher le contenu. [CVADHELP-17748]
- Lorsque la fonction Protection des applications est installée, il se peut que l'interface utilisateur du bureau cesse de répondre, puis revienne à la normale après quelques secondes. [RFLNX-7729]
- Il arrive que le composant Protection des applications ne fonctionne pas comme prévu sur une nouvelle installation de l'application Citrix Workspace. [RFLNX–7858]
- Dans une session de bureau, une fois qu'une page est redirigée à l'aide de CEF-BCR, le focus du clavier peut rester sur la superposition BCR (redirection du contenu du navigateur). Le focus du clavier ne se déplace pas vers d'autres applications ouvertes. [RFLNX-7704]
- Lors d'une réunion Microsoft Teams, il arrive que le rapport d'aspect vidéo ne s'affiche pas comme prévu lorsque vous sélectionnez l'option Fill frame. [HDX-31929]
- Lors d'un appel vidéo Microsoft Teams, Desktop Viewer peut ne plus répondre. [HDX-32435]
- Les tentatives de lancement de bureau ou d'applications avec l'application Citrix Workspace peuvent échouer, et le fichier ICAClient.log affiche le message suivant :

  « En attente de préparation du gestionnaire grpc. »

  [HDX-32575]

2106

Nouveautés dans la version 2106

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

La redirection de contenu du navigateur basée sur CEF est désormais entièrement fonctionnelle. Par défaut, cette fonction est activée.

> **Remarque :**
>
> Cette fonctionnalité n'est pas prise en charge sur la plate-forme armhf.

Pour plus d'informations, consultez la section Activer la redirection du contenu du navigateur basée sur CEF.

Indicateur d'état de la batterie

L'état de la batterie de l'appareil s'affiche désormais dans la zone de notification d'une session Citrix Desktop.

> **Remarque :**
>
> L'indicateur d'état de la batterie n'apparaît pas pour les VDA du serveur.

Pour plus d'informations, consultez Indicateur d'état de la batterie.

Continuité du service (Technical Preview publique)

> **Remarque :**
>
> Cette fonctionnalité est disponible en version Technical Preview publique pour l'application 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 sessions Citrix Virtual Apps and Desktops et Citrix DaaS quel que soit l'état d'intégrité des services cloud.

Pour plus d'informations sur les exigences requises pour prendre en charge la continuité du service sur l'application Citrix Workspace, consultez Configuration système requise.

Pour plus d'informations sur l'installation de la continuité des services avec l'application Citrix Workspace, consultez Installation de la continuité du service.

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

Amélioration du composant Protection des applications (fonctionnalité expérimentale)

Auparavant, les boîtes de dialogue des interfaces Authentication Manager et **Self-Service Plug-in** n'étaient pas protégées même lorsque le composant Protection des applications était installé et activé.

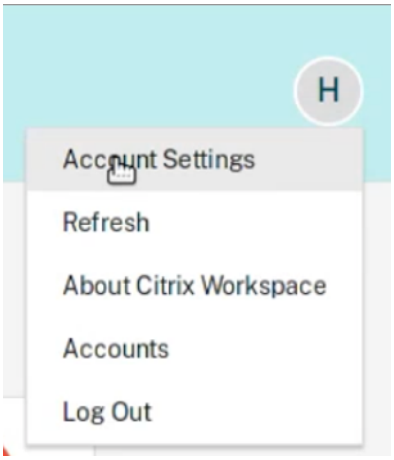
À compter de cette version, l'application Citrix Workspace introduit une option qui vous permet de configurer séparément les fonctionnalités de protection contre les programmes d'enregistrement de frappe et de capture d'écran pour les interfaces Authentication Manager et Self-Service Plug-in.

Pour plus d'informations, consultez Protection des applications.

Améliorations apportées à l'interface utilisateur

Auparavant, le menu des paramètres était disponible à partir de l'option **Préférences** de Desktop Viewer.

À partir de cette version, le menu des paramètres est conforme au Self-Service Plug-in. Les options de menu sont désormais améliorées pour s'aligner sur l'apparence de Citrix Workspace natif. Il en résulte une expérience utilisateur améliorée et plus homogène.



> **Remarque :**
>
> Cette amélioration est disponible par défaut dans l'application Citrix Workspace version 2106 dans les déploiements cloud.

Pour basculer vers l'ancienne apparence native, procédez comme suit :

Accédez à `$ICAROOT/config/AuthManConfig.xml` et définissez la valeur de `WebUISettings` sur **False**.

Améliorations apportées à Microsoft Teams

- Auparavant, lorsque vous cliquiez sur **Partage d'écran**, l'aperçu d'un moniteur principal ou par défaut était uniquement disponible pour le partage d'écran.

  Avec cette version, un aperçu de tous les écrans est affiché sur le menu de sélection d'écran. Vous pouvez sélectionner n'importe quel écran pour le partage d'écran dans l'environnement VDA. Un carré rouge apparaît sur le moniteur sélectionné et une petite image du contenu de l'écran sélectionné s'affiche dans le menu de sélection d'écran.

  En mode transparent, vous pouvez sélectionner un écran à partager parmi tous les écrans. Lorsque Desktop Viewer modifie le mode de fenêtre (agrandir, restaurer ou réduire), le partage d'écran s'arrête.

Problèmes résolus

- Lorsque vous utilisez l'application Citrix Workspace 1912 pour Linux, la redirection du presse-papiers peut échouer et entraîner le blocage de la session. Le problème se produit lorsque de grandes quantités de données sont copiées/collées. [CVADHELP-16210]
- Les appels vidéo Microsoft Teams non optimisés peuvent ne pas avoir de son. L'audio ne peut pas être récupéré tant que vous n'avez pas déconnecté et reconnecté la session. [CVADHELP-16846]
- Les tentatives de téléchargement d'un fichier hébergé sur un réseau local peuvent échouer. [CVADHELP-17337]
- Les sessions lancées sur des terminaux Linux peuvent échouer. Le problème se produit lorsque la stratégie Multi-Stream est activée. [RFLNX-6960]
- Lors de l'utilisation de GStreamer version 1.15.1, la redirection de webcam peut échouer et la session peut être déconnectée. [HDX-30550]

2104

Nouveautés dans la version 2104

Prise en charge du composant Protection des applications sur Red Hat Package Manager (RPM) (fonctionnalité expérimentale)

Le composant Protection des applications est désormais pris en charge sur la version RPM de l'application Citrix Workspace.

Pour plus d'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 des opérations suivantes :

- Connexion initiale
- Reconnexion de la fiabilité de session
- Reconnexion automatique des clients

Cette amélioration réduit le temps de connexion lorsque EDT est le mode préféré. Toutefois, le transport UDP sous-jacent requis n'est pas disponible et TCP doit être utilisé.

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

Optimisation pour 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 sessions Citrix Virtual Apps and Desktops et Citrix DaaS 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.

Problèmes résolus

- 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 poste à poste, 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 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]
- 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]

2103

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 s'affiche. 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>
3  <!--NeedCopy-->
```

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

Pour plus d'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 prenaient 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.

Problèmes résolus

- 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]
- Lors d'un appel vidéo Microsoft Teams, le voyant de la caméra peut clignoter et la vidéo d'aperçu peut s'arrêter. [CVADHELP-16383]
- 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]
- Lorsqu'une session est interrompue ou déconnectée brusquement, le processus `HdxRtcEngine.exe` peut se fermer de façon inattendue. [RFLNX-5885]

2101

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 du composant Protection des applications sur les packages Debian (fonctionnalité expérimentale)

Le composant Protection des applications est désormais pris en charge sur la version Debian de l'application Citrix Workspace.

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

```
1 export DEBIAN_FRONTEND=”noninteractive”
2 sudo debconf-set-selections <<< ”icaclient app_protection/
     install_app_protection select yes”
3 sudo debconf-show icaclient
```



```
* app_protection/install_app_protection: yes
sudo apt install -f ./icaclient_<version>._amd64.deb
<!--NeedCopy-->
```

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.

Problèmes résolus

- Lors de l'utilisation d'un proxy personnalisé, une invite d'authentification supplémentaire peut s'afficher. Le problème est causé par l'infrastructure Chromium Embedded Framework (CEF) utilisée 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 connus

Problèmes connus dans la version 2207

- L'interrogation DNS pour la collecte de données CAS peut se produire pour un lancement direct d'ICA et pour les magasins CAS désactivés. [CVADHELP-20018]
- Lorsque vous utilisez des commandes storebrowse, si vous ajoutez et énumérez un deuxième magasin, le démarrage des applications ou des bureaux à partir du premier magasin peut échouer. Pour contourner ce problème, vous devez énumérer à nouveau ce magasin spécifique avant de lancer des applications ou des bureaux. [RFLNX-8953]
- Dans une session de bureau, lorsque vous lisez une vidéo à l'aide du Lecteur Windows Media, le curseur de la souris peut disparaître sur la vidéo Rave. Ce problème se produit uniquement si vous avez défini les stratégies suivantes comme suit dans DDC :

- « Utiliser codec vidéo pour la compression » sur « Pour les zones changeant constamment »
- « Redirection Windows Media » sur « Autorisée » (paramètre par défaut)
- « Redirection du contenu du navigateur » sur « Autorisée » (paramètre par défaut)
- « InvertCursorEnabled » sur « BOTH » et les valeurs suivantes sont ajoutées dans le fichier ~/.ICAClient/wfclient.ini :
  - InvertCursorEnabled=True
  - InvertCursorRefreshRate=60
  - InvertCursorMode=1

[HDX-37259]

Problèmes connus dans la version 2205

- Lorsqu'une erreur SSL se produit sur un protocole pendant une tentative de connexion TCP et EDT/UDP, les deux connexions peuvent échouer en raison de la condition de concurrence. Cette erreur SSL peut se produire si la configuration TLS diffère entre les protocoles et que le client ne peut pas se connecter via un protocole. Pour contourner le problème, définissez l'attribut HDXoverUDP sur On ou Off dans le fichier ICA. [RFLNX-8747]
- La compression vidéo de la webcam HDX RealTime ne prend pas en charge les caméras au format vidéo MJPEG dans l'application Citrix Workspace. [HDX-40352]
- La vidéo ou une image dans l'application Citrix Workspace peut ne pas s'afficher correctement. Ce problème se produit lorsque l'application Citrix Workspace est utilisée avec le VDA version 2109 ou ultérieure. Pour contourner le problème, procédez comme suit :

  1. Connectez-vous à Citrix Studio.
  2. Modifiez les paramètres de la stratégie Utiliser codec vidéo pour la compression.
  3. Sélectionnez l'option **Pour l'écran entier** dans la liste déroulante **Valeur**. [HDX-40287]

- Lorsque vous ajoutez un magasin à l'aide de la commande `storebrowse -a` et que vous l'énumérez à l'aide de la commande `storebrowse -E`, l'énumération Storebrowse peut échouer. Ce problème se produit uniquement dans le système d'exploitation Raspberry Pi. Pour contourner le problème, procédez comme suit :

  1. Accédez à /opt/Citrix/ICAClient/config/AuthmanConfig.xml.
  2. Ajouter l'entrée suivante :

```
<StorebrowseIPCDisabled> true</StorebrowseIPCDisabled>
<!--NeedCopy-->
```

[RFLNX-8803]

- Lorsque vous ajoutez un magasin avec les paramètres par défaut, l'énumération Storebrowse peut échouer. Ce problème se produit uniquement dans le système d'exploitation Debian 32 bits. Pour contourner le problème, procédez comme suit :

  1. Accédez à /opt/Citrix/ICAClient/config/AuthmanConfig.xml.
  2. Ajouter l'entrée suivante :

```
<GnomeKeyringDisabled>true</GnomeKeyringDisabled>
<!--NeedCopy-->
```

  [RFLNX-8743]

- Il se peut que vous ne parveniez pas à installer le package Debian de l'application Citrix Workspace sur Ubuntu 22.04 LTS. La raison de cet échec est que le package `libidn11` requis pour `ICAClient` n'est pas présent sur Ubuntu 22.04 LTS. Pour contourner le problème, installez `libidn11` indépendamment sur Ubuntu 22.04 LTS avant d'installer le package Debian de l'application Citrix Workspace. [RFLNX-8839]

Problèmes connus dans la version 2203

- Lors du lancement d'une application RDP (Protocole Bureau à distance) publiée avec plusieurs moniteurs dans un terminal Ubuntu, seul un moniteur affiche le contenu même si la machine cliente possède plusieurs moniteurs. La case à cocher « Utiliser tous les moniteurs pour la session à distance » dans l'option d'affichage de l'application RDP est sélectionnée avant la connexion à un bureau distant via RDP. Le problème se produit en mode transparent et en configuration multi-moniteurs. [CVADHELP-16768]
- L'application Citrix Workspace ne transmet pas les paramètres `Clientname` et `clientaddress` à DDC lors de l'énumération des ressources. Par conséquent, `Set-BrokerAccessPolicyRule` filtré avec le nom du client ou l'adresse IP du client peut ne pas fonctionner correctement. [CVADHELP-17667]
- Lorsque vous prévisualisez une vidéo à l'aide de la webcam dans Skype, l'aperçu peut afficher un écran noir. [HDX-37860]

Problème connu dans la version 2202

- Lorsque vous lancez l'interface utilisateur en libre-service avec les paramètres par défaut, le message d'erreur suivant peut s'afficher :

  « La réponse à la demande de jeton secondaire n'est pas 200/400/404 42 »

  Ce problème se produit sur Fedora 35. Pour contourner le problème, installez `gnome-keyring` ou désactivez-le dans `authmanconfig.xml`.

Pour désactiver `gnome-keyring`, procédez comme suit :

1. Accédez à `/opt/Citrix/ICAClient/config/AuthmanConfig.xml`.
2. Ajouter l'entrée suivante :

```
1 ```
2 <GnomeKeyringDisabled>true</GnomeKeyringDisabled>
3 <!--NeedCopy--> ```
```

[RFLNX-8603]

Problèmes connus dans la version 2112

- Dans l'application Citrix Workspace 2112, vous pouvez rencontrer une utilisation élevée du processeur sur le point de terminaison lorsqu'une webcam est activée dans un appel vidéo Microsoft Teams optimisé.

Pour contourner le problème, exécutez la commande suivante dans le terminal :

```
1 mkdir -p /var/.config/citrix/hdx_rtc_engine
2
3 vim /var/.config/citrix/hdx_rtc_engine/config.json
4
5 {
6       ”UseDefaultCameraConfig”:0  }
7  `
8
9 <!--NeedCopy-->
```

[HDX-37168]

- Après avoir installé l'application Citrix Workspace avec la fonction Protection des applications activée sur le système d'exploitation utilisant `glibc 2.34`, le démarrage du système d'exploitation peut échouer lors du redémarrage du système. Pour activer la récupération après l'échec de démarrage du système d'exploitation, effectuez l'une des opérations suivantes :
  - Réinstallez le système d'exploitation. Toutefois, nous ne prenons pas en charge la fonctionnalité Protection des applications sur le système d'exploitation utilisant `glibc 2.34` ou version ultérieure.
  - Accédez au mode de **récupération** du système d'exploitation et désinstallez l'application Citrix Workspace à l'aide du terminal.

  - Démarrez via le système d'exploitation actif et supprimez le fichier `rm -rf /etc/ld.so.preload` du système d'exploitation existant.
    [RFLNX-8358]

- 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. [CVADHELP-16170]

- Lorsque vous installez l'application Citrix Workspace, ajoutez un magasin et lancez un bureau, la fenêtre de session peut ne pas s'afficher si la bibliothèque `libpcscd` n'est pas installée sur Ubuntu 16.04.
  Pour résoudre ce problème, procédez comme suit :

  1. Installez la bibliothèque `libpcscd` dans le client Linux. Par exemple, utilisez la commande `apt install libpcscd` pour installer la bibliothèque `libpcscd` sur Ubuntu 16.04.
  2. Si vous ne parvenez pas à installer la bibliothèque `libpcscd`, remplacez l'attribut `VDSCARDV2.DLL` par l'attribut `VDSCARD.DLL` pour DriverName dans le fichier de configuration `/opt/Citrix/ICAClient/config/module.ini` :

     [SmartCard]

     DriverName= VDSCARD.DLL

     [HDX-36574]

- Dans l'application Citrix Workspace, vous pouvez rencontrer des échecs intermittents lorsque vous répondez ou passez un appel Microsoft Teams. Le message d'erreur suivant s'affiche :

  « L'appel n'a pas pu être établi. »

  Pour contourner le problème, essayez de rétablir l'appel Microsoft Teams. [HDX-38819]

Problèmes connus dans la version 2111

- La session à double saut (ou double-hop) ne prend pas en charge la fonctionnalité Plug and Play du lecteur de carte à puce. [HDX-34582]

- Lorsque vous ouvrez une session sur un magasin cloud, l'écran peut s'afficher en blanc. [RFLNX□8337]

- Lorsque vous tentez 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 :

  « User-defined signal 2 »

  Le problème se produit dans la build de débogage et dans Azure VM Debian 10. [RFLNX-8336]

- Après avoir installé l'application Citrix Workspace avec la fonctionnalité Protection des applications activée sur le système d'exploitation utilisant la bibliothèque glibc 2.34 ou version ultérieure, le démarrage du système d'exploitation peut échouer lors du redémarrage du système. Pour activer la récupération après l'échec de démarrage du système d'exploitation, effectuez l'une des opérations suivantes :
  - Réinstallez le système d'exploitation. Toutefois, nous ne prenons pas en charge la fonctionnalité Protection des applications sur le système d'exploitation utilisant la bibliothèque glibc 2.34 ou version ultérieure.
  - Accédez au mode de **récupération** du système d'exploitation et désinstallez l'application Citrix Workspace à l'aide du terminal.
  - Démarrez via le système d'exploitation actif et supprimez le fichier `rm -rf /etc/ld.so.preload` du système d'exploitation existant. [RFLNX-8358]

Problèmes connus dans la version 2109

- Lorsque vous désinstallez l'application Citrix Workspace, les fichiers de cache obsolètes `$HOME/.local/share/webkitgtk` peuvent ne pas être supprimés automatiquement. Pour résoudre le problème, supprimez manuellement les fichiers de cache. [HDX 28187]
- Les tentatives de lancement de bureaux ou d'applications à l'aide de l'application Citrix Workspace peuvent échouer lorsque la stratégie Multi-Port est activée sur le DDC. [HDX-31016]
- Les tentatives de lancement d'une session à l'aide de l'authentification par carte à puce peuvent échouer. Le problème se produit avec l'application Citrix Workspace pour Linux version 2104 et ultérieure. Pour résoudre le problème, entrez manuellement les informations d'identification de la carte à puce. [CVADHELP 18402]
- Les tentatives de reconnexion à la session peuvent se produire une seule fois lors de la reconnexion automatique des clients. Par conséquent, la stratégie **Reconnexion automatique des clients** peut ne pas fonctionner comme prévu. [HDX 34114]
- Lorsque vous fermez la barre de progression du lancement d'une application, le processus wfica peut échouer. Par conséquent, l'application peut démarrer et disparaître de votre écran. [HDX-34701]

Problèmes connus dans la version 2108

- Lorsque la fonctionnalité Protection des applications est activée, il arrive que la fonctionnalité de protection contre les programmes d'enregistrement de frappe ne fonctionne pas sur l'interface Authentication Manager utilisant la bibliothèque `UIDialogLibWebKit3.so`. [RFLNX-8027]
- Si vous utilisez l'équilibrage de charge globale des serveurs (GSLB), les réponses du système de nom de domaine (DNS) peuvent ne pas être mises en cache pendant la durée de vie (TTL). Par

conséquent, l'authentification à l'aide de WebView peut échouer. [RFLNX-3673]

- Lorsque vous essayez de vous connecter à distance à une machine sur laquelle l'application Citrix Workspace avec la fonction Protection des applications est installée, le serveur x11vnc se bloque et la connexion échoue. Par conséquent, il se peut que vous ne puissiez pas vous connecter à distance à la machine via le serveur x11vnc. [RFLNX-8933]

Problèmes connus dans la version 2106

- Dans une session de bureau, une fois qu'une page est redirigée à l'aide de CEF-BCR, le focus du clavier peut rester sur la superposition BCR (par exemple, recherche YouTube). Le focus du clavier ne se déplace pas vers d'autres applications ouvertes. Le problème se produit uniquement lors des lancements de Self-Service Plugin et de StoreBrowse. Pour contourner le problème, pour déplacer le focus vers d'autres applications, cliquez sur la barre d'outils de session et sélectionnez le bouton **Accueil**. [RFLNX-7704]
- Dans une session de bureau, une fois qu'une page est redirigée à l'aide de CEF-BCR, le focus du clavier se déplace sur l'emplacement actuel de la souris. Le problème est dû à une limitation tierce du CEF open source. [RFLNX-7724]
- Lorsque vous essayez de cliquer sur la superposition BCR (par exemple, recherche YouTube) avec une autre application au premier plan, la page du navigateur n'apparaît pas au premier plan. [RFLNX-7730]
- Une fois qu'une page est redirigée à l'aide de CEF BCR, lorsque vous fermez la page Web redirigée, une erreur de segmentation est capturée dans les journaux d'erreurs. [RFLNX-7667]
- Pendant les appels audio pair à pair de Microsoft Teams, le son peut ne pas fonctionner pendant les 15 premières secondes de l'appel. Pour contourner le problème, dans le fichier `module.ini`, définissez l'attribut `VdcamVersion4Support` sur **False**. [HDX-29526]

Problème connu 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]

Problème connu 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]

Ancienne documentation

Pour les versions de produits qui ont atteint leur fin de vie, consultez la section Ancienne documentation.

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 des 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.

Configuration système requise et compatibilité

October 10, 2022

Exigences

Configuration matérielle requise

Noyau Linux :

- Version 2.6.29 ou ultérieure

Espace disque :

- Au moins 55 Mo
- 110 Mo supplémentaires si vous développez/extrayez le package d'installation sur le disque.
- Un minimum de 1 Go de RAM pour les périphériques system-on-a-chip (SoC) qui utilisent la redirection HDX MediaStream Flash.

Affichage vidéo couleur :

- Écran d'affichage vidéo 256 couleurs ou supérieur

Bibliothèques et codec

Bibliothèques :

- `glibcxx` 3.4.25 ou version ultérieure
- `glibc` 2.27 ou version ultérieure
- gtk 2.20.1 ou version ultérieure
- libcap1 ou libcap2
- `libjson-c` (pour l'instrumentation)
- X11 ou X.Org (Wayland n'est pas pris en charge)
- Assistance `udev`
- Advanced Linux Sound Architecture (ALSA) libasound2
- PulseAudio

Interface utilisateur en libre-service :

- webkit2gtk 2.16.6 ou version ultérieure
- libxml2 2.7.8
- `libxerces-c` 3.1

Bibliothèques de codecs :

- Speex
- Bibliothèques de codecs Vorbis

Configuration requise pour une distribution basée sur Red Hat Package Manager (RPM) :

- `chkconfig`

Configuration réseau requise

Protocole réseau :

- TCP/IP

Configuration requise pour H.264

Pour les appareils x86 :

- Vitesse de processeur minimale de 1,6 GHz

Pour la fonctionnalité de HDX 3D Pro :

- Vitesse de processeur minimale de 2 GHz
- Pilote graphique à accélération matérielle natif

Pour les appareils ARM :

- Une décodeur matériel H.264 est nécessaire pour la prise en charge de H.264 et de HDX 3D Pro.

Redirection Flash HDX MediaStream

Pour consulter toutes les exigences liées à la redirection HDX MediaStream pour Flash, consultez l'article du centre connaissances CTX134786.

Nous vous recommandons d'effectuer des tests avec le dernier plug-in avant de déployer une nouvelle version afin de tirer parti des dernières fonctionnalités et corrections liées à la sécurité.

Configuration requise pour l'intégration du programme CEIP (programme d'amélioration de l'expérience utilisateur)

- `zlib` 1.2.3.3
- `libtar` 1.2 ou version ultérieure
- `libjson` 7.6.1 ou version ultérieure

Configuration requise pour la compression vidéo de webcam HDX RealTime

- Caméra Web compatible Video4Linux
- `GStreamer` 0.10.25 (ou une version 0.10.x ultérieure), comprenant le package de distribution « plugins-good »

  Ou

- `GStreamer` 1.0 (ou une version 1.x ultérieure), comprenant les packages de distribution « plugins-base », « plugins-good », « plugins-bad », « plugins-ugly » et « gstreamer-libav »

Configuration requise pour la redirection HDX MediaStream Windows Media

- `GStreamer` 0.10.25 (ou une version 0.10.x ultérieure), comprenant le package de distribution « plugins-good » En général, la version 0.10.15 ou ultérieure est suffisante pour la redirection HDX MediaStream Windows Media.

Ou

- `GStreamer` 1.0 (ou une version 1.x ultérieure), comprenant les packages de distribution « plugins-base », « plugins-good », « plugins-bad », « plugins-ugly » et « gstreamer-libav »

> **Remarques :**
>
> - Si `GStreamer` n'est pas inclus dans votre distribution Linux, vous pouvez le télécharger sur la page GStreamer.
> - L'utilisation de certains codes (par exemple ceux dans « plugins-ugly ») peut nécessiter l'obtention d'une licence auprès du fabricant de la technologie en question. Contactez votre administrateur système pour obtenir de l'aide.

Configuration requise pour la redirection du contenu du navigateur

- webkit2gtk version 2.16.6
- `glibcxx` version 3.4.25 ou ultérieure

Configuration requise pour Philips SpeechMike

- Accédez au site Web de Philips pour installer les pilotes appropriés.

Exigences relatives au composant Protection des applications

La fonctionnalité Protection des applications fonctionne mieux avec les systèmes d'exploitation suivants, ainsi qu'avec Gnome Display Manager :

- Ubuntu 18.10, Ubuntu 19.04, Ubuntu 19.10 et Ubuntu 20.10 64 bits.
- Debian 9 (64 bits) et versions ultérieures
- CentOS 7.5 (64 bits) et versions ultérieures
- RHEL 7.5 (64 bits) et versions ultérieures
- ARMHF Raspbian 10 (Buster) (32 bits) et versions ultérieures

> **Remarque :**
>
> La fonction Protection des applications ne prend pas en charge les systèmes d'exploitation qui utilisent la bibliothèque `glibc` 2.34 ou une version ultérieure.

Configuration requise pour l'optimisation pour Microsoft Teams

Version minimale :

- Application Citrix Workspace 2006

Logiciel :

- GStreamer 1.0 ou version ultérieure et Cairo 2
- libc++-9.0 ou version ultérieure
- libgdk 3.22 ou version ultérieure
- OpenSSL 1.1.1d
- Distribution Linux x64

Matériel :

- CPU double cœur de 1,8 GHz minimum pouvant prendre en charge une résolution HD 720p lors d'une vidéoconférence pair à pair
- CPU double ou quadricœur avec une vitesse de base de 1.8 GHz et une vitesse Intel Turbo Boost élevée d'au moins 2.9 GHz

Amélioration de l'authentification :

- Bibliothèque Libsecret
- Bibliothèque libunwind-12

Configuration requise pour la continuité du service

Bibliothèques préinstallées obligatoires :

- libwebkit2gtk-4.0-37 version 2.30.1 ou supérieure
- Pour Ubuntu/RHEL/SUSE/Fedora/Debian, installez la dernière version de libwebkit2gtk-4.0-37 version 2.30.1 ou supérieure.
- Pour Raspberry Pi avec système d'exploitation Buster, installez libwebkit2gtk-4.0-37 version 2.30.1.
- gnome-keyring version 3.18.3 ou ultérieure
- Bibliothèque Libsecret installée

> **Remarques :**
>
> À partir de la version 1910, l'application Citrix Workspace fonctionne comme prévu uniquement 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
>
> À partir de la version 2101, l'application Citrix Workspace fonctionne comme prévu uniquement si le système d'exploitation répond à la configuration suivante :
>
> - GCC version 4.9 ou ultérieure
> - glibcxx 3.4.20 ou version ultérieure
>
> À partir de la version 2209, l'application Citrix Workspace fonctionne comme prévu uniquement si le système d'exploitation répond à la configuration suivante :

> `glibcxx` 3.4.25 ou version ultérieure

Matrice de compatibilité

L'application Citrix Workspace 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 la section Considérations 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 et versions ultérieures
  - NetScaler Gateway 10.1 et versions supérieures
  - 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 pour l'autorité de certification de l'organisation doit être installé sur l'appareil de l'utilisateur. Cette installation permet d'accéder aux ressources Citrix à l'aide de l'application Citrix Workspace.

> **Remarque :**
>
> Un avertissement de certificat non approuvé s'affiche si le certificat de la passerelle distante ne peut pas être vérifié lors de la connexion. Cette vérification peut échouer car le certificat racine n'est pas inclus dans le magasin de clés local. Si vous choisissez de continuer avec l'avertissement, les applications sont affichées mais elles risquent de ne pas se lancer. Le certificat racine doit être installé dans le magasin de certificats du client.

Certificats racines

Pour les ordinateurs appartenant à un domaine, utilisez 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, créez 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

Certificat	Autorité émettrice
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 prend en charge les certificats génériques. Toutefois, ils doivent être utilisés conformément à la stratégie de sécurité de votre organisation.

Des alternatives aux certificats génériques existent, par exemple un certificat qui contient la liste des noms de serveurs dans l'extension SAN (Subject Alternative Name) peut être pris en compte. Des autorités de certification publiques et privées émettent ce type de certificat.

Ajouter un certificat intermédiaire à 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, consultez la section Configuration de certificats intermédiaires dans la documentation de 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. Lorsque vous installez le package (généralement racine) :
   a) Copiez le ou les fichiers dans $ICAROOT/keystore/intcerts.
   b) Exécutez la commande suivante après avoir installé le package :

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

Associer une stratégie de validation des certificats de serveur

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

> **Important :**
>
> Avant d'installer l'application Citrix Workspace, 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 utilise tous les certificats fournis par le serveur (ou la passerelle). Comme dans les versions précédentes de l'application Citrix Workspace, elle vérifie que les certificats sont approuvés. Si un certificat n'est pas approuvé, 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.

Si une passerelle est configurée avec ces certificats valides, utilisez la configuration suivante pour une validation plus stricte. Cette configuration détermine exactement le certificat racine utilisé par l'application Citrix Workspace :

- Certificat de serveur exemple
- Certificat intermédiaire exemple
- Certificat racine exemple

L'application Citrix Workspace vérifie que tous ces certificats sont valides. L'application Citrix Workspace vérifie également qu'elle fait déjà confiance à « Certificat racine exemple ». Si l'application Citrix Workspace 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 le certificat DigiCert Baltimore

> Root/Baltimore CyberTrust Root est disponible.
> - Si vous configurez le certificat GTE CyberTrust Global Root sur la passerelle, les connexions à l'application Citrix Workspace 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.

Si une passerelle est configurée avec ces certificats valides, vous pouvez utiliser la configuration suivante, en omettant le certificat racine :

- Certificat de serveur exemple
- Certificat intermédiaire exemple

L'application Citrix Workspace utilise ces deux certificats. Elle recherche un certificat racine sur la machine utilisateur. Si l'application Citrix Workspace 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 a besoin, mais permet également à l'application Citrix Workspace de choisir un quelconque certificat racine valide et approuvé.

Si une passerelle est 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 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 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 certificat est utilisé lorsqu'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 a 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). Cette différence 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 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 ne peut pas trouver tous les certificats intermédiaires, la connexion échoue.

Workspacecheck

Un script, workspacecheck.sh, est 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. Ce script se trouve dans le répertoire `Utilities` du pack d'installation.

Pour exécuter le script workspacecheck.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 `./workspacecheck.sh` pour exécuter le script.

Applications et systèmes d'exploitation non pris en charge

Citrix n'offre pas de prise en charge pour les systèmes d'exploitation et les applications qui ne sont plus pris en charge par leurs fournisseurs.

Lorsque Citrix recherche des informations sur un problème signalé et tente de le résoudre, il essaye également de déterminer si le problème est directement lié à l'absence de prise en charge de l'application ou du système d'exploitation. Pour le savoir plus rapidement, Citrix peut vous demander de tenter de reproduire un problème à l'aide d'une version de l'application ou du système d'exploitation pris en charge. Si le problème semble être lié à l'absence de prise en charge de l'application ou du système d'exploitation, Citrix ne fera pas plus de recherches le concernant.

Installer, désinstaller et mettre à jour

October 10, 2022

Vous pouvez installer l'application Citrix Workspace en téléchargeant le fichier depuis la section Téléchargements du site Web Citrix.

Installation manuelle

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

Packages Debian

Installez le package `Icaclient` 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.

> **Remarque :**
>
> Pour éviter tout problème de compatibilité, assurez-vous d'installer la même version des packages `Icaclient` et `ctxusb`.

Nom du package	Contenu
Packages Debian (Ubuntu, Debian, Linux Mint etc.)	
icaclient_22.7.0.20_amd64.deb	Prise en charge du libre-service, 64 bits x86_64
icaclient_22.7.0.20_i386.deb	Prise en charge du libre-service, 32 bits x86
icaclient_22.7.0.20_armhf.deb	Prise en charge du libre-service, ARM HF
ctxusb_22.7.0.20_amd64.deb	Package USB, 64 bits x86_64
ctxusb_22.7.0.20_i386.deb	Package USB, 32 bits x86
ctxusb_22.7.0.20_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
packagename par le nom du package que vous installez.

Cette procédure utilise une ligne de commande et le gestionnaire de package natif pour Ubuntu, Debian ou 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 :**
>
> Installez le package `icaclient`.

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 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`..

> **Remarques :**
>
> - 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 le composant Protection des applications.

4. Acceptez le EULA.

Installation du composant Protection des applications sur les packages Debian

À partir de la version 2102, le composant Protection des applications est pris en charge sur la version Debian de l'application Citrix Workspace.

Pour installer de façon silencieuse le composant Protection des applications, 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 yes”`

`sudo debconf-show icaclient`

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

<!--NeedCopy-->
```

Installation de la continuité du service sur les packages Debian

À partir de la version 2106, vous pouvez installer la continuité du service sur la version Debian de l'application Citrix Workspace.

Exécutez les commandes suivantes depuis le terminal avant d'installer l'application Citrix Workspace :

```
sudo apt-get update

sudo apt-get install libwebkit2gtk-4.0-37 gnome-keyring libsecret-1-0
```


Packages Red Hat

Installez le package `ICAClient` 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.

> **Remarque :**
>
> Pour éviter tout problème de compatibilité, assurez-vous d'installer la même version des packages `Icaclient` et `ctxusb`.

Nom du package	Contenu
Packages Redhat (Redhat, SUSE, Fedora etc.)	
ICAClient-rhel-22.7.0.20-0.x86_64.rpm	Prise en charge du libre-service, Red Hat (y compris VDA Linux), 64 bits x86_64
ICAClient-rhel-22.7.0.20-0.i386.rpm	Prise en charge du libre-service, Red Hat, 32 bits x86
ICAClient-suse-22.7.0.20-0.x86_64.rpm	Prise en charge du libre-service, SUSE, 64 bits x86_64
ICAClient-suse-22.7.0.20-0.i386.rpm	Prise en charge du libre-service, SUSE, 32 bits x86
ctxusb-22.7.0.20-1.x86_64.rpm	Package USB, 64 bits x86_64
ctxusb-22.7.0.20-1.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 la page Fedora/Red Hat.

Pour plus d'informations sur son utilisation, consultez https://docs.fedoraproject.org/en-US/epel/#how_can_i_use_these_extra_packages.

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

```
`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 :**
>
> Installez le package `icaclient`.

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 .

   > **Remarques :**
   >
   > - `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 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 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://docs.fedoraproject.org/en-US/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)	
linuxx64-22.7.0.20.tar.gz	Intel 64 bits
linuxx86-22.7.0.20.tar.gz	Intel 32 bits
linuxarmhf-22.7.0.20.tar.gz	ARM HF

- 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. Vous pouvez également appuyer sur Entrée pour installer l'application Citrix Workspace à 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 d'intégrer `GStreamer` 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 ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). 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`.

> **Remarques :**
>
> - 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.
> - Lorsque vous désinstallez l'application Citrix Workspace, les fichiers de cache obsolètes `$HOME/.local/share/webkitgtk` peuvent ne pas être supprimés automatiquement. Pour résoudre le problème, supprimez manuellement les fichiers de cache.

Pour désinstaller l'application Citrix Workspace sur 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**.

Pour désinstaller l'application Citrix Workspace sur les systèmes d'exploitation Debian/Ubuntu

Exécutez la commande suivante à partir du dossier d'installation de l'application Citrix Workspace.

```
apt remove icaclient
apt autoremove
```

OU

```
apt remove icaclient
apt purge icaclient
```

Pour désinstaller l'application Citrix Workspace sur les systèmes d'exploitation Fedora/RHEL/CentOS

Exécutez la commande suivante à partir du dossier d'installation de l'application Citrix Workspace.

```
yum remove icaclient
```

Mise à jour

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

Lorsque vous démarrez l'application pour la première fois, que vous effectuez une mise à jour 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

September 13, 2022

Cet article est un document de référence destiné à vous aider à démarrer avec l'application Citrix Workspace pour Linux.

Magasin

Un **magasin** regroupe les applications et les bureaux disponibles pour un utilisateur en un seul endroit. Un utilisateur peut avoir plusieurs magasins et passer d'un magasin à l'autre selon ses besoins. Un administrateur fournit l'URL du magasin contenant des ressources et des paramètres préconfigurés. Vous pouvez accéder à ces magasins via l'application Citrix Workspace.

Types de magasins

Vous pouvez ajouter les types de magasins suivants dans l'application Citrix Workspace : Workspace, StoreFront, Citrix Gateway Store et Magasin Web personnalisé.

Workspace

Citrix Workspace est un magasin d'applications d'entreprise basé sur le cloud qui fournit un accès sécurisé et unifié aux applications, aux bureaux et au contenu (ressources) depuis n'importe où et sur n'importe quel appareil. Ces ressources peuvent être des instances Citrix DaaS, des applications de contenu, des applications locales et mobiles, des applications SaaS et Web, ainsi que des applications de navigateur. Pour plus d'informations, consultez la section Vue d'ensemble de Citrix Workspace.

StoreFront

StoreFront est un magasin d'applications d'entreprise sur site qui regroupe les applications et les bureaux des sites Citrix Virtual Apps and Desktops en un seul magasin facile à utiliser pour les utilisateurs.

Pour plus d'informations, consultez la documentation de StoreFront.

Magasin Citrix Gateway

Configurez Citrix Gateway pour permettre aux utilisateurs de se connecter depuis l'extérieur du réseau interne. Par exemple, les utilisateurs qui se connectent à partir d'Internet ou à partir d'emplacements distants.

Magasins Web personnalisés

À compter de la version 2203, cette fonctionnalité est généralement disponible pour l'application Citrix Workspace. Vous pouvez accéder au magasin Web personnalisé de votre organisation à partir de l'application Citrix Workspace.

Pour utiliser cette fonctionnalité, si Global App Configuration Service est disponible :

L'administrateur doit ajouter le domaine ou le magasin Web personnalisé à la liste des URL autorisées dans Global App Configuration Service. Après avoir ajouté le domaine ou le magasin Web personnalisé, fournissez l'URL du magasin Web personnalisé ou l'adresse e-mail sur l'écran **Ajouter un compte** de l'application Citrix Workspace. Le magasin Web personnalisé s'ouvre dans la fenêtre de l'application Workspace native.

Pour plus d'informations sur la configuration des adresses URL des magasins Web pour les utilisateurs, consultez Global App Configuration Service.

> **Remarque :**
>
> La fonctionnalité d'épinglage de la disposition de plusieurs moniteurs n'est pas prise en charge dans le magasin Web personnalisé.

Pour supprimer le magasin Web personnalisé, accédez à **Comptes** > **Ajouter ou supprimer des comptes**, sélectionnez l'URL du magasin Web personnalisé, puis cliquez sur **Supprimer**.

Avant de commencer, vous devez activer le magasin Web personnalisé dans le fichier `AuthManConfig.xml`. Pour l'activer :

1. Accédez au fichier de configuration `$ICAROOT/config/AuthManConfig.xml`.
2. Ajoutez les entrées suivantes :

```
<key>AppConfigEnabled</key>
<value>true</value>
<!--NeedCopy-->
```

Pour utiliser cette fonctionnalité, si Global App Configuration Service n'est pas disponible :

Apportez les modifications suivantes à la configuration :

1. Accédez au fichier de configuration `$ICAROOT/config/AuthManConfig.xml`.
2. Ajoutez les entrées suivantes :

```
<key>AppConfigEnabled</key>
<value>false</value>
<!--NeedCopy-->
```

3. Ajoutez la liste des URL qui doivent être prises en compte pour le magasin Web personnalisé de la manière suivante.

```
<AllowedWebStoreCache>
<value><URL1></value>
<value><URL2></value>
..
<value>....</value>
</AllowedWebStoreCache>
<!--NeedCopy-->
```


> **Remarque :**
>
> Vous pouvez uniquement utiliser les URL répertoriées dans le fichier `AuthManConfig.xml` pour le magasin Web personnalisé. Vous pouvez ajouter des adresses URL supplémentaires dans le fichier `AuthManConfig.xml` que vous souhaitez prendre en compte pour le magasin Web personnalisé.

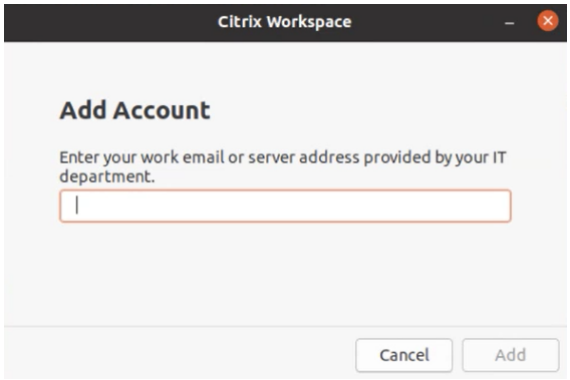
Ajouter l'URL du magasin à l'application Citrix Workspace

Vous pouvez fournir aux utilisateurs les informations de compte dont ils ont besoin pour accéder aux applications et bureaux virtuels à l'aide des éléments suivants :

- En fournissant aux utilisateurs des informations de compte à entrer manuellement
- Configuration de la découverte automatique basée sur une adresse e-mail
- Ajouter un magasin via l'interface de ligne de commande

Fournir aux utilisateurs des informations de compte à entrer manuellement

Une fois l'installation de l'application Citrix Workspace réussie, l'écran suivant s'affiche. Les utilisateurs doivent saisir une adresse e-mail ou une adresse de serveur pour accéder aux applications et aux bureaux. Lorsqu'un utilisateur entre les détails d'un nouveau compte, l'application Citrix Workspace tente de vérifier la connexion. En cas de réussite, l'application Citrix Workspace invite l'utilisateur à se connecter au compte.



Pour permettre aux utilisateurs de créer des comptes manuellement, communiquez leur les informations dont ils ont besoin pour se connecter à leurs applications et bureaux virtuels.

- Pour vous connecter à un magasin Workspace, fournissez l'URL de Workspace.
- Pour les connexions à un magasin StoreFront, indiquez l'adresse URL de ce serveur. Par exemple :`https://servername.company.com`.
- Pour qu'ils puissent se connecter via Citrix Gateway, fournissez aux utilisateurs le nom de domaine complet de Citrix Gateway.

Découverte automatique du magasin basée sur l'adresse e-mail

> **Remarque :**
>
> Cette fonctionnalité est généralement disponible pour l'application Citrix Workspace.

Vous pouvez maintenant fournir votre adresse e-mail dans l'application Citrix Workspace pour détecter automatiquement le magasin associé à l'adresse e-mail. Si plusieurs magasins sont associés à un domaine, le premier magasin renvoyé par Global App Configuration Service est ajouté par défaut comme magasin de choix. Si nécessaire, les utilisateurs peuvent toujours basculer vers un autre magasin.

Pour désactiver cette fonctionnalité, procédez comme suit :

1. Accédez au fichier `$ICAROOT/config/AuthManConfig.xml`.
2. Définissez l'entrée suivante sur false.

```
<key>AppConfigEnabled</key>
<value>false</value>
<!--NeedCopy-->
```

Ajouter un magasin via l'interface de ligne de commande

Installez l'application Citrix Workspace pour Linux en tant qu'administrateur à l'aide de l'interface de ligne de commande.

Pour plus d'informations, consultez la section Storebrowse.

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.
> - 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.

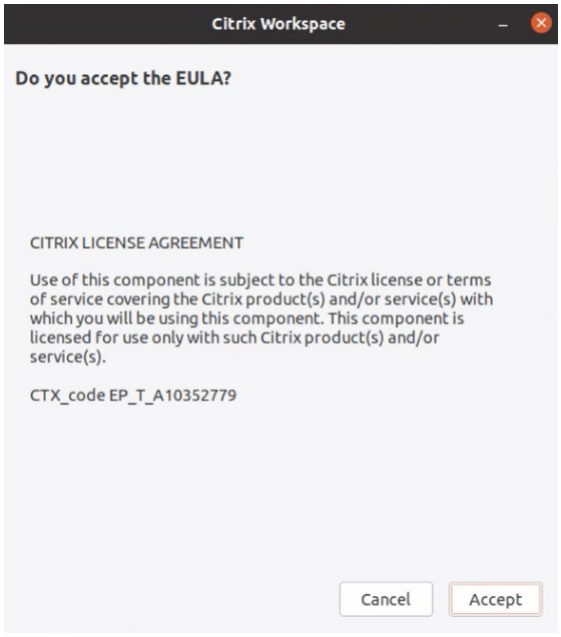
Assurez-vous que la variable d'environnement `ICAROOT` est définie de manière à pointer vers le répertoire d'installation réel.

> **Conseil :**
>
> Les instructions suivantes ne s'appliquent pas aux installations réalisées à partir des packages Web et où le tarball est utilisé. Ces instructions s'appliquent lorsque les exigences relatives au libre-service ne sont pas satisfaites.

Invite de terminal

Pour démarrer l'application Citrix Workspace à l'invite du terminal :

1. Tapez `/opt/Citrix/ICAClient/selfservice`
2. Appuyez sur Entrée (où /opt/Citrix/ICAClient est le répertoire dans lequel vous avez installé l'application Citrix Workspace).
   La boîte de dialogue **Acceptez-vous le CLUF ?** s'affiche.



3. Cliquez sur **Accepter** pour procéder à l'ajout du magasin.

> **Remarque :**
>
> **Acceptez-vous le CLUF ?** s'affiche uniquement si vous accédez à l'application Citrix Workspace pour Linux pour la première fois après l'installation.

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 les éléments suivants :

- Mode d'affichage des ordinateurs de bureau
- Connexion à différentes applications et bureaux
- Gestion de l'accès aux fichiers et aux appareils

Gérer un compte

Pour accéder aux bureaux et aux applications, vous devez disposer d'un compte auprès de Citrix Virtual Apps and Desktops ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). 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. Lorsque vous y êtes invité, authentifiez-vous auprès du serveur.

Affichage de bureau

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 utiliser plusieurs bureaux à l'aide de connexions Citrix Virtual Apps and Desktops ou Citrix DaaS 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 de **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 accède 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.

Connecter

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 ou Citrix DaaS. 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 ou Citrix DaaS. 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. L'ID est 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. À l'aide de ces modifications, 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 ».

   ```
   export 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 les sessions actives sont répertoriées.

2. Procédez comme suit :

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

Configurer

November 2, 2022

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 ne spécifiez qu'une seule valeur, cette valeur est utilisée. Le fichier `$HOME/.ICAClient/All\\_Regions.ini` peut correspondre ou réduire les valeurs possibles définies dans le fichier `$ICAROOT/config/All\\_Regions.ini`, il ne peut pas supprimer 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, considérez que le paramètre `InitialProgram` est suivi d'un signe égal (=) et qu'aucune valeur n'est fournie. Dans cet exemple, la valeur par défaut (ne pas exécuter de programme après connexion) est appliquée.

Priorité

Le fichier `All\\_Regions.ini` spécifie les paramètres qui 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 remplacent ces valeurs 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`. Toutefois, ces valeurs 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`.

Global App Config Service [version Technical Preview publique]

Le nouveau Global App Config Service pour Citrix Workspace permet à un administrateur Citrix de fournir les URL du service Workspace via un service géré de manière centralisée.

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 :

```
1       <key>AppConfigEnabled</key>
2       <value> true </value>
3  <!--NeedCopy-->
```

Pour plus d'informations sur les paramètres d'URL du service Workspace, consultez la documentation Global App Configuration Service.

> **Remarque :**
>
> L'application Citrix Workspace pour Linux utilise Global App Configuration Service uniquement

> pour mettre à disposition les adresses URL du service Workspace.

Workspace Intelligence (version Technical Preview)

La version 2111 de l'application Citrix Workspace est optimisée pour profiter des fonctionnalités Workspace Intelligence au moment de leur publication. Pour plus d'informations, consultez Fonctionnalités de Workspace Intelligence - Micro-apps.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

Prise en charge de la correspondance DPI [Tech Preview]

À partir de la version 2207, les valeurs de résolution d'affichage et d'échelle DPI définies dans l'application Citrix Workspace correspondent aux valeurs de la session des applications et des bureaux virtuels. Vous pouvez définir la valeur d'échelle requise dans le client Linux, et la mise à l'échelle de la session VDA est mise à jour automatiquement.

La mise à l'échelle DPI est principalement utilisée avec les écrans de grande taille et à haute résolution. Cette fonctionnalité permet d'afficher les éléments suivants dans une taille qui peut être visualisée confortablement :

- Applications
- Texte
- Images
- Autres éléments graphiques

Cette fonction est désactivée par défaut. Pour activer cette fonctionnalité, procédez comme suit :

1. Accédez au fichier de configuration $HOME/.ICAClient/wfclient.ini.
2. Accédez à la section [WFClient] et définissez l'entrée suivante :

   DPIMatchingEnabled=TRUE

Limitation :

Actuellement, la fonction de correspondance DPI ne prend pas en charge la mise à l'échelle fractionnelle côté client.

Si la valeur d'échelle DPI est élevée, l'optimisation Microsoft Teams peut ne pas être prise en charge comme prévu.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

Connexion permanente [version Technical Preview]

La fonction de connexion permanente vous permet de rester connecté pendant la durée (2 à 365 jours) configurée par votre administrateur. Lorsque cette fonctionnalité est activée, vous n'avez pas besoin de fournir les informations d'identification de connexion pour l'application Citrix Workspace pendant la période configurée.

Grâce à cette fonctionnalité, les sessions SSO vers Citrix DaaS sont étendues jusqu'à une période de 365 jours. Cette extension est basée sur la durée de vie des jetons de longue durée. Vos informations d'identification sont mises en cache par défaut pendant 4 jours ou pendant la durée de vie du jeton selon la valeur la plus faible, puis étendues lorsque vous devenez actif pendant ces 4 jours (en vous connectant à l'application Citrix Workspace).

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

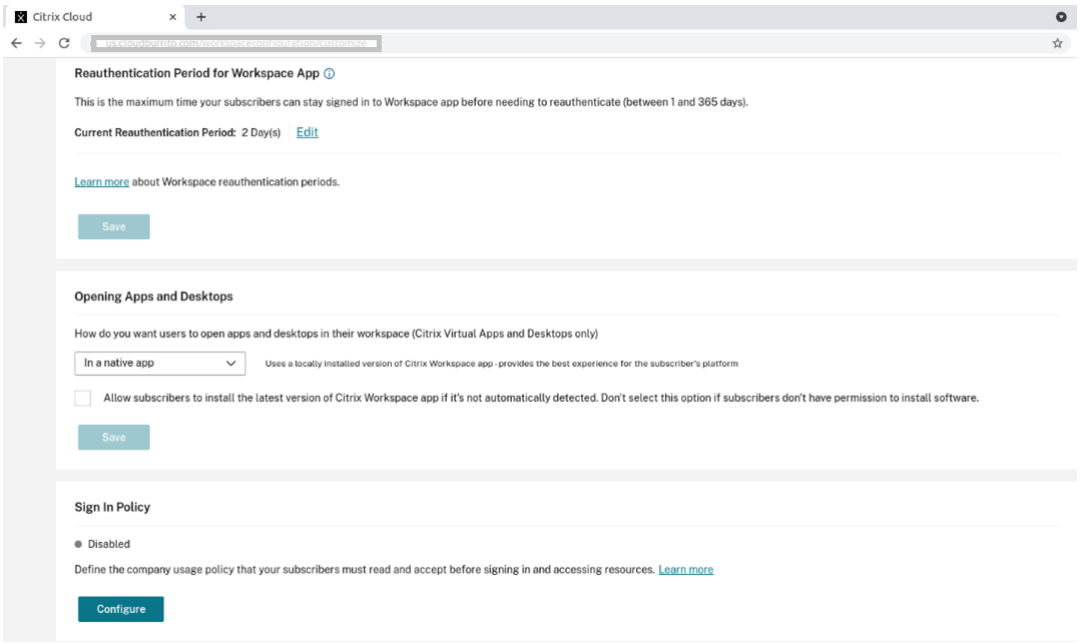
Configuration de la fonctionnalité de connexion permanente

Un administrateur doit configurer la connexion permanente sur l'environnement Workspace à l'aide de la procédure suivante :

1. Connectez-vous à Citrix Cloud.
2. Dans la console Citrix Cloud, cliquez sur le menu dans le coin supérieur gauche de l'écran.
3. Sélectionnez l'option **Configuration de l'espace de travail** > **Personnaliser** > **Préférences**.
4. Faites défiler la page jusqu'à **Période de réauthentification de l'application Workspace**.

5. Cliquez sur **Modifier** en regard du champ **Période de réauthentification actuelle**.
6. Entrez les jours requis dans le champ **Période de réauthentification actuelle**.
7. Vous devez saisir deux jours ou plus dans le champ **Période de réauthentification actuelle**.

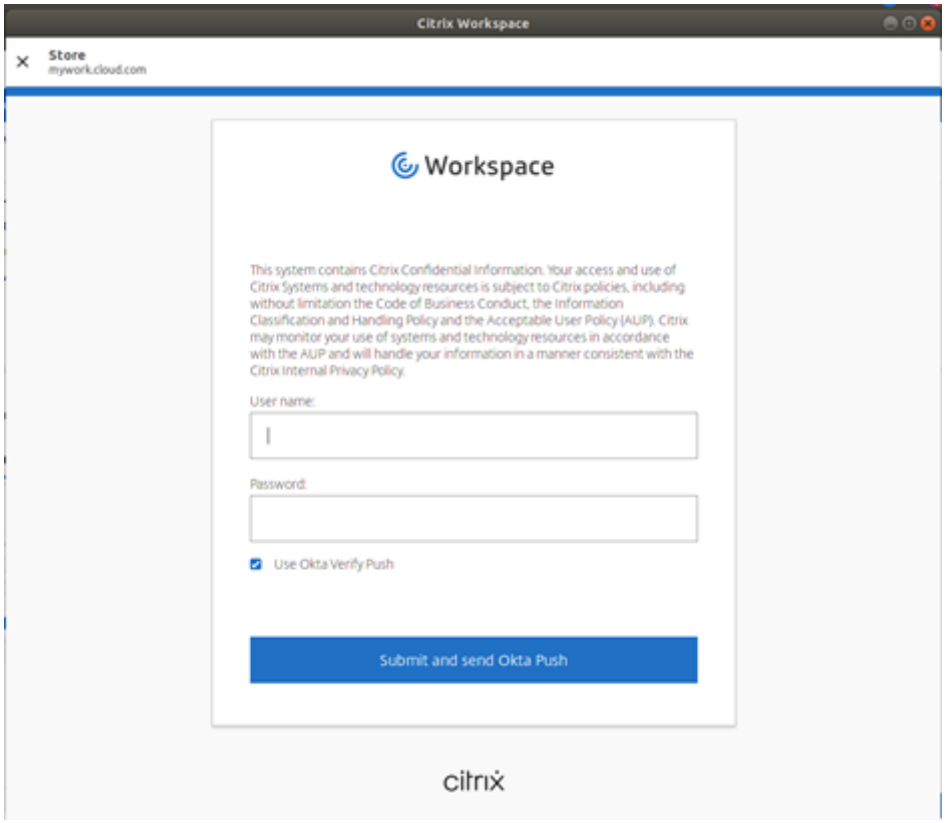
Pour plus d'informations, consultez les instructions de la section **Période de réauthentification de l'application Workspace** dans l'image suivante :



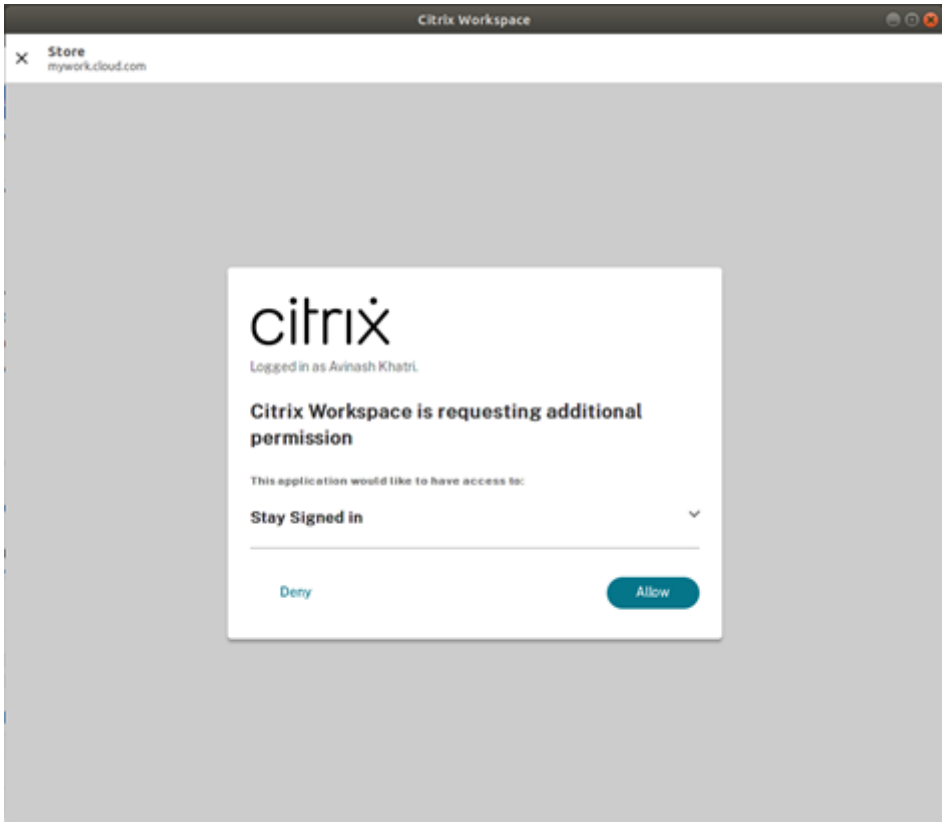
Expérience avec l'authentification améliorée

La fenêtre de connexion permanente est intégrée à la fenêtre libre-service.

1. Accédez à l'application Citrix Workspace.
   La fenêtre d'authentification apparaît.



2. Connectez-vous à l'aide de vos informations d'identification.
   Vous êtes redirigé vers l'invite d'autorisation pour accepter.



3. Cliquez sur **Autoriser**.

> **Remarque :**
>
> Si vous sélectionnez **Refuser** sur l'écran de consentement, une deuxième invite de connexion s'affiche et vous devez vous connecter à l'application Citrix Workspace toutes les 24 heures.

Désactiver la fonction de connexion permanente

Un administrateur peut désactiver la fonctionnalité de connexion persistante dans l'interface utilisateur Citrix Cloud ou dans le fichier `AuthManConfig.xml`. Toutefois, la valeur définie dans le fichier `AuthManConfig.xml` remplace la valeur définie dans l'interface utilisateur Citrix Cloud.

Utilisation de l'interface utilisateur Citrix Cloud

1. Connectez-vous à Citrix Cloud.
2. Dans la console Citrix Cloud, cliquez sur le menu dans le coin supérieur gauche de l'écran.
3. Sélectionnez l'option **Configuration de l'espace de travail** > **Personnaliser** > **Préférences**.
4. Faites défiler la page jusqu'à **Période de réauthentification de l'application Workspace**.
5. Cliquez sur **Modifier** en regard du champ **Période de réauthentification actuelle**.
6. Entrez un jour dans le champ **Période de réauthentification actuelle**.

Utilisation du fichier AuthManConfig.xml

Pour désactiver la fonctionnalité de connexion persistante, procédez comme suit :

1. Accédez au fichier <ICAROOT>/config/AuthManConfig.xml.
2. Définissez les valeurs comme suit :

```
<!-- AuthManLiteEnabled - enable AML - true/false -->

<key>AuthManLiteEnabled</key>

<value>true</value>

<AuthManLite>

<primaryTokenLifeTime>1.00:00:00</primaryTokenLifeTime>

<secondaryTokenLifeTime>0.01:00:00</secondaryTokenLifeTime>

<longLivedTokenSupport>false</longLivedTokenSupport>

<nativeLoggingEnabled>true</nativeLoggingEnabled>

<platform>linux</platform>

<saveTokens>true</saveTokens>

</AuthManLite>
<!--NeedCopy-->
```

Créer de chaînes utilisateur-agent personnalisées dans une demande réseau

À partir de la version 2109, l'application Citrix Workspace introduit une option permettant d'ajouter les chaînes agent-utilisateur dans la demande réseau et d'identifier la source d'une demande réseau. En fonction de cette demande de chaînes agent-utilisateur, vous pouvez décider comment gérer votre demande réseau. Cette fonctionnalité vous permet d'accepter les demandes réseau uniquement à partir d'appareils approuvés.

> **Remarque :**
>
> - Cette fonctionnalité est prise en charge sur les déploiements cloud de l'applications Citrix Workspace. En outre, x86, x64 et ARMHF sont les packages pris en charge.

Pour personnaliser les chaînes agent-utilisateur, procédez comme suit :

1. Recherchez le fichier de configuration `$ICAROOT/config/AuthManConfig.xml`.
2. Ajoutez une valeur à l'entrée suivante :

```
<UserAgentSuffix> </UserAgentSuffix>
```

Exemple qui inclut les éléments App et Version dans le texte personnalisé :

```
<UserAgentSuffix>App/AppVersion </UserAgentSuffix>
```

Si vous ajoutez les éléments App et AppVersion, séparez-les par une barre oblique (“/”).

- Si la demande réseau est effectuée à partir de l'application Citrix Workspace basée sur l'interface utilisateur, la chaîne agent-utilisateur suivante s'affiche dans les demandes réseau :

  ```
  CWAWEBVIEW/CWAVersion App/AppVersion
  ```

- Si la demande réseau n'est pas effectuée à partir de l'application Citrix Workspace basée sur l'interface utilisateur, la chaîne agent-utilisateur suivante s'affiche dans les demandes réseau :

  ```
  CWA/CWAVersion App/AppVersion
  ```

> **Remarques :**
>
> - Si vous n'ajoutez pas l'élément AppVersion à la fin de la chaîne UserAgentSuffix, la version de l'application Citrix Workspace est ajoutée aux demandes réseau.
> - Redémarrez `AuthManagerDaemon` et `ServiceRecord` pour que les modifications prennent effet.

Gestion des feature flag

Si un problème survient avec l'application Citrix Workspace en production, nous pouvons désactiver dynamiquement une fonctionnalité affectée dans l'application Citrix Workspace même après la livraison de la fonctionnalité. Pour ce faire, nous utilisons des commutateurs de fonctionnalité et un service tiers appelé LaunchDarkly.

Vous n'avez pas besoin d'effectuer des configurations pour activer le trafic vers LaunchDarkly, sauf si un pare-feu ou un proxy bloque le trafic sortant. Dans ce cas, vous activez le trafic vers LaunchDarkly via des URL ou adresses IP spécifiques, en fonction des exigences de votre stratégie.
Vous pouvez activer le trafic et la communication vers LaunchDarkly des manières suivantes :

Activer le trafic vers les URL suivantes

- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- firehose.launchdarkly.com
- mobile.launchdarkly.com

- app.launchdarkly.com

Répertorier les adresses IP dans une liste verte

Si vous devez répertorier les adresses IP dans la liste verte, consultez la liste des adresses IP publiques de LaunchDarkly pour obtenir une liste de toutes les plages d'adresses IP actuelles. Vous pouvez utiliser cette liste pour vérifier que les configurations du pare-feu sont mises à jour automatiquement en fonction des mises à jour de l'infrastructure. Pour plus d'informations sur l'état des modifications de l'infrastructure, consultez la page LaunchDarkly Status.

Configuration système requise pour LaunchDarkly

Vérifiez que les applications publiées peuvent communiquer avec les services suivants si le split tunneling sur Citrix ADC est désactivé :

- Service LaunchDarkly
- Service d'écoute APNs

Disposition pour désactiver le service LaunchDarkly

À partir de la version 2205, vous pouvez désactiver le service LaunchDarkly sur l'application Citrix Workspace.

Pour désactiver le service LaunchDarkly, procédez comme suit :

1. Accédez à la section LaunchDarkly dans le dossier `<ICAROOT>/config/module.ini`.
2. Sélectionnez l'entrée `EnableLaunchDarkly` et définissez-la sur *Désactiver*.

Continuité du service

> **Remarque :**
>
> Cette fonctionnalité est généralement disponible pour l'application 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 sessions Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) quel que soit l'état d'intégrité des services cloud.

Pour plus d'informations sur les exigences requises pour prendre en charge la continuité du service sur l'application Citrix Workspace, consultez Configuration système requise.

Pour plus d'informations sur l'installation de la continuité des services avec l'application Citrix Workspace, consultez Installation de la continuité du service.

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

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 s'affiche. L'épinglage permet de relancer une session avec la disposition sélectionnée, ce qui permet d'optimiser l'expérience utilisateur.

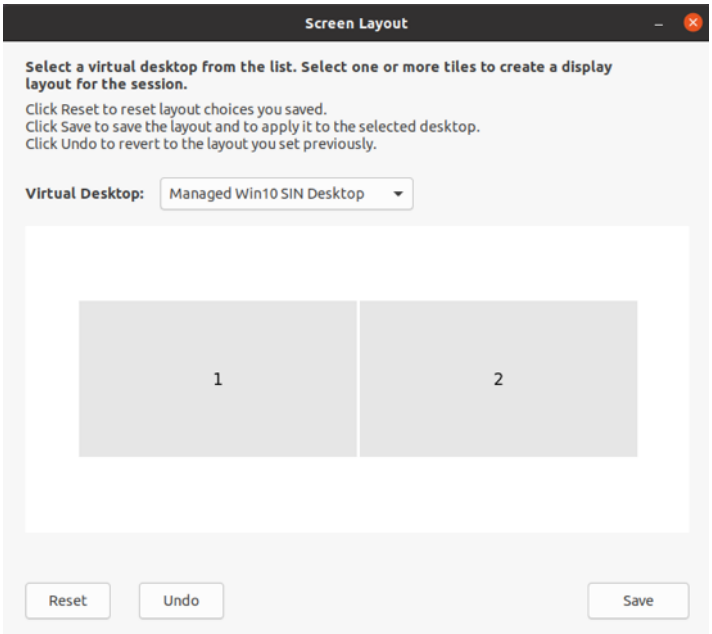
En tant que condition préalable, vous devez activer cette fonctionnalité dans le fichier `AuthManConfig.xml`. Accédez à `$ICAROOT/config/AuthManConfig.xml` et ajoutez les entrées suivantes :

```
1       <key>ScreenPinEnabled</key>
2       <value> true </value>
3  <!--NeedCopy-->
```

Ce n'est qu'après avoir ajouté la clé précédente que vous pouvez voir l'option **Disposition de l'écran** dans l'icône de **l'indicateur d'application**. Pour plus d'informations sur l'icône de l'indicateur d'application, consultez la section Icône de l'indicateur d'application.

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.

Catégories d'applications

Les catégories d'applications permettent aux utilisateurs de gérer des collections d'applications dans l'application Citrix Workspace. Vous pouvez créer des groupes d'applications pour ce qui suit :

- Applications partagées entre différents groupes de mise à disposition
- Applications utilisées par un sous-ensemble d'utilisateurs dans des groupes de mise à disposition

Pour de plus amples informations, consultez Créer un groupe d'applications dans la documentation de Citrix Virtual Apps and Desktops.

Protection des applications

> **Clause d'exclusion de responsabilité :**
>
> Les stratégies Protection des applications fonctionnent en filtrant l'accès aux fonctions requises du système d'exploitation sous-jacent. Les appels d'API spécifiques sont nécessaires pour capturer des écrans ou des frappes de clavier. L'utilisation de cette fonctionnalité signifie que les stratégies Protection des applications peuvent fournir une protection même contre les outils de piratage personnalisés et spécifiques. Cependant, à mesure que les systèmes d'exploitation évoluent, de nouveaux programmes d'enregistrement de frappe et de capture d'écran peuvent émerger. Bien que nous continuions à les identifier et à les traiter, nous ne pouvons pas garantir une protection complète dans des configurations et des déploiements spécifiques.

Le composant Protection des applications est une fonctionnalité complémentaire qui offre une sécurité renforcée lors de l'utilisation de Citrix Virtual Apps and Desktops. Cette fonctionnalité limite le risque d'être infecté par des programmes malveillants d'enregistrement de frappe et de capture d'écran. La fonction 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.

> **Remarques :**
>
> - Cette fonctionnalité est prise en charge lorsque l'application Citrix Workspace est installée à l'aide des paquets Tarball, Debian et Red Hat Package Manager (RPM). De plus, x64 et ARMHF sont les seules architectures prises en charge.
> - Cette fonctionnalité est prise en charge sur les déploiements locaux de Citrix Virtual Apps and Desktops, ainsi que dans les déploiements utilisant Citrix Virtual Apps and Desktops Service avec StoreFront.

La fonction Protection des applications nécessite l'installation d'une licence complémentaire sur votre serveur de licences. Une licence Citrix Virtual Desktops doit être également présente. Pour de plus amples informations sur les licences, consultez la section relative à la **configuration** dans Citrix Virtual Apps and Desktops.

Depuis la version 2108, la fonction Protection des applications est entièrement fonctionnelle. La fonction Protection des applications prend en charge les applications et les sessions de bureau et est activée par défaut. Toutefois, vous devez configurer la fonctionnalité Protection des applications dans le fichier `AuthManConfig.xml` pour l'activer dans les interfaces Authentication Manager et Self-Service Plug-in.

Avec cette version, vous pouvez lancer des ressources protégées à partir de l'application Citrix Workspace pendant que Mozilla Firefox est en cours d'exécution.

À partir de la version 2012, la fonctionnalité Protection des applications est une fonctionnalité expérimentale.

Conditions préalables :

La fonctionnalité Protection des applications fonctionne mieux avec les systèmes d'exploitation suivants, ainsi qu'avec Gnome Display Manager :

- Ubuntu 18.10, Ubuntu 19.04, Ubuntu 19.10 et Ubuntu 20.10 64 bits.
- Debian 9 (64 bits) et versions ultérieures
- CentOS 7.5 (64 bits) et versions ultérieures
- RHEL 7.5 (64 bits) et versions ultérieures
- ARMHF Raspbian 10 (Buster) (32 bits) et versions ultérieures

> **Remarque :**
>
> La fonction Protection des applications ne prend pas en charge les systèmes d'exploitation qui utilisent la bibliothèque `glibc` 2.34 ou une version ultérieure.
>
> Si vous installez l'application Citrix Workspace avec la fonctionnalité Protection des applications activée sur le système d'exploitation utilisant la bibliothèque `glibc` 2.34 ou version ultérieure, le démarrage du système d'exploitation peut échouer lors du redémarrage du système. Pour activer la récupération après l'échec de démarrage du système d'exploitation, effectuez l'une des opérations suivantes :
>
> - Réinstallez le système d'exploitation. Toutefois, nous ne prenons pas en charge la fonctionnalité Protection des applications sur le système d'exploitation utilisant `glibc` 2.34 ou version ultérieure.
> - Accédez au mode de restauration du système d'exploitation et désinstallez l'application Citrix Workspace à l'aide du terminal.
> - Démarrez via le système d'exploitation actif et supprimez le fichier `rm -rf /etc/ld.so.preload` du système d'exploitation existant.

Installer le composant 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 Protection des applications ? Avertissement : vous ne pouvez pas désactiver cette fonctionnalité. Pour désactiver cette fonctionnalité, vous devez désinstaller l'application Citrix Workspace. Pour plus d'informations, contactez votre administrateur système. [default $INSTALLER_N]:"

Entrez **Y** pour installer le composant Protection des applications.

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

Redémarrez votre machine pour que les modifications prennent effet. Le composant Protection des applications fonctionne comme prévu uniquement après le redémarrage de votre machine.

Installation du composant Protection des applications sur les packages RPM :

À partir de la version 2104, le composant Protection des applications est pris en charge sur la version RPM de l'application Citrix Workspace.

Pour installer le composant Protection des applications, procédez comme suit :

1. Installez l'application Citrix Workspace.
2. Installez le package 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 Protection des applications sur les packages Debian :

À partir de la version 2101, le composant Protection des applications est pris en charge sur la version Debian de l'application Citrix Workspace.

Pour installer de façon silencieuse le composant Protection des applications, 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 yes”

sudo debconf-show icaclient
* app_protection/install_app_protection: yes

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

À compter de la version 2106, l'application Citrix Workspace introduit une option qui permet de configurer séparément les fonctionnalités de protection contre les programmes d'enregistrement de frappe et de capture d'écran pour les interfaces Authentication Manager et Self-Service Plug-in.

Configuration de la fonction Protection des applications pour Authentication Manager :

Accédez au fichier `$ICAROOT/config/AuthManConfig.xml` et modifiez-le comme suit :

```
/opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
    authmananti -A 1
     <key>AuthManAntiScreenCaptureEnabled</key>
     <value>true</value>
     <key>AuthManAntiKeyLoggingEnabled</key>
     <value>true </value>

<!--NeedCopy-->
```


Configuration de la fonction Protection des applications pour l'interface de Self-Service Plug-in :

Accédez au fichier `$ICAROOT/config/AuthManConfig.xml` et modifiez-le comme suit :

```
/opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
   protection -A 4
<!-- Selfservice App Protection configuration -->
    <Selfservice>
      <AntiScreenCaptureEnabled>true</AntiScreenCaptureEnabled>
      <AntiKeyLoggingEnabled>true</AntiKeyLoggingEnabled>
    </Selfservice>

<!--NeedCopy-->
```

Problèmes connus :

- Lorsque vous réduisez un écran protégé, le composant Protection des applications continue de s'exécuter en arrière-plan.

Limitation :

- Il se peut que vous ne parveniez pas à lancer de ressources protégées lorsqu'une application installée à partir du Snap Store est en cours d'exécution. Pour contourner le problème, identifiez l'application à l'origine du problème à partir du fichier journal de l'application Citrix Workspace. Fermez également l'application.
- Lorsque vous essayez de prendre une capture d'écran d'une fenêtre protégée, l'écran entier, y compris les applications non protégées en arrière-plan, est grisé.

Indicateur d'état de la batterie

L'état de la batterie de l'appareil s'affiche désormais dans la zone de notification d'une session Citrix Desktop.

> **Remarque :**
>
> À partir de la version 2111, l'indicateur d'état de la batterie s'affiche également pour les VDA de serveur.

L'indicateur d'état de la batterie est activé par défaut.

Pour désactiver l'indicateur d'état de la batterie :

1. Naviguez jusqu'au dossier `<ICAROOT>/config/module.ini`.
2. Accédez à la section `ICA 3.0`.
3. Définissez le `MobileReceiver= Off`.

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

Données collectées	Description	Comment elles sont utilisées
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 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. Vous pouvez vous informer sur la manière dont Google gère les données collectées pour Google Analytics.

Désactivez l'envoi des données CEIP pour Citrix et Google Analytics. Pour cette activité, il existe une exception avec les données collectées pour Google Analytics indiquées par * dans le deuxième tableau de la section suivante. Procédez comme suit pour annuler l'envoi des données CEIP pour Citrix et Google Analytics :

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 :**
>
> Après avoir défini la clé `EnableCeip` sur `Disable`, vous pouvez désactiver l'envoi des deux derniers éléments de données CEIP collectés par Google Analytics. Ces données sont la version du système d'exploitation et la version de l'application Workspace. Pour ce faire, accédez à la section suivante et définissez la valeur comme suit :

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

Section : `GoogleAnalytics`

Entrée : `DisableHeartBeat`

Valeur : True

> **Remarque :**
>
> Aucune donnée n'est collectée pour les utilisateurs de l'Union européenne (UE), de l'Espace économique européen (EEE), de la Suisse et du Royaume-Uni (UK).

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	Langue de l'application Workspace
Méthode de lancement de session	Version du compilateur	Plate-forme matérielle	Configuration du magasin
État du lancement de sessions Citrix Virtual Apps and Desktops	Configuration de l'authentification	Protocole de connexion	Utilisation de la fonctionnalité Redirection du contenu du navigateur
Détails de la location de connexion	Configuration de la fonction Protection des applications		

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.

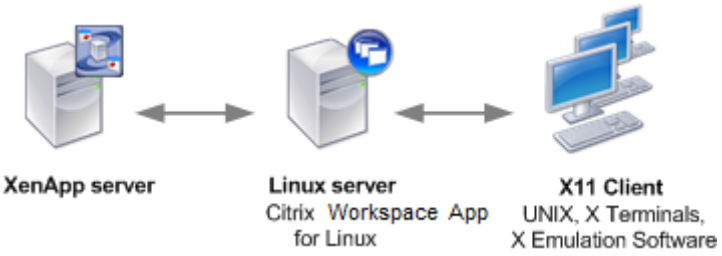
ICA vers proxy X

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 des copies supplémentaires de l'application Citrix Workspace simultanément sur un seul système. Dans ce cas, chaque application Citrix Workspace envoie sa sortie à un appareil différent.

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. Ce serveur peut être 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 prise en charge 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. Vérifiez si l'application Citrix Workspace est installée dans le répertoire d'installation par défaut. Si elle n'est pas installée, vérifiez 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).

L'URL est ouverte à l'aide de l'application serveur dans les cas suivants :

- L'application Citrix Workspace ne possède pas d'application appropriée.
- L'application Citrix Workspace ne peut pas accéder directement au contenu.

La redirection de contenu serveur-client est configurée sur le serveur. Cette fonctionnalité est activée par défaut dans l'application Citrix Workspace si le chemin d'accès inclut les éléments suivants :

- RealPlayer
- 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

   Le chemin d'accès est le répertoire dans lequel se trouve l'exécutable du navigateur. 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

   Ce paramètre entraîne les effets suivants :

   - L'utilitaire `nslaunch` est exécuté pour transférer l'adresse URL dans une fenêtre de navigateur existante.
   - Chaque navigateur de la liste est testé à tour de rôle, jusqu'à ce que le contenu soit affiché.
3. Dans la section [Player], modifiez les paramètres suivants :

   Path=path

Command=command

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

4. 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. Vous pouvez également spécifier des noms de répertoires supplémentaires 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. Changez le paramètre de `CREnabled` à `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. Cette fonctionnalité n'est activée que 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. Cette configuration requiert des ressources processeur supplémentaires pour compresser et décompresser les données, mais permet d'améliorer les per-

formances 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 ou Citrix DaaS, 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.

Pour plus d'informations sur le dépannage, voir Connexions dans la section Dépannage.

Police

Lissage des polices ClearType

Le lissage de polices ClearType améliore la qualité des polices affichées au-delà de celle disponible au moyen des techniques traditionnelles de lissage de polices ou d'anticrénelage. Le lissage de polices ClearType est également appelé rendu de police subpixellaire. Vous pouvez activer ou désactiver cette fonctionnalité.

Vous pouvez également spécifier le type de lissage en procédant comme suit :

1. Accédez à la section [WFClient] du fichier de configuration approprié.
2. Modifiez le paramètre suivant :

   FontSmoothingType = nombre

   Où le 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 **FontSmoothingTypePre**.
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`. Cette valeur 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 de spécifier les emplacements des dossiers spéciaux d'un utilisateur. Par conséquent, ces dossiers restent fixes sur différents types de serveurs et configurations de batterie 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 :

Activez la redirection de dossiers spéciaux en créant une entrée dans le fichier module.ini et spécifiez les emplacements des dossiers comme suit :

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

   [ClientDrive]

   SFRAllowed = True

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 and Desktops et Citrix DaaS 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 des lecteurs clients permet de monter n'importe quel répertoire sur la machine utilisateur locale. La machine utilisateur locale comprend un CD-ROM, un DVD ou une clé USB, disponibles pour l'utilisateur pendant une session. En outre, l'utilisateur local est autorisé à accéder à la machine utilisateur locale. Lorsqu'un serveur est configuré pour autoriser le mappage des lecteurs clients :

- les utilisateurs peuvent accéder à leurs fichiers stockés localement ;
- ils peuvent utiliser les fichiers pendant leur session ;
- ils peuvent ensuite 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 et Citrix DaaS. Cette fonctionnalité 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, vérifiez 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. Ce modèle est applicable

> à la fois à Citrix Virtual Apps and Desktops et Citrix DaaS. 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 un lecteur spécifié sur le serveur à l'ouverture de session. Ce type de mappage peut être utilisé, par exemple, pour mapper tout ou partie d'un répertoire de base utilisateur ou /tmp, ainsi que les points de montage de périphériques de stockage de masse tels que des CD-ROM, DVD ou clés USB.
- Mappage de lecteur client dynamique : cette méthode contrôle les répertoires dans lesquels les périphériques de stockage de masse 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 and Desktops ou Citrix DaaS, 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.

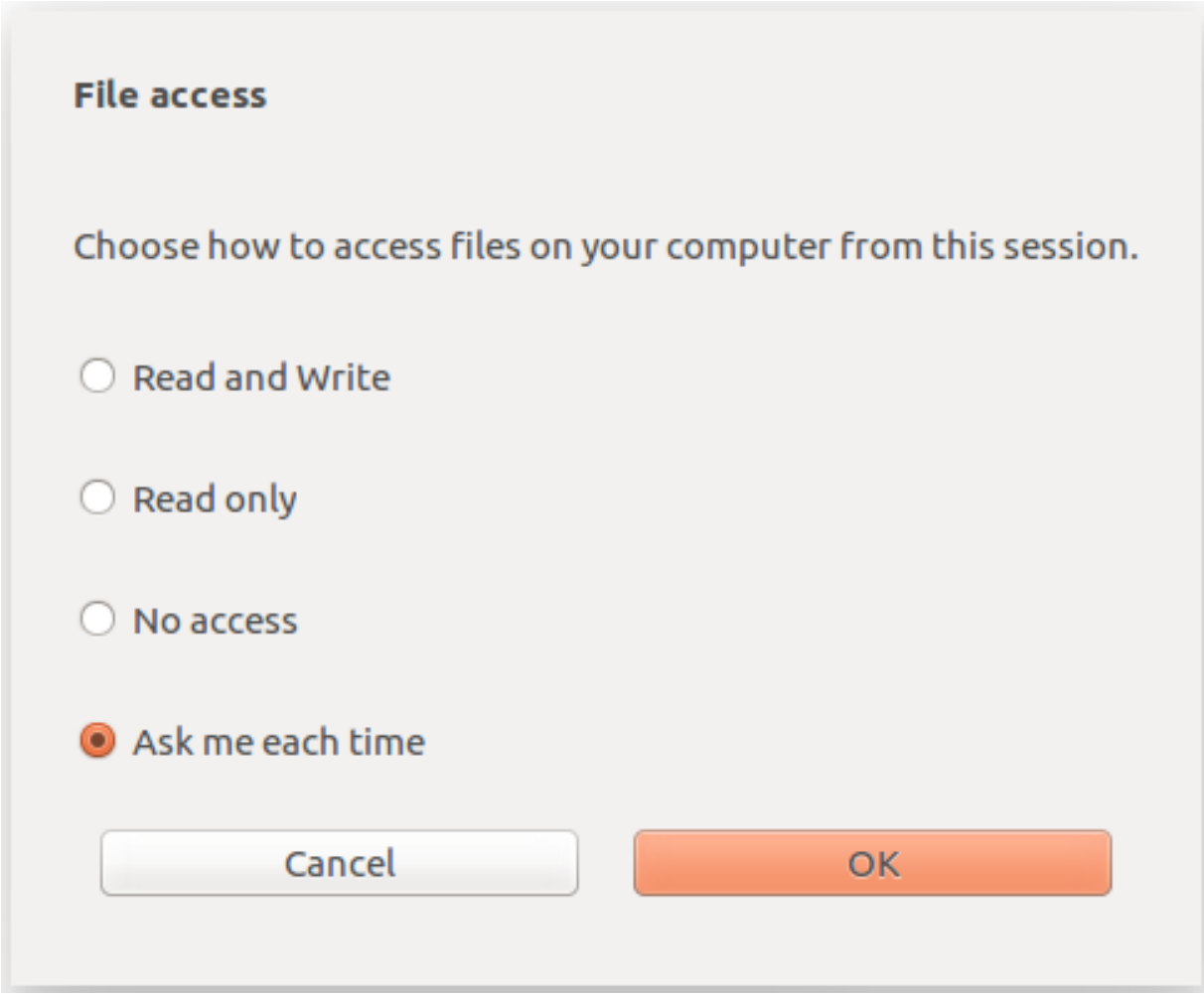
Les utilisateurs peuvent mapper les lecteurs à l'aide de la boîte de dialogue **Préférences**.

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

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

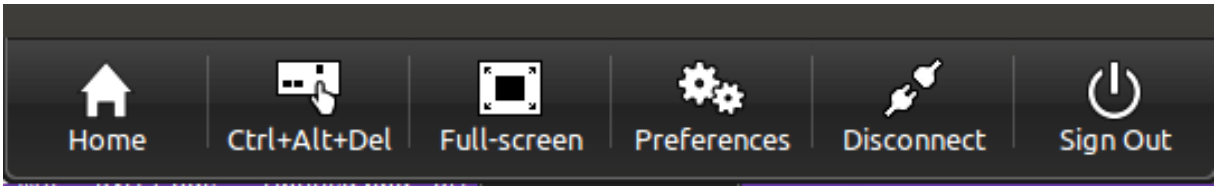
À partir de la version 2012, l'application Citrix Workspace vous permet de configurer l'accès aux fichiers CDM par magasin.

> **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).

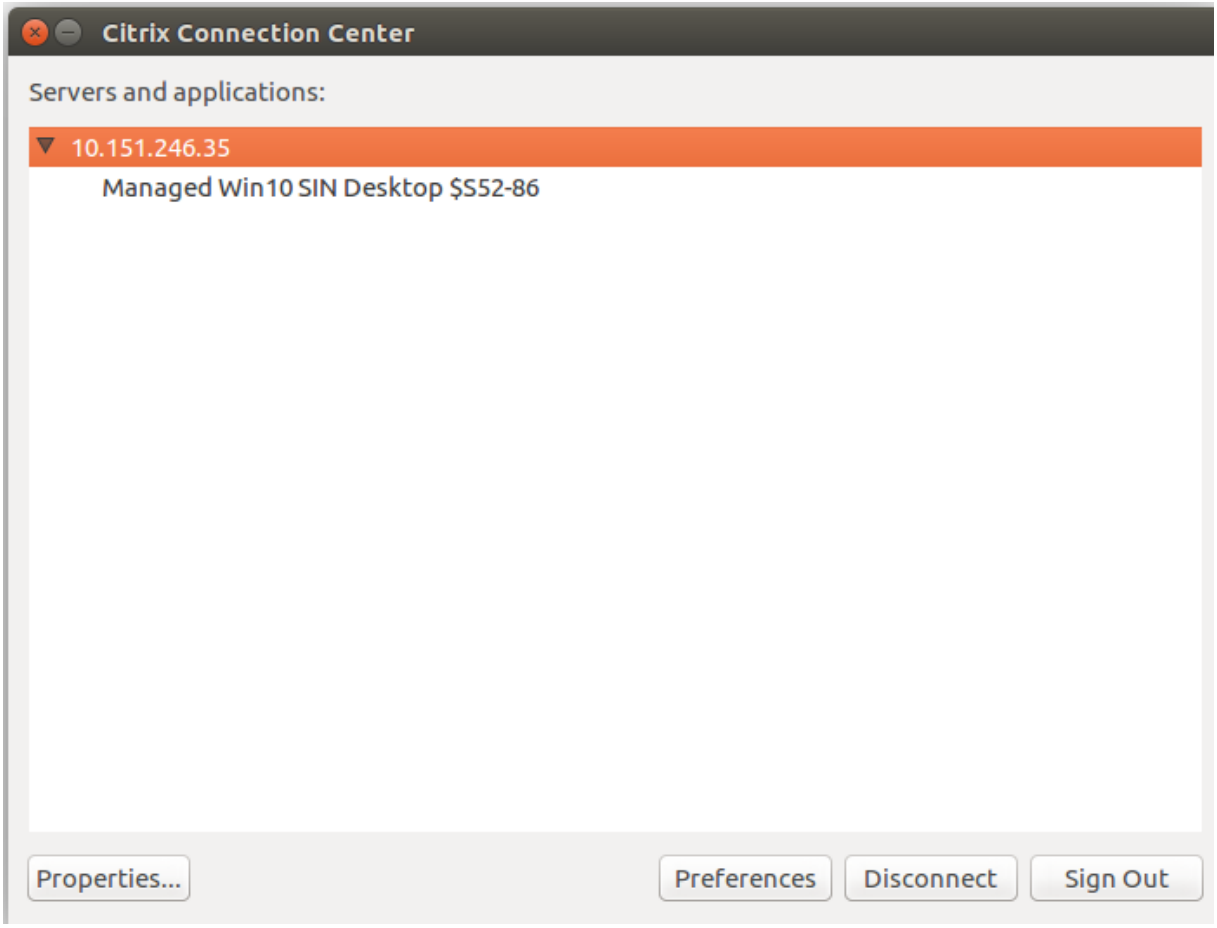


Vous pouvez utiliser le fichier `wfclient.ini` pour configurer les attributs de chemin d'accès et de nom de fichier mappés. Utilisez l'interface graphique pour définir un niveau d'accès aux fichiers comme indiqué dans la capture d'écran précédente.

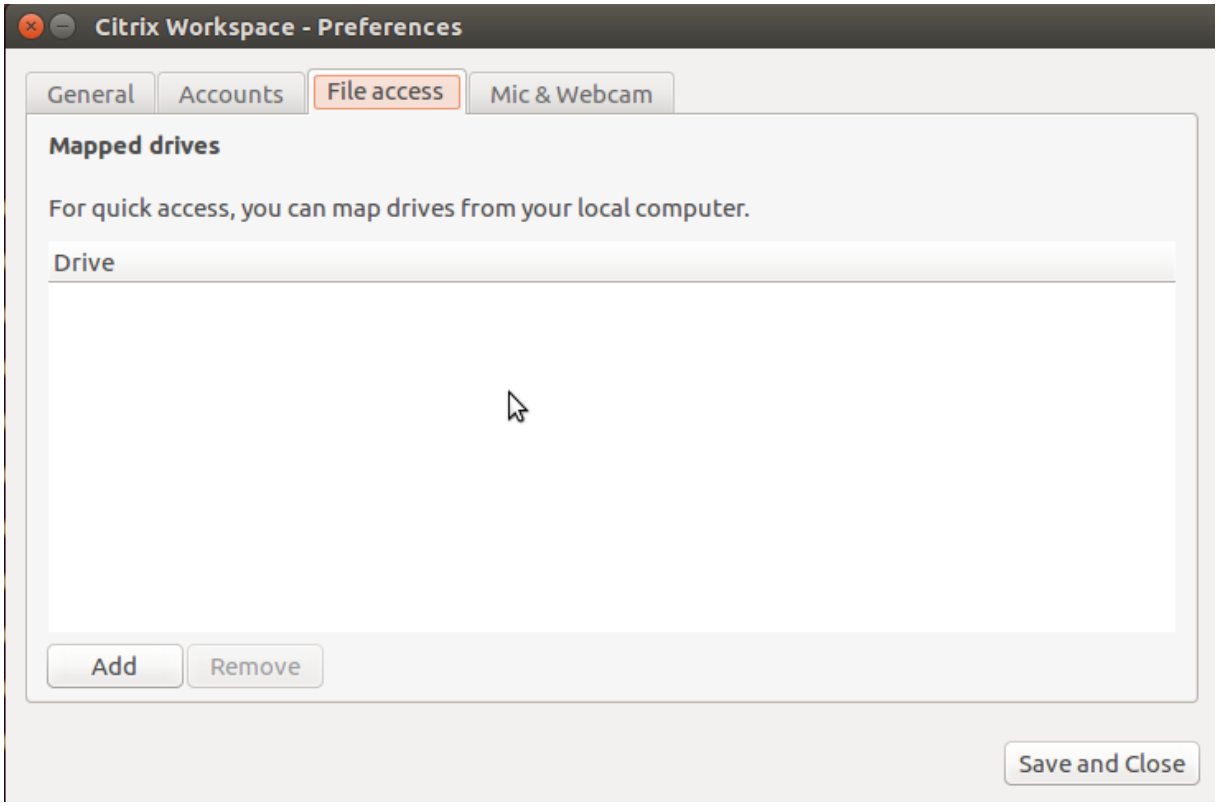
Dans une session de bureau, vous pouvez définir un niveau d'accès aux fichiers en accédant à la boîte de dialogue **Préférences** > **Accès aux fichiers** à partir de Desktop Viewer.



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 and Desktops et Citrix DaaS 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=printer1:printer2:printer3

    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 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 s'avérer nécessaire de mapper manuellement des imprimantes clientes sur Citrix Virtual Apps and Desktops ou Citrix DaaS 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 and Desktops ou Citrix DaaS.
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, cette valeur correspond à 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

À partir de la version 2112, l'attribut `VdcamVersion4Support` du fichier `module.ini` est renommé `AudioRedirectionV4`. La valeur par défaut de `AudioRedirectionV4` est définie sur **False**. Résultat :

- La bibliothèque ALSA est utilisée pour accéder aux périphériques audio et un seul appareil est pris en charge.
- Seul le périphérique audio par défaut portant le nom Citrix HDX Audio apparaît dans la session.
- Une seule application peut utiliser le périphérique audio Citrix HDX à la fois.

Vous pouvez définir la valeur de `AudioRedirectionV4` sur **True**. Résultat :

- La bibliothèque PulseAudio est utilisée pour accéder aux périphériques audio et des appareils supplémentaires sont pris en charge.
- Plusieurs applications peuvent utiliser les périphériques audio à la fois.
- L'application Citrix Workspace affiche tous les périphériques audio locaux disponibles dans une session. Au lieu de Citrix HDX Audio, les périphériques audio apparaissent désormais avec leurs noms de périphérique respectifs. Vous pouvez basculer dynamiquement vers n'importe quel périphérique disponible dans une session.
- Les sessions sont mises à jour de manière dynamique lorsque vous branchez ou supprimez des périphériques audio.
- La redirection de périphérique audio est prise en charge avec HDMI et les périphériques audio Bluetooth.

Pour activer 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 :

   AudioRedirectionV4=True

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

> **Remarques :**
>
> - La fonctionnalité de redirection audio améliorée est disponible en version Technical Preview.
> - L'option **Mic et webcam** de la boîte de dialogue **Préférences** est désactivée par défaut. Pour plus d'informations sur l'activation du micro et de la webcam, reportez-vous à la section Préférences.

L'application Citrix Workspace version 2010 résout les problèmes liés à l'amélioration de la fonctionnalité Multi-Stream ICA.

Limitations connues :

Par défaut, la valeur `AudioRedirectionV4` est définie sur **False**. Si vous n'avez pas modifié la valeur par défaut, les limitations connues suivantes sont présentes :

- 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. Cette limitation est résolue lorsque vous définissez la valeur `AudioRedirectionV4` sur **True**.
- La redirection de périphérique audio n'est pas prise en charge avec les périphériques audio Bluetooth. Cette limitation est résolue lorsque vous définissez la valeur `AudioRedirectionV4` sur **True**.
- 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.
- La redirection de périphérique audio n'est pas prise en charge avec les périphériques audio HDMI. Cette limitation est résolue lorsque vous définissez la valeur `AudioRedirectionV4` sur **True**. Toutefois, l'application Citrix Workspace peut afficher des périphériques audio HDMI qui ne sont pas connectés dans une session.

Lorsque la valeur `AudioRedirectionV4` est définie sur **False**, 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\>
<!--NeedCopy-->
```

Dans cette section, l'information sur la machine se trouve 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.

Amélioration de la qualité audio

Auparavant, la valeur maximale de mise en mémoire tampon de sortie pour lire l'audio de manière fluide était de 200 ms dans l'application Citrix Workspace. Par conséquent, une latence de 200 ms a été ajoutée dans le scénario de lecture. Cette valeur maximale de mise en mémoire tampon de sortie avait également un impact sur les applications audio interactives.

Grâce à cette amélioration, la valeur maximale de mise en mémoire tampon de sortie est réduite à 50 ms dans l'application Citrix Workspace. En conséquence, l'expérience utilisateur avec l'application audio interactive est améliorée. De plus, la durée des boucles (RTT) est réduite de 150 ms.

À partir de la version 2207, vous pouvez sélectionner le seuil de lecture et le pré-tampon audio pulsé appropriés pour améliorer la qualité audio. Pour cette amélioration, les paramètres suivants ont été ajoutés dans la section [ClientAudio] du fichier `module.ini` :

- `PlaybackDelayThreshV4` — Pour spécifier le niveau initial de mise en mémoire tampon de sortie en millisecondes. L'application Citrix Workspace essaie de maintenir ce niveau de mise en mémoire tampon pendant toute la durée d'une session. La valeur par défaut de `PlaybackDelayThreshV4` est 50 ms. Ce paramètre n'est valide que si `AudioRedirectionV4` est défini sur **True**.
- `AudioTempLatencyBoostV4` — Lorsque le débit audio connaît un pic soudain ou n'est pas suffisant pour un réseau instable, cette valeur augmente la valeur de mise en mémoire tampon de sortie. Cette augmentation de la valeur de mise en mémoire tampon de sortie fournit un son fluide. Cependant, l'audio peut être légèrement retardé. La valeur par défaut de `AudioTempLatencyBoostV4` est définie sur 100 ms. Ce paramètre n'est valide que si `AudioRedirectionV4` est défini sur **True** et `AudioLatencyControlEnabled` est défini sur **True**. Par défaut, la valeur de `AudioLatencyControlEnabled` est définie sur True.

Par défaut, la valeur de `AudioRedirectionV4` est définie sur False. Pour activer 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 :

   AudioRedirectionV4=True
3. Redémarrez la session pour que les modifications prennent effet.

Prise en charge améliorée de l'annulation de l'écho audio [Tech Preview]

À partir de la version 2207, l'application Citrix Workspace prend en charge l'annulation de l'écho. Cette fonctionnalité est conçue pour les cas d'utilisation audio en temps réel et améliore l'expérience utilisateur. La fonction d'annulation de l'écho prend en charge l'audio de qualité moyenne, l'audio de faible qualité et l'audio adaptatif. Citrix recommande d'utiliser l'audio adaptatif pour de meilleures performances.

Par défaut, la fonction d'annulation de l'écho est désactivée. Dans les cas d'utilisation en temps réel, il est recommandé d'activer l'annulation de l'écho si le haut-parleur est utilisé à la place du casque.

Pour activer cette fonctionnalité, procédez comme suit :

1. Accédez au dossier <ICAROOT>/config et ouvrez le fichier module.ini.
2. Accédez à la section [ClientAudio] et mettez à jour la valeur du paramètre EnableEchoCancellation comme suit :

```
EnableEchoCancellation =TRUE
```

Limitation :

La fonction d'annulation de l'écho est désactivée pour un son de haute qualité.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

Mapper l'audio du client

Le mappage audio du client permet aux applications exécutées sur le serveur Citrix Virtual Apps and Desktops ou Citrix DaaS 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.

Audio adaptatif

Depuis la version 2109, l'application Citrix Workspace prend en charge l'audio adaptatif. Avec l'audio adaptatif, vous n'avez pas besoin de configurer manuellement les stratégies de qualité audio sur le VDA. L'audio adaptatif optimise les paramètres de votre environnement et remplace les formats de compression audio obsolètes pour offrir une excellente expérience utilisateur. L'audio adaptatif est activé par défaut. Pour plus d'informations, consultez la section Audio adaptatif.

À partir de la version 2112, l'audio adaptatif fonctionne lors de l'utilisation de la diffusion audio UDP (User Datagram Protocol).

Limitation connue :

- L'audio adaptatif nécessite des processeurs prenant en charge Streaming SIMD Extensions (SSE) 4.x. L'application Citrix Workspace peut se fermer lorsque l'audio adaptatif est utilisé avec le processeur CPU qui ne prend pas en charge SSE 4.x.

Activation de l'audio UDP

L'audio UDP peut améliorer la qualité des appels téléphoniques effectués sur Internet. Il utilise UDP au lieu de TCP.

À partir de la version 2112, l'audio adaptatif fonctionne lors de l'utilisation de la diffusion audio UDP. À partir de cette version, l'application Citrix Workspace prend aussi en charge le protocole DTLS (Datagram Transport Layer Security) pour l'audio UDP. Par conséquent, vous pouvez accéder à l'audio UDP via Citrix Gateway. Cette fonctionnalité est désactivée par défaut.

À partir de la version 2202, l'amélioration visant à prendre en charge l'audio UDP via Citrix Gateway est disponible pour l'application Citrix Workspace.

Pour activer 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`. Par défaut, les ports 16500 à 16509 sont utilisés.
2. Par défaut, l'audio adaptatif est activé sur le VDA et prend en charge l'audio UDP. Si vous avez désactivé l'audio adaptatif, définissez les paramètres audio client et serveur comme suit pour prendre en charge l'audio UDP. Par conséquent, l'audio obtenu est 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
		Élevé	Medium (Moyen)	Faible
Qualité audio sur le serveur	Élevé	Élevé	Medium (Moyen)	Faible
Qualité audio sur le serveur	Medium (Moyen)	Medium (Moyen)	Medium (Moyen)	Faible
Qualité audio sur le serveur	Faible	Faible	Faible	Faible

Pour activer l'audio UDP via Citrix Gateway :

1. Accédez au dossier <ICAROOT>/config et ouvrez le fichier module.ini.
2. Accédez à la section [WFClient] et définissez l'entrée suivante :

   EnableUDPThroughGateway=True
3. Accédez à la section [ClientAudio] et définissez l'entrée suivante :

   EnableUDPAudio=True

> **Remarque :**
>
> Si vous utilisez la configuration StoreFront default.ica, la valeur de EnableUDPThroughGateway définie dans la section [Application] est prioritaire sur la valeur définie dans le fichier module.ini. Toutefois, vous ne pouvez définir la valeur EnableUDPAudio dans la section [ClientAudio] uniquement à l'aide du fichier module.ini. En outre, cette valeur n'est pas prioritaire sur la valeur définie dans le fichier de configuration StoreFront default.ica.

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.

UDP sur le client

1. Accédez au fichier $ICAROOT/config/module.ini.
2. Définissez ce qui suit dans la section [ClientAudio] :

   EnableUDPAudio=True

   UDPAudioPortLow=int

   UDPAudioPortHigh=int

3. Définissez ce qui suit dans la section [WFClient] :

   EnableUDPThroughGateway=True

4. Accédez au fichier `$HOME/.ICAClient/wfclient.ini`.

5. Définissez ce qui suit dans la section [WFClient] :

   AllowAudioInput=True

   EnableAudioInput=true

   AudioBandWidthLimit=1

   > **Remarques :**
   >
   > - Les valeurs définies pour les attributs `AllowAudioInput`, `EnableAudioInput` et `AudioBandWidthLimit` dans la section [WFClient] s'appliquent à la fois à l'audio UDP et à l'audio TCP.
   > - 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, puis fermez-la. Cette action crée le dossier `.ICAClient`.
   > - Lorsque la valeur de `AudioBandWidthLimit` est définie sur 1, la qualité audio du client est moyenne.

6. Définissez les stratégies suivantes sur le Domain Delivery Controller (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 de fichier 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 de fichier 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.

Activer l'entrée audio

Pour activer l'entrée audio :

1. Accédez au dossier <ICAROOT>/config et ouvrez le fichier wfclient.ini.
2. Accédez à la section [WFClient] et définissez l'entrée suivante :

   AllowAudioInput=True

> **Remarque :**
>
> La valeur définie pour l'attribut AllowAudioInput s'applique à la fois à l'audio UDP et à l'audio TCP.

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 vers leurs bureaux virtuels lorsque la redirection automatique est activée manuellement via les paramètres du fichier de configuration. La redirection automatique des périphériques USB est désactivée par défaut. Les périphériques USB disponibles pour la connexion à distance sont les suivants :

- Lecteurs Flash
- Smartphones
- PDA
- Imprimantes
- Scanners
- Lecteurs MP3
- Dispositifs de sécurité
- Tablettes

La redirection USB nécessite Citrix Virtual Apps and Desktops 7.6 ou une version ultérieure. Citrix Virtual Apps and Desktops et Citrix DaaS ne prennent pas en charge la redirection USB des périphériques de stockage de masse et requièrent une configuration spéciale pour prendre en charge des périphériques audio. Veuillez consulter la documentation de Citrix Virtual Apps 7.6 pour plus de détails.

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 d'applications et de bureaux virtuels ; 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 l'article 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 ou Citrix DaaS. 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 l'accès distant à une carte réseau dans ce cas. Par défaut, les types de périphériques USB suivants ne sont pas pris en charge dans les applications et bureaux virtuels :

- 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` se trouvant dans le dossier `$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, il est vérifié par rapport à la stratégie USB. Et, si autorisé, redirigé vers le bureau virtuel. Si la stratégie par défaut refuse le périphérique, il n'est disponible que sur le bureau local.

Supposons qu'un utilisateur branche un périphérique USB sur des ordinateurs de bureau accessibles via le mode Desktop Appliance. Dans ce cas, ce périphérique est automatiquement redirigé vers le bureau virtuel une fois que la redirection automatique a été activée manuellement via les paramètres du fichier de configuration. La redirection automatique des périphériques USB est désactivée par défaut. Pour configurer la redirection automatique des périphériques USB, procédez comme suit :

1. Accédez au fichier de configuration `$Home/.ICAClient/wfclient.ini`.
2. Ajouter l'entrée suivante :

DesktopApplianceMode=True

3. Accédez au fichier de configuration `/opt/Citrix/ICAClient/usb.conf`.
4. Définissez l'une des règles de périphérique suivantes :
   - CONNECT — Définissez le mot clé « CONNECT » pour activer la redirection automatique d'un périphérique au démarrage d'une session.
   - ALLOW — Définissez le mot clé « ALLOW » pour autoriser la redirection automatique d'un périphérique uniquement après le début d'une session.
     Toutefois, si le mot clé CONNECT ou ALLOW est défini, l'appareil est automatiquement redirigé lorsqu'il est débranché et branché au cours d'une session.

   Exemple de règle de périphérique :
   CONNECT: vid=046D pid=0002 # Autoriser un périphérique spécifique par vid/pid
   ALLOW: vid=046D pid=0102 # Autoriser un périphérique spécifique par vid/pid

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

Supposons qu'un utilisateur se déconnecte d'un bureau virtuel alors qu'un périphérique de stockage de masse USB est toujours branché sur le bureau local. Dans ce cas, ce périphérique n'est pas redirigé vers le bureau virtuel lorsque l'utilisateur se reconnecte. Pour vérifier 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, l'application Citrix Workspace n'accepte pas le périphérique. 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.

> **Remarques :**
>
> - Supposons que la stratégie de serveur de redirection de périphérique USB client est activée. Dans ce cas, les périphériques de stockage de masse sont dirigés comme des périphériques USB même si le mappage des lecteurs clients est activé.

> • L'application ne prend pas en charge la redirection de périphérique composite pour les périphériques USB.

Classes USB

La règle de stratégie USB par défaut autorise les classes de périphériques USB suivantes :

- 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 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 périphériques apparaissent en général comme spécifiques au fabricant (classe ff).

Classes de périphériques USB

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

- 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 webcams, 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 liste des périphériques USB disponibles pour l'envoi vers des bureaux. Pour mettre à jour la gamme, modifiez la liste des règles par défaut dans le fichier `usb.conf` sur la machine utilisateur dans `$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

Balise	Description
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.

TRUE	Tous les périphériques USB déjà branchés sont disponibles au démarrage. Les périphériques ne sont disponibles au démarrage que s'ils ne sont 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 n'est disponible au démarrage.

> **Remarque :**
>
> Définissez le mot clé « CONNECT » pour activer la redirection automatique d'un périphérique au démarrage d'une session. Définissez le mot clé « ALLOW » pour autoriser la redirection automatique d'un périphérique uniquement après le début d'une session. Toutefois, si le mot clé CONNECT ou ALLOW est défini, l'appareil est automatiquement redirigé lorsqu'il est débranché et branché au cours d'une session.

Redirection de périphérique USB composite

À partir de la version 2207, l'application Citrix Workspace permet de diviser les périphériques USB composites. Un périphérique USB composite peut effectuer plusieurs fonctions. Chacune de ces fonctions est présentée dans une interface différente. Des exemples de périphériques USB composites incluent les périphériques HID composés d'une entrée et d'une sortie audio et vidéo.

Actuellement, la redirection de périphérique USB composite n'est disponible que dans les sessions de bureau. Les appareils divisés apparaissent dans Desktop Viewer.

Auparavant, lorsqu'un périphérique était débranché et rebranché pendant une session, il était redirigé automatiquement. Par conséquent, le périphérique était automatiquement connecté au VDA. Avec cette version, vous devez activer la redirection automatique manuellement via les paramètres du fichier de configuration. La redirection automatique des périphériques USB composites est désactivée par défaut.

USB 2.1 et versions ultérieures prennent en charge la notion de périphériques USB composites selon laquelle plusieurs périphériques enfants partagent une seule connexion avec le même bus USB. Ces périphériques utilisent un espace de configuration unique et une connexion de bus partagée où un numéro d'interface unique 00-ff est utilisé pour identifier chaque machine enfant. Le périphérique

USB composite est différent du concentrateur USB qui fournit une nouvelle origine de bus USB pour d'autres périphériques USB pris en charge indépendamment pour la connexion.

Les périphériques composites détectés sur le point de terminaison client peuvent être transférés à l'hôte virtuel en tant que :

- un seul périphérique USB composite ou
- un ensemble de périphériques enfants indépendants (périphériques partitionnés)

Lorsqu'un périphérique USB composite est transféré, l'ensemble du périphérique devient indisponible pour le point de terminaison. Cette action bloque l'utilisation locale du périphérique pour toutes les applications sur le point de terminaison, y compris le client Citrix Workspace requis pour une expérience HDX optimisée à distance.

Envisagez l'utilisation d'un casque USB avec périphérique audio et bouton HID pour le contrôle du son et du volume. Si l'ensemble du périphérique est transféré à l'aide d'un canal USB générique, le périphérique devient indisponible pour la redirection sur le canal audio HDX optimisé. Toutefois, vous pouvez obtenir la meilleure expérience possible lorsque l'audio est envoyé via le canal audio HDX optimisé, contrairement à l'audio envoyé à l'aide de pilotes audio du côté hôte via la communication USB générique à distance. Cela est dû à la nature bruyante des protocoles audio USB.

Vous remarquerez également des problèmes lorsque le clavier système ou le périphérique de pointage fait partie d'un périphérique composite avec d'autres fonctionnalités intégrées requises pour la prise en charge de sessions à distance. Lorsqu'un périphérique composite complet est transféré, le clavier ou la souris du système devient inutilisable sur le point de terminaison, sauf dans l'application ou la session de bureau à distance.

Pour résoudre ces problèmes, Citrix vous recommande de partitionner le périphérique composite et de transférer uniquement les interfaces enfants qui utilisent un canal USB générique. Ce paramètre garantit que les autres périphériques enfants peuvent être utilisés par les applications sur le point de terminaison client, y compris l'application Citrix Workspace qui fournit des expériences HDX optimisées, tout en autorisant uniquement les périphériques requis à être transférés et disponibles vers la session à distance.

Configurer la redirection automatique de périphériques USB composites

Auparavant, lorsqu'un périphérique était débranché et rebranché pendant une session, il était redirigé automatiquement. Par conséquent, le périphérique était automatiquement connecté au VDA. Avec cette version, vous devez activer la redirection automatique manuellement via les paramètres du fichier de configuration. La redirection automatique des périphériques USB composites est désactivée par défaut.

Pour configurer la redirection automatique des périphériques USB composites, procédez comme suit :

1. Accédez au fichier de configuration $Home/.ICAClient/wfclient.ini.

2. Ajouter l'entrée suivante :

   DesktopApplianceMode=True

3. Accédez au fichier de configuration /opt/Citrix/ICAClient/usb.conf.
4. Définissez l'une des règles de périphérique suivantes :

   - CONNECT — Définissez le mot clé « CONNECT » pour activer la redirection automatique d'un périphérique au démarrage d'une session.
   - ALLOW — Définissez le mot clé « ALLOW » pour autoriser la redirection automatique d'un périphérique uniquement après le début d'une session.

   Toutefois, si le mot clé CONNECT ou ALLOW est défini, l'appareil est automatiquement redirigé lorsqu'il est débranché et branché au cours d'une session.

Exemple de règle de périphérique :

CONNECT: vid=046D pid=0002 # Autoriser un périphérique spécifique par vid/pid‘

ALLOW: vid=046D pid=0102 # Autoriser un périphérique spécifique par vid/pid‘

Règles de périphériques :

Comme pour les périphériques USB standard, les périphériques composites à transférer sont sélectionnés en fonction des règles de périphérique définies dans la configuration de l'application Citrix Workspace. L'application Citrix Workspace utilise ces règles pour décider sur quels périphériques USB la redirection vers la session à distance doit être autorisée ou bloquée.

Chaque règle se compose d'un mot clé d'action (Allow, Connect ou Deny), de deux-points (:), et de zéro ou plusieurs paramètres de filtre qui correspondent aux périphériques réels dans le sous-système USB des points de terminaison. Ces paramètres de filtre correspondent aux métadonnées du descripteur de périphérique USB utilisées par chaque périphérique USB pour s'identifier.

Les règles de périphériques sont saisies sous forme de texte clair : chaque règle s'affiche sur une seule ligne et un commentaire facultatif après le caractère #. Les règles sont mises en correspondance de haut en bas (ordre de priorité décroissant). La première règle qui correspond au périphérique ou à l'interface enfant est appliquée. Les règles suivantes qui sélectionnent le même périphérique ou la même interface sont ignorées.

Pour modifier les règles de périphériques, procédez comme suit :

1. Accédez au fichier /opt/Citrix/ICAClient/usb.conf.
2. Mettez à jour les règles de périphérique si nécessaire.

Exemples de règle de périphérique :

```
ALLOW: vid=046D pid=0102 ## Allow a specific device by vid/pid
```

```
ALLOW: vid=0505 class=03 subclass=01 ## Allow any pid for vendor 0505 w/
subclass=01
```



```
DENY: vid=0850 pid=040C ## deny a specific device (including all child devices)

DENY: class=03 subclass=01 prot=01 ## deny any device that matches all filters

CONNECT: vid=0911 pid=0C1C ## Allow and auto-connect a specific device

ALLOW: vid=0286 pid=0101 split=01 ## Split this device and allow all interfaces

ALLOW: vid=1050 pid=0407 split=01 intf=00,01 ## Split and allow only 2 interfaces

CONNECT: vid=1050 pid=0407 split=01 intf=02 ## Split and auto-connect interface 2

DENY: vid=1050 pid=0407 split=1 intf=03 ## Prevent interface 03 from being remoted
```

Vous pouvez utiliser l'un des paramètres de filtre suivants pour appliquer des règles aux périphériques rencontrés :

Paramètre de filtre	Description
vid=xxxx	ID de fournisseur du périphérique USB (code hexadécimal à quatre chiffres)
pid=xxxx	ID de produit du périphérique USB (code hexadécimal à quatre chiffres)
rel=xxxx	ID de version du périphérique USB (code hexadécimal à quatre chiffres)
class=xx	Code de classe du périphérique USB (code hexadécimal à deux chiffres)
subclass=xx	Code de sous-classe du périphérique USB (code hexadécimal à deux chiffres)
prot=xx	Code de protocole du périphérique USB (code hexadécimal à deux chiffres)
split=1 (ou split=0)	Permet de sélectionner un périphérique composite à partitionner (ou à ne pas partitionner)

Paramètre de filtre	Description
intf=xx[,xx,xx,…]	Permet de sélectionner un ensemble spécifique d'interfaces enfants d'un périphérique composite (liste de codes hexadécimaux à deux chiffres séparée par des virgules)

Les six premiers paramètres permettent de sélectionner les périphériques USB pour lesquels la règle doit être appliquée. Si aucun paramètre n'est spécifié, la règle fait correspondre un périphérique à n'importe quelle valeur pour ce paramètre.

Le forum USB Implementors conserve une liste des valeurs de classe, de sous-classe et de protocole définies sur la page Defined Class Codes. USB-IF conserve également une liste des ID de fournisseur enregistrés. Vous pouvez vérifier le fournisseur, le produit, la version et les ID d'interface d'un périphérique spécifique à l'aide d'un outil gratuit tel que lsusb :

```
 <username@username>-ThinkPad-T470:/var/log$ lsusb

Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub

Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub

Bus 002 Device 002: ID 0bda:0316 Realtek Semiconductor Corp. USB3.0-CRW

Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub

Bus 001 Device 005: ID 138a:0097 Validity Sensors, Inc.

Bus 001 Device 004: ID 5986:111c Acer, Inc Integrated Camera

Bus 001 Device 003: ID 8087:0a2b Intel Corp.

Bus 001 Device 006: ID 17ef:609b Lenovo Lenovo USB Receiver

Bus 001 Device 045: ID 1188:a001 Bloomberg L.P. Lenovo USB Receiver

Bus 001 Device 044: ID 1188:a301 Bloomberg L.P.

Bus 001 Device 043: ID 1188:a901 Bloomberg L.P. Keyboard Hub

Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```



```
26
27 <!--NeedCopy-->
```

```
1      | <username@username>-ThinkPad-T470:/var/log$ lsusb -t
2
3      /:  Bus 04.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 10000
          M
4
5      /:  Bus 03.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 480M
6
7      /:  Bus 02.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/6p, 5000M
8
9      |__ Port 3: Dev 2, If 0, Class=Mass Storage, Driver=usb-storage,
          5000M
10
11     /:  Bus 01.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/12p, 480M
12
13     |__ Port 1: Dev 43, If 0, Class=Hub, Driver=hub/4p, 480M
14
15         |__ Port 1: Dev 46, If 0, Class=Human Interface Device, Driver=
              usbhid, 12M
16
17         |__ Port 4: Dev 45, If 0, Class=Human Interface Device, Driver=
              usbhid, 12M
18
19         |__ Port 4: Dev 45, If 1, Class=Human Interface Device, Driver=
              usbhid, 12M
20
21         |__ Port 2: Dev 44, If 3, Class=Audio, Driver=snd-usb-audio, 12
              M
22
23         |__ Port 2: Dev 44, If 1, Class=Vendor Specific Class, Driver=,
               12M
24
25         |__ Port 2: Dev 44, If 4, Class=Audio, Driver=snd-usb-audio, 12
              M
26
27         |__ Port 2: Dev 44, If 2, Class=Audio, Driver=snd-usb-audio, 12
              M
28
29         |__ Port 2: Dev 44, If 0, Class=Human Interface Device, Driver=
              usbhid, 12M
30
```



```
31      |__ Port 4: Dev 6, If 1, Class=Human Interface Device, Driver=
           usbhid, 12M
32
33      |__ Port 4: Dev 6, If 2, Class=Human Interface Device, Driver=
           usbhid, 12M
34
35      |__ Port 4: Dev 6, If 0, Class=Human Interface Device, Driver=
           usbhid, 12M
36
37      |__ Port 7: Dev 3, If 0, Class=Wireless, Driver=btusb, 12M
38
39      |__ Port 7: Dev 3, If 1, Class=Wireless, Driver=btusb, 12M
40
41      |__ Port 8: Dev 4, If 1, Class=Video, Driver=uvcvideo, 480M
42
43      |__ Port 8: Dev 4, If 0, Class=Video, Driver=uvcvideo, 480M
44
45      |__ Port 9: Dev 5, If 0, Class=Vendor Specific Class, Driver=, 12M
           |
46
47  <!--NeedCopy-->
```

Lorsqu'ils sont présents, les deux derniers paramètres s'appliquent uniquement aux périphériques composites USB. Le paramètre « split » détermine si un périphérique composite doit être transféré en tant que périphérique partitionné ou en tant que périphérique composite unique.

Split=1 indique que les interfaces enfants sélectionnées d'un périphérique composite doivent être transférées en tant que périphériques partitionnés.
Split=0 indique que le périphérique composite ne doit pas être partitionné.

> **Remarque :**
>
> Si le paramètre « split » est omis, Split=0 est la valeur par défaut.

Le paramètre intf sélectionne les interfaces enfants spécifiques du périphérique composite auquel l'action doit être appliquée. S'il est omis, l'action s'applique à toutes les interfaces du périphérique composite.

Prenons l'exemple d'un périphérique USB composite (par exemple, un clavier Bloomberg 4) doté de six interfaces :

- Interface 0 - Clavier HID Bloomberg 4
- Interface 1 - Clavier HID Bloomberg 4
- Interface 2 - HID Bloomberg 4
- Interface 3 - Canal audio du clavier Bloomberg 4
- Interface 4 - Canal audio du clavier Bloomberg 4

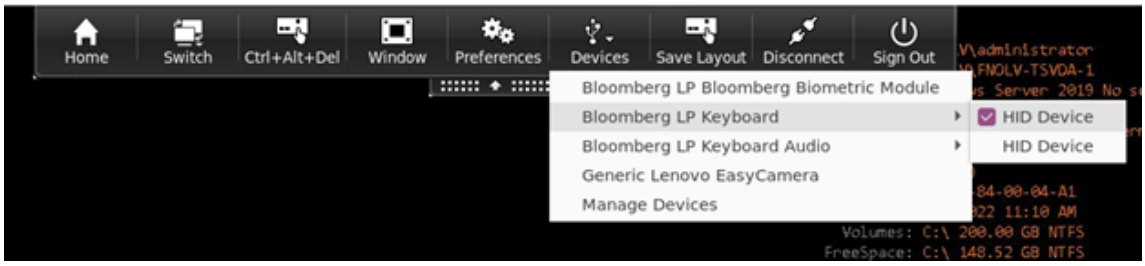
- Interface 5 - Canal audio du clavier Bloomberg 4
- Les règles suggérées pour ce type de périphérique sont les suivantes :

```
CONNECT: vid=1188 pid=9545 split=01 intf=00 ## Bloomberg 4 Keyboard HID

CONNECT: vid=1188 pid=9545 split=01 intf=01 ## Bloomberg 4 Keyboard HID

CONNECT: vid=1188 pid=9545 split=01 intf=02 ## Bloomberg 4 HID

DENY: vid=1188 pid=9545 split=01 intf=03 ## Bloomberg 4 Keyboard Audio
Channel

DENY: vid=1188 pid=9545 split=01 intf=04 ## Bloomberg 4 Keyboard Audio
Channel

DENY: vid=1188 pid=9545 split=01 intf=05 ## Bloomberg 4 Keyboard Audio
Channel
```

Redirection de périphérique USB composite avec Citrix Viewer

Pour connecter les périphériques USB à partir de la section **Périphériques**, procédez comme suit :

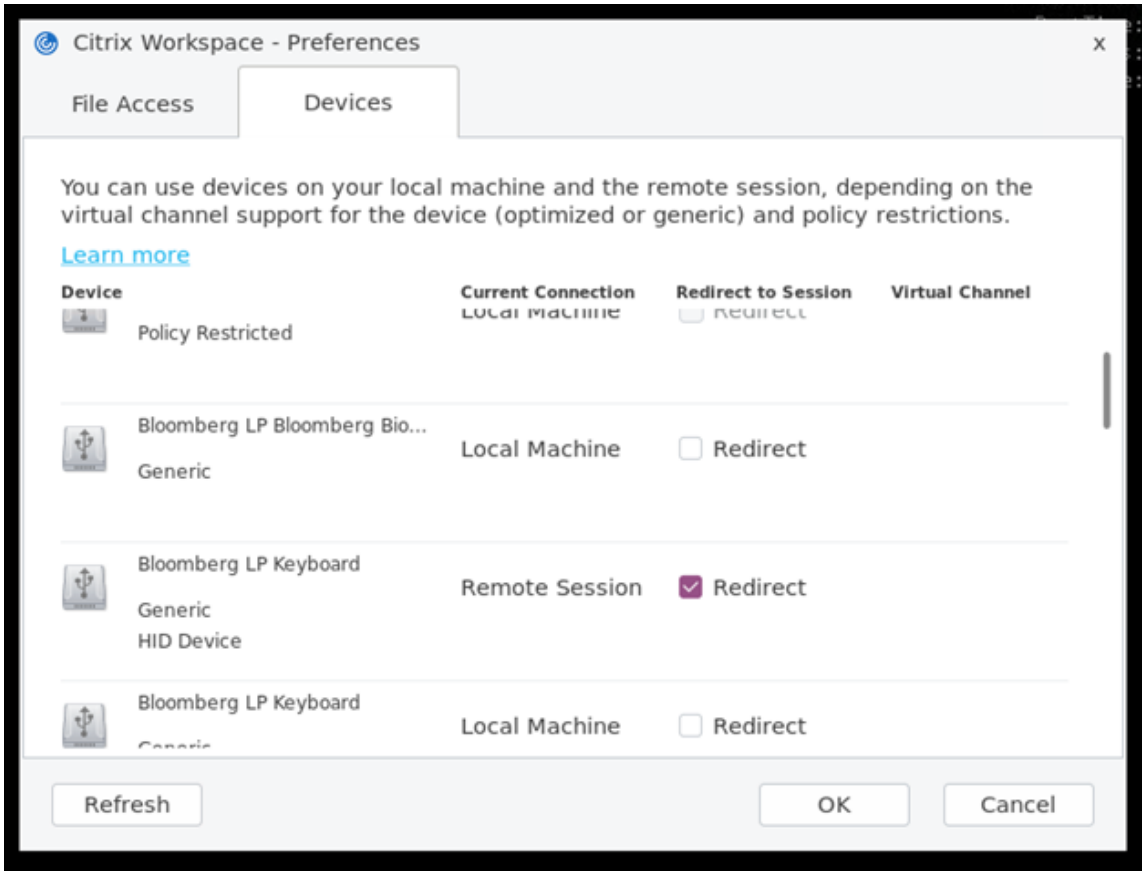
1. Dans une session de bureau, accédez à Desktop Viewer sous **Périphériques**.
   Les périphériques USB divisés apparaissent.



2. Pour connecter un appareil, sélectionnez l'élément de menu requis.

Pour connecter les périphériques USB à partir de la section **Préférences**, procédez comme suit :

1. Accédez à la section **Préférences > Périphériques**.
   Les périphériques USB divisés apparaissent.



2. Activez les cases à cocher en regard des périphériques, selon vos besoins.
3. Cliquez sur **OK**.

La configuration sélectionnée est appliquée à la connexion du périphérique.

> **Remarque :**
>
> Désactivez l'élément de menu ou les cases à cocher en regard des périphériques que vous souhaitez déconnecter.

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 connecter des webcams via la prise en charge USB, désactivez la compression vidéo pour caméra Web HDX RealTime.

Redirection de webcam

Voici quelques indications sur la redirection de la webcam :

- La redirection de webcam est compatible avec et sans RTME.
- La redirection de webcam fonctionne avec les applications 32 bits et 64 bits. Par exemple, Skype, GoToMeeting. Utilisez un navigateur 32 bits ou 64 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.

Redirection de webcam pour applications 64 bits [version Technical Preview]

À partir de la version 2111, la redirection de webcam est prise en charge pour les applications 64 bits.

Configuration système requise

- Infrastructure `GStreamer` 0.1.x ou 1.x selon de la version actuelle installée sur le système
- Version `ICAClient` supérieure à 2106 si `GStreamer` 1.x est utilisé
- Version et plug-ins `Gstreamer` :
  - `gstreamer1.0-plugins-base`
  - `gstreamer1.0-plugins-bad`
  - `gstreamer1.0-plugins-good`
  - `gstreamer1.0-plugins-ugly`
  - `gstreamer1.0-vaapi plugin` et bibliothèque `libva`
  - Bibliothèque x264

> **Remarque :**
>
> La version du plug-in `GStreamer` doit être cohérente avec la version de l'infrastructure `GStreamer`. Par exemple, si vous installez `Gstreamer` 1.2.4, la version de tous les plug-ins `Gstreamer` 1.x doit être 1.2.4.

Configuration de la redirection de Webcam

Procédez comme suit pour activer et configurer la fonctionnalité de redirection de Webcam pour les applications 64 bits sur l'application Citrix Workspace pour Linux.

Étape 1 : Vérifiez la configuration de ICAClient

Définissez la valeur de `AllowAudioInput` sur **True** pour activer la fonctionnalité de redirection de Webcam. Par défaut, cette valeur est définie sur **True** lors de l'installation de `ICAClient`.

Si la valeur de `AllowAudioInput` est définie sur **False**, procédez comme suit pour activer la fonctionnalité de redirection de Webcam :

1. Accédez au fichier de configuration ~/.ICAClient/wfclient.ini et modifiez-le.
2. Définissez la valeur AllowAudioInput sur **True**.

   AllowAudioInput=True

Étape 2 : Vérifiez la configuration de l'encodeur Theora

Une fois que vous avez correctement installé ICAClient et que la valeur de AllowAudioInput est définie sur **True**, l'encodeur Theora est configuré par défaut. Cet encodeur est un encodeur logiciel offrant des performances acceptables. Toutefois, cet encodeur ne prend en charge que les applications 32 bits sur un VDA.

Procédez comme suit pour vérifier que l'encodeur Theora prend en charge les applications 32 bits :

1. Installez Firefox 32 bits sur un VDA.
2. Accédez au site de test de la Webcam https://webcamtests.com/.

L'encodeur Theora ne prend pas en charge la fonctionnalité de redirection de Webcam pour les applications 64 bits sur un VDA. Configurez l'option d'encodeur H264 pour prendre en charge la fonctionnalité de redirection de Webcam pour les applications 64 bits sur VDA.

Étape 3 : Configurez l'encodeur H264

L'encodeur H264 prend en charge la fonctionnalité de redirection de Webcam pour les applications 64 bits sur le VDA. Pour activer l'encodeur H264, procédez comme suit :

1. Accédez au fichier de configuration ~/.ICAClient/wfclient.ini et modifiez-le.
2. Définissez la valeur HDXH264InputEnabled sur **True**.

   HDXH264InputEnabled=True

Procédez comme suit pour vérifier que l'encodeur H264 prend en charge les applications 64 bits :

1. Installez Firefox 64 bits sur un VDA.
2. Accédez au site de test de la Webcam https://webcamtests.com/.

Étape 4 : Vérifiez les dépendances du système

Après avoir configuré l'encodeur H264, si la fonctionnalité de redirection de Webcam ne prend pas en charge les applications 64 bits sur le VDA, vérifiez les dépendances du système.

La fonctionnalité de redirection de Webcam pour l'application 64 bits est basée sur l'infrastructure GStreamer. ICAClient utilise l'infrastructure GStreamer 0.1.x ou 1.x selon la version actuelle installée sur le système.

Étape 4.1 : Vérifiez la version de ICAClient

Vérifiez si la version de ICAClient est supérieure à 2106 au cas où elle utilise GStreamer 1.x. Les versions précédentes de ICAClient peuvent échouer.

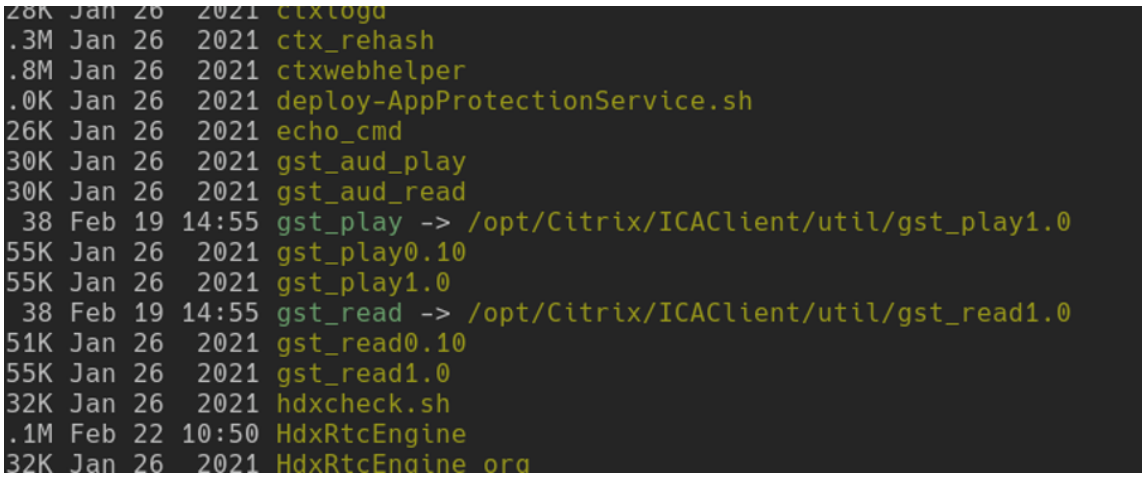
Procédez comme suit pour vérifier que la version de ICAClient est basée sur l'infrastructure GStreamer installée sur votre système :

1. Entrez les commandes suivantes sur une ligne de commande :

```
cd /opt/Citrix/ICAClient/util
<!--NeedCopy-->
```

```
ls -alh
<!--NeedCopy-->
```

2. Vérifiez que gst_read symlink est lié à gst_read1.0 ou gst_read0.1. tel qu'illustré dans l'image suivante :



Vous pouvez également exécuter le script workspaceappcheck.sh dans le répertoire util et vérifier la sortie de la section faisant référence aux dépendances GStreamer.

Citrix recommande d'utiliser la version de ICAClient supérieure ou égale à 2106 et GStreamer 1.x.

Étape 4.2 : Vérifiez la version de Gstreamer et des plug-ins

Outre l'infrastructure GStreamer 1.x, vous devez installer les plug-ins requis suivants :

- Gstreamer1.0-plugins-base
- Gstreamer1.0-plugins-bad

- Gstreamer1.0-plugins-good
- Gstreamer1.0-plugins-ugly
- Gstreamer1.0-vaapi plugin
- ibva library
- x264 library

Pour plus d'informations sur l'installation des plugins précédents, consultez le guide d'installation de GStreamer.

> **Remarque :**
>
> La version du plug-in GStreamer doit être cohérente avec la version de l'infrastructure GStreamer. Par exemple, si vous installez Gstreamer1.2.4, la version de tous les plug-ins Gstreamer1.x doit être 1.2.4.

Exécutez la commande suivante pour vérifier la version actuelle de l'infrastructure GStreamer :

```
1 gst-inspect-1.0 --gst-version
2 <!--NeedCopy-->
```

Pour plus d'informations sur le dépannage, voir Webcam dans la section Dépannage.

Xcapture

Le package de l'application Citrix Workspace comprend une application d'assistance, xcapture. Cette application facilite l'échange de données graphiques entre le presse-papiers du serveur et les applications X Windows non conformes aux spécifications ICCCM sur le bureau. 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.

Curseur

Prise en charge de l'inversion de couleur du curseur

Auparavant, l'application Citrix Workspace affichait un curseur en pointillé de la même couleur que l'arrière-plan noir et blanc d'un texte. Par conséquent, il était difficile de localiser la position du curseur.

À partir de la version 2112, la couleur du curseur s'inverse en fonction de la couleur d'arrière-plan d'un texte. Vous pouvez ainsi facilement localiser la position du curseur dans le texte. Cette fonctionnalité est désactivée par défaut.

Pré-requis :

- 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 `All_Regions.ini`, ajoutez les lignes suivantes à la fin de la section [Virtual Channels\Thinwire Graphics] :

InvertCursorEnabled=

InvertCursorRefreshRate=

InvertCursorMode=

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.

Pour activer cette fonctionnalité, procédez comme suit :

1. Accédez au fichier de configuration `$HOME/.ICAClient/wfclient.ini`.
2. Accédez à la section [Thinwire3.0] et définissez l'entrée suivante :

   InvertCursorEnabled=True

> **Remarque :**
>
> Le curseur ne s'inverse pas lorsque la valeur de la stratégie **Utiliser codec vidéo pour la compression** dans Citrix Studio est définie sur `Do not use video codec`.

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 and Desktops 7.8 (ou version ultérieure) ou Citrix DaaS. 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. Pour plus d'informations sur l'activation 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 la fonctionnalité de souris relative.

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 :
    - 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 activée au préalable dans le 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 du contenu du navigateur

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

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.

À partir de la version 2106, la redirection du contenu du navigateur basée sur CEF est entièrement fonctionnelle. Par défaut, cette fonction est activée.

Si nécessaire, vous pouvez remplacer le fichier `libffmpeg.so` fourni dans le package de l'application Workspace par un fichier `libffmpeg.so` approprié contenant les codecs requis, dans le chemin d'accès `$ICAROOT/cef/libffmpeg.so`.

> **Remarque :**
>
> Cette fonctionnalité n'est pas prise en charge sur la plate-forme ARMHF.

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. Accédez au fichier `$ICAROOT/config/All_Regions.ini` où $ICAROOT est le répertoire d'installation par défaut de l'application Citrix Workspace.
2. Accédez à la section `[Client Engine\WebPageRedirection]` et définissez l'entrée suivante :

   UseCefBrowser=True

Problèmes connus :

- Lorsque vous définissez l'option `UseCefBrowser` sur **True** dans `~/.ICAClient/All_Regions.ini`, l'éditeur IME japonais, chinois (simplifié) 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 (simplifié) et coréen lors de l'utilisation du SaaS sécurisé avec le navigateur Citrix intégré.
- Lorsque vous tentez de lancer une redirection de page Web à l'aide de la redirection du contenu du navigateur basée sur CEF, vous pouvez recevoir une erreur de certificat inconnu. Le problème se produit sur l'application Citrix Workspace version 2106 et versions ultérieures.
  Pour contourner le problème, exécutez la commande suivante dans le terminal pour importer le certificat auto-signé dans `nssdb` :

  ```
  1  certutil -A -n "badssl.cer" -t "C,," -d ~/.pki/nssdb -i ~/
        Downloads/badssl.cer
  2  <!--NeedCopy-->
  ```

  Les arguments des commandes sont les suivants :

  - `-A` - Pour ajouter un certificat à la base de données.
  - `-n` - Le nom du certificat. Cet argument est facultatif et peut être utilisé pour ajouter le surnom.
  - `"badssl.cer"` - Le nom du certificat exporté depuis le site badssl.com.
  - `-t "C,,"` - `-t` est pour TRUSTARGS et C pour le certificat CA. Pour plus d'informations, consultez la documentation de Google.
  - `-d ~/.pki/nssdb` - L'emplacement de la base de données.
  - `-i` - Indique le fichier d'entrée. Cet argument permet d'ajouter l'emplacement et le nom du fichier de certificat.

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.

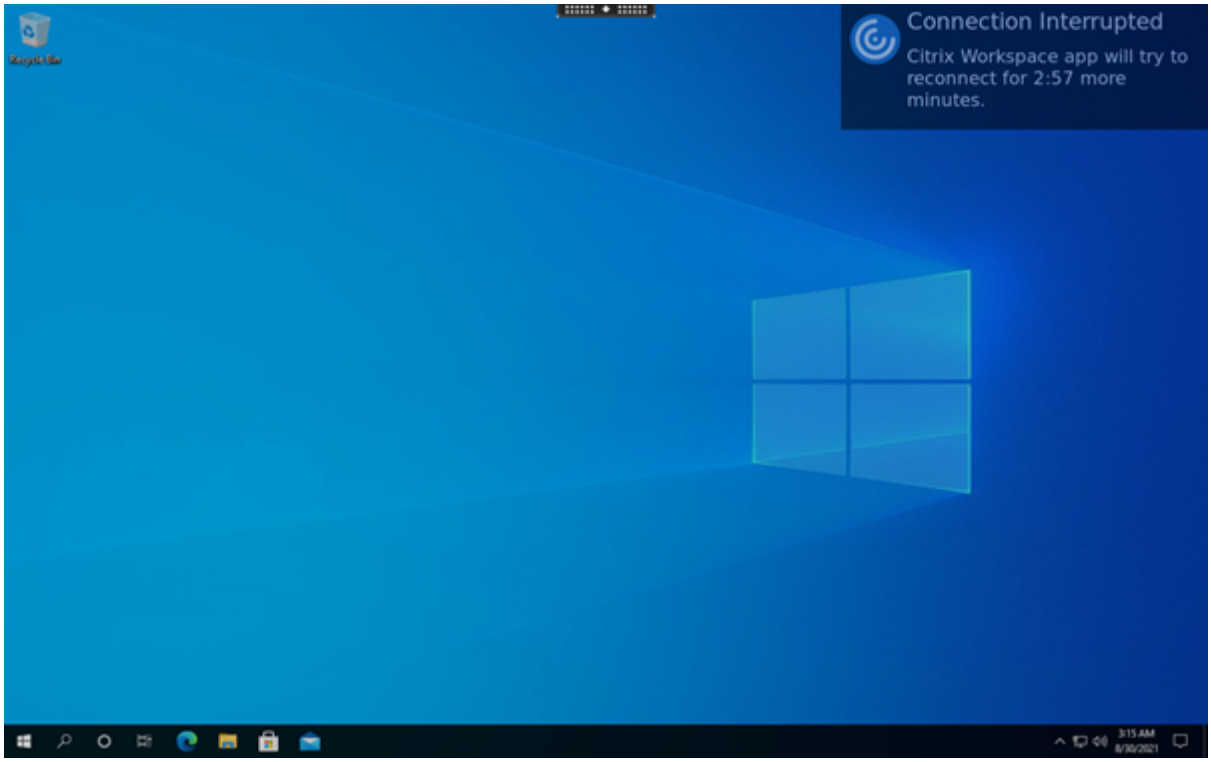
Pour accéder à des instructions sur la configuration de la fonctionnalité de reconnexion automatique des clients HDX Broadcast, consultez la documentation de Citrix Virtual Apps and Desktops.

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.

L'écran change désormais lorsque la fiabilité de session commence. Avec cette amélioration, la fenêtre de session est grisée et un minuteur affiche le temps qui reste avant la prochaine tentative de reconnexion.



> **Conseil**
>
> Vous pouvez modifier la luminosité des nuances de gris utilisées pour une session inactive à l'aide de la stratégie **Niveau de transparence de l'interface durant la reconnexion**. Par défaut, cette valeur est définie sur 80. La valeur maximale ne peut pas dépasser 100 (indique une fenêtre transparente) et la valeur minimale peut être réglée sur 0 (écran entièrement noir).

Lorsqu'une session se reconnecte avec succès, le message de notification disparaît. Vous pouvez interagir avec le bureau comme d'habitude.

À partir de la version 2109, la notification de fiabilité de session est activée par défaut.

Pour désactiver cette amélioration :

1. Accédez au fichier de configuration `/opt/Citrix/ICAClient/config/module.ini`.
2. Dans la section [WFClient], modifiez le paramètre suivant :

```
SRNotification=False
```

> **Remarque :**
>
> Cette fonctionnalité est prise en charge uniquement pour Citrix Virtual Desktops.

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.

Utilisation des stratégies de fiabilité de session

Le paramètre de stratégie Connexions de fiabilité de session active la fiabilité de session.

Le paramètre de stratégie Expiration de délai de la fiabilité de session est réglé par défaut sur 180 secondes, ou trois minutes. Si nécessaire, vous pouvez prolonger la durée pendant laquelle la fiabilité de session maintient une session ouverte. Si c'est le cas, vous n'avez pas besoin de vous réauthentifier.

> **Conseil**
>
> Si vous augmentez la durée pour laquelle une session est gardée ouverte, vous pouvez vous laisser distraire et vous éloigner de votre appareil. Il est alors possible que des utilisateurs non autorisés puissent accéder à la session.

Les connexions entrantes de fiabilité de session utilisent le port 2598, à moins que vous ne changiez le numéro de port défini dans le paramètre de stratégie Numéro de port de la fiabilité de session.

Pour de plus amples informations sur la configuration des stratégies de fiabilité de session, consultez la section Paramètres de stratégie Fiabilité de session.

> **Remarque :**
>
> La fiabilité de session est activée par défaut au niveau du serveur. Pour désactiver cette fonctionnalité, configurez la stratégie gérée par le serveur.

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 technologies améliorent l'expérience utilisateur lors de la connexion aux applications et bureaux hébergés comme suit :

- Redirection HDX MediaStream Windows Media

- Redirection Flash HDX MediaStream
- 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 HDX MediaStream Windows Media

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. En conséquence, les besoins en bande passante pour la lecture de fichiers multimédia sont réduits.

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 qui dépendent 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. La récupération côté client continue à utiliser playbin2, à l'aide de l'option SpeedScreenMMAEnablePlaybin2 de 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.

Remarque 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 suivantes :

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 la section 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 arrière et en avant 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
<!--NeedCopy-->
```

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 - chemin d'installation de l'application Citrix Workspace pour Linux.
- GST_PLUGINS_PATH - 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 :

- Dans les versions antérieures à la version 2106, la redirection de la webcam peut échouer et la session peut être déconnectée lors de l'utilisation de `GStreamer` version 1.15.1 ou ultérieure.

Redirection Flash HDX MediaStream

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. Vérifiez que votre machine utilisateur dispose des fonctionnalités requises. Pour plus d'informations, consultez la section Configuration système requise.
2. Ajoutez les paramètres suivants à la section `wfclient.ini` 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, cette valeur est définie sur **Jamais**. Une boîte de dialogue demande également 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, cette valeur est définie sur **Disabled**.

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

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

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

     Définit la taille du cache côté client, en Mo. Cette valeur peut être comprise entre 25 Mo 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 valeur 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 valeur 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 fournit une option de compression vidéo de webcam pour améliorer l'efficacité de la bande passante pendant une visioconférence. Cette option garantit aux utilisateurs des performances optimales lorsqu'ils utilisent des applications telles que GoToMeeting with HDFaces et Skype Entreprise.

1. Vérifiez que votre machine utilisateur dispose des fonctionnalités requises.
2. Vérifiez que le canal virtuel `Multimedia` est activé. Pour l'activer, ouvrez le fichier `$ICAROOT/config/module.ini` et vérifiez que `MultiMedia` dans la section [ICA3.0] est défini sur `On`.
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 webcam 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 effectuer cette connexion, procédez comme suit :

- 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 :

   AllowAudioInput=False

   Pour plus d'informations, reportez-vous à la section Paramètres par défaut.

2. Ouvrez le fichier `usb.conf`, généralement disponible 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. Pour cette protection, vous pouvez filtrer l'accès à des sites Web et à 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 :

Vérifiez 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 de 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 diffusés 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. Ce paramètre 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 ou Citrix DaaS. 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**. Ce paramètre 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. Vérifiez 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
- 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 appliquer 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/citrix/ICAClient.log`. Sinon, les journaux sont stockés dans `${ HOME } /.ICAClient/logs/ICAClient.log`.

Lorsque l'application Citrix Workspace est installée, un utilisateur appelé `citrixlog` est créé pour gérer la fonctionnalité de journalisation.

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

Module	Classe de journal
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
Journaux d’événements standard	LOG_CLASS
SRCC	TC_SRCC
Connexion SSPI	TC_CSM
Carte à puce	TC_SCARDVD
Selfservice	TC_SS
Extension Selfservice	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

Module	Classe de journal
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
Shell `Wfica`	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
- Verbose

Par défaut, l'option **Journalisation** est définie sur **Uniquement les erreurs**.

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** est recommandé uniquement 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 différentes classes séparées par le symbole de barre verticale.
   Par exemple, `+TC_LIB|+TC_MMVD`.

Le tableau suivant répertorie les modules `wfica` et leurs valeurs de classe de trace correspondantes :

Module	Valeur TraceClasses
Graphiques	TC_TW
EUEM	TC_EUEM
WFICA (Lancement de session)	TC_NCS
Impression	TC_CPM
Séquence de connexion - WD	TC_WD
Séquence de connexion - PD	TC_PD
Séquence de connexion - TD	TC_TD
Fichiers liés au proxy	TC_PROXY
Pilote virtuel multimédia//webcam	TC_MMVD
Pilotes virtuels	TC_VD
Mappage des lecteurs clients	TC_CDM
Audio	TC_CAM
COM (port de communication)	TC_CCM

Module	Valeur TraceClasses
Transparence	TC_TWI
Carte à puce	TC_SCARDVD

Le tableau suivant répertorie le module Centre de connexion et sa valeur de classe de trace correspondante :

Module	Valeur TraceClasses
Centre de connexion	TC_CSM

Le tableau suivant répertorie la valeur de classe de trace pour setWebHelper :

Valeur TraceClasses
Définissez logSwitch sur 1 (pour activer) ou 0 (pour désactiver)
Exemple : logSwitch = 1

Résolution des problèmes :

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 sur la configuration syslog.

Configuration Syslog

Par défaut, tous les journaux syslog sont enregistrés dans /var/log/syslog. Pour configurer le nom et le chemin du fichier journal, modifiez la ligne suivante sous la section [RULES] du 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 vérifier 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 dans le fichier `rsyslog.conf` en remplaçant localhost par l'adresse IP du serveur distant :

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

Collecte des fichiers journaux

Auparavant, aucun outil permettant de collecter les fichiers journaux dans l'application Citrix Workspace n'était disponible. Les fichiers journaux se trouvaient dans des dossiers différents. Vous deviez collecter manuellement les fichiers journaux à partir de ces dossiers différents.

À partir de la version 2109, l'application Citrix Workspace introduit l'outil collectlog.py pour collecter des fichiers journaux à partir de dossiers différents. Vous pouvez exécuter l'outil à l'aide de la ligne de commande. Les fichiers journaux sont générés sous forme de fichier journal compressé. Vous pouvez le télécharger à partir du serveur local.

Conditions préalables

- Python3
- Nécessite un espace supplémentaire pour enregistrer les journaux

À partir de la version 2109, deux nouveaux fichiers sont ajoutés pour collecter les fichiers journaux à l'aide de l'outil collectlog.py :

- `logcollector.ini` : enregistre le nom et le chemin du fichier journal.
- `collectlog.py` : collecte les fichiers journaux et les enregistre en tant que fichier compressé `cwalog_{ timestamp } .tar.gz`.

Par défaut, le composant [hdxteams] est ajouté au fichier logcollector.ini pour collecter les fichiers journaux pour Microsoft Teams. Toutefois, vous pouvez ajouter d'autres composants dans le fichier logcollector.ini à l'aide de la procédure suivante :

1. Accédez au fichier ${ HOME } /.ICAClient/logs/ICAClient.log/logcollector.ini.
2. Ajoutez le composant dont vous avez besoin pour collecter les fichiers journaux conformément à l'exemple suivant :

[component_name]

log_name1 = "log_path1"

log_name2 = "log_path2"

Si vous utilisez la version 2109, collectez les fichiers journaux à l'aide de la procédure suivante :

1. Téléchargez et installez l'application Citrix Workspace sur votre machine Linux.
2. À partir de la ligne de commande, accédez au chemin d'accès /opt/Citrix/ICAClient/util .
3. Exécutez la commande suivante :
   ./collctlog.py -h

   Les informations d'utilisation des commandes suivantes s'affichent :

   ```
   usage: collect_log [-h] [-c CONFIG] [-a ARCHIVE]optional arguments: -h,
    --help show this help message and exit -c CONFIG, --config CONFIG The
   logcollector.ini path & file -a ARCHIVE, --archive ARCHIVE The archive
   path & file
   ```

4. Exécutez les commandes suivantes selon les besoins :
   - ./collectlog.py : collecte les fichiers journaux à l'aide du fichier de configuration à partir du chemin d'accès par défaut et les enregistre en tant que fichiers journaux compressés sur le chemin d'accès par défaut.
   - ./collectlog.py -c /user_specified_path/logcollector.ini : collecte les fichiers journaux à l'aide du fichier de configuration à partir d'un chemin d'accès spécifié par l'utilisateur et les enregistre en tant que fichiers journaux compressés sur le chemin d'accès par défaut.
   - ./collectlog.py -c /user_specified_path/logcollector.ini -a/another_user_spec / – Collects log files using the configuration file from a user-specified path and saves them as a compressed log files at the user-defined path.

   > **Remarque :**
   >
   > Le chemin d'accès par défaut du fichier de configuration logcollector.ini est /opt/Citrix/ICAClient/config/logcollector.ini. Le chemin par défaut du fichier jour-

> nal compressé est `/tmp`.

5. Accédez au dossier `/tmp` et collectez le fichier compressé `cwalog_{ timestamp } .tar.gz`.

> **Remarque :**
>
> Les fichiers journaux sont enregistrés dans le dossier `/tmp` avec le nom de fichier `cwalog_{ timestamp } .tar.gz`.

Optimisation pour Microsoft Teams

Optimisation pour Microsoft Teams de bureau à l'aide de l'application Citrix Workspace et de Citrix Virtual Apps and Desktops ou Citrix DaaS. 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 partage d'écran avec l'optimisation pour Microsoft Teams.

> **Remarque :**
>
> - L'optimisation pour Microsoft Teams est prise en charge uniquement sur les distributions Linux x64.
> - L'optimisation Microsoft est prise en charge dans Citrix Virtual Apps and Desktops et Citrix DaaS.
> - Pour les clients légers qui utilisent Dell Wyse, utilisez l'**éditeur de configuration de Citrix** pour modifier n'importe quel paramètre du fichier `/var/.config/citrix/hdx_rtc_engine/config.json`. Pour de plus amples informations, consultez la documentation de Dell.

Pour plus d'informations sur la façon d'activer la journalisation, suivez les étapes mentionnées dans Journalisation pour Microsoft Teams.

Pour plus d'informations sur la configuration système requise, consultez Configuration requise pour l'optimisation pour Microsoft Teams.

Pour plus d'informations, consultez Optimisation pour la redirection Microsoft Teams et Microsoft Teams.

Améliorations apportées à la configuration audio

Si Microsoft Teams configure les options de contrôle automatique du gain et de suppression du bruit, Microsoft Teams redirigé vers Citrix respecte les valeurs configurées. Sinon, ces options sont activées par défaut. Toutefois, à partir de l'application Citrix Workspace 2104, l'option d'annulation de l'écho

est désactivée par défaut. À partir de l'application Citrix Workspace 2112, les administrateurs peuvent modifier les paramètres par défaut pour résoudre les problèmes d'audio (tels que la voix robotique, une utilisation élevée du processeur provoquant un son saccadé, etc.) en procédant comme suit :

1. Accédez au fichier /var/.config/citrix/hdx_rtc_engine/config.json.
2. Définissez les options suivantes :
   - Définissez la valeur de `EnableAEC` sur 1 pour activer et sur 0 pour désactiver l'annulation de l'écho
   - Définissez la valeur de `EnableAGC` sur 1 pour activer et sur 0 pour désactiver le contrôle automatique du gain
   - Définissez la valeur de `EnableNS` sur 1 pour activer et sur 0 pour désactiver la suppression du bruit

```
mkdir -p /var/.config/citrix/hdx_rtc_engine

vim /var/.config/citrix/hdx_rtc_engine/config.json

{


      ”EnableAEC”:1,”EnableAGC”:1,”EnableNS”:1

 }

<!--NeedCopy-->
```

Une fois l'appel établi, surveillez le journal `webrpc (/tmp/webrpc/<current date>/)` pour les entrées suivantes afin de vérifier que les modifications ont été appliquées :

```
/tmp/webrpc/Wed_Feb__2_14_56_33_2022/webrpc.log:[040.025] Feb 02
   14:57:13.220 webrtcapi.NavigatorUserMedia Info: getUserMedia. audio
   constraints, aec=1, agc=1, ns=1
<!--NeedCopy-->
```

Estimation des performances de l'encodeur pour Microsoft Teams

Le `HdxRtcEngine` est le moteur multimédia WebRTC intégré à l'application Citrix Workspace qui gère la redirection Microsoft Teams. Le `HdxRtcEngine.exe` peut estimer la meilleure résolution vidéo sortante (codage) que le processeur du point de terminaison peut gérer sans surcharge. Les valeurs possibles sont 240p, 360p, 720p et 1080p.

Le processus d'estimation des performances utilise le code macroblock pour déterminer la meilleure résolution possible avec le point de terminaison particulier. La négociation du codec durant un appel inclut la résolution la plus élevée possible. La négociation du codec peut se faire entre les homologues, ou entre l'homologue et le serveur de conférence.

Le tableau suivant répertorie les quatre catégories de performance des points de terminaison et leur résolution **maximale** disponible :

Performances des points de terminaison	Résolution maximale	Valeur de clé de registre
Fast (Rapide)	1080p (1920x1080 16:9 @ 30 fps)	3
Medium (Moyen)	720p (1280x720 16:9 @ 30 fps)	2
Slow (Lent)	360p (640x360 16:9 @ 30 fps ou 640x480 4:3 @ 30 fps)	1
Very slow (Très lent)	240p (320x180 16:9 @ 30 fps, ou 320x240 4:3 @ 30 fps)	0

Pour définir la valeur de résolution de la vidéo sortante (codage), par exemple sur 360p, exécutez la commande suivante à partir du terminal :

```
mkdir -p /var/.config/citrix/hdx_rtc_engine

vim /var/.config/citrix/hdx_rtc_engine/config.json

{


    ”OverridePerformance”:1

 }

<!--NeedCopy-->
```

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

<!--NeedCopy-->
```

La journalisation peut également être activée en ajoutant la ligne suivante au fichier config.json :

```
{

”WebrpcLogLevel”: 0,”WebrtcLogLevel”: 0
 }

<!--NeedCopy-->
```

Ajout de la dépendance de la bibliothèque libunwind-12 pour llvm-12

À partir de la version 2111, une nouvelle dépendance appelée bibliothèque libunwind-12 est ajoutée pour llvm-12. Toutefois, par défaut, elle n'existe pas dans le référentiel d'origine. Installez la bibliothèque libunwind-12 manuellement dans le référentiel en suivant les étapes suivantes :

1. Ouvrez le terminal.
2. Entrez la ligne suivante pour installer le fichier de clé du référentiel `llvm` :

```
 wget -O - https://apt.llvm.org/llvm-snapshot.gpg.key|sudo apt-key
    add
<!--NeedCopy-->
```

3. Entrez la ligne suivante pour configurer la liste source du référentiel `llvm` :


```
 sudo vim /etc/apt/sources.list
<!--NeedCopy-->
```

4. Ajoutez la ligne suivante :

```
deb http://apt.llvm.org/bionic/ llvm-toolchain-bionic-12 main
deb-src http://apt.llvm.org/bionic/ llvm-toolchain-bionic-12 main
<!--NeedCopy-->
```

5. Exécutez la commande suivante pour installer la bibliothèque libunwind-12 :

```
sudo apt-get update
sudo apt-get install libunwind-12
<!--NeedCopy-->
```

Amélioration apportées à l'optimisation de Microsoft Teams

- À partir de la version 2101 de l'application Citrix Workspace :
  - Le programme d'installation de l'application Citrix Workspace est 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.
- À partir de la version 2103 de l'application Citrix Workspace, le codec vidéo VP9 est désactivé par défaut.
- À partir de la version 2104 de l'application Citrix Workspace, la fonctionnalité 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.
- À partir de la version 2106 de l'application Citrix Workspace :
  - Auparavant, lorsque vous cliquiez sur **Partage d'écran**, l'aperçu d'un moniteur principal ou par défaut était uniquement disponible pour le partage d'écran.

    Avec cette version, un aperçu de tous les écrans est affiché sur le menu de sélection d'écran. Vous pouvez sélectionner n'importe quel écran pour le partage d'écran dans l'environnement VDA. Un carré rouge apparaît sur le moniteur sélectionné et une petite image du contenu de l'écran sélectionné s'affiche dans le menu de sélection d'écran.

En mode transparent, vous pouvez sélectionner un écran à partager parmi tous les écrans. Lorsque Desktop Viewer modifie le mode de fenêtre (agrandir, restaurer ou réduire), le partage d'écran s'arrête.

- À partir de la version 2112 de l'application Citrix Workspace :

  > **Remarque :**
  >
  > Les fonctionnalités suivantes sont disponibles uniquement après le déploiement d'une future mise à jour de Microsoft Teams. Lorsque la mise à jour sera déployée par Microsoft, vous pourrez consulter l'article CTX253754 pour la mise à jour de la documentation et l'annonce.

  - **Demander le contrôle dans Microsoft Teams**

    Avec cette version, vous pouvez demander le contrôle lors d'un appel Microsoft Teams lorsqu'un participant partage l'écran. Une fois que vous avez le contrôle, vous pouvez effectuer des sélections ou des modifications sur l'écran partagé.

    Pour prendre le contrôle lorsqu'un écran est partagé, cliquez sur **Demander le contrôle** en haut de l'écran Microsoft Teams. Le participant à la réunion qui partage l'écran peut accepter ou refuser votre demande.

    Tant que vous avez le contrôle, vous pouvez effectuer des sélections, des modifications et d'autres activités sur l'écran partagé. Lorsque vous avez terminé, cliquez sur **Abandonner le contrôle**.

    Limitations :

    * Les utilisateurs d'un client Linux ne peuvent pas *donner* le contrôle à d'autres utilisateurs. En d'autres termes, une fois que l'utilisateur du client Linux commence à partager du contenu, l'option **Donner le contrôle** n'est pas présente dans la barre d'outils de partage. Ce problème est une limitation Microsoft.
    * L'option **Demander le contrôle** n'est pas disponible pendant les appels poste à poste entre un utilisateur optimisé et un utilisateur sur le client de bureau Microsoft Teams natif qui s'exécute sur le point de terminaison. Pour contourner le problème, les utilisateurs peuvent rejoindre une réunion pour obtenir l'option **Demander le contrôle**.

  - **Prise en charge des appels d'urgence dynamiques**

    Avec cette version, l'application Citrix Workspace prend en charge les appels d'urgence dynamiques. Lorsque cette fonction est utilisée avec les forfaits d'appel Microsoft, Operator Connect et Direct Routing, elle permet de :

    * Configurer et acheminer les appels d'urgence
    * Informer le personnel de sécurité

La notification est fournie en fonction de l'emplacement actuel de l'application Citrix Workspace exécutée sur le point de terminaison, au lieu du client Microsoft Teams exécuté sur le VDA.
La loi Ray Baum exige que l'emplacement de la personne effectuant l'appel d'urgence soit transmis au centre de réception des appels d'urgence approprié. À partir de l'application Citrix Workspace 2112 pour Linux, l'optimisation Microsoft Teams avec HDX est conforme à la loi Ray Baum. Pour prendre en charge cette fonctionnalité, la bibliothèque LLDP doit être incluse dans la distribution du système d'exploitation du client léger.

- À partir de la version 2203 de l'application Citrix Workspace :

  Conversation et réunions à fenêtres multiples pour Microsoft Teams

  À partir de cette version, vous pouvez utiliser plusieurs fenêtres pour le chat et les réunions dans Microsoft Teams lorsqu'elles sont optimisées par HDX dans Citrix Virtual Apps and Desktops (2112 ou version ultérieure). Vous pouvez ouvrir plusieurs fenêtres pour les conversations ou les réunions de différentes manières. Pour plus d'informations sur la fonctionnalité pop-out ou multi-fenêtre, consultez Teams Pop-Out Windows for Chats and Meetings.

  Si vous exécutez une ancienne version de l'application Citrix Workspace ou du Virtual Delivery Agent (VDA), notez que Microsoft abandonnera le code de fenêtre unique à l'avenir. Toutefois, une fois cette fonctionnalité en disponibilité générale, vous disposerez d'un minimum de neuf mois pour mettre à niveau vers une version du VDA ou de l'application Citrix Workspace prenant en charge le mode multi-fenêtre (2203 et version supérieure).

  > **Remarque :**
  >
  > Cette fonctionnalité est disponible uniquement après le déploiement d'une future mise à jour de Microsoft Teams. Lorsque la mise à jour sera déployée par Microsoft, vous pourrez consulter l'article CTX253754 pour la mise à jour de la documentation et l'annonce.

- À partir de la version 2207 de l'application Citrix Workspace :

  Prise en charge de la sonnerie secondaire :

  Vous pouvez utiliser la fonction de sonnerie secondaire pour sélectionner un appareil secondaire sur lequel vous souhaitez recevoir la notification d'appel entrant lorsque Microsoft Teams est optimisé (Citrix HDX optimisé dans À propos/Version). Par exemple, imaginez que vous avez défini un haut-parleur comme sonnerie secondaire et que votre point de terminaison est connecté à un casque. Dans ce cas, Microsoft Teams envoie le signal d'appel entrant au haut-parleur même si votre casque est le périphérique principal pour l'appel audio lui-même. Vous ne pouvez pas définir de sonnerie secondaire dans les cas suivants :

  - Lorsque vous n'êtes pas connecté à plusieurs périphériques audio
  - Lorsque le périphérique n'est pas disponible (par exemple, un casque Bluetooth)

> **Remarque :**
>
> Cette fonctionnalité est disponible uniquement après le déploiement d'une future mise à jour de Microsoft Teams. Pour savoir quand la mise à jour sera déployée par Microsoft, consultez la feuille de route Microsoft 365. Vous pouvez également consulter l'article CTX253754 pour la mise à jour de la documentation et l'annonce.

- À partir de la version 2207 de l'application Citrix Workspace :
  - **Activation du partage d'applications :** à partir de l'application Citrix Workspace 2209 pour Linux et Citrix Virtual Apps and Desktops 2109, vous pouvez partager une application à l'aide de la fonctionnalité Partage d'écran de Microsoft Teams.
  - **Améliorations apportées à la prise en charge de la fonction DPI élevé :** lorsque la fonction « DPI élevé » est activée et que vous utilisez des moniteurs 4K, les superpositions vidéo de Microsoft Teams se trouvent à la position et à la taille souhaitées. Quels que soient vos paramètres d'affichage, tels que la disposition sur un ou plusieurs écrans, les superpositions s'affichent toujours correctement et ne sont pas redimensionnées ou apparaissent dans une position indésirable. Pour activer cette amélioration, assurez-vous que le paramètre `DPIMatchingEnabled` du fichier `wfclient.ini` de configuration est défini sur **True**. Pour plus d'informations, consultez Prise en charge de la correspondance DPI.
  - **Mise à niveau du SDK WebRTC :** la version du SDK WebRTC utilisée pour Microsoft Teams optimisé a été mise à niveau vers la version M98.

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

Auparavant disponible en tant que fonctionnalité expérimentale, la fonctionnalité de canal virtuel NSAP est entièrement prise en charge à partir de la version 2006. 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 `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.

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 `All_Regions.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.

> **Remarques :**
>
> - La disposition est écrasée à chaque enregistrement. La disposition est enregistrée uniquement sur StoreFront actif.
> - Si vous lancez des sessions de bureau supplémentaires 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 version commerciale de l'application Citrix Workspace 1808 pour Linux ou version ultérieure 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 mettez à jour 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 possible du profil. 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. Ce changement de couleur indique que l'enregistrement est en cours. Lorsque la disposition est enregistrée, l'icône s'affiche normalement.
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.
- Déploiements des clients avec instances StoreFront supplémentaires

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. Vérifiez 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.

Lanceur Workspace

Citrix propose désormais le lanceur Workspace (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.

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 vous permet de basculer entre leurs dispositions de clavier préférées sur la machine cliente. Cette fonction est désactivée par défaut. Une fois que vous avez activé cette fonctionnalité, la disposition du clavier client se synchronise automatiquement avec la session d'applications et de bureaux virtuels.

À compter de la version 2203, l'application Citrix Workspace prend en charge les trois modes de synchronisation de la disposition du clavier suivants :

- **Synchroniser une seule fois – lorsque la session est lancée** : basé sur la valeur `KeyboardLayout` du fichier wfclient.ini, la disposition du clavier du client est synchronisée avec le serveur lorsque la session est lancée. Si la valeur `KeyboardLayout` est définie sur `0`, le clavier système est synchronisé avec le VDA. Si la valeur `KeyboardLayout` est définie sur une langue spécifique, le clavier spécifique à la langue est synchronisé avec le VDA. Les modifications que vous apportez à la disposition du clavier du client pendant la session ne prennent pas effet immédiatement. Pour appliquer les modifications, déconnectez-vous et connectez-vous à l'application. Le mode **Synchroniser une seule fois - lorsque la session est lancée** est la disposition de clavier par défaut sélectionnée pour l'application Citrix Workspace.
- **Autoriser la synchronisation dynamique** : cette option synchronise la disposition du clavier client sur le serveur lorsque vous modifiez la disposition du clavier client.
- **Ne pas synchroniser** : indique que le client utilise la disposition du clavier présente sur le serveur.

Conditions préalables :

- Activez la fonctionnalité de mappage de disposition du clavier Unicode sur le VDA Windows. Pour obtenir davantage 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 plus d'informations, consultez la section Synchronisation dynamique de la disposition du clavier.
- La synchronisation de la disposition du clavier dépend de la bibliothèque XKB.
- Lorsque vous utilisez un Windows Server 2016 ou Windows Server 2019, accédez au chemin d'accès au Registre `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme`, ajoutez une valeur DWORD avec le nom de clé `DisableKeyboardSync` et définissez la valeur sur `0`.
- 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 `All_Regions.ini`, ajoutez les lignes suivantes à la fin de la section [Virtual Channels\Keyboard] :

KeyboardSyncMode=

KeyboardEventMode=

Configurer la disposition du clavier

L'application Citrix Workspace fournit des paramètres d'interface utilisateur et de configuration pour activer les trois différents modes de synchronisation de la disposition du clavier.

Pour configurer la synchronisation de la disposition du clavier à l'aide de l'interface utilisateur graphique :

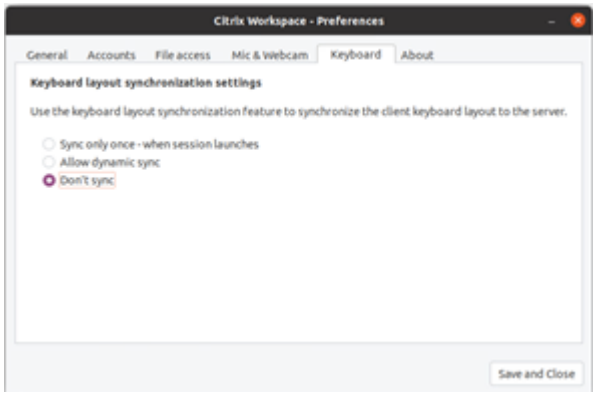
1. À partir de l'icône de l'application Citrix Workspace de la zone de notification, sélectionnez **Préférences**.

   Ou

   Ouvrez le terminal, accédez au chemin d'installation et exécutez la commande suivante :

   ```
   util/configmgr
   ```

   La boîte de dialogue **Citrix Workspace - Préférences** s'affiche.

2. Cliquez sur l'onglet **Clavier**.

   La page **Paramètres de synchronisation de la disposition du clavier** s'affiche.

3. Sélectionnez l'une des options suivantes :

   - **Synchroniser une seule fois - lorsque la session est lancée** : indique que la disposition du clavier n'est synchronisée avec le VDA qu'une seule fois au lancement de la session. Le mode de saisie au clavier Unicode est l'option recommandée pour le mode **Synchroniser une seule fois – lorsque la session est lancée**.
   - **Autoriser la synchronisation dynamique** : indique que la disposition du clavier est synchronisée dynamiquement avec le VDA lorsque le clavier client est modifié dans une session. Le mode de saisie au clavier Unicode est l'option recommandée pour le mode **Autoriser la synchronisation dynamique**.

- **Ne pas synchroniser** : indique que le client utilise la disposition du clavier du serveur, quelle que soit la disposition du clavier sélectionnée dans le client. Le mode de saisie au clavier Scancode est l'option recommandée pour le mode **Ne pas synchroniser**. Vous devez vous assurer que la disposition au clavier du client est la même que celle du VDA si vous configurez l'option Unicode pour **Ne pas synchroniser**.

4. Cliquez sur **Enregistrer** et **Fermer**.

Pour configurer la synchronisation de la disposition du clavier à l'aide des paramètres du fichier de configuration :

Modifiez le fichier de configuration `wfclient.ini` pour activer la disposition du clavier requise.

Synchroniser une seule fois – lorsque la session est lancée :

Lorsque cette fonctionnalité est activée, lors du lancement d'une session, la disposition du clavier active sur la machine cliente est synchronisée avec le VDA. En fonction de la valeur `KeyboardLayout` du fichier `wfclient.ini`, la disposition du clavier du client est synchronisée avec le serveur lors du lancement de la session. Si la valeur `KeyboardLayout` est définie sur `0`, le clavier système est synchronisé avec le VDA. Si la valeur `KeyboardLayout` est définie sur une langue spécifique, le clavier spécifique à la langue est synchronisé avec le VDA.

Pour sélectionner ce mode, procédez comme suit :

1. Accédez au fichier de configuration `$HOME/.ICAClient/wfclient.ini`.
2. Ajoutez les entrées suivantes :

```
KeyboardSyncMode=Once
KeyboardEventMode=Unicode/Scancode
<!--NeedCopy-->
```

Le mode de saisie au clavier Unicode est l'option recommandée pour le mode **Synchroniser une seule fois – lorsque la session est lancée**.

Autoriser la synchronisation dynamique :

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 correctement.

Pour sélectionner ce mode, procédez comme suit :

1. Accédez au fichier de configuration `$HOME/.ICAClient/wfclient.ini`.
2. Ajoutez les entrées suivantes :


```
KeyboardSyncMode=Dynamic
KeyboardEventMode=Unicode (or KeyboardEventMode= Scancode)
<!--NeedCopy-->
```

Le mode de saisie au clavier Unicode est l'option recommandée pour le mode **Autoriser la synchronisation dynamique**.

Ne pas synchroniser :

Lorsque cette fonctionnalité est activée, la disposition du clavier côté VDA est utilisée, quelle que soit la disposition du clavier sélectionnée sur la machine cliente.

Pour sélectionner ce mode, procédez comme suit :

1. Accédez au fichier de configuration `$HOME/.ICAClient/wfclient.ini`.
2. Ajoutez les entrées suivantes :

```
KeyboardSyncMode=No
KeyboardEventMode= Scancode (or KeyboardEventMode= Unicode)
<!--NeedCopy-->
```

Le mode de saisie au clavier Scancode est l'option recommandée pour le mode **Ne pas synchroniser**. Vous devez vous assurer que la disposition du clavier du client est la même que celle du côté du VDA si vous configurez l'option Unicode pour **Ne pas synchroniser**.

> **Remarque :**
>
> Lorsque vous définissez`KeyboardSyncMode=""` (vide) dans le fichier `wfclient.ini`, le mode revient au comportement précédent. 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.

Mode de saisie au clavier

Citrix recommande le mode de saisie au clavier suivant pour les différentes options de synchronisation de la disposition du clavier :

- Mode Scancode pour l'option **Ne pas synchroniser**.
- Mode Unicode pour les options **Autoriser la synchronisation dynamique** et **Synchroniser une seule fois - lorsque la session est lancée**.

Vous pouvez modifier la configuration de `KeyboardEventMode` dans le fichier `wfclient.ini`. Toutefois, pour bénéficier de performances optimales, utilisez les modes recommandés par Citrix pour différents scénarios, les claviers physiques et les appareils clients.

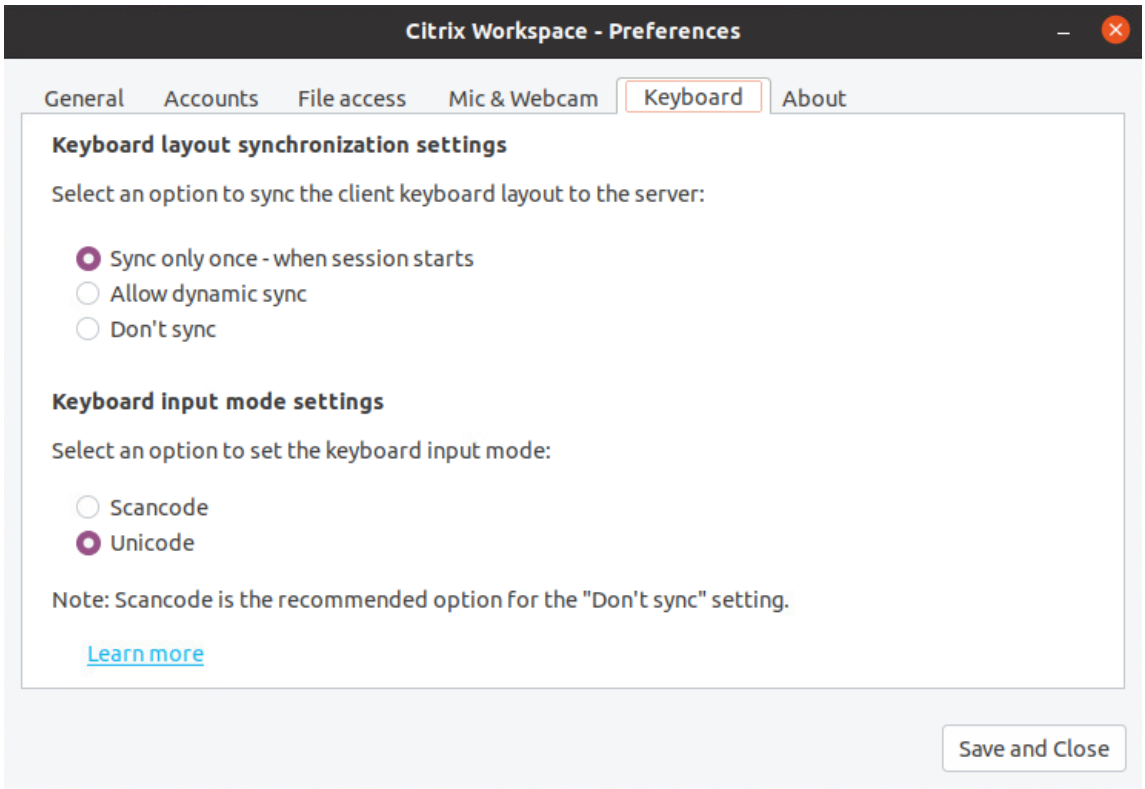
Améliorations apportées au mode de saisie du clavier [version Technical Preview]

Auparavant, vous pouviez activer différents modes de saisie du clavier uniquement en mettant à jour la valeur de `KeyboardEventMode` dans le fichier de configuration. Aucune option d'interface utilisateur n'existait pour sélectionner le mode de saisie du clavier.

À partir de l'application Citrix Workspace 2209, vous pouvez configurer différents modes de saisie du clavier à partir de la nouvelle section **Paramètres du mode de saisie du clavier**. Vous pouvez sélectionner **Scancode** ou **Unicode** comme mode de saisie du clavier.

Pour configurer le mode de saisie du clavier à l'aide de l'interface graphique, procédez comme suit :

1. À partir de l'icône de l'application Citrix Workspace de la zone de notification, sélectionnez **Préférences**.
   La boîte de dialogue **Citrix Workspace - Préférences** s'affiche.
2. Cliquez sur Clavier.
   Vous pouvez voir la section **Paramètres du mode de saisie du clavier** récemment ajoutée.



3. Sélectionnez l'une des options suivantes :
   - **Scancode** : la position des touches du clavier côté client est envoyée au VDA et le VDA génère le caractère correspondant. Applique la disposition du clavier côté serveur.
   - **Unicode** : la touche du clavier côté client est envoyée au VDA et le VDA génère le même caractère dans le VDA. Applique la disposition du clavier côté client.

Par défaut, les paramètres du mode de saisie du clavier sont définis sur **Unicode**. Pour plus d'informations sur le mode de saisie du clavier, consultez la section **Configurer la disposition du clavier** dans la documentation sur la synchronisation de la disposition du clavier.

4. Cliquez sur **Enregistrer et Fermer**.

> **Remarque :**
>
> Les modifications de configuration du clavier prennent effet une fois que vous vous reconnectez à l'application. Si vous modifiez le mode de saisie du clavier dans l'interface utilisateur, la valeur du paramètre `KeyboardEventMode` dans le fichier `wfclient.ini` est également mise à jour automatiquement.

Par exemple, imaginez un scénario dans lequel vous utilisez une disposition de clavier international américain alors que le VDA utilise une disposition de clavier russe.

Lorsque vous choisissez **Scancode** et que vous appuyez sur la touche à côté de Verr Maj, le code `1E` est envoyé au VDA. Le VDA utilise ensuite `1E` pour afficher le caractère ф.

Si vous choisissez Unicode et que vous appuyez sur la touche à côté de Verr Maj, le caractère `a` est envoyé au VDA. Ainsi, même si le VDA utilise la disposition du clavier russe, le caractère `a` apparaît à l'écran.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

Prise en charge des dispositions de clavier étendues [version Technical Preview]

À partir de la version 2209 de l'application Citrix Workspace, le mode de saisie du clavier Scancode prend en charge les dispositions de clavier étendues suivantes :

- Clavier japonais 106
- Claviers portugais ABNT/ABNT2
- Claviers multimédia

Le mode de saisie du clavier Scancode prend en charge les dispositions de clavier étendues, ainsi que tous les modes de synchronisation de la disposition du clavier.

Cette prise en charge est activée par défaut.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

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

Description du clavier client Linux	Disposition du clavier client Linux	Variante de clavier client Linux	Synchronisation avec	ID de paramètres régionaux Windows	Disposition du clavier du VDA Windows (ID)	Disposition du clavier du VDA Linux	Variante de clavier du VDA Linux
Arabe	ara	-	→	ar-SA	00000401	ara	-
Arabe (AZERTY)	ara	azerty	→	ar-DZ	00020401	ara	azerty
Allemand (Autriche)	at	-	→	de-AT	00000407	at	-
Belge (alt. ISO)	be	iso-alternate	→	fr-BE	0000080c	be	iso-alternate
Belge	be	-	→	nl-BE	00000813	be	-
Bulgare	bg	-	→	bg-BG	00030402	bg	-
Bulgare (phonétique traditionnelle)	bg	phonetic	→	bg-BG	00040402	bg	phonetic
Bulgare (nouvelle phonétique)	bg	bas_phonetic	→	bg-BG	00020402	bg	bas_phonetic

Description du clavier client Linux	Disposition du clavier client Linux	Variante de clavier client Linux	Synchronisation avec	ID de paramètres régionaux Windows	Disposition du clavier du VDA Windows (ID)	Disposition du clavier du VDA Linux	Variante de clavier du VDA Linux
Portugais (Brésil)	br	-	→	pt-BR	00000416	br	-
Biélorusse	by	-	→	be-BY	00000423	by	-
Anglais (Canada)	ca	eng	→	en-CA	00000409	ca	eng
Canadien multilingue	ca	multix	→	fr-CA	00011009	ca	multix
Français (Canada, ancienne génération)	ca	fr-legacy	→	fr-CA	00000c0c	ca	fr-legacy
Français (Canada)	ca	-	→	fr-CA	00001009	ca	-
Français (Suisse)	ch	fr	→	fr-CH	0000100c	ch	fr
Allemand (Suisse)	ch	-	→	de-CH	00000807	ch	-
Chinois (Simplifié)	cn	-	→	en-US	00000409	us	-
Tchèque	cz	-	→	cs-CZ	00000405	cz	-
Tchèque (QWERTY)	cz	qwerty	→	cs-CZ	00010405	cz	qwerty
Allemand	de	-	→	de-DE	00000407	de	-
Allemand (Macintosh)	de	mac	→	de-DE	00000407	de	mac
Danois	dk	-	→	da-DK	00000406	dk	-

Description du clavier client Linux	Disposition du clavier client Linux	Variante de clavier client Linux	Synchronisation avec	ID de paramètres régionaux Windows	Disposition du clavier du VDA Windows (ID)	Disposition du clavier du VDA Linux	Variante de clavier du VDA Linux
Estonien	ee	-	→	et-EE	00000425	ee	-
Espagnol (Amérique latine)	es	-	→	es-ES	0000040a	es	-
Espagnol (Macintosh)	es	mac	→	es-ES	0000040a	es	mac
Finnois	fi	-	→	fi-FI	0000040b	fi	-
Français	fr	-	→	fr-FR	0000040c	fr	-
Français (Macintosh)	fr	mac	→	fr-FR	0000040c	fr	mac
Anglais (Royaume-Uni)	gb	-	→	en-GB	00000809	gb	-
Anglais (Macintosh)	gb	mac	→	en-GB	00000809	gb	mac
Anglais (Royaume-Uni, étendu, avec touches Win)	gb	extd	→	en-GB	00000452	gb	extd
Grec	gr	-	→	el-GR	00000408	gr	-
Croate	hr	-	→	hr-HR	0000041a	hr	-
Hongrois	hu	-	→	hu-HU	0000040e	hu	-
Irlandais	ie	-	→	en-IE	00001809	ie	-

Description du clavier client Linux	Disposition du clavier client Linux	Variante de clavier client Linux	Synchronisation avec	ID de paramètres régionaux Windows	Disposition du clavier du VDA Windows (ID)	Disposition du clavier du VDA Linux	Variante de clavier du VDA Linux
Hébreu	il	-	→	he-IL	0002040d	il	-
Anglais (Inde, avec roupie)	in	eng	→	en-IN	00004009	in	eng
Irakien	iq	-	→	ar-IQ	00000401	iq	-
Islandais	is	-	→	is-IS	0000040f	is	-
Italien	it	-	→	it-IT	00000410	it	-
Japonais	jp	-	→	en-US	00000409	us	-
Japonais (Macintosh)	jp	mac	→	en-US	00000409	us	mac
Coréen	kr	-	→	en-US	00000409	us	-
Espagnol (Amérique latine)	latam	-	→	es-MX	0000080a	latam	-
Lituanien	lt	-	→	lt-LT	00010427	lt	-
Lituanien (IBM LST 1205-92)	lt	ibm	→	lt-LT	00000427	lt	ibm
Lituanien (Standard)	lt	std	→	lt-LT	00020427	lt	std
Letton	lv	-	→	lv-LV	00020426	lv	-
Norvégien	no	-	→	nb-NO	00000414	no	-
Polonais	pl	-	→	pl-PL	00000415	pl	-
Polonais (QWERTZ)	pl	qwertz	→	pl-PL	00010415	pl	qwertz

Description du clavier client Linux	Disposition du clavier client Linux	Variante de clavier client Linux	Synchronisation avec	ID de paramètres régionaux Windows	Disposition du clavier du VDA Windows (ID)	Disposition du clavier du VDA Linux	Variante de clavier du VDA Linux
Portugais	pt	-	→	pt-PT	00000816	pt	-
Portugais (Macintosh)	pt	mac	→	pt-PT	00000816	pt	mac
Roumain (standard)	ro	std	→	ro-RO	00010418	ro	std
Serbe	rs	-	→	sr-Cyrl-RS	00000c1a	rs	-
Serbe (Latin)	rs	latin	→	sr-Latn-RS	0000081a	rs	latin
Russe	ru	-	→	ru-RU	00000419	ru	-
Russe (machine à écrire)	ru	typewriter	→	ru-RU	00010419	ru	typewriter
Russe (Macintosh)	ru	mac	→	ru-RU	00000419	ru	mac
Suédois	se	-	→	sv-SE	0000041d	se	-
Suédois (Macintosh)	se	mac	→	sv-SE	0000041d	se	mac
Slovène	si	-	→	sl-SI	00000424	si	-
Slovaque	sk	-	→	sk-SK	0000041b	sk	-
Slovaque (QWERTY)	sk	qwerty	→	sk-SK	0001041b	sk	qwerty
Thaï	th	-	→	th-TH	0000041e	th	-

Description du clavier client Linux	Disposition du clavier client Linux	Variante de clavier client Linux	Synchronisation avec	ID de paramètres régionaux Windows	Disposition du clavier du VDA Windows (ID)	Disposition du clavier du VDA Linux	Variante de clavier du VDA Linux
Thaï (Pattachote)	th	pat	→	th-TH	0001041e	th	pat
Tadjik	tj	-	→	tg-Cyrl-TJ	00000428	tj	-
Turc	tr	-	→	tr-TR	0000041f	tr	-
Turc (F)	tr	f	→	tr-TR	0001041f	tr	f
Chinois (traditionnel)	tw	-	→	en-US	00000409	us	-
Ukrainien	ua	-	→	uk-UA	00000422	ua	-
Anglais (États-Unis)	us	-	→	en-US	00000409	us	-
Anglais (Macintosh)	us	mac	→	en-US	00000409	us	mac
Anglais (Dvorak)	us	dvorak	→	en-US	00010409	us	dvorak
Anglais (Dvorak, gaucher)	us	dvorak-l	→	en-US	00030409	us	dvorak-l
Anglais (Dvorak, droitier)	us	dvorak-r	→	en-US	00040409	us	dvorak-r

Description du clavier client Linux	Disposition du clavier client Linux	Variante de clavier client Linux	Synchronisation avec	ID de paramètres régionaux Windows	Disposition du clavier du VDA Windows (ID)	Disposition du clavier du VDA Linux	Variante de clavier du VDA Linux
Anglais (États-Unis, international, avec touches mortes)	us	intl	→	nl-NL	00020409	us	intl
Vietnamien	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 une restriction concernant les types de fichiers reconnus par l'application Citrix Workspace. Uniquement lorsqu'une application publiée est associée au type de fichier du fichier publié, les cas suivants s'appliquent :

- Le système reconnaît le type de fichier du contenu publié.

- Les utilisateurs peuvent afficher le fichier via l'application Citrix Workspace.

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. Vérifiez 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>
<!--NeedCopy-->
```

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. Vérifiez que le fichier que vous essayez d'ouvrir est activé pour le mappage de lecteur client (CDM).
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 “%**” au 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 l’association de type de fichier côté client.

> **Remarque :**
>
> L’association de type de fichier StoreFront doit être sur ON. Par défaut, l’association de type de fichier est activée.

Prise en charge de Citrix Analytics

À compter de la version 2006, l’application Citrix Workspace est mise à jour 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.

L’application Citrix Workspace pour Linux est conçue pour transmettre en toute sécurité les journaux à Citrix Analytics lorsque l’application déclenche certains événements. Lorsque la fonction est activée, les journaux sont analysés et stockés sur les serveurs Citrix Analytics. 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 ou Citrix DaaS et les serveurs hôtes. Le protocole TUI transmet les messages des composants de l’interface utilisateur [UI] 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`.

À partir de la version 1912, l'indicateur **VDTUI** est 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. 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.

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

Authentification

October 10, 2022

À partir de l'application Citrix Workspace 2012, vous pouvez afficher la boîte de dialogue d'authentification dans l'application Citrix Workspace et stocker les détails sur l'écran de connexion. Cela permet d'obtenir d'optimiser l'expérience.

Les jetons d'authentification sont cryptés et stockés 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 :

Installez 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 `AuthManLiteEnabled` sur **True**.

Amélioration de l'authentification pour Storebrowse

> **Remarque :**
>
> À partir de la version 2205, cette fonctionnalité est généralement disponible pour l'application Citrix Workspace.

À partir de la version 2203, la boîte de dialogue d'authentification est présente dans l'application Citrix Workspace et les détails du magasin s'affichent sur l'écran d'ouverture de session pour une meilleure expérience utilisateur. Les jetons d'authentification sont chiffrés et stockés. Ainsi, vous n'avez pas besoin de saisir de nouveau les informations d'identification lorsque votre système ou votre session redémarre.

L'amélioration de l'authentification prend en charge storebrowse pour les opérations suivantes :

- `Storebrowse -E` : répertorie les ressources disponibles.
- `Storebrowse -L` : lance une connexion à une ressource publiée.
- `Storebrowse -S` : dresse la liste des ressources auxquelles vous avez souscrit.
- `Storebrowse -T` : met fin à toutes les sessions du magasin spécifié.
- `Storebrowse -Wr` : reconnecte les sessions déconnectées mais actives du magasin spécifié. L'option [r] reconnecte toutes les sessions déconnectées.
- `storebrowse -WR` : reconnecte les sessions déconnectées mais actives du magasin spécifié. L'option [R] reconnecte toutes les sessions déconnectées et actives.
- `Storebrowse -s` : abonne la ressource spécifiée à partir d'un magasin donné.
- `Storebrowse -u` : annule l'abonnement de la ressource spécifiée dans un magasin donné.
- `Storebrowse -q` : lance une application à l'aide de l'URL directe Cette commande fonctionne uniquement pour les magasins StoreFront.

> **Remarque :**
>
> - Vous pouvez continuer à utiliser les commandes Storebrowse restantes comme précédemment (en utilisant AuthManagerDaemon).
> - L'amélioration de l'authentification s'applique uniquement aux déploiements dans le cloud.
> - Grâce à cette amélioration, la fonction de connexion permanente est prise en charge.

Amélioration de l'authentification pour la configuration Storebrowse

Par défaut, la fonction d'amélioration de l'authentification est désactivée.

Si gnome-keyring n'est pas disponible, le jeton est stocké dans la mémoire du processus Selfservice.

Pour forcer le stockage du jeton en mémoire, désactivez gnome-keyring en suivant les étapes suivantes :

1. Accédez à `/opt/Citrix/ICAClient/config/AuthmanConfig.xml`.
2. Ajouter l'entrée suivante :

```
<GnomeKeyringDisabled>true</GnomeKeyringDisabled>
<!--NeedCopy-->
```


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 suivante :

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 ligne.

> **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 absolu commençant par « / ».

Après avoir supprimé une carte à puce, configurez le comportement de l'application Citrix Workspace en mettant à jour `SmartCardRemovalAction` 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 and Desktops ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service).

- 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.

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.

Améliorations apportées à la prise en charge des cartes à puce

> **Remarque :**
>
> Cette fonctionnalité est généralement disponible pour l'application Citrix Workspace.

À compter de la version 2112, l'application Citrix Workspace prend en charge la fonctionnalité Plug and Play pour le lecteur de carte à puce.

Lorsque vous insérez une carte à puce, le lecteur de carte à puce la détecte dans le serveur et le client.

Vous pouvez utiliser la fonctionnalité Plug and Play sur différentes cartes en même temps, et elles seront toutes détectées.

Conditions préalables :

Installez la bibliothèque `libpcscd` sur le client Linux.

> **Remarque :**
>
> Cette bibliothèque peut être installée par défaut dans les versions récentes de la plupart des distributions Linux. Cependant, il se peut que vous deviez installer la bibliothèque `libpcscd` dans des versions antérieures de certaines distributions Linux, telles qu'Ubuntu 1604.

Pour désactiver cette amélioration :

1. Naviguez jusqu'au dossier `<ICAROOT>/config/module.ini`.
2. Accédez à la section `SmartCard`.
3. Définissez le `DriverName=VDSCARD.DLL`.

Prise en charge de l'authentification multifacteur (nFactor)

L'authentification multifacteur améliore la sécurité d'une application en exigeant des utilisateurs qu'ils fournissent d'autres 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, consultez Authentification SAML et Authentification multifacteur (nFactor) dans la documentation de Citrix ADC.

Prise en charge de l'authentification à l'aide de FIDO2 [Technical Preview]

Avec cette version, vous pouvez vous authentifier auprès d'applications ou de bureaux virtuels à l'aide de clés de sécurité FIDO2. Les clés de sécurité FIDO2 permettent aux employés de l'entreprise de s'authentifier auprès d'applications ou de bureaux prenant en charge FIDO2 sans entrer de nom d'utilisateur ou de mot de passe. Pour plus d'informations sur FIDO2, consultez Authentification FIDO2.

> **Remarque :**
>
> Si vous utilisez l'appareil FIDO2 via la redirection USB, supprimez la règle de redirection USB de votre appareil FIDO2 du fichier `usb.conf` du dossier `$ICAROOT/`. Cette mise à jour vous permet de passer au canal virtuel FIDO2.

Par défaut, l'authentification FIDO2 est désactivée. Pour activer l'authentification FIDO2, procédez comme suit :

1. Naviguez jusqu'au dossier `<ICAROOT>/config/module.ini`.
2. Accédez à la section `ICA 3.0`.
3. Définissez le `FIDO2= On`.

Cette fonctionnalité prend actuellement en charge les authentificateurs itinérants (USB uniquement) avec code PIN et fonctionnalités tactiles. Vous pouvez configurer l'authentification basée sur les clés de sécurité FIDO2. Pour plus d'informations sur les conditions préalables et l'utilisation de cette fonctionnalité, consultez Autorisation locale et authentification virtuelle à l'aide de FIDO2.

Lorsque vous accédez à une application ou à un site Web prenant en charge FIDO2, une invite s'affiche demandant l'accès à la clé de sécurité. Si vous avez préalablement enregistré votre clé de sécurité avec un code PIN (un minimum de 4 et un maximum de 64 caractères), vous devez saisir le code PIN lors de la connexion.

Si vous avez préalablement enregistré votre clé de sécurité sans code PIN, il vous suffit de toucher la clé de sécurité pour vous connecter.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

Sécuriser les communications

September 28, 2022

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 and Desktops ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) 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 and Desktops ou Citrix DaaS : 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. Ce service permet également aux administrateurs de contrôler, de manière détaillée, l'accès des utilisateurs aux bureaux et aux 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 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 ou Citrix DaaS.

L'application Citrix Workspace prend en charge le protocole SOCKS, ainsi que les éléments suivants :

- Citrix Secure Web Gateway et le Relais SSL Citrix, le protocole proxy sécurisé
- Authentification Stimulation/Réponse Windows NT (NTLM)

La liste des types de proxy pris en charge est limitée aux types Auto, None et Pad 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 chiffrement 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. Si vous utilisez Secure Web Gateway en mode **Normal**, l'application Citrix Workspace ne nécessite aucune configuration.

Si Citrix Secure Web Gateway Proxy est installé sur un serveur dans le réseau sécurisé, vous pouvez l'utiliser en mode Relais. 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.

> **Remarque :**
>
> Citrix Secure Web Gateway version 2.0 ne prend pas en charge le mode Relais.

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 and Desktops ou Citrix DaaS 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

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 compter de la version 2203, la version TLS maximale prise en charge est 1.3.

Vous pouvez contrôler les versions du protocole TLS qui peuvent être négociées en ajoutant les options de configuration suivantes dans la section [WFClient]:

- MinimumTLS=1.1
- MaximumTLS=1.3

Il s'agit des valeurs par défaut, qui sont implémentées en code. Modifiez-les comme bon vous semble.

> **Remarques :**
>
> - 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.
> - TLS 1.0/1.1 fonctionne uniquement avec l'ancien VDI ou Citrix Gateway qui les prend en charge.

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 configuration après le démarrage de self-service ou storebrowse, vous devez taper :
> **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**

Mise à jour de CryptoKit

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

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

TLS v1.3 prend en charge les suites de chiffrement suivantes :

- TLS_AES_128_GCM_SHA256 (0x1301)
- TLS_AES_256_GCM_SHA384 (0x1302)

> **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, voir 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, consultez Suites de chiffrement.

Les suites de chiffrement avec le préfixe TLS_RSA_ ne proposent pas la fonctionnalité Forward Secrecy 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 ou Citrix DaaS, l'application Citrix Workspace 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

> **Remarque :**
>
> Toutes les suites de chiffrement précédentes 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.

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 obtenir des instructions de dépannage, consultez les articles suivants du Centre de connaissances :

- CTX260336
- CTX231524
- CTX203362

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 qui installe 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 les machines 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`

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.

À partir de la version 2103 de l'application Citrix Workspace, lorsque la fiabilité de session est activée, EDT et TCP sont tentés en parallèle lors des opérations suivantes :

- Connexion initiale
- Reconnexion de la fiabilité de session
- Reconnexion automatique des clients

Cette amélioration réduit le temps de connexion lorsque EDT est le mode préféré. Toutefois, le transport UDP sous-jacent requis n'est pas disponible et TCP doit être utilisé.

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

Découverte MTU EDT (Enlightened Data Transport)

L'application Citrix Workspace version 2109 prend désormais en charge la découverte MTU (unité de transmission maximale) dans Enlightened Data Transport (EDT). Cela augmente la fiabilité et la compatibilité du protocole EDT et optimise l'expérience utilisateur.

Pour de plus amples informations, consultez la section Découverte MTU EDT dans la documentation de Citrix Virtual Apps and Desktops.

Prise en charge de IPv6 EDT

À partir de la version 2203 de l'application Citrix Workspace, EDT IPv6 est pris en charge.

Storebrowse

July 18, 2022

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.

Amélioration apportées à l'utilitaire Storebrowse pour la continuité du service

Auparavant, les fichiers de location de connexion Workspace étaient synchronisés avec les fichiers disponibles sur le serveur distant uniquement si vous étiez connecté à l'aide de Self-Service Plug-in. Par conséquent, la fonctionnalité de continuité du service n'était pas prise en charge lorsque vous lanciez des applications ou des sessions de bureau à l'aide de Storebrowse. La plupart des fournisseurs de clients légers tiers utilisent Storebrowse pour se connecter à la plate-forme Workspace ; cependant, la fonctionnalité de continuité du service n'était pas été activée pour ces fournisseurs.

À partir de la version 2109 de l'application Citrix Workspace, les fichiers de location de connexion Workspace sont synchronisés avec les fichiers disponibles sur le serveur distant lorsque vous vous connectez également à l'aide de storebrowse. Cette fonctionnalité aide les fournisseurs de clients légers tiers à accéder à Workspace même en mode hors connexion.

> **Remarque :**
>
> - Cette amélioration n'est disponible que lorsque la continuité du service est activée dans les déploiements cloud. Pour plus d'informations, consultez la section Configurer la continuité du service dans la documentation de Citrix Workspace.
> - Cette amélioration n'est pas disponible si vous avez défini la valeur `AuthManLiteEnabled` sur **True** dans le fichier `$ICAROOT/config/AuthManConfig.xml`. Par défaut, cette valeur est définie sur **False**.

Utilisation des commandes

La section suivante détaille les commandes storebrowse que vous pouvez utiliser à partir de l'utilitaire storebrowse.

Ajouter un magasin

`-a, --addstore`

Description :

Ajoute un 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.

Aide

`-?, -h, --help`

Description :

Fournit des détails sur l'utilisation de l'utilitaire storebrowse.

Répertorier les magasins

`-l --liststore`

Description :

Répertorie les magasins que vous avez ajoutés.

Exemple de commande sur StoreFront :

```
./storebrowse -l
```


Énumération

`-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 de StoreFront :

- `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -E -M https://my.firstexamplestore.net/Citrix/Store/discovery`

Abonné

`-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 de StoreFront :

- `./storebrowse.exe -S https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -S -M https://my.firstexamplestore.net/Citrix/Store/discovery`

Détails

`-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 de StoreFront :

```
./storebrowse.exe -S -M 0x264 https://my.firstexamplestore.net/Citrix/Store
/discovery
```

Dans l'exemple de commande précédent, 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.

Subscribe

```
-s --subscribe
```

Description :

Abonne la ressource spécifiée à partir d'un magasin donné.

Exemple de commande de StoreFront :

```
./storebrowse -s <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

Unsubscribe

```
-u --unsubscribe
```

Description :

Annule l'abonnement de la ressource spécifiée dans un magasin donné.

Exemple de commande de StoreFront :

```
./storebrowse -u <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

Launch

```
-L --launch
```

Description :

Lance une connexion à une ressource publiée. L'utilitaire se ferme automatiquement, et la session reste connectée.

Exemple de commande de StoreFront :

```
./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```


Icônes

```
-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 de StoreFront :

- `./storebrowse -E -i best https://my.firstexamplestore.net/Citrix/Store/discovery`

- `./storebrowse -S -i 16x16 https://my.firstexamplestore.net/Citrix/Store/discovery`

Reconnect session

`-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 de StoreFront :

- `./storebrowse -Wr https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -WR https://my.firstexamplestore.net/Citrix/Store/discovery`

Disconnect session

`-WD --disconnect`

Description :

Déconnecte toutes les sessions du magasin spécifié.

Exemple de commande de StoreFront :

`./storebrowse -WD https://my.firstexamplestore.net/Citrix/Store/discovery`

Terminate session

`-WT --terminate`

Description :

Met fin à toutes les sessions du magasin spécifié.

Exemple de commande de StoreFront :

`./storebrowse -WT https://my.firstexamplestore.net/Citrix/Store/discovery`

Version

```
-v --version
```

Description :

Affiche la version de l'utilitaire storebrowse.

Exemple de commande de StoreFront :

```
./storebrowse -v
```

Root directory

```
-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 de StoreFront :

```
./storebrowse -r /opt/Citrix/ICAClient
```

Username, Password, Domain

```
-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 de StoreFront :

```
./storebrowse -E https://my.firstexamplestore.net/Citrix/Store/discovery -U
 user1 -P password -D domain-name
```

Delete store

```
-d --deletestore
```

Description :

Annule l'enregistrement d'un magasin auprès du démon ServiceRecord.

Exemple de commande de StoreFront :

```
./storebrowse -d https://my.firstexamplestore.net/Citrix/Store/discovery
```


Configure self-service

```
-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 de StoreFront :

```
./storebrowse -c SharedUserMode=True
```

Add CR file

```
-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 de StoreFront :

```
./storebrowse -C <path to CR file>
```

Synchroniser les fichiers de location de connexion

```
-o --synclease
```

Description :

Commence à synchroniser les fichiers de location de connexion Workspace avec les fichiers disponibles sur le serveur distant pour le magasin spécifié. Cette commande permet de mettre à jour le magasin par défaut et déclenche la synchronisation du fichier de location. Une erreur apparaît si la continuité du service est désactivée.

Commande :

```
./storebrowse -o *URL of Store *
```

Exemple de commande de StoreFront :

```
./storebrowse -o https://my.firstexamplestore.net
```


Close storebrowse daemon

`-K --killdaemon`

Description :

Arrête le processus de démon storebrowse. Toutes les informations d'identification et tous les jetons sont alors effacés.

Exemple de commande de StoreFront :

```
./storebrowse -K
```

List error codes

`-e --listerrorcodes`

Description :

Répertorie les codes d'erreur enregistrés.

Exemple de commande de StoreFront :

```
./storebrowse -e
```

Store gateway

`-g --storegateway`

Description :

Définit la passerelle par défaut pour un magasin qui est déjà enregistré auprès du démon ServiceRecord.

Exemple de commande de 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.

Quick launch

`-q, --quicklaunch`

Description :

Lance une application à l'aide de l'URL directe. Cette commande fonctionne uniquement pour les magasins StoreFront.

Exemple de commande de StoreFront :

```
.\storebrowse.exe -q <https://my.firstexamplestore.net/Citrix/Store/resources
/v2/Q2hJkOlmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix
/Store/discovery>
```

Daemonize

```
-n --nosingleshot
```

Description :

Exécute toujours le démon pour le processus storebrowse.

Exemple de commande de StoreFront :

```
./storebrowse -n
```

File parameters

```
-F --fileparam
```

Description :

Lance un fichier avec le chemin d'accès du fichier et la ressource spécifiés.

Exemple de commande de 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 ferme le démon storebrowse. Si vous ne mentionnez pas explicitement cette commande, le processus storebrowse se ferme au bout d'une heure.

Dépanner

November 2, 2022

Cet article contient des informations destinées à aider les administrateurs à résoudre tous les problèmes rencontrés avec l'application Citrix Workspace.

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 `compat-openssl10` à l'aide de la commande.

   ```
   sudo yum install compat-openssl10.x86_64
   ```

2. 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 Citrix Workspace 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 :
>
> `WaylandEnable=false` dans `/etc/gdm/custom.conf` ou dans `/etc/gdm3/custom.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

La connexion peut échouer lors de la reconnexion à une session avec un nombre de couleurs plus élevé que celui exigé par l'application Citrix Workspace. Cet échec se produit lorsque la mémoire disponible sur le serveur est insuffisante.

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 échouer si la mémoire disponible sur le serveur est toujours insuffisante.

Nom Internet complet

Citrix vous recommande de configurer le serveur de nom de domaine (DNS) sur votre réseau. Cette configuration vous permet de résoudre les noms 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 hostname 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 avancée 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 EDT, 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 EDT 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 plus d'informations, veuillez consulter 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'authentification 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 ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) sur le serveur. Utilisez également la version la plus récente de 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 l'application Citrix Workspace pour Linux ou Citrix Virtual Apps and Desktops ou Citrix DaaS** : 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.

Affichage

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.

Le tearing est évité lorsque les données sont capturées sur le VDA. Le tearing n'est pas introduit lorsque les données sont transmises au client. Cependant, 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 `vsync` pour initier le dessin de

l'image suivante. Selon le matériel graphique du client et le gestionnaire de fenêtres que vous utilisez, les deux groupes de solutions suivants sont disponibles pour empêcher le screen tearing :

- 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"

 Identifier    "Intel Graphics"
 Driver        "intel"
 Option        "AccelMethod" "sna"
 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 crée des icônes de fenêtre compatibles avec la plupart des gestionnaires de fenêtres. Cependant, ces icônes ne sont pas entièrement compatibles 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 entraîner des problèmes d'affichage pour les fichiers suivants :

- Fichiers enregistrés sur le serveur et affichés localement
- Fichiers enregistrés localement et affichés sur le 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 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 spécifique.
- Deux valeurs définissent des écrans situés dans les coins supérieur gauche et inférieur droit de la zone requise.
- Quatre valeurs 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\[,y,z\]\]\]
   ```

   Les valeurs w, x, y et z correspondent aux numéros d'écrans de l'étape 1 des étapes précédentes. La valeur unique w spécifie un écran spécifique. Les deux valeurs w et x définissent des écrans situés dans les coins supérieur gauche et inférieur droit de la zone requise. Les 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 aux sessions d'applications et de bureaux virtuels
   > - 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 peut-être pas sortir d'une session plein écran afin d'utiliser des applications locales ou une autre session Ce problème se produit car l'interface utilisateur du système client est masquée

et la fonctionnalité Transparence du clavier désactive la commande de clavier habituelle, par exemple Alt+Tab, et envoie au lieu de cela la commande au serveur.

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. Avec cette solution, la fonctionnalité Transparence du clavier est désactivée. Toutefois, vous devrez peut-être remplacer le **fichier ICA en ajoutant ce** paramètre dans le fichier All_regions.ini.

Webcam

Mettre à jour la webcam par défaut

Actuellement, la redirection de webcam dans l'application Citrix Workspace pour Linux ne prend en charge qu'une webcam à la fois. La webcam sélectionnée par défaut est mappée sur le chemin du périphérique `/dev/video0` qui est, en général, la webcam intégrée des ordinateurs portables.

Pour répertorier tous les appareils dotés de fonctionnalités vidéo dans le système, vous devez installer les outils v4l à l'aide de la commande suivante :

```
sudo apt-get install v4l-util
<!--NeedCopy-->
```

Listez les périphériques vidéo à l'aide de la commande suivante :

```
v4l2-ctl --list-devices
<!--NeedCopy-->
```

Vous obtiendrez le résultat suivant :

```
user@user-pc:~ $ v4l2-ctl --list-devices
UVC Camera (046d:09a6) (usb-0000:00:14.0-1):
    /dev/video2
    /dev/video3
    /dev/media1
Integrated Camera: Integrated C (usb-0000:00:14.0-8):
    /dev/video0
    /dev/video1
    /dev/media0
<!--NeedCopy-->
```


Comme dans l'exemple précédent, deux webcams sont disponibles. Vous pouvez utiliser n'importe laquelle d'entre elles. Citrix recommande d'utiliser le premier index. Il existe un problème connu avec Ubuntu, de sorte que vous pouvez voir plusieurs index pour une webcam. Dans cet exemple, vous pouvez utiliser /dev/video0 et /dev/video2.

Pour définir une autre webcam par défaut, procédez comme suit :

1. Accédez au fichier de configuration ~/.ICAClient/wfclient.ini et modifiez-le.
2. Dans la section [WFClient], ajoutez le paramètre suivant.

   HDXWebCamDevice=<device path>

Par exemple, ajoutez HDXWebCamDevice=/dev/video2 pour définir la webcam mappée sur /dev/video2 dans un système.

Test des capacités

Sur le client, le module de redirection de Webcam peut être utilisé dans différents modes pour tester des composants isolés dans les conditions de l'environnement du client.

Mode de production et de débogage

Ce mode compare la vidéo affichée côté VDA et les tampons réels produits par l'encodeur du côté client. Il permet de tester l'ensemble du pipeline.

Pour activer ce mode :

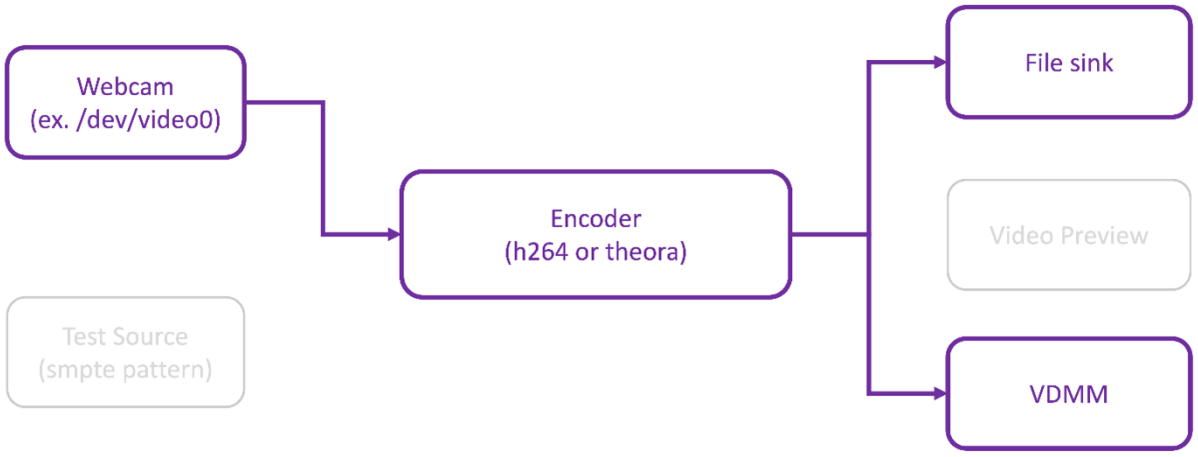
1. Accédez au fichier de configuration ~/.ICAClient/wfclient.ini et modifiez-le.
2. Définissez la valeur HDXWebcamDebug sur **True**.

   HDXWebcamDebug = True

Une fois ce mode activé, l'encodeur génère les fichiers suivants avec les tampons, en fonction de l'encodeur utilisé :

- Pour l'encodeur H264 : /tmp/file_mode_buffers.h264
- Pour l'encodeur Theora : /tmp/file_mode_buffers.theora

Le schéma suivant décrit les modes de production et de débogage :



Mode testeur de Webcam

Ce mode permet de tester la Webcam isolée du reste des éléments du pipeline.

```
./gst_read --buffers | -b BUFFERS_AMOUNT  [ --input_device | -i
   WEBCAM_DEVICE; default=/dev/video0]
<!--NeedCopy-->
```

Pour activer le mode testeur de webcam, exécutez les commandes suivantes à partir des lignes de commande :

```
   cd /opt/Citrix/ICAClient/util
   <!--NeedCopy-->
```

```
   `$./gst_read -b 100 /dev/video0
   <!--NeedCopy-->
```

Une fois ce mode activé, un aperçu vidéo apparaît et crée le fichier suivant avec les tampons bruts de la Webcam :

/tmp/webcam_buffers.buff

Le seul commutateur requis pour le mode testeur de Webcam sont les options `--buffers (-b)`. Vous pouvez également spécifier la Webcam à tester. Par exemple, comme ce qui suit :

- ./gst_read -buffers 150
- ./gst_read –buffers 100 –input_device /dev/video2

Le schéma suivant décrit le mode testeur de Webcam :

Mode testeur d'encodeur

Ce mode permet de tester l'encodeur isolé du pipeline.

```
./gst_read --output_file | -o FILE_NAME [ --buffers | -b BUFFER_AMOUNT; default=10 0 ]  [ --enableH264  | -e ]
<!--NeedCopy-->
```

Pour activer le mode testeur de l'encodeur, exécutez les commandes suivantes à partir des lignes de commande :

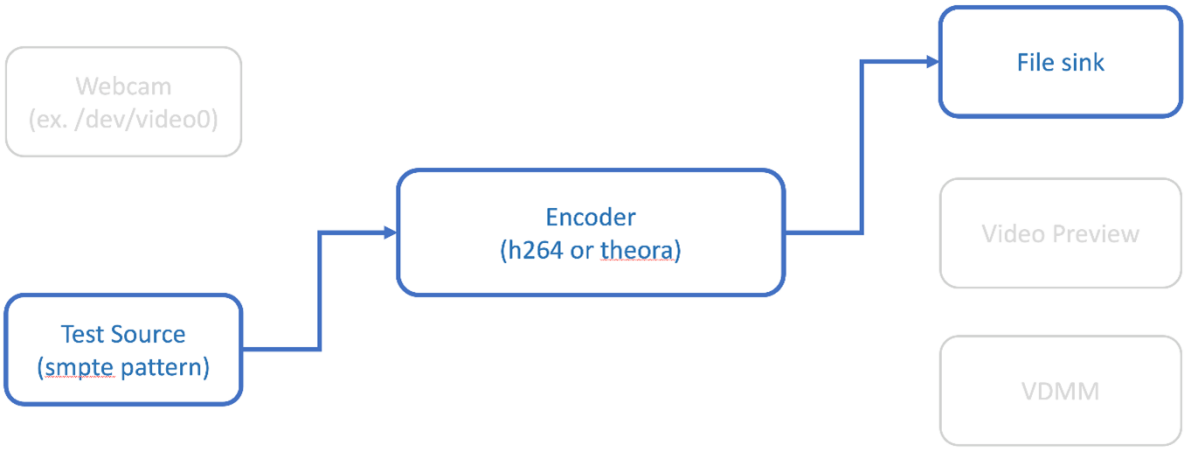
```
cd /opt/Citrix/ICAClient/util
<!--NeedCopy-->
```

```
./gst_read -o ~/file_buffers.h264 -e
 <!--NeedCopy-->
```

Le seul commutateur requis pour ce mode sont les options `--output_file (-o)`. Vous pouvez également tester les encodeurs Theora ou H264 et la quantité de mémoire tampon à générer. Par exemple, comme ce qui suit :

- Pour H264 : ./gst_read –output_file ~/file_buffers.h264 –buffers 200 –enableH264
- Pour Theora : ./gst_read -o ~/file_buffers.theora -b 100

Le diagramme suivant décrit le mode testeur d'encodeur :



Encodeur logiciel H264

Si l'encodeur H264 logiciel ne fonctionne pas correctement, vous devez vérifier ses dépendances en suivant les étapes suivantes :

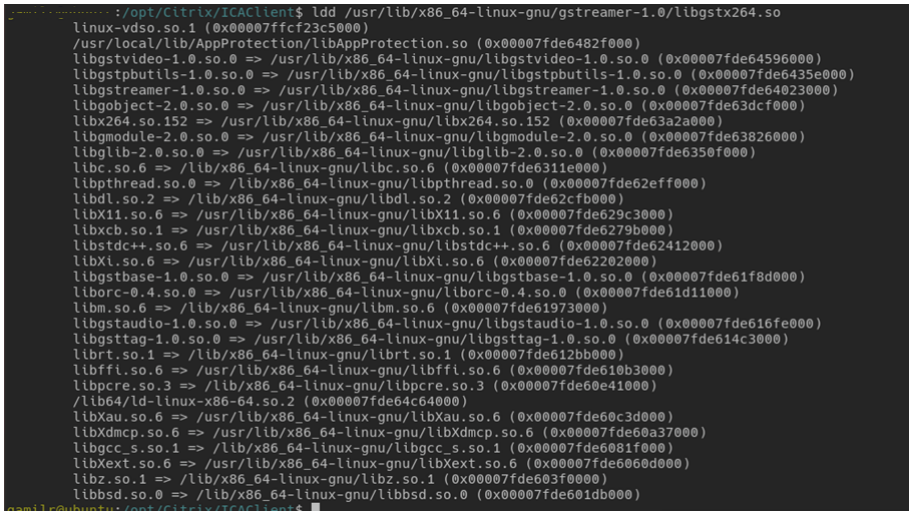
1. Vérifiez que le plug-in `GStreamer` x264 se trouve dans le système et qu'il fait partie de `gstreamer-plugins-ugly`. S'il est disponible dans la bibliothèque `libgstx264.so`, exécutez la commande suivante pour le vérifier :

```
gst-inspect-1.0 x264
<!--NeedCopy-->
```

!Image de vérification de x264 `GStreamer`

2. Exécutez la commande suivante pour vérifier les dépendances de la bibliothèque `libgstx264.so` :

```
ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
<!--NeedCopy-->
```

Si le fichier `libgstx264.so` n'est pas présent, vous devez installer les plugins GStreamer Ugly en utilisant la commande suivante :

```
sudo apt-get install gstreamer1
0-plugins-ugly
<!--NeedCopy-->
```

Encodeur matériel H264

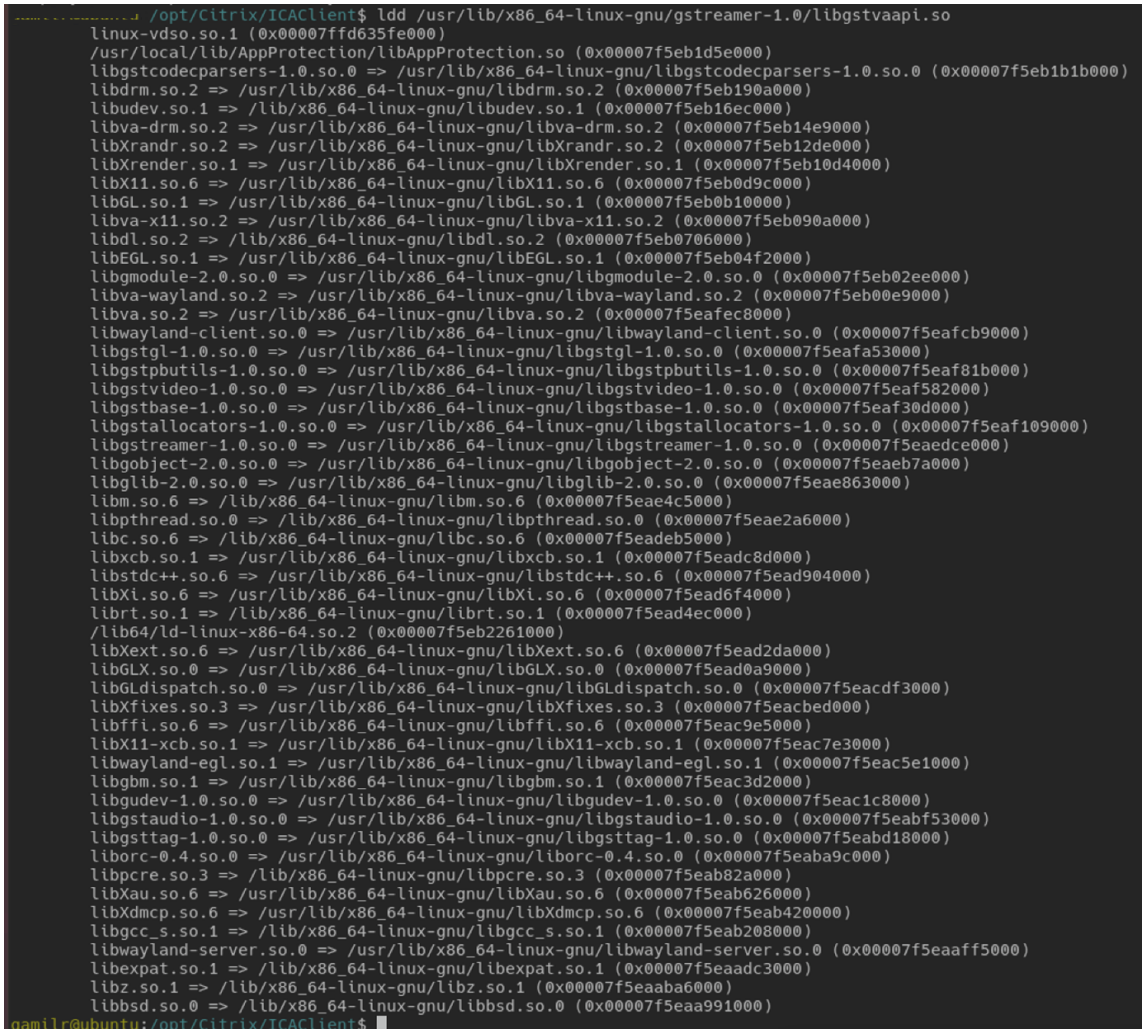
1. Vérifiez que le plug-in `vaapi GStreamer` se trouve dans le système et qu'il fait partie de `gstreamer1.0-vaapi`. S'il est disponible dans la bibliothèque `libgstvaapi.so`, exécutez la commande suivante pour le vérifier :

   ```
   gst-inspect-1.0 vaapi
   <!--NeedCopy-->
   ```

   !Image de vérification de `vaapi GStreamer`

2. Exécutez la commande suivante pour vérifier les dépendances de la bibliothèque libgstvaapi.so :

   ```
       ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstvaapi.so
   <!--NeedCopy-->
   ```

3. Résolvez les dépendances manquantes.

Pour installer et configurer `vaapi`, suivez le guide d'installation de `GStreamer vappi`.

Collecter les journaux des infrastructures GStreamer internes et de gst_read

Au lieu des journaux `ICAClient` standard, vous devez collecter les journaux du module `gst_read`.

Procédez comme suit pour collecter les journaux :

1. Ouvrez un terminal et exécutez les commandes suivantes :

```
export GST_DEBUG=2, gst_read_debug:6
<!--NeedCopy-->
```



```
export GST_DEBUG_FILE=~/gst_read.log
<!--NeedCopy-->
```

> **Remarque :**
>
> Cette variable définit le niveau de journalisation et le fichier dans lequel les stocker. Dans ce cas, nous définissons le niveau 2 pour l'infrastructure `GStreamer` et le niveau 7 pour le module `gst_read`. Pour de plus amples informations, consultez ce document. Il est recommandé de définir uniquement les niveaux d'erreur et d'avertissement pour l'infrastructure `GStreamer` interne et le niveau de journalisation pour `gst_read`.

2. Téléchargez un fichier ICA d'un VDA valide.
3. Sur le même terminal, exécutez la commande suivante pour démarrer une session VDA :

```
cd /opt/Citrix/ICAClient
<!--NeedCopy-->
```

```
./wfica   <ICA file path>/vda.ica
<!--NeedCopy-->
```

Le fichier `gst_read.log` est généré avec l'infrastructure `GStreamer` interne et les journaux `gst_read`.

Inspections des pipelines GStreamer

Pour voir les pipelines actuels créés par l'infrastructure `GStreamer`, procédez comme suit :

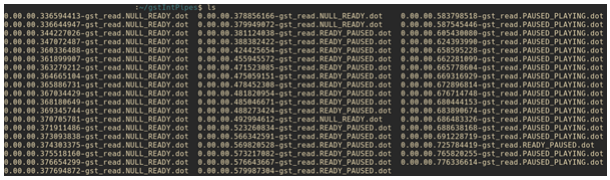
1. Créez un dossier pour stocker les fichiers DOT, par exemple : `gstIntPipes`.
2. Ouvrez un terminal et exportez `GST_DEBUG_DUMP_DOT_DIR=<Absolute path>/gstIntPipes`. Cette variable indique à `GStreamer` où stocker les fichiers DOT.
3. Téléchargez un fichier ICA d'un VDA valide.
4. Sur le même terminal, exécutez les commandes suivantes pour démarrer une session VDA :

```
cd /opt/Citrix/ICAClient/
<!--NeedCopy-->
```



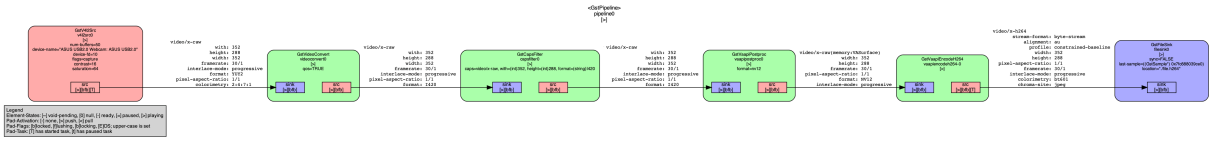
```
./wfica <ICA file path>/vda.ica
<!--NeedCopy-->
```

5. Le répertoire `gstIntPipes` inclut les fichiers DOT. `GStreamer` génère un fichier DOT pour chaque changement d'état dans le pipeline. Par conséquent, vous pouvez inspecter tous les processus de création du pipeline. Voici un exemple d'ensemble de fichiers DOT :

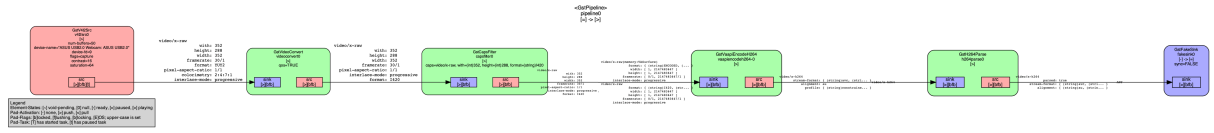


6. Installez un utilitaire de fichiers DOT pour voir une représentation visuelle des pipelines. Par exemple, Graphviz. Les images suivantes sont des exemples de création correcte et incorrecte du pipeline :

Pipeline créé avec succès :



Le pipeline ne peut pas être lié :



> **Remarque :**
>
> Pour agrandir les images précédentes ou toute autre image, cliquez avec le bouton droit sur l'image, sélectionnez **Ouvrir l'image dans un nouvel onglet** et zoomez sur le navigateur selon vos besoins.

Comme le montre l'image précédente, le second pipeline n'est pas en mesure de relier l'élément `GstCapsFilter` et l'élément `GstVaapiEncodeH264`. Les capacités ne sont jamais totalement négociées. Pour de plus amples informations, consultez ce document.

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 redirection

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 and Desktops ou Citrix DaaS 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 du bureau ou de l'élément de menu.
- Vérifiez le fichier Citrix Virtual Apps and Desktops ou Citrix DaaS 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 ce fichier 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 ce fichier 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. Consultez également la section 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 ce fichier sur le serveur, soit vous reconfigurez le navigateur.

Autres

Problèmes de connexion

Vous pouvez également rencontrer les problèmes suivants.

Fermer une session

Pour savoir si le serveur a demandé à l'application Citrix Workspace de fermer une session, utilisez le programme *wfica*. Ce programme consigne une entrée chaque fois qu'il reçoit une commande de fermeture de session en provenance du serveur.

Pour enregistrer ces informations via le système syslog, ajoutez *SyslogThreshold* avec la valeur 6 à la section [WFClient] du fichier de configuration. Ce paramètre 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, veuillez consulter la section Installer et configurer.

  Si l'application Citrix Workspace était installée à l'emplacement par défaut, supprimez le répertoire `/opt/Citrix/ICAClient` ou `$HOME/ICAClient/platform` 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 exemple, 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. Ce paramètre 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. Ce problème 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 l'application Citrix Workspace rejette généralement le format. En conséquence, le serveur demande un autre format ou il restitue le média lui-même.

Dans quelques situations, l'absence d'un plug-in approprié est 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. Ce paramètre 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

Errors

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

April 19, 2022

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 ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service).

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 plus d'informations, veuillez consulter Citrix Virtual Channel SDK 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, consultez la section Citrix Workspace app for Linux Command Reference.

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 ».

Ce SDK permet 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. Ce SDK permet aux développeurs de créer des extensions de plug-in pour le composant de moteur ICA (`wfica`) de l'application Citrix Workspace. 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 plus d'informations, consultez la section Application Citrix Workspace pour Linux - SDK d'optimisation de la plate-forme.

Référence des paramètres ICA

February 11, 2022

Le fichier de référence des paramètres ICA inclut des paramètres de registre et des listes de paramètres de fichiers ICA, permettant aux administrateurs de personnaliser le comportement de l'application Citrix Workspace. Vous pouvez également l'utiliser pour corriger des comportements inattendus de l'application.

Référence des paramètres ICA (PDF)

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