Nouveautés

Jul 10, 2017

Nouveautés dans la version 13.6

Transport adaptatif

- Le transport adaptatif pour XenApp et XenDesktop optimise le transport de données à l'aide d'un nouveau protocole Citrix appelé EDT (Enlightened Data Transport) qui est utilisé à la place de TCP lorsque cela est possible. Comparé à TCP et UDP, EDT offre une expérience utilisateur supérieure sur les connexions WAN et Internet longue distance, tout en assurant une capacité à monter en charge élevée du serveur et une utilisation efficace de la bande passante. EDT repose sur UDP et améliore le transfert de données pour tous les canaux virtuels ICA, y compris la communication à distance d'écran Thinwire, le transfert de fichiers (mappage des lecteurs clients), l'impression, la redirection multimédia, etc. Lorsque UDP n'est pas disponible, le transport adaptatif bascule automatiquement vers TCP. Pour plus d'informations, consultez la section Transport adaptatif.
- Vous devez activer le paramètre de stratégie HDX Adaptive Transport dans Citrix Studio. Vous pouvez le désactiver à partir des paramètres de Receiver.
- Cette fonctionnalité est prise en charge uniquement pour les connexions directes qui ne passent pas par NetScaler Gateway.

Stratégie de validation des certificats de serveur

Citrix Receiver pour Linux 13.6 et versions ultérieures introduit une nouvelle stratégie de validation des certificats de serveur plus stricte, ce qui peut affecter les démarrages de sessions. Pour plus d'informations, consultez Stratégie de validation des certificats de serveur et les articles CTX224709 et CTX221453 du centre de connaissances.

Prise en charge d'un nouveau mode de souris relative

Pour plus d'informations, reportez-vous à la section Souris relative.

Problèmes résolus

Jul 10, 2017

Receiver pour Linux 13.6

Les problèmes suivants ont été résolus depuis la version 13.5 :

Clavier

- Après la mise à niveau vers Citrix Receiver pour Linux 13.5, la saisie au clavier peut ne pas fonctionner dans une session cliente.

  [#LC7591]

Session/Connexion

- Le message d'erreur suivant peut s'afficher lors de l'utilisation de Citrix Receiver pour Linux :

  "The X Request 139.27 caused error: "8: BadMatch (invalid parameter attributes)"."

  [#LC6682]

- Le message d'erreur suivant peut s'afficher lors de l'utilisation de Citrix Receiver pour Linux :

  "The X Request 24.0 caused error: "5: BadAtom (invalid Atom parameter)"."

  [#LC6733]

Receiver pour Linux 13.5

Les problèmes suivants ont été résolus depuis la version 13.4 :

Redirection HDX MediaStream Flash

- Si vous redimensionnez une fenêtre Microsoft Internet Explorer avec la Redirection Flash HDX MediaStream activée, les sites Web avec du contenu Flash peuvent ne pas être redimensionnés en fonction de la taille de la fenêtre Internet Explorer modifiée.

  [#LC6126]

Session/Connexion

- Lorsque vous regardez un clip multimédia dans une session de bureau sur un Client léger HP, le lecteur Windows Media peut générer le message d'erreur suivant :

  « Le Lecteur Windows Media a rencontré un problème lors de la lecture du fichier. »

  Dans certains scénarios, une fenêtre vide ou noire peut s'afficher.

[#LC5508]

- Les menus déroulants des applications publiées peuvent disparaître immédiatement après l'affichage lorsqu'elles sont lancées à partir de Citrix Receiver pour Linux.

  [#LC5574]

- Lorsque vous lancez une session puis que vous annulez la barre de progression de la connexion, le processus wfica peut envoyer un signal SIGTERM à tous les processus du groupe de processus. Les processus peuvent se fermer de manière inattendue lors du partage du groupe de processus.

  [#LC5858]

- Dans un environnement à plusieurs moniteurs, lorsqu'une application transparente est exécutée sur le second moniteur, le fait de basculer entre des espaces de travail dans Gnome 3 peut entraîner la restitution incorrecte de l'application transparente. Le problème se produit lorsque l'option « Espaces de travail uniquement sur l'écran principal » est activée sur Gnome 3.

  [#LC5897]

- Le raccourci clavier « Ctrl+Alt+Suppr » dans la barre d'outils Desktop Viewer peut ne pas fonctionner dans les sessions VDA Linux.

  [#LC6164]

- Lorsque vous tentez de lancer une application en cliquant sur l'icône de bureau correspondant, l'application peut ne pas démarrer.

  [#LC6285]

- Les tentatives de démarrage d'une session dont la prise en charge de l'encodage H.264 est activée sur un VDA Linux peuvent entraîner une erreur segfault dans wfica.

  [#LC6603]

Exceptions système

- Les tentatives de connexion à certains sites XenApp ou XenDesktop peuvent entraîner la fermeture inattendue de AuthManagerDaemon.

  [#LC6166]

Expérience utilisateur

- Lorsque vous lancez une application transparente qui contient plusieurs fenêtres enfants, il se peut que vous ne puissiez pas déplacer certaines fenêtres enfants. Il est aussi possible que vous ne puissiez pas modifier le focus de ces fenêtres.

  [#LC4342]

- Lorsque vous vous déconnectez d'un bureau local alors que la boîte de dialogue de saisie des informations d'identification en libre-service est ouverte, les autres tentatives de connexion au libre-service peuvent échouer et le libre-service peut ne jamais progresser au-delà de la boîte de dialogue d'authentification.

[#LC4939]

- Lorsque vous lancez Microsoft Excel en mode transparent, il arrive parfois que le focus clavier ne se déplace pas sur la fenêtre « Rechercher » dans l'application.

  [#LC5964]

Interface utilisateur

- Les icônes « Sametime » peuvent ne pas s'afficher dans la zone de notification lors de l'utilisation de Citrix Receiver pour Linux.

  [#LC3956]

- Lorsque vous déplacez la fenêtre de conversation de Microsoft Lync vers une nouvelle position, il est possible que la fenêtre ne soit pas redessinée complètement.

  [#LC5583]

- Les tentatives de déplacement de la fenêtre « Rechercher » dans Microsoft Excel lancé en mode transparent peuvent échouer.

  [#LC5963]

- Lors de la réduction d'une fenêtre enfant (par exemple, la fenêtre principale de Spy ++ est la fenêtre parente et la fenêtre de détection de fenêtres spécifiées est la fenêtre enfant), la taille de la barre de titre réduite peut s'afficher en plus petit.

  [#LC6210]

Receiver pour Linux 13.4

Les problèmes suivants ont été résolus depuis la version 13.3 :

Problèmes liés aux machines clientes

- Lorsque le mappage de lecteur client est activé, l'accès aux lecteurs mappés peut parfois prendre plus de temps que prévu.

  [#LC3930]

Améliorations

- Cette version prend en charge l'utilisation d'une souris relative, une fonctionnalité 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 XenApp ou XenDesktop 7.8. 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.
Cela met la fonctionnalité en service tout en la gardant inactive jusqu'à ce que vous l'activiez.

- Pour activer la fonctionnalité :

Tapez Ctrl/F12.
Une fois que la fonctionnalité est activée, tapez de nouveau sur Ctrl/F12 pour synchroniser la position du pointeur de la souris avec le client (les positions du pointeur du client et du serveur ne sont pas synchronisées lors de l'utilisation de la souris relative).

- Pour désactiver la fonctionnalité :

Tapez Ctrl-Maj/F12.
La fonctionnalité est également désactivée lorsqu'une fenêtre de session perd le focus.

* 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.

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

RelativemouseOnChar=F11
RelativeMouseOnShift=Shift
RelativemouseOffChar=F11
RelativeMouseOffShift=Shift

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 Citrix Receiver. Les valeurs pour RelativeMouseOnShift et RelativeMouseOffShift définissent les touches de modification à utiliser et sont répertoriées sous l'en-tête [Hotkey Shift States].

[#LC5000]

Ouverture de session/Authentification

- La version 13.3 de Citrix Receiver pour Linux ne parvient pas à transmettre certains paramètres de ligne de commande, y compris l'option -clearpassword, à des versions anciennes de XenApp. Par conséquent, les tentatives de connexion des utilisateurs se soldent par un échec.

  [#LC4594]

Session/Connexion

- Les tentatives de lancement d'une session utilisateur en mode plein écran à l'aide de l'option de ligne de commande « -span » peuvent échouer.

  [#LC3394]

- Après le redimensionnement du second moniteur dans une configuration à double moniteur, la barre des tâches de Windows peut ne pas réussir à revenir sur son emplacement d'origine.

  [#LC3856]

- Une erreur segfault dans wfica peut entraîner la déconnexion ou le blocage des sessions durant les mises à jour de l'écran qui résultent d'activités telles que la mise en surbrillance ou le défilement.

  [#LC3947]

- Lors de la reconnexion à une session multi-écran sur Ubuntu 14.04, la fenêtre de session s'affiche sur un seul écran au lieu de s'afficher sur tous les écrans.

  [#LC4181]

- Les tentatives de connexion à un magasin anonyme peuvent échouer avec les messages d'erreur suivants :

  « NoWebUIAuth 0 » et « Impossible de traiter votre demande »

  [#LC4270]

- Les tentatives de lancement d'un bureau publié peuvent échouer lors de l'utilisation d'un hôte proxy SSL tel que le Relais SSL.

  [#LC4739]

- Une instance publiée d'Internet Explorer peut perdre le focus et être dupliquée lorsqu'une fenêtre contextuelle s'affiche dans la fenêtre de navigateur d'origine.

  [#LC5066]

Cartes à puce

- Lors de l'utilisation d'une carte à puce avec pnabrowse, le code PIN ne peut pas être transmis au VDA et l'authentification peut échouer. La session est lancée mais l'écran de connexion s'affiche.

  [#LC4241]

Exceptions système

- Après la lecture de multimédia avec le Lecteur Windows Media sur un client Linux basé sur ARM hf, les sessions se déconnectent.

  [#LC4625]

Expérience utilisateur

- La qualité audio du micro dans les sessions exécutées sur XenApp/XenDesktop 7.6 peut être médiocre.

  [#LC3124]

- Dans les implémentations ARM hf, il arrive parfois que la barre des tâches ne clignote pas pour indiquer la présence de nouveaux messages Lync 2010.

  [#LC3688]

- Après le déverrouillage d'une session utilisateur dans une configuration multi-écran, il est possible que la position des fenêtres réduites ne soit pas rétablie correctement et les fenêtres semblent ne pas répondre.

  [#LC3984]

- Lorsque vous lancez une application sur un poste Gnome 3 et que vous maximisez l'application, la position du curseur de la souris peut être décalée d'une distance correspondant à la barre supérieure de Gnome 3.

  [#LC4738]

- La redirection de la webcam ne fonctionne pas toujours dans les sessions exécutées sur les VDA version 7.6.

  [#LC4751]

Interface utilisateur

- La fonction Copier/coller échoue parfois d'un serveur à un autre, et d'un serveur à une machine utilisateur.

  [#LC4157]

- Le curseur de la souris disparaît lors de la lecture d'une vidéo en plein écran et ne réapparaît pas tant que la vidéo reste en plein écran.

  [#LC4428]

- Une erreur de type faute de segment peut se produire lorsque certaines applications publiées tierces génèrent une boîte de dialogue. Le curseur n'est plus visible lorsque vous essayez de vous reconnecter à une application qui s'est fermée de manière inattendue.

  [#LC4955]

Receiver pour Linux 13.3

Les problèmes suivants ont été résolus depuis la version 13.2 :

Session/Connexion

- Après le rétablissement d'une fenêtre en mode transparent agrandie, certaines parties du bureau ne sont pas actualisées automatiquement. Cela se produit uniquement dans certains environnements de bureau, tels que Ubuntu 12.04 Unity 2D.

  [#LC0602]

- Lors de l'utilisation du paramètre « ProxyType=Secure », une erreur de segmentation peut se produire.

  [#LC3396]

- Les tentatives de copie et de collage de contenu provenant d'une application publiée vers une application locale peuvent entraîner la fermeture inattendue du processus du composant moteur de ICA (wfica) avec une erreur de segmentation.

  [#LC3480]

- Dans certains cas, la liste des applications mises en cache peut ne plus être synchronisée.

  [#556245]

Exceptions système

- Dans certains cas, l'authentification par carte à puce peut entraîner la fermeture inattendue d'une session.

  [#582550]

Expérience utilisateur

- Grâce à cette correction, les informations relatives au fuseau horaire russe peuvent être mises à jour dans Receiver pour Linux.

  Pour activer cette correction :

  - Pour XenApp 6.5, vous devez installer au minimum le Hotfix Rollup Pack 5 ou des Hotfix Rollup Pack ultérieurs pour rediriger tous les fuseaux horaires correctement.
  - Pour les VDA XenApp et XenDesktop 7.6 exécutés sur des systèmes d'exploitation serveur, vous devez installer la correction ICATS760WX64014.
  - Si le système d'exploitation du serveur est Windows Server 2008 R2 Service Pack 1, vous devez installer la correction la correction Microsoft KB2870165 sur le serveur.
  - Mettez à jour le système d'exploitation du serveur et de la machine utilisateur pour appliquer les dernières informations de fuseau horaire.
  - Vous devez installer le correctif Microsoft KB2998527 pour Windows puis mettre à jour les données de fuseau horaire pour Linux.

  [#LC1971]

Interface utilisateur

- Les icônes des applications publiées peuvent ne pas s'afficher correctement sur la barre des tâches.

  [#LC3405]

- Le icônes dans les sessions de fenêtres transparentes peuvent ne pas s'afficher sur la barre des tâches lors de l'utilisation de plates-formes ARM hard float (armhf).

  [#LC4051]

- Un message de dépendance inapproprié est affiché lors du démarrage de selfservice après l'installation de Citrix Receiver avec un package de distribution tar.gz sur Fedora 21.

  [#582071]

Receiver pour Linux 13.2

Les problèmes suivants ont été résolus depuis la version 13.1 :

HDX Plug and Play

- La webcam risque de ne pas fonctionner avec Citrix GoToMeeting et Cisco WebEx lors de l'utilisation du pack d'optimisation HDX RealTime (Linux) pour Microsoft Lync 2010. Pour activer entièrement ce correctif, vous devez installer une correction pour Receiver pour Linux et une correction pour le pack d'optimisation HDX RealTime (Linux) pour Microsoft Lync 2010 qui contiennent la correction #LA0339.

  Remarque : après l'installation de ce correctif, si vous démarrez Microsoft Lync dans une session VDA alors qu'une

vidéoconférence Citrix GoToMeeting ou Cisco WebEx est en cours d'exécution, la webcam risque de ne pas fonctionner. Si cela se produit, arrêtez et redémarrez la caméra à partir de la vidéoconférence.

[#LC0339]

Ouverture de session/Authentification

- Lorsque les utilisateurs ouvrent une session avec une carte à puce à l'aide de l'interface utilisateur Unicon, les utilisateurs ne peuvent pas énumérer ou démarrer des applications si la carte à puce contient plus de deux certificats et si un seul d'entre eux est un certificat d'authentification. Si la carte à puce contient un certificat client pour l'authentification, les utilisateurs peuvent énumérer et démarrer des applications, toutefois le message d'erreur suivant s'affiche toujours : « Cert Client Authentication OID info set, but unexpected value:... »

  [#LC2098]

Administration d'une batterie/d'un serveur

- Si les connexions avec Receiver pour Linux transitent via un réseau privé virtuel (VPN), Receiver échoue lorsque vous démarrez une application publiée.

  [#LC1284]

- Si vous exécutez la commande « ctx_rehash » pour installer un certificat racine ou intermédiaire sur la machine utilisateur, la création du hachage ou lien correct échoue avec le message d'erreur : « Erreur lors de l'ajout du magasin : AM_ERROR_HTTP_SERVER_CERTIFICATE_NOT_TRUSTED[65150]. » Lorsque cela se produit, Receiver ne peut pas utiliser le certificat et les tentatives d'ajout d'un magasin échouent.

  [#LC1513]

- Avec ce correctif, si l'utilisateur ajoute un magasin en exécutant la commande « $ICAROOT/util/storebrowse --addstore < URL du magasin> » ou en utilisant le Self-Service Plug-in et que le paramètre « découverte » n'est pas inclus dans l'URL, alors le paramètre « découverte » est ajouté automatiquement à l'URL.

  [#LC1517]

Session/Connexion

- Lors de l'agrandissement de la fenêtre d'une application Microsoft Office publiée en mode transparent, la fenêtre est agrandie, mais son contenu peut être décalé et il est possible que le cadre du haut et celui de gauche n'apparaissent pas.

  [#LC0118]

- Dans un environnement comportant plusieurs moniteurs, si le deuxième moniteur est pivoté ou qu'il a une résolution différente, lorsque vous démarrez une application publiée en mode transparent et que vous agrandissez la fenêtre, le serveur n'affiche pas la fenêtre agrandie et cette dernière est inutilisable.

  Pour activer cette correction, dans le fichier $HOME/.ICAClient/wfclient.ini, dans la section [WFClient], ajoutez l'entrée « TWIAvoidFullScreenWhenMaximized =True ».

  [#LC0354]

- Dans un environnement comportant plusieurs moniteurs, si la fenêtre d'une l'application publiée en mode transparent est agrandie et restaurée plusieurs fois, il peut arriver qu'un arrière-plan gris s'affiche sur le deuxième moniteur à la place de la

fenêtre d'application.

[#LC0355]

- Dans un environnement comportant plusieurs moniteurs, le redimensionnement de la fenêtre d'une application publiée en mode transparent dans le deuxième moniteur peut échouer lors de l'utilisation du redimensionnement du côté client.

  [#LC0356]

- Lorsque basculez d'une session de Bureau à distance (RDP) publié à une autre en mode plein écran, telle que mstsc1 et mstsc2, la barre de connexion n'est pas actualisée et affiche mstsc2 comme la fenêtre principale, même après le basculement vers mstsc1.

  [#LC0437]

- Les tentatives de démarrage d'une session en utilisant Receiver pour Linux peuvent provoquer la déconnexion de la session lors du transfert de données en continu par le biais de la redirection USB générique Citrix ou la redirection de lecteur client.

  [#LC0522]

- Lors de la tentative d'ouverture de session à l'Interface Web à l'aide de l'adresse IP, une erreur de segmentation peut se produire et pnabrowse se ferme de manière inattendue.

  [#LC0648]

- Lorsque vous basculez entre une application publiée et Microsoft SQL Server 2012 Management Studio, et que les utilisateurs agrandissent les deux fenêtres puis réduisent uniquement la fenêtre de l'application publiée, la fenêtre de Microsoft SQL Server 2012 Management Studio n'est pas régénérée correctement et certaines parties de la fenêtre ne sont pas actualisées.

  [#LC0739]

- Le focus de la fenêtre reste sur la fenêtre principale au lieu de basculer vers la boîte de dialogue. Par exemple, lorsque vous essayez de fermer une version publiée de Bloc-notes avec le contenu modifié, un message s'affiche pour vous demander si vous souhaitez enregistrer le contenu. La boîte de dialogue du message n'est pas la fenêtre active.

  [#LC0952]

- Receiver pour Linux peut se fermer de manière inattendue lors de la copie d'une image à partir d'une application publiée vers une application locale.

  [#LC1017]

- Les tentatives de démarrage d'une session en utilisant Receiver pour Linux peuvent échouer via Citrix NetScaler Gateway.

  [#LC1103]

- Une fenêtre d'erreur vide peut s'afficher lorsqu'un utilisateur ouvre une application dans une session VDA qui requiert la caméra Web, quand cette dernière est déjà utilisée par une application locale.

  [#LC1135]

- Lorsque vous vous connectez à un VDA XenDesktop 5.6 et que la machine utilisateur est connectée à deux moniteurs,

un problème d'affichage peut se produire dans le second moniteur. En outre, lorsque vous agrandissez la fenêtre dans le second moniteur, la fenêtre peut ne pas s'agrandir entièrement sur l'écran.

[#LC1148]

- Lorsqu'une session est démarrée ou redimensionnée, le plug-in de tampon de trame peut rester sur l'écran.

  [#LC1515]

- Receiver échoue si une adresse URL de serveur proxy automatique est configurée sur la machine utilisateur. L'erreur syslog suivante s'affiche dans le journal :

  Ubuntu1204LTSi386 kernel : [xxxx.xxxxxx] wfica [xxxx] segfault at 2 ip bxxxxxxx sp bxxxxxxx error 4 in libproxy.so[bxxxxxxx+xxxx]

  [#LC1584]

- Lorsque la fiabilité de session est activée et que les données sont transférées en continu par le biais de la redirection USB générique Citrix, la session existante peut se déconnecter.

  [#LC1588]

- La version 64 bits de Receiver pour Linux peut ne pas réussir à enregistrer le plug-in de navigateur.

  [#LC1712]

- Sur les systèmes sur lesquels la correction #LC1127 est installée, Receiver pour Linux 13.1.3 peut cesser de répondre lors de la déconnexion d'une session de bureau publiée par XenDesktop.

  [#LC2365]

- Lorsque les utilisateurs ouvrent une session avec Receiver pour Linux, qu'ils essayent de coller du contenu d'un bureau hébergé publié dans XenApp 5.0, et qu'ils cliquent sur le bouton droit et placent le curseur de la souris sur l'option de collage, la session se déconnecte et une erreur de segmentation peut se produire.

  [#LC2467]

- Lorsque vous êtes connecté avec Receiver pour Web, après le téléchargement du fichier de provisioning (.cr) StoreFront Services et l'exécution de la commande « ./util/storebrowse -C /tmp/receiverconfig.cr », le dialogue « Add Service Record Add Store » ne s'affiche pas et le magasin n'est pas créé.

  [#LC2669]

- Lors de l'utilisation de Receiver pour Linux 13.1, si les utilisateurs cliquent avec le bouton droit sur une icône dans la zone de notification de Windows, la session Receiver peut cesser de répondre et les entrées de clavier et de souris ne fonctionnent pas tant que la session n'est pas fermée et rouverte.

  [#LC2824]

Expérience utilisateur

- Un message d'erreur peut s'afficher lorsque vous parcourez un document volumineux dans Receiver pour Linux. Les utilisateurs doivent répondre au message d'erreur pour continuer à travailler dans la session.

[#LC1127]

- Si la résolution d'écran d'origine d'une machine utilisateur est modifiée au cours d'une session Receiver, la session ne conserve pas le paramètre de plein écran. Par conséquent, la taille de la session peut changer si bien qu'elle ne correspond pas aux résolutions de l'écran d'origine et de l'écran actuel.

  [#LC1222]

- Si le nom de l'icône contient une barre oblique inversée (\), les icônes d'application risquent de ne pas s'afficher correctement dans Receiver pour Linux.

  [#LC1364]

- Les tentatives de copie et de collage de contenu provenant d'applications Java vers des applications publiées peuvent échouer ou c'est le contenu copié précédemment sur le Presse-papiers qui est collé. Le problème se produit lorsque Receiver pour Linux ne parvient pas à synchroniser le Presse-papiers de la machine utilisateur avec les informations du Presse-papiers du serveur.

  [#LC1856]

- Sur un périphérique léger Hewlett-Packard qui utilise le décodeur matériel pour graphiques H.264, dans une session VDA et après le démarrage d'une application dans la session, les tentatives de copie et collage de texte dans les documents ouverts échouent. En outre, la copie de texte échoue d'une fenêtre d'application vers une autre fenêtre d'application qui est en cours d'exécution dans un VDA.

  [#LC2985]

Interface utilisateur

- Si StoreFront est configuré avec un groupe d'agrégation et si le nom de l'application contient une barre oblique inversée (\), le démarrage des applications dans Receiver pour Linux peut échouer. Le message d'erreur suivant s'affiche :

  « Fichier ICA endommagé »

  [#LC1268]

Receiver pour Linux 13.1

Les problèmes suivants ont été résolus depuis la version 13.0 :

Redirection HDX Mediastream Windows Media

- Receiver for Linux 13.0 choisit la sortie Motion JPEG (MJPEG) pour la webcam bien que la sortie YUYV soit disponible.

  [#LA5740]

Redirection HDX MediaStream Flash

- Lorsque HDX MediaStream pour Flash est activé, le rechargement de certaines vidéos Flash dans Internet Explorer peut échouer.

  [#LA4345]

- Lors de lecture d'une vidéo sur YouTube, l'audio et la vidéo peuvent ne pas être lus correctement dans Internet Explorer. Ce problème se produit lorsque les utilisateurs se connectent avec Receiver pour Linux et que la redirection HDX MediaStream Flash est activée.

  [#LA5833]

- Lorsque la redirection HDX Flash est activée et que vous sélectionnez le contrôle de la taille vidéo sur YouTube, la redirection flash est effectuée sur le serveur.

  [#LA5834]

Clavier

- Lorsque vous utilisez des combinaisons comprenant les touches Alt, Maj ou CTRL, ces clés peuvent rester inactives dans une session distante.

  [#LA5730]

- Cette correction résout le problème suivant avec l'interprétation de l'état de la touche Verrouillage des majuscules :

  Lorsque vous déplacez le pointeur de la souris en dehors d'une fenêtre d'application publiée puis que vous revenez dans la fenêtre, et que vous appuyez sur plusieurs touches sur le pavé numérique alors que la touche Verrouillage majuscule est activée, la première touche sur laquelle vous appuyez sur le pavé numérique ne s'affiche pas dans la session.

  [#LC0146]

Session/Connexion

- Lorsque la *Redirection de Presse-papiers client* est activée, la copie et le collage de fichiers dans une session cliente (par exemple, avec l'Explorateur Windows publié en mode fenêtre transparente) peut échouer.
  [#LA5254]

- Les fenêtres d'application publiée sans entrée de barre des tâches ne parviennent pas à prendre le focus sauf si une autre fenêtre d'application existe pour la même application.

  [#LA5617]

- Lors du déplacement d'une fenêtre transparente, il est possible que la fenêtre ne soit pas correctement affichée dans certains scénarios.

  Pour activer cette correction, au choix dans le fichier ~/.ICAClient/wfclient.ini ou le fichier config/All_Regions.ini, ajoutez l'entrée "TWIRedrawAfterMove=TRUE" à la section [WFClient].

  [#LA5669]

- Cette correction améliore le débit de transfert de fichier dans les environnements à latence faible.

  [#LA5725]

- Receiver for Linux 13.0 choisit la sortie Motion JPEG (MJPEG) pour la webcam bien que la sortie YUYV soit disponible.

  [#LA5742]

- Les requêtes DNS qui renvoient de multiples réponses pour une seule recherche, comme c'est souvent le cas dans une

configuration en round-robin, peuvent entraîner l'échec des tentatives de connexion sécurisée et la fermeture inattendue de Receiver.

[#LA5752]

- Lors de la restauration d'une fenêtre qui a été agrandie sur le serveur, la fenêtre locale est restaurée mais le contenu de la fenêtre n'est pas correct et il y a un décalage au niveau de la souris.

  [#LA5926]

- Si vous déplacez la fenêtre d'une application publiée lancée en mode Fenêtre transparente, il est possible que le contenu de la fenêtre soit corrompu. Pour résoudre le problème, procédez comme suit :

  - Sur le serveur, définissez la stratégie « Afficher le contenu de la fenêtre lors d'un cliquer déplacer » sur « Interdit ».
  - Sur la machine utilisateur, dans le fichier « $HOME/wfclient.ini », localisez la section [WFClient] et ajoutez les entrées « TWICoordinateWinPosition=True » et « TWIRedrawAfterMove=True ».

  [#LA5935]

- Les sessions sur des VDA 7.5 avec une stratégie **Affichage visuel** et le paramètre **Qualité visuelle** défini sur une valeur autre que la valeur par défaut (moyenne) peuvent ne pas répondre dès qu'elles sont lancées.

  [#LC0043]

- Les tentatives de connexion à des applications ou bureaux publiés via NetScaler Gateway peuvent échouer et le message d'erreur suivante s'affiche :

  Cannot contact server for application <>.
  Server browser command contains an invalid parameter.
  The server name cannot be resolved.

  Le problème se produit dans les scénarios dans lesquels une Secure Ticket Authority supplémentaire est configurée pour NetScaler Gateway et StoreFront.

  [#LC0059]

- Lors de la tentative d'authentification auprès de l'Interface Web à l'aide d'un ticket Kerberos, une erreur de segmentation peut se produire et pnabrowse se ferme de manière inattendue.

  [#LC0065]

- Lorsque vous appuyez sur Alt+Tab pour passer d'une fenêtre ouverte à une autre et pour ramener la fenêtre d'ouverture de session Remote Desktop au premier plan, la fenêtre ne parvient pas à prendre le focus.

  [#LC0069]

- Lorsque le curseur se trouve dans les limites d'une fenêtre d'application et que vous cliquez sur Alt+Tab, la fenêtre n'est pas toujours ramenée au premier plan.

  [#LC0070]

- Le déplacement d'une fenêtre lancée par Receiver pour Linux peut laisser une ombre derrière-elle.

  [#LA0128]

- Cette correction empêche l'affichage occasionnel d'un message d'erreur injustifié et inattendu indiquant un problème de connectivité et qui présentent les options Quitter et Réessayer aux utilisateurs.

  [#LC0129]

- L'audio UDP peut échouer de manière inattendue quelques minutes après le lancement de la session.

  [#LC0137]

- Les sessions XenDesktop peuvent cesser de répondre lors du transfert de données via un port série avec Receiver pour Linux.

  [#LC0296]

- Lorsque les utilisateurs se connectent avec Receiver pour Linux et le client léger HP t610 exécuté sur un système d'exploitation HP ThinPro 4.4 et que le fuseau horaire est défini sur GMT +8 dans les emplacements suivants, le message d'erreur « Votre fuseau horaire actuel n'est pas reconnu » s'affiche :

  - Singapour
  - Bruneï
  - Makassar
  - Kuala Lumpur
  - Kuching
  - Manille

  [#LC0299]

- Lorsque vous basculez de Microsoft Word à Microsoft Terminal Services Client (MSTSC), le contenu qui s'affiche dans la fenêtre peut être corrompu.

  [#LC0308]

- La commande pnabrowse -WT ne parvient pas à mettre fin à une session de bureau.

  Pour activer cette correction, dans le fichier $HOME/wfclient.ini, dans la section [WFClient], ajoutez l'entrée « LogoffDesktopThroTWI=True ».

  [#LC0345]

- Les tentatives d'interaction avec certaines listes déroulantes peuvent échouer avec Receiver pour Linux.

  [#LC0365]

Observation

- Si la résolution du client Linux est modifiée et qu'une application publiée est lancée à partir du serveur XenApp à l'aide de Receiver pour Linux, l'observateur peut ne pas actualiser son affichage correctement lorsque la session est observée à partir de la console de gestion.

  [#LA5165]

Exceptions système

- Receiver pour Linux peut échouer si vous activez PersistentCacheSize.

[#LC0528]

Divers

- Les packages tarball et RPM ne s'intègrent pas avec GStreamer sur les distributions récentes de Fedora, Red Hat et CentOS AMD (x86_64).

  [#LA4212]

- Si un certificat PKI x.509 avec certaines contraintes de stratégie est installé sur NetScaler Gateway, le lancement d'une application à l'aide de Receiver pour Linux peut échouer avec une erreur SSL 85.

  Pour démarrer des applications, vous devez définir les clés suivantes dans le fichier All_Regions.ini :
  [Network\SSL]
  EnableCertificatePolicyVerification=1

  [#LA5609]

- L'amélioration apportée à cette fonctionnalité ajoute la prise en charge des certificats SHA-2 à Receiver pour Linux.

  [#LC0136]

Receiver pour Linux 13.0

Redirection HDX Mediastream Windows Media

- Lorsque HDX RealTime est activé, une fuite de mémoire peut être observée par le processus gst_read lorsqu'il redirige des données de la webcam.

  [#LA1933]

Clavier

- Lors de la connexion à partir de Receiver pour Linux à un bureau virtuel Windows 7, le message « Verrouillage majuscule activé » sur l'écran d'ouverture de session de Windows 7 peut ne pas refléter avec exactitude l'état de la touche Verr. maj sur le client tant que vous n'appuyez pas sur une touche.

  [#LA1784]

- Lorsque vous basculez entre applications locales et applications publiées, la première touche sur laquelle vous appuyez après avoir appuyé sur Ctrl est ignorée ou une touche autre que celle sur laquelle vous avez appuyé peut s'afficher.

  [#LA3397]

- **Important** : l'installation de cette correction sur des systèmes sur lesquels le correctif #LA1965 est installé entraîne le dysfonctionnement de ce correctif. N'installez pas cette correction sur des systèmes sur lesquels vous avez installé le correctif #1965 car il est nécessaire.

  Certaines touches de raccourci, telles que la combinaison de touches Alt-Tab, peuvent ne pas être envoyées à la session et sont au lieu de cela interprétées par le client.

  Description de la correction #LA1965 :

Lors de la connexion en mode non transparent, il est possible qu'un utilisateur Receiver pour LINUX observe un écran gris clignotant (pendant environ une seconde) avant qu'une application ou un bureau publié ne s'affiche.

[#LA3660]

- Lorsqu'une application publiée est configurée afin d'exécuter une macro sur l'une des touches LED (Verrouillage des majuscules, Verrouillage numérique et Arrêt de défilement), et que vous utilisez l'une de ces touches, la macro est exécutée plusieurs fois.

  Pour activer cette correction, ajoutez l'entrée « BypassSetLED=True » à la section [WFClient] du fichier wfclient.ini figurant dans le dossier ~/.ICAClient. Si le dossier ~/.ICAClient n'existe pas, modifiez le fichier /opt/Citrix/ICAClient/nls/en/wfclient.ini.

  [#LA3825]

- Lors de l'utilisation de la version japonaise de Receiver pour Linux dans une session de bureau virtuel, l'état de la touche Verr. maj sur la barre IME peut être incorrect lorsque vous appuyez sur les touches Maj+Eisu.

  [#LA4072]

- Lors de l'utilisation de Receiver pour Linux dans une session de bureau virtuel sur laquelle l'éditeur IME japonais est installé et sélectionné sur le VDA, vous pouvez observer des différences entre l'état de la touche Verr. maj sur la barre IME et sur le point de terminaison lorsque vous appuyez sur les touches Maj+Eisu.

  [#LA4422]

Session/Connexion

- Dans un environnement multi-écran, Receiver pour Linux peut définir la taille d'une fenêtre agrandie incorrectement dans un second écran. Par conséquent, la taille de la fenêtre peut être supérieure à la taille de l'écran.

  [#LA0663]

- Lors du lancement de IBM Lotus Notes avec une autre application publiée (par exemple, Microsoft Excel) dans une session, toute tentative d'ouverture d'une pièce jointe peut entraîner à tort l'actualisation de la fenêtre de pièce jointe, qui s'affiche par-dessus les autres fenêtres. De ce fait, les instances d'autres fenêtres peuvent s'afficher en tant que rectangle noir (ou une autre couleur d'arrière-plan).

  [#LA1490]

- Lorsque la redirection du fuseau horaire est activée, l'heure affichée et appliquée dans la session peut être conforme à ce qui est prévu. Toutefois, lors de la tentative d'ouverture de Date et heure sur le Panneau de configuration, le message d'erreur suivant s'affiche :

  « Votre fuseau horaire actuel n'est pas reconnu. Sélectionnez un fuseau horaire valide à l'aide du lien ci-dessous. »

  [#LA1828]

- Sur les systèmes sur lesquels le gestionnaire de fenêtres IceWM est installé, la commande **-span o** ne parvient pas à étendre la session sur deux écrans. Au lieu de cela, la session est affichée sur un seul écran.

  [#LA2178]

- Les tentatives d'ouverture d'un fichier dont le nom contient le symbole 5C - Yen (encodage Shift-JIS) à partir d'un périphérique USB mappé du coté client peuvent échouer.

  [#LA2183]

- Cette correction étend le paramètre SucConnTimeout (http://support.citrix.com/proddocs/topic/ica-settings/ica-settings-succonntimeout.html) de façon à ce qu'il soit appliqué non seulement par les applications publiées mais aussi par les bureaux publiés. Par conséquent, les bureaux sont lancés après le nombre de secondes spécifiées par le paramètre SucConnTimeout.

  Pour modifier la valeur du paramètre SucConnTimeout :

  Modifiez la section [WFClient] du fichier ~/.ICAClient/wfclient.ini comme suit :

  ```
  [WFClient]
  Version=2

  SucConnTimeout=60
  KeyboardLayout=(User Profile)
  KeyboardMappingFile=automatic.kbd
  KeyboardDescription=Automatic (User Profile)
  ```

  Si le dossier ~/.ICAClient/ ne figure pas dans le répertoire de base de l'utilisateur, modifiez le fichier /opt/Citrix/ICAClient/nls/en/wfclient.ini comme indiqué ci-dessus. Le fichier sera copié dans le dossier ~/.ICAClient lorsque l'utilisateur se connecte pour la première fois. Vous pouvez également ajouter ApplySucConnTimeoutToDesktops=True à la même section que SucConnTimeout le cas échéant.

  [#LA2679]

- Les tentatives de lancement d'une application publiée à partir de Receiver pour Linux à l'aide d'informations d'identification avec Centrify peuvent échouer.

  [#LA3270]

- Cette amélioration permet à Receiver pour Linux d'accéder en lecture et écriture à des fichiers mappés sur des lecteurs clients qui utilisent le système de fichiers XFS.

  [#LA3610]

- Lors vous basculez d'un espace de travail A vers un espace de travail B et que vous retournez sur l'espace de travail A, la dernière fenêtre a avoir le focus sur cet espace de travail ne récupère pas le focus.

  Remarque : cette correction résout le problème avec les environnements de bureau KDE, Xfce et Gnome. Elle ne fonctionne pas avec les bureaux Unity.

  [#LA3432]

- L'utilisation de pnabrowse dans un environnement comportant plusieurs domaines peut échouer lors de l'utilisation d'un domaine alternatif pour l'authentification utilisateur. Le problème se produit car l'implémentation du code d'origine sépare le nom d'utilisateur et le domaine. Par conséquent, l'utilisation de pnabrowse avec un autre domaine ne fonctionne pas.

À titre d'exemple, un utilisateur peut être référencé en tant qu'utilisateur1@cette.société ou en tant qu'utilisateur1@ce.local (où le domaine principal est *cette.société* et le domaine alternatif est *ce.local*). Cette correction assure le bon fonctionnement dans les deux cas suivants :

> ./pnabrowse -L desk -U utilisateur1 -D cette.société -P société123
> ./pnabrowse -L desk -U utilisateur1@ce.local -P société123

[#LA3551]

- Les canaux virtuels personnalisés peuvent ne pas s'initialiser avec une reconnexion automatique par Receiver pour LINUX.

  [#LA3572]

- Même si l'option « Placer automatiquement le pointeur sur le bouton par défaut dans les boîtes de dialogue » (fonctionnalité qui permet de déplacer le pointeur de la souris sur le bouton par défaut lorsqu'une boîte de dialogue est ouverte) est activée sur le serveur, la fonctionnalité peut ne pas fonctionner correctement dans une application publiée à l'aide de Receiver pour LINUX.

  [#LA4285]

- Le bord droit et la partie inférieure de certaines fenêtres applicatives Java (par exemple, jEdit) en mode transparent peuvent ne pas être régénérés correctement lorsqu'ils sont déplacés ou restaurés.

  Pour activer cette correction, ajoutez l'entrée « TWISetFocusBeforeRestore=True » dans la section [WFClient] du fichier $HOME/.ICAClient/wfclient.ini.

  [#LA4450]

- La redirection de périphérique USB peut être lente dans Receiver pour LINUX dans les déploiements NetScaler.

  [#LA4549]

- Lorsque vous déplacez une fenêtre d'application publiée (par exemple, Token 2) autrement que par sa barre de titre, il est possible que la fenêtre applicative transparente soit réduite.

  Pour activer cette correction, ajoutez l'entrée « TWIMoveResizeHideWindowType=2 » à la section [WFClient] du fichier wfclient.ini.

  [#LA4737]

Exceptions système

- Si vous définissez CommPollSize=On dans module.ini, le processus wfica.exe peut se fermer de manière inattendue.

  [#LA2155]

- Les tentatives d'impression depuis une application Java dans un bureau publié peuvent entraîner la fermeture inattendue de Receiver pour Linux.

  [#LA3321]

- Receiver peut se fermer de manière inattendue lors du collage d'un volume important de données à partir du Presse-papiers.

[#LA3608]

- Receiver peut se fermer de manière inattendue. Le problème se produit lorsqu'une application publiée contient plus de 50 caractères chinois dans la barre de titre.

  [#LA4119]

Expérience utilisateur

- Si vous appuyez sur la touche ALT tout en déplaçant une fenêtre d'application publiée autrement que par sa barre de titre, le contenu de la fenêtre n'est pas déplacé avec le contour de la fenêtre. De plus, lorsque vous relâchez le bouton de la souris, le mouvement de déplacement que vous venez de réaliser est répété.

  [#LA0837]

- Le pointeur de souris peut ne pas être positionné correctement lors de l'agrandissement de la deuxième fenêtre d'écran. Les menus et les boutons peuvent ne pas être activés correctement lorsque vous les survolez avec le pointeur de la souris. Le problème se produit si la résolution verticale en pixels du second écran est inférieure à celle de l'écran principal.

  Exemple : l'écran 1 est défini sur 1920x1080 et l'écran 2 sur 1280x1024 pixels. Lorsque vous lancez une application publiée sur l'écran 1 et que vous déplacez et agrandissez l'application sur l'écran 2, le pointeur de la souris peut être positionné à un centimètre de tout bouton cible. Par conséquent, une info-bulle peut s'afficher pour le bouton Agrandir alors que le pointeur se trouve à un centimètre du bouton.

  [#LA2071]

- Lorsqu'un menu contextuel relatif à l'icône de zone de notification d'une application publiée transparente est ignoré, la zone du menu contextuel n'est pas correctement redessinée et une partie du menu est toujours visible.

  [#LA4139]

Interface utilisateur

- Cette amélioration apportée à l'utilitaire pnabrowse permet d'afficher des icônes à résolution plus élevée pour les ressources publiées.

  [#LA1994]

- Une entrée de barre des tâches appelée « Fenêtre sans titre » peut s'afficher lors du développement d'un menu déroulant dans une application publiée.

  [#LA3422]

Divers

- Cette amélioration vous permet de limiter la redirection USB à partir d'un client donné par utilisateur. Pour limiter la redirection USB pour un utilisateur spécifique, exécutez les commandes suivantes sur le client en tant qu'utilisateur racine ou administrateur :

  1. Supprimez la partie setuid du binaire ctxusb :
     # chmod u-s /opt/Citrix/ICAClient/ctxusb
  2. Insérez un périphérique USB et localisez le périphérique dans le système de fichiers à l'aide de :

ls –lR /dev/bus/usb

3. Attribuez des autorisations à l'utilisateur (par exemple, à l'utilisateur1), où /dev/bus/usb/001/041 correspond au périphérique USB de l'étape 2 :
   # chown user1 /dev/bus/usb/001/041

[#LA1952]

- L'intégration de GStreamer (application tierce) à Citrix Receiver peut échouer avec la version 12.04 de Ubuntu.

  [#LA2016]

- Sur les systèmes 64 bits, par exemple la distribution Ubuntu 64 bits, le script hdxcheck.sh ne parvient pas à localiser les versions 32 bits des bibliothèques suivantes, libpcsclite.so, libcrypto.so, libjpeg.so, libldapsdk.so et libcap.so, ce qui entraîne l'affichage des messages d'avertissement suivants :

  "Warning! - libpcsclite.so missing, check that the file exists.
  Warning! - libcrypto.so is not installed. This is required if you use NTLM proxies.
  Warning! - libjpeg.so is not installed! This is needed for Speedscreen Image and Browser Acceleration.
  Warning! - libldapsdk.so is not installed! This is only needed if you use Novell Netware Services.
  A compatible version of libcap could not be located!"

  Le problème se produit car le script tente de localiser ces bibliothèques uniquement sous /user/lib. Dans les distributions Linux 64 bits, les versions 32 bits de ces bibliothèques peuvent être installées sous /usr/lib/i386-linux-gnu où /lib/i386-linux-gnu/. Avec cette correction, le script tente également de localiser les bibliothèques sous /lib. Si les tentatives sont fructueuses, les messages suivants s'affichent à la place des messages d'avertissement :

  "Success! - Libpcsclite.so installed. Smartcard support enabled.
  Success! All OS dependencies found!
  A compatible version of libcap is installed!"

  [#LA2204]

- Cette amélioration prend en charge l'infrastructure multimédia open source playbin2 sur le HP T510. Pour activer la prise en charge de playbin2, vous devez définir les options suivantes dans le fichier All_Regions.ini :

  SpeedScreenMMAClosePlayerOnEOS=True
  SpeedScreenMMAEnablePlaybin2=True

  [#LA2566]

- Cette correction résout un certain nombre de problèmes rencontrés dans #LA2566, une amélioration qui permet la prise en charge de l'infrastructure multimédia open source playbin2 sur le HP T510.

  [#LA2757]

Problèmes connus

Jul 10, 2017

Problèmes connus avec Citrix Receiver pour Linux 13.6

Les problèmes connus suivants existent dans cette version :

- L'adresse URL de StoreFront n'est pas ajoutée si Citrix Receiver pour Linux est installé dans un chemin d'accès traduit personnalisé qui contient un ou plusieurs caractères à 4 octets.

  [RFLNX-613]

- Lorsque vous mettez à niveau Citrix Receiver, les nouveaux paramètres ne peuvent pas être ajoutés au fichier $HOME/.ICAClient/All_Regions.ini. Le problème se produit car le fichier $HOME/.ICAClient/All_Regions.ini d'un utilisateur est créé à partir d'un modèle lorsque l'utilisateur lance une session pour la première fois. Aucune tentative de modification de la configuration personnelle All_Regions.ini de l'utilisateur n'est effectuée lors de la mise à niveau. Cela signifie que les nouvelles entrées ajoutées au modèle All_Regions.ini ne sont pas automatiquement ajoutées au fichier All_Regions.ini d'un utilisateur existant, et les nouvelles entrées sont bloquées par défaut.

  Pour contourner le problème, si vous n'avez pas modifié le fichier $HOME/.ICAClient/All_Regions.ini d'origine, supprimez-le. La mise à niveau crée un nouveau fichier All_Regions.ini. Si vous avez modifié ce fichier, déplacez-le vers un emplacement de sauvegarde. Établissez une connexion pour entraîner la création du fichier All_Regions.ini à l'aide du modèle le plus récent. Comparez votre version avec le nouveau fichier $HOME/.ICAClient/All_Regions.ini, à l'aide d'outils tels que diff et meld, et importez votre configuration personnelle.

  [RFLNX-706]

- Avec la redirection HDX MediaStream Windows Media avec GStreamer1.0 activé, OpenGL peut entraîner l'affichage inopiné de fenêtres contextuelles sur certaines plates-formes.

  [RFLNX-949]

- Avec la redirection HDX MediaStream Windows Media avec GStreamer1.4 ou version ultérieure activée, en mode de récupération (Fetch) du côté serveur, certains fichiers multimédias (de type MPG1, MPEG2 et H264) ne sont pas lus.

  [RFLNX-952]

- Sur une machine avec ajustement de la fréquence du processeur telle que le Raspberry Pi, si l'audio est saccadé ou que vous rencontrez des problèmes de performance, Citrix vous recommande de définir le gouverneur sur le mode Performance. Pour afficher votre gouverneur Performance actuel pour chaque noyau, exécutez la commande suivante, où est le noyau"

  cat /sys/devices/system/cpu/cpu/cpufreq/scaling_governor

  Par défaut, ce paramètre est un paramètre à la demande, et n'est pas toujours suffisamment dynamique pour fournir les performances en temps-réel que vous souhaitez.
  Pour définir le gouverneur sur le mode Performance, exécutez la commande suivante sous root :

echo performance > /sys/devices/system/cpu/cpu/cpufreq/scaling_governor

Répétez cette commande pour chaque noyau .

[RFLNX-1003]

- Le plug-in du décodeur avec accélération matérielle H264 pour le Pi HDX Ready ne fonctionne pas correctement si vous modifiez la résolution du tampon de trame avec les paramètres framebuffer_width et framebuffer_height dans le fichier /boot/config.txt. Une solution consiste à modifier la résolution du Pi avec les paramètres hdmi_group et hdmi_mode.

  [RFLNX-1049]

- L'installation de la version tar.gz de Citrix Receiver entraîne une erreur de groupe non valide. L'erreur se produit car le système d'exploitation ne dispose pas d'un groupe nommé « sys » et le message d'erreur suivant s'affiche :

  "chgrp: invalid group: sys"

  Pour contourner le problème, exécutez setupwfc avec HOST_SYS_GROUP_NAME défini sur le groupe souhaité.

  HOST_SYS_GROUP_NAME= ./setupwfc

  Puis entrez un nom de groupe pour les fichiers installés.

  [RFLNX-1377]

- Tente de faire échouer une connexion UDT si votre unité de transmission maximale (MTU) de réseau est inférieure à 1500.

  Pour contourner le problème, réduisez la taille des paquets UDP générés. Pour ce faire, réduisez suffisamment la taille de udtMSS de façon à ce que les paquets UDP générés puissent être envoyés sur votre réseau MTU. Pour obtenir davantage d'informations, veuillez consulter l'article CTX224373 du centre de connaissances.

  [RFLNX-1390]

- L'estimation de la bande passante peut ne pas être mise à jour avec les connexions de transport adaptatif. Cela entraîne un comportement erratique des fonctionnalités qui dépendent d'une lecture précise de la bande passante de session. Par exemple :
  - Débit de session global plus faible que prévu, ou en cas de modification des conditions de réseau une fois que la session a été établie (réduction de la bande passante disponible), le client peut essayer d'envoyer plus de données que ce que le réseau peut traiter.
  - Vitesse de transmission codée incorrecte ou inappropriée des graphiques H264.
  - Comportement erratique de la fonction de transcodage de MediaStream.

  [RFLNX-1408]

Problèmes connus dans Citrix Receiver pour Linux 13.5

Les problèmes connus suivants ont été observés dans cette version :

- L'adresse URL de StoreFront n'est pas ajoutée si Citrix Receiver pour Linux est installé dans un chemin d'accès traduit personnalisé qui contient un ou plusieurs caractères à 4 octets.

  [RFLNX-613]

- Avec la redirection HDX MediaStream Windows Media avec GStreamer1.0 activé, OpenGL peut entraîner l'affichage inopiné de fenêtres contextuelles sur certaines plates-formes.

  [RFLNX-949]

- Avec la redirection HDX MediaStream Windows Media avec GStreamer1.4 ou version ultérieure activée, en mode de récupération (Fetch) du côté serveur, certains fichiers multimédias (de type MPG1, MPEG2 et H264) ne sont pas lus.

  [RFLNX-952]

- Sur une machine avec ajustement de la fréquence du processeur telle que le Raspberry Pi, si l'audio est saccadé ou que vous rencontrez des problèmes de performance, Citrix vous recommande de définir le gouverneur sur le mode Performance. Pour afficher votre gouverneur Performance actuel pour chaque noyau, exécutez la commande suivante, où est le noyau"

  cat /sys/devices/system/cpu/cpu/cpufreq/scaling_governor

  Par défaut, ce paramètre est un paramètre à la demande, et n'est pas toujours suffisamment dynamique pour fournir les performances en temps-réel que vous souhaitez.
  Pour définir le gouverneur sur le mode Performance, exécutez la commande suivante sous root :

  echo performance > /sys/devices/system/cpu/cpu/cpufreq/scaling_governor

  Répétez cette commande pour chaque noyau .

  [RFLNX-1003]

- Le plug-in du décodeur avec accélération matérielle H264 pour le Pi HDX Ready ne fonctionne pas correctement si vous modifiez la résolution du tampon de trame avec les paramètres framebuffer_width et framebuffer_height dans le fichier /boot/config.txt. Une solution consiste à modifier la résolution du Pi avec les paramètres hdmi_group et hdmi_mode.

  [RFLNX-1049]

Problèmes connus dans Citrix Receiver pour Linux 13.4

Les problèmes connus suivants ont été observés dans cette version :

- Il est impossible de réduire une session en mode plein écran en mode fenêtre à l'aide de la barre d'outils de Desktop Viewer lors de l'utilisation de l'argument '-span o' pour remplacer la redirection de la fenêtre de session.

  Pour résoudre ce problème, n'utilisez pas l'option '-span o'. Utilisez un gestionnaire de fenêtres avec prise en charge de _NET_WM_FULLSCREEN_MONITORS ou désactivez Desktop Viewer.

[#634855]

- La session secondaire peut ne pas s'afficher lorsque vous cliquez sur son nom sous le bouton Basculer de Desktop Viewer.

  [#648716]

- Receiver pour Linux peut cesser de répondre indéfiniment lors du basculement de l'interface X1 vers l'interface classique.

  Si l'interface en libre-service affiche l'erreur « NoWebUI 0 », redémarrez le processus de libre-service pour rétablir l'interface en libre-service à son état initial.

  [#652810]

- La redirection Flash utilise un emplacement incorrect pour les clients multi-écrans.

  Lors de l'utilisation de la redirection Flash sur un client comportant de multiples écrans, le contenu Flash peut s'afficher sur le mauvais écran où en dehors de l'écran. Pour éviter ce problème, assurez-vous que la session est exécutée sur tous les écrans disponibles avant d'essayer d'utiliser la fonctionnalité de redirection Flash.

  [#653550]

- La mise à jour de cette version peut entraîner des erreurs en raison des options supprimées dans le fichier All_Regions.ini.

  [#654826]

- La redirection de webcam HDX est désactivée pendant 45 secondes au démarrage.

  Pour éviter ce problème, ajoutez une entrée à la section [wfclient] de ~/.ICAClient/wfclient.ini (ou $ICAROOT/config/module.ini) HDXRTMEWebCamLaunchDelayTime=0.

  Si vous prévoyez d'utiliser le plug-in RTME à la place de la redirection de webcam HDX, ne changez pas cette valeur.

Problèmes connus dans Citrix Receiver pour Linux 13.3

Les problèmes connus suivants ont été observés dans cette version :

- Citrix Receiver ne reconnaît pas la carte à puce PIV lors du démarrage d'un bureau pour la première fois.

  [#491235]

- Des messages d'erreur ambigus sont affichés lorsque Citrix Receiver ne peut pas trouver le serveur immédiatement après le redémarrage.

  [#553886]

- Un message incorrect s'affiche lorsque le délai de la fiabilité de session expire.

[#556899]

- Un message d'erreur (par exemple, « Erreur inconnue 1000047 ») s'affiche lors de la connexion à un VDA sur lequel le protocole SSlv3 est activé.

  [#558641]

- Une erreur réseau générique s'affiche lors de la connexion à un serveur StoreFront sur lequel le protocole SSLv3 est activé.

  [#558653]

- La modification de SharedUserMode à l'aide de storebrowse, -c SharedUserMode[=value] requiert que la casse corresponde exactement au paramètre de la valeur.Lors de l'utilisation du paramètre de la valeur pour storebrowse, -c SharedUserMode[=value] vous devez spécifier une casse identique à l'aide de « True » ou « False » Aucun message d'erreur ne s'affiche si un paramètre de valeur non valide est utilisé. Par exemple, -c SharedUserMode=True.

  [#559402]

- Lors de la connexion à un serveur de terminal (par exemple RDS) sur lequel seul le protocole SSLv3 est activé, la connexion échoue comme prévu mais il est possible qu'elle n'échoue pas avec un échec de protocole de transfert homologue SSL.

  [#567407]

- Échec de l'entrée de webcam USB générique sur les systèmes 64 bits.

  [#568556]

- La commande storebrowse –d n'efface pas les informations de magasin précédemment effacées du cache créées par le libre-service. Cela signifie que si le magasin est ajouté par la suite, l'interface de libre-service se charge à partir de l'état de cache précédent.

  [#569806]

- Les nouvelles valeurs TLS ne sont pas appliquées aux connexions au serveur StoreFront à l'aide des commandes selfservice/storebrowse lorsque des valeurs TLS sont modifiées après acceptation du contrat de licence (EULA). Veuillez noter qu'AuthManager ne peut pas lire pas un réglage TLS modifié lorsqu'il est en cours d'exécution.

  [#570725]

- Le Centre de connexion ne prend pas en charge IPv6.

  [#571743]

- Lors de la spécification d'une valeur négative dans une entrée de configuration d'entier telle que TCPRecvBufferSize dans $HOME/.ICAClient/All_Regions.ini, la valeur est incorrectement transmise à WFICA en tant

que valeur positive. Pour résoudre ce problème, utilisez $ICAROOT/config/module.ini pour définir une valeur négative pour TCPRecvBufferSize.

[#575474]

- Les processus de GStreamer Helper affichent un avertissement lié à un problème de thread GLIB.

  [#580753]

- Le plug-in du navigateur ARMEL ne fonctionne pas avec cette version.

  [#588044]

- Si vous rencontrez des problèmes de mappage incorrect des fuseaux horaires avec les sessions XenApp/XenDesktop 7.6, assurez-vous que la correction référencée dans l'article CTX142640 est installée, et suivez les étapes de l'entrée 7 [Correction ICATS760WX64014].Si le problème n'est toujours pas résolu, essayez de changer /etc/timezone (ou /etc/localtime si /etc/timezone n'est pas présent) en lien symbolique pour un nom de ville sous /usr/share/zoneinfo/...

  Si votre fuseau horaire n'est toujours pas pris en charge, vous devrez peut-être ouvrir un ticket d'assistance pour qu'un mappage soit ajouté au serveur.

  [#LC1061, #606648]

- Dans le SDK d'optimisation de plate-forme, les plug-ins des environnements non-X11 présentent deux problèmes :

  - Les sessions sur des serveurs Windows pour XenDesktop 7.x échouent si la fiabilité de session est utilisée.
  - La vidéo est corrompue sur les sessions utilisant une profondeur de couleur de 16 bits.

    Ces problèmes sont présents dans les implémentations d'exemple du plug-in SDL_plugin basé sur les bibliothèques SDL et du plug-in FB_plugin basé sur le tampon de trame du noyau brut. Tout autre plug-in développé par l'utilisateur présentera les mêmes problèmes.

Problèmes connus dans Citrix Receiver pour Linux 13.2.1

Les problèmes connus suivants ont été observés dans cette version :

- Le plug-in du navigateur ARMEL (utilisé pour le lancement de sessions à partir d'un navigateur Web) ne se lance pas, ce qui empêche l'utilisateur de lancer une session. Pour résoudre ce problème, utilisez les paramètres du navigateur pour désactiver le plug-in, ce qui permet à un mécanisme de secours de prendre le relais.

  [#580782]

- Lors de l'exécution sur SLED 11sp3, le lancement de storebrowse ou de selfservice à partir d'un terminal peut entraîner l'affichage de messages d'erreur sur plusieurs programmes indiquant « libidn.so.11: no version information available. ». Ce problème n'a que très peu, voire aucun effet sur le comportement de Citrix Receiver.

  [#582512]

- La redirection Flash n'est pas disponible sur les clients 64 bits. Si cette capacité est importante dans votre environnement, contactez l'équipe de gestion des produits Citrix ou consultez les forums de support pour des conseils supplémentaires.

  [#582627]

- Receiver ne parvient pas à ajouter des applications favorites lorsque vous sélectionnez Ajouter aux favoris dans la vue Détails. Ce problème se produit lors de l'exécution de SuSE SLED 11sp3 sans installation des mises à jour. Pour éviter ce problème, assurez-vous que la version minimum du package libwebkit-1_0-2 est 1.2.7-0.17.1 (ou une version supérieure).

  [#585295]

- Un problème tiers se produit dans la version EPEL 2.2.4 de libwebkitgtk+. Citrix recommande d'utiliser le référentiel EPEL (Extra Packages for Enterprise Linux) pour obtenir la version GTK+2 de libwebkitgtk sur RedHat 7 et Centos 7. Toutefois, un problème avec la version EPEL fournie se produit lorsque des caractères japonais/chinois sont utilisés dans les noms des applications hébergées sur le serveur. Par conséquent, Receiver ne peut pas offrir de méthode permettant de fournir une version de libwebkitgtk stable sur RedHat 7 et Centos 7 appropriée pour la saisie de caractères APAC.

  [#586967]

- Sur certaines plates-formes, l'installation du client à partir d'une distribution 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 suivante : gst-inspect-0.10 -- gst-disable-registry-fork --version. Après l'exécution de cette commande, vous devriez pouvoir exécuter de nouveau le fichier tarball sans rencontrer de blocage.

  [#587640]

- Dans certains environnements de bureau Gnome, un client peut crasher lors du démarrage de l'application Bureau à distance Microsoft (Mstsc). Ce problème se produit après la connexion à un bureau à distance. Après la saisie des informations d'identification, il est impossible de fermer la session correctement en cliquant sur le symbole 'X' (une erreur indique qu'un problème s'est produit et que le système ne peut pas être rétabli.) [0587922]

  [#587922]

- Le Lecteur Windows Media affiche un message d'erreur indiquant que « Le Lecteur Windows Media a rencontré un problème lors de la lecture du fichier » ; Cette erreur peut être ignorée en fermant le message d'erreur puis en cliquant sur l'icône Lecture.

  [#588009]

- Le Lecteur Windows Media peut ne pas parvenir à lire des fichiers audio/vidéo sur un bureau Windows 7 lorsqu'il est démarré à partir d'un Receiver 64 bits. Ce problème est dû à un problème connu avec Ubuntu 14.04 ; les composants GStreamer requis ne sont pas installés. Consultez la section « Le lecteur Windows Media ne parvient pas à lire certains formats de fichiers » dans la rubrique Dépannage.

[#588298]

- Le lecteur Windows Media ne parvient pas à lire certains formats de fichiers.

Problèmes connus dans Citrix Receiver pour Linux 13.2

Les problèmes connus suivants ont été observés dans cette version :

- Un nouveau script a été ajouté afin de créer des associations de types de fichiers client-serveur. Ce script, ctx_app_bind, vous permet d'utiliser une application publiée pour ouvrir un type de fichier spécifique. Ce script accepte le nom de l'application publiée, un fichier d'exemple ou un type MIME, et vous permet facultativement d'inclure un nom de serveur ou une adresse URL.
  Par exemple

  : ctx_app_bind example_file published_app_name server
  ctx_app_bind application/some-mime-name published_app_name

  Utilisez l'option –p pour utiliser pnabrowse plutôt que storebrowse pour le lancement de la session.

  Remarque : Citrix vous recommande d'exécuter ce script avec précaution. Il n'a pas été testé avec tous les environnements d'OS possibles.

  [#558649]

- Si un utilisateur ne parvient pas à se connecter au magasin, vous pouvez activer les journaux de connexion sur Receiver pour identifier et résoudre le problème. Pour activer la collecte des journaux de connexion dans Receiver :

  1. Modifiez le fichier /opt/citrix/ICAClient/config/AuthManConfig.xml avec les paramètres suivants en tant qu'utilisateur doté de privilèges d'administrateur :

  TracingEnabled
  true

  LoggingMode
  verbose

  2. Mettez fin aux processus suivants : AuthManagerDaemon, selfservice, ServiceRecord, storebrowse.

  3. Démarrez Receiver et connectez-vous au magasin.

  4. Consultez les journaux sous $HOME/.ICAClient/logs.

  La compression vidéo de caméra Web HDX RealTime requiert la configuration suivante :

  - Webcam compatible Video4Linux

  - GStreamer 0.10.25 (ou une version 0.10.x ultérieure), comprenant le pack de distribution « plugins-good »

  [#559817]

- Lorsque vous utilisez Linux Receiver X1 pour supprimer une application, l'application persiste lorsque vous fermez la

session et que vous retournez sur le magasin.

[#561719]

Problèmes connus avec Citrix Receiver pour Linux 13.1

Les problèmes connus suivants ont été observés dans cette version :

- Vous ne pouvez pas déconnecter ou fermer la session de bureaux virtuels à partir du Centre de connexion. Le bouton Déconnecter n'est pas disponible et le bouton Fermer la session ne fonctionne pas. Pour contourner ce problème, déconnectez ou fermez la session à partir du bureau, et non pas du Centre de connexion. Ce problème ne se produit pas avec les applications virtuelles.

  [#423651, #424847]

- Une erreur s'affiche si un utilisateur ouvre l'interface utilisateur en libre-service pour se connecter au magasin StoreFront, puis qu'il ferme la fenêtre Receiver pour Linux lorsque la boîte de dialogue Gestionnaire d'authentification est ouverte.

  [#430193]

- Receiver pour Linux n'autorise pas les connexions à un magasin StoreFront non sécurisé (http://). En fonction de la configuration du magasin, l'utilisateur recevra un message d'erreur du type « Erreur : Impossible de récupérer le document de découverte » [], ou la connexion initiale sera établie via http, mais les communications suivantes basculeront sur https. Si vous utilisez l'adresse IP en tant que nom d'hôte, il est possible que des erreurs faisant référence à Citrix XenApp Services (anciennement PNAgent) s'affichent. Utilisez https:// explicitement ou n'ajoutez pas le préfixe http:// au nom du serveur lors de la saisie de l'URL.

  [#473027, #478667 et #492402]

- Receiver pour Linux ne prend pas en charge l'ouverture de session avec une carte à puce contenant de multiples certificats d'authentification.

  [#488614]

- Si Receiver pour Linux signale une erreur de segmentation lors de l'accès à des cartes à puce, cela peut être dû à un problème avec la bibliothèque PKCS#11. Vous pouvez vérifier la bibliothèque avec l'utilitaire pkcs11-tool. L'utilitaire pkcs11-tool fait partie du package opensc. Exemple de test :

  pkcs11-tool --module /usr/lib/libgtop11dotnet.so -

  Si ce dernier signale également une erreur de segmentation, vous devez contacter le fournisseur du pilote. Vous pouvez également essayer un pilote provenant d'une autre source pour le même type de carte. Ce problème a été rencontré avec le pilote Gemalto .NET inclus dans Fedora 19 et Fedora 20.

  [#493172]

- Receiver pour Linux prend en charge de multiples lecteurs de carte ; toutefois, seule une carte à puce peut être utilisé à la fois.

[#494524]

- Le nom d'hôte de la machine Linux doit comporter 20 caractères ou moins pour que les connexions fonctionnent. Ce paramètre peut être consulté et défini à l'aide de la commande hostname. Tout utilisateur peut consulter le nom d'hôte, mais pour le définir, vous devez être un utilisateur racine ou disposer de privilèges d'administrateur.

  [#494740]

- Lorsque vous travaillez avec XenDesktop en mode plein écran dans Receiver pour Linux 13.x, il se peut que l'écran de veille local ne s'active pas. Il s'agit d'un problème tiers, et le comportement peut varier en fonction du système d'exploitation client.

  [#496398]

- Si vous insérez une carte à puce incorrecte lors de la tentative de connexion à un magasin StoreFront, il est possible qu'un message d'erreur tel que « erreur de protocole » ou « Magasin spécifié introuvable » s'affiche, ce qui n'explique pas le problème.

  [#496904]

- Sur certains périphériques de faible puissance et dans une session en mode plein écran, le processus d'ouverture de session avec authentification par carte à puce peut prendre plus longtemps que prévu et le délai imparti expire. Vous pouvez éviter ce problème en désactivant l'utilisation de H264. Pour désactiver l'utilisation de H624, procédez comme suit :
  1. Ouvrez le fichier wfclient.ini.
  2. Localisez la section « Thinwire3.0 ».
  3. Ajoutez l'entrée « H264Enabled=False ».

  Ce problème a été observé sur une machine armhf (ARM hard float), sans accélération matérielle H264.

  [#497720]

- Si un serveur PNAgent autorise l'utilisateur à changer des mots de passe expirés en contactant le contrôleur de domaine directement, vous ne pouvez le faire qu'avec la version compatible MIT de la bibliothèque libkcpm.so. Ceci est causé par des problèmes avec la version compatible Heimdal. Cette restriction s'applique à x86, armel et x64 (qui utilise x86 pnabrowse). Cela ne s'applique pas à armhf.

  [#498037]

- Receiver pour Linux requiert la librairie libpng12.so, toutefois cette dernière n'est pas normalement disponible dans les référentiels standard pour les systèmes Fedora. Dans ce cas, recherchez un RPM approprié pour votre système sur Internet. Pour openSUSE, la bibliothèque libpng12.so est disponible, mais elle doit être installée séparément.

  [#501937]

- Une correction pour 12.1 a ajouté un code de sortie pnabrowse E_SSLSDK_PASSWORD_LOCKED avec la valeur 220. Le

code de sortie E_PASSWORD_EXPIRED est passé à 239 par rapport à sa valeur documentée de 238. Dans 13.0, la valeur de E_SSLSDK_PASSWORD_LOCKED est passée à 240, ce qui a rétabli la valeur correcte de E_PASSWORD_EXPIRED. Toutefois, les valeurs répertoriées par pnabrowse -errno affichent toujours des significations non corrigées pour les valeurs 220 à 240.

[#502550]

Problèmes connus avec Citrix Receiver pour Linux 13

Les problèmes connus suivants ont été observés dans cette version :

Problèmes d'installation

- libxerces-c 3.1 est un composant nécessaire pour cette version. Toutefois, il n'est pas disponible dans certaines distributions Linux qui utilisent le packaging RPM. Si ce composant est manquant dans votre distribution, recherchez-le sur un site Web et ajoutez-le à votre installation système Linux.

  [#384324]

- Sur les plates-formes qui ne respectent pas les conditions nécessaires à libxerces ou libwebkitgtk (ou les deux), vous pouvez installer Receiver à l'aide du package tarball, ou forcer l'installation des packages Debian ou RPM, et utiliser Receiver pour Web pour démarrer des connexions. Par exemple, vous ne pouvez pas installer le package RPM sur des systèmes CentOS car ils nécessitent libwebkitgtk-1.0.so.0, qui n'est pas disponible dans ces environnements. Pour contourner ce problème, installez le pack avec --nodeps ou --force, ou utilisez le pack Tarball à la place. Lancez ensuite un navigateur et entrez l'URL de votre magasin Receiver pour Web.

  [#426176]

- Vous pouvez utiliser le package RPM pour installer Receiver sur la version 32 bits de OpenSUSE 13.1, mais ce dernier échoue lors de l'exécution. Pour contourner ce problème, commencez par télécharger et installer le package RPM suivant et recommencez l'installation : ftp://rpmfind.net/linux/opensuse/factory/repo/oss/suse/i586/libpng12-0-1.2.50-7.3.i586.rpm.

  [#429879]

- Après l'installation de Receiver à partir d'un package RPM 64 bits dans un environnement Fedora 19.1 64 bits, vous devez effectuer des étapes supplémentaires avant d'utiliser pnabrowse ou le moteur de client, wfica, pour lancer des connexions. (Ces étapes permettent de résoudre les problèmes liés à storebrowse et selfservice, dont le fonctionnement ne peut pas être assuré en raison de limitations dans la version de curl dans cet environnement.) Pour contourner ce problème :

1. Installez le package 32 bits libpng12 à l'aide de la commande suivante :

   yum install libpng12.i686

2. Pour minimiser le nombre d'erreurs audio, installez le plug-in ALSA 32 bits à l'aide de la commande suivante :

   yum install alsa-plugins-pulseaudio.i686

3. Pour minimiser le nombre d'erreurs GtK, installez les packages suivants à l'aide des commandes suivantes :

   yum install adwaita-gtk2-theme.i686
   yum install PackageKit-gtk3-module.i686
   yum install libcanberra-gtk2.i686

4. Pour permettre le démarrage de connexions à partir de Firefox, installez le plug-in nspluginwrapper.i686 et enregistrez-le auprès du navigateur Web à l'aide des commandes suivantes :

   yum install nspluginwrapper.i686
   mozilla-plugin-config

   [#429886]

Problèmes d'ordre général

- La reprise de la lecture audio peut être bruyante. Le bruit est présent uniquement lorsque l'audio est mis en pause puis redémarré, et pas lorsqu'il est lu la première fois. Cela a été observé avec les connexions XenDesktop impliquant la fonctionnalité Remote PC Access. Il n'existe pas de solution pour ce problème.

  [#308772]

- Certains types de médias peuvent uniquement lire du contenu sur la machine utilisateur si le codec approprié est disponible sur le serveur, même si GStreamer est en mesure de se connecter directement à la source du média et de la lire à l'aide des décodeurs de la machine. Il n'existe pas de solution pour ce problème.

  [#339394]

- Sur Ubuntu 12.04 avec un bureau Gnome 3, les icônes de la zone de notification correspondant aux applications publiées ne s'intègrent avec le bureau natif. Au lieu de cela, ils apparaissent dans une fenêtre de zone de notification distincte. Il n'existe pas de solution pour ce problème.

  [#395140]

- Les utilisateurs Linux ne peuvent pas utiliser leurs adresses de messagerie pour configurer les magasins StoreFront. Ils doivent au lieu de cela ajouter l'URL des magasins requis à l'aide de la page Comptes de la boîte de dialogue Préférences. Vous pouvez également fournir un fichier de provisioning contenant les informations de compte qui est utilisé pour créer un nouveau compte.

  [#395394]

- La prise en charge proxy des commandes storebrowse et selfservice n'est pas disponible par défaut. Pour utiliser un serveur proxy avec un serveur StoreFront, définissez la variable d'environnement http_proxy avant de démarrer l'une de ces commandes. Utilisez le format suivant pour la variable d'environnement :

  .[:]

[#403729]

- La redirection de contenu du client vers le serveur (en déplaçant du contenu publié sur une icône de bureau) ne fonctionne pas l'interface utilisateur en libre-service. Il n'existe pas de solution pour ce problème.

  [#403739]

- Le module de sécurité Security-Enhanced Linux (SELinux) dans RedHat Fedora peut affecter le fonctionnement du mappage de lecteurs clients et les fonctionnalités de redirection USB (sur XenApp et XenDesktop). Si vous avez besoin d'une ou de ces deux fonctionnalités, désactivez SELinux avant de les configurer sur le serveur.

  [#413554]

- La fonctionnalité de redirection Flash HDX MediaStream n'a pas été testée sur la plate-forme hard float (armhf), car, dans cette version, Receiver ne fonctionne pas avec les plug-ins Flash sur cette plate-forme.

  [#414253]

- Si vous configurez une fréquence d'images webcam qui n'est pas prise en charge par la webcam, la valeur par défaut est une valeur différente, qui peut être plus élevée que prévu.

  [#414576]

- Si, dans Receiver, vous définissez une résolution autre que celle par défaut pour une webcam, la vidéo n'est pas streamée la première fois que vous l'utilisez avec Citrix GoToMeeting. La webcam semble active et gst_read est en cours d'exécution, mais aucune image n'est affichée. Pour contourner ce problème, arrêtez et redémarrez la webcam dans GoToMeeting.

  [#414878]

- Si aucune décoration de fenêtre n'est présente dans l'environnement de bureau (par exemple, dans l'environnement LXDE avec les décorations désactivées), vous ne pourrez peut-être pas fermer les boîtes de dialogue de libre-service.

  [#416689]

- Avec certaines versions de XenApp ou XenDesktop, après le démarrage d'un bureau ou d'une application, vous ne pouvez pas vérifier le nom du serveur utilisé pour une connexion car aucun serveur n'est répertorié dans le Centre de connexion. Pour contourner ce problème, cliquez sur Propriétés. Le nom du serveur est affiché dans la boîte de dialogue Propriétés.

  [#417114]

- Si, lors de l'ouverture de session sur Receiver, vous entrez vos informations d'identification après un délai d'environ cinq minutes, l'interface utilisateur en libre-service n'affiche pas vos applications. Pour contourner ce problème, sélectionnez Actualiser les applications dans le menu déroulant de l'interface utilisateur et retapez vos informations d'identification.

  [#417564]

- Un administrateur qui observe la session d'un utilisateur peut rencontrer des erreurs d'affichage si la taille de son écran est inférieure à celle de la machine de l'utilisateur. Par exemple, des barres de défilement peuvent ne pas tenir sur l'écran de l'administrateur, et certaines parties de l'écran de l'utilisateur peuvent être inaccessibles. Il n'existe pas de solution pour ce problème. En outre, le redimensionnement de la session observée à partir de la machine de l'administrateur peut déconnecter la session sur la machine utilisateur. Pour contourner ce problème, cliquez sur le bouton Restaurer dans la fenêtre de session sur l'ordinateur de l'administrateur (pas sur la machine utilisateur).

  [#418672, #418690]

- L'interface utilisateur en libre-service et les composants StoreFront associés (Authentication Manager et le démon Service Record) ne sont pas pris en charge sur Fedora en raison d'incompatibilités entre les bibliothèques. Receiver s'installe sans erreurs mais ne fonctionne pas après l'installation. Pour contourner ce problème, démarrez Receiver via l'Interface Web (un ancien composant) ou Receiver pour Web.

  [#419662]

- Lorsque les utilisateurs s'abonnent à de nombreuses applications ou de nombreux bureaux, l'interface utilisateur en libre-service comprend une barre de défilement. Cette dernière disparaît (comme prévu) lorsque l'interface utilisateur est redimensionnée pour afficher toutes les icônes d'application et de bureau. Cependant, la barre de défilement ne s'affiche pas lorsque l'interface utilisateur est réduite. Ce problème a été observé uniquement sur Ubuntu 13.04. Pour contourner le problème, cliquez sur l'option de menu Actualiser, répétez l'opération de redimensionnement plusieurs fois ou arrêtez et redémarrez Receiver.

  [#422520]

- La première fois qu'une connexion est établie, vous pouvez observer un délai qui varie considérablement selon le réseau. Une connexion 3G sera probablement plus lente qu'une connexion ADSL.

  [#423663]

- Lorsque vous entrez une adresse de magasin HTTPS dans l'interface utilisateur en libre-service, le message d'erreur suivant s'affiche si aucun certificat n'est présent : « Votre compte ne peut pas être ajouté à l'aide de cette adresse de serveur. Assurez-vous que l'adresse entrée est correcte. » Cette erreur s'affiche si l'adresse est correcte, mais qu'aucun certificat n'est présent. Pour contourner ce problème, installez un certificat.

  [#423757, #424674]

- Vous pouvez appliquer une stratégie XenDesktop pour augmenter le taux de trame maximal dans les sessions Receiver au-delà de 30 trames par seconde (i/s). Toutefois, cette valeur n'est pas reconnue et le taux de trame dans les sessions ne dépasse jamais cette valeur, car elle est limitée par la fonctionnalité de contrôle de flux. Ce problème a été observé dans XenDesktop 7 et 7.1. Pour contourner ce problème, désactivez le contrôle de flux.

  [#423950]

- Pour changer de compte (et accéder à des applications et bureaux à partir d'un autre magasin), vous devez utiliser le menu Comptes dans l'interface utilisateur en libre-service. Ceci n'est pas toujours évident pour les utilisateurs.

[#424027]

- Si vous utilisez storebrowse dans plusieurs langues qui ne sont pas codées en UTF-8, certaines parties du texte dans la boîte de dialogue d'ouverture de session peuvent être corrompues. Par exemple, en langue espagnole, aucun texte ne s'affiche sur le bouton Ouvrir une session. Pour contourner ce problème, basculez vers un système utilisant des paramètres régionaux UTF-8 (par exemple, en créant un script de wrapper autour storebrowse, et des exécutables du Service Record et du démon Authentication Manager).

  [#424052]

- Vous ne pouvez pas déconnecter ou fermer la session de bureaux virtuels à partir du Centre de connexion. Le bouton Déconnecter n'est pas disponible et le bouton Fermer la session ne fonctionne pas. Pour contourner ce problème, déconnectez ou fermez la session à partir du bureau, et non pas du Centre de connexion. Ce problème ne se produit pas avec les applications virtuelles.

  [#424847]

- Lorsque storebrowse est utilisé pour démarrer une session sur un bureau virtuel dans un groupe dans lequel tous les bureaux sont désactivés, une valeur d'état de sortie de 255 EXEC_FAILED est affichée (parfois après un certain délai), ce qui indique que le démarrage a échoué. Toutefois, au lieu de cela, le démarrage ou l'enregistrement du bureau est en cours et il sera bientôt disponible. Pour contourner ce problème, indiquez aux utilisateurs qui rencontrent ce problème d'essayer de redémarrer le bureau, ou assurez-vous qu'un script de démarrage s'acquitte de cette tâche.

  [#425076, #425103]

- Dans les versions en japonais et chinois simplifié de Receiver, les raccourcis clavier ne fonctionnent pas dans certaines boîtes de dialogue.

  [#425275, #425278, #425281, #425332]

- Dans les versions en allemand, français et espagnol de Receiver exécutées sur la plate-forme Ubuntu, les raccourcis clavier ne sont pas visibles dans certaines boîtes de dialogue, mais ils sont opérationnels.

  [#425282, #425285, #425289, #425294, #425339]

- Dans la version allemande de Receiver, des raccourcis clavier dupliqués sont présents dans certaines boîtes de dialogue.

  [#425284, #425338]

- L'outil openssl c_rehash est utilisé pour importer et hasher des certificats racine qui sont utilisés pour sécuriser les communications avec StoreFront. Certaines versions de c_rehash ne gèrent pas correctement les certificats qui contiennent des fins de ligne de style MS-DOS. Si la sortie de c_rehash ne génère pas les liens symboliques pour votre certificat, vous devez convertir les fins de ligne pour le format UNIX. Vous pouvez le faire à l'aide de la ligne de commande tr suivante :

  tr -d '\r' < root_certificate_name.pem > new_root_certificate_name.pem

Exécutez ensuite le script c_rehash sur le nouveau certificat racine créé à partir de cette commande.

[#425775]

- Sur les plates-formes Debian, le démon ctxusbd ne redémarre pas lorsque le système redémarre, ce qui entraîne l'échec de redirection USB. Ceci est dû au fait que le script init, /etc/init.d/ctxusbd, contient une variable, ###INIT_UDEV ###, qui doit être étendue sur udev. Pour contourner ce problème, modifiez /etc/init.d/ctxusbd comme suit. Pour ce faire, vous devez disposer des autorisations racine :

  sed -ie's,###INIT_UDEV###,udev,g' /etc/init.d/ctxusbd

  Ensuite, réexécutez manuellement insserv (avec les autorisations racine) :

  /sbin/insserv /etc/init.d/ctxusbd

  Ce problème a été observé sur les plates-formes Debian uniquement.

  [#425810]

- Lors de la connexion à des sites Agent Program Neighborhood, les certificats absents ou qui ont expiré peuvent causer le clignotement de l'interface utilisateur de Receiver, inviter l'utilisateur à entrer ses informations d'identification à plusieurs reprises ou consommer beaucoup d'UC. Pour contourner ce problème, Citrix vous recommande d'installer vos certificats correctement et de les mettre à jour régulièrement. Ce problème ne se produit pas lorsque vous vous connectez à des sites StoreFront.

  [#425848]

- Les icônes dans l'interface utilisateur en libre-service risquent de ne pas s'afficher lorsque de nouveaux utilisateurs recherchent des applications ou des bureaux. Pour contourner ce problème, cliquez sur Actualiser les applications.

  [#426364]

- Lorsque vous utilisez pnabrowse pour vous connecter à un site Agent Program Neighborhood sécurisé par HTTPS sur certains serveurs Microsoft Server 2012 dans des environnements armhf (hard float), un message d'erreur générique s'affiche et la connexion échoue. La cause de ce problème n'est pas entièrement connue, mais elle est peut-être due au fait que le nom de domaine complet des serveurs (FQDN) se termine par .local, ou que la taille de clé spécifiée dans le champ de clé publique du certificat sur les serveurs est 2 048 bits et non 1 024 bits. Ce problème ne se produit pas avec storebrowse et a été uniquement observé dans les environnements armhf.

  [#426420]

- Si vous fermez Receiver (en cliquant sur Fermer la session dans l'interface utilisateur libre-service), puis que vous essayez de vous connecter à un bureau ou une application et que vous annulez lorsque vous êtes invité à entrer vos informations d'identification, le message « Impossible de traiter la demande » s'affiche. Vous pouvez ignorer ce message. Vous avez été déconnecté avec succès.

  [#426424]

- Une erreur de segmentation se produit, et Receiver échoue, lorsque vous utilisez l'interface utilisateur en libre-service pour la première fois pour vous connecter à un site Agent Program Neighborhood, que vous cliquez sur Annuler dans la boîte de dialogue d'ouverture de session, puis que vous cliquez sur Actualiser les applications et que vous fermez la fenêtre de Receiver. Il n'existe pas de solution pour ce problème.

  [#426625]

- Plusieurs les processus qui appellent le magasin de données ou les procédures de chargement simultanément peuvent entraîner une perte de données dans les fichiers qui sont en mémoire (par exemple, StoreCache.xml). La dernière modification apportée à un fichier donné est conservée ; les modifications précédentes sont perdues. Il n'y a aucun risque que le fichier soit endommagé.

  [#426692]

- Si vous supprimez puis que vous ajoutez un magasin, la page Comptes de la boîte de dialogue Préférences n'affiche pas le nouveau magasin tant que vous n'avez pas fermé puis rouvert la boîte de dialogue.

  [#426735]

- Lorsque la préférence Reconnecter les applications et les bureaux est définie sur Lorsque je démarre ou que j'actualise des applications et qu'une connexion à un bureau ou une application est en cours, la sélection de l'option Actualiser les applications dans le menu de Receiver bloque l'interface utilisateur tant que la connexion n'est pas établie.

  [#426761]

- Aucun message d'erreur ne s'affiche lorsque vous essayez d'ajouter un magasin ou une passerelle qui figure déjà dans Receiver. Il n'existe pas de solution pour ce problème, mais aucune entrée dupliquée n'est créée et le magasin existant ou la passerelle existante continue de fonctionner correctement.

  [#427379]

- Les menus dans les applications publiées disparaissent lorsque les utilisateurs cliquent dessus. Cela a été observé dans les fenêtres d'application agrandies dans les environnements de bureau GNOME 3 sur Ubuntu 12.04 mais pas dans les environnements Unity sur Ubuntu 12.04.3.

  [#429686]

- Attention : une limitation dans Windows signifie que le niveau de volume de l'audio est au maximum lorsqu'une session se reconnecte automatiquement après un problème réseau. Il n'existe pas de solution pour ce problème.

  [#430160]

- Les préférences de Receiver affectent uniquement les nouvelles sessions ou les sessions reconnectées, et non pas les sessions déconnectées. À titre d'exemple, vous pouvez démarrer Citrix GoToMeeting à partir d'un bureau virtuel puis vous déconnecter de la session de bureau (mais pas de GoToMeeting). Vous pouvez ensuite sélectionner Utiliser mon micro et

ma webcam sur la page Mic et Webcam de la boîte de dialogue Préférences, mais cela ne démarre pas la webcam dans la session GoToMeeting. Pour contourner ce problème, fermez et redémarrez la session affectée (dans cet exemple, la session GoToMeeting).

[#430692]

- Si selfservice est exécuté à partir d'un terminal, et que le terminal est fermé avant selfservice, le signal de fermeture standard est envoyé à tous les processus d'avant-plan hébergés par le terminal. Les autres processus Linux Receiver tels que les démons Service Record et Authentication Manager n'ignorent pas ce signal mais en revanche selfservice l'ignore. Cela peut entraîner le blocage de selfservice car les processus desquels il dépend sont fermés. Pour contourner ce problème, démarrez les démons à l'aide de storebrowse dans une fenêtre, puis dans une autre fenêtre, exécutez selfservice. Cela vous permet de fermer la fenêtre de terminal exécutant selfservice mais les démons continuent de fonctionner en arrière-plan, et l'interface utilisateur reste active.

  [#430697]

Configuration système requise

Jul 10, 2017

Appareils

- Linux kernel version 2.6.29 ou ultérieure, avec glibcxx 3.4.15 ou version ultérieure, glibc 2.11.3 ou version ultérieure, gtk 2.20.1 ou version ultérieure, libcap1 ou libcap2 et prise en charge de udev.
- Pour l'interface utilisateur en libre-service :
  - libwebkit ou libwebkitgtk 1.0
  - libxml2 2.7.8
  - libxerces-c 3.1
- Bibliothèques de codecs ALSA (libasound2), Speex et Vorbis.
- 55 Mo d'espace disque minimum pour la version installée de Receiver et au moins 110 Mo en cas de décompression du pack d'installation sur le disque. Vous pouvez vérifier l'espace disque disponible en entrant la commande suivante dans une fenêtre de terminal :
  df -k
- Au moins 1 Go de RAM pour les périphériques system-on-a-chip (SoC) qui utilisent la redirection HDX MediaStream Flash.
- Écran d'affichage vidéo 256 couleurs ou supérieur.
- Gestion réseau TCP/IP.

H.264

Pour les périphériques x86, des processeurs d'une vitesse minimum de 1.6 GHz affichent les sessions sur écran unique avec résolution standard (par exemple, 1280 x 1024) sans problème. Si vous utilisez la fonctionnalité HDX 3D Pro, un pilote graphique à accélération matérielle natif et une vitesse de processeur minimale de 2 GHz sont requis.

Pour les périphériques ARM, un décodeur matériel H.264 est nécessaire pour la prise en charge de H.264 et de HDX 3D Pro. Des vitesses d'horloge plus rapides profitent également aux performances.

Redirection HDX MediaStream Flash

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

Citrix recommande 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.

compression vidéo pour caméra Web HDX RealTime.

La compression vidéo de caméra Web HDX RealTime requiert la configuration suivante :
- caméra Web compatible Video4Linux ;
- GStreamer 0.10.25 (ou une version 0.10.x ultérieure), comprenant le pack de distribution « plugins-good ».
  Ou GStreamer 1.0 (ou une version 1.x ultérieure), comprenant les packs de distribution « plugins-base », « plugins-good », « plugins-bad », « plugins-ugly » et « gstreamer-libav ».

Redirection HDX Mediastream Windows Media

La redirection HDX MediaStream Windows Media requiert :
- GStreamer 0.10.25 (ou une version 0.10.x ultérieure), comprenant le pack de distribution « plugins-good » ; en général, la version 0.10.15 ou supérieure est suffisante pour la redirection HDX MediaStream Windows Media.

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

Remarque : si GStreamer n'est pas inclus dans votre distribution Linux, vous pouvez le télécharger sur http://gstreamer.freedesktop.org. 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. Renseignez-vous auprès de votre département juridique pour déterminer si les codes que vous envisagez d'utiliser requièrent des licences supplémentaires.

Philips SpeechMike

Si vous envisagez d'utiliser des périphériques Philips SpeechMike avec Receiver, vous devrez peut-être installer les pilotes adéquats sur la machine utilisateur. Visitez le site Web de Philips pour consulter les informations qui vous intéressent et télécharger les logiciels appropriés.

Prise en charge des cartes à puce

Pour configurer la prise en charge de carte à puce dans Citrix Receiver pour Linux, le site StoreFront Services doit être configuré pour autoriser l'authentification par carte à puce.

> ## Remarque
>
> Remarque : les cartes à puce ne sont pas prises en charge avec le site XenApp Services pour les configurations Interface Web (anciennement PNAgent), ou avec le site « PNAgent d'ancienne génération » qui peut être fourni par un serveur StoreFront.

Citrix Receiver pour Linux prend en charge les lecteurs de carte à puce compatibles avec PCSC-Lite et les cartes à puce avec pilotes PKCS#11 pour la plate-forme Linux appropriée. Par défaut, Receiver pour Linux place désormais opensc-pkcs11.so dans l'un des emplacements standards. Pour vous assurer que Receiver pour Linux trouve opensc-pkcs11.so dans un emplacement non-standard ou un autre pilote PKCS#11, stockez l'emplacement dans un fichier de configuration en suivant les étapes suivantes :

1. Localisez le fichier de configuration : $ICAROOT/config/AuthManConfig.xml
2. Localisez la ligne PKCS11module et ajoutez l'emplacement du pilote à l'élément qui suit immédiatement la line. Remarque : si vous entrez un nom de fichier, Receiver accède à ce fichier dans le répertoire $ICAROOT/PKCS#11. Vous pouvez également utiliser un chemin d'accès absolu commençant par "/".

Pour configurer le comportement de Citrix Receiver pour Linux lorsqu'une carte est retirée, mettez à jour SmartCardRemovalAction dans le fichier de configuration en suivant les étapes suivantes :

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

Le comportement par défaut est 'noaction'. Aucune mesure n'est prise pour effacer les informations d'identification stockées et les jetons générés concernant la carte à puce 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.

Serveurs Citrix

- XenApp : toutes les versions actuellement prises en charge par Citrix. Pour de plus amples informations, consultez le tableau des produits Citrix.

- XenDesktop : toutes les versions actuellement prises en charge par Citrix. Pour de plus amples informations, consultez le tableau des produits Citrix.
- VDI-in-a-Box : toutes les versions actuellement prises en charge par Citrix. Pour de plus amples informations, consultez le tableau des produits Citrix.
- Vous pouvez accéder à Citrix Receiver pour Linux 13.5 par le biais d'un navigateur en conjonction avec StoreFront Receiver pour Web et l'Interface Web, avec ou sans le plug-in NetScaler Gateway.
  StoreFront :

  - StoreFront 3.x, 2.6, 2.5 et 2.1
    Permet d'accéder directement aux magasins StoreFront.

  - StoreFront configuré avec un site Citrix Receiver pour Web
    Permet d'accéder aux magasins StoreFront à partir d'un navigateur Web. Pour connaître les limitations de ce déploiement, reportez-vous à la section « Remarques importantes » dans les sites Receiver pour Web.

  Utiliser l'Interface Web en conjonction avec le client VPN NetScaler :

  - Sites Web Interface Web 5.4 pour Windows
    Permet d'accéder à des applications et bureaux virtuels à partir d'un navigateur Web.

  - Interface Web 5.4 pour Linux avec sites XenApp Services ou XenDesktop Services.
- Méthodes de déploiement de Citrix Receiver auprès de vos utilisateurs :
  - Autorisez les utilisateurs à effectuer un téléchargement depuis receiver.citrix.com, puis une configuration à l'aide d'une adresse e-mail ou de services en conjonction avec StoreFront.
  - Offre d'installation depuis un site Citrix Receiver pour Web (configuré avec StoreFront).
  - Offre d'installation de Receiver à partir de l'Interface Web Citrix 5.4.

Navigateur

Citrix vous recommande d'utiliser la dernière version de Mozilla Firefox ou Google Chrome.
Remarque : pour de plus amples informations sur les modifications apportées à la prise en charge du plug-in NPAPI de Google Chrome, consultez l'article Preparing for NPAPI being disabled by Google Chrome sur le blog de Citrix.

Connectivité

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

- Pour les connexions LAN :
  - StoreFront utilisant StoreFront Services ou des sites Citrix Receiver pour Web
  - Interface Web 5.4 pour Windows utilisant des sites XenApp Services où XenApp Services
- Pour les connexions sécurisées à distance ou locales :
  - Citrix NetScaler Gateway 11.1
  - Citrix NetScaler Gateway 11.0
  - Citrix NetScaler Gateway 10.5
  - Citrix NetScaler Gateway 10.1
  - Citrix Access Gateway édition Enterprise 10
  - Citrix Access Gateway édition Enterprise 9.x
  - Citrix Access Gateway VPX

  Pour de plus amples informations sur les versions de NetScaler Gateway et Access Gateway prises en charge par StoreFront, reportez-vous à la section Configuration système requise pour StoreFront.

Remarque : les références à NetScaler Gateway mentionnées dans cette rubrique s'appliquent également à Access Gateway, sauf indication contraire.

À propos des connexions sécurisées et des certificats

Remarque : pour de plus amples informations sur les certificats de sécurité, reportez-vous aux rubriques figurant sous les sections Sécuriser les connexions et Sécuriser les communications.

Certificats privés (auto-signés)

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

Remarque : si le certificat de la passerelle distante ne peut pas être vérifié lors de la connexion (car le certificat racine n'est pas inclus dans le magasin de clés), une erreur relative à un certificat non approuvé s'affiche. Le certificat racine doit être installé dans le magasin de certificats des clients.

Installation de certificats racine sur des machines utilisateur

Pour de plus amples informations sur l'installation de certificats racine sur des machines utilisateur ainsi que sur la configuration de l'Interface Web afin d'utiliser des certificats, reportez-vous à la section Sécuriser les communications de Receiver.

Certificats génériques

Les certificats génériques remplacent les certificats de serveur individuel pour n'importe quel serveur situé dans le même domaine. Citrix Receiver pour Linux prend en charge les certificats génériques, toutefois, ils doivent être uniquement utilisés conformément à la stratégie de sécurité de votre organisation. En pratique, des alternatives aux certificats génériques existent, par exemple un certificat qui contient la liste des noms de serveurs dans l'extension SAN (Subject Alternative Name) peut être pris en compte. Ce type de certificat peut être émis par des autorités de certification publiques et privées.

Certificats intermédiaires et NetScaler Gateway

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

Stratégie de validation des certificats de serveur

La stratégie de validation des certificats de serveur de Citrix Receiver pour Linux est plus stricte.

Important

Avant d'installer cette version de Citrix Receiver pour Linux, vérifiez que les certificats sur le serveur ou la passerelle sont correctement configurés comme indiqué ci-dessous. Les connexions peuvent échouer si :

- la configuration du serveur ou de la passerelle comprend un certificat racine incorrect
- la configuration du serveur ou de la passerelle ne comprend pas tous les certificats intermédiaires
- la configuration du serveur ou de la passerelle comprend un certificat ayant expiré ou un certificat intermédiaire non valide
- la configuration du serveur ou de la passerelle comprend un certificat intermédiaire croisé

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

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

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

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

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

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

Important

Certaines autorités de certification disposent de plus d'un certificat racine. Si vous avez besoin de cette validation plus stricte, assurez-vous que votre configuration utilise le certificat racine approprié. Par exemple, il existe actuellement deux certificats (« DigiCert »/« GTE CyberTrust Global Root » et « DigiCert Baltimore Root »/« Baltimore CyberTrust Root ») qui peuvent valider les mêmes certificats de serveur. Sur certaines machines utilisateur, les deux certificats racine sont disponibles. Sur les autres machines, seul (« DigiCert Baltimore Root »/« Baltimore CyberTrust Root ») est disponible. Si vous configurez « GTE CyberTrust Global Root » sur la passerelle, les connexions Citrix Receiver pour Linux sur ces machines utilisateur échouent. Consultez la documentation de l'autorité de certification pour déterminer quel certificat racine doit être utilisé. Notez également que les certificats racine expirent éventuellement, comme tous les certificats.

Remarque

Certains serveurs et certaines passerelles n'envoient jamais le certificat racine, même si cela est configuré. Une validation plus stricte n'est par conséquent pas possible.

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

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

Citrix Receiver pour Linux utilisera ensuite ces deux certificats. Il recherche ensuite un certificat racine sur la machine utilisateur. S'il en trouve un qui est validé et également approuvé (tel que « Certificat racine exemple) », la connexion réussit.

Sinon, la connexion échoue. Veuillez noter que cette configuration fournit le certificat intermédiaire dont Citrix Receiver pour Linux a besoin, mais permet également à Citrix Receiver pour Linux de choisir un quelconque certificat racine valide et approuvé.

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

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

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

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

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

Important

Certaines autorités de certification utilisent un certificat intermédiaire avec signature croisée. Ce cas de figure est destiné aux situations dans lesquelles il existe plus d'un certificat racine, et qu'un certificat racine antérieur est toujours en cours d'utilisation en même temps qu'un certificat racine plus récent. Dans ce cas, il y aura au moins deux certificats intermédiaires. Par exemple, le certificat racine antérieur « Class 3 Public Primary Certification Authority » et le certificat intermédiaire avec signature croisée « VeriSign Class 3 Public Primary Certification Authority - G5 » correspondant. Toutefois, un certificat racine antérieur « VeriSign Class 3 Public Primary Certification Authority - G5 » correspondant est également disponible, et il remplace « Class 3 Public Primary Certification Authority ». Le certificat racine antérieur n'utilise pas de certificat intermédiaire avec signature croisée.

Remarque

Le certificat intermédiaire avec signature croisée et le certificat racine ont le même nom de sujet (Émis pour), mais le certificat intermédiaire avec signature croisée a un nom d'émetteur différent (Émis par). Cela permet de différencier le certificat intermédiaire avec signature croisée d'un certificat intermédiaire ordinaire (tel « Certificat intermédiaire exemple 2 »).

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

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

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

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

- « Certificat intermédiaire avec signature croisée 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 Citrix Receiver pour Linux ne peut pas trouver tous les certificats intermédiaires, la connexion échoue.

Configuration utilisateur requise

Même si vous n'avez pas besoin d'ouvrir une session en tant qu'utilisateur privilégié (root) afin d'installer Citrix Receiver pour Linux, la prise en charge des connexions USB est uniquement activée lorsque vous installez et configurez Receiver en tant qu'utilisateur privilégié. Les installations effectuées par des utilisateurs non privilégiés permettront cependant à ces derniers d'accéder aux ressources publiées à l'aide de StoreFront via l'un des navigateurs pris en charge ou de l'interface utilisateur native de Receiver.

Vérifier que votre machine répond à la configuration système requise

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

Pour exécuter le script hdxcheck.sh

1. Ouvrez une fenêtre de terminal.
2. Tapez cd $ICAROOT/util, puis appuyez sur ENTRÉE pour accéder au répertoire Utilities du pack d'installation.
3. Tapez ./hdxcheck.sh pour exécuter le script.

Installer et configurer

Jul 10, 2017

Les packages suivants sont disponibles pour Citrix Receiver pour Linux. Vous pouvez accéder aux packages à partir de la section de téléchargement du site Web de Citrix.

Nom du package	Contenu
Packages Debian (Ubuntu, Debian, Linux Mint etc.)	
icaclient_13.6.0.10243651_amd64.deb	Prise en charge du libre-service, 64 bits x86_64
icaclient_13.6.0.10243651_i386.deb	Prise en charge du libre-service, 32 bits x86
icaclient_13.6.0.10243651_armhf.deb	Prise en charge du libre-service, ARM HF
icaclient_13.6.0.10243651_armel.deb	Prise en charge du libre-service, ARM EL
icaclientWeb_13.6.0.10243651_amd64.deb	Receiver Web uniquement, 64 bits x86_64
icaclientWeb_13.6.0.10243651_i386.deb	Receiver Web uniquement, 32 bits x86
icaclientWeb_13.6.0.10243651_armhf.deb	Receiver Web uniquement, ARM HF
icaclientWeb_13.6.0.10243651_armel.deb	Receiver Web uniquement, ARM EL
ctxusb_2.7.10243651_amd64.deb	Package USB, 64 bits x86_64
ctxusb_2.7.10243651_i386.deb	Package USB, 32 bits x86
ctxusb_2.7.10243651_armhf.deb	Package USB, ARM HF
ctxusb_2.7.10243651_armel.deb	Package USB, ARM EL
Packages Redhat (Redhat, SUSE, Fedora etc.)	
ICAClient-rhel-13.6.0.10243651-0.x86_64.rpm	Prise en charge du libre-service, RedHat (y compris VDA Linux), 64 bits x86_64

ICAClient-rhel-13.6.0.10243651-0.i386.rpm	Prise en charge du libre-service, RedHat, 32 bits x86
ICAClientWeb-rhel-13.6.0.10243651-0.x86_64.rpm	Receiver Web uniquement, RedHat, 64 bits x86_64
ICAClientWeb-rhel-13.6.0.10243651-0.i386.rpm	Receiver Web uniquement, RedHat, 32 bits x86
ICAClient-suse-13.6.0.10243651-0.x86_64.rpm	Prise en charge du libre-service, SUSE, 64 bits x86_64
ICAClient-suse-13.6.0.10243651-0.i386.rpm	Prise en charge du libre-service, SUSE 11, 32 bits x86
ICAClient-suse11sp3-13.6.0.10243651-0.x86_64.rpm	Prise en charge du libre-service, SUSE 11 sp3 (y compris VDA Linux), 64 bits x86_64
ICAClient-suse11sp3-13.6.0.10243651-0.i386.rpm	Prise en charge du libre-service, SUSE 11 sp3, 32 bits x86
ICAClientWeb-suse-13.6.0.10243651-0.x86_64.rpm	Receiver Web uniquement, SUSE, 64 bits x86_64
ICAClientWeb-suse-13.6.0.10243651-0.i386.rpm	Receiver Web uniquement, SUSE, 32 bits x86
ctxusb-2.7.10243651-1.x86_64.rpm	Package USB, 64 bits x86_64
ctxusb-2.7.10243651-1.i386.rpm	Package USB, 32 bits x86
Tarballs (installation par script pour n'importe quelle distribution)	
linuxx64-13.6.0.10243651.tar.gz	Intel 64 bits
linuxx86-13.6.0.10243651.tar.gz	Intel 32 bits
linuxarmhf-13.6.0.10243651.tar.gz	ARM EL
linuxarm-13.6.0.10243651.tar.gz	ARM HF

icaclient_13.6.0.10243651_armel.deb La différence entre les packs qui offrent la prise en charge de Receiver Web et ceux qui offrent la prise en charge du libre-service tient au fait que ces derniers comprennent des dépendances requises pour le libre-service en plus de celles requises pour Receiver Web. Les dépendances du libre-service sont un sur-ensemble de celles

requises pour Receiver Web, mais les fichiers installés sont identiques.

Si vous n'avez besoin que de la prise en charge de Receiver Web, ou que votre distribution ne dispose pas des packs nécessaires pour prendre en charge le libre-service, installez uniquement le pack Receiver Web.

> ### Remarque
>
> Si votre distribution le permet, installez Citrix Receiver à partir du package Debian ou RPM. Ces fichiers sont généralement plus faciles à utiliser, car ils installent automatiquement tout autre package requis. Si vous voulez contrôler l'emplacement d'installation, installez Citrix Receiver à l'aide du pack tarball.

Pour installer Citrix Receiver pour Linux à partir d'un package Debian

Si vous installez Receiver à l'aide du package Debian sur Ubuntu, il peut s'avérer pratique d'ouvrir les packages dans le Ubuntu Software Centre.

Dans les instructions suivantes, remplacez ***nomdupack*** avec le nom du pack que vous installez.

Cette procédure utilise une ligne de commande et le gestionnaire de package natif pour Ubuntu/Debian/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 pack qui télécharge tous les logiciels requis manquants. Si aucun gestionnaire de pack n'est disponible, Citrix vous recommande **gdebi**, un outil de ligne de commande qui remplit cette fonction.

Pour installer un 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 3 packages suivants en tapant **gdebi packagename.deb**. Par exemple :

- gdebi icaclient_13.4.0.10109380_amd64.deb
- gdebi icaclient_13.4.0.10109380_amd64.deb
- gdebi ctxusb_2.7.10109380_amd64.deb

Remarque : pour utiliser dpkg dans les exemples ci-dessus, remplacez « gdebi » par « dpkg -i ».

Un utilisateur doit installer le pack icaclient ou icaclientWeb. Le pack ctxusb est facultatif. Il permet de prendre en charge la redirection USB générique.

4. Si vous utilisez dkpg, installez les dépendances manquantes en tapant sudo **apt-get -f install**.
5. Acceptez le EULA.

Pour installer Citrix Receiver pour Linux à partir d'un pack RPM

Si vous installez Citrix Receiver à partir du package RPM sur SUSE, utilisez l'utilitaire YaST ou Zypper, et non l'utilitaire RPM. L'utilitaire RPM ne télécharge et n'installe aucune des dépendances nécessaires ; il installe uniquement le package .rpm. Si les dépendances nécessaires sont manquantes, vous recevrez un message d'erreur.

Remarque : pour suivre un exemple d'installation à l'aide d'un package RPM, consultez l'article du blog Citrix Installation de

Citrix Receiver pour Linux 13.2.1 sur SUSE Linux Enterprise Desktop.

Dans les instructions suivantes, remplacez ***nomdupack*** avec le nom du pack que vous installez.
Remarque : si vous recevez une erreur indiquant que l'installation « ... requiert libwebkitgtk-1.0.so.0 » sur les distributions Red Hat (RHEL, CentOS, Fedora, etc.), ajoutez le référentiel EPEL (vous trouverez des informations supplémentaires sur https://fedoraproject.org/wiki/EPEL) pour ajouter le package manquant, ou utilisez la variante Web du package.

Pour définir le référentiel EPEL sur Red Hat

1. Téléchargez le package RPM source approprié ici :

    https://fedoraproject.org/wiki/EPEL#How_can_I_use_these_extra_packages.3

2. Par exemple, pour Red Hat Enterprise 7.x :

    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, Citrix vous recommande d'utiliser **zypper install** sur une ligne de commande sur OpenSUSE ou **yum localinstall** sur Fedora/Red Hat.

Après avoir défini le référentiel EPEL, installez Receiver à partir du package RPM.

1. Ouvrez une session en tant qu'utilisateur (racine) privilégié.

2. Exécutez l'installation pour les 3 packages suivants en tapant zypper dans packagename.rpm.

Remarque : un utilisateur doit installer le pack icaclient ou icaclientWeb. Le pack ctxusb est facultatif. Il permet de prendre en charge la redirection USB générique.

3. Ouvrez une fenêtre de terminal.

    Pour les installations SUSE :

    zypper in ICAClient-suse-13.4.0.10109380-0.x86_64.rpm

    zypper in ICAClient-suse-13.4.0.10109380-0.x86_64.rpm

    zypper in ctxusb-2.7.10109380-1.x86_64.rpm

    Pour les installations Red Hat :

    yum localinstall ICAClient-rhel-13.4.0.10109380-0.i386.rpm

    yum localinstall ICAClientWeb-rhel-13.4.0.10109380-0.i386.rpm

    yum localinstall ctxusb-2.7.10109380-1.i386.rpm

4. Acceptez le EULA.

Pour installer Citrix Receiver pour Linux à partir d'un pack tarball
Remarque : le package tarball ne vérifie pas les dépendances et n'installe pas non plus les dépendances. Toutes les dépendances système devront être résolues indépendamment.

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

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

Pour un utilisateur non privilégié, le répertoire d'installation par défaut est $HOME/ICAClient/plate-forme. (où 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, entrez y et appuyez sur Entrée.

7. Vous pouvez choisir d'intégrer ou non Receiver à votre environnement de bureau. L'installation crée une option de menu à partir de laquelle les utilisateurs peuvent démarrer Receiver. Tapez **y** lorsque vous y êtes invité pour activer l'intégration.

8. Si vous avez déjà installé GStreamer, vous pouvez choisir de l'intégrer à Receiver, ce qui permet la prise en charge de l'accélération multimédia HDX Mediastream.Pour intégrer GStreamer à Receiver, entrez y lorsque vous y êtes invité.

Remarque : sur certaines plates-formes, l'installation du client à partir d'une distribution 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 l'exécution de cette commande, vous pouvez exécuter de nouveau le fichier tarball sans rencontrer de blocage.

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 XenDesktop et XenApp.Entrez 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 ce programme, entrez 3 et appuyez sur Entrée.

Personnaliser une installation de Citrix Receiver pour Linux

Jul 10, 2017

Vous pouvez personnaliser une configuration avant l'installation en modifiant le contenu du package de Citrix Receiver et en reconditionnant les fichiers. Vos modifications seront appliquées à chaque version installée à l'aide du package modifié.

Pour personnaliser une installation de Citrix Receiver pour Linux

1. Développez le fichier du package de Citrix Receiver dans un répertoire vide. Le fichier du pack 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 pack Citrix Receiver. À titre d'exemple, vous pouvez également ajouter un nouveau certificat racine TLS au pack si vous souhaitez utiliser un certificat à partir d'une autorité de certification ne faisant pas partie de l'installation standard de Receiver. Pour ajouter un nouveau certificat racine TLS au package, consultez la rubrique
   — Installer des certificats racine sur des machines utilisateur
   dans le site de documentation sur les produits de Citrix. Pour de plus amples informations sur les certificats intégrés, consultez la rubrique
   — Configurer et activer SSL et TLS
   dans le site de documentation sur les produits de Citrix.
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. La forme exacte de cette information est sans importance.
5. Enregistrez, puis fermez le fichier.
6. Ouvrez la liste des fichiers de pack, platform/platform.psf (par exemple, linuxx86/linuxx86.psf pour la plate-forme Linux/x86).
7. Actualisez la liste des fichiers du pack pour refléter les modifications que vous avez apportées au pack. Si ce fichier n'est pas mis à jour, des erreurs peuvent se produire au moment de l'installation de votre nouveau pack. Parmi ces modifications, il peut s'agir de mettre à jour la taille des fichiers que vous avez modifiés ou d'ajouter de nouvelles lignes pour tous les fichiers ajoutés au pack. Les colonnes de la liste des fichiers du pack sont :
   - Type de fichier
   - Chemin d'accès relatif
   - Sous-pack (qui doit toujours être défini sur cor)
   - Autorisations
   - Propriétaire
   - Groupe
   - Taille
8. Enregistrez, puis fermez le fichier.
9. Utilisez la commande tar pour reconditionner le fichier du pack Receiver, par exemple : tar czf ../newpackage.tar.gz * où newpackage est le nom du nouveau fichier du pack Receiver.

Démarrer Citrix Receiver pour Linux

Jul 10, 2017

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

Si Citrix Receiver n'est pas installé dans le répertoire d'installation par défaut, assurez-vous que la variable d'environnement ICAROOT est définie de manière à pointer vers le répertoire d'installation réel.

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

Pour démarrer Citrix Receiver à l'invite du terminal

À partir de l'invite du terminal, entrez /opt/Citrix/ICAClient/selfservice et appuyez sur ENTRÉE (où /opt/Citrix/ICAClient est le répertoire dans lequel vous avez installé Citrix Receiver).

Pour démarrer Citrix Receiver à partir du bureau Linux

Vous pouvez démarrer Citrix Receiver à partir d'un environnement de bureau pour Linux en y accédant à l'aide d'un gestionnaire de fichiers.

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

Utiliser Citrix Receiver pour Linux en tant que ICA vers proxy X

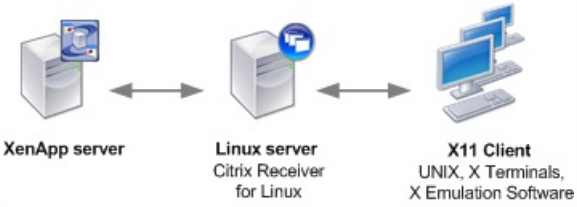
Jul 10, 2017

Vous pouvez utiliser une station de travail exécutant Citrix Receiver 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 Citrix Receiver n'est pas disponible.

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

Lorsque vous exécutez Citrix Receiver, 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. Ainsi, vous pouvez exécuter plusieurs copies de Citrix Receiver simultanément sur un même système, chacune envoyant sa sortie sur une machine différente.

Ce graphique montre un système avec Citrix Receiver 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 Citrix Receiver 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 Citrix Receiver n'est pas disponible, vous avez besoin d'un serveur supplémentaire faisant office de proxy. Il peut s'agir d'un ordinateur sous Linux.

Fonctionnalités prises en charge

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 devez accéder à l'imprimante UNIX manuellement depuis le serveur à l'aide de l'impression LPD, ou utiliser une imprimante réseau.
- La redirection des entrées multimédia n'est pas censée fonctionner car elle nécessite une webcam sur l'ordinateur qui exécute Citrix Receiver, 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 Citrix Receiver 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 <proxy server name>
4. Si Receiver n'est pas installé dans le répertoire d'installation par défaut, assurez-vous que la variable d'environnement ICAROOT est définie de manière à pointer vers le répertoire d'installation réel.
5. Localisez le répertoire dans lequel Citrix Receiver a été installé. À l'invite de commande, tapez selfservice &.

Pour désinstaller Citrix Receiver pour Linux

Jul 10, 2017

Cette procédure a été testée avec le pack tarball. Supprimez les packs 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/plate-forme. La variable de plate-formeest 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.

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.

> ## Remarque
>
> Pour désinstaller Citrix Receiver pour Linux, vous devez avoir ouvert une session en tant qu'utilisateur identique à celui qui a réalisé l'installation.

Se connecter

Jul 10, 2017

Citrix Receiver 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 de Citrix Receiver

La page d'accueil de Citrix Receiver affiche les applications et les bureaux virtuels mise 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 XenApp ou Citrix XenDesktop. À l'aide de la page Préférences > Comptes, les utilisateurs peuvent effectuer la configuration eux-mêmes en entrant l'adresse URL d'un serveur StoreFront ou, si la découverte de compte par e-mail est configurée, en entrant leur 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 PNAgent, l'URL du magasin est affichée et identifie de manière unique le magasin.

Après la connexion à un magasin, le self-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 Citrix Receiver et les serveurs XenApp et XenDesktop. Le cas échéant, vous pouvez également modifier ces paramètres pour des connexions individuelles.

Le reste de cette section contient des procédures permettant de réaliser des tâches courantes effectuées par les utilisateurs de Citrix Receiver. Bien que certaines tâches et responsabilités respectives des administrateurs et des utilisateurs puissent coïncider, le terme « utilisateur » est employé dans cette section 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
- Résoudre les problèmes de connexion aux ressources
- Personnaliser Receiver à l'aide de fichiers de configuration

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

Jul 10, 2017

Vous créez les connexions aux serveurs lorsque vous cliquez sur une icône de bureau ou d'application sur la page d'accueil de Receiver. 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

Avant de commencer, assurez-vous que le magasin est connu par Citrix Receiver. Si nécessaire, ajoutez-le à l'aide de la commande suivante :

./util/storebrowse –addstore

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

     ./util/storebrowse -E
   - Liste des bureaux et applications auxquels vous êtes abonné :

     ./util/storebrowse -S
2. Exécutez la commande suivante pour démarrer le bureau ou l'application :
   ./util/storebrowse – L

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 la section Connexion via un 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. Notez qu'en raison du large éventail de navigateurs et de systèmes d'exploitation, il est possible qu'une configuration manuelle soit requise.

Si vous avez besoin de configurer manuellement les fichiers .mailcap et MIME pour Firefox, Mozilla ou Chrome, utilisez les modifications de fichier suivantes de manière à ce que les fichiers .ica lancent l'exécutable de Receiver, wfica. Pour utiliser d'autres navigateurs, vous devez modifier la configuration du navigateur en conséquence.

1. Exécutez les commandes suivantes pour l'installation non administrateur de Citrix Receiver. Les paramètres de ICAROOT sont susceptibles de changer s'ils sont installés sur un emplacement autre que l'emplacement par défaut. Vous pouvez tester le résultat avec la commande « xdg-mime query default application/x-ica » qui doit renvoyer « wfica.desktop ».
   setenv ICAROOT=/opt/Citrix/ICAClient

   xdg-icon-resource install --size 64 "$ICAROOT/icons/000_Receiver_64.png Citrix-Receiver"

   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 une 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;

Notez que vous devrez peut-être configurer Firefox sur la page Préférences/Applications. Pour « Citrix ICA settings file content », sélectionnez « Citrix Receiver Engine (default) » dans le menu déroulant. Ou sélectionnez « Use other ... » et sélectionnez le fichier /usr/share/applications/wfica.desktop (pour une installation administrateur de Receiver) ou $HOME/.local/share/applications/wfica.desktop (pour une installation non administrateur).

Résoudre les problèmes de connexion aux ressources

Jul 10, 2017

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. Cela met fin à la session et ferme toutes les applications ouvertes.
- Déconnectant une session. Cela coupe 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.

Pour gérer une connexion

1. Sur le menu Receiver, cliquez sur Centre de connexion.
   Les serveurs qui sont utilisés sont affichés et, pour chaque serveur, les sessions actives sont répertoriées.

2. Procédez comme suit :
   - Sélectionnez un serveur, déconnectez-vous, fermez la session ou affichez les propriétés.
   - Sélectionnez une application et fermez la fenêtre dans laquelle elle est affichée.

Personnaliser à l'aide de fichiers de configuration

Jul 10, 2017

À propos des fichiers de configuration

Pour modifier des paramètres avancés ou moins courants, vous pouvez modifier les fichiers de configuration de Receiver. 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.

Sachez que, 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.

Appliquer valeur par défaut à tous les utilisateurs de Citrix Receiver

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

> **Remarque**
>
> vous n'avez pas besoin d'ajouter d'entrée au fichier All_Regions.ini pour une valeur de configuration devant être lue à partir de module.ini, sauf si vous souhaitez autoriser d'autres fichiers de configuration à remplacer la valeur dans le fichier module.ini. Si une entrée du fichier All_Regions.ini définit une valeur spécifique, la valeur du fichier module.ini n'est pas utilisée.

Appliquer des modifications aux nouveaux utilisateurs de Citrix Receiver

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, elles s'appliquent à tous les futurs nouveaux utilisateurs de Citrix Receiver.

Appliquer des modifications à toutes les connexions pour des utilisateurs spécifiques

Si vous souhaitez que ces modifications s'appliquent à toutes les connexions pour un utilisateur spécifique, modifiez le fichier wfclient.ini dans le répertoire $HOME/.ICAClient de l'utilisateur en question. Les paramètres de ce fichier s'appliquent aux futures connexions pour cet utilisateur.

Valider les entrées du fichier de configuration

Si vous souhaitez 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 possible, cette valeur est utilisée. Notez que $HOME/.ICAClient/All_Regions.ini peut uniquement correspondre ou réduire les valeurs possibles définies par $ICAROOT/config/All_Regions.ini, il ne peut pas éliminer les restrictions. Pour de plus amples informations, veuillez consulter le fichier All_Regions.ini dans le répertoire $ICAROOT/config.

> **Remarque**
>
> si une entrée apparaît dans plusieurs fichiers de configuration, une valeur dans le fichier wfclient.ini prévaut sur une valeur dans le fichier module.ini.

À propos des paramètres dans les fichiers

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

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

Priorité

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

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

1. All_Regions.ini. Les valeurs de ce fichier écrasent celles dans :
   - Le fichier .ica de connexion
   - 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 de la connexion où le fichier wfclient.ini, mais elles ne sont pas limitées par des entrées dans le fichier All_Regions.ini.

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

> **Remarque**
>
> il existe des exceptions à cet ordre de priorité. Par exemple, le code lit certaines valeurs spécifiquement dans le fichier wfclient.ini pour des raisons de sécurité, pour s'assurer qu'elles ne sont pas définies par un serveur.

Configurer les connexions Citrix XenApp (anciennement PNAgent) à l'aide de l'Interface Web

Jul 10, 2017

Cette rubrique s'applique uniquement aux déploiements utilisant des sites XenApp Services sur l'Interface Web ou des sites « PNA d'ancienne génération » sur StoreFront.

Les options telles que selfservice, storebrowse et pnabrowse permettent aux utilisateurs de se connecter à des ressources publiées (c'est-à-dire des applications et des bureaux de serveur publiés) via un serveur exécutant un site XenApp Services. Ces programmes peuvent lancer des connexions directement ou peuvent être utilisés pour créer des éléments de menu par le biais desquels les utilisateurs peuvent accéder à des ressources publiées. pnabrowse peut également créer des éléments de bureau à cette fin.

Des options personnalisables pour tous les utilisateurs exécutant Citrix XenApp sur votre réseau sont définies dans un fichier de configuration, config.xml, qui est stocké sur le serveur de l'Interface Web. Lorsqu'un utilisateur lance l'un de ces programmes, les données de configuration sont lues à partir du serveur. Ce programme met ensuite à jour ses paramètres et son interface utilisateur de manière périodique, selon l'intervalle spécifié dans le fichier config.xml.

> ## Important
>
> Le fichier config.xml affecte toutes les connexions définies par le site XenApp Services.

Publier du contenu

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

Il existe toutefois une restriction concernant les types de fichiers reconnus par Receiver. Pour que le système puisse reconnaître le type de fichier du contenu publié et pour que les utilisateurs puissent le visualiser dans Receiver, une application publiée doit être associée au type de fichier du fichier publié. À titre d'exemple, pour visualiser un fichier Adobe PDF à l'aide de Receiver, 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.

Optimiser

Jul 10, 2017

En optimisant votre environnement, vous obtenez des performances maximales de la part de Citrix Receiver et offrez une meilleure expérience utilisateur. Vous pouvez améliorer et optimiser les performances comme suit :

- Mappage des machines utilisateur
- Configuration de la prise en charge USB
- Amélioration des performances pour les connexions à faible bande passante
- Amélioration des performances multimédias
- Optimisation des performances des mosaïques d'écran

Mappage des machines utilisateur

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

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

Mappage des lecteurs clients

Le mappage des lecteurs clients permet d'affecter des lettres de lecteur du serveur XenApp ou XenDesktop 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 Receiver.

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

Deux types de mappage de lecteur sont disponibles :

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

Lorsque Citrix Receiver se connecte à XenApp ou XenDesktop, 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 plus d'informations, veuillez consulter la

documentation relative à XenApp et XenDesktop.

Les utilisateurs peuvent mapper les lecteurs à l'aide de la boîte de dialogue Préférences. Pour de plus amples informations sur ce sujet, consultez la section Définir les préférences.

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

Mappage des imprimantes clientes

Citrix Receiver 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, XenApp 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 de tous les utilisateurs Receiver (ceux-ci correspondant dans ce cas aux personnes utilisant le programme selfservice pour la première fois après la modification).
2. dans la section [WFClient] du type de fichier :
   ClientPrinterList=printer1:printer2:printer3

   où printer1, printer2, etc. correspondent aux noms des imprimantes sélectionnées. Séparez les entrées de nom d'imprimante par deux-points (:).

3. Enregistrez, puis fermez le fichier.

Mappage d'imprimantes clientes sur XenApp pour Windows

Citrix Receiver pour Linux prend en charge le pilote d'imprimante universel PS Citrix. C'est la raison pour laquelle, dans la plupart des cas, il est inutile de définir une configuration locale pour les utilisateurs souhaitant imprimer sur des imprimantes réseau ou sur des imprimantes locales connectées aux machines utilisateur. Il peut toutefois s'avérer nécessaire de mapper manuellement des imprimantes clientes sur XenApp 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 Citrix Receiver, établissez une connexion avec le serveur et ouvrez une session sur un ordinateur exécutant

XenApp.

2. Dans le menu Démarrer, cliquez sur Paramètres > Imprimantes.
3. Dans le menu Fichier, cliquez sur 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. Dans la plupart des cas, il s'agit d'une imprimante au nom standard, semblable à celles créées par les Services Bureau à distance natifs, tels que « HP LaserJet 4 depuis NomClient dans la session 3 ».

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

Mappage d'imprimantes clientes sur XenApp pour UNIX

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

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

Mappage audio du client

Le mappage audio du client permet aux applications fonctionnant sur le serveur XenApp ou XenDesktop 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 plus d'informations, veuillez consulter la documentation relative à XenApp et XenDesktop.

Remarque : le mappage audio du client n'est pas pris en charge pour les connexions à Citrix XenApp sur UNIX.

Pour définir un périphérique audio autre que celui par défaut

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 Personnaliser Receiver à l'aide de fichiers de configuration.
2. Ajoutez l'option suivante, en créant la section si besoin est :

[ClientAudio]

AudioDevice = <device>

où l'information device se situe dans le fichier de configuration ALSA de votre système d'exploitation.
Remarque : l'emplacement de cette information peut varier en fonction des systèmes d'exploitation Linux. Pour plus de détails sur l'emplacement de cette information, Citrix vous recommande de consulter la documentation de votre système d'exploitation.

Configuration de la prise en charge USB

La prise en charge USB permet aux utilisateurs d'interagir avec une large gamme de périphériques USB connectés au bureau virtuel. Les utilisateurs peuvent brancher des périphériques USB sur leurs ordinateurs et les périphériques sont redirigés sur leurs bureaux virtuels. Les périphériques USB suivants sont pris en charge : lecteurs flash, smartphones, ordinateurs de poche, imprimantes, scanners, lecteurs MP3, périphériques de sécurité et tablettes.

La redirection USB nécessite XenApp 7.6 (ou version ultérieure) ou XenDesktop. Veuillez noter que XenApp ne prend pas en charge la redirection USB des périphériques de stockage de masse et requiert une configuration spéciale pour prendre en charge des périphériques audio. Veuillez consulter la documentation XenApp 7.6 pour plus de détails.

Les fonctions isochrones des périphériques USB tels que les webcams, les micros, les haut-parleurs et les casques sont prises en charge dans les environnements LAN (réseaux locaux) à faible latence et à haut débit, bien que dans la plupart des cas, la redirection audio ou de webcam standard est tout à fait appropriée.

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

- Claviers
- Souris
- Cartes à puce
- Casques
- Caméras Web

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 CTX 119722.
Par défaut, certains types de périphériques USB ne sont pas pris en charge pour l'accès distant via XenDesktop. Par exemple, une carte d'interface réseau peut être reliée à la carte système par une connexion USB interne. Il n'est pas conseillé de configurer un accès distant dans ce cas. Par défaut, les types de périphériques USB suivants ne sont pas pris en charge pour une utilisation dans une session XenDesktop :

- Dongles Bluetooth
- Cartes d'interface réseau intégrées
- Concentrateurs USB

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

Pour permettre l'envoi des périphériques USB sur les bureaux virtuels, activez la règle de stratégie USB. Pour plus d'informations, veuillez consulter la documentation de XenDesktop.

Fonctionnement de la prise en charge USB

Lorsqu'un utilisateur branche un périphérique USB, ce dernier est comparé à la stratégie USB, et s'il est autorisé, il est redirigé

sur le bureau virtuel. Si la stratégie par défaut refuse le périphérique, il n'est disponible que sur le bureau local.

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

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

Périphériques de stockage de masse

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

Remarque : si vous connectez un périphérique de stockage de masse à un poste de travail Linux configuré pour refuser la prise en charge à distance de ce type d'équipement USB, le périphérique n'est pas accepté par le logiciel Receiver et un navigateur de fichiers Linux 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, procédez comme suit : dans la barre de menus Debian, sélectionnez Desktop > Preferences > Removable Drives and Media, puis cliquez sur l'onglet Storage. Sous Removable Storage, désélectionnez la case à cocher Browse removable media when inserted.
Remarque : si la stratégie de serveur Redirection du périphérique USB client est activée, les périphériques de stockage de masse sont toujours redirigés en tant que périphériques USB même si le mappage du lecteur client est activé.

Caméras Web

De manière générale, la compression vidéo de caméra Web HDX RealTime offre des performances optimales. Toutefois, dans certaines circonstances, vous pouvez demander aux utilisateurs de connecter leur caméra Web à l'aide d'un port USB. Pour ce faire, vous devez désactiver la compression vidéo de webcam HDX RealTime. Pour plus d'informations veuillez consulter la section Configurer une compression vidéo de caméra Web HDX RealTime.

Classes USB autorisées par défaut

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

Audio (Classe 01)

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

Interface physique (Classe 05)

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

Acquisition d'images fixes (Classe 06)

Comprend scanners et appareils photo numériques. Les appareils photo numériques prennent généralement en charge la classe d'acquisition d'images fixes qui utilise le protocole PTP (Picture Transfer Protocol) ou MTP (Media Transfer Protocol) pour transférer des images sur un ordinateur ou un autre périphérique. Les appareils photo peuvent également apparaître

comme périphériques de stockage de masse et il est possible de configurer un appareil photo pour utiliser les deux classes, par le biais des menus fournis par l'appareil photo.

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

Imprimantes (Classe 07)

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

Les imprimantes fonctionnent correctement sans prise en charge USB.

Stockage de masse (Classe 08)

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

- 01 Périphériques flash limités
- 02 Lecteurs de CD/DVD (ATAPI/MMC-2)
- 03 Lecteurs de bandes (QIC-157)
- 04 Lecteurs de disquettes (UFI)
- 05 Lecteurs de disquettes (SFF-8070i)
- 06 La plupart des périphériques de stockage de masse utilisent cette variante de SCSI.

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

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

Sécurité du contenu (Classe 0d)

Les périphériques de sécurité du contenu assurent la protection du contenu, en général pour la gestion des licences ou des droits numériques. Cette classe comprend les dongles.

Santé personnelle (Classe 0f)

Ces appareils comprennent des capteurs de pression artérielle, des moniteurs de pouls, des podomètres, des piluliers et des spiromètres.

Spécifique au fabricant et à l'application (Classes fe et ff)

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

Classes de périphériques USB refusées par défaut

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

Communications et contrôle CDC (Classes 02 et 0a)

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

La stratégie USB par défaut n'autorise pas ces périphériques, car l'un d'entre eux peut fournir la connexion au bureau virtuel.

Périphériques d'interface utilisateur (Classe 03)

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

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

La stratégie USB par défaut n'autorise ni les claviers USB (classe 03, sous-classe 01, protocole 1), ni les souris USB (classe 03, sous-classe 01, protocole 2). Ceci est dû au fait que la majorité des claviers et souris sont correctement gérés sans prise en charge USB et 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.

Mise à jour de la liste des périphériques USB disponibles pour l'accès à distance

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

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

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

DENY: class=09 # Hub devices

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

DENY: class=0b # Smartcard

DENY: class=e0 # Wireless Controllers

DENY: class=02 # Communications and CDC Control

DENY: class=03 # UVC (webcam)

DENY: class=0a # CDC Data

ALLOW: # Ultimate fallback: allow everything else

Création de 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
Class	Classe du descripteur de périphérique ou d'un descripteur d'interface
Sous-classe	Sous-classe du descripteur de périphérique ou d'un descripteur d'interface
Prot	Protocole à partir du descripteur de périphérique ou d'un descripteur d'interface

Balise	Description

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 de fin, introduit par #. 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

Configurer des modes de démarrage

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

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

Amélioration des performances pour les connexions à faible bande passante

Citrix recommande d'utiliser la version la plus récente de XenApp ou de XenDesktop sur le serveur et de Receiver 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 Receiver et la façon dont vous utilisez ce dernier.

- **Configurez votre connexion Receiver** : la configuration de vos connexions Receiver peut réduire la bande passante requise par ICA et améliorer les performances.
- **Modifiez la façon dont Receiver est utilisé** : modifier la façon dont Receiver est utilisé 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 XenApp et Receiver pour Linux** : Citrix améliore les performances à chaque nouvelle version ; de ce fait, de nombreuses fonctions nécessitent la dernière version de Receiver et du logiciel serveur.

Configuration des 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 Receiver, cette fonctionnalité est désactivée pour le clavier et uniquement activée pour la souris sur les connexions à latence élevée. Consultez le *— Guide de référence OEM de Citrix Receiver pour Linux* .
- **Activer la compression de données** : la compression des données réduit le volume des données transférées via la connexion. Ce processus requiert des ressources processeur supplémentaires pour compresser et décompresser les données, mais permet d'améliorer les performances des connexions à faible bande passante. Utilisez les paramètres de stratégie Citrix Qualité audio et Compression d'image pour activer cette fonctionnalité.
- **Réduire la taille de la fenêtre** : modifiez la taille de fenêtre jusqu'à ce que vous atteigniez une taille de lecture confortable. Sur le site XenApp Services, définissez les options de session.
- **Réduire le nombre de couleurs** : réduit le nombre de couleurs à 256. Sur le site XenApp Services, 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.

Activation de l'audio UDP

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

Tenez compte de ce qui suit :

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

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

		Qualité audio sur le client		
		Élevé	Modéré	Faible
	Élevé	Élevé	Modéré	Faible

Qualité audio sur le serveur	Modéré	Modéré	Modéré	Faible
	Faible	Faible	Faible	Faible

Si l'audio UDP est activé mais que la qualité n'est pas moyenne, la transmission audio utilisera TCP et non UDP.

Modification de la manière d'utiliser Receiver

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

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

Amélioration des performances multimédias

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

- Redirection HDX Mediastream Windows Media
- Redirection Flash HDX MediaStream
- Compression vidéo de webcam HDX RealTime
- Prise en charge H.264

Configuration de la 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. Ainsi, les besoins en bande passante pour la lecture de fichiers multimédia sont limités.

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

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

Citrix Receiver comprend un tableau de traduction texte configurable, MediaStreamingConfig.tbl, pour la traduction des GUID des formats multimédia spécifiques à Windows en types MIME utilisables par GStreamer. Vous pouvez mettre à jour le

tableau de traduction en effectuant les opérations suivantes :

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

Avec la récupération côté client, vous pouvez également autoriser la machine utilisateur à streamer du multimédia directement depuis des adresses URL au format http://, mms:// ou rtsp:// plutôt que via un serveur Citrix. Le serveur est chargé de diriger la machine utilisateur vers le multimédia et d'envoyer les commandes de contrôle (y compris Lecture, Pause, Stop, Volume, Recherche) mais 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 Citrix Receiver afin de permettre au processus d'installation de configurer Citrix Receiver 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 diffuseront 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. À titre d'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 Citrix Receiver sur la machine, sélectionnez l'option GStreamer si vous utilisez le script tarball (ceci est réalisé automatiquement pour les packages .deb et .rpm).

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

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

Note à propos de GStreamer 1.0 :

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

1. Localisez le répertoire d'installation des plug-ins GStreamer. En fonction de votre distribution, de l'architecture du système d'exploitation et de la manière dont vous installez GStreamer, l'emplacement d'installation des plug-ins varie. Le chemin d'accès de l'installation par défaut est /usr/lib/x86_64-linux-gnu/gstreamer-1.0 ou $HOME /.local/share/gstreamer-1.0.
2. Localisez le répertoire d'installation de Citrix Receiver 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/plate-forme (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.

Configuration de la redirection HDX MediaStream Flash

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

1. Assurez-vous que votre machine utilisateur dispose des fonctionnalités requises. Pour plus d'informations, veuillez consulter la section Configuration requise.
2. Ajoutez les paramètres suivants à la section [WFClient] du fichier wfclient.ini (pour toutes les connexions effectuées par un utilisateur spécifique) ou à la section [Client Engine\Application Launching] du fichier All_Regions.ini (pour tous les utilisateurs de votre environnement) :

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

   - **HDXFlashEnableServerSideContentFetching=Disabled | Enabled**
     Active ou désactive la récupération de contenu côté serveur pour Receiver. Par défaut, cette option est définie sur **Disabled**.

   - **HDXFlashUseServerHttpCookie=Disabled | Enabled**
     Active ou désactive la redirection des cookies HTTP. Par défaut, cette option est définie sur **Disabled**.

   - **HDXFlashEnableClientSideCaching=Disabled | Enabled**
     Active ou désactive la mise en cache côté client du contenu Web récupéré par Receiver. Par défaut, cette option est définie sur **Enabled**.

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

- **HDXFlashServerSideContentCacheType=Persistent | Temporary | NoCaching**
  Définit le type de mise en cache utilisé par Receiver pour le contenu récupéré côté serveur. Par défaut, cette option est définie sur **Persistent**.
  Remarque : ce paramètre est requis uniquement 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.

Configurer une compression vidéo de caméra Web HDX RealTime

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

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

Désactiver la compression vidéo de caméra Web HDX RealTime

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

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

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

   HDXWebCamEnabled=Off

   Pour plus d'informations, reportez-vous à Personnaliser Receiver à l'aide de fichiers de configuration.

2. Ouvrez le fichier usb.conf, généralement situé sous $ICAROOT/usb.conf.
3. Supprimez ou ajoutez en commentaire la ligne suivante :

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

Configuration de la prise en charge de H.264

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

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

complexes mais très peu de texte ou du texte non critique.

Important : pour configurer cette fonctionnalité, n'utilisez pas de paramètre sans perte dans la stratégie XenDesktop Qualité visuelle. Si vous utilisez un paramètre avec perte, le codage H.264 est désactivé sur le serveur et ne fonctionne pas dans Receiver.

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

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

Pour désactiver le suivi de texte uniquement

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

Optimisation des performances des mosaïques d'écran

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

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

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

Améliorer l'expérience utilisateur

Jul 10, 2017

Vous pouvez améliorer l'expérience de vos utilisateurs grâce aux fonctionnalités prises en charge suivantes :

- Définition de préférences
- Configuration du lissage de polices ClearType
- Configuration de la redirection de dossiers spéciaux
- Configuration de la redirection de contenu du serveur vers le client
- Contrôle du comportement du clavier
- Utilisation de xcapture
- Reconnexion automatique des utilisateurs
- Garantir la fiabilité de session
- Souris relative

Définition de préférences

Vous pouvez définir des préférences en cliquant sur Préférences dans le menu de Citrix Receiver. Vous pouvez contrôler la façon dont les bureaux sont affichés, vous connecter à différentes applications et différents bureaux, et gérer l'accès aux périphériques et fichiers.

Pour gérer un compte

Pour accéder aux bureaux et applications, vous devez disposer d'un compte avec XenDeskop ou XenApp. Votre service d'assistance informatique peut vous aider à ajouter un nouveau compte pour Citrix Receiver à cette fin, ou ils peuvent vous demander d'utiliser un serveur NetScaler Gateway ou Access Gateway différent pour un compte existant. Vous pouvez également supprimer des comptes à partir de Citrix Receiver.

1. Sur la page Comptes de la boîte de dialogue Préférences, effectuez l'une des opérations suivantes :
   - Pour ajouter un compte, cliquez sur Ajouter. Votre service d'assistance peut également fournir un fichier de provisioning avec les informations de compte que vous pouvez utiliser pour créer un nouveau compte.
   - 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. Vous devrez peut-être vous authentifier auprès du serveur.

Pour modifier l'affichage de vos bureaux

Cette fonctionnalité n'est pas disponible avec les sessions Citrix XenApp pour UNIX.

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

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

Receiver pour Linux est maintenant doté d'une barre d'outils **Vous pouvez activer Desktop Viewer** qui permet de modifier de manière dynamique la configuration de la fenêtre de votre session distante à partir des paramètres d'origine spécifiés par la configuration mentionnée ici.

Desktop Viewer

Différentes entreprises ont différents besoins d'entreprise. Votre configuration requise pour la manière dont les utilisateurs accèdent aux bureaux virtuels d'un utilisateur à un autre et peut varier lorsque vos besoins sont en constante évolution. L'expérience utilisateur relative à la connexion aux bureaux virtuels et le degré d'intervention de l'utilisateur dans la configuration des connexions dépendent de la manière dont vous avez configuré Receiver pour Linux.

Utilisez Desktop Viewer lorsque vos utilisateurs doivent interagir avec leur bureau virtuel. Le bureau virtuel de l'utilisateur peut être un bureau virtuel publié ou un bureau dédié ou partagé. Dans ce scénario d'accès, la barre d'outils de Desktop Viewer permet à l'utilisateur de passer d'une session en mode fenêtre à une session en mode plein écran, et prend également en charge le multi-écrans pour les moniteurs d'intersection. Les utilisateurs peuvent basculer entre les sessions de bureau et travailler avec plusieurs bureaux à l'aide de connexions XenDesktop 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.

En tant que fonctionnalité d'accessibilité de Desktop Viewer, la combinaison Ctrl+Alt+Attn affiche les boutons de la barre d'outils Desktop Viewer dans une fenêtre contextuelle.

Pour activer ou désactiver Desktop Viewer ou changer la séquence des touches d'accessibilité, reportez-vous aux entrées de configuration avancée disponibles dans le guide OEM de Linux.

Pour se reconnecter aux sessions automatiquement

Citrix Receiver ne peut pas 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.

Pour contrôler la méthode d'accès 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 ne peut pas y accéder en écriture.
   - Aucun accès : n'autorise ni le bureau ni l'application à accéder aux fichiers locaux.*
   - Toujours me demander : affiche une invite chaque fois que le bureau ou l'application requiert un accès aux fichiers locaux.
2. Si vous avez sélectionné l'une des options qui accorde l'accès aux fichiers locaux, vous pouvez également gagner du temps lors de l'accès à des emplacements sur votre machine utilisateur. Cliquez sur Ajouter, spécifiez l'emplacement et sélectionnez un lecteur à mapper.

Pour définir un micro ou une webcam

Vous pouvez modifier la façon dont une application ou un bureau virtuel accède à votre micro 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.

Pour configurer le 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.

Configuration du lissage de polices ClearType

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

FontSmoothingType = number

où number peut prendre l'une des valeurs suivantes :

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

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

Important : le serveur peut configurer FontSmoothingType via le fichier ICA. Cela prévaut sur la valeur définie dans la section [WFClient]. Si le serveur définit la valeur sur 0, la préférence locale est déterminée par un autre paramètre dans la section [WFClient] :
FontSmoothingTypePref = number

où number peut prendre l'une des valeurs suivantes :

Valeur	Comportement
0	Aucun lissage
1	

Valeur	Comportement
2	Lissage standard
3	Lissage ClearType (subpixellaire horizontal) (comportement par défaut)

Configuration de la redirection de dossiers spéciaux

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

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

La redirection de dossiers spéciaux vous permet d'indiquer les emplacements des dossiers spéciaux d'un utilisateur afin que ceux-ci demeurent à un emplacement fixe sur les différents types de serveur et configurations de batteries de serveurs. Ceci est particulièrement 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

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

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

   SFRAllowed = True

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

   DesktopFolder = desktop

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

   DesktopFolder = $HOME/.ICAClient/desktop

   - Vous pouvez indiquer n'importe quel composant du chemin sous forme de variable d'environnement, par exemple $HOME.
   - Vous pouvez indiquer des valeurs pour ces deux paramètres.
   - Les répertoires que vous indiquez doivent être disponibles via le mappage des machines clientes ; ils doivent donc se trouver dans la sous-arborescence d'une machine cliente mappée.
   - Vous devez utiliser les lettres de lecteur C ou suivantes.

Configuration de la 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 (Hypertext Transfer Protocol) ;
- HTTPS (Secure Hypertext Transfer Protocol) ;
- RTSP (Real Player) ;
- RTSPU (Real Player) ;
- PNM (Real Players plus anciens).

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

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

> **Remarque**
>
> Pour de plus amples informations sur RealPlayer pour Linux, visitez http://www.real.com/resources/unix/.

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

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

   Command=command

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

   $ICAROOT/nslaunch netscape,firefox,mozilla

   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

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

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. De plus, vous pouvez indiquer plusieurs noms de répertoire sous forme d'une liste de noms séparés par deux points. Si ces paramètres ne sont pas spécifiés, le $PATH utilisateur actuel est employé.

Pour désactiver la redirection de contenu serveur vers client à partir de Receiver

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

Contrôle du comportement du clavier

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

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

Utilisation de xcapture

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

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

Pour lancer xcapture à partir de la ligne de commande

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

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.

Reconnexion automatique des utilisateurs

Cette rubrique décrit la fonction HDX Broadcast - Reconnexion automatique des clients. Citrix recommande d'utiliser cette dernière en conjonction 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 de reconnexion automatique des clients HDX Broadcast, Citrix Receiver peut détecter les déconnexions de session involontaires et reconnecter automatiquement les utilisateurs à leur session.

Lorsque cette fonctionnalité est activée sur le serveur, les utilisateurs n'ont pas besoin de se reconnecter manuellement pour continuer à travailler. Citrix Receiver 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, Citrix Receiver 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 XenApp et XenDesktop.

Garantir la fiabilité de session

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

Grâce à la fonctionnalité de fiabilité de session HDX Broadcast, la fenêtre d'une application publiée est toujours affichée même si la connexion à l'application subit des interruptions. Par exemple, les utilisateurs dotés de connexions sans fil entrant

dans un tunnel peuvent perdre leur connexion à l'entrée d'un tunnel, pour la reprendre à la sortie. Durant l'interruption, les données de l'utilisateur, les touches sur lesquelles ils appuient et d'autres interactions sont toutes stockées, et l'application semble figée. Lorsque la connexion est rétablie, ces interactions sont réappliquées dans l'application.

Lorsque la reconnexion automatique des clients et la fiabilité de session sont configurées, la fiabilité de session a priorité s'il y a un problème de connexion. La fiabilité de session essaye de rétablir une connexion à la session existante. Il peut s'écouler jusqu'à 25 secondes avant qu'un problème de connexion soit détecté, et la tentative de reconnexion peut prendre beaucoup de temps (la valeur par défaut est de 180 secondes). 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 Receiver ne peuvent pas remplacer les réglages du serveur. Pour plus d'informations sur ces derniers, veuillez consulter la documentation relative à XenApp et XenDesktop.

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.

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 XenApp ou XenDesktop 7.8 (ou version ultérieure). Elle est désactivée par défaut.

Pour mettre la fonctionnalité en service :

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

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

Conseil

Reportez-vous à la section *Valeurs de souris relative alternatives* pour de plus amples informations sur la mise en service des fonctionnalités de souris relative.

Pour activer la fonctionnalité :

Tapez Ctrl/F12.

Une fois que la fonctionnalité est activée, tapez de nouveau sur Ctrl/F12 pour synchroniser la position du pointeur de la souris avec le client (les positions du pointeur du client et du serveur ne sont pas synchronisées lors de l'utilisation de la 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 Citrix Receiver. Les valeurs pour **RelativeMouseOnShift** et **RelativeMouseOffShift** définissent les touches de modification à utiliser et sont répertoriées sous l'en-tête [Hotkey Shift States].

Sécuriser

Jul 10, 2017

Dans cet article :

- Connexion via un serveur proxy
- Connexion avec Secure Gateway ou le Relais SSL Citrix
- Connexion via NetScaler Gateway

Pour sécuriser les communications entre votre batterie de serveurs et Citrix Receiver, vous pouvez intégrer vos connexions Citrix Receiver à la batterie de serveurs grâce à un large choix de technologies de sécurité, dont :

- Un serveur proxy SOCKS ou serveur proxy sécurisé (également appelé serveur de sécurité, serveur proxy HTTPS ou serveur proxy de tunneling TLS). Vous pouvez utiliser les serveurs proxy pour limiter l'accès à l'intérieur et à l'extérieur de votre réseau, et pour gérer les connexions entre Receiver et les serveurs. Receiver prend en charge les protocoles de proxy SOCKS et de proxy sécurisé.
- Secure Gateway ou solutions de relais SSL avec protocoles TLS. Les versions TLS 1.0 à 1.2 sont prises en charge.
- 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 Receiver 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.

Connexion via un 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 Citrix Receiver et votre déploiement Citrix XenApp ou Citrix XenDesktop. Citrix Receiver prend en charge le protocole SOCKS, de même que Secure Gateway et le Relais SSL Citrix, le protocole proxy sécurisé et l'authentification Stimulation/Réponse Windows NT (NTLM).

La liste des types de proxy pris en charge est limitée aux types Auto, None et Wpad par le contenu des fichiers Trusted_Regions.ini et Untrusted_Regions.ini. Si vous devez utiliser 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.

Connexion via un 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 la fonctionnalité NTLM requiert la présence de la bibliothèque OpenSSL (libcrypto.so) sur la machine utilisateur.

Cette bibliothèque est généralement incluse dans les distributions Linux. Le cas échéant, elle est également téléchargeable à partir du site http://www.openssl.org/.

Connexion avec Secure Gateway ou le Relais SSL Citrix

Vous pouvez intégrer Receiver avec Secure Gateway ou le service Relais SSL (Secure Sockets Layer) Citrix. Receiver prend en charge le protocole TLS. TLS (Transport Layer Security) est la dernière version normalisée du protocole SSL. Le groupe de travail Internet Engineering Taskforce (IETF) l'a rebaptisé TLS lorsqu'il est devenu responsable du développement de SSL sous la forme d'une norme ouverte. TLS garantit la sécurité des communications de données grâce à l'authentification des serveurs, au cryptage du flux de données et aux contrôles d'intégrité des messages. Certaines organisations, notamment des organisations gouvernementales américaines, requièrent l'utilisation du protocole TLS pour la sécurisation de leurs communications de données. Ces organisations peuvent nécessiter l'utilisation d'une cryptographie validée, comme la norme FIPS 140 (Federal Information Processing Standard). La norme FIPS 140 est une norme de cryptographie.

Connexion avec la passerelle Secure Gateway

Vous pouvez utiliser la passerelle Secure Gateway en mode Normal ou en mode Relais afin de fournir un canal sécurisé de communication entre Citrix Receiver et le serveur. Il n'est pas nécessaire de configurer Citrix Receiver si vous utilisez la passerelle Secure Gateway en mode Normal et si les utilisateurs se connectent via l'Interface Web.

Citrix Receiver utilise des paramètres configurés à distance sur le serveur exécutant l'Interface Web pour se connecter aux serveurs exécutant Secure Gateway. Pour plus d'informations sur la configuration des paramètres de serveur proxy pour Citrix Receiver, veuillez consulter la documentation de l'Interface Web.

Si le proxy Secure Gateway est installé sur un serveur dans le réseau sécurisé, vous pouvez l'utiliser en mode Relais. Pour plus d'informations, veuillez consulter la documentation de XenApp (Secure Gateway).

Si vous utilisez le mode Relais, le serveur Secure Gateway fonctionne comme un serveur proxy. Dans ce cas, vous devez configurer Citrix Receiver pour qu'il utilise :

- le nom de domaine complet du serveur Citrix Secure Gateway ;
- le numéro de port du serveur Citrix Secure Gateway. Veuillez noter que le mode Relais n'est pas pris en charge par Secure Gateway, version 2.0.

Le nom de domaine complet (FQDN) doit contenir, dans l'ordre, les trois composants suivants :
- Nom d'hôte
- Domaine intermédiaire
- Domaine de tête

Par exemple : my_computer.my_company.com est un nom de domaine complet car il liste (dans cet ordre) un nom d'hôte (mon_ordinateur), un domaine intermédiaire (mon_entreprise) et un domaine de niveau supérieur (com). La combinaison du domaine intermédiaire et du domaine de tête (mon_entreprise.com) est généralement appelée nom de domaine.

Connexion avec le Relais SSL Citrix

Par défaut, le Relais SSL Citrix utilise le port TCP 443 du serveur XenApp 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 auprès de Citrix Receiver.

Le Relais SSL Citrix vous permet de sécuriser les communications suivantes.

- Entre une machine utilisateur et un serveur sur lesquels TLS est activé.
- Avec l'Interface Web, entre le serveur XenApp et le serveur Web.

Pour obtenir des informations sur la configuration et l'utilisation du Relais SSL en vue de sécuriser l'installation, veuillez consulter la documentation de XenApp. Pour obtenir des informations sur la configuration de l'Interface Web en vue d'utiliser le cryptage TLS, veuillez consulter la documentation de l'Interface Web.

Configuration et activation de TLS

Vous pouvez contrôler les versions du protocole TLS qui peuvent être négociées en ajoutant les options de configuration suivantes dans la section [WFClient]:

- MinimumTLS=1.0
- MaximumTLS=1.2

Il s'agit des valeurs par défaut, qui sont implémentées en code. Modifiez-les comme bon vous semble.

Remarque : ces valeurs seront lues chaque fois qu'un programme démarre. Si vous les modifiez après le démarrage de selfservice ou storebrowse, vous devez taper : **killall AuthManagerDaemon ServiceRecord selfservice storebrowse.**

Remarque : cette version de Citrix Receiver pour Linux désactive l'utilisation du protocole SSLv3.
Pour les connexions TCP entre Receiver et XenApp/XenDesktop, Citrix Receiver pour Linux prend en charge TLS 1.0, 1.1 et 1.2 avec les suites de chiffrement suivantes :

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Pour les connexions UDP entre Receiver et XenApp/XenDesktop, Citrix Receiver pour Linux prend en charge DTLS 1.0 avec les suites de chiffrement suivantes :

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Installation de 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, Citrix Receiver prend en charge les certificats suivants.

Certificat	Autorité émettrice
Class4PCA_G2_v2.pem	VeriSign Trust Network
Class3PCA_G2_v2.pem	VeriSign Trust Network

BTCTRoot.pem	Baltimore Cyber Trust Root
GTECTGlobalRoot.pem	GTE Cyber Trust Global Root
Pcs3ss_v4.pem	Class 3 Public Primary Certification Authority
GeoTrust_Global_CA.pem	GeoTrust
DigiCertGlobalRootCA.pem	DigiCert Global Root CA

Il n'est pas nécessaire d'obtenir et d'installer des certificats racine sur les machines utilisateur pour pouvoir utiliser des certificats émis par ces autorités de certification. Cependant, si vous choisissez d'utiliser une autorité de certification différente, vous devez alors obtenir un certificat racine auprès de celle-ci, que vous installez ensuite sur chaque machine utilisateur.

Citrix Receiver pour Linux prend en charge les clés RSA de longueur 1024, 2048 et 3072. Les certificats racine avec des clés RSA de longueur de 4 096 bits sont aussi pris en charge.

Remarque : Receiver pour Linux 13.0 utilise c_rehash à partir de la machine locale. La version 13.1 et les versions suivantes utilisent l'outil ctx_rehash comme décrit dans les étapes suivantes.

Utiliser un certificat racine

Si vous avez besoin d'authentifier un certificat de serveur qui a été émis par une autorité de certification et qui n'a pas encore été approuvé par la machine utilisateur, suivez les instructions suivantes avant d'ajouter un magasin StoreFront.

1. Obtenez le certificat racine au format PEM.
   Conseil : si vous ne trouvez aucun certificat de ce format, utilisez l'utilitaire openssl pour convertir un certificat au format CRT en un fichier .pem.
2. En tant qu'utilisateur qui a installé le package (généralement racine) :
   1. Copiez le fichier dans $ICAROOT/keystore/cacerts.
   2. Exécutez la commande suivante :
      $ICAROOT/util/ctx_rehash

Utiliser un certificat intermédiaire

Si votre serveur StoreFront ne peut pas fournir les certificats intermédiaires correspondant au certificat qu'il utilise, ou que vous devez installer 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 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) :
   1. Copiez le ou les fichiers dans $ICAROOT/keystore/intcerts.
   2. Exécutez la commande suivante en tant qu'utilisateur qui a installé le package :

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

Activation de la prise en charge des cartes à puce

Citrix Receiver pour Linux assure la prise en charge de différents lecteurs de carte à puce. Si la prise en charge des cartes à puce est activée à la fois sur le serveur et sur Receiver, vous pouvez utiliser des cartes à puce aux fins suivantes :

- Authentification d'ouverture de session par carte à puce. Servez-vous de cartes à puce pour authentifier les utilisateurs auprès des serveurs Citrix XenApp.
- Prise en charge des applications recourant à une carte à puce. Autorisez les applications recourant à une carte à puce à 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.
- Vous devez installer le pilote approprié au lecteur de carte à puce.
- Vous devez installer le package PC/SC Lite.
- Vous devez installer et exécuter le démon pcscd, qui fournit le middleware permettant d'accéder à la carte à puce à l'aide de PC/SC.
- Sur un système 64 bits, les versions 64 bits et 32 bits du package « libpscslite1 » doivent être présentes.

Important : vous utilisez le terminal SunRay avec le logiciel serveur SunRay version 2.0 ou ultérieure, vous devez installer le pack de contournement SRCOM PC/SC, disponible au téléchargement à l'adresse http://www.sun.com/.
Pour plus d'informations sur la configuration de la prise en charge des cartes à puce sur vos serveurs, veuillez consulter la documentation de XenDesktop et XenApp.

Connexion via NetScaler Gateway

Citrix NetScaler Gateway (anciennement Access Gateway) sécurise les connexions aux magasins StoreFront, et permet aux administrateurs de contrôler, de façon détaillée, l'accès utilisateur aux bureaux et applications.

Pour se connecter à des bureaux et des applications via NetScaler Gateway

1. Spécifiez l'URL NetScaler Gateway qui vous a été fournie par votre administrateur. Vous pouvez effectuer cette opération de l'une des manières suivantes :
   - La première fois que vous utilisez l'interface utilisateur en libre-service, vous êtes invité à entrer l'adresse URL dans la boîte de dialogue Ajouter compte.
   - Lorsque vous utilisez l'interface utilisateur en libre-service ultérieurement, entrez l'URL en cliquant sur Préférences > Comptes > Ajouter .
   - Si vous établissez une connexion avec la commande storebrowse, entrez l'adresse URL sur la ligne de commande.

   L'URL spécifie la passerelle et, éventuellement, un magasin spécifique :

   - Pour vous connecter au premier magasin que Receiver détecte, utilisez une URL au format https://passerelle.société.com.
   - Pour vous connecter à un magasin spécifique, utilisez une URL au format https://passerelle.société.com? . Veuillez noter que 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 probablement 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 NetScaler Gateway.
   Une fois l'authentification terminée, vos bureaux et applications sont affichés.

Dépannage

Jul 10, 2017

Cet article contient des informations destinées à aider les administrateurs à résoudre tous les problèmes rencontrés avec Citrix Receiver pour Linux.

- Problèmes de connexion
- Problèmes d'affichage
- Problèmes relatifs au navigateur
- Autres problèmes
- Erreurs de configuration des connexions
- Erreurs de configuration dans le fichier wfclient.ini
- Erreurs de fichiers PAC
- Autres erreurs
- Envoi d'informations de diagnostic à l'assistance Citrix

Problèmes de connexion

Vous pouvez rencontrer les problèmes de connexion suivants.

Le lecteur Windows Media ne parvient pas à lire certains formats de fichiers.

Citrix Receiver ne dispose peut-être pas des plug-ins GStreamer requis pour traiter un format demandé. Lorsque cela se produit, le serveur demande généralement un format différent. Il arrive parfois que la vérification de la présence d'un plug-in approprié indique à tort qu'un tel plug-in est effectivement présent. Cela est généralement détecté et entraîne l'affichage d'une boîte de dialogue d'erreur sur le serveur indiquant que le Lecteur Windows Media a rencontré un problème lors de la lecture d'un fichier. Il suffit généralement de lire de nouveau le fichier dans la session car cela entraîne le rejet du format par Citrix Receiver, et 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 n'est pas détectée et le fichier n'est pas lu correctement, bien que l'indicateur de progression avance comme prévu dans le Lecteur Windows Media.

Pour éviter l'affichage de cette boîte de dialogue d'erreur ou l'échec de la lecture dans les sessions futures :

1. Ajoutez de façon temporaire l'option de configuration « SpeedScreenMMAVerbose=On » à la section [WFClient] de $Home/.ICAClient/wfclient.ini, par exemple.
2. Redémarrez WFICA à partir d'un libre-service qui a été démarré à partir d'un terminal.
3. Lisez une vidéo qui génère cette erreur.
4. Notez (dans la sortie de traçage) le type mime associé à la trace du plug-in manquant, ou le type mime qui devrait être pris en charge mais dont la lecture échoue (par exemple, "video/x-h264..").
5. Modifiez $ICAROOT/config/MediaStreamingConfig.tbl ; sur la ligne sur laquelle figure le type mime, insérez un '?' entre ':' et le type mime. Cela désactive le format.
6. Répétez les étapes 2 à 5 (ci-dessus) pour tout autre format multimédia qui génère cette erreur.
7. Distribuez ce MediaStreamingConfig.tbl modifié aux autres machines qui disposent du même ensemble de plug-ins GStreamer.

Remarque : éventuellement, après avoir identifié le type mime, il est possible d'installer un plug-in GStreamer pour le décoder.

Impossible de se connecter correctement à une ressource publiée ou à une session

de bureau

Si, lors de l'établissement d'une connexion à un serveur Windows, une boîte de dialogue présente le message « Connecting to server... » (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 la gestion des licences, consultez la section Obtenir une licence pour votre produit.

Les connexions se soldent quelquefois par un échec lors des tentatives de reconnexion à des sessions

Il peut arriver que la reconnexion à une session avec un nombre de couleurs plus élevé que celui exigé par Receiver entraîne l'échec de la connexion. Ce problème est dû à un manque de mémoire disponible sur le serveur. En cas d'échec de la reconnexion, Receiver tente d'utiliser le nombre de couleurs initial. Sinon, le serveur tente de démarrer une nouvelle session avec le nombre de couleurs requis, en laissant la session initiale dans l'état déconnecté. La deuxième connexion peut toutefois échouer si la mémoire disponible sur le serveur est toujours insuffisante.

Impossible d'établir une connexion avec un serveur à l'aide de son nom Internet complet

Citrix vous recommande de configurer le DNS (Domain Name Server) sur votre réseau afin de pouvoir résoudre le nom des serveurs auxquels vous souhaitez vous connecter. Si le DNS n'est pas configuré, vous ne pourrez peut-être pas résoudre le nom du serveur en adresse IP. Vous pouvez également spécifier le serveur à l'aide de son adresse IP, plutôt que son nom, mais veuillez noter que les connexions TLS requièrent un nom de domaine complet et non une adresse IP.

Un message d'erreur de type « Proxy detection failure » (Échec de détection du proxy) s'affiche au moment de la connexion

Si votre connexion est configurée de manière à utiliser la détection automatique des serveurs proxy et qu'un message d'erreur de type « Proxy detection failure: Javascript error » (Échec de détection du proxy : erreur JavaScript) s'affiche lorsque vous tentez de vous connecter, copiez le fichier wpad.dat dans le répertoire $ICAROOT/util. Exécutez la commande suivante, où NomHôte désigne le nom d'hôte du serveur auquel vous tentez de vous connecter :

cat wpad.dat | ./pacexec pac.js FindProxyForURL http://NomHôte NomHôte 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 ...;

Les sessions sont très lentes à démarrer

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 contourner le problème, exécutez un démon entropy-generating tel que rngd (basé sur le matériel) ou haveged (de Magic Software).

Je veux configurer un paramètre 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=
```

Pour configurer deux ports série ou plus, ajoutez les entrées suivantes dans le fichier de configuration $ICAROOT/config/module.ini :

```
LastComPortNum=2
ComPort1=
ComPort2=
```

Erreurs de connexion

Un message d'erreur indiquant « Erreur de connexion : Une erreur de protocole s'est produite lors de la communication avec le service Authentication Service » s'affiche. Plusieurs problèmes peuvent être à l'origine de cette condition :

- L'ordinateur local et l'ordinateur distant ne peuvent pas négocier un protocole TLS commun.
- L'ordinateur distant demande un certificat client inapproprié. IIS ne doit « accepter » ou « demander » de certificats que pour « Citrix/Authentication/Certificate ».
- Autres problèmes.

Problèmes d'affichage

Pourquoi ai-je des problèmes de screen tearing ?

Le screen tearing (déchirure d'écran) se produit lorsque deux images différentes (ou plus) apparaissent simultanément sur l'écran, en blocs horizontaux. Cela est plus fragrant dans les zones larges sur lesquelles du contenu est fréquemment modifié. Bien que les données soient capturées sur le VDA de manière à éviter le tearing, et qu'elles soient transmises au client de manière à ne pas introduire de tearing, X11 (le sous-système graphique de Linux/Unix) ne fournit pas de méthode cohérente permettant de dessiner sur l'écran de manière à éviter le tearing.

Pour éviter le screen tearing, Citrix préconise l'approche standard qui consiste à synchroniser le dessin de l'application avec le dessin de l'écran ; en d'autres termes, attendre vsvnc pour initier le dessin de l'image suivante. Il existe un certain nombre d'options lors de l'utilisation de Linux ; elles dépendent du matériel graphique dont vous disposez sur le client et du gestionnaire de fenêtres que vous utilisez. Ces options sont divisées en deux groupes de solutions :

- Paramètres du processeur graphique X11
- Utilisation d'un gestionnaire de composition

Configuration du processeur graphique X11

Pour les processeurs Intel HD Graphics, créez un fichier dans xorg.conf.d appelé **20-intel.conf** avec le contenu suivant :

```
Section "Device"
        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). Vous devrez installer « ComprizConfig Settings Manager. »

  Exécutez « ComprizConfig Settings Manager »
  Sous « General->Composition », décochez « Undirect Fullscreen Windows »
  Remarque : « ComprizConfig Settings Manager » doit être utilisé 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

Des touches incorrectes s'affichent lorsque j'utilise le clavier

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 lors du déplacement de fenêtres transparentes

Certains gestionnaires de fenêtres signalent constamment la nouvelle position de la fenêtre lors des déplacements, 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

Receiver crée des icônes de fenêtre compatibles avec la plupart des gestionnaires de fenêtres, mais qui ne le sont pas complètement avec la convention de communication entre clients X.

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.

Problèmes de visibilité 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.

Problèmes de clignotement des couleurs à l'écran

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 peuvent se mettre 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.

Changement rapide de couleurs avec les affichages 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 rapidement 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, Receiver 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 des caractères japonais sur l'écran

Receiver utilise le codage de caractères EUC-JP ou UTF-8 pour le japonais tandis que le serveur applique le codage de caractères SJIS. Receiver ne procède à aucune conversion entre ces jeux de caractères. Cela peut donc entraîner des problèmes d'affichage de fichiers enregistrés sur le serveur et ouverts localement ou inversement (des fichiers locaux visualisés à partir du serveur). Ce problème concerne également les caractères japonais contenus dans les paramètres utilisés dans le passage de paramètres étendu.

Création d'une session s'étendant sur plusieurs écrans

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. Pour de plus amples informations, reportez-vous à la section Améliorer l'expérience utilisateur.

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. S'il s'agit de la valeur complète de l'option, wfica se ferme ensuite.

Si o est spécifié, la fenêtre de la session prend l'attribut de redirection override-redirect.

Attention : il est déconseillé d'appliquer cette valeur d'option. Elle doit être spécifiée en dernier recours, pour être utilisée avec des gestionnaires de fenêtres non coopératifs. Dans ce cas, la fenêtre de la session n'est pas visible pour le gestionnaire de fenêtres, ne possède pas d'icône associée et ne peut pas être réempilée. Elle ne disparaît qu'une fois la session fermée.
Si a est spécifié, Receiver tente de créer une session couvrant tous les moniteurs.

Receiver suppose que le reste de la valeur de l'option -span est une liste de numéros d'écrans. Une valeur unique sélectionne un écran précis, deux valeurs définissent des écrans situés dans les coins supérieur gauche et inférieur droit de la zone requise, quatre spécifient des écrans situés sur les bords supérieur, inférieur, gauche et droit de la zone.

En supposant que le paramètre o n'a pas été spécifié, wfica utilise le message _NET_WM_FULLSCREEN_MONITORS pour demander une configuration de fenêtre appropriée au gestionnaire de fenêtres, si celui-ci est pris en charge. Sinon, il utilise les indicateurs de taille et de position pour demander la configuration souhaitée.

Vous pouvez exécuter la commande suivante pour tester la prise en charge du gestionnaire de fenêtres :

xprop -root | grep _NET_WM_FULLSCREEN_MONITORS

Si la commande ne génère aucune sortie, cela signifie que le gestionnaire n'est pas pris en charge. Dans ce cas, vous devrez peut-être utiliser une fenêtre de type override-redirect. Pour configurer une fenêtre de type override-redirect, utilisez -span o.

Pour créer une session couvrant plusieurs écrans à partir de la ligne de commande :

1. À l'invite de commandes, entrez la commande suivante :
   /opt/Citrix/ICAClient/wfica -span h

   La liste des numéros des écrans connectés à la machine utilisateur est imprimée dans stdout et wfica se ferme.

2. Prenez note de ces numéros d'écrans.
3. À l'invite de commandes, entrez la commande suivante :
   /opt/Citrix/ICAClient/wfica -span [w[,x[,y,z]]]

   où w, x, y et z correspondent aux numéros des écrans obtenus à l'étape 1 ci-dessus et où la valeur unique w indique un écran unique, deux valeurs w et x définissent des écrans situés dans les coins supérieur gauche et inférieur droit de la zone requise et quatre valeurs w, x, y et z spécifient des écrans situés sur les bords supérieur, inférieur, gauche et droit de la zone.

   Important : vous devez définir la variable WFICA_OPTS avant de démarrer selfservice ou de vous connecter à l'interface Web 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"
   Notez que cette modification s'applique à la fois aux sessions XenApp et XenDesktop.
   Si vous avez déjà démarré selfservice ou storebrowse, vous devez supprimer les processus qu'ils ont démarrés pour que la nouvelle variable d'environnement prenne effet. Supprimez-les avec :
   killall AuthManagerDaemon ServiceRecord storebrowse

Je ne peux pas sortir d'une session plein écran afin d'utiliser des applications locales ou une autre session

Cela 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 contourner ce problème, utilisez CTRL+F2 pour désactiver temporairement la fonctionnalité Transparence du clavier jusqu'à ce que le focus revienne à la fenêtre de session. Vous pouvez également définir TransparentKeyPassthrough sur No dans $ICAROOT/config/module.ini. Cela désactive la fonctionnalité Transparence du clavier, toutefois vous devrez peut-être remplacer le fichier ICA en ajoutant ce paramètre dans le fichier All_regions.ini.

Problèmes relatifs au navigateur

Lors de l'activation d'un lien dans une session Windows, le contenu s'affiche dans un navigateur local

La redirection de contenu serveur vers client est activée dans le fichier wfclient.ini. Cette situation entraîne l'exécution d'une application locale. Pour désactiver la redirection de contenu serveur vers client, consultez la section Définir la redirection de contenu du serveur vers le client.

Lors de l'accès à des ressources publiées, le 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. Si vous établissez une connexion via Interface Web, il se peut que vous accédiez à la page d'accueil d'Interface Web présentant la liste des ressources. 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.

Pour configurer un autre navigateur à des fins d'utilisation avec l'Interface Web

Les étapes varient d'un navigateur à l'autre, mais vous pouvez configurer les types de données MIME dans le navigateur afin que le fichier $ICAROOT/wfica soit exécuté en tant qu'application d'assistance lorsque le navigateur rencontre des données de type MIME application/x-ica ou un fichier .ica.

Le programme d'installation ne prend pas en charge un navigateur spécifique

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.

Lorsque je lance des bureaux ou applications dans Firefox, rien ne se produit

Essayez d'activer le plug-in ICA.

Le plug-in ICA est activé dans Firefox, toutefois les sessions de bureau et d'application ne démarrent pas

Essayez de désactiver le plug-in ICA.

Autres problèmes

Vous pouvez rencontrer les problèmes supplémentaires suivants.

Je veux savoir si le serveur a demandé à Receiver de fermer une session

Vous pouvez utiliser le programme *wfica* afin de consigner une entrée chaque fois que Receiver 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. Cela permet la journalisation des messages qui ont la priorité LOG_INFO ou une priorité plus élevée. La valeur par défaut pour *SyslogThreshold* est de 4 (=LOG_WARNING).

De même, pour que *wfica* envoie les informations en tant qu'erreur standard, ajoutez *PrintLogThreshold* avec la valeur 6 à la section [WFClient]. La valeur par défaut pour *PrintLogThreshold* est de 0 (=LOG_EMERG).

Reportez-vous à la documentation du système d'exploitation pour obtenir des instructions sur la configuration de votre système syslog.

Les paramètres de mon fichier de configuration ne fonctionnent plus

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.

Problèmes survenant lors de l'exécution d'applications publiées ayant accès à un port série

Si une application publiée doit accéder 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 contourner 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.

Impossible de démarrer Receiver

Si Receiver ne démarre pas et que 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 Receiver 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 Receiver 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 Receiver à l'emplacement par défaut. Pour de plus amples informations sur l'installation de Receiver, consultez la section Téléchargement et installation de Receiver pour Linux.

  Si Receiver était installé à l'emplacement par défaut, supprimez le répertoire /opt/Citrix/ICAClient où $HOME/ICAClient/platform avant de procéder à la réinstallation.

Dysfonctionnement des 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. Cela mappe la combinaison de touches locales Alt+Ctrl+F1 sur Alt+F1 :
  - Modifiez Hotkey1Shift=Ctrl+Maj sur Hotkey1Shift=Alt+Ctrl.
- Le mode Direct sur le clavier envoie toutes les combinaisons de touches directement vers le serveur. Elles ne sont pas traitées localement. Pour configurer le mode Direct, dans la section [WFClient] de $HOME/.ICAClient/wfclient.ini, définissez TransparentKeyPassthrough sur Remote.
- Reconfigurez le gestionnaire de fenêtres afin qu'il supprime les combinaisons de touches par défaut.

Je souhaite activer un 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.

Je veux trouver le numéro de version de Citrix SSLSDK ou OpenSSL

Pour confirmer le numéro de version de Citrix SSLSDK ou OpenSSL que vous exécutez, vous pouvez exécuter la commande suivante :
strings libctxssl.so | grep "Citrix SSLSDK"
Vous pouvez également exécuter cette commande sur AuthManagerDaemon ou PrimaryAuthManager

Je veux utiliser un clavier japonais sur le client

Pour configurer l'utilisation d'un clavier japonais, mettez à jour l'entrée suivante dans le fichier de configuration wfclient.ini :
KeyboardLayout=Japanese (JIS)

Je veux utiliser un clavier ABNT2 sur le client

Pour configurer l'utilisation d'un clavier ABNT2, mettez à jour l'entrée suivante dans le fichier de configuration wfclient.ini :
KeyboardLayout=Brazilian (ABNT2)

Certaines touches sur mon 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.

Erreurs de configuration des connexions

Ces erreurs peuvent se produire suite à une entrée de connexion mal configurée.

E_MISSING_INI_SECTION - Verify the configuration file: "...". The section "..." is missing in the configuration file. (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 - Verify the configuration file: "...". The section "..." must contain an entry "...". (La section « ... » doit contenir une entrée « ... ».)

Le fichier de configuration a été modifié de manière incorrecte ou est endommagé.

E_INI_VENDOR_RANGE - Verify the configuration file: "...". The X server vendor range "..." in the configuration file is invalid. (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 - Cannot write file: "..." (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 - Cannot create file: "..." (E_CANNOT_CREATE_FILE : impossible de créer le fichier : « ... ».)

Un problème s'est produit lors de la création d'une nouvelle base de données de connexions.

E_PNAGENT_FILE_UNREADABLE - Cannot read XenApp file "...": No such file or directory. (E_PNAGENT_FILE_UNREADABLE : impossible de lire le fichier XenApp « ... » : aucun fichier ou répertoire de ce nom n'existe.)

— Ou —

Cannot read XenApp file "...": Permission denied. (Impossible de lire le fichier XenApp « ... » : Permission refusée.)

Vous tentez d'accéder à une ressource via un menu ou un élément de bureau, mais le fichier XenApp lié à la ressource n'est pas disponible. Actualisez la liste des ressources publiées en sélectionnant Application Refresh dans le menu View, puis tentez d'accéder à nouveau à la ressource. Si l'erreur persiste, vérifiez les propriétés de l'icône de bureau ou de l'élément de menu, ainsi que le fichier XenApp 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.

Proxy detection failure: Improper auto-configuration URL. (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.

Proxy detection failure : .PAC script HTTP download failed: Connect failed. (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.

Proxy detection failure: .PAC script HTTP download failed: Path not found. (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. Corrigez cette erreur sur le serveur ou reconfigurez le navigateur.

Proxy detection failure: .PAC script HTTP download failed. (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.

Proxy detection failure: Empty auto-configuration script. (Échec de détection du proxy : script de configuration automatique vide.)

Le fichier PAC est vide. Soit vous corrigez cette erreur sur le serveur, soit vous reconfigurez le navigateur.

Proxy detection failure: No JavaScript support. (Échec de détection du proxy : aucune prise en charge JavaScript.)

Le fichier exécutable PAC ou le fichier texte pac.js est manquant. Réinstallez Receiver.

Proxy detection failure: JavaScript error. (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 Problèmes de connexion.

Proxy detection failure: Improper result from proxy auto-configuration script. (Échec de détection du proxy : résultats erronés provenant du script de configuration automatique vide.)

Une réponse mal formulée a été envoyée par le serveur. Soit vous corrigez cette erreur sur le serveur, soit vous reconfigurez le navigateur.

Autres erreurs

Cette rubrique dresse la liste d'autres messages d'erreur courants pouvant s'afficher lors de l'utilisation de Receiver.

An error occurred. The error code is 11 (E_MISSING_INI_SECTION). Please refer to the documentation. Exiting. (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 Receiver 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 - The option "..." is invalid. (E_BAD_OPTION : l'option « ... » n'est pas valide.)

Argument manquant pour l'option « ... ».

E_BAD_ARG - The option "..." has an invalid argument: "...". (E_BAD_ARG : l'option « ... » comporte un argument non valide : « ... ».)

Argument non valide spécifié pour l'option « ... ».

E_INI_KEY_SYNTAX - The key "..." in the configuration file "..." is invalid. (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 nouveau fichier de configuration.

E_INI_VALUE_SYNTAX - The value "..." in the configuration file "..." is invalid. (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 nouveau fichier de configuration.

E_SERVER_NAMELOOKUP_FAILURE - Cannot connect to server "...". (E_SERVER_NAMELOOKUP_FAILURE : la connexion au serveur « ... » a échoué.)

Impossible de résoudre le nom du serveur.

Cannot write to one or more files: "...". Correct any disk full issues or permissions problems and try again. (Impossible d'écrire dans un ou plusieurs fichiers : « ... ». Corrigez les éventuels problèmes de disques saturés ou de permissions insuffisantes, puis réessayez.)

Recherchez des problèmes de disques saturés ou de permissions insuffisantes. Si un problème est détecté puis résolu, réessayez l'opération ayant généré le message d'erreur.

Server connection lost. Rétablissez la connexion, puis réessayez. These files might be missing data: "...". (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.

Envoi d'informations de diagnostic à l'assistance Citrix

Si vous rencontrez des problèmes liés à l'utilisation de Receiver, 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 Receiver

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 Receiver 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.

SDK et API

Jul 10, 2017

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 XenApp ou XenDesktop. Cette version du SDK prend en charge l'écriture de nouveaux canaux virtuels pour Receiver pour Linux. Si vous souhaitez écrire des pilotes virtuels pour d'autres plates-formes clientes, contactez 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 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 sur le SDK, veuillez consulter Citrix Virtual Channel SDK for Citrix Receiver for Linux 13.6.

Paramètres et références de ligne de commande

Pour plus d'informations sur les paramètres et références de ligne de commande, consultez Citrix Receiver for Linux 13.6 Command Reference.

SDK d'optimisation de la plate-forme

Dans le cadre de l'initiative HDX SoC pour Citrix Receiver pour Linux, nous avons développé le « SDK d'optimisation de la plate-forme » afin d'offrir un écosystème d'appareils à faible coût, faible consommation et très performants dans des formats innovants.

Le SDK d'optimisation de la plate-forme peut être utilisé par les développeurs désireux d'améliorer les performances des appareils Linux en leur permettant de créer des extensions de plug-in pour le composant de moteur ICA (wfica) de Citrix Receiver pour Linux. Les plug-ins sont intégrés en tant que bibliothèques partageables qui sont chargées dynamiquement par wfica. Ces plug-ins peuvent vous aider à optimiser les performances de vos appareils Linux en activant les fonctions suivantes :

- Décodage accéléré des données JPEG et H.264 utilisées pour afficher l'image de la session
- Contrôle de l'allocation de mémoire utilisée pour afficher l'image de la session
- Amélioration des performances en prenant le contrôle de l'affichage de bas niveau de l'image de la session
- Services de sortie graphique et d'entrée utilisateur pour les environnements de système d'exploitation qui ne prennent pas en charge X11

Pour plus d'informations, consultez la section Citrix Receiver pour Linux - SDK d'optimisation de la plate-forme.

Certificate Identity Declaration SDK

Credential Insertion SDK